C. R. Acad. Sci. Paris, Ser. I 334 (2002) 97-100

Théorie des nombres/Number Theory

Deformations and derived categories *

Frauke M. Bleher^a, Ted Chinburg^b

^a Department of Mathematics, University of Iowa, Iowa City, IA 52242-1419, USA
^b Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA

Received 2 October 2001; accepted 10 December 2001

Note presented by Jean-Pierre Serre.

Abstract We generalize the deformation theory of representations of profinite groups developed by Mazur and Schlessinger to complexes of modules for such groups. As an example, we determine the universal deformation ring of the compact étale hypercohomology of μ_p on certain affine CM elliptic curves studied by Boston and Ullom. To cite this article: F.M. Bleher, T. Chinburg, C. R. Acad. Sci. Paris, Ser. I 334 (2002) 97–100. © 2002 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

Déformations et catégories dérivées

Résumé Nous généralisons la théorie de déformation des représentations des groupes profinis développée par Mazur et Schlessinger aux complexes de modules sur de tels groupes. Comme exemple nous déterminons l'anneau de déformation universelle de l'hypercohomologie étale compacte de μ_p sur certaines courbes elliptiques affines de type CM étudiées par Boston et Ullom. Pour citer cet article : F.M. Bleher, T. Chinburg, C. R. Acad. Sci. Paris, Ser. I 334 (2002) 97–100. © 2002 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

1. Introduction

Suppose k is a finite field of characteristic p and that G is a profinite group. In [11,12], Mazur developed a deformation theory of finite dimensional representations of G over k using results of Schlessinger [16]. This theory has become a basic tool in arithmetic geometry (see, e.g., [17,18,6,4] and their references). In this paper we generalize the theory by considering objects V^{\bullet} in the derived category $D^{-}([[kG]])$ of bounded above complexes of profinite modules over the completed group algebra [[kG]] of G over k. Our main result, Theorem 1, states that under certain natural conditions on V^{\bullet} and G, the functor of deformations of V^{\bullet} in the derived at versal deformation ring, and this ring is universal if the endomorphism ring of V^{\bullet} in the derived category is equal to the scalar multiplications provided by k.

We have two reasons for pursuing this generalization. The first is that in arithmetic geometry, objects in derived categories occur in a natural way as hypercohomology complexes of sheaves. Such complexes often carry more information than their individual cohomology groups, and the same is true when one considers deformations. Further, complexes have already played an important role in deformation theory (*see*, e.g., [8,9]). Our second motivation is to study how deformation rings behave under derived equivalences between blocks of group rings. When G is finite, Morita equivalences can be useful in

E-mail addresses: fbleher@math.uiowa.edu (F.M. Bleher); ted@math.upenn.edu (T. Chinburg).

^{© 2002} Académie des sciences/Éditions scientifiques et médicales Elsevier SAS. Tous droits réservés S1631-073X(02)02237-9/FLA

computing deformation rings (*cf.* [1], and [2] for related applications). Derived equivalences are conjectured to exist in greater generality than Morita equivalences (*cf.* [5,15]), and to use them in this context one needs a deformation theory of complexes.

After stating Theorem 1 in Section 2 of this Note, we discuss in Section 3 an example relating to elliptic curves X over Q. Let S be a large finite set of primes containing p, and let G_S be the Galois group of the maximal algebraic extension of Q unramified outside S. Define $\overline{X}[p]$ to be the p-torsion points of $\overline{X} = \overline{\mathbf{Q}} \otimes X$. Deformations of $\overline{X}[p]$ as a G_S -module play, e.g., a central role in the proof of Fermat's last theorem [18,17,6]. Let U be the complement of the origin in X, and define $\overline{U} = \overline{\mathbf{Q}} \otimes_{\mathbf{Q}} U$. Then the compact étale hypercohomology $H_c^{\bullet}(\overline{U}, \mu_p)$ is a two-term complex with $H_c^1(\overline{U}, \mu_p) \cong \overline{X}[p]$. We show that for some CM elliptic curves studied by Boston and Ullom [3], the versal deformation of $H_c^{\bullet}(\overline{U}, \mu_p)$ as a complex of G_S -modules is universal and completely split, in the sense that it is isomorphic to a complex of $[[(\mathbf{Z}/p)G_S]]$ -modules having trivial boundary maps. In the course of proving this result, we establish some sufficient conditions for the complete splitting of the hypercohomology $H^{\bullet}(\overline{A}, \mathcal{F})$ of a constructible sheaf \mathcal{F} of k-vector spaces on an abelian variety A over \mathbf{Q} , where $\overline{A} = \overline{\mathbf{Q}} \otimes A$. For an arbitrary affine elliptic curve \overline{U} , the versal deformation of $H_c^{\bullet}(\overline{U}, \mu_p)$ will not be completely split, and it is an open problem to determine when this deformation is universal. It would be very interesting to find geometric or automorphic constructions of quotients of the versal deformation of $H_c^{\bullet}(\overline{U}, \mu_p)$ corresponding to the various extra conditions on deformations of $\overline{X}[p]$ used in [6].

2. Quasi-lifts and deformation functors

Let W = W(k) be the ring of infinite Witt vectors over the finite field k. Define \widehat{C} to be the category of complete local Noetherian rings with residue field k. The morphisms in \widehat{C} are continuous W-algebra homomorphisms which induce the identity on k. Let C be the subcategory of Artinian objects in \widehat{C} . If $R \in$ $Ob(\widehat{C})$, define [[RG]] to be the completed group algebra over R of the profinite group G. For background about profinite completions, profinite modules and the cohomology of profinite groups, see [14]. Let $\widehat{\otimes}_R$ be the completed tensor product in the category PMod(R) of profinite R-modules. Let $D^-([[RG]])$ be the derived category of the homotopy category of complexes of profinite [[RG]]-modules which are bounded above. We will say that a complex M^{\bullet} in $D^-([[RG]])$ has finite profinite R-tor dimension if it has finite tor dimension in $D^-(PMod(R))$.

DEFINITION. – Let V^{\bullet} be a complex in $D^{-}([[kG]])$ which has only finitely many non-zero cohomology groups, all of which are finite. A quasi-lift of V^{\bullet} over an object R of \widehat{C} is a pair (M^{\bullet}, ϕ) consisting of a complex M^{\bullet} in $D^{-}([[RG]])$ which has finite profinite R-tor dimension together with an isomorphism $\phi: k \widehat{\otimes}_{R}^{L} M^{\bullet} \to V^{\bullet}$ in $D^{-}([[kG]])$, where $\widehat{\otimes}_{R}^{L}$ is the left derived functor of $\widehat{\otimes}_{R}$. Two quasi-lifts (M^{\bullet}, ϕ) and (M'^{\bullet}, ϕ') are isomorphic if there is an isomorphism $M^{\bullet} \to M'^{\bullet}$ in $D^{-}([[RG]])$ which carries ϕ to ϕ' . A deformation of V^{\bullet} over R is an isomorphism class of quasi-lifts of V^{\bullet} .

DEFINITION. – Let $\widehat{F} = \widehat{F}_{V^{\bullet}}$ (resp. $F = F_{V^{\bullet}}$) be the functor from \widehat{C} (resp. C) to the category of sets which sends each object R of \widehat{C} to the set $\widehat{F}(R)$ (resp. F(R)) of all deformations of V^{\bullet} over R.

DEFINITION. – A profinite group G has finite profinite cohomology if $H^{j}(G, M)$ is finite for each discrete finite [[kG]]-module M and all integers j.

We can now state our main result.

THEOREM 1. – Suppose that G has finite profinite cohomology.

(a) The functor F has a pro-representable hull (cf. [16], Def. 2.7 and [12], §18) and \widehat{F} is continuous (cf. [12]). Thus there is an object $R(G, V^{\bullet}) \in Ob(\widehat{C})$ and a deformation $(U(G, V^{\bullet}), \phi_{V^{\bullet}})$ of V^{\bullet} over $R(G, V^{\bullet})$ with the following property. For each $R \in Ob(\widehat{C})$, the map $Hom_{\widehat{C}}(R(G, V^{\bullet}), R) \to \widehat{F}(R)$ induced by $\alpha \to R \widehat{\otimes}_{R(G, V^{\bullet}), \alpha}^{L} U(G, V^{\bullet})$ is surjective, and this map is bijective if R is the ring $k[\varepsilon]/\varepsilon^{2}k[\varepsilon]$ of dual numbers over k.

- (b) The tangent space $t_F = F(k[\varepsilon]/\varepsilon^2 k[\varepsilon])$ is isomorphic as a k-vector space to $\operatorname{Ext}^1_{D^-([[kG]])}(V^{\bullet}, V^{\bullet})$.
- (c) If $\operatorname{Hom}_{D^{-}([[kG]])}(V^{\bullet}, V^{\bullet}) \cong k$, then \widehat{F} is represented by $R(G, V^{\bullet})$ in \widehat{C} .

We call $R(G, V^{\bullet})$ in part (a) (resp. (c)) of this theorem the versal (resp. universal) deformation ring of V^{\bullet} . In part (a), we call $U(G, V^{\bullet})$ the versal deformation complex of V^{\bullet} . The pair $(R(G, V^{\bullet}), U(G, V^{\bullet}))$ is determined up to an isomorphism, which is canonical in Theorem 1(c).

As in Mazur's work, the proof of Theorem 1 consists of checking Schlessinger's criteria for prorepresentability in [16] followed by an additional continuity argument. Instead of using matrix representations and cocycle calculations, we adapt the homological methods used in [13], Chap. VI. The most difficult part of the proof is to show that in part (b), one obtains an isomorphism $h: t_F \to \operatorname{Ext}_{D^-([[kG]])}^1(V^{\bullet}, V^{\bullet})$ by using the triangle $V^{\bullet} \to M^{\bullet} \to V^{\bullet} \stackrel{h(M^{\bullet})}{\longrightarrow} V^{\bullet}[1]$ associated to each $M^{\bullet} \in t_F$ after identifying εM^{\bullet} and $M^{\bullet}/\varepsilon M^{\bullet}$ with V^{\bullet} . In a later paper we will consider the relation of $\operatorname{Ext}_{D^-([[kG]])}^0(V^{\bullet}, V^{\bullet})$ to obstructions.

3. Abelian varieties and affine elliptic curves

Let X be an abelian variety over \mathbf{Q} of dimension d with origin \underline{O} . Define $\overline{X} = \overline{\mathbf{Q}} \otimes_{\mathbf{Q}} X$, $G_{\mathbf{Q}} = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and let k be a finite field of characteristic p. Suppose \mathcal{F} is a constructible sheaf of k-vector spaces on the étale topology of X whose restriction to \overline{X} is constant. Denote by $\mathcal{F}(n)$ the *n*th Tate twist $\mathcal{F}(\mu_p^{\otimes n})$ of \mathcal{F} . Define $\overline{U} = \overline{\mathbf{Q}} \otimes (X - \underline{O})$. By [13], Corollary VI.2.8, Theorem VI.1.1, the hypercohomology $H^{\bullet}(\overline{X}, \mathcal{F})$ and the compact hypercohomology $H_c^{\bullet}(\overline{U}, \mathcal{F})$ define objects in $D^-([[kG_{\mathbf{Q}}]])$ which have finitely many non-zero cohomology groups, all of which are finite.

THEOREM 2. – If p > 2d, both $H^{\bullet}(\overline{X}, \mathcal{F})$ and $H^{\bullet}_{c}(\overline{U}, \mathcal{F})$ are completely split in $D^{-}([[kG_{\mathbf{Q}}]])$, in the sense that they are isomorphic to complexes having trivial boundary maps. If there is a non-degenerate k-bilinear pairing of constructible sheaves $\mathcal{F} \times \mathcal{F} \to k(d)$, then the same conclusion holds provided p > 2d - 2.

The proof of this theorem uses ideas of Deninger and Murre [7] and of Künnemann [10]. Let $m_n : \overline{X} \to \overline{X}$ be multiplication by an integer *n*. One shows that if p > 2d, the endomorphisms of $H^{\bullet}(\overline{X}, \mathcal{F})$ produced by the m_n as *n* varies are sufficient to split $H^{\bullet}(\overline{X}, \mathcal{F})$. Suppose now that \mathcal{F} has a non-degenerate *k*-bilinear pairing to k(d). One can then use the existence of a rational point (the origin \underline{O}) on X, in addition to the étale duality theorem, to produce some additional endomorphisms of $H^{\bullet}(\overline{X}, \mathcal{F})$, leading to a slightly sharper result.

Because multiplication defines a non-degenerate pairing $\mu_p \times \mu_p \to \mu_p(1) = \mu_p^{\otimes 2}$, we have the following corollary.

COROLLARY 3. – With the notations of Theorem 2, suppose d = 1, so that X is an elliptic curve. For all primes p, the complexes $H^{\bullet}(\overline{X}, \mu_p)$ and $H^{\bullet}_{c}(\overline{U}, \mu_p)$ are completely split in $D^{-}([[kG_{O}]])$.

For the rest of this section we will suppose d = 1 and $k = \mathbb{Z}/p$. Let *S* be a finite set of places of \mathbb{Q} containing the prime *p*, the archimedean place as well as all primes dividing the conductor *N* of *X*. The $G_{\mathbb{Q}}$ -module $H_c^i(\overline{U}, \mu_p)$ is isomorphic to \mathbb{Z}/p with trivial action if i = 2, to the *p*-torsion $\overline{X}[p]$ of the elliptic curve \overline{X} if i = 1 and to {0} otherwise. It follows that the action of $G_{\mathbb{Q}}$ on these cohomology groups factors through the Galois group G_S of the maximal algebraic extension of \mathbb{Q} unramified outside *S*. Hence by Corollary 3, $H_c^{\bullet}(\overline{U}, \mu_p)$ is isomorphic to the inflation of the two-term split complex V^{\bullet} in $D^-([[kG_S]])$ whose *i*th degree term is $H_c^i(\overline{U}, \mu_p)$ considered as a G_S -module. For a kG_S -module *Y*, define $R(G_S, Y)$ to be the versal deformation ring of *Y* in the sense of Mazur [11], §1.2. Define $W\langle n \rangle$ to be the ring of formal power series over *W* on *n* commuting indeterminates.

PROPOSITION 4. – Suppose d = 1, $k = \mathbb{Z}/p$, $\operatorname{Hom}_{G_S}(k, \overline{X}[p]) = 0 = H^2(G_S, \overline{X}[p])$, and the versal deformation ring $R(G_S, \mathbb{Z}/p)$ (resp. $R(G_S, \overline{X}[p])$) is topologically isomorphic to $W\langle n_1 \rangle$ (resp. $W\langle n_2 \rangle$).

Then the versal deformation ring $R(G_S, V^{\bullet})$ is isomorphic to $W\langle n_1 + n_2 \rangle$, and the versal deformation complex $U(G_S, V^{\bullet})$ is completely split in $D^{-}([[R(G_S, V^{\bullet})G_S]])$. If $R(G_S, \overline{X}[p])$ is a universal deformation ring, then so is $R(G_S, V^{\bullet})$.

This proposition is proved by noting that since V^{\bullet} is completely split, it has a versal completely split deformation ring $R^{sp}(G_S, V^{\bullet})$ in the obvious sense, which is the tensor product over W of the versal deformation rings of the cohomology groups of V^{\bullet} . The conditions of the Proposition together with Theorem 1(b) imply that the canonical map $R(G_S, V^{\bullet}) \rightarrow R^{sp}(G_S, V^{\bullet})$ induces an isomorphism on tangent spaces, which forces $R(G_S, V^{\bullet})$ to be isomorphic to $R^{sp}(G_S, V^{\bullet}) \cong W\langle n_1 + n_2 \rangle$. In this sense, the hypotheses of Proposition 4 imply there are no deformation obstructions.

Our last result now follows from work of Boston and Ullom [3]. By a quadratic progression, we mean a set of integers of the form $\mathbb{Z} \cap \{f(x) : x \in \mathbb{Q}\}$ for some quadratic polynomial $f(x) \in \mathbb{Q}[x]$. The Dirichlet density of the set of primes in such a progression is 0.

THEOREM 5. – Suppose X is an elliptic curve of conductor N with complex multiplication by the ring of integers \mathcal{O} in an imaginary quadratic field L of class number 1. There is a set T' of rational primes consisting of a finite set which can be effectively determined together with some (possibly no) primes in quadratic progression such that the following is true. Suppose $p \notin T'$, p splits in L, and that S is the set of places of **Q** determined by prime numbers dividing pN together with the Archimedean place of **Q**. Then the hypotheses of Proposition 4 hold, and the versal deformation ring $R(G_S, V^{\bullet})$ is universal and isomorphic to $W\langle 4 \rangle$.

⁵ Supported (respectively) by NSA Young Investigator Grant MDA904-01-1-0050 and NSF Grant DMS00-70433.

References

- [1] Bleher F.M., Chinburg T., Universal deformation rings and cyclic blocks, Math. Ann. 318 (2000) 805-836.
- [2] Bleher F.M., Chinburg T., Applications of universal deformations to Galois theory, Preprint, 2001.
- [3] Boston N., Ullom S.V., Representations related to CM elliptic curves, Math. Proc. Cambridge Philos. Soc. 113 (1993) 71–85.
- [4] Breuil C., Conrad B., Diamond F., Taylor R., On the modularity of elliptic curves over Q: Wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001) 843–939.
- [5] Broué M., Isométries parfaites, types de blocs, catégories dérivées, Astérisque 181-182 (1990) 61-92.
- [6] Cornell G., Silverman J.H., Stevens G. (Eds.), Modular Forms and Fermat's Last Theorem (Boston, 1995), Springer-Verlag, Berlin, 1997.
- [7] Deninger C., Murre J., Motivic decomposition of Abelian schemes and the Fourier transform, J. Reine Angew. Math. 422 (1991) 201–219.
- [8] Illusie L., Complexe cotangent et déformations. I, Lecture Notes in Math., Vol. 239, Springer-Verlag, Berlin, 1971.
- [9] Illusie L., Complexe cotangent et déformations. II, Lecture Notes in Math., Vol. 283, Springer-Verlag, Berlin, 1972.
- [10] Künnemann K., On the Chow motive of an Abelian scheme, in: Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., Vol. 55, Part 1, American Mathematical Society, Providence, RI, 1994, pp. 189–205.
- [11] Mazur B., Deforming Galois representations, in: Galois Groups over Q (Berkeley, CA, 1987), Springer-Verlag, Berlin, 1989, pp. 385–437.
- [12] Mazur B., Deformation theory of Galois representations, in: Modular Forms and Fermat's Last Theorem (Boston, 1995), Springer-Verlag, Berlin, 1997, pp. 243–311.
- [13] Milne J.S., Étale cohomology, Princeton University Press, Princeton, 1980.
- [14] Ribes L., Zalesskii P., Profinite Groups, Ergeb. Math. Grenzgeb., Vol. 40, Springer-Verlag, Berlin, 2000.
- [15] Rickard J., The Abelian defect group conjecture, in: Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), Doc. Math., Extra, Vol. II, 1998, pp. 121–128.
- [16] Schlessinger M., Functors of Artin rings, Trans. Amer. Math. Soc. 130 (1968) 208–222.
- [17] Taylor R., Wiles A., Ring-theoretic properties of certain Hecke algebras, Ann. Math. 141 (1995) 553–572.
- [18] Wiles A., Modular elliptic curves and Fermat's last theorem, Ann. Math. 141 (1995) 443-551.