Math. Nachr. **206** (1999), 85 – 110

Explicit Universal Deformations of Even Galois Representations

By GEBHARD BÖCKLE of Mannheim

(Received January 7, 1997)
(Revised Version July 24, 1997)

Abstract. We investigate the case of deformations of even Galois representations. Our methods are the group theoretic ones mainly developed by NIGEL BOSTON to study odd representations. We present conditions for Borel and tame cases under which the universal deformation ring is isomorphic to $\mathbb{Z}_p[[T]]$ and where we compute the universal deformation explicitly. Furthermore we produce a family of examples of totally real S_3 extensions which satisfy the above conditions in the tame case and we give examples in the Borel case. Finally we study the change of the deformation space under enlarging the ramification and thus give an example of an even representation that is not twist – finite.

1. Introduction

In 1986 MAZUR introduced the concept of deformations of Galois representations and showed the existence of a universal one for many reasonable sets of restrictions on the deformations [Maz]. Using Galois cohomology and obstruction theory, he was able to determine the deformation space explicitly in particularly amenable cases. He found examples where the universal deformation ring is isomorphic to $\mathbb{Z}_p[[T_1, T_2, T_3]]$ for odd two – dimensional representations and to $\mathbb{Z}_p[[T]]$ for even ones. In general, he was able to give a lower bound on the dimension of the deformation ring modulo the ideal generated by p, namely 3 or 1, respectively. Yet the structure of the universal deformation remained unclear.

In [BoMa] the problem of explicit examples and the structure of those was addressed for a family of neat odd two – dimensional residual representations. Furthermore in [Bos1] a number of methods based on pro – p Galois theory were developed to determine universal deformations. A variation of these methods was presented in [Bos2] to study the universal deformation under enlarging the set of primes that can ramify. Almost all cases considered were odd.

1991 *Mathematics Subject Classification.* 11R33, 11R39.
Keywords and phrases. Even Galois representations, universal deformations.

Our goal here is to apply the methods in [Bos1] and [Bos2] to study some even cases. In Section 2, we briefly recall the main tools from [Bos1] and some ideas behind them to consider some basic deformation problems in the even case. There the image of a complex conjugation is either the identity or its negative, and so the splitting field is totally real or a CM field, respectively. In both cases, the number of indeterminates of the universal deformation ring depends only on the largest totally real subfield, Remark 2.9. In the tame unobstructed case this number is one, and so the corresponding Galois representation is the cyclotomic p-extension, Theorem 2.11. We also discuss those Borel cases which are related to pro-p Poincaré groups, Theorem 2.12. Unlike in the odd case they cannot be neat as in [Bos1, §9], yet they are unobstructed and rigid in the sense of MAZUR.

Section 3 contains explicit examples for the tame as well as the Borel case. In the tame case we will exhibit a family of totally real S_3 extensions together with a representation, that satisfies the conditions given in Section 2. The case where we do not have any examples is the one where the image of the residual representation contains $\mathrm{SL}_2(k)$ for some finite field k.

The last section contains results about enlarging the set of ramified primes which are mostly valid for even and odd cases. We begin by collecting results based on what is called prime-to-adjoint in [Bos1]. Next for even dihedral cases we can compute the universal deformation under fairly general assumptions as long as a certain part of the universal deformation stays abelian, Theorem 4.5. Then we briefly revisit the results in [Bos2] and show how they apply in general, independently of even or odd. We observe that in all cases considered, the number of relations is equal to the cohomologically determined number, $\dim_k H^2(G_{\mathbb{Q}_q}, \mathrm{ad})$, as one might expect from [Maz], see Remark 4.10. The calculations are essentially the ones in [Bos2]. In loc. cit. in the case where three relations are given but two are expected, and where it is stated that the three are dependent, we make this more precise, by explicitly showing that one of them is superfluous.

Finally we construct examples where the universal deformation of tame cases is not twist-finite by considering larger sets of ramification. All other known examples in the even case seem twist-finite. Furthermore this example carries some of the properties that one might expect by looking at the corresponding odd case as done in [Bos2], where one can interpret the growth of the universal deformation space by the appearance of new modular forms as in RIBET's "raising the level". The question that remains is if there are indeed several new lifts to characteristic zero, or if there is a natural obstruction why there cannot be more such lifts.

2. The basic deformation problem

2.1. Basics

Let k be a finite field of characteristic $p > 2$, $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ a Galois representation, G the image of $\bar{\rho}$ inside $\mathrm{GL}_2(k)$ and L the Galois extension of $\mathbb{Q}$ corresponding to G. The field L is called the splitting field of $\bar{\rho}$. The representation $\bar{\rho}$

will be called even or odd if $\det \bar{\rho}(c)$ is $+1$ or -1, respectively, where c is any complex conjugation in $G_{\mathbb{Q}}$.

Let $\mathcal{C}$ be the category of complete noetherian local rings with residue field k and local ring homomorphisms which induce the identity on residue fields. If R is an object of $\mathcal{C}$, then it is a quotient of $W(k)[[T_1, \ldots, T_r]]$ for some r. For R in $\mathcal{C}$ we define $\Gamma_2(R) := \ker(\mathrm{GL}_2(R) \to \mathrm{GL}_2(k))$.

Two lifts $\rho, \rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ of $\bar{\rho}$ are called strictly equivalent if there is an $M \in \Gamma_2(R)$ such that $\rho = M\rho' M^{-1}$. A strict equivalence class of lifts of $\bar{\rho}$ to R is called a deformation. Given a finite set S of places of $\mathbb{Q}$ that contains the prime p, we define the functor $F_S : \mathcal{C} - - \to \mathit{Sets}$ by

$$F_S(R) \;=\; \{\text{deformations of } \bar{\rho} \text{ to } R \text{ unramified outside } S\}\,.$$

The following theorem is known by [Maz, Ram].

Theorem 2.1. *If the centralizer of* $\mathrm{im}(\bar{\rho})$ *in* $GL_2(k)$ *is the set of scalar matrices, then* F_S *is representable. This means there exists a pair* (R_S, ρ_S) *where* $R_S \in \mathcal{C}$ *and* $\rho_S : G_{\mathbb{Q}} \to GL_2(R_S)$ *unramified outside* S*, unique up to isomorphism, such that*

$$F_S(R) \;\cong\; Hom_{\mathcal{C}}(R_S, R)\,,$$

where the isomorphism is induced from composing the representation ρ_S *with elements of* $Hom_{\mathcal{C}}(R_S, R)$.

From now on we will assume that $\bar{\rho}$ satisfies the condition in the theorem.

Remark 2.2. There are many other interesting sets of deformation conditions – at least in the case of odd residual representations – that have been considered, in particular concerning the behavior at the prime p. The above references also discuss many such examples.

As $\Gamma_2(R)$ is a pro$-p$ group, it follows that any lift ρ unramified outside S has to factor through the maximal pro$-p$ extension of G that is a quotient of $G_{\mathbb{Q}}$ and unramified outside S. In fact this is the extension of G by P_S, the Galois group of the maximal pro$-p$ extension of L that is unramified outside all places of L above S, which occurs as the quotient of $G_{\mathbb{Q}}$. We denote this extension by G_S. Our approach to study R_S is by investigating the properties of P_S as described in [Koch].

Definition 2.3. For a pro$-p$ group P we denote by $\Phi(P)$ the *Frattini subgroup of* P, i. e., the topological closure of $[P,P]P^p$, and by $\overline{P}$ the Frattini quotient $P/\Phi(P)$, i. e., the maximal elementary p-abelian quotient of P.

Proofs of the following useful facts can be found in [Bos1, §2] or derived easily.

Lemma 2.4. *Let* P *be a pro*$-p$ *group and* A *be a finite group of order prime to* p.

1. *If* r *is the rank of* P*, i. e., the minimal number of topological generators of* P*, then* $\overline{P} \cong \mathbf{F}_p^r$.

2. *If E is profinite containing P as a normal subgroup such that $E/P \cong A$, then E is a semi-direct product of P and A. The action of A on P is, up to conjugation, uniquely determined by the action on $\overline{P}$.*

3. *If A acts on $\overline{P}$ and V is an A-invariant subspace, then one can find an A-invariant subgroup Q in P whose generators map onto V under $P \to \overline{P}$. Furthermore if N is the normal topological closure of Q in P, then $\overline{P/N} \cong \overline{P}/V$ as A-modules.*

4. *If P, P' are pro-p groups with an action of A and if we have a decreasing filtration $\{P'_n\}$ of P' such that all subquotients are $\mathbf{F}_p[A]$-modules and such that $Hom_{\mathbf{F}_p[A]}(\overline{P}, \overline{P'_n/P'_{n+1}}) = 0$ for all n, then any A-equivariant homomorphism from P to P' is zero.*

5. *For $R \in \mathcal{C}$, and $A \subset GL_2(R)$ one has a filtration $\{P'_n\}$ of $\Gamma_2(R)$ as in the previous part, where each subquotient is isomorphic to $M_2(k)$, and where A acts via $A \to GL_2(k)$ and $GL_2(k)$ via conjugation on $M_2(k)$.*

If the order of $G = \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{im}(\bar{\rho})$ is prime to p, we will call $\bar{\rho}$ tame. In this case, by part 2, G will act on P_S and on $\Gamma_2(W(k))$, and thus via $W(k) \to R$ canonically on any $\Gamma_2(R)$, for $R \in \mathcal{C}$. One can obtain the following equivalence of functors [Bos1, §6].

Theorem 2.5. *If $\bar{\rho}$ is tame, then the functor F_S is equivalent to the functor E_S on $\mathcal{C}$ given by*

$$E_S(R) = \{G\text{-equivariant homomorphisms from } P_S \text{ to } \Gamma_2(R)\}.$$

Let K be any finite Galois extension of $\mathbb{Q}$ with Galois group H. For l a place of $\mathbb{Q}$, H_l will denote the corresponding local Galois group. $P_{S,K}$ will be the Galois group of the maximal pro-p extension of K unramified outside S. Let S' be the places of K above S. By $\overline{E}$ and $\overline{E}_\nu$ we denote the global and local units modulo p-powers of K and K_ν respectively ($\nu \in S'$). C_p denotes the elements in the class group $\mathrm{Cl}(K)$ of order p, $\overline{C}$ the class group modulo p-powers. By class field theory one obtains the following exact sequence of $\mathbf{F}_p[H]$-modules [Koch, Satz 11.8]

$$0 \longrightarrow \mathcal{V}_S \longrightarrow \mathcal{V}_\emptyset \longrightarrow \bigoplus_{\nu \in S'} \overline{E}_\nu \longrightarrow \overline{P}_{S,K} \longrightarrow \overline{C} \longrightarrow 0 \tag{2.1}$$

where $\mathcal{V}_\emptyset$, and $\mathcal{V}_S$ can be described explicitly, $\mathcal{V}_\emptyset$ is an extension of C_p by $\overline{E}$ and the map from

$$\overline{E} \subset \mathcal{V}_\emptyset \longrightarrow \bigoplus_{\nu \in S'} \overline{E}_\nu$$

is induced from the one sending global to local units.

Regarding the Galois module structures the following is known [Bos1, BoUl].

Lemma 2.6. *If p does not divide the order of H, then as $\mathbf{F}_p[H]$-modules.*

1. $\overline{E} \oplus \mathbf{F}_p^{triv} \cong \mu_p(K) \oplus \mathrm{Ind}_{H_\infty}^{H} \mathbf{F}_p^{triv}$.
2. $\bigoplus_{\nu \in S'} \overline{E}_\nu \cong \mathbf{F}_p[H] \oplus \left(\bigoplus_{l \in S - \{p\}} \mathrm{Ind}_{H_l}^{H} \mu_p \right)$.
3. $C_p \cong \overline{C}$.

We recall the classification of the subgroups of $\mathrm{PGL}_2(k)$ [Dic, §255, 260].

Theorem 2.7. *If H is a finite subgroup of $PGL_2(k)$, then one of the following holds.*
1. *H is conjugate to a subgroup of the upper triangular matrices inside $PGL_2(k')$, k' the unique quadratic extension of k, (Borel case).*
2. *H is conjugate to $PGL_2(k')$ or $PSL_2(k')$ for a subfield k' of k.*
3. *H is isomorphic to A_4, S_4, A_5 or the dihedral group D_r of order $2r$ for some r not divisible by p.*

2.2. The number of variables of the universal deformation

The next lemma ties together statements of [Maz] and [Bos1] regarding the number of generators of the maximal ideal of $\overline{R}_S = R_S/(p)$. Let $\mathfrak{m}_S$ be the maximal ideal of R_S, $\overline{\mathfrak{m}}_S$ that of $\overline{R}_S$. Let $\mathrm{ad} = \mathrm{ad}_{\bar\rho} = \overline{\Gamma_2(W(k))} \cong M_2(k)$ with the action of G coming from the adjoint action of $\mathrm{GL}_2(k)$ composed with the inclusion $\bar\rho : G \to \mathrm{GL}_2(k)$. Note that the adjoint action of $\mathrm{GL}_2(k)$ on $M_2(k)$ factors through $\mathrm{PGL}_2(k)$, as scalar matrices act trivial. Also in all case $\mathrm{ad} \cong k^{triv} \oplus \mathrm{ad}^0$ where ad^0 are the matrices of trace zero in $M_2(k)$.

Proposition 2.8. *Let G' be the image of G in $PGL_2(k)$ with fixed field L', P'_S the Galois group of the maximal outside S unramified extension of L', and G'_S the corresponding extension of G' by P'_S.*
1. *There is a natural isomorphism $Hom\big(\overline{\mathfrak{m}}_S/(\overline{\mathfrak{m}}_S)^2, k\big) \cong H^1(G_{\mathbb{Q},S}, ad)$.*
2. *By the inflation - restriction sequence*

$$0 \longrightarrow H^1(G, ad) \longrightarrow H^1(G_{\mathbb{Q},S}, ad) \longrightarrow H^1\big(\overline{P}_S, ad\big)^G \longrightarrow H^2(G, ad)$$

and one has the same sequence with P'_S and G' replacing P_S and G. In particular

$$H^1\big(G_{\mathbb{Q},S}, ad\big) \cong H^1(G_S/(\Phi(P_S)), ad) \cong H^1\big(G'_S/\big(\Phi\big(P'_S\big)\big), ad\big).$$

3. *If $\bar\rho$ is tame, then*

$$H^1\big(G_{\mathbb{Q},S}, ad\big) \cong Hom\big(\overline{P}_S, ad\big)^G \cong Hom\big(\overline{P}'_S, ad\big)^{G'}.$$

Furthermore, if ad is written as a direct sum of irreducible $k[G]$ - modules $\bigoplus V_i$, then the k dimension of $\overline{\mathfrak{m}}_S/\big(\overline{\mathfrak{m}}_S\big)^2$ is the number of components of $\overline{P}_S \otimes k$ as a $k[G]$ - module that are isomorphic to one of the V_i's and also the number of such components of $\overline{P}'_S \otimes k$.

Proof. The isomorphism in 2.8 can be found in [Maz], and it reflects two ways of computing the set of deformations from $G_{\mathbb{Q}}$ to $\mathrm{GL}_2\big(k[\varepsilon]/(\varepsilon^2)\big)$. The sequence with P_S in 2.8 follows if one observes that $\ker(\bar\rho)$ acts trivially on ad and hence that

$$H^1(\ker(\bar\rho), \mathrm{ad})^G \cong Hom(\ker(\bar\rho), \mathrm{ad})^G \cong Hom\big(\overline{P}_S, \mathrm{ad}\big)^G,$$

the one with P'_S by observing that even $\ker(G_{\mathbb{Q}} \to G')$ acts trivial on ad. For the second half one compares the given inflation - restriction sequence with that for

$$1 \longrightarrow P_S/\Phi(P_S) \longrightarrow G_S/\Phi(P_S) \longrightarrow G \longrightarrow 1,$$

respectively the sequence with the primes.

The isomorphisms in 2.8 follow from the inflation-restriction sequences in 2.8 as here we assume that the orders of G and G' are prime to p. For the last part, we need to decompose ad into irreducible $k[G]$-modules. We assumed that the centralizer of $\mathrm{im}(\bar{\rho})$ in $\mathrm{GL}_2(k)$ is the set of scalars and that the order of $\mathrm{im}(\bar{\rho})$ is prime to p, so by the above classification Theorem 2.7, the image in $\mathrm{PGL}_2(k)$ has to be one of the groups in case 2.7. In any case $\mathrm{ad} = k^{triv} \oplus \mathrm{ad}^0$. Now ad^0 is irreducible unless we are in the dihedral case in which it decomposes into a non-trivial one-dimensional and an irreducible two-dimensional representation for $r > 2$ and into three distinct non-trivial one-dimensional representations for $r = 2$. In particular the V_i are not isomorphic. Now the statement about dimensions is a simple consequence of counting homomorphisms between modules in a semi-simple category. The case where the image is cyclic of order prime to p, which is included in the Borel case in Theorem 2.7, does not occur, as we assumed that the centralizer of $\mathrm{im}(\bar{\rho})$ consists of the homothethies only. □

Remark 2.9. 1. For even representations the image of a complex conjugation is the identity matrix or the negative of it. So if one considers its image in $\mathrm{PGL}_2(k)$ it is the identity. By using G' in instead of G on sees that at least for infinitesimal deformations there is no difference between either case. This stems from the fact that the kernel of $G \to G'$ is of order prime to p and so all higher cohomology groups of this with p-torsion coefficients vanish.

2. Part 2.8 can also be seen by appealing to 2.4. By combining several parts of it one can see that any deformation of type S of $\bar{\rho}$ has to factor through an extension P_S^0 of G where P_S^0 is a quotient of P_S whose p-Frattini quotient consists exactly of the components in 2.8 that express the dimension of $\overline{\mathfrak{m}}_S/(\overline{\mathfrak{m}}_S)^2$.

3. The term $H^1(G, \mathrm{ad})$ is often zero, as remarked already in [Maz], even if $\bar{\rho}$ is not tame. At the same time for $p > 3$, in the non-tame case, $H^2(G, \mathrm{ad})$ is never zero as one then has two obviously non-equivalent extensions of G by ad^0. Let

$$d : \mathrm{GL}_2(W(k)/p^2) \longrightarrow (W(k)/p^2)^* \quad \text{and} \quad \pi : \mathrm{GL}_2(W(k)/p^2) \longrightarrow \mathrm{GL}_2(k)$$

be the determinant map and the reduction modulo p, resp. Then

$$\pi^{-1}(\mathrm{im}(\bar{\rho})) \cap \ker\left(d^{|k|-1}\right) \quad \text{and} \quad \mathrm{im}(\bar{\rho})(1 + \varepsilon \mathrm{ad}^0) \subset \mathrm{GL}_2(k[\varepsilon]/(\varepsilon^2))$$

are such extensions - one contains an element of order p^2, the other doesn't. For $p = 3$ both have elements of order 9, so they are not necessarily different. Precise statements about the size of $H^i(G, \mathrm{ad})$ are given in the following lemma for the case $k = \mathbf{F}_p$.

Hence the difficult part in actually determining the size of $H^1(G_{\mathbb{Q}}, \mathrm{ad})$ from that of $Hom(\overline{P}_S, \mathrm{ad})^G$, apart from the calculation of $\overline{P}_S$, is the map

$$Hom(\overline{P}_S, \mathrm{ad})^G \longrightarrow H^2(G, \mathrm{ad}).$$

For given S, it is not at all apparent how to do this, as it would require explicit knowledge of the group $G_S/(\Phi(P_S))$, i.e., the way in which $\overline{P}_S$ is an extension of G - or at least that part of $\overline{P}_S$ that provides G-equivariant homomorphisms to ad.

On the other hand, if one assumes that S contains S_0, the set consisting of p, ∞ and the primes where $\bar{\rho}$ ramifies, and a set of auxiliary primes for S_0 as the sets Q_n constructed in [TaWi, §4], which can be done quite generally, also for many even representations, then by [Neu, Satz 3.1], as all the local extension problems can be solved, the map $Hom(\bar{P}_S, \mathrm{ad}^0)^G \to H^2(G, \mathrm{ad}^0)$ is surjective. Thus for $p \geq 5$ one can find surjective lifts onto $\mathrm{SL}_2(\mathbb{Z}/(p^2))$ if $\bar{\rho}$ surjects onto $\mathrm{SL}_2(\mathbf{F}_p)$. If in addition $H^2(G, \mathbf{F}_p^{triv}) = 0$, one obtains a lift $G_{\mathbb{Q}} \to E$ for any extension E of G by ad. For non-split extensions such that ad^0 is an irreducible $\mathbf{F}_p[G]$-module, the surjectivity of the lift onto the ad^0 part follows. One can certainly improve this to obtain surjective lifts onto $\mathrm{GL}_2(\mathbb{Z}/(p^2))$ for surjective $\bar{\rho}$ onto $\mathrm{GL}_2(\mathbf{F}_p)$, provided $p \geq 5$, after possibly further enlarging S. For other solutions concerning this extension problem see [Kha].

Lemma 2.10. *Suppose $k = \mathbf{F}_p$, $p \geq 3$. If G contains a subgroup H such that the image of H in $PGL_2(\mathbf{F}_p)$ is isomorphic to $C_p \rtimes C_r$ with $r > 2$, then $H^1(G, ad^0) = 0$. Under the same assumptions one has $H^1(G, \mathbf{F}_p^{triv}) = H^2(G, \mathbf{F}_p^{triv}) = 0$.*

In particular this holds for $G = GL_2(\mathbf{F}_p)$, all $p > 2$, and $G = SL_2(\mathbf{F}_p)$, all $p > 5$. Explict calculations show $\dim_{\mathbf{F}_5} H^1(SL_2(\mathbf{F}_5), ad^0) = 1$ and $H^1(SL_2(\mathbf{F}_3), ad^0) = 0$. Furthermore for $p > 3$ and G the dihedral group D_p inside $GL_2(\mathbf{F}_p)$ one computes $\dim_{\mathbf{F}_p} H^1(D_p, ad^0) = 1$.

For the second cohomology one finds $\dim_{\mathbf{F}_p} H^2(G, ad^0) = 1$ for $p > 3$ for all the groups considered above, while $H^2(SL_2(\mathbf{F}_3), ad^0) = 0$.

The proof follows easily from the proof in [Fla, Lemma 1.2], based on properties of the transfer map [Bro, III.10.3], and part 2.9 of the previous remark.

2.3. The basic deformation problem in tame cases

Theorem 2.11. *Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(k)$ be a tame even irreducible representation. We denote by S a finite set of places containing p, ∞ and all places where $\bar{\rho}$ ramifies. We assume that $\bar{\rho}$ is neat at p, i. e., as $k[G']$-modules the p quotient $\overline{C'}$ of the class group of L' has no common component with ad, and the cokernel of $\overline{E} \to \bigoplus_{\nu \in S'} \overline{E}_\nu$ tensored with k has only k^{triv} as a common component with ad. Let $\rho_0 : G \to GL_2(W(k))$ be a given lift of $\bar{\rho}$. Let L^∞ be the cyclotomic p extension of L. Then the universal deformation (ρ_S, R_S) of*

$$\bar{\rho} : G_{\mathbb{Q}} \longrightarrow GL_2(k)$$

factors through $Gal(L^\infty/\mathbb{Q}) \cong \mathbb{Z}_p \times G$, R_S is isomorphic to $W(k)[[T]]$, and if γ is a fixed topological generator of $\mathbb{Z}_p \cong Gal(L^\infty/L)$, then $\rho_S : Gal(L^\infty/\mathbb{Q}) \to GL_2(W(k)[[T]])$ is explicitly given by ρ_0 on G and by sending γ to $(1+T)$ times the identity matrix.

Proof. By Lemma 2.6 and Proposition 2.8, the conditions that we impose are equivalent to $\overline{\mathfrak{m}}_S/(\overline{\mathfrak{m}}_S)^2 \cong k^{triv}$. By the remark above this implies that ρ_S factors though a pro-p extension P_S^0 of G whose p Frattini quotient is isomorphic to $\mathbf{F}_p^{triv}$ and which is unramified outside S. But the cyclotomic p extension of L is such an extension, so its Galois group which is isomorphic to $\mathbb{Z}_p$ must be P_S^0. As $L_\infty \cong L\mathbb{Q}^\infty$, $\mathbb{Q}^\infty$ the

cyclotomic p extension of $\mathbb{Q}$, G has to act trivially on $\mathrm{Gal}(L^\infty/L)$. The choice of ρ_0 fixes the ambiguity that arises as one considers lifts up to strict equivalence. □

2.4. The deformation problem for some Borel cases

Now we consider the case where G lies inside the upper triangular matrices of $\mathrm{GL}_2(k)$ and has non-trivial image in the unipotent as well as in the diagonal part of $\mathrm{PGL}_2(k)$. Those conditions are, up to base change, equivalent to the condtion that the centralizer of G in $\mathrm{GL}_2(k)$ is the set of homotethies, as needed in Theorem 2.1. Hence we will assume these conditions throughout this subsection.

The group G is clearly solvable, and if we denote by A the diagonal matrices in G, and by U the unipotent part, then

$$1 \longrightarrow U \longrightarrow G \longrightarrow A \longrightarrow 1.$$

The field with A as its Galois group is denoted by F and it is obviously an abelian extension of $\mathbb{Q}$. We assume that the image of G is inside the upper triangular matrices. Again we want to study pro-p extensions of G. The fact that p does divide G seems a problem at first, but one observes that the extension of U by a pro-p group is a pro-p group itself, and so the idea is to let A act on this pro-p group.

We denote by A' the quotient to A in $\mathrm{PGL}_2(k)$. If A acts via the characters χ_1, χ_2 on the diagonal inside $\mathrm{GL}_2(k)$, we define $\chi = \chi_1\chi_2^{-1}$ which is then a character of A' into k^*. The A-module structure on ad is the one given by trivial action along the diagonal, by χ on the right upper corner and by χ^{-1} on the lower left corner. In particular, if χ has order two the latter two modules are isomorphic, and vice versa - order one is excluded by the condition on the centralizer of G in $\mathrm{GL}_2(k)$.

Unlike in the odd case [Bos1, §9], the deformation problem that we have to consider here cannot be neat above F or L. If it were neat above L, then by [Mov, Prop. 5], it would have to be neat above F, too. But in the neat even case, the only extension possible is the cyclotomic one with a trivial A action on the p Frattini quotient. But U has a non-trivial action by A. On the other hand the case that we will consider below is unobstructed in the sense of MAZUR, i.e., $H^2(G_{\mathbb{Q},S}, \mathrm{ad}) = 0$. As we are in the even case this means that $\dim_k H^1(G_{\mathbb{Q},S}, \mathrm{ad}) = 1$ or in other words that after fixing the determinant, the lifts to $\mathbb{Z}_p$ are rigid. As we calculate the universal deformation explicitely, this can also be seen by simply examining it for the case of fixed determinant.

The case next simple to the case of P_S being a free pro-p group, is the case that P_S is a Poincaré group. Fortunately there is a complete characterization of those in [Win1]. At the same time it is not hard to determine the most general non-abelian pro-p group on two generators that can fit into $\mathrm{GL}_2(\mathbb{Z}_p)$ with a lift of the action of A on it where the image of one generator in U is the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. It turns out that this itself is a Poincaré group, and so this concept seems to be ideally suited to our problem. Regarding Poincaré quotients of P_S, one should also consult the excellent survey article [Win2, Theorem 6] and bear in mind that for even Galois representation the field L, if totally complex, is always a CM field. An alternative approach to the Borel case as treated here would be the use of Iwasawa theory, as the image of our deformations will have to be metabelian.

For the next theorem, we will simply assume that P_S is a Poincaré group. Later in Proposition 3.7, we will give more precise conditions and examples for this to happen. If P_S has a quotient that is a Poincaré group of the type described below, then one can at least conclude that the universal deformation ring surjects onto the ring given in the following theorem, and that there are lifts to characteristic zero.

Theorem 2.12. *Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(k)$ be upper triangular as described above. We assume that S contains p, ∞ and the primes where $\bar{\rho}$ ramifies, and is such that $P_{S,F}$, the Galois group of the maximal pro-p extension of F unramified outside S, is a Poincaré group of rank two, i. e.,*

$$P_S \cong \left\langle s, t | sts^{-1}t^{-1} = t^{p^n} \right\rangle$$

for some $n \geq 1$. Equivalently P_S is a semi-direct product of $\mathbb{Z}_p$ acting non-trivially on $\mathbb{Z}_p$. The number n can be determined from P_S^{ab}, i. e., from global class field theory.

Then we can pick s, t so that A acts trivially on s and via χ on t. Furthermore $R_S = W(k)[[T]]$ and the universal deformation is given by

$$G_{\mathbb{Q}} \longrightarrow P_S \rtimes A \longrightarrow GL_2(W(k)[[T]])$$

where the second map is $\bar{\rho}$ composed with the Teichmüller lift $k^* \times k^* \to W(k)^* \times W(k)^*$ on A, and on s, t it is given by

$$s \longmapsto \begin{pmatrix} (1+T)(1+p^n) & 0 \\ 0 & 1+T \end{pmatrix}, \quad t \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Proof. By our assumption

$$P_S \cong \left\langle s, t | [s,t] = t^{p^n} \right\rangle,$$

and so every element of P_S can be written in the form $s^\alpha t^\beta$ with $\alpha, \beta \in \mathbb{Z}_p$. Now we consider the following diagram where the horizontal arrows are surjective and the bottom row represents the p Frattini quotients.

$$\begin{array}{ccc} P_S & \xrightarrow{g} & \mathbb{Z}_p \\ \downarrow & & \downarrow \\ \overline{P}_S & \xrightarrow{\bar{g}} & \mathbb{Z}/(p) \end{array}$$

The group $\mathbb{Z}_p$ on the top right is the Galois group of the maximal cyclotomic p-extension of F, hence it has trivial A action. The whole diagram is A-equivariant. Furthermore $\overline{P}_S \cong \mathbf{F}_p^{triv} \oplus \mathbf{F}_p^{\chi}$ by our assumption on $\bar{\rho}$.

To identify the A action, let σ be a generator of $\mathbb{Z}_p$, let $s' = s^\alpha t^\beta$ be a lift in P_S that maps to an element in $\overline{P}_S$ with trivial A action. Then the subgroup generated in P_S by s' must be $\mathbb{Z}_p$ and by the uniqueness of an A action, Lemma 2.4, A has to act trivially on this subgroup. In particularly the map g splits A-equivariantly. By

considering the map on p Frattini quotients and using the fact that t gets mapped to 0 in $\mathbb{Z}_p$, the element α must be a unit in $\mathbb{Z}_p$. If we replace s by s' which does not change the relation in P_S we may assume that $s' = s$.

Regarding the action of A on t, it is clear that the kernel of $\bar{g}$ is exactly the part of $\overline{P}_S$ on which A acts as χ. As the image of t generates this kernel, A acts via χ on the image of t and hence by the uniqueness of such an operation it acts in the same way on the subgroup generated by t.

We fix the lift from A to the diagonal of $\mathrm{GL}_2(W(k))$ that was described in the statement of the theorem. Using this, any lift $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ of $\bar{\rho}$ induces an A-equivariant map $P_S \to \mathrm{GL}_2(R)$. A acts trivial on s, and so its image has to be a diagonal matrix of the type $\begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix}$ with $T_i \in \mathfrak{m}$ the maximal ideal of R. The action of A on the image of t is given by χ and its reduction modulo $\mathfrak{m}$ generates U. Hence it is of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ where x is a unit in R. By replacing t by a prime to p power with an exponent in $\mathbb{Z}_p^*$ we can achieve $x = 1$. After fixing the image of A and t we used up all the freedom given by considering lifts up to strict equivalence. Finally from the commutativity relation between s and t it follows that $1 + T_1 = (1 + T_2)(1 + p^n)$. Now it is easy to see that R_S and ρ_S as given satisfy the necessary universality condition. □

3. Examples

3.1. A family of examples in the tame case

Here we will construct an explicit family of polynomials analogous to the construction in [BoMa] which satisfy the conditions in Theorem 2.11.

Let $f(x) = x^3 - a^2x - 1$ where $a \geq 2$ is an integer such that $p = 4a^6 - 27$ is prime. Then clearly $p \equiv 1 \pmod 4$. The splitting field L of f over $\mathbb{Q}$ is totally real with Galois group S_3. In fact L is inside the Hilbert class field $F = \mathbb{Q}(\sqrt{p})$, which is obvious as p is the discriminant of the above polynomial. Hence the only prime that ramifies in L over $\mathbb{Q}$ is p. So we let $S = \{p\}$. The prime $p \geq 229$ will also be the residue characteristic of the finite field that we consider. The reason why we choose the coefficient of x to be $-a^2$, and not just $-a$, is to have explicit expressions for fundamental units as will be apparent later on.

We obtain a continuous absolutely irreducible even representation

$$\bar{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(L/\mathbb{Q}) \cong S_3 \longrightarrow GL_2(\mathbf{F}_p).$$

For $S_3 \to GL_2(\mathbf{F}_p)$ one can take for example the reduction mod p of the representation $\rho_0 : S_3 \to GL_2(\mathbb{Z}[\frac{1}{2}])$ given in [BoMa, Prop. 11].

Theorem 3.1. *Let L be the splitting field of $f(x) = x^3 - a^2x - 1$ where $a \geq 2$ is an integer, such that $p = 4a^6 - 27$ is prime. Assume that p satisfies the Ankeney-Artin-Chowla conjecture and the following congruence condition:*

$$\left(u\left(\frac{3}{2a^2}\right) - 1\right)(2a^3 + 9)/6 - \left(u\left(\frac{3}{3 - 2a^3}\right) - 1\right)$$

$$\not\equiv \frac{1}{243}\left(4a^6-27\right)\left(9/4+a^3\right) \pmod{\left(4a^6-27\right)^2}$$

where for $x \in \mathbb{Z}_p$ we let $u(x) = x/x^p$. Then $\bar{\rho}$ satisfies the assumptions of Theorem 2.11.

The Ankeney – Artin – Chowla conjecture predicts that for any prime $p \equiv 1 \pmod 4$ the coefficient B in the expression $u = A + B\sqrt{p}$ for the fundamental unit is not divisible by p, see [AAC].

According to Bouniakowski's conjecture there are infinitely many primes of the form $4a^6 - 27$. In fact he conjectures that all polynomial expressions $g(x)$, apart from the ones that have a trivial integral divisor due to congruences, represent infinitely many primes; here a prime q is such a divisor if $g(x) \pmod q$ is divisible by $x^q - x$ over $\mathbb{F}_q[x]$. In fact using PARI – gp, one can show that the conditions given in the above theorem are satisfied for all the 108 primes that arise for a between 2 and 1000.

To prove the theorem we will show that the p part of the class group $Cl(L)$ is zero and that the map $\iota : \overline{E}_L \to \bigoplus_{\nu|p} \overline{E}_{L_\nu}$ is injective. Hence by 2.6 and the sequence (2.1) above it this will imply that the cokernel is isomorphic to $\mathbf{F}_p^{triv}$ which was to be shown. The proofs of those facts will be the content of the following two subsections. We begin be fixing the notation for the calculations to come, and exhibiting some elementary properties of L.

Let α_i $(i = 1, 2, 3)$ be the three roots of f in L and let S_3 have generators τ, σ where τ has order 3 and σ has order 2, and τ permutes the three roots α_i cyclically. We let $K_i = \mathbb{Q}(\alpha_i)$. Sometimes we will refer to K_1 as K, to K_2 as K^τ and to K_3 as K^{τ^2}, and as above $F = \mathbb{Q}(\sqrt{p})$. For any number field M we denote by E_M its group of global units and by E_{M_ν} the group of local units at a place ν. We will suppress M from the notation if it is clear from the context.

Regarding the factorization of (p) in the above fields, one observes that $(p) = (\pi)^2$ in F, where $\pi = \sqrt{p}$, and that (π) splits completely in L, say $\pi = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ corresponding to the above fields K_i. To investigate how (p) splits in K, we compute f modulo p as

$$f(x) \equiv \left(x + \frac{3}{2a^2}\right)^2\left(x - \frac{3}{a^2}\right).$$

Thus $(p) = \mathfrak{p}_1\mathfrak{p}_2^2$ in O_K with prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$, and we must have $\mathfrak{p}_1 = \mathfrak{P}_1^2$ and $\mathfrak{p}_2 = \mathfrak{P}_2\mathfrak{P}_3$.

From this decomposition of (p) we conclude that $K_{\mathfrak{p}_1}$ is isomorphic to $\mathbb{Q}_p$, and $K_{\mathfrak{p}_2}$ is isomorphic to the unique totally ramified extension of degree 2 of $\mathbb{Q}_p$, and so are $L_{\mathfrak{P}_i}$ for $i = 1, 2, 3$ and E_π with the obvious identifications.

3.2. The class group of L

To begin we shall compute the fundamental units and the regulator of K.

Proposition 3.2. *For $a \geq 3$, $p = 4a^6 - 27$ and K as above we have*
1. *α_1 and $\alpha_1 + a$ form a system of fundamental units for K.*

2. *The regulator R_K of K satisfies*

$$3\log^2 a + 2\log a \;>\; R_K \;>\; \log^2 a - 0.3\log a\,.$$

Proof. Part 3.2 follows from [Ste, Satz 7, S.173] after replacing x by $x+a$.

For part 3.2 one uses the definition of the regulator as the determinant of the logarithms of the embeddings of a system of fundamental units, $R_K = \log|\alpha_1|\log|\alpha_2+a| - \log|\alpha_2|\log|\alpha_1+a|$, where we assume that the α_i are ordered so that $\alpha_1 > \alpha_2 > \alpha_3$. To get the estimates one only needs the following estimates on the roots:

$$a \;<\; \alpha_1 \;<\; a+\frac{1}{a^2} \quad\text{and}\quad -\frac{2}{a^2} \;<\; \alpha_2 \;<\; -\frac{1}{a^2}\,. \qquad \square$$

Proposition 3.3. *The class number of L is not divisible by p.*

Proof. We follow the method in MAZUR [Maz, Thm IV.1, S. 67]. From results of MOSER who applies BRAUER'S theory of computing the class number of L through the class numbers of its subfields [Mos], we know that $h_L = \frac{c}{9} h_K^2 h_E$, where $c \in \{1,3,9\}$. Thus we are reduced to showing that p doesn't divide either of h_E or h_K.

For h_E one can quote the result in [Nar, VIII.2., Prop 8.2] which says that $h_E \le \sqrt{p}$.

For h_K one can find in [Nar, p. 401] the inequality

$$R_K h_K \;<\; .088\sqrt{p}\log^2(p)$$

which was obtained by LAVRIK. From the previous corollary we have the estimate $R_K > \log^2 a\left(3 - \frac{0.3}{\log a}\right)$ where $a^6 = (p+27)/4$. We get

$$h_K \;<\; 1.3\sqrt{p}\,\frac{\log^2 p}{\log^2(p+27)/4}$$

which is always less than p as $p \ge 229$, the minimal p that can occur (for $a=3$). $\square$

3.3. The injectivity of $\iota_L : \overline{E}_L \to \bigoplus_{\nu|p} \overline{E}_{L_\nu}$

As one has neither local nor global p-th roots of unity, by Dirichlet's unit theorem we know that $\overline{E}_L$ is a five-dimensional $\mathbf{F}_p$ vector space. Thus to show injectivity, we are going to show that the image of ι_L has dimension five. This will be accomplished by considering the corresponding maps ι_F and ι_K and their relations to ι_L. Note that by results of MOSER [Mos, Thm III.5, S. 62], one has

$$[E_L : E_K E_{K^\tau} E_F] \;=\; c\,,$$

where $c \in \{1,3,9\}$, and thus $\overline{E}_L = \overline{E}_K \overline{E}_{K^\tau} \overline{E}_F$ for the p-Frattini quotients.

From 2.6 we know that $\bigoplus_{\nu|p} \overline{E}_{L_\nu} \cong \mathbf{F}_p[S_3]$ where $S_3 \cong \mathrm{Gal}(L/\mathbb{Q})$. So we have

$$\bigoplus_{\nu|p} \overline{E}_{L_\nu} \;\cong\; \mathbf{F}^{\mathrm{triv}} \oplus \mathbf{F}^{\sigma} \oplus V_2 \oplus V_2$$

with $\mathbf{F}^{\sigma}$ the one-dimensional representation on which σ acts non trivially and V_2 the unique irreducible two-dimensional representation.

Lemma 3.4. *The image of $\overline{E}_F$ under ι_L is $\mathbf{F}^\sigma$ inside $\bigoplus_{\nu|p} \overline{E}_{L_\nu}$.*

Proof. We consider the following diagram:

$$\begin{array}{ccc} \overline{E}_F & \xrightarrow{\iota_F} & \overline{E}_{F_\pi} \\ \downarrow & & \downarrow \\ \overline{E}_L & \xrightarrow{\iota_L} & \bigoplus_{\nu|p} \overline{E}_{L_\nu} \end{array}$$

As F and hence F_π are τ-invariant this diagram is a diagram of $\mathbf{F}_p[S_3]$-modules. The action of σ on E_F sends a fundamental unit u_0 to $\pm u_0^{-1}$; thus it acts on $\overline{E}_F$ as the map sending x to $-x$.

At this point we need the Ankeney-Artin-Chowla conjecture. Let $u_0 = A + B\sqrt{p}$ be a fundamental unit of E. By the the conjecture we know that $\frac{B}{A}$ is a unit in F_π. For any p we have that $\sqrt{p}$ is a uniformizing parameter in F_π. Therefore $\overline{1 + \frac{B}{A}\sqrt{p}}$, the image of u_0 in $\overline{E}_{F_\pi}$, is nonzero, and so ι_F is injective. Finally the left vertical map is clearly injective, too, establishing the lemma. □

Next we will compute the image of $\overline{E}_K$ in $\overline{E}_{K_{\mathfrak{p}_1}} \oplus \overline{E}_{K_{\mathfrak{p}_2}}$. We have already seen that α and $\alpha + a$ form a set of fundamental units of K. Without loss of generality we assume that K is the σ-invariant subfield of L.

Lemma 3.5. *The map $\iota_K : \overline{E}_K \to \overline{E}_{K_{\mathfrak{p}_1}} \oplus \overline{E}_{K_{\mathfrak{p}_2}}$ is injective.*

Proof. We will show that the images of α and $\alpha + a$ are linearly independent in $\overline{E}_{K_{\mathfrak{p}_2}}$ by explicitly computing them. Say π_1 is a uniformizing parameter of $K_{\mathfrak{p}_2}$. Then

$$\begin{aligned} \overline{E_{K_{\mathfrak{p}_2}}} &\cong \overline{\mathbf{F}_p^\times \times (1 + (\pi_1))} \cong \overline{1 + (\pi_1)} \\ &\cong \frac{\overline{1 + (\pi_1)}}{(1 + (\pi_1))^p} \cong \frac{\overline{1 + (\pi_1)}}{1 + (\pi_1)^3} \\ &\cong \mathbf{F}_p \times \mathbf{F}_p \,. \end{aligned} \tag{3.1}$$

The second isomorphism involves Teichmüller lifts. For any $x \in \mathbb{Z}_p^*$ one can write $x = \omega(x)u$ where u is a one-unit and $\omega(x)$ is a $(p-1)$-st root of unity. Modulo $(1 + (\pi_1))^p$ one can compute u as $u(x) = x/x^p$.

Knowing that $f(x) \boxminus \left(x + \frac{3}{2a^2}\right)^2 \left(x - \frac{3}{a^2}\right) \pmod p$, it is an easy exercise to see that $\beta = \alpha + \frac{3}{2a^2}$ is a uniformizing parameter of $K_{\mathfrak{p}_2}$, and thus we can assume $\pi_1 = \beta$. From the identification in (2) we get

$$\overline{\alpha_1} = \overline{\frac{-3}{2a^2} + \pi_1} = \overline{u\left(\frac{-3}{2a^2}\right)\left(1 - \frac{2a^2}{3}\pi_1\right)} \quad \text{and} \tag{3.2}$$

$$\overline{\alpha_1 + a} = \overline{\frac{-3}{2a^2} + a + \pi_1} = \overline{u\left(\frac{2a^3 - 3}{2a^2}\right)\left(1 - \frac{2a^2}{3 - 2a^3}\pi_1\right)}. \tag{3.3}$$

Clearly $\overline{\alpha_1}$ is not trivial, i.e., equal to $\bar{1}$, as it is non-trivial modulo (π_1^2), and so to establish linear independence it is enough to show that $\overline{\alpha_1 + a}$ cannot be written as a power of $\overline{\alpha_1}$. Assume the contrary. Then we can find an integer k such that

$$u\left(\frac{-3}{2a^2}\right)^k \left(1 - \frac{2a^2}{3}\pi_1\right)^k \equiv u\left(\frac{2a^3-3}{2a^2}\right)\left(1 - \frac{2a^2}{3-2a^3}\pi_1\right) \pmod{\pi_1^3}.$$

One obtains two equations modulo p. The first one arises by considering this modulo π_1^2 and yields $k \equiv \frac{3}{3-2a^3} \pmod{p}$. Using this after subtracting 1 on both sides one has an equation with leading term π_1^2. This equation can be transformed to the first congruence condition given in Theorem 3.1. One needs to replace p by an expression in π_1^2. To do this we observe that $\pi_1 - \frac{3}{2a^2}$ satisfies $x^3 - a^2x - 1 = 0$, which implies $p \equiv 36a^4\pi_1^2 \pmod{\pi_1^3}$. □

Next we note that the image of $\overline{E}_{\mathbb{Q}_p}$ in $\bigoplus_{\nu|p} \overline{E}_{L_\nu}$ is exactly the trivial one-dimensional part V_{triv}.

Denote by H the image of $\overline{E}_K$ in $\bigoplus_{\nu|p} \overline{E}_{L_\nu}$, where we consider the diagram

$$\begin{array}{ccc} \overline{E}_K & \xrightarrow{\iota_K} & \overline{E}_{K_{\mathfrak{p}_1}} \oplus \overline{E}_{K_{\mathfrak{p}_2}} \\ \downarrow & & \downarrow \\ \overline{E}_L & \xrightarrow{\iota_L} & \bigoplus_{\nu|p} \overline{E}_{L_\nu} \end{array}$$

Lemma 3.6. *H and $\mathbf{F}^{triv}$ intersect trivially in $\bigoplus_{\nu|p} \overline{E}_{L_\nu}$, and H has dimension two in $\bigoplus_{\nu|p} \overline{E}_{L_\nu}$.*

Proof. This is an easy consequence of 2.6 where the $\mathbf{F}_p[G]$ structures of the two groups at the bottom are described. As the above diagram commutes, H is clearly in the image of $\overline{E}_L$. But as an $\mathbf{F}_p[G]$-module this does not contain $\mathbf{F}_p^{triv}$ as a summand. The bottom map is a map of $\mathbf{F}_p[G]$-modules, and hence the image of H cannot meet the $\mathbf{F}_p^{triv}$. The statement about the dimension follows as the horizontal map on the right is injective. □

Proof. Now we prove the injectivity of ι_L. As K is the σ-invariant subfield of L, it follows that H is σ-invariant. Clearly $\mathbf{F}^{triv}$ is σ-invariant, too, and by the previous lemmas those two subspaces together span a three-dimensional σ-invariant subspace of $\bigoplus_{\nu|p} \overline{E}_{L_\nu} \cong \mathbf{F}_p[S_3]$. By representation theory this must be the set of all σ-invariant elements. Thus the τ-orbit of H must coincide with $V_2 \oplus V_2$ inside $\bigoplus_{\nu|p} \overline{E}_{L_\nu}$. But the τ-orbit of H is the sum of the images of $\overline{E_K}$, $\overline{E_{K^\tau}}$ and $\overline{E_{K^{\tau^2}}}$ and thus inside the image of $\overline{E_L}$. Hence the image of $\overline{E_L}$ contains $V_2 \oplus V_2$ and also $\mathbf{F}^\sigma$, the image of $\overline{E}_F$. Therefore it must have dimension at least 5. □

3.4. Examples in the Borel case

We now describe conditions which are derived from [Win1, Cor.] under which $P_{S,F}$ is a Poincaré group which appears at the base level of a universal deformation of

residual Borel type as described in Theorem 2.12. In fact we will use the conditions given in [Koch, Satz 11.16] which are equivalent to those above in the case $d = 1$ in the notation of [Koch, Satz 11.16].

Let F be a totally real cyclic extension of $\mathbb{Q}$ of degree m prime to p that is unramified at all primes q such that $N(\mathfrak{q}) \cong 1 \pmod{p}$ for $\mathfrak{q}$ in F above q. We assume that $\mathcal{V}_{S,F} = 0$ so in particular the p part of the class group of F is trivial and F has no local roots of unity at p. Let q be a prime that is inert for $F/\mathbb{Q}$ and so that A_q which is isomorphic to A acts as χ on $\mu_p(F_q)$. By the Cebotarev density theorem there exists a set of positive density with this property. Let L be the extension of degree p corresponding by global class field theory to the image of E_q/E_q^p in the five term sequence (2.1). Then $\mathrm{Gal}(L/F) \cong E_q/E_q^p \cong \mathbf{F}_p^\times$ as an A-module, and thus $\mathrm{Gal}(L/\mathbb{Q}) \cong C_p \rtimes C_m$. We now choose f large enough so that m divides $p^f - 1$ and let $k = \mathbf{F}_{p^f}$. Thus we obtain a representation

$$\bar{\rho} \; : \; \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(k)$$

with upper triangular image. Let $n = \mathrm{ord}_p(q^m - 1)$.

Proposition 3.7. *Under the above assumptions $P_{S,F}$ is a Poincaré group of rank two and the universal deformation of $\bar{\rho}$ is as described in* 2.12.

In the case $m = 2$, and ramification at p one can give particularly simple conditions under which all the above holds. As mentioned above the existence of q is irrelevant, as by Cebotarev there always exists an infinite number. For $F = \mathbb{Q}(\sqrt{d})$, where $d > 0$ is square free, the above conditions mean that d has no prime divisors $l \equiv 1 \pmod{p}$, p divides d, and if $u = A + B\sqrt{d}$ is a fundamental unit of F, then $B \not\equiv 0 \pmod{p}$.

4. Enlarging the ramification

4.1. The principle of prime-to-adjointness

In this subsection we assume that $\bar{\rho}$ is absolutely irreducible and that $\mathrm{im}(\bar{\rho})$ has order prime to p, so projected onto $\mathrm{PGL}_2(k)$ its image is dihedral or A_4, S_4 or A_5. We will call the first case projectively dihedral and the other ones exceptional. Note that projectively dihedral means that $\mathrm{im}(\bar{\rho})$ is non-abelian and contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(k)$.

As we have seen in Lemma 2.4, mainly part 4, and Proposition 2.8, the part of P_S that is really relevant is the part that is, loosely speaking, not prime to the adjoint representation. The way that P_S maps into $\Gamma_2(R)$ depends largely on the way that its p Frattini quotient maps G-equivariantly to ad. This is made explicit in Corollary 4.3. Again the method we use goes back to [Bos1] and the following two lemmas are implicitly from there.

We begin by briefly recalling the possible module structures of ad under any subgroups of $\mathrm{GL}_2(k)$ of order prime to p.

Lemma 4.1. *Let H be a subgroup of $GL_2(k)$ and acting on ad in this way. Assume $p \nmid |H|$. Then the structure of ad as a $k[H]$-module is one of the following.*

1. *If H is inside the scalars, then $ad \cong (k^{triv})^4$.*
2. *If H is inside a split Cartan subgroup, but not in the center, then $ad \cong (k^{triv})^2 \oplus k^{\phi_H} \oplus k^{\phi_H^{-1}}$ for some character ϕ_H. ϕ_H can be made explicit if we assume that the elements of H are 2 by 2 matrices $x = (x_{i,j})$ in diagonal form. Then $\phi_H(x) = x_{1,1}x_{2,2}^{-1}$ for $x \in H$.*
3. *If H is not in the center, but inside a non-split Cartan subgroup, then $ad \cong (k^{triv})^2 \oplus V_2$ for some irreducible representation V_2 of H.*
4. *If H is projectively dihedral, and ψ is the action of the C_2 quotient of H that sends $x \in k$ to $-x$, then $ad \cong k^{triv} \oplus k^{\psi} \oplus V_2$ for some irreducible V_2.*
5. *In all other cases $ad \cong k^{triv} \oplus ad^0$ where ad^0 is irreducible.*

For primes $q \neq p$, we saw in the description of $\overline{P}_S$ in 2.6 and the paragraph above that increasing S to $S' = S \cup \{q\}$ enlarges $\overline{P}_S$ by a summand that is a quotient of $\mathrm{Ind}_{G_\mathfrak{q}}^{G} \chi$ where χ is the action of $G_\mathfrak{q}$ on the local p-th roots of unity, tensored with k, where we choose a prime $\mathfrak{q}$ in L over q. Replacing H by $G_\mathfrak{q}$ after applying Frobenius reciprocity, one obtains the following lemma, where the cases are numbered as in the previous lemma.

Lemma 4.2. *ad and $\mathrm{Ind}_{G_\mathfrak{q}}^{G} \chi$ share the following irreducible $k[G]$-modules as summands.*

1. *If χ is non-trivial, there is no common summand, else they share all of ad.*
2. *If $\chi \neq triv$, $\phi_{G_\mathfrak{q}}$, $\phi_{G_\mathfrak{q}}^{-1}$, there is no common summand. If $\chi = triv$, they share k^{triv} and one other irreducible summand of ad whose restriction to $G_\mathfrak{q}$ is trivial. In the other two cases they share a summand that is inside ad^0.*
3. *If $\chi \neq triv$ they share no common summand, else they share k^{triv} and one other irreducible summand of ad.*
4. *If $\chi \neq triv$, ψ there is no common summand, for $\chi = triv$ they share k^{triv}, and for $\chi = \psi$ one summand of ad^0.*
5. *If $\chi \neq triv$ they share no common summand, else they share k^{triv}.*

If G is projectively dihedral, say $1 \to G_1 \to G \to C_2 \to 1$ with G_1 abelian, then they share $k^{triv} \oplus k^{\psi}$ provided that $\chi = triv$ in case 4.2, or that $G_\mathfrak{q} \subset G_1$ and $\chi = triv$ in case 4.2, or that $\chi = \psi$ in case 4.2, or that $\chi = triv$ in case 4.2.

Cases 4.2 and 4.2 can obviously only occur at primes that ramify in L. If q doesn't ramify, then cases 4.2 and 4.2 are exactly those where the image of the Frobenius element at q has distinct eigenvalues. The following result is immediate.

Corollary 4.3. *Assume $\mathcal{V}_S = 0$. If we increase S by a prime q such that $G_\mathfrak{q}$ is abelian or exceptional and that $\chi \neq triv$, $\phi_{G_\mathfrak{q}}$, $\phi_{G_\mathfrak{q}}^{-1}$ then $(\rho_{S'}, R_{S'}) \cong (\rho_S, R_S)$.*

Proof. By Theorem 2.5, we only need to compare G-equivariant maps from P_S and $P_{S'}$ to $\Gamma_2(R)$. By Lemma 2.4, $\Gamma_2(R)$ has a filtration with all subquotients being isomorphic to ad. Also as we assume $\mathcal{V}_S = 0$, $\overline{P}_{S'} = \overline{P}_S \oplus \mathrm{Ind}_{G_\mathfrak{q}}^{G} \chi$. By the same lemma any element of $P_{S'}$ with non-trivial image in the Frattini quotient with image

completely inside $\mathrm{Ind}_{G_q}^{G}\chi$ must map to the identity in $\Gamma_2(R)$ under a G-equivariant homomorphism. Let N be the normal subgroup generated by such elements. Then, again by the same lemma $P_{S'}/N$ maps onto P_S and they have isomorphic Frattini quotients. Furthermore, again as $\mathcal{V}_S = 0$, by [Koch, §11], all relations necessary in presentations of P_S and $P_{S'}$ are local. So $P_{S'}/N$ has all the relations of P_S and two more, expressible in fixed lifts of generators of the Frattini quotient of the former. Thus as the former maps onto the latter group and as they have isomorphic Frattini quotients they must be isomorphic. Hence

$$Hom_G(P_{S'}, \Gamma_2(R)) \cong Hom_G(P_{S'}/N, \Gamma_2(R)) \cong Hom_G(P_S, \Gamma_2(R)).$$ □

Remark 4.4. In fact a more careful analysis shows that the above lemma also holds if one doesn't assume that $\mathcal{V}_S = 0$. To see this one has to strengthen part 4 of Lemma 2.4 to include the influence of relations. One can further improve this lemma to a version where one doesn't have to assume that A has order prime to p, by replacing A by a profinite group that is the extension of a finite group (with order not necessarily prime to p) by a pro-p group and that acts continuously on P, P'. Here one can take $A = G_S$. Then the relevant condition for the previous corollary to hold is that $Hom_G(\mathrm{Ind}_{G_q}^{G}\chi, \mathrm{ad}^{s.s.}) = 0$ where now $G = \mathrm{im}(\bar{\rho})$ is not supposed to be prime to p. The superscript "s. s." refers to the semisimplification of ad as a G-module. Only in the Borel case ad and $\mathrm{ad}^{s.s.}$ are different, but even there the corollary still holds.

4.2. A result in the projectively dihedral case

In the case that $\bar{\rho}$ is odd, already if $\bar{\rho}$ is neat at p one has three free parameters and the deformations to $\mathrm{GL}_2(\mathbb{Z}_p)$ have typically a rather large image. Not so in the even case where we showed that in the case where $\bar{\rho}$ is neat at p there is only one parameter, which acts as a scalar. Thus the image is rather restricted. This observation can be used nicely in the projectively dihedral case to determine the universal deformation for larger sets S than just $S = \{p, \infty\}$ provided that one confines the image of P_S in such a way that it is abelian. Then one can describe the universal deformation to the extent that one can describe abelian extensions of number fields via class field theory. Essentially one can freely add primes for which the image of Frob_p has distinct eigenvalues and lies inside $G_1 = \bar{\rho}(\mathrm{Gal}(L/F))$, where F is the quadratic subfield corresponding to the canonical C_2 quotient of any projectively dihedral group - or a fixed C_2 quotient if the image of $\bar{\rho}$ in $\mathrm{PGL}_2(k)$ is isomorphic to D_2.

Theorem 4.5. *Given ρ, f, ρ_0 such that G is projectively dihedral and that no irreducible $k[G]$-submodule of $\bar{P}_S \otimes k$ is isomorphic to the two-dimensional irreducible $k[G]$ component of ad. Let F_S^{ab} be the maximal abelian p-extension of F unramified outside S, Γ its Galois group over F and $L^\infty = LF_S^{ab}$. As the order of G is prime to p, $\Gamma = \Gamma^{triv} \oplus \Gamma^F$ where G acts trivially on Γ^{triv} and non-trivially via $Gal(F/\mathbb{Q})$ on Γ^F. We assume that ρ_0 maps the elements of $Gal(L/F)$ to diagonal matrices, which can be done by an appropriate choice of basis for the representation described by ρ_0 provided k is large enough. Then the universal deformation of $\bar{\rho}$, unramified outside*

S, is given by $R_S = W(k)[[\Gamma]]$ and

$$\rho_S : G_{\mathbb{Q}} \longrightarrow Gal(L^\infty/\mathbb{Q}) \cong (Gal(L/F) \times \Gamma) \ltimes Gal(F/\mathbb{Q}) \longrightarrow GL_2(W(k)[[\Gamma]])$$

up to isomorphism, where the first map is the canonical surjection and the second is given by ρ_0 on G, by sending $\gamma \in \Gamma^{triv}$ to γ times the identity matrix, and by sending $\gamma \in \Gamma^F$ to the diagonal matrix with diagonal (γ, γ^{-1}).

Proof. We fix a lift of G to $\mathrm{GL}_2(W(k))$ such that G_1 has its image inside the diagonal matrices. Our assumptions on P_S are chosen so that its image in $\mathrm{GL}_2(R)$ for any deformation ρ to R has to lie inside the commutator subgroup of G_1 considered as a subgroup of $\mathrm{GL}_2(R)$, because the part of $\overline{P}_S$ that is prime to ad is irrelevant. But this is the set of diagonal matrices which is commutative. Hence $P_S \to \mathrm{GL}_2(R)$ factors through P_S^{ab}.

Let $\tilde{P}_S$ be the maximal quotient of P_S^{ab} whose p Frattini quotient is the $k[G]$-submodule of $\overline{P}_S$ that consists of all components isomorphic to k^{triv} or k^{ψ}, ψ the non-trivial C_2 action on k. Then $\mathrm{Gal}(L/F)$ acts trivially on the p Frattini quotient of $\tilde{P}_S$, hence on the whole group. This implies that the corresponding Galois extension is already defined over F. Thus this extension over F must be a subextension of F_S^{ab} as defined in the statement of the theorem. Clearly F_S^{ab} and L are disjoint over F and thus L^∞ as a tensor product is well-defined.

The structure of Γ is also clear, as the Leopoldt conjecture is trivially true over a real quadratic field, and it implies that Γ modulo the Galois group of the maximal cyclotomic p extension is finite. Finally, the image of Γ inside the diagonal matrices is uniquely determined by the action of $\mathrm{Gal}(F/\mathbb{Q}) \cong C_2$. Using this it is easy to verify the above claims concerning (R_S, ρ_S). □

Remark 4.6. 1. The last paragraph of Lemma 4.2 lists all instances where Theorem 4.5 still applies after enlarging S to $S' = S \cup \{q\}$ and where (R_S, ρ_S) is different from $(R_{S'}, \rho_{S'})$.

2. Theorem 4.5 also allows contributions from the class group as long as they do not contain the two-dimensional irreducible component of ad.

3. The assumption on the shape of the image of $\bar{\rho}$, respectively its lift to $\mathrm{GL}_2(W(k))$, is superfluous. The conclusion still holds with the exception that the images of the elements of Γ^F are slightly more difficult to describe.

4. One can formulate Theorem 4.5 also for tame, exceptional G. The condition then is simply that the only $k[G]$-module that ad and $\overline{P}_S \otimes k$ share is k^{triv}, or equivalently that ad^0 is not contained in $\overline{P}_S$. Yet on closer inspection, it turns out that, in the exceptional case, these assumptions are almost equivalent to those in the basic Theorem 2.11. The only case in which this result is stronger than 2.11 is when the splitting field L is wildly ramified with local Galois group surjecting onto A_4 or S_4 - at least the former case can occur which one can easily conclude from part of Lemma 2.6 applied to $\mathbb{Q}_2(\zeta_7)$. The argument is the following.

Suppose that $\overline{C}$ contains a copy of $\mathbb{F}_p^{triv}$. This means that there is an unramified $\mathbb{Z}/(p)$ extension $\tilde{G}$ of G on which G acts trivially. It is not hard to see that this implies $\tilde{G} = G \times \mathbb{Z}/(p)$. Then it would follow that there exists an unramified non-trivial extension of $\mathbb{Q}$, a clear contradiction.

Suppose we have a prime q in S such that L_q contains p-th roots of unity and such that the corresponding part $\mathrm{Ind}_{G_q}^{G} \mu_p$ of $\overline{P}_S$ contains $\mathbf{F}_p^{triv}$. By Frobenius reciprocity this means that G_q must act trivially on μ_p, i.e., that the p-th roots of unity are already in $\mathbb{Q}_q$. One can now go through the classification in Lemma 4.2. This implies that one must be in case (v). As G_q is solvable, its quotient in $\mathrm{PGL}_2(k)$ must be either A_4 or S_4, and hence $q = 2$ - the absolute Galois group of $\mathbb{Q}_q$ is an extension of $(\hat{\mathbb{Z}}/\mathbb{Z}_q) \rtimes \hat{\mathbb{Z}}$ by a pro-q group.

As the cokernel of $\overline{E} \to \sum_{\nu \in \{p\}'} \overline{E}_\nu$ always contains exactly one copy of $\mathbf{F}_p^{triv}$ by Lemma 2.6, our analysis above is sufficient in light of sequence (1) above Lemma 2.6.

4.3. The universal deformation space under enlarging ramification

Here we will simply revisit [Bos2] in order to see to what extend the results there on enlarging the ramification are still valid for even Galois representation. In fact it turns out that all of the results there, that are not alluding to modular forms, remain valid and that the assumptions $a_p \equiv \pm(1+p) \pmod{l}$ and $p \not\equiv 1 \pmod{l}$ - in the notation from there - can be replaced by slightly more general assumptions. The reason for having those assumptions in [Bos2] was simply that those are exactly the assumptions that one needs in the case corresponding to modular forms of weight two and trivial character.

Unlike in [Bos2], there seems to be no interpretation of the results about increasing the ramification in the even case, mainly due to the lack of some kind of forms that would naturally produce even representations. In some rare cases there seem to be relations to Maass forms and two-dimensional complex Galois representations - see [Boe]. Yet the example at the end of this section does suggest that increasing the number of primes that can ramify has similar effects as in the odd case. Although the main question - namely the existence of new deformations to characteristic zero cannot be answered.

We will begin by stating a theorem on the effect on the universal deformation of enlarging the set of primes that can ramify, which holds for even and odd representations. The proof is a simple modification of Sections 1 and 2 in [Bos2] and for the part $f_0 = 1$ of [TaWi, Lemma, p. 569]. Except for one little calculation in the case $f_0 = 2$ in Theorem 4.7, we will just state the necessary lemmas and leave the verifications to the reader, see [Bos2]. For a deformation-theoretic motivation why the number of relations should be the number that we give and that was given in [Bos2], we refer to Remark 4.10.

Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ be any representation such that the centralizer of $\bar{\rho}(G_{\mathbb{Q}})$ is exactly the scalar matrices. $\bar{\rho}$ can be even or odd with splitting field L. We let S be a finite set of rational primes containing p. We let q be a prime not in S, $\mathfrak{q}$ a prime in L above q, $f = |G_{\mathfrak{q}}|$, $f_0 = \min\{m \mid q^m \equiv 1 \pmod{p}\}$ and denote by ξ the f_0-th root of unity in $\mathbf{F}_p$ (or its Teichmüller lift to $\mathbb{Z}_p$) such that $\xi \equiv q \pmod{p}$. We assume

1. $\bar{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues, in k, so $\bar{\rho}(\mathrm{Frob}_q) \sim d \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$ where we denote by ζ the element in k^* as well as its lift to $W(k)^*$.
2. L is unramified at q.
3. $N\mathfrak{q} \equiv 1 \pmod{p}$.

4. $\xi \in \{1, \zeta, \zeta^{-1}\}$.

Note that unless the last two conditions are satisfied, the universal deformations for S and for $S' = S \cup \{q\}$ agree, by prime-to-adjointness, Corollary 4.3 and the remark after it.

Theorem 4.7. *Assume the above assumptions are satisfied and let $S' = S \cup \{q\}$. Then*

1. *If $f_0 > 2$, then there exist power series $r_1, \ldots, r_n, \Phi \in W(k)[[T_1, \ldots, T_m, T]]$, such that if $r = T(q - \Phi)$, then*

$$R_{S'} \cong W(k)[[T_1, \ldots, T_m, T]]/(r_1, \ldots, r_n, r)$$

and $R_S \cong W(k)[[T_1, \ldots, T_m]]/(\bar{r}_1, \ldots, \bar{r}_n)$ where $r_i \pmod{T} = \bar{r}_i$.

2. *If $f_0 = 2$ (so $\zeta = \xi = -1$), given T, U and $V = \sqrt{1 + UT} \in W(k)[[U, T]]$, we define h_i for $i = 0, 1, \ldots$ to be the polynomials in V satisfying the recurrence relation $h_{i+1} - 2Vh_i + h_{i-1} = 0$ with $h_0 = 0$, $h_1 = 1$. Then there are power series $r_1, \ldots, r_n, \Phi$, in the ring $W(k)[[T_1, \ldots, T_m, T, U]]$, such that if $s = T(h_q - \Phi^{-1})$, $t = U(h_q - \Phi)$, then*

$$R_{S'} \cong W(k)[[T_1, \ldots, T_m, T, U]]/(r_1, \ldots, r_n, s, t)$$

and $R_S \cong W(k)[[T_1, \ldots, T_m]]/(\bar{r}_1, \ldots, \bar{r}_n)$ where $r_i \pmod{(T, U)} = \bar{r}_i$.

3. *If $f_0 = 1$, let $N = \max\{m \mid q \equiv 1 \pmod{p^m}\}$. Then there are power series $r_1, \ldots, r_n$, in the ring $W(k)[[T_1, \ldots, T_m, U, T]]$, such that if $s = (1 + U)^{p^N} - 1$, $t = (1 + T)^{p^N} - 1$, then*

$$R_{S'} \cong W(k)[[T_1, \ldots, T_m, T, U]]/(r_1, \ldots, r_n, s, t)$$

and $R_S \cong W(k)[[T_1, \ldots, T_m]]/(\bar{r}_1, \ldots, \bar{r}_n)$ where $r_i \pmod{(T, U)} = \bar{r}_i$.

The corresponding map $\alpha : R_{S'} \to R_S$ sends T, resp. U and T to 0.

Lemma 4.8. *The Galois group over $\mathbb{Q}_q$ of the maximal pro-p extension of L_q is isomorphic to $\mathbb{Z}_p \rtimes (\mathbb{Z}_p \times \mathbb{Z}/(f))$ where the action of $(z, x) \in \mathbb{Z}_p \times \mathbb{Z}/(f) = Z$ on $y \in \mathbb{Z}_p = Y$, written additively, is given by $(z, x)y = \xi^x (q\xi^{-1})^z y$. Y is the inertia subgroup and X a lift of the residual Galois group, so that $(1, 1) \in X$ is a Frobenius element for this Galois group.*

Lemma 4.9. *Given a lift $\rho : G_{\mathbb{Q}} \to GL_2(R)$ of $\bar{\rho}$ we may assume, using strict equivalence, that*

$$\rho(Frob_q) = \rho((0, 1)) = \tilde{d} \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix} \quad \text{and} \quad \rho((1, 1)) = D \begin{pmatrix} 1 & 0 \\ 0 & \phi \end{pmatrix}$$

where $(0, 1)$ and $(1, 1)$ are in Z. With these choices one obtains the following for $\rho(y)$ where $y \in Y$ is a generator

$$f_0 = 1 \qquad \rho(y) = \begin{pmatrix} \tau & 0 \\ 0 & \upsilon \end{pmatrix}, \text{ where } \tau, \upsilon \in \mathfrak{m}_R,$$

$$f_0 = 2 \qquad \rho(y) = \begin{pmatrix} \sqrt{1+v\tau} & \tau \\ v & \sqrt{1+v\tau} \end{pmatrix}, \quad \textit{where} \quad \tau, v \in \mathfrak{m}_R,$$

$$f_0 > 2 \qquad \rho(y) = \begin{pmatrix} 1 & 0 \\ \tau & 1 \end{pmatrix} \textit{ - or the transpose if } \xi = \zeta^{-1}, \textit{ where } \tau \in \mathfrak{m}_R.$$

This applies in particular to the universal deformation $\rho_{S'}$. Furthermore the relations r, s, t in the theorem above are derived from the form of $\rho(y)$ in this lemma.

Proof. We will only remark on the proof of the case $f_0 = 2$, as here in [Bos2] three relations are given, and it is stated afterwards that there is a relation among the three. The three relations given there are the two relations we stated, and the extra relation $r = g_q - V$, where g_q is defined by the same recursion as h_q with different initial values $g_0 = 1$ and $g_1 = V$. We will now briefly explain, why the two we state are sufficient.

The three relations in [Bos2] come from the following equation for matrices.

$$\begin{pmatrix} V & T\Phi^{-1} \\ U\Phi & V \end{pmatrix} = \begin{pmatrix} g_q & Th_q \\ Uh_q & g_q \end{pmatrix}$$

where g_q, h_q are polynomials in $V = \sqrt{1+UT}$. As is remarked in [Bos2], one has the relation $g_q^2 - UTh_q^2 = 1$, as the right hand matrix has determinant one. The same is true for the left hand matrix, as $V^2 - UT = 1$. The three relations r, s, t are precisely the relations coming from equating the matrix entries, as the one-one and two-two entries are the same. Because of the observation on the determinants, one of the three relations is superfluous. To be precise, we show that r is in the ideal generated by s, t.

$$r(g_q + V) = g_q^2 - V^2 = \left(1 - UTh_q^2\right) - \left(1 - UT\Phi\Phi^{-1}\right) = -sUh_q - tT\Phi^{-1}.$$

But $g_q + V \equiv 2 \pmod{\mathfrak{m}}$, i.e., it is a unit, and so $r \in (s,t)$. □

Remark 4.10. 1. In agreement with Proposition 2.8, provided $\mathcal{V}_S = 0$, the number of variables of $R_{S'}$ grows by one in the first case and by two in the other two cases.

2. In the case that $f_0 > 2$, the assumption that both eigenvalues of the Frobenius are in k is automatically satisfied. This follows from

$$\det(\bar{\rho}(\mathrm{Frob}_p)) = d^2\left(\xi^{\pm 1}\right), \quad \mathrm{trace}(\bar{\rho}(\mathrm{Frob}_p)) = d\left(1 + \xi^{\pm 1}\right) \in k^*, \quad \xi \in \mathbf{F}_p^*.$$

If the eigenvalues are distinct, but not in k, the above presentations of $R_{S'}$ are valid after tensoring over $W(k)$ with $W(k')$, where k' is the unique qudratic extension of k.

3. In [Bos2] the eigenvalues are distinct, because of the congruence conditions, and they are in k, as one of them is always ± 1 [Bos2, Lemma 3]. Also under the conditions there the cases $f > 2$ and $f = 2$ directly correspond to the cases $p \not\equiv \pm 1 \pmod{l}$ and $p \cong -1 \pmod{l}$, resp., f agrees with f_0 and ξ with ζ.

4. Reconsidering the case $f_0 = 2$ and explicitly giving two equations as was done here, was stimulated by the following observation, that is already present in [Maz]. If the ring $R_S/(p)$ has the expected dimension, i.e., one in the even and three in the odd case, then by propositions two and five from loc. cit., the ring $R_S/(p)$ is actually a complete intersection. If in addition R_S is flat over $W(k)$ it has to be a complete

intersection itself. So from this one should expect that, at least modulo p, if the number of variables increases by two, the number of equations should not increase by more than two.

5. Also what we found, in all the cases considered, is that the number of additional equations needed to describe R_S, when adding the prime q to S, is exactly $\dim_k H^2(G_{\mathbb{Q}_q}, \mathrm{ad})$, where we consider ad restricted to $G_{\mathbb{Q}_q}$ – this is an easy exercise using Tate local duality. This is a restatement of the previous item, as for large sets S, large meaning that the obstruction $\mathcal{V}_S$ vanishes, the increment of the number of variables in the universal deformation ring is the increment of the k-dimension of $H^1(G_{\mathbb{Q},S}, \mathrm{ad})$ if we replace S by $S \cup \{q\}$, and this is the increment of the k-dimension of $H^2(G_{\mathbb{Q},S}, \mathrm{ad})$ which, under the assumption that S is large, is the k-dimension of $H^2(G_{\mathbb{Q}_q}, \mathrm{ad})$.

As an example we will now present a universal deformation which is not twist-finite, but whose residual representation is tame and absolutely irreducible. Twist-finite means that after twisting the universal representation with a suitable p-adic character of $G_{\mathbb{Q}}$ it will have finite image. Typical examples for a twist-finite representation are those arising from 4.5 and from 3.1.

Example 4.11. We fix a tame absolutely irreducible even representation $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$ that is neat at p and let $S = \{p\}$. Then we pick a prime q such that Frob_q has distinct eigenvalues in k and is not of order 2. By the Cebotarev density theorem it is obvious that sufficiently many primes of this type exist. Let $S' = S \cup \{q\}$. So from the above we have an explicit description of the universal deformation ring

$$R_{S'} \cong W(k)[[T_1, T]]/(r_1, \ldots, r_n, r)$$

where T divides r_i for $i = 1, \ldots, n$, $r = T(q - \Phi)$ and $r_1, \ldots, r_n, r \in W(k)[[U, T]]$.

Now we make the following additional assumptions. We assume that the splitting field L has dihedral Galois group D_n of order $2n$ that embeds into the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(k)$, that Frob_q generates C_n inside D_n, and that $n > 2$. As in Lemma 4.9, we may assume that the image under the universal deformation of a generator of the inertia group of $G_{\mathbb{Q}_q}$ is $\left(\begin{smallmatrix} 1 & T \\ 0 & 1 \end{smallmatrix}\right)$, where we assume that a lift of D_n to $\mathrm{GL}_2(W(k))$ has been chosen so that the the image of C_n is contained in the diagonal matrices, and so that $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is in the image. We enlarge k if necessary. By conjugation with the latter element we find that $\left(\begin{smallmatrix} 1 & 0 \\ T & 1 \end{smallmatrix}\right)$ is in the image as well.

Lemma 4.12. *The topologically closed subgroup of $SL_2(W(k)[[T]])$ generated by $\left(\begin{smallmatrix} 1 & 0 \\ T & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & T \\ 0 & 1 \end{smallmatrix}\right)$ is the set of all matrices*

$$\begin{pmatrix} 1 + a(t) & b(t) \\ c(t) & 1 + d(t) \end{pmatrix}$$

of determinant one, with a, b, c, $d \in (p, t) \subset W(k)[[T]]$ such that a, d are even and b, c are odd power series, i. e., in the power series expansion of a, d all odd powers

If T have zero coefficient and similarly in the expansion for b, c all even powers of T have zero coefficient.

This can be shown by first working modulo T^2 and then increasing recursively the exponent and computing some commutators.

From the five term sequence 2.1 on can compute that P_S has three generators, and, for instance by [Koch, §11], one can see that they are given by the generators of the local inertia groups and by the generator of the cyclotomic p extension of L. Hence their image in $\mathrm{GL}_2(W(k)[[U,T]])$ without imposing any relations, only the constraints from the G action, and using strict equivalence, are

$$\begin{pmatrix} 1 & 0 \\ T & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1+U & 0 \\ 0 & 1+U \end{pmatrix}.$$

This implies for the element $D\begin{pmatrix} 1 & 0 \\ 0 & \phi \end{pmatrix}$ in Lemma 4.9, which has to be an expression in the above three matrices and the lifts of G, that ϕ must be ζ plus T^2 times a power series in $W(k)[[T]]$.

As the pro-p group $P_{S'}$ has only local relations, and up to Galois conjugates only one [Koch, §11] there are no further relations among the elements U, T but the one computed in [Bos2] and quoted above, namely $T(q-\Phi)=0$. By the Weierstraß preparation theorem we can rewrite the second factor

$$\begin{aligned} q-\Phi &= q-\zeta+T^2 f(T) \\ &= p^\kappa a_0 + T^2 a_2 + T^3 a_3 + \cdots \\ &= p^j(b_0 + b_2 T^2 + \cdots + T^r)u \end{aligned}$$

where u is a unit in $W(k)[[T]]$, the b_i have positive valuation, and $0 \le j \le \kappa$. We note that $r=0$ in the case $\kappa = j$. One obtains

$$R_S \;\cong\; W(k)[[U,T]]/\left(Tp^j\left(b_0 + b_2T^2 + \ldots + b_rT^r\right)\right).$$

From the above lemma it is more or less obvious that the image of $G_{\mathbb{Q}}$ under ρ_S cannot be twist-finite. If $0 < j$, we consider the image of R_S in $k[[T]]$ where we send U to T and p to 0. By the above lemma the image generated by P_S, which has to be topologically closed by the compactness of P_S and the continuity of the homomorphism, contains all matrices as claimed in the lemma and all scalar matrices and hence cannot be twist-finite. In fact the order of the image modulo T^{n+1} is $p^{(5n-2)/2}$ while the order of $\Gamma_2\left(k[[T]]/\left(T^{n+1}\right)\right)$ has order p^{4n}.

In the other case we let α be one of the solutions of $b_0 + b_2T^2 + \cdots + T^r = 0$. Then α must have positive valuation and we consider the image obtained by mapping R_S to $W(k)[\alpha]$ by sending T and U to α. Again by the above lemma, the image of P_S in $\mathrm{GL}_2(W(k)[\alpha])$ cannot be twist-finite.

Finally there seems another remark worth while. In the odd case, as done in [Bos2], the growth of the universal deformation space corresponds directly to the appearance of new modular forms of higher level. If, in a vague analogy, based on the fact that even deformations should be rigid once the determinant is fixed, one would consider lifts to $W(k)$, or a finite extension of it, with a given fixed determinant as forms,

then will there arise new forms if one increases the set of primes that can ramify appropriately? If above $j < k$ or even better $j = 0$, then this would obviously be the case. The natural question that occurs now is the following.

Problem 4.13. Let K be a totally real algebraic number field. Let $g \in G_{\mathbb{Q}}$ be such that its image generates $\mathrm{Gal}(\bigcup_n K(\zeta_{p^n})/K(\zeta_p))$. Let A be a local complete noetherian k-algebra. Do there exist Galois representations $\rho : G_K \to \mathrm{GL}_2(A)$, unramified outside a finite set of places, sending g to the identity, such that the image of ρ is infinite? What about the special case $A = \mathbf{F}_p[[T]]$?

If the image is always finite, then clearly $j = 0$ and so all the solutions of $b_0 + b_2T^2 + \cdots + T^r = 0$ will give lifts to characterstic zero that lie in a finite extension of $W(k)$. On the other hand this question seems not so easy as a finite image in all such cases would imply that the dimension of the universal deformation ring modulo p is one in the even case, which might be expected, but is not known. At the same time, if in the above example one has $j > 0$, then modulo p the universal deformation space would be $k[[S,T]]$ and thus this would provide an example where the dimension is indeed bigger than one. These observations can be generalized as follows.

Let K be a totally real number field and $\bar{\rho} : G_K \to GL_2(k)$ an absolutely irreducible Galois representation which is even at all infinite places. Let S be a set of places of K, and R_S the universal deformation ring for deformations of $\bar{\rho}$ unramified outside S. Let $\overline{R}_S = R_S/(p)$, $\overline{R}'_S$ the quotient of $\overline{R}_S$ for deformations with fixed determinant equal to $\det(\bar{\rho})$, and Γ_S the Galois group of the maximal outside S unramified abelian pro-p extension of K. It is not hard to see that

$$\overline{R}_S = \overline{R}'_S \hat{\otimes} k[[\Gamma_S]] .$$

Theorem 4.14. *Under the assumptions of the previous paragraph, the following are equivalent.*

1. *The Krull dimension of $\overline{R}_S$ is one.*
2. *K satisfies the Leopoldt conjecture and all deformations of $\bar{\rho}$ to rings $R \in \mathcal{C}$ of characteristic p are twist-finite.*

If one wants to avoid the Leopoldt conjecture, the following equivalence holds.

1. *The Krull dimension of $\overline{R}'_S$ is zero, i. e., $\overline{R}'_S$ is finite.*
2. *All deformations of $\bar{\rho}$ to rings $R \in \mathcal{C}$ of characteristic p are twist-finite.*

It is a conjecture by MAZUR, *that the Krull dimension of $\overline{R}'_S$ is always zero, and so if this were true, indeed all deformations of $\bar{\rho}$ were twist-finite. In particular, one could never have $SL_2(\mathbf{F}_p[[T]])$ in the image of such a representation, or the subgroup described in Lemma* 4.12.

Proof. As the Krull dimension of $k[[\Gamma_S]]$ is always greater or equal to one, the first equivalence follows from the second by the remark preceding the theorem.

Also if $\overline{R}'_S$ is finite, then clearly the image of any deformation must be twist finite. To show the converse, we assume that the image of $\bar{\rho}_S$, the reduction of ρ_S modulo p, is twist finite. Then $\bar{\rho}'_S$, corresponding to $\overline{R}'_S$, has finite image. Let N be the intersection of im $(\bar{\rho}'_S)$ with the kernel of $GL_2(\overline{R}'_S) \to GL_2(k)$. Thus N is a finite p

group, say of exponent p^n. Let $\mathfrak{m}$ be the maximal ideal of $\overline{R}'_S$. By considering the subrepresentations of ad^0 one can find elements $\sigma_i \in G_K$ and matrices $A_i \in \mathrm{GL}_2(k)$ such that

$$A_i \bar{\rho}'_S(\sigma_i) A_i^{-1} \equiv \begin{pmatrix} 1+T_i & 0 \\ 0 & 1-T_i \end{pmatrix} \pmod{\mathfrak{m}^2}$$

where $T_1, \ldots, T_s$ denotes a set of generators of $\mathfrak{m}/\mathfrak{m}^2$. If necessary, we first enlarge k to a field k' that contains all eigenvalues of all elements of $\bar{\rho}$, which can be done as this would only replace $\overline{R}'_S$ by $\overline{R}'_S \otimes_k k'$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv A_i \bar{\rho}'_S(\sigma_i)^{p^n} A_i^{-1} \equiv \begin{pmatrix} 1+T_i^{p^n} & 0 \\ 0 & 1-T_i^{p^n} \end{pmatrix} \pmod{\mathfrak{m}^{p^n+1}},$$

and so $(T_1^{p^n}, \ldots, T_s^{p^n}) \in \mathfrak{m}^{p^n+1}$. – It is perhaps not completely obvious, that $A \equiv \left(\begin{smallmatrix} 1+T_i & 0 \\ 0 & 1-T_i \end{smallmatrix}\right) \pmod{\mathfrak{m}^2}$ implies that $A^{p^n} \equiv \left(\begin{smallmatrix} 1+T_i^{p^n} & 0 \\ 0 & 1-T_i^{p^n} \end{smallmatrix}\right) \pmod{\mathfrak{m}^{p^n+1}}$ over a ring of characteristic p. But it can be checked by a somewhat tedious but straightforward calculation. – This implies that

$$\mathfrak{m}^{sp^n-1} \subset (T_1^{p^n}, \ldots, T_s^{p^n}) \mathfrak{m}^{(s-1)p^n-1} \subset \mathfrak{m}^{sp^n}.$$

Hence $\mathfrak{m}^{sp^n-1} = 0$, and so $\overline{R}'_S$ is artinian. □

The above problem might be compared with conjectures of FONTAINE and MAZUR [FoMa, §7] concerning representations of G_F into $\mathrm{GL}_n(W(k))$, F any number field, that are unramified at all primes above p and only ramified at finitely many primes, where as usual k has characteristic p. They conjecture that in this case the image of the representation must be finite.

Acknowledgements

I would like to thank very much Professor N. BOSTON *for his continuing support for this project, which comprises a large part of my thesis, and for many interesting discussions I had with him, and furthermore Professor* B. MAZUR *for several helpful comments, and the referee for carfully reading the manuscript. Large parts of this were written while benefitting from an invitation of Professer* H. CARAYOL *at the Université Louis Pasteur at Strasbourg.*

References

[AAC] ANKENY, N.C., ARTIN, E., CHOWLA, S.: The Class Number of Real Quadratic Number Fields, Ann. Math. **56**, (3) (1952), 479–493

[Boe] BÖCKLE, G.: Points in the Deformation Space of an Even Galois Representation Corresponding to Maass Wave Forms, preprint

[Bos1] BOSTON, N.: Explicit Deformations of Galois Representations, Invent. Math. **103** (1990), 181–196

[Bos2] BOSTON, N.: Families of Galois Representations – Increasing the Ramification, Duke Math. Journ. **66**, Vol. **3** (1992), 357–367

[BoMa] BOSTON, N., and MAZUR, B.: Explicit Universal Deformations of Galois Representations, Adv. Stud. Pure Math **17** (1989), 1 - 21

[BoUl] BOSTON, N., and ULLOM, S.: Representations Related to CM Elliptic Curves, Math. Proc. Camb. Phil. Soc. **113** (1993), 71 - 85

[Bro] BROWN, K. S.: Cohomology of Groups, GTM 87, Springer - Verlag, 1982

[Dic] DICKSON, L. E.: Linear Groups with an Exposition of the Galois Field Theory, Teubner, Leipzig, 1901

[FoMa] FONTAINE, J. - M., and MAZUR, B.: Geometric Galois Representations. In: Elliptic Curves, Modular Forms and Fermat's Last Theorem, ed. by J. COATES, International Press, Cambridge.

[Fla] FLACH, M.: A Finiteness Theorem for the Symmetric Square of an Elliptic Curve, Invent. Math. **109** (1992), 307 - 327

[Kha] KHARE, C.: Base Change, Lifting and Serre's Conjecture, J. Number Theory **63**, No. 2 (1997), 387 - 395

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

[Maz] MAZUR, B.: Deforming Galois Representations, in Galois groups over $\mathbb{Q}$, ed. IHARA et al., Springer - Verlag, 1987

[Mov] MOVAHHEDI, A.: Sur les p - Extensions des Corps p - Rationnels, Math. Nachr. **149** (1990), 163 - 176

[Mos] MOSER, N.: Unités et Nombres des Classes d'une Extension Galoisienne Diédrale de $\mathbb{Q}$, Abh. Math. Sem. Univ. Hamburg **48** (1979), 151 - 178

[Nar] NARKIEWICZ, W.: Elementary and Analytical Theory of Algebraic Numbers, PWN - Polish Scientific Publishers, Warsaw, 1974

[Neu] NEUKIRCH, J.: Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen, J. reine angew. Math. **259** (1973), 1 - 47

[Neu1] NEUMANN, O.: Relativ - quadratische Zahlkörper, deren Klassenzahl durch drei teilbar ist, Math. Nachr. **56** (1973), 281 - 306

[Neu2] NEUMANN, O.: On p - Closed Number Fields and an Analogue of Riemann's Existence Theorem. In: Algebraic Number Fields (L - Functions and Galois Properties), Ed. A. FRÖHLICH, Academic Press, 1977

[Ram] RAMAKRISHNA, R.: On a Variation of Mazur's Deformation Functor, Comp. Math. **87** (1993), 269 - 286

[Ste] STENDER, H. - J.: Einheiten für eine allgemeine Klasse total reeller algebraischer Zahlkörper, J. Reine Angew. Math. **257** (1972), 151 - 178

[TaWi] TAYLOR, R., and WILES, A.: Ring Theoretic Properties of Certain Hecke Algebras, Ann. of Math. **141**, No. 3 (1995), 553 - 572

[Win1] WINGBERG, K.: On Galois Groups of p - Closed Algebraic Number Fields with Restricted Ramification II, J. reine angew. Math. **416** (1991), 187 - 194

[Win2] WINGBERG, K.: Galois Groups of Poincaré Type over Algebraic Number Fields. In: Galois Groups over $\mathbb{Q}$, ed. IHARA et al., Springer - Verlag, 1987

Lehrstuhl für Mathematik (Prof. Pink)
Universität Mannheim
D 7, 27
D - 68131 Mannheim
Germany
e - mail:
boeckle@math.uni - mannheim.de