TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 365, Number 11, November 2013, Pages 6149–6165
S 0002-9947(2013)05848-5
Article electronically published on May 14, 2013

INVERSE PROBLEMS FOR DEFORMATION RINGS

FRAUKE M. BLEHER, TED CHINBURG, AND BART DE SMIT

Abstract. Let W be a complete Noetherian local commutative ring with residue field k of positive characteristic p. We study the inverse problem for the universal deformation rings $R_W(\Gamma, V)$ relative to W of finite dimensional representations V of a profinite group Γ over k. We show that for all p and $n \geq 1$, the ring $W[[t]]/(p^n t, t^2)$ arises as a universal deformation ring. This ring is not a complete intersection if $p^n W \neq \{0\}$, so we obtain an answer to a question of M. Flach in all characteristics. We also study the 'inverse inverse problem' for the ring $W[[t]]/(p^n t, t^2)$; this is to determine all pairs (Γ, V) such that $R_W(\Gamma, V)$ is isomorphic to this ring.

1. Introduction

Let W be a complete Noetherian local commutative ring with residue field k of positive characteristic p. Suppose Γ is a profinite group and that V is a continuous finite dimensional representation of Γ over k. Here the topology on V is discrete, so the image of the continuous homomorphism $\Gamma \to \mathrm{Aut}_k(V)$ is finite. In §2 we recall the definition of a deformation of V over a complete Noetherian local commutative W-algebra with residue field k. Under a mild hypothesis on the representation ($\mathrm{End}_{k\Gamma}(V) = k$) and on the profinite group Γ (Hypothesis 2.1 below), there is a unique universal deformation over the so-called universal deformation ring $R_W(\Gamma, V)$. We will recall its basic properties in the next section.

In this paper we consider the following inverse problem:

Question 1.1. Which complete Noetherian local W-algebras R with residue field k are isomorphic to $R_W(\Gamma, V)$ for some Γ and V as above?

It is important to emphasize that in this question W is fixed, but Γ and V are not fixed. Thus for a given W-algebra R, one would like to construct both a profinite group Γ and a continuous finite dimensional representation V of Γ over k for which $R_W(\Gamma, V)$ is isomorphic to R.

One can also consider the following "inverse inverse" problem:

Question 1.2. Suppose R is a complete Noetherian local W-algebra with residue field k. What are all pairs (Γ, V) as above such that $R \cong R_W(\Gamma, V)$?

Received by the editors February 24, 2012 and, in revised form, April 5, 2012.
2010 *Mathematics Subject Classification.* Primary 11F80; Secondary 11R32, 20C20.
Key words and phrases. Universal deformation rings, complete intersections, inverse problems.
The first author was supported in part by NSF Grant DMS0651332 and NSA Grant H98230-11-1-0131. The second author was supported in part by NSF Grants DMS0801030 and DMS1100355. The third author was funded in part by the European Commission under contract MRTN-CT-2006-035495.

The goal of this paper is to answer Questions 1.1 and 1.2 for the rings $R = W[[t]]/(p^n t, t^2)$, where n is a positive integer. More precisely, we prove the following main results.

Theorem 1.3. *For every $n \geq 1$ there is a representation V of a finite group Γ over k such that $R_W(\Gamma, V)$ is isomorphic to*

$$W[[t]]/(p^n t, t^2)$$

as a W-algebra. If $p^n W \neq 0$, then this ring is not a complete intersection.

Note that $W[[t]]/(p^n t, t^2)$ is not even a Cohen-Macaulay ring in general.

Theorem 1.4. *Suppose that k is perfect and let $\mathrm{W}(k)$ be the ring of infinite p-Witt vectors over k. Then there exists a complete classification, given in Theorem 3.1, of all profinite groups Γ and all continuous finite dimensional representations V of Γ over k such that the following conditions hold:*

1. *$\mathrm{End}_{k\Gamma}(V) = k$ and Hypothesis 2.1 holds;*
2. *V is projective as a module over kG, where G denotes the image of Γ in $\mathrm{Aut}_k(V)$;*
3. *the universal deformation of V is faithful as a representation of Γ;*
4. *the universal deformation ring $R_W(\Gamma, V)$ is isomorphic to*

$$\mathrm{W}(k)[[t]]/(p^n t, t^2).$$

There is an extensive literature concerning explicit computations of universal deformation rings (often with additional deformation conditions). In [6], Böckle gives a survey of recent results on presentations of deformation rings and of applications of such presentations to arithmetic geometry. This includes many examples of rings which are known to be deformation rings. There is also a discussion in [6] of how one can show that deformation rings are complete intersections as well as the relevance of presentations to arithmetic, e.g. to Serre's conjectures in the theory of modular forms and Galois representations.

The problem of constructing representations having universal deformation rings which are not complete intersections was first posed by M. Flach [8]. The first example of a representation of this kind was found by Bleher and Chinburg when $\mathrm{char}(k) = 2$; see [3, 4]. A more elementary argument proving the same result was given in [7]. Theorem 1.3 gives an answer to Flach's question for all possible residue fields of positive characteristic.

As of this writing we do not know of a complete local commutative Noetherian ring R with perfect residue field k of positive characteristic which cannot be realized as a universal deformation ring of the form $R_{\mathrm{W}(k)}(\Gamma, V)$ for some profinite Γ and some representation V of Γ over k.

Theorem 1.3 and the formulation of the inverse problem in Question 1.1 first appeared in [5]. In subsequent work on the inverse problem, Rainone found in [16] some other rings which are universal deformation rings and not complete intersections; see Remark 4.3.

The sections of this paper are as follows.

In §2 we recall the definitions of deformations and of versal and universal deformation rings and describe how versal deformation rings change when extending the residue field k (see Theorem 2.2).

In §3 we consider arbitrary perfect fields k of characteristic p and we take $W = \mathrm{W}(k)$. In Theorem 3.1, which implies Theorem 1.4, we give a sufficient and

necessary set of conditions on a representation $\tilde{V}$ of a finite group Γ over k for the universal deformation ring $R_{\mathrm{W}(k)}(\Gamma, \tilde{V})$ to be isomorphic to $R = \mathrm{W}(k)[[t]]/(p^n t, t^2)$. The proof that these conditions are sufficient involves first showing that $R_{\mathrm{W}(k)}(\Gamma, \tilde{V})$ is a quotient of $\mathrm{W}(k)[[t]]$ by proving that the dimension of the tangent space of the deformation functor associated to $\tilde{V}$ is one. We then construct an explicit lift of $\tilde{V}$ over R and show that this cannot be lifted further to any small extension ring of R which is a quotient of $\mathrm{W}(k)[[t]]$.

In §4 we prove Theorem 1.3. We use Theorem 2.2 to reduce the proof of Theorem 1.3 to the case in which $k = \mathbb{F}_p = \mathbb{Z}/p$ and $W = \mathrm{W}(k) = \mathbb{Z}_p$. In the latter case we provide explicit examples using Theorem 3.1 and twisted group algebras of the form $\mathbb{F}_{p^2}^{\dagger} G_0$ where $G_0 = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. Some further examples illustrating Theorem 1.3 are given in §5.

2. Deformation rings

Let Γ be a profinite group, let k be a field of characteristic $p > 0$, and let W be a complete Noetherian local ring with residue field k. We denote by $\hat{\mathcal{C}}$ the category of all complete Noetherian local W-algebras with residue field k. Morphisms in $\hat{\mathcal{C}}$ are W-algebra homomorphisms — they are continuous and they induce the identity map on residue fields.

Let V be a finite dimensional vector space over k that is endowed with a continuous k-linear action of Γ, i.e., a continuous group homomorphism from Γ to the discrete group $\mathrm{Aut}_k(V)$. A *lift* of V over a ring $A \in \hat{\mathcal{C}}$ is then a pair (M, ϕ) consisting of a finitely generated free A-module M on which Γ acts continuously together with a Γ-equivariant isomorphism $\phi\colon\ k \otimes_A M \to V$ of k-vector spaces. We define the set $\mathrm{Def}_V(A)$ of *deformations* of V over A to be the set of isomorphism classes of lifts of V over A. If $\alpha : A \to A'$ is a morphism in $\hat{\mathcal{C}}$, then we define the map

$$\mathrm{Def}_V(\alpha)\colon\ \mathrm{Def}_V(A) \to \mathrm{Def}_V(A') \quad \text{by} \quad [M, \phi] \mapsto [A' \otimes_{A,\alpha} M, \phi_\alpha]$$

where ϕ_α is the composition

$$k \otimes_{A'} (A' \otimes_{A,\alpha} M) \cong k \otimes_A M \xrightarrow{\phi} V.$$

With these definitions $\mathrm{Def}_V(-)$ is a functor from $\hat{\mathcal{C}}$ to the category of sets.

We can describe $\mathrm{Def}_V(A)$ in terms of matrix groups as follows. By choosing a k-basis of V we can identify V with k^d. The Γ-action on V is then given by a continuous homomorphism $\rho : \Gamma \to \mathrm{GL}_d(k)$. Let A be a ring in $\hat{\mathcal{C}}$ and denote the reduction map $\mathrm{GL}_d(A) \to \mathrm{GL}_d(k)$ by π_A. By a *lift* of ρ over a ring A in $\hat{\mathcal{C}}$ we mean a continuous homomorphism $\tau : \Gamma \to \mathrm{GL}_d(A)$ such that $\pi_A \circ \tau = \rho$. Such a lift defines a Γ-action on $M = A^d$ and with the obvious isomorphism $\phi : M \otimes_A k \to V$ such a lift defines a deformation $[M, \phi]$ of V over A. Two lifts $\tau, \tau' : \Gamma \to \mathrm{GL}_d(A)$ of ρ over A give rise to the same deformation if and only if they are *strictly equivalent*, that is, if one can be brought into the other by conjugation by a matrix in the kernel of π_A. In this way the choice of a basis of V gives rise to an identification of $\mathrm{Def}_V(A)$ with the set $\mathrm{Def}_\rho(A)$ of strict equivalence classes of lifts of ρ over A.

The functor $\mathrm{Def}_V(-) = \mathrm{Def}_\rho(-)$ is representable if there is a ring R in $\hat{\mathcal{C}}$, and a lift (U, ϕ_U) of V over R so for all A in $\hat{\mathcal{C}}$ the map

$$f_A : \mathrm{Hom}_{\hat{\mathcal{C}}}(R, A) \to \mathrm{Def}_V(A) \qquad \alpha \mapsto \mathrm{Def}_V(\alpha)([U, \phi_U])$$

is bijective. If this is the case, then R is said to be the universal deformation ring of V and we write $R = R_W(\Gamma, V) = R_W(\Gamma, \rho)$. The defining property determines R uniquely up to a unique isomorphism.

A slightly weaker notion can be useful if the functor $\mathrm{Def}_V(-)$ is not representable. The ring $k[\epsilon]$ of dual numbers with $\epsilon^2 = 0$ has W-algebra structure such that the maximal ideal of W annihilates $k[\epsilon]$. One says R is a versal deformation ring of V if the maps f_A are surjective for all A, and bijective for $A = k[\epsilon]$. These conditions determine $R = R_W(\Gamma, V) = R_W(\Gamma, \rho)$ uniquely up to isomorphism, but the isomorphism need not be unique. By Mazur [15, Prop. 20.1] the functor $\mathrm{Def}_V(-)$ is continuous, which means that one only needs to check the surjectivity of f_A for Artinian A.

We will suppose from now on that Γ satisfies the following p-finiteness condition used by Mazur in [14, §1.1]:

Hypothesis 2.1. *For every open subgroup J of finite index in Γ, there are only finitely many continuous homomorphisms from J to $\mathbb{Z}/p$.*

It follows by [14, §1.2] that for Γ satisfying Hypothesis 2.1, all finite dimensional continuous representations V of Γ over k have a versal deformation ring. It is shown in [10, Prop. 7.1] that if $\mathrm{End}_{k\Gamma}(V) = k$, then V has a universal deformation ring.

A proof of the following base change result is given in an appendix (see §6). For finite extensions of k, this was proved by Faltings (see [21, Ch. 1]).

Theorem 2.2. *Let Γ, k, W and V be as above. Suppose that we have a local homomorphism $W \to W'$ of complete Noetherian local rings, and denote the residue field of W' by k'. Then the versal deformation ring $R_{W'}(\Gamma, V \otimes_k k')$ is the completion of the local ring $W' \otimes_W R_W(\Gamma, V)$.*

3. The inverse inverse problem for $R = \mathrm{W}(k)[[t]]/(p^n t, t^2)$

In this section k denotes a perfect field k of positive characteristic p, and $W = \mathrm{W}(k)$ is the ring of infinite p-Witt vectors over k, which is a complete discrete valuation ring of characteristic 0, residue field k, and uniformizer p.

We let Γ be a profinite group satisfying Hypothesis 2.1, and we let V be a finite dimensional continuous representation of Γ over k that satisfies $\mathrm{End}_{k\Gamma}(V) = k$. By the previous section we then know that universal deformation ring $R_W(\Gamma, V)$ exists.

We let K be the kernel of the group homomorphism $\Gamma \to \mathrm{Aut}_k(V)$ and we let G be the image. Then G is a finite group, and we make the additional assumption that V is projective as a kG-module. The group Γ acts by conjugation on K, and if K is abelian, then this makes K into a $\mathbb{Z}G$-module.

Since V is a projective kG-module there is a unique deformation $[V_W, \varphi]$ of the kG module V to W such that V_W is projective as a WG-module [19, Prop. 42, §14.4]. Note that φ then provides an identification of $V_W/pV_W = V_W \otimes_W k$ with V. Note also that $M_W = \mathrm{End}_W(V_W)$ has the structure of a (possibly non-commutative) W-algebra by composition of endomorphisms. The natural G-action on M_W by conjugation also makes it into a WG module, and since V_W is a projective WG-module, so is M_W. In the same way the k-algebra $M = \mathrm{End}_k(V) = M_W/pM_W$ is a projective kG-module.

Theorem 3.1. *For all k, Γ, V as above, and all $n \geq 1$ the following statements (i) and (ii) are equivalent.*

(i) *The group* Γ *acts faithfully on the universal deformation of* V*, and the universal deformation ring* $R_W(\Gamma, V)$ *is isomorphic to* $W[[t]]/(p^n t, t^2)$.

(ii) *The following conditions hold:*

(a) *the group* $\mathrm{Hom}^{cont}(K, M)^G$ *of continuous* G*-equivariant homomorphisms from* K *to* M *has dimension* 1 *as a vector space over* k*;*

(b) *there is a continuous injective* G*-equivariant homomorphism*

$$\alpha\colon\ K \to M_W/p^n M_W$$

such that

- *there exist* $g, h \in K$ *with*

$$\alpha(g) \circ \alpha(h) \not\equiv \alpha(h) \circ \alpha(g) \bmod pM_W/p^n M_W,$$

or

- $n = 1$, $p = 2$ *and there is no* $a \in k$ *such that for all* $g \in K$ *we have* $\alpha(g)^2 = a\,\alpha(g)$.

Each of conditions (i) and (ii) implies that the group Γ *is finite and* K *is abelian.*

Note that Theorem 3.1 implies Theorem 1.4. To show Theorem 1.3, we construct in Section 4 examples for which the conditions in Theorem 3.1(ii) are satisfied. The rest of this section is devoted to the proof of Theorem 3.1. We first establish some basic cohomological results that will be used in the proof.

Lemma 3.2. *With the assumptions prior to the statement of Theorem* 3.1 *the following conditions hold:*

(1) $H^i(G, M_W/p^\ell M_W) = 0$ *for all* $i \geq 1$ *and* $\ell \geq 0$*;*

(2) $H^1(\Gamma, M)$ *and* $\mathrm{Hom}^{cont}(K, M)^G$ *are isomorphic vector spaces over* k*;*

(3) *the restriction map* $H^2(\Gamma, M) \to H^2(K, M)$ *is injective.*

Proof. To see (1), note that $M_W/p^\ell M_W$ is a projective module over the group ring $(W/p^\ell W)G$, so it is cohomologically trivial as a $\mathbb{Z}G$-module.

The inflation-restriction sequence for $M = M_W/pM_W$ now gives an exact sequence

$$0 = H^1(G, M) \longrightarrow H^1(\Gamma, M) \longrightarrow H^1(K, M)^G \longrightarrow H^2(G, M) = 0.$$

Using the equalities $H^1(K, M)^G = \mathrm{Hom}^{cont}(K, M)^G$ we see that (2) holds.

It remains to show (3). Since M is a finitely generated projective kG-module, $\mathrm{Hom}^{cont}(K, M)$ is isomorphic to a direct summand of a kG-module that is induced from the trivial subgroup of G, so $H^1(K, M) = \mathrm{Hom}^{cont}(K, M)$ is a cohomologically trivial kG-module. This implies that the Lyndon/Hochschild-Serre spectral sequence for $H^2(\Gamma, M)$ degenerates, and we get isomorphisms

$$\begin{aligned} H^2(\Gamma, M) &\cong H^0(G, H^2(K, M)) \\ &\cong H^2(K, M)^G \subset H^2(K, M), \end{aligned}$$

where the composite map is the restriction map [20, Theorem 6.8.2]. □

Lemma 3.3. *Condition (ii)(a) in Theorem* 3.1 *is equivalent to the condition that* $R_W(\Gamma, V)$ *is of the form* $W[[t]]/I$ *where the ideal* I *is contained in* $\mathfrak{m} = (p, t^2)$.

Proof. For a ring A in $\hat{\mathcal{C}}$ we denote its maximal ideal by $\mathfrak{m}_A$. The cotangent space t_A^* of A is the vector space $\mathfrak{m}_A/(\mathfrak{m}_A^2 + pA)$ over k. Recall that a morphism $A \to B$ in $\hat{\mathcal{C}}$ is surjective if and only if the induced map $t_A^* \to t_B^*$ is surjective,

and that $\dim_k t_A^*$ is the minimal number s so that A is isomorphic to a quotient of $W[[t_1, \ldots, t_s]]$. For $R = R_W(\Gamma, V)$ the tangent space $t_R = \mathrm{Hom}_k(t_R^*, k)$ is naturally isomorphic to $H^1(\Gamma, M)$ [14, p. 391]. Combining this with the previous lemma we see that condition (ii)(a) in Theorem 3.1 is equivalent to $\dim_k t_R = 1$. Rings of the form stated clearly have 1-dimensional cotangent spaces. Conversely, if t_R^* is 1-dimensional, then any morphism $W[[t]] \to R$ in $\hat{\mathcal{C}}$ sending t to an element of $\mathfrak{m}_R$ which is not zero in t_R^*, is surjective and its kernel is contained in (p, t^2). □

3.1. **Proof that (ii) implies (i) in Theorem 3.1.** Throughout this subsection, we assume that condition (ii) of Theorem 3.1 holds. Put $d = \dim_k(V)$, choose a basis of V_W over W and let the G-action on V_W be given by $\rho_W \colon G \to \mathrm{GL}_d(W)$. We put

$$\begin{aligned} R &= W[[t]]/(p^n t, t^2) \\ &= W \oplus (W/p^n W)t. \end{aligned}$$

The morphism $R \to W$ in $\hat{\mathcal{C}}$ sending t to 0 gives rise to an exact sequence of groups

$$0 \longrightarrow \mathrm{M}_d(W/p^n W) \xrightarrow{\varphi} \mathrm{GL}_d(R) \longrightarrow \mathrm{GL}_d(W) \longrightarrow 1$$

where $\varphi(A) = 1 + tA$. Note that the action of $\mathrm{GL}_d(W)$ on $\mathrm{M}_d(W/p^n W)$ induced by the exact sequence is given by the conjugation action on $\mathrm{M}_d(W)$, taken modulo p^n. Using our basis of V_W we can identify $\mathrm{M}_d(W/p^n W)$ with $M_W/p^n M_W$ and this identification respects G-action. Thus, condition (ii) provides an injective homomorphism α in the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \longrightarrow & \Gamma & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \vdots{\scriptstyle \rho_R} & & \downarrow{\scriptstyle \rho_W} & & \\ 0 & \longrightarrow & \mathrm{M}_d(W/p^n W) & \xrightarrow{\varphi} & \mathrm{GL}_d(R) & \longrightarrow & \mathrm{GL}_d(W) & \longrightarrow & 1. \end{array} \tag{3.1}$$

Note that the rows in this diagram are exact. By [1, p. 179], the obstruction to the existence of a homomorphism ρ_R which makes (3.1) commute lies in the group $H^2(G, \mathrm{M}_d(W/p^n W))$. By Lemma 3.2 part (1), this is a trivial group, so ρ_R exists. Since α and ρ_W are injective, the map ρ_R is also injective. Thus, Γ acts faithfully on the deformation over R associated to ρ_R, so it certainly acts faithfully on the universal deformation.

Writing $R^{\mathrm{u}} = R(\Gamma, V)$ the universal property of deformation rings provides us with a unique morphism $\gamma : R^{\mathrm{u}} \to R$ in $\hat{\mathcal{C}}$ and a lift $\rho^{\mathrm{u}} \colon \Gamma \to \mathrm{GL}_d(R^{\mathrm{u}})$ such that the composite map $\gamma \circ \rho^{\mathrm{u}} : \Gamma \to \mathrm{GL}_d(R)$ is strictly equivalent to ρ_R. We will show that γ is an isomorphism.

Consider the surjection $\beta : R \to R/pR \cong k[t]/(t^2)$. If γ is not surjective, then $\beta \circ \gamma$ would be the composition of the residue map $r : R^{\mathrm{u}} \to k$ with the natural k-algebra inclusion $\iota : k \to k[t]/(t^2)$. This would imply that

$$\beta \circ \rho_R : \Gamma \to \mathrm{GL}_d(R/pR) = \mathrm{GL}_d(k[t]/(t^2))$$

is strictly equivalent to $\beta \circ \gamma \circ \rho^{\mathrm{u}} = \iota \circ r \circ \rho^{\mathrm{u}}$. However, by condition (ii)(b) there is an element $g \in K$ so that $\alpha(g)$ does not lie in $pM_W/p^n M_W = pM_d(W/p^n W)$. This g is in the kernel of $\iota \circ r \circ \rho^{\mathrm{u}}$ but not in the kernel of $\beta \circ \rho_R$, so these representations cannot be strictly equivalent. We conclude that $\gamma : R(\Gamma, V) \to R$ is surjective. Thus we can and will replace ρ^{u} by a strictly equivalent lift so that $\gamma \circ \rho^{\mathrm{u}} = \rho_R$.

Now define a morphism $\pi\colon\ W[[t]] \to R^{\mathrm{u}}$ in $\hat{\mathcal{C}}$ by letting $\pi(t)$ be any element in R^{u} that is mapped by γ to $t \in R$. By condition (ii)(a) and Lemma 3.3 we then see that π is surjective. In the chain of surjections

$$W[[t]] \longrightarrow R^{\mathrm{u}} \longrightarrow R \longrightarrow W$$

we will write t for the image of t in any of the rings. So we have $t = 0$ in W, and $t^2 = p^n t = 0$ in R, and our aim is to show that $t^2 = p^n t = 0$ in R^{u}. Note that

$$R^{\mathrm{u}}/tR^{\mathrm{u}} = W \quad \text{and} \quad R^{\mathrm{u}}/(tR^{\mathrm{u}} + p^n R^{\mathrm{u}}) = W/p^n W.$$

Suppose that we are in the first case of condition (b) of (ii), that is, we have

$$\alpha(g) \circ \alpha(h) \not\equiv \alpha(h) \circ \alpha(g) \mod pM_W/p^n M_W$$

for certain $g, h \in K$. Write $\rho^{\mathrm{u}}(g) = 1 + tA$ and $\rho^{\mathrm{u}}(h) = 1 + tB$ with $A, B \in \mathrm{M}_d(R^{\mathrm{u}})$ whose images modulo (p^n, t) are $\alpha(g)$ and $\alpha(h)$. Since K is abelian we have

$$(1 + tA)(1 + tB) = (1 + tB)(1 + tA),$$

so $t^2(AB - BA) = 0$. The matrix $AB - BA$ now has some entry which is a unit in R^{u}. Hence $t^2 = 0$ in R^{u} and A has an entry which is a unit in R^{u}. Our element $g \in K$ has order dividing p^n. Hence

$$1 = (1 + tA)^{p^n} = 1 + p^n tA$$

so $p^n tA = 0$. Since A has an entry which is a unit, it follows that $p^n t = 0$ in R^{u}.

Now suppose that we are in the second case of condition (b) of (ii), so we have $n = 1$ and $p = 2$. For each $g \in K$ write $\rho^{\mathrm{u}}(g) = 1 + tA_g$ with $A_g \in \mathrm{M}_d(R^{\mathrm{u}})$ such that $A_g \equiv \alpha(g) \bmod (p, t)$ where $(p, t) = (2, t)$. Since all $g \in K$ are annihilated by 2 we have

$$1 = (1 + tA_g)^2 = 1 + 2tA_g + t^2 A_g^2.$$

Let us now consider the free R^{u}-module $P = \mathrm{Map}(K, M_d(R^{\mathrm{u}}))$. This contains the elements $v_1\colon\ g \mapsto A_g$ and $v_2\colon\ g \mapsto A_g^2$. Then on the one hand, the identity above shows that $2tv_1 + t^2 v_2 = 0$. On the other hand the second case of condition (b) of (ii) implies that the images of v_1 and v_2 in $P \otimes_{R^{\mathrm{u}}} k$ are linearly independent over k. By Nakayama's lemma this means that v_1 and v_2 are part of a basis of P over R^{u}. So it follows that $2t = t^2 = 0$ in R^{u}.

3.2. **Proof that (i) implies (ii) in Theorem 3.1.** Throughout this subsection, we assume that condition (i) of Theorem 3.1 holds. Property (ii)(a) of Theorem 3.1 follows from Lemma 3.3.

The action of G on V_W gives a morphism

$$R = R(\Gamma, V) = W[[t]]/(p^n t, t^2) \to W.$$

There is only one such morphism and it sends $t \in R$ to 0. Since we are assuming that R is the universal deformation ring $R(\Gamma, V)$ and $R \to W$ is surjective, we can now find maps ρ_W, ρ_R and α as in the commutative diagram (3.1). The map ρ_R is injective by assumption (i) so α is also injective, G-equivariant and continuous. Since $\mathrm{M}_d(W/p^n W)$ is abelian and has the discrete topology, this implies K is finite and abelian, so Γ is also finite.

In order to prove (ii)(b) we now assume that (ii)(b) does not hold, and we will derive a contradiction. The first step in doing this is to lift ρ_R to a suitable extension

R' of R, i.e., to a ring R' in $\hat{\mathcal{C}}$ with an ideal I such that $R'/I = R$. In all cases that we will consider we have $I^2 = 0$, so we have an exact sequence

(3.2)
$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & \overset{\rho'}{\swarrow} & \downarrow{\scriptstyle \rho_R} & & \\ 0 & \longrightarrow & \mathrm{M}_d(I) & \xrightarrow{\varphi} & \mathrm{GL}_d(R') & \longrightarrow & \mathrm{GL}_d(R) & \longrightarrow & 1 \end{array}$$

where $\varphi(A) = 1 + A$. We now show how to choose R' and produce the restriction of the lift ρ' to K.

Let us write

$$\overline{\alpha}\colon\ K \to M = M_d(k)$$

for the map sending $g \in K$ to $\alpha(g) \bmod pM_W/p^nM_W$. Since we assumed that (ii)(b) does not hold, the set $\overline{\alpha}(K)$ is contained in a commutative sub-k-algebra of $\mathrm{M}_d(k)$.

If $p \neq 2$, then we take

$$\begin{aligned} R' &= W[[t]]/(p^n t, pt^2, t^3) \\ &= W \ \oplus\ (W/p^nW)t \ \oplus\ kt^2 \end{aligned}$$

and we let

$$\rho'(g) = 1 + \alpha(g)t + \overline{\alpha}(g)^2 t^2/2$$

for $g \in K$. Using that the elements $\overline{\alpha}(K)$ commute in $M_d(k)$ one easily shows that this exponential map is a homomorphism $K \to \mathrm{GL}_d(R')$.

Now suppose that $p = 2$ and $n \geq 2$. We take R' as above. For $g \in K$ we now claim that g and $1 + t\alpha(g) \in \mathrm{GL}_d(R')$ have the same order. To see this we note first that

$$\begin{aligned} (1 + t\alpha(g))^2 &= 1 + 2t\alpha(g) + t^2\,(\overline{\alpha}(g) \circ \overline{\alpha}(g)) \quad \text{and} \\ (1 + t\alpha(g))^{2^i} &= 1 + 2^i t\alpha(g) \qquad \text{for } 2 \leq i \leq n. \end{aligned}$$

If g has order 1, the claim is clear from the fact that α is injective. For g of order 2 we have $\alpha(g) \in \mathrm{M}_d(2^{n-1}W/2^nW)$, so $\overline{\alpha}(g) = 0$ and the first equality implies $(1 + t\alpha(g))^2 = 1$. Conversely, if $(1 + t\alpha(g))^2 = 1$, then this equality implies $2\alpha(g) = 0$, so $2g$ is the identity because α is injective. The second equality and the injectivity of α similarly imply that g and $1+t\alpha(g)$ have the same order if either has order 2^i for some $i > 1$. Next, we remark that the elements $1 + t\alpha(g) \in \mathrm{GL}_d(R')$ with g ranging over K commute with each other because the elements of $\overline{\alpha}(K)$ commute in M. Since K is finite and abelian, we can write K as a direct sum of cyclic groups. By setting

$$\rho'(g) = 1 + t\alpha(g)$$

for a generator of each of these cyclic groups, we obtain a lift $\rho' : K \to \mathrm{GL}_d(R')$ of the restriction of ρ_R to K.

Now suppose that $p = 2$ and $n = 1$. Our assumption that condition (ii)(b) fails then provides us with an element $a \in k$ such that for all $g \in K$ we have $\alpha(g)^2 = a\,\alpha(g)$. Choose an element $\hat{a} \in W$ with image a in $W/pW = k$, and define

$$R' = W[[t]]/(2t^2, t^3, 2t + \hat{a}t^2).$$

Then $R = R'/I$ when I is the 1-dimensional vector space over k generated by t^2, and in R' we have $2t = -\hat{a}t^2$ and $2t^2 = 0 = t^3$. For any $g \in K$ now choose $A_g \in \mathrm{M}_d(R')$ with $A_g \bmod (p,t) = \alpha(g)$. Then we have

$$(1 + tA_g)^2 = 1 + 2tA_g + t^2A_g^2 = 1 + t^2(-a\alpha(g) + \alpha(g)^2) = 1.$$

Since the elements of $\alpha(K)$ commute in $M = \mathrm{M}_d(k)$ and the element t^2 is annihilated by (p,t) in R', we also know that the elements $1+tA_g \in \mathrm{GL}_d(R')$ all commute when g ranges over K. So we can find a lift $\rho' : K \to \mathrm{GL}_d(R')$ of the restriction of ρ_R to K by setting

$$\rho'(g) = 1 + tA_g$$

for g in an $\mathbb{F}_2$-basis of K.

In summary, in all cases we produced an extension R' of R, and

$$\rho' \colon\ K \to \mathrm{GL}_d(R')$$

lifting the restriction of ρ_R to K. Moreover, $R = R'/I$ where the ideal I is a k-vector space of dimension 1. We now claim that we can extend the homomorphism ρ' to Γ so that diagram (3.2) is commutative. Note that the group $\mathrm{M}_d(I)$ has a conjugation action by $\mathrm{GL}_d(R)$, and through ρ_R it has a Γ-action. This $k\Gamma$-module $M_d(I)$ is isomorphic to M, so the obstruction to the existence of a lift ρ' is a class in $H^2(\Gamma, M)$. We know that this lift exists if we restrict to K, so the restriction of this class to K is trivial in $H^2(K, M)$. But by Lemma 3.2 (3) this restriction map on cohomology groups is injective, so the first class was trivial as well. This shows the existence of ρ' lifting ρ_R.

By the deformation ring property, this implies that the morphism $R' \to R$ is split, i.e., there is a morphism $R \to R'$ so that the composition $R \to R' \to R$ is the identity. But then the maps are isomorphisms on the (one-dimensional) cotangent spaces, so they are also surjective and R is isomorphic to R' which is clearly false. With this contradiction the proof of Theorem 3.1 is complete.

4. The inverse problem for $R = W[[t]]/(p^n t, t^2)$

In this section, we use Theorem 3.1 to prove Theorem 1.3. We first establish a special case.

Theorem 4.1. *Suppose $n \geq 1$. Define*

$$G_0 = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) \quad \text{and} \quad G = \mathbb{F}_{p^2}^* \rtimes G_0$$

where G_0 acts on the multiplicative group $\mathbb{F}_{p^2}^*$ by restricting the natural action of G_0 on $\mathbb{F}_{p^2}$ to $\mathbb{F}_{p^2}^*$. The natural action of G_0 and $\mathbb{F}_{p^2}^*$ on $V = \mathbb{F}_{p^2}$ makes V into a projective and simple $\mathbb{F}_pG$-module. The endomorphism ring $M = \mathrm{End}_{\mathbb{F}_p}(V)$ is isomorphic to the twisted group ring $\mathbb{F}_{p^2}^\dagger G_0$ a an $\mathbb{F}_p$-algebra. There exists a simple projective $\mathbb{F}_pG$-module V' such that

$$M \cong V' \oplus \mathbb{F}_pG_0 \tag{4.3}$$

as $\mathbb{F}_pG$-modules. Let K be a projective $(\mathbb{Z}/p^n)G$-module such that

$$\mathbb{F}_p \otimes_{\mathbb{Z}/p^n} K \cong V'$$

as $\mathbb{F}_pG$-modules. Let Γ be the semidirect product

$$\Gamma = K \rtimes_\delta G$$

where $\delta : G \to \mathrm{Aut}(K)$ is the group homomorphism given by the G-action on the $(\mathbb{Z}/p^n)G$-module K. Let V also stand for the inflation of V to an $\mathbb{F}_p\Gamma$-module. Then we have a $\mathbb{Z}_p$-algebra isomorphism

$$R_{\mathbb{Z}_p}(\Gamma, V) \cong \mathbb{Z}_p[[t]]/(p^n t, t^2).$$

Proof. If $p = 2$, then G is isomorphic to the symmetric group S_3 on 3 letters and V is the unique simple projective $\mathbb{F}_p G$-module, up to isomorphism. If $p \geq 3$, then the order of G is relatively prime to p and V is also a simple projective $\mathbb{F}_p G$-module.

Since $V = \mathbb{F}_{p^2}$ is a Galois algebra over $\mathbb{F}_p$ with Galois group G_0, it follows that $M = \mathrm{End}_{\mathbb{F}_p}(V)$ is canonically isomorphic to the twisted group ring $\mathbb{F}_{p^2}^{\dagger} G_0$ as an $\mathbb{F}_p$-algebra. This isomorphism defines an $\mathbb{F}_p G$-module structure on $\mathbb{F}_{p^2}^{\dagger} G_0$ by conjugation as follows. Let $G_0 = \langle \sigma \rangle$, let $\mathbb{F}_{p^2}^* = \langle \zeta \rangle$ and let $x = b_0 + b_1\sigma \in \mathbb{F}_{p^2}^{\dagger} G_0$, so $b_0, b_1 \in \mathbb{F}_{p^2}$. Then

$$\sigma.x = \sigma x \sigma^{-1} = (b_0)^p + (b_1)^p \sigma \quad \text{and} \tag{4.4}$$

$$\zeta.x = \zeta x \zeta^{-1} = b_0 + b_1 \zeta^{1-p} \sigma. \tag{4.5}$$

We have $\mathbb{F}_{p^2}^{\dagger} G_0 = \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2}\sigma$ as $\mathbb{F}_p$-vector spaces. The above G-action on $\mathbb{F}_{p^2}^{\dagger} G_0$ implies that both $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^2}\sigma$ are $\mathbb{F}_p G$-submodules of $\mathbb{F}_{p^2}^{\dagger} G_0$. It follows for example from the normal basis theorem that $\mathbb{F}_{p^2} \cong \mathbb{F}_p G_0$ as $\mathbb{F}_p G$-modules, where $\mathbb{F}_{p^2}^* \subset G$ acts trivially by conjugation on $\mathbb{F}_{p^2}$. Thus to prove (4.3) it suffices to show that $V' = \mathbb{F}_{p^2}\sigma$ is a simple projective $\mathbb{F}_p G$-module. Since V is a projective $\mathbb{F}_p G$-module, so are $M = \mathrm{End}_{\mathbb{F}_p}(V) \cong \mathbb{F}_{p^2}^{\dagger} G_0$ and V'. Considering the action of $\mathbb{F}_{p^2}^* = \langle \zeta \rangle$ on $\mathbb{F}_{p^2}\sigma$, we see that the action of ζ has eigenvalue ζ^{1-p}. Since ζ^{1-p} lies in $\mathbb{F}_{p^2} - \mathbb{F}_p$, it follows that $V' = \mathbb{F}_{p^2}\sigma$ is a simple projective $\mathbb{F}_p G$-module. Moreover,

$$\mathrm{Hom}_{(\mathbb{Z}/p)G}(V', \mathbb{F}_p G_0) = 0$$

because $\mathbb{F}_p G_0$ has $\mathbb{F}_p$-dimension 2 and is not isomorphic to V' since $\mathbb{F}_{p^2}^*$ acts trivially on $\mathbb{F}_p G_0$.

For ease of notation we set $W = \mathrm{W}(\mathbb{F}_p) = \mathbb{Z}_p$. Let V_W be a projective WG-module such that $\mathbb{F}_p \otimes_W V_W \cong V$ as $\mathbb{F}_p G$-modules. Let $M_W = \mathrm{End}_W(V_W)$. To complete the proof, it will suffice to show that G, K, M and M_W satisfy the conditions in Theorem 3.1(ii) when $k = \mathbb{F}_p$.

For all p, K is a finitely generated $(\mathbb{Z}/p^n)G$-module. Define $\Gamma = K \rtimes_\delta G$ where $\delta : G \to \mathrm{Aut}(K)$ is the group homomorphism given by the G-action on the $(\mathbb{Z}/p^n)G$-module K. Since by our above calculations, $M \cong (K/pK) \oplus \mathbb{F}_p G_0$ as $(\mathbb{Z}/p)G$-modules, it follows that

$$\begin{aligned} \mathrm{Hom}^{cont}(K, M)^G &= \mathrm{Hom}_{(\mathbb{Z}/p)G}(K/pK, M) \\ &\cong \mathrm{Hom}_{(\mathbb{Z}/p)G}(V', V' \oplus \mathbb{F}_p G_0) \\ &\cong \mathbb{F}_p \end{aligned}$$

giving condition (a) of Theorem 3.1(ii). Since K and $M_W/p^n M_W$ are projective $(\mathbb{Z}/p^n)G$-modules, it follows that $\mathrm{Hom}_{(\mathbb{Z}/p^n)G}(K, M_W/p^n M_W)$ is a projective $(\mathbb{Z}/p^n)$-module H such that

$$H/pH = \mathrm{Hom}_{\mathbb{F}_p G}(K/pK, M) \cong \mathbb{F}_p.$$

Therefore,

$$\mathrm{Hom}_{(\mathbb{Z}/p^n)G}(K, M_W/p^n M_W) \cong \mathbb{Z}/p^n$$

and there exists an injective $(\mathbb{Z}/p^n)G$-module homomorphism $\alpha : K \to M_W/p^n M_W$ whose image is not contained in $pM_W/p^n M_W$. By the above calculations in the twisted group algebra $\mathbb{F}_{p^2}^{\dagger} G_0$, we see that the image of α mod $pM_W/p^n M_W$ is isomorphic to $\mathbb{F}_{p^2}\sigma$. Since for example

$$(\sigma)\cdot(\zeta\sigma) = \zeta^p \neq \zeta = (\zeta\sigma)\cdot(\sigma)$$

in the algebra $\mathbb{F}_{p^2}^{\dagger} G_0 \cong M$, we obtain that the image of α mod $pM_W/p^n M_W$ is not commutative with respect to the multiplication in the ring $M_W/p^n M_W$. This gives condition (b) of Theorem 3.1(ii) and completes the proof. □

Remark 4.2. If $p > 3$, we can replace the group G in Theorem 4.1 by the symmetric group S_3 and V by a 2-dimensional simple projective $\mathbb{F}_p S_3$-module (which is unique up to isomorphism). It then follows that

$$M = \mathrm{Hom}_{\mathbb{F}_p}(V, V) \cong \mathbb{F}_p[\mathbb{Z}/2] \oplus V$$

as $\mathbb{F}_p G$-modules, which means that we can take $V' = V$ in this case.

Remark 4.3. As mentioned in the introduction, in subsequent work on Question 1.1, Rainone proved in [16] that if $p > 3$ and $1 \leq m \leq n$, the ring $\mathbb{Z}_p[[t]]/(p^n, p^m t)$ is a universal deformation ring relative to $W = \mathbb{Z}_p$. These rings and the rings of Theorems 1.3 and 4.1 form disjoint sets of isomorphism classes. Rainone's work gave the first negative answers to two questions of Bleher and Chinburg (Question 1.2 of [4] and Question 1.1 of [2]). Later we observed that Theorem 4.1 also gives a negative answer to Question 1.2 of [4] when $p > 2$.

Completion of the Proof of Theorem 1.3. Let k, p, W and n be as in Theorem 1.3. By Theorem 4.1, there is a finite group Γ and a representation V_0 of Γ over $\mathbb{F}_p$ such that $\mathrm{End}_{\mathbb{F}_p G}(V_0) = \mathbb{F}_p$ and the universal deformation ring $R_{\mathbb{Z}_p}(\Gamma, V_0)$ is isomorphic to $\mathbb{Z}_p[[t]]/(p^n t, t^2)$. Let $V = k \otimes_{\mathbb{F}_p} V_0$. Then

$$\mathrm{End}_{kG}(V) \cong k \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p G}(V_0) \cong k.$$

By Theorem 2.2, the universal deformation ring $R_W(\Gamma, V)$ is isomorphic to the completion of $W \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[t]]/(p^n t, t^2)$ with respect to its maximal ideal. This completion is isomorphic to $W[[t]]/(p^n t, t^2)$. It remains to show that this ring is not a complete intersection if $p^n W \neq \{0\}$. This is clear if W is regular. In general, if one assumes that $W[[t]]/(p^n t, t^2)$ is a complete intersection, then W is a quotient S/I for some regular complete local commutative Noetherian ring S and a proper ideal I of S. If $S' = S[[t]]$, then

$$W[[t]]/(p^n t, t^2) = S'/I'$$

when I' is the ideal of S' generated by I, $p^n t$ and t^2. Since

$$\dim W[[t]]/(p^n t, t^2) = \dim W,$$

we obtain by [13, Thm. 21.1] that

$$\begin{aligned} \dim_k(I'/m_{S'} I') &= \dim S' - \dim(S'/I') \\ &= \dim S + 1 - \dim(S/I) \\ &\leq \dim_k(I/m_S I) + 1. \end{aligned} \tag{4.6}$$

Using power series expansions, we see that

$$\dim_k(I'/m_{S'} I') = \dim_k(I/m_S I) + 2$$

if $p^nW \neq \{0\}$. Since this contradicts (4.6), $W[[t]]/(p^nt, t^2)$ is not a complete intersection if $p^nW \neq \{0\}$. This completes the proof of Theorem 1.3.

Remark 4.4. The referee of this paper asked whether in our examples of universal deformation rings $R_W(\Gamma, V)$ which are not complete intersections, we have $H^3(\Gamma, \mathrm{End}_k(V)) = 0$. Consider, for example, the case when $n = 1$ in Theorem 4.1 so that $k = \mathbb{F}_p$. We claim that $H^3(\Gamma, \mathrm{End}_{\mathbb{F}_p}(V)) \neq 0$.

To see this, recall that $G = \mathbb{F}_{p^2}^* \rtimes G_0$ where $G_0 = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ and G_0 acts on $\mathbb{F}_{p^2}^*$ using the natural action of G_0 on $\mathbb{F}_{p^2}$. The $\mathbb{F}_pG$-module V is defined to be $V = \mathbb{F}_{p^2}$ with the natural actions of G_0 and $\mathbb{F}_{p^2}^*$. By (4.3), we have

$$\mathrm{End}_{\mathbb{F}_p}(V) \cong V' \oplus \mathbb{F}_pG_0$$

for a simple projective $\mathbb{F}_pG$-module V'. Letting $K = V'$, we then have $\Gamma = K \rtimes_\delta G$ where $\delta : G \to \mathrm{Aut}(K)$ is given by the G-action on $K = V'$. Let $\Gamma_0 = K \rtimes_\delta \mathbb{F}_{p^2}^*$. Using that $\mathbb{F}_pG_0 \cong \mathrm{Ind}_{\Gamma_0}^{\Gamma}\mathbb{F}_p$ where $\mathbb{F}_p$ is the trivial simple $\mathbb{F}_p\Gamma_0$-module, we obtain

$$\mathrm{End}_{\mathbb{F}_p}(V) \cong V' \oplus \mathrm{Ind}_{\Gamma_0}^{\Gamma}\mathbb{F}_p.$$

By Frobenius reciprocity, we have

$$H^3(\Gamma, \mathrm{Ind}_{\Gamma_0}^{\Gamma}\mathbb{F}_p) \cong H^3(\Gamma_0, \mathbb{F}_p).$$

Using the Kummer sequence $1 \to \mu_p \to \mathbb{C}^* \xrightarrow{p} \mathbb{C}^* \to 1$ where μ_p is the subgroup of p^{th} roots of unity in $\mathbb{C}^*$, we see that the quotient group $H^2(\Gamma_0, \mathbb{C}^*)/p \cdot H^2(\Gamma_0, \mathbb{C}^*)$ is isomorphic to a subgroup of $H^3(\Gamma_0, \mathbb{F}_p)$.

If $p = 2$, then $\Gamma = S_4$ and $\Gamma_0 = A_4$, and we have $H^2(A_4, \mathbb{C}^*) \cong \mathbb{Z}/2$, which implies $H^3(\Gamma, \mathrm{End}_{\mathbb{F}_p}(V)) \neq 0$ when $p = 2$.

Now suppose that $p \geq 3$. Since $H^1(\Gamma_0, \mathbb{C}^*) = \mathrm{Hom}(\Gamma_0, \mathbb{C}^*)$ and the maximal abelian quotient of Γ_0 is isomorphic to $\mathbb{F}_{p^2}^*$, it follows that $H^2(\Gamma_0, \mathbb{F}_p)$ injects into $H^2(\Gamma_0, \mathbb{C}^*)$. Therefore, to show that $H^3(\Gamma, \mathrm{End}_{\mathbb{F}_p}(V)) \neq 0$, it suffices to prove that $H^2(\Gamma_0, \mathbb{F}_p) \neq 0$. Using the short exact sequence

$$1 \to K \to \Gamma_0 \to \mathbb{F}_{p^2}^* \to 1$$

and that $H^i(K, \mathbb{F}_p)$ is cohomologically trivial as a module for $\mathbb{F}_{p^2}^*$ for all $i \geq 0$, we see that $H^2(\Gamma_0, \mathbb{F}_p) \cong H^0(\mathbb{F}_{p^2}^*, H^2(K, \mathbb{F}_p))$. Consider the function $c : K \times K \to \bigwedge^2 K$ given by the wedge product. It follows from the bilinearity of the wedge product that c is a 2-cocycle. Since $p \geq 3$, the anti-commutativity of the wedge product implies that c is not a 2-coboundary. Furthermore, c is an invariant 2-cocycle with respect to the action of $\mathbb{F}_{p^2}^*$ on $K \times K$ and on $\bigwedge^2 K$. Here $\bigwedge^2 K$ can be identified with $\mathbb{F}_p$ with trivial action by $\mathbb{F}_{p^2}^*$ in view of (4.5) since $K \cong \mathbb{F}_{p^2}\sigma$ as an $\mathbb{F}_pG$-module. It follows that c defines a non-zero element in $H^0(\mathbb{F}_{p^2}^*, H^2(K, \mathbb{F}_p))$. Therefore, we obtain $H^3(\Gamma, \mathrm{End}_{\mathbb{F}_p}(V)) \neq 0$ for all primes p.

Remark 4.5. To construct more examples to which Theorem 3.1 applies, there are two fundamental issues. One must construct a group G and a projective kG-module V for which both the left kG-module structure and the ring structure of $M = \mathrm{Hom}_k(V, V)$ can be analyzed sufficiently well to be able to produce a G-module K having the properties in the theorem. When one can identify the ring $\mathrm{Hom}_k(V, V)$ with a twisted group algebra, as in the proof of Theorem 4.1, this can be very useful in checking condition (ii)(b) of Theorem 3.1. A natural approach to analyzing the kG-module structure of M is to note that the Brauer character ξ_M of

M is the tensor product $\xi_V \otimes \xi_{V^*}$ of the Brauer characters of V and its k-dual V^*. For example, if V is induced from a representation X of a subgroup H of G, then ξ_V is given by the usual formula for the character of an induced representation. If $\dim_k(X) = 1$, the analysis of the ring structure of M becomes a combinatorial problem using X and coset representatives of H in G. We carry out this program with some further examples in the next section.

5. Further examples

In all the examples for Theorem 1.3 which were discussed in §4, the dimension of V is 2. In this section, we weaken this restriction on the dimension. Let W be a complete Noetherian local commutative ring with residue field k of positive characteristic p. We prove the following result.

Theorem 5.1. *Suppose $d \geq 2$ is an integer such that either $d < p-1$ or $d = p^f$ for some positive integer f. There exists a profinite group Γ satisfying Hypothesis 2.1 and a continuous representation V of Γ over k of degree d such that the versal deformation ring $R_W(\Gamma, V)$ is isomorphic to $W[[t]]/(t^2, pt)$.*

Proof. Because of Theorem 2.2 it suffices to prove Theorem 5.1 when $k = \mathbb{F}_p$ and $W = \mathrm{W}(\mathbb{Z}_p)$, which allows us to use Theorem 3.1.

Let $\Omega = \{1, 2, \ldots, d+1\}$, and let S_{d+1} be the symmetric group on Ω. For each prime power $q = p^f$, the projective general linear group $\mathrm{PGL}_2(\mathbb{F}_q)$ acts faithfully and triply transitively on the projective line $\mathbb{P}^1(\mathbb{F}_q)$ and is thus isomorphic to a subgroup of S_{q+1}. If $d < p-1$ let $G = S_{d+1}$, and if $d = q = p^f \geq 2$ let $G = \mathrm{PGL}_2(\mathbb{F}_q)$ be viewed as a subgroup of $S_{d+1} = S_{q+1}$.

Consider the natural $(d+1)$-dimensional representation N of S_{d+1} with $\mathbb{F}_p$-basis $\{b_1, \ldots, b_{d+1}\}$ such that for all $\sigma \in S_{d+1}$ and all $i \in \Omega$, $\sigma.b_i = b_{\sigma(i)}$. On restricting to G, N is also a $(d+1)$-dimensional representation of G over $\mathbb{F}_p$. Let T be the 1-dimensional $\mathbb{F}_p$-subspace of N generated by $(b_1 + \cdots + b_{d+1})$, and let V be the d-dimensional $\mathbb{F}_p$-subspace of N with $\mathbb{F}_p$-basis

$$\{b_1 - b_2, b_2 - b_3, \ldots, b_d - b_{d+1}\}.$$

Then T and V are $\mathbb{F}_pG$-submodules of N, where G acts trivially on T. In fact, since $p \nmid (d+1)$ we have $N = T \oplus V$. Since T and V can be lifted to $\mathbb{Z}_pG$-modules $\hat{T}$ and $\hat{V}$ which are free over $\mathbb{Z}_p$ and since G acts doubly transitively on Ω, it follows that $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \hat{V}$ is an absolutely irreducible representation of G over $\mathbb{Q}_p$ (see e.g. [11, Ex. 9 on p. 877]). If $d < p-1$, then the order of $G = S_{d+1}$ is relatively prime to p which immediately implies that V is a simple and projective $\mathbb{F}_pG$-module. If $d = q$ and $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then the Sylow p-subgroups of G have order q which implies by [19, Prop. 46 on p. 136] that $V = \hat{V}/p\hat{V}$ is a simple and projective $\mathbb{F}_pG$-module. Note that in this case the character of G corresponding to $\hat{V}$ is the Steinberg character of $\mathrm{PGL}_2(\mathbb{F}_q)$.

Let $K = V$ and let $\delta : G \to \mathrm{Aut}(K)$ be the group homomorphism given by the action of G on $K = V$. Define $\Gamma = K \rtimes_\delta G$ and view V also as an $\mathbb{F}_p\Gamma$-module via inflation. Let $M = \mathrm{End}_{\mathbb{F}_p}(V)$. To prove Theorem 5.1, it suffices to prove that G, K and M satisfy the conditions in Theorem 3.1(ii) when $k = \mathbb{F}_p$ and $n = 1$.

For an $\mathbb{F}_pG$-module X, let X^* denote its $\mathbb{F}_p$-dual. Consider

$$\mathrm{End}_{\mathbb{F}_p}(N) \cong N^* \otimes_{\mathbb{F}_p} N \cong N \otimes_{\mathbb{F}_p} N.$$

We can identify $\mathrm{End}_{\mathbb{F}_p}(N)$ with $\mathrm{Mat}_{d+1}(\mathbb{F}_p)$, where we identify $b_i \otimes b_j$ with the elementary matrix $E_{i,j}$ which has coefficient 1 at position (i,j) and coefficient 0 otherwise. Since $M = \mathrm{End}_{\mathbb{F}_p}(V) \cong V^* \otimes_{\mathbb{F}_p} V \cong V \otimes_{\mathbb{F}_p} V$, M can be identified with the subspace of $\mathrm{End}_{\mathbb{F}_p}(N)$ with $\mathbb{F}_p$-basis $\{D_{i,j} \mid 1 \leq i,j \leq d\}$, where

$$D_{i,j} = E_{i,j} - E_{i,j+1} - E_{i+1,j} + E_{i+1,j+1}$$

for all $1 \leq i,j \leq d$. Note that $\mathrm{End}_{\mathbb{F}_p}(N)$ and M are $\mathbb{F}_p S_{d+1}$-modules by letting S_{d+1} act by conjugation, i.e. $\sigma.E_{i,j} = E_{\sigma(i),\sigma(j)}$ for all $\sigma \in S_{d+1}$. In particular, it follows that $\mathrm{End}_{\mathbb{F}_p}(N)$ and M are $\mathbb{F}_p G$-modules.

We now show that the irreducible representation V occurs with multiplicity 1 in M. For $\mathbb{F}_p G$-modules X and Y, let

$$\langle X, Y \rangle = \dim_{\mathbb{F}_p} \mathrm{Hom}_{\mathbb{F}_p G}(X,Y) = \dim_{\mathbb{F}_p} \left(X^* \otimes_{\mathbb{F}_p} Y\right)^G.$$

Since V is a simple projective $\mathbb{F}_p G$-module which is isomorphic to its $\mathbb{F}_p$-dual V^*, it follows that the multiplicity of V in M is equal to

$$\langle V, M \rangle = \dim_{\mathbb{F}_p} \left(V \otimes_{\mathbb{F}_p} V \otimes_{\mathbb{F}_p} V\right)^G.$$

Using that $N = T \oplus V$, we obtain that

$$N \otimes_{\mathbb{F}_p} N \otimes_{\mathbb{F}_p} N \cong T \ \oplus \ V^3 \ \oplus \ (V \otimes_{\mathbb{F}_p} V)^3 \ \oplus \ (V \otimes_{\mathbb{F}_p} V \otimes_{\mathbb{F}_p} V).$$

Since $V^G = 0$ and $\dim_{\mathbb{F}_p} \left(V \otimes_{\mathbb{F}_p} V\right)^G = \langle V, V \rangle = 1$, it follows that

$$\langle V, M \rangle = \dim_{\mathbb{F}_p} \left(N \otimes_{\mathbb{F}_p} N \otimes_{\mathbb{F}_p} N\right)^G - 4. \tag{5.7}$$

Note that $N \otimes_{\mathbb{F}_p} N \otimes_{\mathbb{F}_p} N$ is the representation of G corresponding to the diagonal action of G on the set Ω of all triples (a,b,c) with $a,b,c \in \{1,\ldots,d+1\}$. This implies that $\dim_{\mathbb{F}_p} \left(N \otimes_{\mathbb{F}_p} N \otimes_{\mathbb{F}_p} N\right)^G$ is equal to the number of G-orbits on Ω. Since G acts triply transitively on Ω, this number is equal to 5. By (5.7), it follows that $\langle V, M \rangle = 1$, i.e. V occurs with multiplicity 1 in M. Therefore, condition (ii)(a) of Theorem 3.1 is satisfied for $K = V$ when $n = 1$.

Let ρ be the $(d+1)$-cycle $\rho = (1, 2, \cdots, d+1) \in S_{d+1}$, and define

$$x_1 = \begin{pmatrix} d-1 & 0 & -1 & \cdots & -1 \\ 0 & -d+1 & 1 & \cdots & 1 \\ -1 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -1 & 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Since $x_1 = (d-1)D_{1,1} + \sum_{\ell=2}^{d} (d+1-\ell)\,(D_{1,\ell} + D_{\ell,1})$, we see that $x_1 \in M$. Define

$$x_j = \rho^{j-1}.x_1$$

for $2 \leq j \leq d$. An easy matrix calculation shows that the subspace of M with $\mathbb{F}_p$-basis $\{x_1, \ldots, x_d\}$ is an $\mathbb{F}_p S_{d+1}$-submodule of M which is isomorphic to V. On restricting the action to G, we see that the additive group homomorphism $\alpha : K = V \to M$, defined by $\alpha(b_j - b_{j+1}) = x_j$ for $1 \leq j \leq d$, is an injective G-equivariant homomorphism. Since $x_1 x_2 \neq x_2 x_1$ in $M \subset \mathrm{Mat}_d(\mathbb{F}_p)$, condition (ii)(b) of Theorem 3.1 is satisfied when $n = 1$. This completes the proof of Theorem 5.1. □

6. Appendix: Proof of Theorem 2.2

We assume the notation in the statement of Theorem 2.2. Let $R = R_W(\Gamma, \rho)$. Recall that $\Omega = W' \otimes_W R$ and R' is the completion of Ω with respect to its unique maximal ideal $\mathfrak{m}_\Omega$. Define $\hat{\mathcal{C}}'$ to be the category of all complete local commutative Noetherian W'-algebras with residue field k'. Let $\nu : \Gamma \to \mathrm{GL}_d(R)$ be a versal lift of ρ over R, and let

$$\nu' : \Gamma \to \mathrm{GL}_d(R')$$

be the lift of ρ' over R' defined by

$$\nu'(g) = (1 \otimes \nu(g)_{i,j})_{1 \le i,j \le d}$$

for all $g \in \Gamma$.

The first step is to show that if $A' \in \mathrm{Ob}(\mathcal{C}')$ is an Artinian W'-algebra with residue field k' and $\tau' : \Gamma \to \mathrm{GL}_d(A')$ is a lift of ρ' over A', then there is a morphism $\alpha : R' \to A'$ in $\hat{\mathcal{C}}'$ such that

$$[\tau'] = [\alpha \circ \nu'].$$

Since A' is Artinian, $\mathrm{Hom}_{\hat{\mathcal{C}}'}(R', A')$ is equal to the space $\mathrm{Hom}_{\mathrm{cont}}(\Omega, A')$ of continuous W'-algebra homomorphisms which induce the identity map on the residue field k'. Because of Hypothesis 2.1, one can find a finite set $S \subseteq \Gamma$ such that $\tau'(S)$ is a set of topological generators for the image of τ'. Since ρ' and ρ have the same image in $\mathrm{GL}_d(k) \subset \mathrm{GL}_d(k')$, there exists for each $g \in S$ a matrix $t(g) \in \mathrm{Mat}_d(W)$ such that all entries of the matrix $\tau'(g) - t(g)$ lie in the maximal ideal $\mathfrak{m}_{A'}$ of A'. Let $T \subseteq \mathfrak{m}_{A'}$ be the finite set of all matrix entries of $\tau'(g) - t(g)$ as g ranges over S. Then there is a continuous homomorphism

$$f : W[[x_1, \ldots, x_m]] \to A'$$

with $m = \#T$ and $\{f(x_i)\}_{i=1}^m = T$. Since A' has the discrete topology, the image B of f must be a local Artinian W-algebra with residue field k. Since $\tau'(S)$ is a set of topological generators for the image of τ', it follows that τ' defines a lift of ρ over B. Because $\nu : \Gamma \to \mathrm{GL}_d(R)$ is a versal lift of ρ over the versal deformation ring $R = R_W(\Gamma, \rho)$ of ρ, there is a morphism $\beta : R \to B$ in $\hat{\mathcal{C}}$ such that $\tau' : \Gamma \to \mathrm{GL}_d(B)$ is conjugate to $\beta \circ \nu$ by a matrix in the kernel of

$$\pi_B : \mathrm{GL}_d(B) \to \mathrm{GL}_d(B/\mathfrak{m}_B) = \mathrm{GL}_d(k).$$

Let $\beta' : R \to A'$ be the composition of β with the inclusion $B \subset A'$. Define $\alpha : R' \to A'$ to be the morphism in $\hat{\mathcal{C}}'$ corresponding to the continuous W'-algebra homomorphism $\Omega = W' \otimes_W R \to A'$ which sends $w' \otimes r$ to $w' \cdot \beta'(r)$ for all $w' \in W'$ and $r \in R$. It follows that α satisfies $[\tau'] = [\alpha \circ \nu']$.

The second step is to show that when $k'[\epsilon]$ is the ring of dual numbers over k', then $\mathrm{Hom}_{\hat{\mathcal{C}}'}(R', k'[\epsilon])$ is canonically identified with the set $\mathrm{Def}_{\rho'}(k'[\epsilon])$ of deformations of ρ' over $k'[\epsilon]$. Since $k'[\epsilon]$ is Artinian, it suffices to show that $\mathrm{Hom}_{\mathrm{cont}}(\Omega, k'[\epsilon])$ is identified with $\mathrm{Def}_{\rho'}(k'[\epsilon])$. Let

$$\begin{aligned} T(W', \Omega) &= \frac{\mathfrak{m}_\Omega}{\mathfrak{m}_\Omega^2 + \Omega \cdot \mathfrak{m}_{W'}} \quad \text{and} \\ T(W, R) &= \frac{\mathfrak{m}_R}{\mathfrak{m}_R^2 + R \cdot \mathfrak{m}_W} \end{aligned}$$

so that we have natural isomorphisms

$$\begin{aligned} \mathrm{Hom}_{\mathrm{cont}}(\Omega, k'[\epsilon]) &\cong \mathrm{Hom}_{k'}(T(W', \Omega), k') \quad \text{and} \\ \mathrm{Hom}_{\hat{\mathcal{C}}}(R, k[\epsilon]) &\cong \mathrm{Hom}_{k}(T(W, R), k). \end{aligned}$$

Since $\mathrm{Ad}(\rho') = k' \otimes_k \mathrm{Ad}(\rho)$, we have from [15, Prop. 21.1] that there are natural isomorphisms

$$\begin{aligned} \mathrm{Def}_{\rho'}(k'[\epsilon]) &= H^1(\Gamma, \mathrm{Ad}(\rho')) \\ &= k' \otimes_k H^1(\Gamma, \mathrm{Ad}(\rho)) \\ &= k' \otimes_k \mathrm{Def}_{\rho}(k[\epsilon]). \end{aligned}$$

Hence it suffices to show that the natural homomorphism

$$\mu : k' \otimes_k T(W, R) \to T(W', \Omega)$$

is an isomorphism of k'-vector spaces. Since $\mathfrak{m}_W$ is finitely generated, one can reduce to the case when $W = k$, by considering generators α of $\mathfrak{m}_W$ and successively replacing W by $W/(W\alpha)$ and R by $R/(R\alpha)$. One then divides W' and Ω further by ideals generated by generators for $\mathfrak{m}_{W'}$ to be able to assume that $W' = k'$. However, the case when $W = k$ and $W' = k'$ is obvious, since then

$$\begin{aligned} T(k', \Omega) &= \mathfrak{m}_\Omega/\mathfrak{m}_\Omega^2 \\ &\cong k' \otimes_k \left(\mathfrak{m}_R/\mathfrak{m}_R^2\right) \\ &= k' \otimes T(k, R). \end{aligned}$$

This completes the proof of Theorem 2.2.

Acknowledgments

The authors would like to thank M. Flach for correspondence about his question. The second author would also like to thank the University of Leiden for its hospitality during the spring of 2009 and the summer of 2010.

References

[1] E. Artin and J. Tate, Class Field Theory. W.A. Benjamin, 1967. MR0223335 (36:6383)
[2] F. M. Bleher and T. Chinburg, Universal deformation rings and cyclic blocks. Math. Ann. 318 (2000), 805–836. MR1802512 (2001m:20013)
[3] F. M. Bleher and T. Chinburg, Universal deformation rings need not be complete intersections. C. R. Math. Acad. Sci. Paris 342 (2006), 229–232. MR2196003 (2007b:20053)
[4] F. M. Bleher and T. Chinburg, Universal deformation rings need not be complete intersections. Math. Ann. 337 (2007), 739–767. MR2285736 (2008g:11093)
[5] F. M. Bleher, T. Chinburg and B. de Smit, Deformation rings which are not local complete intersections, March 2010. arXiv:1003.3143
[6] G. Böckle, Presentations of universal deformation rings. In: L-functions and Galois representations, 24–58, London Math. Soc. Lecture Note Ser., 320, Cambridge Univ. Press, Cambridge, 2007. MR2392352 (2009e:11102)
[7] J. Byszewski, A universal deformation ring which is not a complete intersection ring. C. R. Math. Acad. Sci. Paris 343 (2006), 565–568. MR2269865 (2007i:20051)
[8] T. Chinburg, Can deformation rings of group representations not be local complete intersections? In: Problems from the Workshop on Automorphisms of Curves. Edited by Gunther Cornelissen and Frans Oort, with contributions by I. Bouw, T. Chinburg, Cornelissen, C. Gasbarri, D. Glass, C. Lehr, M. Matignon, Oort, R. Pries and S. Wewers. Rend. Sem. Mat. Univ. Padova 113 (2005), 129–177. MR2168985 (2006d:14027)

[9] H. Darmon, F. Diamond and R. Taylor, Fermat's Last Theorem. In : R. Bott, A. Jaffe and S. T. Yau (eds), Current developments in mathematics, 1995, International Press, Cambridge, MA., 1995, pp. 1–107. MR1474977 (99d:11067a)
[10] B. de Smit and H. W. Lenstra, Explicit construction of universal deformation rings. In: G. Cornell, J. H. Silverman and G. Stevens (eds), Modular Forms and Fermat's Last Theorem (Boston, MA, 1995), Springer-Verlag, Berlin-Heidelberg-New York, 1997, pp. 313–326. MR1638482
[11] D. S. Dummit and R.M. Foote, Abstract Algebra. Third edition. John Wiley & Sons, 2004. MR2286236 (2007h:00003)
[12] A. Grothendieck, Éléments de géométrie algébrique, Chapitre IV, Quatriéme Partie. Publ. Math. IHES 32 (1967), 5–361. MR0238860 (39:220)
[13] H. Matsumura, Commutative Ring Theory. Cambridge Studies in Advanced Mathematics, Vol. 8, Cambridge University Press, Cambridge, 1989. MR1011461 (90i:13001)
[14] B. Mazur, Deforming Galois representations. In: Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), Springer-Verlag, Berlin-Heidelberg-New York, 1989, pp. 385–437. MR1012172 (90k:11057)
[15] B. Mazur, An introduction to the deformation theory of Galois representations. In: G. Cornell, J. H. Silverman and G. Stevens (eds), Modular Forms and Fermat's Last Theorem (Boston, MA, 1995), Springer-Verlag, Berlin-Heidelberg-New York, 1997, pp. 243–311. MR1638481
[16] R. Rainone, On the inverse problem for deformation rings of representations. Master's thesis, Universiteit Leiden, Thesis Advisor: Bart de Smit, June 2010. http://www.math.leidenuniv.nl/en/theses/205/
[17] M. Schlessinger, Functors of Artin Rings. Trans. of the AMS 130 (1968), 208–222. MR0217093 (36:184)
[18] J. P. Serre, Corps Locaux. Hermann, Paris, 1968. MR0354618 (50:7096)
[19] J. P. Serre, Linear Representations of Finite Groups. Springer-Verlag, New York, 1977. MR0450380 (56:8675)
[20] C. Weibel, An Introduction to Homological Algebra, Cambridge University Press, 1994. MR1269324 (95f:18001)
[21] A. Wiles, Modular elliptic curves and Fermat's last theorem. Ann. of Math. 141 (1995), 443–551. MR1333035 (96d:11071)

Department of Mathematics, University of Iowa, Iowa City, Iowa 52242-1419
E-mail address: frauke-bleher@uiowa.edu

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6395
E-mail address: ted@math.upenn.edu

Mathematisch Instituut, University of Leiden, P.O. Box 9512, 2300 RA Leiden, The Netherlands
E-mail address: desmit@math.leidenuniv.nl