

Applications of versal deformations to Galois theory

Frauke M. Bleher and Ted Chinburg

Abstract. In this paper we study which solutions to an embedding problem can be constructed using a versal deformation of a group representation over an algebraically closed field of positive characteristic. This question reduces (at least stably) to finding which representations of finite groups have faithful versal deformations. We determine exactly when a versal deformation of a representation of a finite group is faithful in case the representation belongs to a cyclic block and its endomorphisms are given by scalar multiplications.

Mathematics Subject Classification (2000). Primary 20C05; Secondary 12F12, 14G32.

Keywords. Versal deformations, Galois theory, embedding problems, cyclic blocks.

1. Introduction

In this paper we study which solutions to an embedding problem can be constructed using a versal deformation of a group representation. This leads to the problem of determining when a versal deformation of a representation of a finite group is faithful. We give a complete solution to this problem for representations belonging to cyclic blocks whose endomorphisms are given by scalar multiplications.

A (finite) embedding problem is specified by giving two continuous group surjections $\pi : \Gamma \rightarrow T$ and $\lambda : G \rightarrow T$ in which Γ is a profinite group and G and T are finite groups. A solution of this embedding problem is a continuous homomorphism $h : \Gamma \rightarrow G$ such that $\lambda \circ h = \pi$. If h is surjective, then h is called a proper solution.

In Galois theory, Γ is taken to be a quotient of $\text{Gal}(\overline{N}/N)$ by a closed subgroup, where \overline{N} is a separable closure of a field N . A proper solution h of the embedding problem gives a G -extension $\overline{N}^{\text{Ker}(h)}$ of N containing the T -extension $\overline{N}^{\text{Ker}(\pi)}$. One would like to find h , and the corresponding field $\overline{N}^{\text{Ker}(h)}$, in a constructive way. For example, one would like to describe how to find h and construct $\overline{N}^{\text{Ker}(h)}$ via

The first author was supported in part by NSA Young Investigator Grant MDA904-01-1-0050. The second author was supported in part by NSF Grants DMS97-01411 and DMS00-70433.

values of special functions, or from Galois representations associated to modular forms, automorphic representations or the cohomology of algebraic varieties.

Suppose now that V is the inflation from T to Γ of a representation of T over an algebraically closed field k with positive characteristic. A versal deformation $U(\Gamma, V)$ associated to V (see [16, §1.2]), if it exists, is the isomorphism class of a lift of V over a local ring $R(\Gamma, V)$ having residue field k . We recall the defining properties of $U(\Gamma, V)$ and $R(\Gamma, V)$ in section 2. Both are known to exist if either Γ satisfies certain finiteness conditions [16, §1.1] or if $\text{End}_{k\Gamma}(V) = k$ (see [7]). If $\text{End}_{k\Gamma}(V) = k$, $U(\Gamma, V)$ is actually a universal deformation, and $R(\Gamma, V)$ and $U(\Gamma, V)$ are unique up to a unique isomorphism. In some situations of arithmetic interest, $U(\Gamma, V)$ is conjectured or proved to be constructible via modular forms; see [22], [9], [10] and [11].

Suppose a versal deformation $U(\Gamma, V)$ exists. We say in Definition 2.2 that a proper solution h to the above embedding problem arises from $U(\Gamma, V)$ if the kernel of the action of Γ on $U(\Gamma, V)$ is contained in the kernel of h . To motivate this, suppose Γ is a quotient of $\text{Gal}(\overline{N}/N)$ as above. Then h arises from $U(\Gamma, V)$ if and only if $\overline{N}^{\text{Ker}(h)}$ is contained in the subfield $N(\Gamma, V)$ of \overline{N} cut out by $U(\Gamma, V)$, in the sense that $N(\Gamma, V)$ is the fixed field of the kernel of $U(\Gamma, V)$ acting on \overline{N} . Thus if one has a construction of $N(\Gamma, V)$, one can attempt to identify $\overline{N}^{\text{Ker}(h)}$ inside this field.

It is not difficult to show (Theorem 2.5) that the question of whether all proper solutions to an embedding problem arise from a versal deformation can be reduced to studying when versal deformations of representations of finite groups are faithful. We will show (Theorem 3.2) that if $\text{Ker}(\lambda)$ is a p -group, then there is a faithful representation V of T such that $U(G, V)$ is a faithful G -module. This implies (Remark 3.3(b)) that each finite solvable extension of a given field can be constructed using a finite sequence of versal deformations. We also prove (Theorem 3.4) that one can detect when a versal deformation of a representation of a finite group is faithful from versal deformation rings associated to quotients of the group through which the representation factors. Our main result concerns when a versal deformation of a representation of a finite group is faithful. We obtain the following complete answer to this question for representations belonging to cyclic blocks and having endomorphism ring equal to k .

Let V be a representation of a finite group G over k such that $\text{End}_{kG}(V) = k$. Let K be the kernel of the action of G on V . Suppose V belongs to a cyclic block $B_{G,V}$ of kG . (For background on cyclic blocks see [1, Chapter V] and also section 4.) The block $B_{G,V}$ is either a matrix algebra over k , or there is a tree associated to $B_{G,V}$, called the Brauer tree $\Lambda(B_{G,V})$, which can be used to describe the composition series of all indecomposable $B_{G,V}$ -modules. Each vertex of $\Lambda(B_{G,V})$ has a positive integral multiplicity, which is 1 except for at most one vertex, which is called the exceptional vertex if it exists. We call $\Lambda(B_{G,V})$ a star with central exceptional vertex if all edges are adjacent to one vertex, called the center, and every vertex except possibly the center has multiplicity 1.

We can now state our main result.

Theorem 1.1. *The universal deformation $U(G, V)$ is a faithful representation of G if and only if K is a p -group, the Brauer tree $\Lambda(B_{G,V})$ is a star with central exceptional vertex and, in case $\Lambda(B_{G,V})$ has more than one edge, V is not a simple kG -module.*

We prove this theorem using the determination in [5] of the universal deformation rings of representations belonging to cyclic blocks.

In section 5 we discuss examples which illustrate Theorem 1.1. An example involving non-cyclic blocks, which is completed in an appendix (see section 6), concerns the double cover \tilde{A}_5 of the alternating group A_5 . Embedding problems associated to \tilde{A}_5 have been of longstanding interest (see [21, §2.4], [18]).

2. Versal deformations and embedding problems

Let k be an algebraically closed field of positive characteristic p . By a representation of the profinite group Γ over k we will mean a finite dimensional vector space V over k having the discrete topology together with a continuous k -linear action of Γ . Define $W = W(k)$ to be the ring of infinite Witt vectors over k . Let \mathcal{C} be a subcategory of the category \mathcal{C}^{top} of local topological W -algebras A with residue field k . A lift of V over A is a pair consisting of a topological $A\Gamma$ -module M which is a free A -module together with a $k\Gamma$ -module isomorphism $\phi_M : k \otimes_A M \rightarrow V$. A deformation of V over A is an isomorphism class of lifts (see [16, 7]). We say that with respect to \mathcal{C} , V has a versal deformation ring $R(\Gamma, V) \in \mathcal{C}$ and a versal deformation $U(\Gamma, V)$ if for each $A \in \mathcal{C}$ and each lift M of V over A , there is a (possibly not unique) morphism $\mu : R(\Gamma, V) \rightarrow A$ in \mathcal{C} so that there is an isomorphism between M and $A \otimes_{R(\Gamma, V), \mu} U(\Gamma, V)$ which respects ϕ_M and $\phi_{U(\Gamma, V)}$. If μ is unique for all A and all M , we will say $R(\Gamma, V)$ and $U(\Gamma, V)$ are universal. If $R(\Gamma, V)$ and $U(\Gamma, V)$ are universal, both $R(\Gamma, V)$ and $U(\Gamma, V)$ are unique up to a unique isomorphism.

For various \mathcal{C} , Γ and V it is known that versal (respectively universal) deformation rings and deformations exist. For example, if \mathcal{C} is the full subcategory $\mathcal{C}^{\text{Noeth}}$ of complete Noetherian objects in \mathcal{C}^{top} , one always has versal $R(\Gamma, V)$ and $U(\Gamma, V)$ provided Γ satisfies certain finiteness conditions [16, §1.1]. Furthermore, $U(\Gamma, V)$ and $R(\Gamma, V)$ are unique up to a (not necessarily unique) isomorphism. For arbitrary profinite Γ and \mathcal{C} the full subcategory $\mathcal{C}^{\text{ProArt}}$ of objects in \mathcal{C}^{top} which are the projective limits of their discrete Artinian quotients, it is known by [7] that universal $R(\Gamma, V)$ and $U(\Gamma, V)$ exist if $\text{End}_{k\Gamma}(V) = k$.

Suppose $U(\Gamma, V)$ is a versal deformation over $R(\Gamma, V)$. Let $\rho(\Gamma, V) : \Gamma \rightarrow \text{Aut}_{R(\Gamma, V)}(U(\Gamma, V))$ be a group homomorphism determining $U(\Gamma, V)$ as Γ -module. Here $\text{Aut}_{R(\Gamma, V)}(U(\Gamma, V))$ is isomorphic to $\text{GL}_n(R(\Gamma, V))$.

Lemma 2.1. *Suppose, as a Γ -module, V has a versal deformation $U(\Gamma, V)$ and a versal deformation ring $R(\Gamma, V)$ with respect to \mathcal{C} . The kernel $K(\Gamma, V) \subset \Gamma$ of $\rho(\Gamma, V)$ does not depend on the choice of versal deformation $U(\Gamma, V)$. Let H be a closed normal subgroup of Γ through which the action of Γ on V factors. Then there exists a unique closed ideal I of $R(\Gamma, V)$ which is minimal with respect to the property that $(R(\Gamma, V)/I) \otimes_{R(\Gamma, V), \tau_H} U(\Gamma, V)$ has trivial action of H , where $\tau_H : R(\Gamma, V) \rightarrow R(\Gamma, V)/I$ is the canonical surjection. Moreover, $R(\Gamma, V)/I$ is the maximal continuous quotient of $R(\Gamma, V)$ which is a versal deformation ring for V regarded as a Γ/H -module, and $(R(\Gamma, V)/I) \otimes_{R(\Gamma, V), \tau_H} U(\Gamma, V)$ is a versal deformation for V as Γ/H -module.*

We denote $R(\Gamma, V)/I$ by $R(\Gamma/H, V, \tau_H)$ and $(R(\Gamma, V)/I) \otimes_{R(\Gamma, V), \tau_H} U(\Gamma, V)$ by $U(\Gamma/H, V, \tau_H)$.

Proof. The kernel $K(\Gamma, V)$ does not depend on the choice of versal deformation $U(\Gamma, V)$, because if $R(\Gamma, V) \rightarrow R'$ is a ring homomorphism in \mathcal{C} , then $K(\Gamma, V)$ acts trivially on the tensor product $R' \otimes_{R(\Gamma, V)} U(\Gamma, V)$.

The rest of the lemma follows from the fact that if \mathcal{I} is a collection of closed ideals J of $R(\Gamma, V)$ with the property that $(R(\Gamma, V)/J) \otimes_{R(\Gamma, V), \nu_J} U(\Gamma, V)$ has trivial action of H , where $\nu_J : R(\Gamma, V) \rightarrow R(\Gamma, V)/J$ is the canonical surjection, then the intersection I of all ideals in \mathcal{I} also has this property. \square

From now on we assume there exist versal $R(\Gamma, V)$ and $U(\Gamma, V)$ with respect to \mathcal{C} . Suppose that the representation V of Γ is inflated from a representation of T via the surjection $\pi : \Gamma \rightarrow T$. We will denote this representation of T also by V . We may then view V as a representation of G via inflation through the surjection $\lambda : G \rightarrow T$. Lemma 2.1 insures that there exist versal $R(T, V)$ and $U(T, V)$. We will assume that there exist versal $R(G, V)$ and $U(G, V)$ with respect to \mathcal{C} .

Definition 2.2. A proper solution $h : \Gamma \rightarrow G$ to the embedding problem defined by $\pi : \Gamma \rightarrow T$ and $\lambda : G \rightarrow T$ will be said to arise from a versal deformation $U(\Gamma, V)$ if $K(\Gamma, V) \subset \text{Ker}(h)$.

Note that by Lemma 2.1, Definition 2.2 does not depend on the choice of versal deformation $U(\Gamma, V)$. Since it is in general difficult to find $K(\Gamma, V)$, we would like a sufficient condition for h to arise from $U(\Gamma, V)$ which involves only V as a representation of the finite group G .

Definition 2.3. We will say that V distinguishes G if $K(G, V)$ is trivial. This is equivalent to each versal deformation $U(G, V)$ of V as a representation of G being faithful. We will say that V stably distinguishes G if there is a surjection $\mu : \tilde{G} \rightarrow G$ of finite groups such that V inflated to \tilde{G} distinguishes \tilde{G} .

Note that if V is a faithful representation of G , then V distinguishes G .

Example 2.4. The construction of the universal deformation of a 1-dimensional representation given by Mazur in [16] has the following consequences. If $\dim_k(V) = 1$, then V defines a homomorphism $\chi_V : G \rightarrow k^*$ whose image is cyclic and of order prime to p . The group G is distinguished by V if and only if it is isomorphic to the product of this image with a finite abelian p -group. This is the case if and only if G is stably distinguished by V .

The following result shows that studying which proper solutions to embedding problems arise from versal deformations reduces to determining which versal deformations of representations of finite groups are faithful.

Theorem 2.5. *Let $\pi : \Gamma \rightarrow T$ and $\lambda : G \rightarrow T$ define an embedding problem, and let V be a representation of T over k as before.*

- (i) *If V distinguishes G , then all proper solutions $h : \Gamma \rightarrow G$ of the embedding problem defined by π and λ arise from each versal deformation $U(\Gamma, V)$.*
- (ii) *Suppose h is a proper solution of the embedding problem defined by π and λ which arises from a versal deformation $U(\Gamma, V)$. Then there is a finite group \tilde{G} and a surjection $\mu : \tilde{G} \rightarrow G$ with the following properties. There is a proper solution $\tilde{h} : \Gamma \rightarrow \tilde{G}$ to the embedding problem defined by $\pi : \Gamma \rightarrow T$ and $\tilde{\lambda} = \lambda \circ \mu : \tilde{G} \rightarrow T$ such that $h = \mu \circ \tilde{h}$. The inflation of V to \tilde{G} distinguishes \tilde{G} . In particular, V stably distinguishes G .*

Proof. Let $U(G, V)$ be a versal deformation for V . In part (i) we assume V distinguishes G , so $U(G, V)$ is a faithful representation of G . The inflation of $U(G, V)$ via the surjection $h : \Gamma \rightarrow G$ must have the form $R(G, V) \otimes_{R(\Gamma, V)} U(\Gamma, V)$ for a continuous $W(k)$ -algebra homomorphism $R(\Gamma, V) \rightarrow R(G, V)$. Thus the kernel $K(\Gamma, V)$ of $\rho(\Gamma, V)$ must be contained in the kernel of the surjection h , proving (i).

Conversely, we now suppose the hypotheses of (ii). Since $\rho(\Gamma, V) : \Gamma \rightarrow \text{Aut}_{R(\Gamma, V)}(U(\Gamma, V))$ is continuous,

$$K(\Gamma, V) = \text{Ker}(\rho(\Gamma, V)) = \bigcap_J \text{Ker}(\rho_J(\Gamma, V))$$

where J runs over the open ideals of $R(\Gamma, V)$ and

$$\rho_J(\Gamma, V) : \Gamma \rightarrow \text{Aut}_{R(\Gamma, V)/J}(U_J(\Gamma, V))$$

is the homomorphism induced by the Γ -module $U_J(\Gamma, V) = (R(\Gamma, V)/J) \otimes_{R(\Gamma, V)} U(\Gamma, V)$. Since $\text{ker}(h)$ has finite index in Γ , there is a J for which

$$\text{Ker}(\rho_J(\Gamma, V)) \subset \text{Ker}(h). \tag{2.1}$$

Let \tilde{G} be the image of $\rho_J(\Gamma, V)$. Since $R(\Gamma, V)/J$ is Artinian and $\rho_J(\Gamma, V)$ is continuous, \tilde{G} is finite. Because h is surjective, (2.1) gives canonical surjections $\mu : \tilde{G} \rightarrow G$ and $\tilde{h} : \Gamma \rightarrow \tilde{G}$ such that $h = \mu \circ \tilde{h}$. Thus \tilde{h} is a proper solution of

the embedding problem defined by $\pi : \Gamma \rightarrow T$ and $\tilde{\lambda} = \lambda \circ \mu : \tilde{G} \rightarrow T$. All that remains to be shown is that the inflation of V to \tilde{G} via $\tilde{\lambda} : \tilde{G} \rightarrow T$ distinguishes \tilde{G} .

We need to show that each versal deformation $U(\tilde{G}, V)$ is faithful as a \tilde{G} -module. Observe that since $\tilde{G} = \text{Image}(\rho_J(\Gamma, V))$, the module $U_J(\Gamma, V)$ is a faithful deformation of V as representation of \tilde{G} over the ring $R(\Gamma, V)/J$. By the definition of versal deformations, there is thus a ring homomorphism $R(\tilde{G}, V) \rightarrow R(\Gamma, V)/J$ such that $U_J(\Gamma, V)$ is isomorphic to $(R(\Gamma, V)/J) \otimes_{R(\tilde{G}, V)} U(\tilde{G}, V)$. Hence the faithfulness of $U_J(\Gamma, V)$ implies $U(\tilde{G}, V)$ must also be faithful, as required. \square

3. Groups distinguished by versal deformations

In view of Theorem 2.5, we are interested in when V distinguishes or stably distinguishes G . The case of greatest interest is when the kernel K of the action of G on V is large. Let $\overline{G} = G/K$.

Proposition 3.1. *If V stably distinguishes G then K is a p -group.*

Proof. One readily reduces to the case in which V distinguishes G . In this case, the natural surjection $\tau_K : R(G, V) \rightarrow R(\overline{G}, V, \tau_K)$ from Lemma 2.1 has pro- p kernel, since $R(G, V)$ and $R(\overline{G}, V, \tau_K)$ are local rings with the same residue field k . Hence the kernel of the induced homomorphism

$$\begin{aligned} \text{GL}_n(R(G, V)) &= \text{Aut}_{R(G, V)}(U(G, V)) \rightarrow \text{Aut}_{R(\overline{G}, V, \tau_K)}(U(\overline{G}, V, \tau_K)) \\ &= \text{GL}_n(R(\overline{G}, V, \tau_K)) \end{aligned}$$

is also a pro- p group. Thus if V distinguishes G , so that $U(G, V)$ is a faithful G -module, the kernel K of the action of G on V must be a pro- p group. Since G is finite, this implies K is a p -group. \square

If $\pi : \Gamma \rightarrow T$ and $\lambda : G \rightarrow T$ define an embedding problem, then $\text{Ker}(\lambda)$ is a subgroup of K . Hence Proposition 3.1 shows that one will not solve embedding problems using versal deformations, in the sense of Theorem 2.5, if $\text{Ker}(\lambda)$ is not a p -group. However, embedding problems in which $\text{Ker}(\lambda)$ is a p -group are of definite interest, for instance in trying to realize solvable groups as Galois groups over function fields such as $\mathbb{Q}(x)$. To cite an interesting example, the theory of modular towers developed by P. Bailey and M. Fried in [3] provides an infinite family of solutions to embedding problems over $\mathbb{Q}(x)$ in which $\text{Ker}(\lambda)$ is a p -group.

We have the following converse to Proposition 3.1.

Theorem 3.2. *Let $\mathcal{C} = \mathcal{C}^{\text{Noeth}}$, and suppose $\text{Ker}(\lambda)$ is a p -group. There exists a faithful representation V of T which distinguishes G . More precisely, there is such a V and a lift M of $\text{Infl}_T^G V$ over a local Artinian ring R with residue field k such that M is a faithful G -module.*

Proof. Suppose first that T is trivial, so that $G = \text{Ker}(\lambda)$ is a p -group. It will suffice to show that there is an R as in the statement of the Theorem and a faithful representation $\rho : G \rightarrow \text{GL}_n(R)$ for some $n \geq 1$ such that the reduction $\bar{\rho} : G \rightarrow \text{GL}_n(R/m_R) = \text{GL}_n(k)$ of ρ is trivial.

To construct ρ , we will use the following fact: There is a finite Galois extension L of the power series field $k((t))$ which is totally ramified and has Galois group $G = \text{Gal}(L/k((t)))$. One can prove this fact, even for k which are not algebraically closed, in the following way. By [12, Thm. 3.11], there exists an étale Galois cover $X \rightarrow \mathbf{A}_k^1$ of the affine line over k with Galois group G which is totally split over the origin. This cover is then regular, or equivalently geometrically irreducible. Let \bar{X} be the projective closure of X , so that \bar{X} is a G -cover of the projective line \mathbf{P}_k^1 which can ramify only over the point ∞ at infinity on \mathbf{P}_k^1 . Let ∞' be a point of \bar{X} over ∞ , and let $I_{\infty'} \subset G$ be its inertia group. If $I_{\infty'}$ is a proper subgroup of G , then a maximal proper subgroup J containing $I_{\infty'}$ is normal in G because G is nilpotent. But then \bar{X}/J is a non-trivial geometrically connected étale Galois p -cover of \mathbf{P}_k^1 , which does not exist by the Hurwitz Theorem. Hence $\bar{X} \rightarrow \mathbf{P}_k^1$ is totally ramified over ∞ . Thus if we take t to be a uniformizing parameter for \mathbf{P}_k^1 at ∞ , the completion over ∞' of the function field of \bar{X} gives an extension L of $k((t))$ of the required kind.

For each finite extension F of $k((t))$, let B_F be the integral closure of $k[[t]]$ in F . Define $v_F : B_F - \{0\} \rightarrow \mathbb{Z}$ to be the surjective discrete valuation, and let $\pi_F \in B_F$ be a uniformizing parameter, so that $v_F(\pi_F) = 1$. Since $L/k((t))$ is a totally ramified G -extension, G must equal the first wild ramification group of this extension. Hence by [20, Prop. IV.5],

$$v_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right) \geq 1 \tag{3.1}$$

for all non-trivial $\sigma \in G$. Choose a finite extension $Z/k((t))$ which is totally ramified, of degree $m > \#G$, with m prime to p . The compositum LZ is a totally ramified extension of $k((t))$, and LZ/Z is Galois with Galois group G . We claim that

$$v_{LZ}(\sigma(\alpha) - \alpha) > v_{LZ}(\pi_Z) = \#G \tag{3.2}$$

for all $\alpha \in B_{LZ}$. Since LZ/Z is totally ramified, any uniformizer π_{LZ} of LZ is an algebra generator for B_{LZ} over B_Z . Hence by [20, Lemme IV.1(c)], it will suffice to show (3.2) when $\alpha = \pi_{LZ}$. Since $v_{LZ}(\pi_L) = [Z : k((t))] = m$ and $v_{LZ}(\pi_Z) = \#G$ are coprime, we can choose π_{LZ} to have the form $\pi_L^a \cdot \pi_Z^b$ for some integers a and b . Since $\sigma \in G$ fixes Z , we have

$$\sigma(\pi_{LZ}) - \pi_{LZ} = (\sigma(\pi_L^a) - \pi_L^a) \cdot \pi_Z^b. \tag{3.3}$$

From (3.1) we have $v_L\left(\frac{\sigma(\pi_L^a)}{\pi_L^a} - 1\right) \geq 1$, so

$$v_L(\sigma(\pi_L^a) - \pi_L^a) \geq v_L(\pi_L^a) + 1. \tag{3.4}$$

Using (3.4) in (3.3) gives

$$\begin{aligned}
v_{LZ}(\sigma(\pi_{LZ}) - \pi_{LZ}) &= v_{LZ}(\sigma(\pi_L^a) - \pi_L^a) + v_{LZ}(\pi_Z^b) \\
&= [LZ : L] \cdot v_L(\sigma(\pi_L^a) - \pi_L^a) + v_{LZ}(\pi_Z^b) \\
&\geq [LZ : L] \cdot (v_L(\pi_L^a) + 1) + v_{LZ}(\pi_Z^b) \\
&= v_{LZ}(\pi_L^a \cdot \pi_Z^b) + [LZ : L] \\
&> v_{LZ}(\pi_{LZ}) + \#G
\end{aligned} \tag{3.5}$$

since we chose Z so $[LZ : L] = [Z : k((t))] = m > \#G$. This implies (3.2).

The discrete valuation ring B_{LZ} is a free B_Z -module of rank $\#G$. The elements of G act B_Z -linearly on B_{LZ} . This action gives a faithful representation $\tilde{\rho} : G \rightarrow \mathrm{GL}_n(B_Z)$ with $n = \#G$. The inequality (3.2) implies that for all $\sigma \in G$ and all $\alpha \in B_{LZ}$, $\sigma(\alpha) - \alpha \in \pi_Z B_{LZ}$. Therefore the image of $\tilde{\rho}$ must be in the subgroup of $\mathrm{GL}_n(B_Z)$ of matrices congruent to the identity matrix modulo $m_{B_Z} = \pi_Z B_Z$. Since G is finite, we can now take the ring R to be a sufficiently large Artinian quotient of B_Z and $\rho : G \rightarrow \mathrm{GL}_n(R)$ to be the image of $\tilde{\rho}$ under the homomorphism induced by the quotient homomorphism $B_Z \rightarrow R$. This proves Theorem 3.2 when T is trivial.

Suppose now that T is not trivial. We have shown that there is an integer $n \geq 1$ so that if V_0 is the n -dimensional trivial representation of the p -group $A = \mathrm{Ker}(\lambda)$, then there is a lift M_0 of V_0 over a local Artinian ring R with residue field k such that M_0 is a faithful A -module. Define $V = \mathrm{Ind}_A^G V_0$. Then V is a faithful representation of $T = G/A$ over k , and $M = \mathrm{Ind}_A^G M_0$ is a lift of V over R which is a faithful G -module. This completes the proof. \square

Remark 3.3.

- (a) When $\mathrm{Ker}(\lambda)$ in Theorem 3.2 is abelian, we can take the ring R to be the group ring $k[\mathrm{Ker}(\lambda)]$ and V to be $\mathrm{Ind}_{\mathrm{Ker}(\lambda)}^G k$. This is because the multiplication action of $\mathrm{Ker}(\lambda)$ on R makes R a lift of the trivial representation k of $\mathrm{Ker}(\lambda)$, and $M = \mathrm{Ind}_{\mathrm{Ker}(\lambda)}^G R$ is a lift of V over R which is faithful as a G -module.
- (b) Theorem 3.2 implies that if G is solvable, and L is a G -extension of a given field N , there is a finite increasing sequence $\{L_j\}_{j=1}^r$ of Galois subfields over N such that $L_1 = N$, $L_r = L$, and L_{j+1} is contained in the fixed field of a versal deformation of the inflation of a representation of $\mathrm{Gal}(L_j/N)$. In this sense, finite solvable extensions of a given field can be constructed using versal deformations, giving an alternative to the usual construction of such extensions by radicals.

We now give a criterion for when V distinguishes G using versal deformation rings. Consider the following condition.

$$\begin{aligned}
&\text{For all nontrivial normal subgroups } J \text{ of } G \text{ contained in } K, \\
&\text{the natural surjection of rings } \tau_J : R(G, V) \rightarrow R(G/J, V, \tau_J) \\
&\text{given in Lemma 2.1 is not the identity.}
\end{aligned} \tag{3.6}$$

Theorem 3.4. *The module V distinguishes G if and only if Condition (3.6) holds.*

Proof. Since V is a faithful representation of \overline{G} , V distinguishes \overline{G} . Suppose V does not distinguish G , so $U(G, V)$ is not faithful as a representation of G . Let $J = K(G, V)$. Then $J \subseteq K$, because $U(\overline{G}, V, \tau_K) = R(\overline{G}, V, \tau_K) \otimes_{R(G, V), \tau_K} U(G, V)$ is a faithful representation of \overline{G} . Let Q be the kernel of $\tau_J : R(G, V) \rightarrow R(G/J, V, \tau_J)$. Then $\text{Infl}_{G/J}^G U(G/J, V, \tau_J) = R(G/J, V, \tau_J) \otimes_{R(G, V), \tau_J} U(G, V)$ is annihilated by Q . Since $U(G, V)$ is a G/J -module, it follows that there exists a ring homomorphism $\mu : R(G/J, V, \tau_J) \rightarrow R(G, V)$ so that

$$U(G, V) = R(G, V) \otimes_{R(G/J, V, \tau_J), \mu} \text{Infl}_{G/J}^G U(G/J, V, \tau_J).$$

Hence $U(G, V)$ is also annihilated by Q . Since $U(G, V)$ is a free $R(G, V)$ -module, it follows that $Q = \{0\}$ and τ_J is the identity.

On the other hand if there is a nontrivial normal subgroup J of G , $J \subseteq K$ such that $\tau_J : R(G, V) \rightarrow R(G/J, V, \tau_J)$ is the identity, then

$$U(G, V) = R(G/J, V, \tau_J) \otimes_{R(G, V), \tau_J} U(G, V) = \text{Infl}_{G/J}^G U(G/J, V, \tau_J).$$

So $U(G, V)$ is not faithful. □

4. Cyclic blocks

In this section we want to determine when a representation belonging to a cyclic block of the group ring of a finite group has a faithful versal deformation. We will prove Theorem 1.1, which gives a complete answer to this problem for representations having endomorphism ring k . The proof relies on results proved in [5].

For the convenience of the reader we recall from [1, Chapter V] some properties of cyclic blocks. Suppose G is a finite group and B is a block of kG having cyclic defect groups. If B has trivial defect groups, then B is isomorphic to a matrix algebra over k . Otherwise there is a tree, $\Lambda(B)$, associated to B which is called the Brauer tree of B . The edges of $\Lambda(B)$ correspond to the isomorphism classes of simple B -modules. A leaf vertex of $\Lambda(B)$ is a vertex which adjoins exactly one edge, and an edge is called a leaf edge if it adjoins a leaf vertex. An edge which is not a leaf edge is called an interior edge. The tree $\Lambda(B)$ has at most one distinguished vertex, called the exceptional vertex, with multiplicity $m > 1$. All nonexceptional vertices have multiplicity 1. The tree $\Lambda(B)$ is called a star if all edges are adjacent to one vertex, called the center. If additionally the exceptional vertex is the center or all vertices are nonexceptional, we say $\Lambda(B)$ is a tree with central exceptional vertex.

Suppose V is a representation of G over k such that $\text{End}_{kG}(V) = k$. Let K be the kernel of the action of G on V , and let $\overline{G} = G/K$. We assume that K is nontrivial. Then with respect to the category $\mathcal{C} = \mathcal{C}^{\text{ProArt}}, R(G, V), U(G, V), R(\overline{G}, V)$ and $U(\overline{G}, V)$ exist and are universal (see [7]). In particular, they are all unique up to a unique isomorphism. Condition (3.6) is thus equivalent to the

condition

For all nontrivial normal subgroups J of G contained in K , (4.1)
 the ring homomorphism $R(G, V) \rightarrow R(G/J, V)$ associated to
 the natural surjection $G \rightarrow G/J$ is not an isomorphism.

Suppose V belongs to a block $B_{G,V}$ of kG with cyclic defect group D_G . Then V belongs to a block $B_{\bar{G},V}$ of $k\bar{G}$ which also has cyclic defect groups (see [5, Lemma 9.2]), one of which will be called $D_{\bar{G}}$. By [5, Lemma 9.2], $D_{G/J}$ is contained in a conjugate of the image of D_G in G/J for each normal subgroup J of G contained in K . Hence all such $D_{G/J}$ are cyclic and of order at least that of $D_{\bar{G}}$.

To prove Theorem 1.1, we first analyze Condition (4.1) in the following two propositions.

Proposition 4.1. *Suppose $D_{\bar{G}}$ is nontrivial and that Condition (4.1) is satisfied. Then it follows that for all J in Condition (4.1), the map $\Lambda(B_{G/J,V}) \rightarrow \Lambda(B_{G,V})$ induced by inflation is a graph isomorphism of stars with different multiplicities located at the center of the star.*

Proof. Let J be as in Condition (4.1). By the remarks just preceding the statement of Proposition 4.1, $D_{G/J}$ is cyclic and nontrivial. So the Brauer tree $\Lambda(B_{G/J,V})$ is well-defined. By [5, Lemma 9.2] it follows that the map $\Lambda(B_{G/J,V}) \rightarrow \Lambda(B_{G,V})$ induced by inflation is a graph isomorphism of trees. Because of the description of the indecomposable modules for cyclic blocks in [13, 14], it follows that this graph isomorphism sends the exceptional vertex of $\Lambda(B_{G/J,V})$ to the exceptional vertex of $\Lambda(B_{G,V})$ if the multiplicity of $\Lambda(B_{G/J,V})$ is greater than 1.

Suppose the multiplicities of the exceptional vertices of $\Lambda(B_{G/J,V})$ and $\Lambda(B_{G,V})$ were equal. Then $\#D_G = \#D_{G/J}$ (see [1, Chapter V]). By [5, Theorem 1.2], the only cases when the isomorphism type of $R(G, V)$ (respectively $R(G/J, V)$) does not determine $\#D_G$ (respectively $\#D_{G/J}$) are when V lies in the orbit under the Heller operator of a leaf edge S in $\Lambda(B_{G,V})$ (respectively in $\Lambda(B_{G/J,V})$) which does not have an exceptional leaf vertex. Hence, because we assume Condition (4.1) to be satisfied, V must be as in one of these cases. But then, since $\Lambda(B_{G/J,V})$ and $\Lambda(B_G)$ are isomorphic trees which have the same exceptional vertex, it follows that S defines in both $\Lambda(B_{G,V})$ and $\Lambda(B_{G/J,V})$ a leaf edge which does not have an exceptional leaf vertex. So $R(G/J, V) = W = R(G, V)$ by [5, Theorem 1.2]. This contradicts Condition (4.1). Hence the multiplicities of the exceptional vertices of $\Lambda(B_{G/J,V})$ and $\Lambda(B_{G,V})$ are different. In particular, the multiplicity of $\Lambda(B_{G,V})$ has to be strictly greater than 1.

Suppose $\Lambda(B_{G,V})$ is not a star with central exceptional vertex. Then there exists either (a) a path of two edges S, U where S is a leaf edge with exceptional leaf vertex, or (b) a path of three edges R, S, U where the common vertex of R and S is exceptional. Consider the projective cover $P_{S,G/J}$ of S as a G/J -module. The description of the indecomposable modules for cyclic blocks as given in [13, 14] shows that no indecomposable $B_{G,V}$ -module can be isomorphic to the inflation of

$P_{S,G/J}$ from G/J to G . This is a contradiction. So the Brauer trees of $B_{G,V}$ and $B_{G/J,V}$ are stars with different multiplicities located at the center of the star. \square

Define $d^j(V) = \dim_k \hat{H}^j(G, \text{Hom}_k(V, V))$ for $j \in \mathbb{Z}$, where \hat{H}^j denotes the j -th Tate cohomology group. The following result shows to what extent the converse of Proposition 4.1 holds.

Proposition 4.2. *Assume that K is a p -group. Suppose $D_{\overline{G}}$ is nontrivial and $\Lambda(B_{G,V})$ is a star with central exceptional vertex. Then for all nontrivial normal subgroups J of G which are contained in K it follows that $\Lambda(B_{G/J,V})$ is a star with central exceptional vertex of strictly smaller multiplicity than the one of $\Lambda(B_{G,V})$.*

One has $d^j(V) \leq 1$ for all $j \geq 0$. If $d^1(V) \neq 0$ or $d^2(V) \neq 0$, then Condition (4.1) is satisfied. If $d^1(V) = 0 = d^2(V)$, then $R(G, V) = W = R(\overline{G}, V)$, and Condition (4.1) is not satisfied.

Proof. By the remarks just prior to Proposition 4.1, $D_{G/J}$ is cyclic nontrivial and of order at most that of D_G . By [5, Lemma 9.2] it follows that the map $\Lambda(B_{G/J,V}) \rightarrow \Lambda(B_{G,V})$ induced by inflation is a bijection of trees, and the multiplicity of the exceptional vertex of $\Lambda(B_{G/J,V})$ is bounded by that of the exceptional vertex of $\Lambda(B_{G,V})$. Because of the description of the indecomposable modules for cyclic blocks in [13, 14], it follows that this graph isomorphism sends the exceptional vertex of $\Lambda(B_{G/J,V})$ to the exceptional vertex of $\Lambda(B_{G,V})$ if the multiplicity of $\Lambda(B_{G/J,V})$ is greater than 1. Hence the exceptional vertex of $\Lambda(B_{G/J,V})$ is at the center. Suppose the multiplicities of the exceptional vertices of $\Lambda(B_{G,V})$ and $\Lambda(B_{G/J,V})$ were equal. Then every projective indecomposable $\Lambda(B_{G,V})$ -module would be inflated from G/J . However, J is a nontrivial normal p -subgroup of G , so J does not act trivially on any projective indecomposable $\Lambda(B_{G,V})$ -module. This contradiction shows the exceptional vertex of $\Lambda(B_{G/J,V})$ has strictly smaller multiplicity than that of $\Lambda(B_{G,V})$.

By [5, Theorem 1.2], $d^j(V) \leq 1$ for all $j \geq 0$. The explicit determination of the universal deformation rings in [5, Theorem 1.2] shows that the universal deformation rings are nonisomorphic for G and G/J unless $d^1(V) = 0 = d^2(V)$, in which case the universal deformation rings are in both cases the ring of Witt vectors W . \square

Remark 4.3. The conditions for $d^j(V)$ in Proposition 4.2 can also be expressed using the stable Auslander–Reiten quiver associated to $B_{G,V}$ (see [5, Section 3]). For background on Auslander–Reiten quivers see, for example, [2]. Let e_G be the number of isomorphism classes of simple $B_{G,V}$ -modules. If $e_G = 1$ then $\text{End}_{kT}(V) = k$ implies V is isomorphic to the unique simple $B_{T,V}$ -module. For such V one has $d^1(V) \neq 0 \neq d^2(V)$. Suppose now that $e_G > 1$ and as before that $\text{End}_{kT}(V) = k$. Then $d^1(V) \neq 0$ or $d^2(V) \neq 0$ if and only if V lies at distance d with $1 \leq d \leq e_G - 1$ from the boundary of the stable Auslander–Reiten quiver of

$B_{G,V}$. Also $d^1(V) = 0 = d^2(V)$ if and only if V lies at the boundary of the stable Auslander–Reiten quiver.

Propositions 4.1 and 4.2 need the assumption that $D_{\overline{G}}$ is nontrivial. For blocks $B_{\overline{G},V}$ with trivial defect group $D_{\overline{G}}$, we have the following result.

Lemma 4.4. *If $D_{\overline{G}}$ is trivial and D_G is nontrivial, then V corresponds to a leaf edge of $\Lambda(B_{G,V})$ which has a nonexceptional leaf vertex.*

Proof. See the proof of [5, Theorem 1.6] in section 9 in [5]. \square

The following theorem gives some insight into the possible behaviors of the kernel K of V as a normal subgroup of G .

Theorem 4.5. *Let K_p be a Sylow p -subgroup of K . Further let $K' = \text{Ker}(\rho(G, V))$ be the kernel of $U(G, V)$ as a representation of G . So $K' \leq K$.*

- (i) *One has $K_p \leq sD_Gs^{-1}$ for some $s \in G$.*
- (ii) *If $D_{\overline{G}}$ is trivial, then $K_p = sD_Gs^{-1}$ for some $s \in G$.*
- (iii) *Suppose that $d^1(V) \neq 0$ or $d^2(V) \neq 0$. Then the group K' is a p' -group, and the quotient group K/K' is a p -group. So K is a semidirect product $K = K' \rtimes K_p$.*

Proof. Since V is relatively D_G -projective, as a G -module, V is a direct summand of $\text{Ind}_{D_G}^G \text{Res}_{D_G}^G V$. By Mackey's Theorem (see for example [1, Lemma 8.7]), $\text{Res}_{K_p}^G V$ is a direct summand of

$$\bigoplus_{s \in K_p \backslash G / D_G} \text{Ind}_{K_p \cap sD_Gs^{-1}}^{K_p} s \otimes (\text{Res}_{D_G}^G V).$$

Since $\text{Res}_{K_p}^G V$ is a trivial K_p -module, by Krull–Remak–Schmidt, there is an $s \in K_p \backslash G / D_G$ such that $\text{Ind}_{K_p \cap sD_Gs^{-1}}^{K_p} s \otimes (\text{Res}_{D_G}^G V)$ has a summand with trivial K_p -action. Since the trivial module for K_p has a Sylow p -subgroup as vertex and K_p is a p -group, it follows that $K_p \cap sD_Gs^{-1} = K_p$ which is (i).

We now turn to the proof of (ii). If D_G is trivial, then K_p is as well by part (i), so (ii) holds. We now suppose D_G is nontrivial. Considering the projection $\pi : kG \rightarrow k\overline{G}$, it follows that $\pi(B_{G,V})$ is a sum of blocks of $k\overline{G}$. If one of these blocks had a nontrivial defect group, there would be a bijection between the Brauer trees of this block and of $B_{G,V}$ by [5, Lemma 9.2], which is impossible. So all these blocks have defect 0. Since K is the kernel of V , V is an indecomposable $k\overline{G}$ -module and thus a projective simple $k\overline{G}$ -module. This means that V is also a simple kG -module. By Lemma 4.4, the module V corresponds to a leaf edge of the Brauer tree of $B_{G,V}$ which has a nonexceptional leaf vertex. Thus [5, Theorem 3.2] implies V lies at the boundary of the stable Auslander–Reiten quiver of $B_{G,V}$.

Claim. *There is an indecomposable $B_{G,V}$ -module which lies at the boundary of the stable Auslander–Reiten quiver of $B_{G,V}$ and which has vertex D_G .*

Proof of Claim. Let D_1 be the unique subgroup of D_G of order p , let N_1 be the normalizer of D_1 in G . Let B_1 be the Brauer correspondent of $B_{G,V}$ in kN_1 , so B_1 also has D_G as a defect group. By the proof of [4, Theorem 6.5.5], the Green correspondence defines an isomorphism between the stable Auslander–Reiten quivers of $B_{G,V}$ and B_1 . Thus to prove the claim, we are free to replace G by N_1 , so that D_1 becomes normal in G and $\Lambda(B_{G,V})$ is a star with central exceptional vertex. If $D_G = D_1$, any simple module X for $B_{G,V} = B_1$ lies at the boundary of the stable Auslander–Reiten quiver, and X must have vertex D_G because it is not projective. Suppose now that D_1 is a proper subgroup of D_G . Then D_1 acts trivially on each simple $B_{G,V}$ -module X , since D_1 is a normal p -subgroup of G . The block $B_{G/D_1,X}$ of $k(G/D_1)$ to which X belongs has nontrivial defect group D_G/D_1 (see the proof of [6, Lemma 8.7]). By induction there exists an indecomposable $B_{G/D_1,X}$ -module Y which lies at the boundary of the stable Auslander–Reiten quiver of $B_{G/D_1,X}$ and which has vertex D_G/D_1 . Since $\Lambda(B_{G/D_1,X})$ is a star with central exceptional vertex, X lies in the orbit of Y under the Heller operator, so also has vertex D_G/D_1 as $B_{G/D_1,X}$ -module. It follows that the inflation of X to G has vertex D_G as $B_{G,V}$ -module, which proves the Claim.

We continue now with the proof of part (ii). Since the application of the Heller operator does not change vertices of modules and since V lies at the boundary of the stable Auslander–Reiten quiver of $B_{G,V}$, it follows that V has vertex D_G . Since V is a projective $k\bar{G}$ -module, it follows that V , as a G -module, is relatively K -projective, and thus relatively K_p -projective. This means D_G is conjugate to a subgroup of K_p . On the other hand, part (i) shows that K_p is conjugate to a subgroup of D_G . So K_p and D_G are conjugate in G . This proves (ii).

For part (iii) we assume that $d^1(V) \neq 0$ or $d^2(V) \neq 0$. From [5, Theorem 1.2], it follows that the order of D_G can be retrieved from the isomorphism type of $R(G, V)$. Since K' is the kernel of the universal deformation $U = U(G, V)$, U is also a universal deformation $U(G/K', V)$ for G/K' with universal deformation ring $R(G/K', V) \cong R(G, V)$. Suppose the order of K' is divisible by p . Because K'_p is contained in K_p , and K_p is contained in a conjugate of D_G by part (i), the order of the defect groups changes when going from G to G/K' . But this means that $R(G, V)$ and $R(G/K', V)$ cannot be isomorphic. So K' is a p' -group. Since $U = U(G, V)$ is faithful as a G/K' -module it follows as in the proof of Proposition 3.1 that K/K' is a p -group. This proves (iii). \square

Remark 4.6. Theorem 4.5 shows that if $B_{G,V}$ has nontrivial cyclic defect groups, there are two possibilities. If V distinguishes G , then the kernel of V , as a G -module, is a p -group lying inside a defect group of the block $B_{G,V}$ to which V belongs. If V does not distinguish G , then there is a normal subgroup K' of

G which lies inside the kernel of V so that V distinguishes G/K' . Moreover, if $d^1(V) \neq 0$ or $d^2(V) \neq 0$, then K' is a p' -group.

We are now able to prove Theorem 1.1.

Proof of Theorem 1.1. Suppose first that V distinguishes G . Then by Proposition 3.1, K is a p -group. By Theorem 3.4, Condition (4.1) is satisfied. If $D_{\overline{G}}$ is nontrivial, Proposition 4.1 shows that $\Lambda(B_{G,V})$ is a star with central exceptional vertex. So by Proposition 4.2, since Condition (4.1) is satisfied, it follows that $d^1(V) \neq 0$ or $d^2(V) \neq 0$. Consider now the case when $\Lambda(B_{G,V})$ has more than one edge. If V were simple, then V would correspond to a leaf edge of $\Lambda(B_{G,V})$ with a nonexceptional leaf vertex, since $\Lambda(B_{G,V})$ is a star with central exceptional vertex. Hence $d^1(V)$ and $d^2(V)$ would both be zero by [5, Proposition 1.3]. This is a contradiction. Hence V is not simple if $\Lambda(B_{G,V})$ has more than one edge. If $D_{\overline{G}}$ is trivial, then by [5, Theorem 1.2], $R(\overline{G}, V) = W$. If D_G were trivial, then also $R(G, V) = W$ and Condition (4.1) would not be satisfied. Hence D_G is nontrivial. By Lemma 4.4, V corresponds to a leaf edge of $\Lambda(B_{G,V})$ having a nonexceptional leaf vertex. If $\Lambda(B_{G,V})$ has only one edge, $\Lambda(B_{G,V})$ is a star with central exceptional vertex. If $\Lambda(B_{G,V})$ had more than one edge, then by [5, Proposition 1.3], $R(G, V) = W$ and Condition (4.1) would not be satisfied. This is a contradiction. Therefore, $\Lambda(B_{G,V})$ has the required form.

Suppose now that K is a p -group, $\Lambda(B_{G,V})$ is a star with central exceptional vertex, and, in case $\Lambda(B_{G,V})$ has more than one edge, that V is not simple. In particular, D_G is nontrivial. By [5, Theorem 1.2 and Proposition 1.3], this means that $d^1(V) \neq 0$ or $d^2(V) \neq 0$. By Theorem 3.4, it suffices to verify Condition (4.1). If $D_{\overline{G}}$ is nontrivial, this follows from Proposition 4.2. If $D_{\overline{G}}$ is trivial, Lemma 4.4 shows that V is a leaf edge of $\Lambda(B_{G,V})$ with nonexceptional leaf vertex. In particular, V is a simple kG -module. Because of the assumptions, this means that $\Lambda(B_{G,V})$ has only one edge. Hence [5, Proposition 1.3] shows that $R(G, V) = WD_G$ and $R(\overline{G}, V) = W$. Further, for all normal nontrivial subgroups J of G which lie inside K , $R(G/J, V) = WD_{G/J}$. It follows from Theorem 4.5 that $K = D_G$. Therefore, by the remarks just prior to the statement of Proposition 4.1, $D_{G/J}$ is conjugate to a subgroup of D_G/J . Hence Condition (4.1) is satisfied. This completes the proof of Theorem 1.1.

5. Examples

In this section we want to study a few examples of embedding problems and the question of whether all their proper solutions arise from versal deformations. For simplicity, we will consider those representations V of T with $\text{End}_{kT}(V) = k$, since under this condition we have universal deformations with respect to the category $\mathcal{C}^{\text{ProArt}}$ (see [7]). Additionally, Condition (3.6) can be replaced by Condition (4.1).

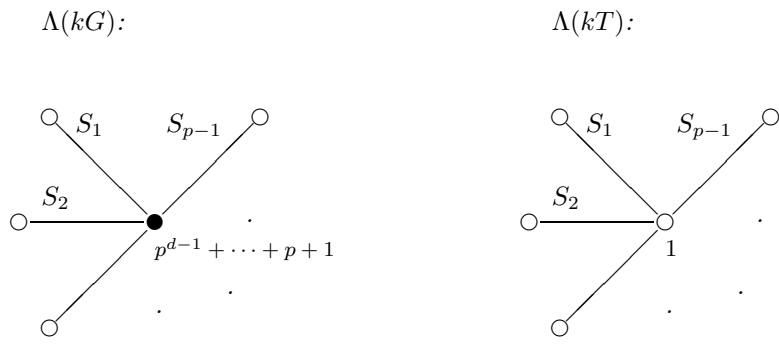
In view of Theorem 2.5 we consider whether there is a representation V of T with $\text{End}_{kT}(V) = k$ so that V distinguishes G . We will use Theorem 1.1 and Theorem 3.4 with Condition (3.6) replaced by Condition (4.1) to determine whether V distinguishes G .

Our first two examples deal with cyclic blocks. The third example looks at a tame block case.

Example 5.1. We first suppose T is the cyclic group $T = (\mathbb{Z}/p\mathbb{Z})^*$, and G is a semidirect product $G = (\mathbb{Z}/p\mathbb{Z}) \rtimes_{\delta} (\mathbb{Z}/p\mathbb{Z})^*$ where $a \in (\mathbb{Z}/p\mathbb{Z})^*$ acts on $(\mathbb{Z}/p\mathbb{Z})$ by multiplication by a^{δ} , $1 \leq \delta \leq p - 1$. Further let V be a faithful 1-dimensional kT -module.

Since G has a unique normal Sylow p -subgroup which is isomorphic to the cyclic group $\mathbb{Z}/p\mathbb{Z}$, all blocks of kG have cyclic defect groups. By [5, Example 8.4], kG has $\text{gcd}(\delta, p - 1)$ blocks whose Brauer trees are all stars with central exceptional vertex and $(p - 1)/\text{gcd}(\delta, p - 1)$ edges. If $\delta < p - 1$, then each Brauer tree has more than one edge. If $\delta = p - 1$, then each Brauer tree has exactly one edge. By Theorem 1.1, since V is a simple kG -module, V does not distinguish G if $\delta < p - 1$. If $\delta = p - 1$, then V distinguishes G . Note that for $\delta = p - 1$, G is a direct product $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^*$.

Example 5.2. In our second example we suppose $p \geq 3$, $d \geq 2$ and that G is a semidirect product $G = (\mathbb{Z}/p^d\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^*$, where we assume that $(\mathbb{Z}/p\mathbb{Z})^*$ acts faithfully on $\mathbb{Z}/p^d\mathbb{Z}$. Let T be the quotient group $(\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^*$ of G . Then, by [5, Example 8.4], $\Lambda(kG)$ and $\Lambda(kT)$ are both stars with central exceptional vertex and $p - 1$ edges. Note that the multiplicity of the exceptional vertex of $\Lambda(kG)$ (respectively $\Lambda(kT)$) is $p^{d-1} + \dots + p + 1$ (respectively 1).



Let V be a 2-dimensional uniserial kT -module. So for example $V = \begin{smallmatrix} S_1 \\ S_2 \end{smallmatrix}$. Then it follows that V is a faithful kT -module, since otherwise the kernel of V would be $\mathbb{Z}/p\mathbb{Z}$. But then V would be a representation of $(\mathbb{Z}/p\mathbb{Z})^*$ and thus would be the direct sum of two simple modules. This is a contradiction. So V is a faithful

kT -module. By Theorem 1.1, V distinguishes G .

An arithmetic instance of Examples 5.1 and 5.2 arises from considering how to construct cyclic degree p^d extensions L of $\mathbb{Q}(\zeta_p)$ which are Galois over \mathbb{Q} and such that $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ acts on $\text{Gal}(L/\mathbb{Q}(\zeta_p)) \cong \mathbb{Z}/p^d\mathbb{Z}$ via a particular character. If $d = 1$, Example 5.1 shows one cannot construct all such L from universal deformations of indecomposable representations of $T = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. If $d \geq 2$, Example 5.2 shows that one can construct all such L from the universal deformation of any 2-dimensional indecomposable representation V of $T = \text{Gal}(L'/\mathbb{Q})$, where L' is the degree p extension of $\mathbb{Q}(\zeta_p)$ contained in L . When L is unramified, solving these embedding problems is of classical interest in connection with the eigenspaces of the p -part of the ideal class group of $\mathbb{Q}(\zeta_p)$ (see [23], [19], [15]).

Example 5.3. In our third example we consider the case when $p = 2$, T is the alternating group A_5 of degree 5 and G is its double cover $G = \tilde{A}_5 \cong \text{SL}_2(\mathbb{Z}/5\mathbb{Z})$. Suppose V is one of the two 2-dimensional simple kT -modules. Then V is a faithful kT -module since T is simple. By [4, Section 6.6], V belongs to the principal block B_0 of kT which has Kleinian 4-groups as defect groups and is thus a tame block. Note that the principal block of kG has quaternion defect groups of order 8 and is also tame.

By [4, Theorem 6.6.3], B_0 has 3 simple modules and $\text{Ext}_{kT}^1(V, V) = 0$. This means that $k \otimes_W R(T, V) = k$ (see [7, Section 5]). So $R(T, V)$ is a quotient ring of W . Because A_5 has no ordinary irreducible character of degree 2, it follows that $R(T, V) = W/2^n W$ for some integer $n \geq 1$. Since $G = \text{SL}_2(\mathbb{Z}/5\mathbb{Z})$ does have an ordinary irreducible character of degree 2 which reduces to V modulo 2, it follows that, as G -module, V does have a lift over W . This means that $R(G, V)$ properly surjects onto $R(T, V)$. So Condition (4.1) is satisfied and V distinguishes G by Theorem 3.4.

We show in the next section that in fact $R(T, V) = k$ and $R(G, V) = W$. The construction of a $G = \tilde{A}_5$ extension L/N which contains a given $T = A_5$ extension L'/N is a famous problem and has been studied by many authors. For example, it is shown in [21, Section 2.4] that the obstruction to being able to construct such a G -extension is the second Stiefel–Whitney class of the trace form of L'/N . When $N = \mathbb{Q}(t)$ and t is an indeterminate, some calculations of this obstruction are given in [18].

6. Appendix: The double cover of A_5

In this section we adopt the notations of Example 5.3 of section 5. Thus T is the alternating group $A_5 \cong \text{SL}_2(\mathbb{F}_4)$ and G is its double cover $G = \tilde{A}_5$. For V we take one of the two 2-dimensional irreducible representations of T over an algebraically

closed field k of characteristic $p = 2$. Our goal is to prove:

Proposition 6.1. *The universal deformation rings $R(T, V)$ and $R(G, V)$ are isomorphic to k and to W , respectively.*

The decomposition matrix for the principal block of $k\tilde{A}_5$ is given in [8, p. 305]. This matrix shows that there is an absolutely irreducible ordinary character χ of \tilde{A}_5 whose image under the decomposition map is the Brauer character of V . Further the values of χ lie in W , since W contains all roots of unity of order prime to 2. The decomposition matrix also shows χ occurs with multiplicity 1 in the character of the projective $W\tilde{A}_5$ -cover of V . Hence χ is the character of a representation $\tilde{\lambda} : \tilde{A}_5 \rightarrow \text{GL}_2(W)$ which lifts V over W . Since χ is irreducible and A_5 has no 2-dimensional ordinary irreducible representation, it must be the case that $\tilde{\lambda}(-1) = -I$ where -1 is the nontrivial element of the center of \tilde{A}_5 and I is the identity matrix in $\text{GL}_2(W)$. Let H be the subgroup of $\text{GL}_2(W/4W)$ which is the inverse image of $\text{SL}_2(\mathbb{F}_4)$ under reduction modulo 2. We conclude that there is a commutative diagram

$$\begin{array}{ccccccc}
 1 & \rightarrow & \{\pm 1\} & \rightarrow & \tilde{A}_5 & \rightarrow & A_5 & \rightarrow & 1 \\
 & & \downarrow & & \downarrow \lambda & & \downarrow \phi & & \\
 1 & \rightarrow & 1 + 2M_2(W/4W) & \rightarrow & H & \rightarrow & \text{SL}_2(\mathbb{F}_4) & \rightarrow & 1
 \end{array} \tag{6.1}$$

in which $\phi : A_5 \rightarrow \text{SL}_2(\mathbb{F}_4)$ is a matrix representation afforded by V , and λ is the reduction of $\tilde{\lambda}$ modulo 4. Thus in particular, ϕ is an isomorphism. In the bottom row of this diagram, one has an isomorphism

$$\delta : 1 + 2M_2(W/4W) \rightarrow M_2(k)^+ \tag{6.2}$$

sending $1 + 2\alpha \pmod 4$ to $\alpha \pmod 2$, where $M_2(k)^+$ is the additive group of $M_2(k)$.

Lemma 6.2. *Let $\beta \in H^2(A_5, M_2(k)^+)$ be the extension class defined by the bottom row of Diagram (6.1) and the inverse of the map δ in (6.2). To prove Proposition 6.1, it will suffice to show that the extension class β is nontrivial.*

Proof. By Example 5.3 of section 5, $R(T, V) = W/p^n W$ for some integer $n \geq 1$, where $T = A_5$. Thus to show $R(T, V) = k = W/pW$, it will suffice to show that V has no lift as a representation of T over $W/4W$. The existence of such a lift is equivalent to the splitting of the bottom row of Diagram (6.1), which is equivalent to the triviality of β . As for $R(G, V)$ when $G = \tilde{A}_5$, we have already seen that as a representation of G , V has a lift over W . Thus to prove $R(G, V) = W$, it will suffice to show that $H^1(G, \text{Hom}_k(V, V)) = \{0\}$, since then $R(G, V)/p(R, V) = k$. So to complete the proof of Lemma 6.2, we will show that if $H^1(G, \text{Hom}_k(V, V)) \neq \{0\}$ then $\beta = 0$. Suppose $h : G \rightarrow \text{Hom}_k(V, V)$ is a one-cycle which is not a one-boundary. If h were trivial on the nontrivial element -1 of the center of $G = \tilde{A}_5$, then h would be the inflation of a one-cycle of A_5 . However, we showed in Example 5.3 of section 5 that $H^1(A_5, \text{Hom}_k(V, V)) = \text{Ext}_{kA_5}^1(V, V) = \{0\}$. Thus if $h(-1) =$

0 then h would be a boundary, contrary to assumption. Therefore $h(-1)$ must be nontrivial. Because h is a one-cycle and -1 is central, we find from the definition of one-cycles that then conjugation action of \tilde{A}_5 on $\text{Hom}_k(V, V)$ is trivial on $h(-1)$. Therefore $h(-1)$ is a scalar matrix, and since it is nonzero, we can multiply h by a scalar in order to be able to assume that $h(-1) = I$ is the multiplicative identity of $\text{Hom}_k(V, V)$. We now use h to define a splitting $s : \text{SL}_2(\mathbb{F}_4) \rightarrow H$ of the bottom row of Diagram (6.1) in the following way. Let $\tilde{\gamma}$ be an element of \tilde{A}_5 , with image γ in A_5 . Define

$$s(\gamma) = \tilde{\lambda}(\tilde{\gamma}) \cdot \delta^{-1}(h(\tilde{\gamma}))$$

where δ is as in (6.2). Using the fact that $\tilde{\lambda}(-1) = -I$, it follows that s is well-defined and a splitting of the bottom row of Diagram (6.1), hence $\beta = 0$. \square

We now define kA_5 -modules C and C' by the diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & \{0, I\} & \rightarrow & M_2(k)^+ & \rightarrow & C & \rightarrow & 0 \\ & & \downarrow a & & \downarrow b & & \downarrow c & & \\ 0 & \rightarrow & k & \rightarrow & M_2(k)^+ & \rightarrow & C' & \rightarrow & 0 \end{array} \quad (6.3)$$

in which I in the upper left corner is the identity matrix in $M_2(k)^+$, the left arrow a is the natural inclusion, the middle arrow b is the identity map, and c is the induced map on cokernels.

Lemma 6.3. *To show that the extension class β defined in Lemma 6.2 is not trivial, it will suffice to prove that $H^1(A_5, C') = 0$.*

Proof. Let $\beta_0 \in H^2(A_5, \{\pm 1\})$ be the extension class of the top row of Diagram (6.1), so that β_0 is the unique nontrivial element of order two in $H^2(A_5, \{\pm 1\})$. We have a commutative diagram

$$\begin{array}{ccc} H^2(A_5, \{\pm 1\}) & \rightarrow & H^2(A_5, 1 + 2M_2(W/4W)) \\ \downarrow & & \downarrow \\ H^2(A_5, \{0, I\}) & \rightarrow & H^2(A_5, M_2(k)^+) \end{array} \quad (6.4)$$

in which the vertical arrows are isomorphisms induced by the isomorphism δ of (6.2). The image of β_0 under the composition of the homomorphisms in the top row and the right column of Diagram (6.4) is the class β of Lemma 6.2. Hence to show β is nontrivial, it will suffice to show that the map in the bottom row of Diagram (6.4) is injective. By the long exact cohomology sequence of the top row of Diagram (6.3), it will thus suffice to show $H^1(A_5, C) = 0$. The right column of Diagram (6.3) gives an exact sequence

$$0 \rightarrow C'' \rightarrow C \rightarrow C' \rightarrow 0 \quad (6.5)$$

in which $C'' \cong k/\{0, I\}$ has trivial A_5 -action. Therefore

$$H^1(A_5, C'') = \text{Hom}(A_5, C'') = 0.$$

Hence the long exact cohomology sequence of (6.5) shows $H^1(A_5, C) = 0$ if $H^1(A_5, C') = 0$. \square

Completion of the proof of Proposition 6.1. To show that $H^1(A_5, C') = 0$ we look at the exact sequence

$$0 \rightarrow U \rightarrow C' = M_2(k)^+/k \xrightarrow{\text{tr}} k \rightarrow 0 \quad (6.6)$$

where tr is the usual trace map. A simple matrix calculation shows that as a kA_5 -module, C' has no submodule isomorphic to k with trivial A_5 -action. This means that U has to be one of the two irreducible 2-dimensional kA_5 -modules, and $H^0(A_5, C') = 0$. In the long exact cohomology sequence of (6.6)

$$\dots \rightarrow H^0(A_5, C') \rightarrow H^0(A_5, k) \rightarrow H^1(A_5, U) \rightarrow H^1(A_5, C') \rightarrow H^1(A_5, k) \rightarrow \dots$$

we also have $H^0(A_5, k) = k$ and $H^1(A_5, k) = \text{Hom}(A_5, k) = 0$. Thus to show that $H^1(A_5, C') = 0$ it suffices to show that $\dim_k H^1(A_5, U) = 1$. By [4, Theorem 6.6.3(ii)], the two irreducible 2-dimensional kA_5 -modules occur both with multiplicity 1 in $\text{rad}(P_1)/\text{rad}^2(P_1)$, where P_1 is the projective cover of the trivial simple kA_5 -module k and rad denotes the Jacobson radical. Since U is one of the two 2-dimensional irreducible kA_5 -modules, this means that

$$H^1(A_5, U) = \text{Ext}_{kA_5}^1(k, U) = \text{Hom}_{kA_5}(\text{rad}(P_1)/\text{rad}^2(P_1), U) = k.$$

References

- [1] J. L. Alperin, *Local Representation Theory*, Cambridge studies in advanced mathematics 11, Cambridge University Press, Cambridge, 1986.
- [2] M. Auslander, I. Reiten and S. Smalø, *Representation Theory of Artin Algebras*. Cambridge studies in advanced mathematics 36, Cambridge University Press, Cambridge, 1995.
- [3] P. Bailey and M. D. Fried, Hurwitz monodromy, spin separation and higher levels of a Modular Tower, in: *Arithmetic fundamental groups and noncommutative algebra*, 79–220, Proc. Symp. Pure Math. vol. 70, American Math. Society, 2002.
- [4] D. J. Benson, *Representations and Cohomology I*, Cambridge studies in advanced mathematics 30, Cambridge University Press, Cambridge, 1991.
- [5] F. M. Bleher and T. Chinburg, Universal deformation rings and cyclic blocks, *Math. Ann.* **318** (2000), 805–836.
- [6] E. C. Dade, Blocks with cyclic defect groups, *Ann. of Math.* **84** (1966), 22–48.
- [7] B. de Smit and H. W. Lenstra, Explicit construction of universal deformation rings, in: *Modular Forms and Fermat's Last Theorem* (Boston, MA, 1995), pp. 313–326, Springer-Verlag, New York, 1997.
- [8] K. Erdmann, *Blocks of Tame Representation Type and Related Algebras*, Lecture Notes in Mathematics, Vol. 1428, Springer-Verlag, Berlin–Heidelberg–New York, 1990.
- [9] F. Gouvêa, *Arithmetic of p -adic modular forms*, Lecture Notes in Mathematics, Vol. 1304, Springer-Verlag, Berlin–Heidelberg–New York, 1988.
- [10] F. Gouvêa, Deforming Galois representations: controlling the conductor, *J. Number Theory* **34** (1990), 95–113.

- [11] F. Gouvêa and B. Mazur, On the density of modular representations, in: *Computational perspectives in Number Theory* (Chicago 1995), pp. 127–142, AMS/IP Stud. Adv. Math., Amer. Math. Soc., Providence, R.I., 1997.
- [12] D. Harbater, Embedding problems with local conditions, *Israel Journal of Mathematics* **118** (2000), 317–355.
- [13] G. J. Janusz, Indecomposable modules for finite groups, *Ann. of Math.* **89** (1969), 209–241.
- [14] H. Kupisch, Unzerlegbare Moduln endlicher Gruppen mit zyklischer p -Sylow-Gruppe, *Math. Z.* **108** (1969), 77–104.
- [15] S. Lang, *Cyclotomic Fields*, Graduate Texts in Mathematics, Vol. 59, Springer-Verlag, New York-Heidelberg, 1978.
- [16] B. Mazur, Deforming Galois representations, in: *Galois groups over \mathbb{Q}* (Berkeley, CA, 1987), pp. 385–437, Springer-Verlag, New York, 1989.
- [17] B. Mazur, Deformation theory of Galois representations, in: *Modular Forms and Fermat's Last Theorem* (Boston, MA, 1995), pp. 243–311, Springer-Verlag, New York, 1997.
- [18] J.-F. Mestre, Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois A_n , *J. Algebra* **131** (1990), 483–495.
- [19] K. Ribet, A modular construction of unramified p -extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.
- [20] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968.
- [21] J.-P. Serre, L'invariant de Witt de la forme $\text{Tr}(x^2)$, *Comment. Math. Helv.* **59** (1984), 651–676.
- [22] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Annals of Math.* **141** (1995), 553–572.
- [23] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, Vol. 83, Springer-Verlag, New York, 1997.

F. Bleher
Department of Mathematics
University of Iowa
Iowa City, IA 52242-1419
USA
e-mail: fbleher@math.uiowa.edu

T. Chinburg
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA
e-mail: ted@math.upenn.edu

(Received: January 30, 2001)



To access this journal online:
<http://www.birkhauser.ch>
