Illinois Journal of Mathematics
Volume 47, Number 3, Fall 2003, Pages 899–919
S 0019-2082

DEFORMATIONS WITH RESPECT TO AN ALGEBRAIC GROUP

FRAUKE M. BLEHER AND TED CHINBURG

Abstract. Let $\mathcal{G}$ be a smooth linear algebraic group over the ring of Witt vectors of a finite field k. In this paper, we study deformations of representations of a profinite group into the points $\mathcal{G}(k)$ of $\mathcal{G}$ over k. We show that the $\mathcal{G}$-deformation functor has a versal deformation ring, and we generalize criteria of Tilouine concerning when this ring is universal. If $\mathcal{G}$ is an algebraic subgroup of GL_n, we study when the $\mathcal{G}$-deformation functor is a subfunctor of the GL_n-deformation functor studied by Mazur. When $\mathcal{G}$ is an orthogonal group, this leads to studying versal versions of results of Serre and Fröhlich about the connection between Stiefel-Whitney classes, spinor norms and Hasse-Witt invariants of orthogonal Galois representations.

1. Introduction

Let k be a finite field of positive characteristic p. Define $W = W(k)$ to be the ring of infinite Witt vectors over k, and suppose Γ is a profinite group. In [10], Mazur developed a deformation theory of finite dimensional representations of Γ over k using results of Schlessinger. For a more general construction, see the work of de Smit and Lenstra [4]. Universal deformation rings have become a basic tool in arithmetic geometry (see, e.g., [3], [18], [16], [1] and their references).

In [17], Tilouine studied universal deformations of representations ρ of Γ into the points $\mathcal{G}(k)$ over k of a specified smooth linear algebraic group $\mathcal{G}$ over W. He showed in [17, Thm. 3.3] that there is a universal deformation of ρ provided $\mathcal{G}$ has smooth center, the connected component of the identity of the centralizer of ρ is contained in the center of $\mathcal{G} \otimes_W k$, and Γ satisfies Mazur's finiteness condition (Φ_p) [10, p. 387]. In this paper we make no assumptions about the center of $\mathcal{G}$, and we consider a slightly different functor than the

Received September 11, 2002; received in final form May 15, 2003.

2000 *Mathematics Subject Classification.* Primary 20C20. Secondary 11E81, 11E88.

The first author was supported in part by NSA Young Investigator Grant MDA904-01-1-0050 and by NSF Grant DMS01-39737. The second author was supported in part by NSF Grant DMS00-70433.

one considered by Tilouine. In Theorem 2.7 we show that this functor, which we call the $\mathcal{G}$-deformation functor, always has a versal deformation provided Γ satisfies Mazur's condition (Φ_p). We also obtain in Theorem 2.7 a necessary and sufficient condition, called the centralizer lifting property, for this versal deformation to be universal. In Theorem 2.8 we deduce from Theorem 2.7 a generalization of the above mentioned sufficient condition for universality proved by Tilouine.

In Section 3, we prove Theorem 2.7 using Schlessinger's criteria, and we also prove Theorem 2.8. In Section 4, we assume that $\mathcal{G}$ is a subgroup of another smooth linear algebraic group $\mathcal{H}$ over W. When the $\mathcal{H}$-deformation functor is representable, we give in Theorem 4.1 necessary and sufficient criteria for the $\mathcal{G}$-deformation functor to be a subfunctor of the $\mathcal{H}$-deformation functor. We then look at classical cases when $\mathcal{H} = \mathrm{GL}_n$ and show that for $\mathcal{G} = \mathrm{SL}_n$ one has a subfunctor if p does not divide n. For symplectic and orthogonal groups, one has subfunctors for $p > 2$.

In Section 5, we specialize to the case in which $\mathcal{G}$ is an orthogonal group and $p > 2$. In this case, we interpret the $\mathcal{G}$-deformation functor in terms of orthogonal lifts of orthogonal representations. In Section 6 we consider versal versions of results of Serre and Fröhlich about the connection between Stiefel-Whitney classes, spinor norms and Hasse-Witt invariants associated to orthogonal representations of Galois groups. In this context, we prove that different specializations at geometric points of the spectrum of the versal orthogonal deformation ring all give rise to the same second Stiefel-Whitney class. We also discuss the related problem of generalizing Fontaine's ring B_{cris} for representations of the absolute Galois group of a p-adic local field which are defined over fields of positive transcendence degree over $\mathbb{Q}_p$.

2. Deformation functors for algebraic groups

Suppose k is a finite field of positive characteristic p, $W = W(k)$ is the ring of infinite Witt vectors over k, and Γ is a profinite group. Define $\hat{\mathcal{C}}$ to be the category of complete local Noetherian rings with residue field k. The morphisms in $\hat{\mathcal{C}}$ are continuous W-algebra homomorphisms which induce the identity on k. Let $\mathcal{C}$ be the subcategory of Artinian objects in $\hat{\mathcal{C}}$.

Hypothesis 2.1. Throughout this paper, we assume that $\mathcal{G}$ is a smooth linear algebraic group over W, and that $\rho : \Gamma \to \mathcal{G}(k)$ is a continuous representation of Γ into $\mathcal{G}(k)$, where $\mathcal{G}(k)$ has the discrete topology.

Definition 2.2. Suppose $R \in \mathrm{Ob}(\hat{\mathcal{C}})$. Let $\kappa_{\mathcal{G},R} : \mathcal{G}(R) \to \mathcal{G}(k)$ be the natural surjection. Define $\hat{\mathcal{G}}$ to be the formal group of $\mathcal{G}$, defined by $\hat{\mathcal{G}}(R) = \mathrm{Ker}(\kappa_{\mathcal{G},R})$ for all R. Let $E_{\mathcal{G}}(R)$ be the set of continuous homomorphisms $\pi : \Gamma \to \mathcal{G}(R)$ which lift ρ, in the sense that the composition $\kappa_{\mathcal{G},R} \circ \pi$ is equal to ρ. Then $\hat{\mathcal{G}}(R)$ acts by conjugation on $E_{\mathcal{G}}(R)$. The elements of $E_{\mathcal{G}}(R)/\hat{\mathcal{G}}(R)$ are called the *$\mathcal{G}$-deformations of ρ over R.*

Definition 2.3. Let $\hat{F}_{\mathcal{G}} = \hat{F}_{\mathcal{G},\rho} : \hat{\mathcal{C}} \to \text{Sets}$ be the functor which sends each object R of $\hat{\mathcal{C}}$ to the set $\hat{F}_{\mathcal{G}}(R) = E_{\mathcal{G}}(R)/\hat{\mathcal{G}}(R)$. Let $F_{\mathcal{G}} = F_{\mathcal{G},\rho}$ be the restriction of $\hat{F}_{\mathcal{G}}$ to $\mathcal{C}$. We call $\hat{F}_{\mathcal{G}}$ the *$\mathcal{G}$-deformation functor.*

Remark 2.4. For $\mathcal{G} = \mathrm{GL}_n$, $\hat{F}_{\mathrm{GL}_n,\rho}$ is the deformation functor considered by Mazur in [10].

Definition 2.5. The functor $F_{\mathcal{G}}$ will be said to have the *centralizer lifting property*, if the following is true for each surjective morphism $A_1 \xrightarrow{\alpha} A_0$ in $\mathcal{C}$ with nilpotent kernel. Let π_1 be an element of $E_{\mathcal{G}}(A_1)$, and define $\pi_0 = \alpha\pi_1 \in E_{\mathcal{G}}(A_0)$. Define $Z_{\hat{\mathcal{G}}}(\pi_i)$ to be the subgroup of $\hat{\mathcal{G}}(A_i)$ consisting of all elements commuting (elementwise) with the image of π_i in $\mathcal{G}(A_i)$. We require for all A_1, A_0, π_1 and π_0 as above that the natural homomorphism $\lambda : Z_{\hat{\mathcal{G}}}(\pi_1) \to Z_{\hat{\mathcal{G}}}(\pi_0)$ is surjective. Note that the surjectivity of λ depends only on $[\pi_1] \in F_{\mathcal{G}}(A_1) = E_{\mathcal{G}}(A_1)/\hat{\mathcal{G}}(A_1)$ and the ring homomorphism $A_1 \xrightarrow{\alpha} A_0$, but not on the choice of representative π_1 for $[\pi_1]$.

Definition 2.6. (Mazur, [10, p. 387]) A group Γ satisfies the *finiteness condition* (Φ_p), if $H^1(\Gamma, M)$ is finite for each finite discrete Γ-module M of p-power order.

We can now state our main results about the existence and uniqueness of versal and universal $\mathcal{G}$-deformations and $\mathcal{G}$-deformation rings.

Theorem 2.7. *Suppose Γ satisfies (Φ_p).*

(i) *The functor $F_{\mathcal{G}}$ has a pro-representable hull* (*cf.* [14, Def. 2.7] *and* [11, §1.2]), *and $\hat{F}_{\mathcal{G}}$ is continuous* (*cf.* [11]). *Thus there is an object $R_{\mathcal{G}}(\Gamma,\rho) \in \mathrm{Ob}(\hat{\mathcal{C}})$ and a $\mathcal{G}$-deformation $[\pi_{\mathcal{G}}(\Gamma,\rho)]$ of ρ over $R_{\mathcal{G}}(\Gamma,\rho)$ with the following property. For each $R \in \mathrm{Ob}(\hat{\mathcal{C}})$, the map $\mathrm{Hom}_{\hat{\mathcal{C}}}(R_{\mathcal{G}}(\Gamma,\rho), R) \to \hat{F}_{\mathcal{G}}(R)$ induced by $\alpha \to [\alpha \circ \pi_{\mathcal{G}}(\Gamma,\rho)]$ is surjective, and this map is bijective if R is the ring of dual numbers $k[\epsilon]$ where $\epsilon^2 = 0$. We call $R_{\mathcal{G}}(\Gamma,\rho)$ the versal $\mathcal{G}$-deformation ring of ρ and $[\pi_{\mathcal{G}}(\Gamma,\rho)]$ the versal $\mathcal{G}$-deformation of ρ. Both $R_{\mathcal{G}}(\Gamma,\rho)$ and $[\pi_{\mathcal{G}}(\Gamma,\rho)]$ are unique up to non-canonical isomorphisms.*

(ii) *The functor $\hat{F}_{\mathcal{G}}$ is represented by $R_{\mathcal{G}}(\Gamma,\rho)$ if and only if $F_{\mathcal{G}}$ has the centralizer lifting property from Definition 2.5. In this case, the universal $\mathcal{G}$-deformation ring $R_{\mathcal{G}}(\Gamma,\rho)$ and the universal $\mathcal{G}$-deformation $[\pi_{\mathcal{G}}(\Gamma,\rho)]$ are both unique up to canonical isomorphisms.*

For a smooth linear algebraic group $\mathcal{H}$ over W, let $\mathcal{H}_k$ be the group scheme $k \otimes_W \mathcal{H}$, and let $\mathrm{Lie}(\mathcal{H}_k)$ be the Lie algebra of $\mathcal{H}_k$.

Theorem 2.8. *Suppose Γ satisfies (Φ_p), and that there is an algebraic subgroup $\mathcal{J}$ of $\mathcal{G}$ over W which has the following properties:*

(a) *The group scheme $\mathcal{J}$ is smooth over W.*
(b) *For all $R \in \mathrm{Ob}(\mathcal{C})$ and all $\pi \in E_{\mathcal{G}}(R)$, $\hat{\mathcal{J}}(R) \subseteq Z_{\hat{\mathcal{G}}}(\pi)$.*
(c) *The natural injection $\mathrm{Lie}(\mathcal{J}_k) \to \mathrm{Lie}(\mathcal{G}_k)$ induces an isomorphism between $\mathrm{Lie}(\mathcal{J}_k)$ and the centralizer of ρ in $\mathrm{Lie}(\mathcal{G}_k)$.*

Then the versal $\mathcal{G}$-deformation ring $R_{\mathcal{G}}(\Gamma, \rho)$ is universal.

Remark 2.9. If $\mathcal{J}$ is the center of $\mathcal{G}$, Theorem 2.8 is the criterion proved by Tilouine in [17, Thm. 3.3]. Note that in this case, condition (b) holds automatically. To find other $\mathcal{J}$ for which the conditions of Theorem 2.8 hold, it is often useful to take advantage of information concerning the group Γ.

Example 2.10. Suppose Γ is perfect and satisfies (Φ_p). Suppose $\mathcal{G}$ is a product $\mathcal{H} \times \mathcal{H}'$ of smooth linear algebraic groups over W such that $\mathcal{H}'$ is solvable. For all R in $\mathcal{C}$ and $\pi \in E_{\mathcal{G}}(R)$, the image of $\pi : \Gamma \to \mathcal{G}(R)$ lies in the subgroup $\mathcal{H}(R)$. In particular, $\rho : \Gamma \to \mathcal{G}(k)$ factors through a representation $\rho' : \Gamma \to \mathcal{H}(k)$. It follows that if a subgroup $\mathcal{J}'$ of $\mathcal{H}$ having the properties listed in Theorem 2.8 for the representation ρ' exists, then $\mathcal{J} = \mathcal{J}' \times \mathcal{H}'$ is a subgroup having these properties for ρ. Note that if $\mathcal{H}'$ is not abelian, $\mathcal{J}$ is larger than the center of $\mathcal{G}$.

3. Schlessinger's criteria and continuity

In this section, we use Schlessinger's criteria to prove Theorem 2.7, following the arguments in Mazur [10, 11]. We also prove Theorem 2.8.

Suppose $A_0, A_1, A_2 \in \mathrm{Ob}(\mathcal{C})$ and that we have a diagram

$$\begin{tikzcd} A_1 \arrow[dr, "\alpha_1"'] & & A_2 \arrow[dl, "\alpha_2"] \\ & A_0 & \end{tikzcd} .$$

Let A_3 be the pullback $A_3 = A_1 \times_{A_0} A_2 = \{(a_1, a_2) \in A_1 \times A_2 \mid \alpha_1(a_1) = \alpha_2(a_2)\}$, and let $\alpha_{31} : A_3 \to A_1$ and $\alpha_{32} : A_3 \to A_2$ be the natural surjections. Then $\alpha_1 \, \alpha_{31} = \alpha_2 \, \alpha_{32}$. Assume that $\alpha_1 : A_1 \to A_0$ is a small extension, i.e., α_1 is surjective with kernel $t \cdot A_1$ such that $t \cdot m_{A_1} = 0$. Set $E_i = E_{\mathcal{G}}(A_i)$ and $G_i = \hat{\mathcal{G}}(A_i)$ for $i = 0, 1, 2, 3$. Consider the natural map

$$b : F_{\mathcal{G}}(A_3) \to F_{\mathcal{G}}(A_1) \times_{F_{\mathcal{G}}(A_0)} F_{\mathcal{G}}(A_2) \,,$$

which is the same as

$$\begin{array}{rccc} b: & E_3/G_3 & \to & E_1/G_1 \times_{E_0/G_0} E_2/G_2 \\ & [\pi_3] & \mapsto & [\pi_1] \times_{[\pi_0]} [\pi_2] \end{array} \tag{3.1}$$

where $\pi_1 = \alpha_{31}\pi_3$, $\pi_2 = \alpha_{32}\pi_3$, and $\pi_0 = \alpha_1\pi_1 = \alpha_2\pi_2$. Schlessinger's criteria (H1) through (H4) for $F_{\mathcal{G}}$ are as follows:

(H1) The map b is surjective.
(H2) The map b is bijective if $A_0 = k$ and $A_1 = k[\epsilon]$.
(H3) The tangent space $t_{F_{\mathcal{G}}} = F_{\mathcal{G}}(k[\epsilon])$ is finite dimensional over k.
(H4) The map b is bijective if $A_2 = A_1$ and $\alpha_2 = \alpha_1$.

PROPOSITION 3.1. *Suppose Γ satisfies (Φ_p). Then Schlessinger's criteria* (H1), (H2) *and* (H3) *are always satisfied for $F_{\mathcal{G}}$. Schlessinger's criterion* (H4) *is satisfied if and only if $F_{\mathcal{G}}$ satisfies the centralizer lifting property from Definition 2.5.*

LEMMA 3.2. *The map b is surjective.*

Proof. The closed immersion $\mathrm{Spec}(A_0) \to \mathrm{Spec}(A_1)$ is defined by a nilpotent ideal. Because $\mathcal{G}$ is assumed to be smooth over W, the homomorphism $\mathcal{G}(A_1) \to \mathcal{G}(A_0)$ induced by α_1 is surjective by the Jacobian criterion for formal smoothness [9, 28.C]. Thus $G_1 \to G_0$ is surjective. Suppose $[\pi_1] \in E_1/G_1$ and $[\pi_2] \in E_2/G_2$ have the property that $[\alpha_1\pi_1] = [\alpha_2\pi_2]$ in E_0/G_0. Then $\alpha_2\pi_2 = g_0(\alpha_1\pi_1)g_0^{-1}$ for some $g_0 \in G_0$. Since $G_1 \to G_0$ is surjective, g_0 lifts to an element $g_1 \in G_1$ with $\alpha_1 g_1 = g_0$. Hence

$$\alpha_2\pi_2 = \alpha_1(g_1\pi_1g_1^{-1}) ,$$

and $g_1\pi_1g_1^{-1}$ and π_2 define an element $\pi_3 \in E_3$. □

We get the following criterion for the injectivity of b (cf. [10, Lemma 1]). As in Definition 2.5, let π_1 be an element in E_1 and π_0 its image in E_0. As before, for $i = 0, 1$, set $Z_{\hat{\mathcal{G}}}(\pi_i)$ equal to the subgroup of G_i consisting of all elements commuting with the image of π_i in $\mathcal{G}(A_i)$.

LEMMA 3.3. *Suppose $\pi_1 \in E_1$.*

(i) *If the homomorphism $Z_{\hat{\mathcal{G}}}(\pi_1) \to Z_{\hat{\mathcal{G}}}(\pi_0)$ induced by α_1 is surjective, then b is injective.*
(ii) *Suppose $A_2 = A_1$ and $\alpha_2 = \alpha_1$. If b is injective, then $Z_{\hat{\mathcal{G}}}(\pi_1) \to Z_{\hat{\mathcal{G}}}(\pi_0)$ is surjective.*

Proof. To prove (i), suppose $\pi_3, \pi_3' \in E_3$ so that $b([\pi_3]) = [\pi_1] \times_{[\pi_0]} [\pi_2]$ and $b([\pi_3']) = [\pi_1'] \times_{[\pi_0']} [\pi_2']$. We have to show that $b([\pi_3]) = b([\pi_3'])$ implies $[\pi_3] = [\pi_3']$. Suppose $b([\pi_3]) = b([\pi_3'])$, i.e., $[\pi_1] = [\pi_1']$ and $[\pi_2] = [\pi_2']$. Then there exist $g_i \in G_i$ for $i = 1, 2$ with

$$\begin{aligned} \pi_1' &= g_1\pi_1g_1^{-1} , \\ \pi_2' &= g_2\pi_2g_2^{-1} . \end{aligned}$$

If we denote by $g_{i,0}$ the image of g_i in G_0 under α_i, then

$$g_{1,0}\pi_0g_{1,0}^{-1} = g_{2,0}\pi_0g_{2,0}^{-1} .$$

Hence $g_{1,0}^{-1}g_{2,0} \in Z_{\hat{\mathcal{G}}}(\pi_0)$. By assumption, $g_{1,0}^{-1}g_{2,0}$ can be lifted to $h_1 \in Z_{\hat{\mathcal{G}}}(\pi_1)$. We define $\tilde{g}_1 = g_1 h_1$. By the definition of $Z_{\hat{\mathcal{G}}}(\pi_1)$ it follows that

$$\pi_1' = g_1\pi_1 g_1^{-1} = (g_1h_1)\pi_1(g_1h_1)^{-1} = \tilde{g}_1\pi_1\tilde{g}_1^{-1}$$

and

$$\tilde{g}_{1,0} = g_{1,0}h_{1,0} = g_{10}(g_{1,0}^{-1}g_{2,0}) = g_{2,0}\ .$$

Therefore, $\tilde{g}_1$ and g_2 define $g_3 \in G_3$ with $\pi_3' = g_3\pi_3 g_3^{-1}$.

To prove (ii), we assume $A_2 = A_1$ and $\alpha_2 = \alpha_1$. Suppose $h_0 \in Z_{\hat{\mathcal{G}}}(\pi_0)$. Since $\mathcal{G}$ is smooth over W, there exists $h \in G_1$ with $\alpha_1 h = h_0$. Then $\pi_1' = h\pi_1 h^{-1}$ satisfies $\alpha_1\pi_1' = \pi_0 = \alpha_1\pi_1$, and we thus obtain elements $[\pi_1 \times_{\pi_0} \pi_1]$ and $[\pi_1 \times_{\pi_0} \pi_1']$ of E_3/G_3. Since $[\pi_1] = [\pi_1']$ in $E_1/G_1 = E_2/G_2$ and b is injective, there must be an equality

$$[\pi_1 \times_{\pi_0} \pi_1] = [\pi_1 \times_{\pi_0} \pi_1']$$

in E_3/G_3. This means that there is an element $g_3 = g_1 \times_{g_0} g_1'$ of G_3 such that

$$g_3(\pi_1 \times_{\pi_0} \pi_1)g_3^{-1} = \pi_1 \times_{\pi_0} \pi_1'\ .$$

One now sees that the element $x = g_1' g_1^{-1}$ lies in $\mathrm{Ker}(G_1 \to G_0)$, and $x\pi_1 x^{-1} = \pi_1'$. Thus $x^{-1}h \in Z_{\hat{\mathcal{G}}}(\pi_1)$ has image h_0 under α_1, so $Z_{\hat{\mathcal{G}}}(\pi_1) \to Z_{\hat{\mathcal{G}}}(\pi_0)$ is surjective. □

Remark 3.4. As before, let $\mathcal{G}_k$ be the group scheme $k \otimes_W \mathcal{G}$ and let $\mathrm{Lie}(\mathcal{G}_k)$ be the Lie algebra of $\mathcal{G}_k$. Viewing $\mathcal{G}$ as a subgroup of GL_n for some integer n, we may identify $\mathrm{Lie}(\mathcal{G}_k)$ with the k-vector space $\mathrm{Mat}_n(k)$ of all $n\times n$ matrices M over k such that $1+\epsilon M$ is an element of $\mathcal{G}(k[\epsilon])$, where 1 is the identity matrix. The group Γ acts on $\mathrm{Lie}(\mathcal{G}_k)$ through the adjoint action $\mathrm{ad}(\rho)$ which is defined by letting $\gamma \in \Gamma$ act as conjugation by $\rho(\gamma)$. In the following, we use the notation

$$z^\gamma = \mathrm{ad}(\rho)(\gamma)\, z = \rho(\gamma)\, z\, \rho(\gamma)^{-1} \tag{3.2}$$

for $z \in \mathrm{Lie}(\mathcal{G}_k)$.

Proof of Proposition 3.1. By Lemma 3.2, (H1) is satisfied.

For (H2), we consider the case when $A_0 = k$ and $A_1 = k[\epsilon]$ is the ring of dual numbers. In this case G_0 is the trivial group, which implies that $Z_{\hat{\mathcal{G}}}(\pi_0)$ is trivial for all $\pi_0 \in E_0$. Hence by Lemma 3.3(i), (H2) follows.

For (H3), we have to show that the tangent space $t_{F_{\mathcal{G}}} = F_{\mathcal{G}}(k[\epsilon])$ is finite dimensional over k. Using the canonical embedding $k \to k[\epsilon]$ defined by $a \mapsto \epsilon\, a$, we find that if $\pi \in E_{\mathcal{G}}(k[\epsilon])$, then there is a one-cocycle $c \in Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k))$ such that

$$\pi(\gamma) = (1 + \epsilon\, c(\gamma))\, \rho(\gamma)$$

for all $\gamma \in \Gamma$. This induces a vector space isomorphism

$$\begin{array}{cccc} \tau_{\mathcal{G}}: & t_{F_{\mathcal{G}}} & \to & H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k)) \\ & [\pi] & \mapsto & \langle c \rangle \end{array} \tag{3.3}$$

where $\langle c\rangle$ denotes the cohomology class of c. Because of condition (Φ_p), $H^1(\Gamma,\mathrm{Lie}(\mathcal{G}_k))$ is a finite dimensional k-vector space, so condition (H3) holds.

Condition (H4) is satisfied if and only if the map b is bijective when $A_2 = A_1$ and $\alpha_2 = \alpha_1$. By Lemma 3.3 this will be the case if and only if $F_{\mathcal{G}}$ has the centralizer lifting property, which completes the proof of Proposition 3.1. □

Proof of Theorem 2.7. Because of Proposition 3.1 we only have to show that $\hat{F}_{\mathcal{G}}$ is continuous, i.e., for all $R \in \mathrm{Ob}(\hat{\mathcal{C}})$

$$\hat{F}_{\mathcal{G}}(R) = \varprojlim_i F_{\mathcal{G}}(R/m_R^i)\ .$$

This follows as in the proof of [11, §20 Prop. 1], since $\mathcal{G}(R) = \varprojlim_i \mathcal{G}(R/m_R^i)$. □

In the proof of Theorem 2.8 we make use of the exponential map defined in [17]. For the convenience of the reader we summarize the properties we need in the following remark.

Remark 3.5. Suppose we have a short exact sequence

$$0 \to I \longrightarrow A_1 \xrightarrow{\alpha} A_0 \to 0$$

with $A_0, A_1 \in \mathrm{Ob}(\mathcal{C})$, $I \subset A_1$ and $I \cdot m_{A_1} = 0$. Then for each smooth linear algebraic group $\mathcal{H}$ over W there is a canonical short exact sequence of groups

$$0 \to I \otimes_k \mathrm{Lie}(\mathcal{H}_k) \xrightarrow{\exp_{\mathcal{H}}} \hat{\mathcal{H}}(A_1) \xrightarrow{\alpha} \hat{\mathcal{H}}(A_0) \to 0 \tag{3.4}$$

where the exponential map $\exp_{\mathcal{H}}$ is defined in [17, §3.5]. There it is also shown that if $\mathcal{H} = \mathcal{G}$, then for all $x \in I \otimes_k \mathrm{Lie}(\mathcal{G}_k)$, for all $\pi_1 \in E_{\mathcal{G}}(A_1)$ and for all $\gamma \in \Gamma$

$$\pi_1(\gamma)\exp_{\mathcal{G}}(x)\,\pi_1(\gamma)^{-1} = \exp_{\mathcal{G}}\left(\mathrm{ad}(\rho)(\gamma)\,x\right)\ .$$

Moreover, if $\mathcal{H}$ is a smooth subgroup scheme of $\mathcal{G}$ over W, then

$$\exp_{\mathcal{G}}\Big|_{I\otimes \mathrm{Lie}(\mathcal{H}_k)} = \exp_{\mathcal{H}}\ .$$

Proof of Theorem 2.8. Because of Theorem 2.7 we only have to show that $F_{\mathcal{G}}$ has the centralizer lifting property. Since $\mathcal{J}$ is supposed to be smooth over W, it is enough to prove the following claim.

Claim. *$Z_{\hat{\mathcal{G}}}(\pi) = \hat{\mathcal{J}}(R)$ for all $R \in \mathrm{Ob}(\mathcal{C})$ and for all $\pi \in E_{\mathcal{G}}(R)$.*

Proof of Claim. We prove the claim by induction. The claim is certainly true for $R = k$ since in this case $\pi = \rho$ and $Z_{\hat{\mathcal{G}}}(\pi)$ is the trivial group. Suppose now we have a short exact sequence

$$0 \to tA_1 \longrightarrow A_1 \xrightarrow{\alpha} A_0 \to 0$$

where $A_0, A_1 \in \mathrm{Ob}(\mathcal{C})$, $t \cdot m_{A_1} = 0$ and $tA_1 \cong k$. Then, as in (3.4), for each smooth linear algebraic group $\mathcal{H}$ over W there is a short exact sequence of groups

$$0 \to tA_1 \otimes_k \mathrm{Lie}(\mathcal{H}_k) \xrightarrow{\exp_{\mathcal{H}}} \hat{\mathcal{H}}(A_1) \xrightarrow{\alpha} \hat{\mathcal{H}}(A_0) \to 0\,. \tag{3.5}$$

Let $\pi_1 \in E_{\mathcal{G}}(A_1)$, $\pi_0 = \alpha\pi_1 \in E_{\mathcal{G}}(A_0)$, and assume by induction that $Z_{\hat{\mathcal{G}}}(\pi_0) = \hat{\mathcal{J}}(A_0)$. By condition (b) of Theorem 2.8, $\hat{\mathcal{J}}(A_1) \subseteq Z_{\hat{\mathcal{G}}}(\pi_1)$. Let $h \in Z_{\hat{\mathcal{G}}}(\pi_1)$ with image $h_0 = \alpha h$ in $Z_{\hat{\mathcal{G}}}(\pi_0) = \hat{\mathcal{J}}(A_0)$. Since $\mathcal{J}$ is smooth over W by condition (a) of Theorem 2.8, there exists $h_1 \in \hat{\mathcal{J}}(A_1) \subseteq Z_{\hat{\mathcal{G}}}(\pi_1)$ with $\alpha h_1 = h_0$. Then hh_1^{-1} lies in the kernel of α. Hence there exists $x \in tA_1 \otimes_k \mathrm{Lie}(\mathcal{G}_k)$ with $\exp_{\mathcal{G}}(x) = hh_1^{-1}$. Since we assumed $tA_1 \cong k$ as k-vector spaces, let $ta \in tA_1$ be the element sent to $1 \in k$ under this isomorphism. Then x has the form $x = ta \otimes z$ for a unique $z \in \mathrm{Lie}(\mathcal{G}_k)$, and for all $\gamma \in \Gamma$ we have

$$\begin{aligned} \exp_{\mathcal{G}}(ta \otimes z) &= hh_1^{-1} \\ &\overset{(*)}{=} \pi_1(\gamma)\, hh_1^{-1}\, \pi_1(\gamma)^{-1} \\ &= \exp_{\mathcal{G}}\left(\mathrm{ad}(\rho)(\gamma)\, x\right) = \exp_{\mathcal{G}}\left(ta \otimes z^{\gamma}\right) \end{aligned}$$

where z^{γ} is defined as in (3.2), and the equality $(*)$ is true because $hh_1^{-1} \in Z_{\hat{\mathcal{G}}}(\pi_1)$. Hence

$$z = z^{\gamma} = \mathrm{ad}(\rho)(\gamma)\, z$$

for all $\gamma \in \Gamma$, and z lies in the centralizer of ρ in $\mathrm{Lie}(\mathcal{G}_k)$. This implies by condition (c) of Theorem 2.8 that $z \in \mathrm{Lie}(\mathcal{J}_k)$. Hence $x \in tA_1 \otimes_k \mathrm{Lie}(\mathcal{J}_k)$, and $hh_1^{-1} = \exp_{\mathcal{G}}(x) = \exp_{\mathcal{J}}(x) \in \hat{\mathcal{J}}(A_1)$. Therefore, $h \in \hat{\mathcal{J}}(A_1)$, which completes the proof of the claim, and hence the proof of Theorem 2.8. □

4. Subfunctors

In this section we continue to use the notations of Sections 2 and 3. Our objective is to prove the following result.

THEOREM 4.1. *Let $\mathcal{G}$ and $\mathcal{H}$ be smooth linear algebraic groups over W, and suppose $\mathcal{G}$ is a subgroup of $\mathcal{H}$. Suppose the functor $\hat{F}_{\mathcal{H}}$ is representable. Then $\hat{F}_{\mathcal{G}}$ is a subfunctor of $\hat{F}_{\mathcal{H}}$ if and only if the natural map on the tangent spaces $t_{F_{\mathcal{G}}} = F_{\mathcal{G}}(k[\epsilon]) \to F_{\mathcal{H}}(k[\epsilon]) = t_{F_{\mathcal{H}}}$ is injective. In this case, $\hat{F}_{\mathcal{G}}$ is representable.*

Here $\hat{F}_{\mathcal{G}}$ is a subfunctor of $\hat{F}_{\mathcal{H}}$ if and only if the natural map

$$\iota_{\mathcal{G},\mathcal{H},R} : E_{\mathcal{G}}(R) \to E_{\mathcal{H}}(R)$$

induces an injection

$$\overline{\iota}_{\mathcal{G},\mathcal{H},R} : \hat{F}_{\mathcal{G}}(R) \to \hat{F}_{\mathcal{H}}(R) \tag{4.1}$$

for all $R \in \mathrm{Ob}(\hat{\mathcal{C}})$. After proving Theorem 4.1, we will consider the cases in which $\mathcal{G}$ is special linear, symplectic, or orthogonal, respectively, and $\mathcal{H} = \mathrm{GL}_n$.

Let us begin with some well-known constructions with one-cocycles and deformations. Suppose we have an exact sequence

$$0 \to I \longrightarrow A_1 \xrightarrow{\alpha} A_0 \to 0$$

with $A_0, A_1 \in \mathrm{Ob}(\mathcal{C})$, $I \subset A_1$ and $I \cdot m_{A_1} = 0$. Then, as in (3.4), we have a short exact sequence of groups

$$0 \to \mathrm{Lie}(\mathcal{G}_k) \otimes I \xrightarrow{\exp} \hat{\mathcal{G}}(A_1) \xrightarrow{\alpha} \hat{\mathcal{G}}(A_0) \to 0\ . \tag{4.2}$$

Suppose $\xi \in E_{\mathcal{G}}(A_1)$. Let $\xi_0 = \alpha\xi \in E_{\mathcal{G}}(A_0)$. Suppose X is in the group of one-cocycles $Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$. Then there exists an element $X(\xi) \in E_{\mathcal{G}}(A_1)$ defined by

$$X(\xi)(\gamma) = \exp(X(\gamma))\, \xi(\gamma) \tag{4.3}$$

for $\gamma \in \Gamma$. We have $\alpha X(\xi) = \xi_0$, and $(X + X')(\xi) = X(X'(\xi))$ if $X' \in Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$. If X is the one-coboundary $\gamma \mapsto z^\gamma - z$ associated to an element $z \in \mathrm{Lie}(\mathcal{G}_k) \otimes I$, and $h = \exp(z)$, then

$$X(\xi)(\gamma) = h^{-1}\exp(z^\gamma)\, \xi(\gamma) = h^{-1}\ \xi(\gamma)\ h\ \xi(\gamma)^{-1}\ \xi(\gamma) = h^{-1}\ \xi(\gamma)\ h\ . \tag{4.4}$$

Thus $X(\xi)$ is conjugate to ξ by $h^{-1} \in \hat{\mathcal{G}}(A_1)$. It follows that we have a map

$$\begin{array}{rccc} T_\xi : & H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I) & \to & F_{\mathcal{G}}(\alpha)^{-1}([\xi_0]) \\ & \langle X \rangle & \mapsto & [X(\xi)] \end{array} \tag{4.5}$$

where $\langle X \rangle$ is the cohomology class of X.

LEMMA 4.2. *Suppose, as above, that* $\xi \in F_{\mathcal{G}}(\alpha)^{-1}([\xi_0])$. *Then* T_ξ *is surjective. Let* X *be an element of* $Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$, *and define* $\xi' = X(\xi)$. *Then* $T_\xi^{-1}(T_\xi(\langle X \rangle)) = \langle X \rangle$ *if and only if* $Z_{\hat{\mathcal{G}}}(\xi') \to Z_{\hat{\mathcal{G}}}(\xi_0)$ *is surjective, where* $Z_{\hat{\mathcal{G}}}(\xi')$, *as in Definition 2.5, is the centralizer of* ξ' *in* $\hat{\mathcal{G}}(A_1)$.

Proof. Suppose $[\xi'] \in F_{\mathcal{G}}(\alpha)^{-1}([\xi_0])$. Then there exists $g_0 \in \hat{\mathcal{G}}(A_0)$ such that $\xi_0 = \alpha\xi = g_0 \alpha\xi' g_0^{-1}$. Since $\mathcal{G}$ is smooth over W, g_0 lifts to an element $g \in \hat{\mathcal{G}}(A_1)$ with $\alpha g = g_0$. For $\xi'' = g\xi' g^{-1}$ we have $[\xi''] = [\xi']$ and $\alpha\xi'' = \xi_0 = \alpha\xi$. It follows that $\xi'' = X(\xi)$ for a unique cocycle $X \in Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$. Hence T_ξ is surjective.

Suppose now that $X \in Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$, $\xi' = X(\xi)$, and that $Z_{\hat{\mathcal{G}}}(\xi') \to Z_{\hat{\mathcal{G}}}(\xi_0)$ is surjective. Let X_1 be an element of $Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$ such that $T_\xi(\langle X \rangle) = T_\xi(\langle X_1 \rangle)$. We have to show that $\langle X \rangle = \langle X_1 \rangle$ in $H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$. Let $\xi_1 = X_1(\xi)$. Since $T_\xi(\langle X \rangle) = T_\xi(\langle X_1 \rangle)$, one has

$$\xi' = g\ \xi_1\ g^{-1} \tag{4.6}$$

for some $g \in \hat{\mathcal{G}}(A_1)$. From $\alpha\xi' = \xi_0 = \alpha\xi_1$ we see that $g_0 = \alpha g$ lies in $Z_{\hat{\mathcal{G}}}(\xi_0)$. By assumption, there is an element $g_1 \in Z_{\hat{\mathcal{G}}}(\xi')$ such that $\alpha g_1 = g_0$. Replacing g by $g_1^{-1}g$, we can assume that αg is the identity element of $\hat{\mathcal{G}}(A_0)$. Hence $g = \exp(z)$ for some $z \in \mathrm{Lie}(\mathcal{G}_k) \otimes I$. Define

$$L(\gamma) = g\ \xi_1(\gamma)\ g^{-1}\ \xi_1(\gamma)^{-1} = \exp(z - z^\gamma)$$

for $\gamma \in \Gamma$. Now (4.6) shows for $\gamma \in \Gamma$ that

$$\exp(X(\gamma))\,\xi(\gamma) = g\ \xi_1(\gamma)\ g^{-1} = L(\gamma)\ \xi_1(\gamma) = \exp(z - z^\gamma + X_1(\gamma))\,\xi(\gamma)\ .$$

This shows that $\gamma \mapsto \exp(X_1 - X)$ is the map $\gamma \mapsto \exp(z^\gamma - z)$. Hence the injectivity of exp proves that $X_1 - X$ is the element $\gamma \mapsto z^\gamma - z$ of $B^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$, so $\langle X\rangle = \langle X_1\rangle$ in $H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$ as claimed.

Conversely, suppose $X \in Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$, $T_\xi^{-1}(T_\xi(\langle X\rangle)) = \langle X\rangle$ and $\xi' = X(\xi)$. Suppose $g_0 \in Z_{\hat{\mathcal{G}}}(\xi_0)$. We need to show there exists an element $g_1 \in Z_{\hat{\mathcal{G}}}(\xi')$ with $\alpha g_1 = g_0$. Since $\mathcal{G}$ is smooth over W, there is a $g \in \hat{\mathcal{G}}(A_1)$ with $\alpha g = g_0$. Consider $\xi_1 = g\xi' g^{-1}$. Then $[\xi_1] = [\xi']$ in $F_{\mathcal{G}}(\alpha)^{-1}([\xi_0])$. Since $T_\xi^{-1}(T_\xi(\langle X\rangle)) = \langle X\rangle$, we have $\xi_1 = X_1(\xi)$ for some $X_1 \in Z^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$ such that $\langle X\rangle = \langle X_1\rangle$ in $H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$. Thus there is a $z \in \mathrm{Lie}(\mathcal{G}_k) \otimes I$ such that $X_1(\gamma) - X(\gamma) = z^\gamma - z$ for $\gamma \in \Gamma$. Define $h = \exp(z)$. Then for $\gamma \in \Gamma$ we have

$$\begin{aligned} g\,\xi'(\gamma)\,g^{-1} &= \xi_1(\gamma) = \exp(X_1(\gamma))\,\xi(\gamma) \\ &= \exp(z^\gamma - z + X(\gamma))\,\xi(\gamma) = h^{-1}\exp(z^\gamma)\,\xi'(\gamma) \\ &= h^{-1}\,\xi'(\gamma)\,h, \end{aligned}$$

where the last equality follows as in (4.4). This shows that $g_1 = hg \in Z_{\hat{\mathcal{G}}}(\xi')$, and since αh is the identity element of $\hat{\mathcal{G}}(A_0)$ we have $\alpha g_1 = \alpha g = g_0$. This completes the proof of Lemma 4.2. □

Corollary 4.3. *Suppose $F_{\mathcal{G}}(\alpha)^{-1}([\xi_0])$ is non-empty. Then $F_{\mathcal{G}}(\alpha)^{-1}([\xi_0])$ is a principal homogeneous set for $H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes I)$ if and only if $Z_{\hat{\mathcal{G}}}(\xi') \to Z_{\hat{\mathcal{G}}}(\xi_0)$ is surjective for all $\xi' \in \alpha^{-1}\xi_0 \subset E_{\mathcal{G}}(A_1)$.*

Remark 4.4. If $g \in \hat{\mathcal{G}}(A_1)$ and $\xi' = g\xi g^{-1}$, then $T_\xi(\langle X\rangle) = T_{\xi'}(\langle X\rangle^g)$, where $\langle X\rangle^g = \langle X^g\rangle$ when X^g is the one-cocycle defined by $\exp(X^g(\gamma)) = g\exp(X(\gamma))\,g^{-1}$ for all $\gamma \in \Gamma$. This follows from the equality $X^g(\xi')(\gamma) = g\ X(\xi)(\gamma)\ g^{-1}$ for $\gamma \in \Gamma$.

Proof of Theorem 4.1. By definition, $\overline{\iota}_{\mathcal{G},\mathcal{H},k[\epsilon]}$ is injective if $\hat{F}_{\mathcal{G}}$ is a subfunctor of $\hat{F}_{\mathcal{H}}$. So we will suppose for the rest of the proof that $\overline{\iota}_{\mathcal{G},\mathcal{H},k[\epsilon]}$ is injective, with the objective of proving that $\hat{F}_{\mathcal{G}}$ is a subfunctor of $\hat{F}_{\mathcal{H}}$ and that it is representable.

Suppose we have a short exact sequence

$$0 \to tA_1 \longrightarrow A_1 \xrightarrow{\alpha} A_0 \to 0 \tag{4.7}$$

where $A_0, A_1 \in \mathrm{Ob}(\mathcal{C})$, $t \cdot m_{A_1} = 0$ and $tA_1 \cong k$ as k-vector spaces. Let $ta \in tA_1$ be the element sent to $1 \in k$ under this isomorphism. Then every element in $\mathrm{Lie}(\mathcal{G}_k) \otimes tA_1$ has the form $z \otimes ta$ for a unique $z \in \mathrm{Lie}(\mathcal{G}_k)$. We get an isomorphism of abelian groups

$$\begin{array}{rccc} \alpha_{\mathcal{G}}: & H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k)) & \to & H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes tA_1) \\ & \langle c \rangle & \mapsto & \langle X \rangle \end{array} \tag{4.8}$$

where $X(\gamma) = c(\gamma) \otimes ta$ for all $\gamma \in \Gamma$. We also have the following commutative diagram

$$\begin{array}{ccc} F_{\mathcal{G}}(k[\epsilon]) & \xrightarrow{\bar{\iota}_{\mathcal{G},\mathcal{H},k[\epsilon]}} & F_{\mathcal{H}}(k[\epsilon]) \\ \downarrow \tau_{\mathcal{G}} & & \downarrow \tau_{\mathcal{H}} \\ H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k)) & \xrightarrow{\lambda} & H^1(\Gamma, \mathrm{Lie}(\mathcal{H}_k)) \end{array} \tag{4.9}$$

where $\tau_{\mathcal{G}}$ and $\tau_{\mathcal{H}}$ are the isomorphisms from (3.3), $\bar{\iota}_{\mathcal{G},\mathcal{H},k[\epsilon]}([\pi]) = [\pi]$, and hence $\lambda(\langle c \rangle) = \langle c \rangle$. Since by assumption $\bar{\iota}_{\mathcal{G},\mathcal{H},k[\epsilon]}$ is injective, λ is also injective.

Since both functors $\hat{F}_{\mathcal{G}}$ and $\hat{F}_{\mathcal{H}}$ are continuous, to prove Theorem 4.1 it is enough to prove that $\bar{\iota}_{\mathcal{G},\mathcal{H},R}$ from (4.1) is injective for $R \in \mathrm{Ob}(\mathcal{C})$. By induction, we can assume that $\bar{\iota}_{\mathcal{G},\mathcal{H},A_0}$ is injective for A_0 as in (4.7), and we have to prove that $\bar{\iota}_{\mathcal{G},\mathcal{H},A_1}$ is injective. To show this, we can assume $E_{\mathcal{G}}(A_1)$ is non-empty. Let ξ be an element of $E_{\mathcal{G}}(A_1)$. Define $\xi_0 = \alpha\xi$, $\xi' = \iota_{\mathcal{G},\mathcal{H},A_1}(\xi) \in E_{\mathcal{H}}(A_1)$, and $\xi_0' = \alpha\xi' = \iota_{\mathcal{G},\mathcal{H},A_0}(\xi_0)$. From Lemma 4.2 we have a commutative diagram

$$\begin{array}{ccc} H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k) \otimes tA_1) & \xrightarrow{\phi} & H^1(\Gamma, \mathrm{Lie}(\mathcal{H}_k) \otimes tA_1) \\ \downarrow T_{\xi} & & \downarrow T_{\xi'} \\ F_{\mathcal{G}}(\alpha)^{-1}([\xi_0]) & \xrightarrow{\bar{\iota}_{\mathcal{G},\mathcal{H},A_1}} & F_{\mathcal{H}}(\alpha)^{-1}([\xi_0']) \end{array} \tag{4.10}$$

in which the vertical homomorphisms are surjective, and $\phi = \alpha_{\mathcal{H}}\, \lambda\, \alpha_{\mathcal{G}}^{-1}$, where λ is the homomorphism defined in (4.9) and $\alpha_{\mathcal{G}}$ and $\alpha_{\mathcal{H}}$ are the isomorphisms from (4.8). Since we have shown that λ is injective, so is ϕ. On the other hand, since we have assumed $\hat{F}_{\mathcal{H}}$ is representable, Proposition 3.1 shows $F_{\mathcal{H}}$ has the centralizer lifting property. Therefore, Corollary 4.3 implies that $T_{\xi'}$ in (4.10) is bijective. Hence T_{ξ} must be bijective as well, since it is surjective and ϕ is injective. The commutativity of (4.10) now forces the morphism $\bar{\iota}_{\mathcal{G},\mathcal{H},A_1}$ to be injective. By our previous remarks, this shows $\hat{F}_{\mathcal{G}}$ is a subfunctor of $\hat{F}_{\mathcal{H}}$. Since T_{ξ} is bijective, Corollary 4.3 shows that $F_{\mathcal{G}}$ has the centralizer lifting property. Hence by Theorem 2.7, $\hat{F}_{\mathcal{G}}$ is representable. This completes the proof of Theorem 4.1. $\square$

LEMMA 4.5. *Consider the short exact sequence of Lie algebras*

$$0 \to \mathrm{Lie}(\mathcal{G}_k) \longrightarrow \mathrm{Lie}(\mathcal{H}_k) \xrightarrow{\pi} \mathfrak{c} \to 0, \tag{4.11}$$

where $\gamma \in \Gamma$ *acts on these Lie algebras through the adjoint action* $\mathrm{ad}(\rho)$ *as described in Remark 3.4. Then the following are equivalent:*

(i) *The natural map* $t_{F_\mathcal{G}} \to t_{F_\mathcal{H}}$ *is injective.*
(ii) *The map* $\mathrm{Lie}(\mathcal{H}_k)^\Gamma \xrightarrow{\pi} \mathfrak{c}^\Gamma$ *is surjective.*
(iii) *The sequence* $0 \to \mathrm{Lie}(\mathcal{G}_k) \longrightarrow \pi^{-1}(\mathfrak{c}^\Gamma) \xrightarrow{\pi} \mathfrak{c}^\Gamma \to 0$ *splits as a sequence of* $k\Gamma$*-modules.*

Proof. The equivalence of (i) and (ii) follows from the long exact group cohomology sequence associated to (4.11):

$$0 \longrightarrow [\mathrm{Lie}(\mathcal{G}_k)]^\Gamma \longrightarrow [\mathrm{Lie}(\mathcal{H}_k)]^\Gamma \xrightarrow{\pi} \mathfrak{c}^\Gamma \longrightarrow H^1(\Gamma, \mathrm{Lie}(\mathcal{G}_k)) \xrightarrow{\iota_{\mathcal{G},\mathcal{H},k[\epsilon]}} H^1(\Gamma, \mathrm{Lie}(\mathcal{H}_k)) \longrightarrow \cdots .$$

Assume now (ii). Then there exists a section $s : \mathfrak{c}^\Gamma \to [\mathrm{Lie}(\mathcal{H}_k)]^\Gamma$ of k-vector spaces with $\pi\, s = \mathrm{id}$. Since Γ acts trivially on both the domain and the codomain of s, s is a section of $k\Gamma$-modules. Thus we can use s to define a splitting of the sequence of $k\Gamma$-modules given in part (iii). Conversely, if (iii) holds, let $s : \mathfrak{c}^\Gamma \to \pi^{-1}(\mathfrak{c}^\Gamma)$ be a splitting of the sequence in part (iii) which is a $k\Gamma$-module homomorphism. Then for every $x \in \mathfrak{c}^\Gamma$, $s(x)$ is in $[\pi^{-1}(\mathfrak{c}^\Gamma)]^\Gamma = [\mathrm{Lie}(\mathcal{H}_k)]^\Gamma$. Since $\pi(s(x)) = x$, the map $[\mathrm{Lie}(\mathcal{H}_k)]^\Gamma \xrightarrow{\pi} \mathfrak{c}^\Gamma$ in part (ii) is surjective. □

COROLLARY 4.6. *If the sequence* (4.11) *splits as a sequence of* $k\Gamma$*-modules, then* $t_{F_\mathcal{G}}$ *is a subspace of* $t_{F_\mathcal{H}}$.

Proof. Suppose $s : \mathfrak{c} \to \mathrm{Lie}(\mathcal{H}_k)$ is a splitting of (4.11) which is a $k\Gamma$-module homomorphism. Then for every $x \in \mathfrak{c}^\Gamma$, $s(x)$ is in $[\mathrm{Lie}(\mathcal{H}_k)]^\Gamma$. Since $\pi(s(x)) = x$, this implies part (ii), and hence part (i), of Lemma 4.5. □

We now use the criteria in Theorem 4.1, Lemma 4.5, and Corollary 4.6 to study some classical cases when $\mathcal{H} = \mathrm{GL}_n$. In the following, $\mathfrak{gl}_{n,k}$ denotes the Lie algebra of GL_n over k.

4.1. Special linear groups and symplectic groups.

LEMMA 4.7. *Suppose* $\rho : \Gamma \to \mathrm{SL}_n(k)$ *is a continuous representation of* Γ *into the special linear group* $\mathrm{SL}_n(k)$ *such that* $\hat{F}_{\mathrm{GL}_n,\rho}$ *is representable. If* p *does not divide* n*, then* $\hat{F}_{\mathrm{SL}_n,\rho}$ *is a subfunctor of* $\hat{F}_{\mathrm{GL}_n,\rho}$*. If the only elements in* $\mathrm{GL}_n(k)$ *centralizing the image of* ρ *are scalars, then* $\hat{F}_{\mathrm{SL}_n,\rho}$ *is a subfunctor of* $\hat{F}_{\mathrm{GL}_n,\rho}$ *if and only if* p *does not divide* n.

Proof. For $\mathcal{G} = \mathrm{SL}_n$,

$$\mathrm{Lie}(\mathcal{G}_k) = \{M \in \mathrm{Mat}_n(k) \mid \mathrm{Trace}(M) = 0\} .$$

Thus π in the sequence (4.11) is given by the trace, and $\mathfrak{c} = k$ with trivial Γ-action. Hence $\mathfrak{c}^\Gamma = \mathfrak{c}$. If p does not divide n, then $\pi([\mathfrak{gl}_{n,k}]^\Gamma) = \mathfrak{c}^\Gamma$. If p divides n and the only elements in $\mathrm{GL}_n(k)$ centralizing the image of ρ are scalars, then $\pi([\mathfrak{gl}_{n,k}]^\Gamma) = 0$. Hence the statement follows by Theorem 4.1 and Lemma 4.5. □

LEMMA 4.8. *Suppose p is odd, and $\rho : \Gamma \to \mathrm{Sp}_{2m}(k)$ is a continuous representation of Γ into the symplectic group $\mathrm{Sp}_{2m}(k)$ such that $\hat{F}_{\mathrm{GL}_{2m},\rho}$ is representable. Then $\hat{F}_{\mathrm{Sp}_{2m},\rho}$ is a subfunctor of $\hat{F}_{\mathrm{GL}_{2m},\rho}$.*

Proof. Any $2m$-dimensional perfect skew-symmetric form over W can be represented, with respect to a suitable basis, by the $2m \times 2m$ matrix

$$S = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} . \tag{4.12}$$

We define the symplectic algebraic group Sp_{2m} of rank m over W by

$$\mathrm{Sp}_{2m}(B) = \{A \in \mathrm{GL}_{2m}(B) \mid A^T S A = S\}$$

for all W-algebras B, where A^T denotes the transpose of the matrix A. Then Sp_{2m} is smooth over W for all odd p. For $\mathcal{G} = \mathrm{Sp}_{2m}$,

$$\begin{aligned} \mathrm{Lie}(\mathcal{G}_k) &= \{M \in \mathrm{Mat}_{2m}(k) \mid M^T S = -SM\} \\ &= \left\{ \begin{pmatrix} X & Y \\ Z & L \end{pmatrix} \mid X = -L^T, Y = Y^T, Z = Z^T \right\}, \end{aligned}$$

where $X, Y, Z, L \in \mathrm{Mat}_m(k)$. Then π in the sequence (4.11) is given by

$$\pi\left(\begin{pmatrix} X & Y \\ Z & L \end{pmatrix} \right) = \begin{pmatrix} X + L^T & Y - Y^T \\ Z - Z^T & L + X^T \end{pmatrix}$$

for each $2m \times 2m$ matrix $\begin{pmatrix} X & Y \\ Z & L \end{pmatrix} \in \mathfrak{gl}_{2m,k}$, and

$$\mathfrak{c} = \{M \in \mathrm{Mat}_{2m}(k) \mid M^T S = SM\} .$$

It follows that $\mathfrak{c}$ is a k-subspace of $\mathfrak{gl}_{2m,k}$, which is stable under conjugation by elements in $\mathrm{Sp}_{2m}(k)$. Thus $\mathfrak{c}$ is a $k\Gamma$-submodule of $\mathfrak{gl}_{2m,k}$. Moreover, since $\mathrm{Lie}(\mathcal{G}_k) \cap \mathfrak{c} = \{0\}$, the sequence (4.11) splits as a sequence of $k\Gamma$-modules, and thus Lemma 4.8 follows from Corollary 4.6. □

4.2. Orthogonal groups.

LEMMA 4.9. *Suppose p is odd, and let $O(q)$ be the orthogonal group over W corresponding to an n-dimensional perfect symmetric quadratic form q over W. Let $\rho:\Gamma\to O(q)(k)$ be a continuous representation of Γ into $O(q)(k)$ such that $\hat{F}_{\mathrm{GL}_n,\rho}$ is representable. Then $\hat{F}_{O(q),\rho}$ is a subfunctor of $\hat{F}_{\mathrm{GL}_n,\rho}$.*

Proof. Any n-dimensional perfect symmetric quadratic form q over W is equivalent to a diagonal quadratic form given by a matrix

$$Q_\eta = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \eta \end{pmatrix}\,, \tag{4.13}$$

where η is a unit in W. (In fact, every such Q_η is equivalent either to Q_1 or to Q_ω for a fixed non-square ω in W.) We define the corresponding orthogonal algebraic group $O_{n,\eta}$ over W by

$$O_{n,\eta}(B) = \{A\in \mathrm{GL}_n(B)\bigm| A^TQ_\eta A = Q_\eta\}$$

for all W-algebras B. Then $O_{n,\eta}$, and therefore $O(q)$, is smooth over W for all odd p. For $\mathcal{G}=O_{n,\eta}$,

$$\begin{aligned}\mathrm{Lie}(\mathcal{G}_k) &= \{M\in \mathrm{Mat}_n(k)\bigm| M^TQ_\eta = -Q_\eta M\}\\ &= \left\{\begin{pmatrix} X & y\\ z & 0\end{pmatrix}\bigm| X=-X^T, y^T=-\eta z\right\},\end{aligned}$$

where $X\in\mathrm{Mat}_{n-1}(k)$, and y and z^T are column vectors of length $n-1$. Then π in the sequence (4.11) is given by

$$\pi\left(\begin{pmatrix} X & y\\ z & w\end{pmatrix}\right) = \begin{pmatrix} X+X^T & y+\eta z^T\\ z+\eta^{-1}y^T & 2w\end{pmatrix}$$

for each $n\times n$-matrix $\begin{pmatrix} X & y\\ z & w\end{pmatrix}\in\mathfrak{gl}_{n,k}$, and

$$\mathfrak{c} = \{M\in\mathrm{Mat}_n(k)\bigm| M^TQ_\eta = Q_\eta M\}\,.$$

It follows that $\mathfrak{c}$ is a k-subspace of $\mathfrak{gl}_{n,k}$, which is stable under conjugation by elements in $O_{n,\eta}(k)$. Thus $\mathfrak{c}$ is a $k\Gamma$-submodule of $\mathfrak{gl}_{n,k}$. Moreover, since $\mathrm{Lie}(\mathcal{G}_k)\cap\mathfrak{c}=\{0\}$, the sequence (4.11) splits as a sequence of $k\Gamma$-modules, and thus Lemma 4.9 follows from Corollary 4.6. $\square$

5. Orthogonal deformation functors

HYPOTHESIS 5.1. Suppose k is a finite field of odd characteristic p. We denote the n-dimensional symmetric bilinear pairing over W corresponding to the matrix Q_η, $\eta\in W^*$, in equation (4.13) by $\langle -,-\rangle_\eta$. We assume that V is a continuous n-dimensional representation of Γ over k such that there exists a symmetric perfect Γ-invariant bilinear pairing

$$\langle -,-\rangle_V\,:\,V\times V\to k\,.$$

Thus there is a unit $\eta_V \in W^*$ such that if the Γ-action on V is ignored, V is isometric to the vector space k^n with the pairing $\langle -,-\rangle_{\eta_V}$ over k. Hence there is an orthogonal basis $\{v_i\}_{i=1}^n$ of V over k such that the action of Γ on V is given by a continuous homomorphism

$$\rho = \rho_V \,:\, \Gamma \to O_{n,\eta_V}(k)\ .$$

Definition 5.2. Suppose $(V, \langle -,-\rangle_V)$ is isometric to $(k^n, \langle -,-\rangle_{\eta_V})$, where $\eta_V \in W^*$. An *orthogonal lift* of $(V, \langle -,-\rangle_V)$ over $R \in \mathrm{Ob}(\hat{\mathcal{C}})$ is a triple $(M, \langle -,-\rangle_M, \phi)$, where M is a free R-module of rank n with a continuous Γ-action and

$$\langle -,-\rangle_M \,:\, M \times M \to R$$

is a symmetric perfect Γ-invariant bilinear pairing. The morphism $\phi : k \otimes_R M \to V$ is a fixed isomorphism of representations of Γ over k which, on ignoring the Γ-action, induces an isometry between the pairings $k \otimes_R \langle -,-\rangle_M$ and $\langle -,-\rangle_V$. We require that, on ignoring the Γ-action, there is an isometry between $(M, \langle -,-\rangle_M)$ and $(R^n, \langle -,-\rangle_{\eta_V})$ whose reduction mod m_R is an isometry between $(V, \langle -,-\rangle_V)$ and $(k^n, \langle -,-\rangle_{\eta_V})$ when we identify V with $k \otimes_R M$ via ϕ. In particular, there is an orthogonal basis $\{m_i\}_{i=1}^n$ of M as a free R-module such that $\langle m_i, m_i\rangle_M = 1$ for $i = 1, \ldots, n-1$, and $\langle m_n, m_n\rangle_M = \eta_V$. We call such a basis an η_V-orthogonal basis of M.

Two orthogonal lifts $(M, \langle -,-\rangle_M, \phi)$ and $(M', \langle -,-\rangle_{M'}, \phi')$ are *isomorphic* if there is an isomorphism $M \to M'$ of continuous representations of Γ over R which carries ϕ to ϕ', and, on ignoring the Γ-action, $\langle -,-\rangle_M$ to $\langle -,-\rangle_{M'}$. An *orthogonal deformation* of V over R is an isomorphism class of orthogonal lifts of V.

Definition 5.3. Let $\hat{F}^{\mathrm{ort}} = \hat{F}_V^{\mathrm{ort}} : \hat{\mathcal{C}} \to \mathrm{Sets}$ be the functor which sends each object R of $\hat{\mathcal{C}}$ to the set $\hat{F}^{\mathrm{ort}}(R)$ of all orthogonal deformations of V over R. Let $F^{\mathrm{ort}} = F_V^{\mathrm{ort}}$ be the restriction of $\hat{F}^{\mathrm{ort}}$ to $\mathcal{C}$. We call $\hat{F}^{\mathrm{ort}}$ the *orthogonal deformation functor*.

Theorem 5.4. *The two functors* $\hat{F}_V^{\mathrm{ort}}$ *and* $\hat{F}_{O_{n,\eta_V},\rho}$ *from Definition 2.2 are naturally isomorphic.*

Proof. It is enough to prove that the orbit space $E_{O_{n,\eta_V}}(R)/\hat{O}_{n,\eta_V}(R)$ can be identified with the set of orthogonal deformations of $(V, \langle -,-\rangle_V)$ over R for all $R \in \mathrm{Ob}(\hat{\mathcal{C}})$.

Let $\{v_i\}_{i=1}^n$ be an η_V-orthogonal basis of V over k relative to ρ. Suppose $(M, \langle -,-\rangle_M, \phi)$ is an orthogonal lift of $(V, \langle -,-\rangle_V)$ over R. By definition, there is an η_V-orthogonal basis for M as a free R-module. Since ϕ induces an isometry and O_{n,η_V} is smooth over W, we can find an η_V-orthogonal basis $\{m_i\}_{i=1}^n$ of M over R such that $\phi(1 \otimes m_i) = v_i$ for all i. With respect to this basis, the action of Γ on M is given by a continuous homomorphism

$$\pi : \Gamma \to O_{n,\eta_V}(R)$$

such that $\kappa_{O_{n,\eta_V},R}\,\pi = \rho$. Hence $\pi \in E_{O_{n,\eta_V}}(R)$. If $(M', \langle -,- \rangle_{M'}, \phi')$ is an isomorphic orthogonal lift of $(V, \langle -,- \rangle_V)$ over R, then the associated $\pi' : \Gamma \to O_{n,\eta_V}(R)$ must be in the orbit of π under the action of $\hat{O}_{n,\eta_V}(R)$ by definition of isomorphic orthogonal lifts.

Conversely, every $\pi \in E_{O_{n,\eta_V}}(R)$ defines a representation M of Γ over R. Since $\kappa_{O_{n,\eta_V},R}\,\pi = \rho$, it follows that M can be extended to an orthogonal lift of $(V, \langle -,- \rangle_V)$ over R. If $\pi' \in E_{O_{n,\eta_V}}(R)$ lies in the same $\hat{O}_{n,\eta_V}(R)$-orbit as π, then it is obvious that the associated orthogonal lift M' is isomorphic to M. □

6. Versal Stiefel-Whitney classes and Hasse-Witt invariants

In this section we continue to use the notations and assumptions of Section 5. Thus V is a continuous n-dimensional orthogonal representation of Γ over a finite field k of odd characteristic p. We will also assume that Γ satisfies Mazur's finiteness condition (Φ_p). Let $\mathcal{G} = O_{n,\eta_V}$; in particular, $\mathcal{G}$ is smooth over the Witt vectors W. By Theorems 2.7 and 5.4, there is a versal orthogonal deformation ring $R_{\mathcal{G}}(\Gamma,\rho)$ and a versal orthogonal deformation $U_{\mathcal{G}}(\Gamma,\rho)$, which are unique up to a non-canonical isomorphism. Our goal is to attach to $U_{\mathcal{G}}(\Gamma,\rho)$ Stiefel-Whitney classes and Hasse-Witt invariants, and to consider generalizations to this context of results comparing such invariants due to Serre [15], Fröhlich [7], Esnault, Kahn and Vieweg [5], Saito [12], [13], and Cassou-Noguès, Erez and Taylor [2].

Let $R = R_{\mathcal{G}}(\Gamma,\rho)$. Then the module $U = U_{\mathcal{G}}(\Gamma,\rho)$ is free of rank n over R, and has a continuous action of Γ. There is a perfect symmetric Γ-invariant bilinear pairing on U,

$$\langle -,- \rangle_U \,:\, U \times U \to R\,.$$

Define $Y = \mathrm{Spec}(R)$. Define $\mathbf{O}(U)$ to be the sheaf of groups on the étale topology of Y associated to the orthogonal group $O(U) = R \otimes_W O_{n,\eta_V} = R \otimes_W \mathcal{G}$. Because $p > 2$, there is a central extension

$$1 \longrightarrow \mu_2 \longrightarrow \tilde{\mathbf{O}}(U) \xrightarrow{\pi} \mathbf{O}(U) \to 1 \tag{6.1}$$

of étale sheaves defined in the following way (see [12, §0] or [5, §1.9]). Define $\mathbf{Cl}(U)$ to be the sheaf on the étale topology of Y which is associated to the Clifford algebra of U. Let I be the involutory automorphism of $\mathbf{Cl}(U)$ induced by -1 on U. Define t to be the involutory anti-automorphism of $\mathbf{Cl}(U)$ induced by the identity on U, and let $N : \mathbf{Cl}(U) \to \mathbb{G}_a$ be the norm defined by $N(x) = t(x)\cdot x$. Define a subsheaf $\mathbf{C}(U)^\times$ of $\mathbf{Cl}(U)^\times$ by $\mathbf{C}(U)^\times = \{x \in \mathbf{Cl}(U)^\times : x \text{ is homogeneous and } I(x)Ux^{-1} = U\}$. Define $\tilde{\mathbf{O}}(U) = \mathrm{Ker}(N :$

$\mathbf{C}(U)^\times \to \mathbb{G}_m$). The central extension (6.1) results on defining $\pi : \tilde{\mathbf{O}}(U) \to \mathbf{O}(U)$ by $\pi(x) = (u \to I(x)ux^{-1})$.

The boundary map $\delta : H^0(Y, \mathbf{O}(U)) \to H^1(Y, \mu_2)$ in étale cohomology associated to (6.1) is the spinor norm

$$\mathrm{sp} : O(U) \to H^1(Y, \mu_2). \tag{6.2}$$

See [12, §0] for a discussion of properties of the spinor norm.

Define the first Stiefel-Whitney class $\mathrm{sw}_1(U) \in H^1(\Gamma, \mu_2(R))$ by

$$\mathrm{sw}_1(U) = \det(U) \in \mathrm{Hom}(\Gamma, \mu_2(R)) = H^1(\Gamma, \mu_2(R)). \tag{6.3}$$

We associate a second Stiefel-Whitney class to each geometric point $\overline{y}$ of Y in the following way. Because (6.1) is an exact sequence in the étale topology on Y, it gives an exact sequence of groups

$$1 \longrightarrow \mu_2(\kappa(\overline{y})) \longrightarrow \tilde{O}(U)(\kappa(\overline{y})) \xrightarrow{\pi} O(U)(\kappa(\overline{y})) \to 1\ , \tag{6.4}$$

which is the same as

$$1 \longrightarrow \mu_2(\kappa(\overline{y})) \longrightarrow \tilde{O}_{n,\eta_V}(\kappa(\overline{y})) \xrightarrow{\pi} O_{n,\eta_V}(\kappa(\overline{y})) \to 1\ .$$

Pulling back the orthogonal representation U over $R = R_{\mathcal{G}}(\Gamma, \rho)$ via the homomorphism $R \to \kappa(\overline{y})$ gives a representation $\rho_{U,y} : \Gamma \to O_{n,\eta_V}(\kappa(\overline{y}))$ which is well-defined up to isomorphism. Viewing $\rho_{U,y}$ as an element of $H^1(\Gamma, O_{n,\eta_V}(\kappa(\overline{y})))$, we let

$$\mathrm{sw}_2(U, \overline{y}) \in H^2(\Gamma, \mu_2(\kappa(\overline{y}))) = H^2(\Gamma, \{\pm 1\}) \tag{6.5}$$

be the image of $\rho_{U,y}$ under the boundary map in cohomology associated to the sequence (6.4). In a similar way, we can define a second Stiefel-Whitney class $\mathrm{sw}_2(V) \in H^2(\Gamma, \mu_2(\overline{k})) = H^2(\Gamma, \{\pm 1\})$ associated to the original orthogonal representation V over k.

Theorem 6.1. *For all geometric points $\overline{y}$ there is an equality* $\mathrm{sw}_2(U, \overline{y}) = \mathrm{sw}_2(V)$ *in* $H^2(\Gamma, \{\pm 1\})$.

Proof. Let k^s be a fixed separable closure of k. Define R^{sh} to be the strict henselization of the local ring $R = R_{\mathcal{G}}(\Gamma, \rho)$. Thus R^{sh} is the direct limit $\varinjlim A$ over all commutative diagrams

$$\begin{tikzcd} A \arrow[rr, "\gamma"] & & k^s \\ & R \arrow[ul, "\alpha"] \arrow[ur, "\beta"'] & \end{tikzcd} \tag{6.6}$$

of essentially étale R-algebras A in which α is the local homomorphism defining the R-algebra structure of A, γ is a local R-algebra homomorphism, and β is the composition of the residue map $R \to k = R/m_R$ with the inclusion of k into a k^s. For more details, see [8, Chapter IV, §18.8.6].

The geometric point $\overline{y} \to Y$ has as image a point $y \in \mathrm{Spec}(R)$. We now construct an R-algebra homomorphism

$$R^{\mathrm{sh}} \to (R_y)^{\mathrm{sh}} \tag{6.7}$$

where R_y is the localization of R at y.

Since R^{sh} is faithfully flat over R by [8, Prop. IV.18.8.8(iii)], the morphism $\mathrm{Spec}(R^{\mathrm{sh}}) \to \mathrm{Spec}(R)$ is surjective. Hence we can find a prime ideal y' of R^{sh} over y, and the residue field $\kappa(y')$ is a separable algebraic extension of $\kappa(y)$. Fix an embedding of $\kappa(y')$ into a separable closure $\kappa(y)^s$ of $\kappa(y)$. For each diagram (6.6), let a be the ideal $y' \cap A$ of A. This induces an embedding of $\kappa(a)$ into $\kappa(y)^s$. The resulting diagram

$$\begin{array}{ccc} A_a & \xrightarrow{\gamma_a} & \kappa(y)^s \\ {\scriptstyle\alpha_a}\nwarrow & & \nearrow{\scriptstyle\beta_a} \\ & R_y & \end{array} \tag{6.8}$$

occurs in the direct limit defining $(R_y)^{\mathrm{sh}}$. A morphism between two diagrams of the kind in (6.6) gives rise to a unique morphism between the corresponding diagrams of the kind in (6.8). Hence by the definition of direct limits, there is an R_y-algebra homomorphism $\nu : \varinjlim A_a \to (R_y)^{\mathrm{sh}}$, where the direct limit on the left is over all diagrams (6.8) arising from diagrams (6.6) appearing in the definition of R^{sh}. We thus have a natural R-algebra homomorphism $R^{\mathrm{sh}} = \varinjlim A \to \varinjlim A_a$, and the composition of this with ν gives the required R-algebra homomorphism (6.7).

Since (6.1) is an exact sequence of sheaves in the étale topology, it gives an exact sequence of stalks at the geometric points $\mathrm{Spec}(\overline{k})$ and $\mathrm{Spec}(\kappa(\overline{y}))$. This gives the middle two exact rows in the following diagram:

(6.9)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2(\overline{k}) & \longrightarrow & \tilde{O}_{n,\eta_V}(\overline{k}) & \longrightarrow & O_{n,\eta_V}(\overline{k}) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mu_2(R^{\mathrm{sh}}) & \longrightarrow & \tilde{O}_{n,\eta_V}(R^{\mathrm{sh}}) & \longrightarrow & O_{n,\eta_V}(R^{\mathrm{sh}}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mu_2((R_y)^{\mathrm{sh}}) & \longrightarrow & \tilde{O}_{n,\eta_V}((R_y)^{\mathrm{sh}}) & \longrightarrow & O_{n,\eta_V}((R_y)^{\mathrm{sh}}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mu_2(\kappa(\overline{y})) & \longrightarrow & \tilde{O}_{n,\eta_V}(\kappa(\overline{y})) & \longrightarrow & O_{n,\eta_V}(\kappa(\overline{y})) & \longrightarrow & 1 \end{array}$$

The maps from the second to the third rows result from (6.7). The maps from the second to the first row, and from the third to the fourth row, result from the fact that R^{sh} (resp. $(R_y)^{\mathrm{sh}}$) has residue field $k^s \subset \overline{k}$ (resp. $\kappa(y)^s \subset \kappa(\overline{y})$). Finally, the vertical homomorphisms in the left column are all isomorphisms, since the residue characteristic p is odd and $\mu_2(\overline{k}) = \mu_2(R^{\mathrm{sh}}) = \mu_2((R_y)^{\mathrm{sh}}) = \mu_2(\kappa(\overline{y})) = \{\pm 1\}$.

The versal orthogonal deformation U gives a homomorphism $\gamma : \Gamma \to O(U)(R) = O_{n,\eta_V}(R)$, and the composition of γ with the map $O_{n,\eta_V}(R) \to$

$O_{n,\eta_V}(R^{\mathrm{sh}})$ is a group homomorphism $\gamma^s : \Gamma \to O_{n,\eta_V}(R^{\mathrm{sh}})$. Consider the obstruction to lifting γ^s to the middle group $\tilde{O}_{n,\eta_V}(R^{\mathrm{sh}})$ in the second row of (6.9). By choosing a set-theoretic lift of $\tilde{O}_{n,\eta_V}(R^{\mathrm{sh}}) \to O_{n,\eta_V}(R^{\mathrm{sh}})$, one can in the usual way define a two-cocycle $z : \Gamma \times \Gamma \to \mu_2(R^{\mathrm{sh}}) = \{\pm 1\}$ whose class in $H^2(\Gamma, \{\pm 1\})$ is the obstruction to lifting γ^s to $\tilde{O}_{n,\eta_V}(R^{\mathrm{sh}})$. The diagram (6.9) shows this obstruction is the same as the one associated to the first (resp. last) row of (6.9) and the composition of γ^s with the homomorphisms $O_{n,\eta_V}(R^{\mathrm{sh}}) \to O_{n,\eta_V}(\overline{k})$ (resp. $O_{n,\eta_V}(R^{\mathrm{sh}}) \to O_{n,\eta_V}(\kappa(\overline{y}))$). This is because by choosing compatible sections from the right-most groups to the groups forming the middle terms of the rows of (6.9), the two-cocycle z is carried to the corresponding two-cocycles for the other rows. This implies Theorem 6.1. □

We now turn to the problem of associating Hasse-Witt invariants to U which would generalize those considered by Serre and Fröhlich.

For simplicity we will suppose that $\Gamma = \mathrm{Gal}(\overline{L}/L)$ for some p-adic local field L. Let y be a point of Y such that $\kappa(y)$ has characteristic 0. Since $Y = \mathrm{Spec}(R)$ and $R = R_{\mathcal{G}}(\Gamma, \rho)$ is a W-algebra, we find that $\kappa(y)$ is an algebra over the fraction field $F(W)$ of the Witt vectors W. Define U_y to be the continuous orthogonal representation of Γ over $\kappa(y)$ which results from specializing U at y.

Problem 6.2. *Can one construct a $\kappa(y)$-algebra B_y with continuous Γ-action having the following properties?*

(a) $B_y^{\Gamma} = \kappa(y)$.
(b) *Let Γ act diagonally on $B_y \otimes_{\kappa(y)} U_y$, and define $D_y = (B_y \otimes_{\kappa(y)} U_y)^{\Gamma}$. Then $\dim_{\kappa(y)}(D_y) = \dim_{\kappa(y)}(U_y) = n$.*
(c) *The multiplication form $B_y \times B_y \to B_y$ and the orthogonal pairing on $U_y \times U_y \to \kappa(y)$ give a perfect symmetric pairing*

$$\langle -, - \rangle_y : D_y \times D_y \to B_y^{\Gamma} = \kappa(y). \tag{6.10}$$

Example 6.3. (Saito [12]) Suppose $\kappa(y) = \mathbb{Q}_p$, and that U_y is a crystalline representation of $\Gamma = \mathrm{Gal}(\overline{L}/L)$. Then the ring B_y can be taken to be Fontaine's ring B_{cris} (cf. [6]).

If one can solve Problem 6.2 affirmatively, then one can consider the Hasse-Witt invariants of the quadratic form in (6.10).

Let $N = \kappa(y) \cdot L$ be the compositum of $\kappa(y)$ and L. Then there are restriction maps

$$\begin{array}{rccc} \mathrm{res}^N_{\kappa(y)} : & H^2(\kappa(y), \{\pm 1\}) & \to & H^2(N, \{\pm 1\}) \,, \\ \mathrm{res}^N_L : & H^2(L, \{\pm 1\}) & \to & H^2(N, \{\pm 1\}) \,. \end{array}$$

One can compare the restriction of the Hasse-Witt invariants from $\kappa(y)$ to N with the restrictions of the Stiefel-Whitney classes from L to N.

For example, suppose $\kappa(y)$ is a subfield of L. In [12, Theorem 1], Saito makes some further hypotheses about D_y, which are satisfied in the context of Example 6.3. He proves that under these hypotheses, there is a relation between the first and second Hasse-Witt invariants of (6.10), the spinor norm defined in (6.2) and the Stiefel-Whitney classes defined in (6.3) and (6.5). This relationship generalizes the one proved by Fröhlich in [7].

The significance of Theorem 6.1 to Hasse-Witt invariants is that the Stiefel-Whitney class terms which arise in Saito's formulas do not depend on the choice of the point y. This gives a relationship between the Hasse-Witt invariants of the D_y associated to all y for which $\kappa(y) = \mathbb{Q}_p$ and U_y is crystalline, for example.

The main question is whether one can generalize these results to a situation in which $\kappa(y)$ is not $\mathbb{Q}_p$, or more generally, to y for which $\kappa(y)$ is not a subfield of L. In general, the versal deformation ring $R = R_{\mathcal{G}}(\Gamma, \rho)$ will be of dimension larger than one, and this leads to representations of Γ over fields $\kappa(y)$ which are of positive transcendence degree over $\mathbb{Q}_p$. The $\kappa(y)$-algebra B_y one is looking for in Problem 6.2 can thus be viewed as a generalization of Fontaine's B_{cris} for representations of Γ over such $\kappa(y)$. Eventually, one would like a version of B_{cris} which applies over all of $Y = \text{Spec}(R)$, rather than to individual specializations at points $y \in Y$.

References

[1] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[2] P. Cassou-Noguès, B. Erez, and M. J. Taylor, *Invariants of a quadratic form attached to a tame covering of schemes*, J. Théor. Nombres Bordeaux **12** (2000), 597–660.

[3] G. Cornell, J. H. Silverman, and G. Stevens, ed., *Modular Forms and Fermat's Last Theorem (Boston, MA, 1995)*, Springer-Verlag, Berlin-Heidelberg-New York, 1997.

[4] B. de Smit and H. W. Lenstra, *Explicit construction of universal deformation rings*, Modular Forms and Fermat's Last Theorem (Boston, MA, 1995), Springer-Verlag, Berlin-Heidelberg-New York, 1997, pp. 313–326.

[5] H. Esnault, B. Kahn, and E. Viehweg, *Coverings with odd ramifications and Stiefel-Whitney classes*, J. Reine Angew. Math. **44** (1993), 145–188.

[6] J. M. Fontaine, *Le corps des périodes p-adiques. With an appendix by Pierre Colmez*, Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque **223** (1994), pp. 59–111.

[7] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123.

[8] A. Grothendieck, *EGA IV, Etude locale des schémas et des morphismes de schemas*, I.H.E.S. Publ. Math. **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[9] H. Matsumura, *Commutative Algebra*, Benjamin, New York, 1970.

[10] B. Mazur, *Deforming Galois representations*, Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), Springer-Verlag, Berlin-Heidelberg-New York, 1989, pp. 385–437.

[11] B. Mazur, *Deformation theory of Galois representations*, Modular Forms and Fermat's Last Theorem (Boston, MA, 1995), Springer-Verlag, Berlin-Heidelberg-New York, 1997, pp. 243–311.

[12] T. Saito, *The sign of the functional equation of the L-function of an orthogonal motive*, Invent. Math. **120** (1995), 119–142.

[13] ———, *Note on Stiefel-Whitney class in étale cohomology*, preprint, 2001.

[14] M. Schlessinger, *Functors of Artin Rings*, Trans. Amer. Math. Soc. **130** (1968), 208–222.

[15] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), 651–676.

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

[17] J. Tilouine, *Deformations of Galois representations and Hecke algebras*, Published for the Mehta Research Institute, Narosa Publishing House, New Delhi, 1996.

[18] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443–551.

F. Bleher, Department of Mathematics, University of Iowa, Iowa City, IA 52242-1419, USA

E-mail address: `fbleher@math.uiowa.edu`

T. Chinburg, Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA

E-mail address: `ted@math.upenn.edu`