pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Explicit Construction of Universal Deformation Rings

B. de Smit and H. W. Lenstra, Jr.

Abstract. Let V be an absolutely irreducible representation of a profinite group G over the residue field k of a noetherian local ring $\mathcal{O}$. For local complete $\mathcal{O}$-algebras A with residue field k the representations of G over A that reduce to V over k are given by $\mathcal{O}$-algebra homomorphisms $R \to A$, where R is the universal deformation ring of V. We show this with an explicit construction of R. The ring R is noetherian if and only if $H^1(G, \mathrm{End}_k(V))$ has finite dimension over k.

1. Introduction

Let G be a profinite group and let k be a field. By a *k-representation* of G we mean a finite dimensional vector space over k with the discrete topology, equipped with a continuous k-linear action of G. If V is a k-representation of G and A is a complete local ring with residue field k, then a *deformation* of V in A is an isomorphism class of continuous representations of G over A that reduce to V modulo the maximal ideal of A; precise definitions are given in Section 2. We denote by $\mathrm{Def}(V, A)$ the set of such deformations.

Let V be an absolutely irreducible k-representation of G. The object of this chapter is to give a straight-forward construction of a ring R, the *universal deformation ring*, which represents the functor $\mathrm{Def}(V, -)$. In a purely algebraic setting, without considerations of continuity, a similar construction was already given by Procesi in the seventies [9, Chap. IV, Lemma 1.7; 10]. The existence of R in the present context was deduced first by Mazur [8] with Schlessinger's criteria for pro-representability [12]. An alternative construction was given recently by Faltings (see [5] and Section 7 below).

The main result of this chapter, formulated below as Theorem (2.3), is actually a little more general than Mazur's. Following Schlessinger, Mazur works only with noetherian rings, and this forces him to assume at the outset that a certain cohomology group is finite. For our argument, the noetherian condition is a hindrance, and we find it more convenient to follow Grothendieck [6] and work with not necessarily noetherian rings that are projective limits of artinian rings. This allows us to drop Mazur's cohomological condition; it reappears only at the end, as a necessary and sufficient condition for R to be noetherian.

Acknowledgement. The authors thank N. Boston, E. Das, B. Edixhoven, and C. Procesi for their assistance. The first author was employed by the Erasmus Universiteit Rotterdam while most of this paper was being written. Both authors received support from the Nederlandse Organisatie voor Wetenschappelijk Onderzoek. The second author was supported by the National Science Foundation under Grant No. DMS 9224205.

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Our construction of R proceeds in three steps. First we let G be finite, and we consider the functor that assigns to A a certain set of homomorphisms $G \to \mathrm{GL}_n(A)$. Proving that this functor is representable is very easy: one just defines the corresponding 'universal' ring by generators and relations. Next, we take a projective limit and obtain a similar result for arbitrary profinite G (Proposition (2.5)). To conclude the construction, we pass to the closed subring generated by the traces of the elements of G; the proof that this ring has the required properties makes use of an argument of Serre [3, Théorème 2].

It is in the last step of the construction that the absolute irreducibility of V is crucially used. In Wiles's proof of Fermat's Last Theorem the existence of deformation rings is only needed for such V. Wiles also uses the fact that such deformation rings are generated by traces [13, pp. 509–512], so the approach above is particularly suitable for Wiles's applications. It is, however, of interest to observe that the universal deformation ring also exists when V, instead of being absolutely irreducible, satisfies the weaker condition $\mathrm{End}_{k[G]}(V) = k$. In the noetherian case this was shown by Ramakrishna [11], as a consequence of Schlessinger's criteria. The general case is proved in Section 7. Instead of taking the subring generated by the traces we pass to the subring generated by a larger collection of elements, as suggested by an argument due to Faltings [5, Section 2.6]. We do not know whether a similar result holds in Procesi's purely algebraic setting.

Following Ramakrishna [11] we indicate in Section 6 how one can impose additional conditions on the deformations to obtain "ordinary" and "flat" deformation rings.

2. Main results

We denote the maximal ideal of a local ring A by $\mathfrak{m}_A$.

(2.1) Local complete rings. Let $\mathcal{O}$ be a noetherian local ring with residue field k. We denote by $\mathcal{C}$ the category of local topological $\mathcal{O}$-algebras A that satisfy the following two conditions: the natural map $\mathcal{O} \to A/\mathfrak{m}_A$ is surjective (so that k is also the residue field of A), and the map from A to the projective limit of its discrete artinian quotients is a topological isomorphism. Equivalently, the second condition asserts that A is complete and that its topology can be given by a collection of open ideals $\mathfrak{a}$ for which $A/\mathfrak{a}$ is artinian. Morphisms in $\mathcal{C}$ are continuous $\mathcal{O}$-algebra homomorphisms.

(2.2) Deformations. Let $\mathcal{O}$ and k be as above, let A be a ring in $\mathcal{C}$, and let G be a topological group. A *representation* of G over A, or an A-*representation* of G, is a finitely generated free A-module M with a continuous A-linear action of G; here we give M the product topology via an A-module isomorphism $M \cong_A A^n$, a topology that is independent of the choice of the isomorphism. Two A-representations M and M' are said to be *isomorphic* if there is an $A[G]$-module isomorphism $M \xrightarrow{\sim} M'$, and we denote this by $M \cong_{A[G]} M'$.

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Let V be a k-representation of G. By a *deformation* of V in A we mean an isomorphism class of A-representations W of G for which $W \otimes_A k \cong_{k[G]} V$. The set of such deformations is denoted by $\mathrm{Def}(V, A)$. A morphism $f\colon A \to A'$ in $\mathcal{C}$ gives rise to a map $f_*\colon \mathrm{Def}(V, A) \to \mathrm{Def}(V, A')$ that sends the class of a representation W over A to the class of $W \otimes_A A'$.

Throughout the paper V is a representation of a profinite group G over the residue field k (with the discrete topology) of a noetherian local ring $\mathcal{O}$, and $\mathcal{C}$ is as above.

(2.3) Theorem. *If V is absolutely irreducible then*

(1) *there is a ring R in $\mathcal{C}$ and a deformation $D \in \mathrm{Def}(V, R)$ such that for all rings A in $\mathcal{C}$ we have a bijection $\mathrm{Hom}_{\mathcal{C}}(R, A) \xrightarrow{\sim} \mathrm{Def}(V, A)$ given by $f \mapsto f_*(D)$;*
(2) *the pair (R, D) is determined up to unique $\mathcal{C}$-isomorphism by the property in (1);*
(3) *the ring R is noetherian if and only if $\dim_k H^1(G, \mathrm{End}_k(V)) < \infty$;*
(4) *if R is noetherian then the following hold: R is $\mathfrak{m}_R$-adically complete and for each A in $\mathcal{C}$ we have a well-defined bijection*

$$\mathrm{Hom}_{\mathcal{O}\text{-Alg}}(R, A) \xrightarrow{\sim} \mathrm{Def}(V, A)$$

given by $f \mapsto f_*(D)$.

Recall that V is *absolutely irreducible* if $V \otimes_k K$ is a simple $K[G]$-module for every field extension K of k. The H^1 in (3) denotes the continuous cohomology group of the discrete G-module $\mathrm{End}_k(V)$, on which the G-action is given by $(g\varphi)(v) = g\varphi(g^{-1}v)$ for $\varphi \in \mathrm{End}_k(V)$ and $v \in V$. By "$\mathrm{Hom}_{\mathcal{O}\text{-Alg}}$" we denote the set of $\mathcal{O}$-algebra homomorphisms.

Statement (2) of the theorem follows from (1) by the standard uniqueness argument for universal objects. Statement (4) will follow immediately from (1) and the following proposition.

(2.4) Proposition. *Suppose A is a noetherian ring in $\mathcal{C}$. Then the topology on A is equal to the $\mathfrak{m}_A$-adic topology, and A is $\mathfrak{m}_A$-adically complete. Furthermore, every $\mathcal{O}$-algebra homomorphism $A \to A'$ with A' in $\mathcal{C}$ is continuous.*

The proof of (2.4) and the proof of part (3) of (2.3) are postponed to Section 5. By (2.4), the category $\mathcal{C}'$ whose objects are complete noetherian local $\mathcal{O}$-algebras with residue field k and whose morphisms are $\mathcal{O}$-algebra homomorphisms is a full subcategory of $\mathcal{C}$. We will use later that a closed sub-$\mathcal{O}$-algebra A' of a ring A in $\mathcal{C}$ is again in $\mathcal{C}$, which follows from the fact that a sub-$\mathcal{O}$-algebra of an artinian ring in $\mathcal{C}$ is again an artinian ring in $\mathcal{C}$. However, if A is in $\mathcal{C}'$ then A' need not be in $\mathcal{C}'$.

We will show (1) by an explicit construction, which starts by representing an easier functor. For this we will write representations as homomorphisms to matrix groups. Let V be any k-representation of G. If one

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

chooses a k-basis $v_1, \ldots, v_n$ for V, then the G-action on V is given by a continuous homomorphism $\overline{\rho}: G \to \mathrm{GL}_n(k)$. Now let W be a representation of G over some A in $\mathcal{C}$ such that $W/\mathfrak{m}_A W = W \otimes_A k \cong_{k[G]} V$. By Nakayama's lemma elements $w_1, \ldots, w_n \in W$ such that $w_i \mapsto v_i$ form an A-basis of W. The G-action on W is then given by a continuous group homomorphism $\rho: G \to \mathrm{GL}_n(A)$ such that the composite map $G \to \mathrm{GL}_n(A) \to \mathrm{GL}_n(k)$ is $\overline{\rho}$. We denote the set of such maps ρ by $\mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A))$. Here "CHom" denotes the set of continuous homomorphisms, and the subscript $\overline{\rho}$ expresses the condition that the homomorphisms considered reduce to $\overline{\rho}$ over the residue field k of A.

(2.5) Proposition. *There are a ring R_b in $\mathcal{C}$ and a map*

$$\rho_b \in \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(R_b))$$

such that for each A in $\mathcal{C}$ we have a bijection

$$\mathrm{Hom}_{\mathcal{C}}(R_b, A) \xrightarrow{\sim} \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A))$$

that sends a $\mathcal{C}$-morphism f to the composite map

$$G \xrightarrow{\rho_b} \mathrm{GL}_n(R_b) \xrightarrow{f} \mathrm{GL}_n(A).$$

The pair (R_b, ρ_b) is determined up to unique isomorphism by this property.

The ring R_b will be constructed in Section 3 as a projective limit over the discrete quotients of G of complete $\mathcal{O}$-algebras that are explicitly defined by generators and relations. The map ρ_b defines a representation $W_b = R_b^n$ of G in R_b such that $W_b \otimes_{R_b} k \cong_{k[G]} V$. We now let R be the smallest closed sub-$\mathcal{O}$-algebra of R_b that contains the traces of all matrices $\rho_b(g)$ with $g \in G$. Note that R is in $\mathcal{C}$ again. The following result asserts that we can define the representation W_b of G over the subring R. We let D be the $R[G]$-isomorphism class of this R-representation.

(2.6) Proposition. *Let W be a representation of G over some ring A in $\mathcal{C}$ and let $A' \subset A$ be an inclusion of rings in $\mathcal{C}$ so that A' has the induced topology of A. Suppose that A' contains the traces of all endomorphisms of W that are given by multiplication with an element of G, and suppose that $W \otimes_A A/\mathfrak{m}_A$ is absolutely irreducible. Then there is an A'-representation W' of G such that $W' \otimes_{A'} A \cong_{A[G]} W$.*

Proposition (2.6) is a variation of results due to Serre [3, Théorème 2] and Mazur [8, Proposition 4]. See Section 4 for a proof.

Let us assume (2.6) for the moment and prove that the pair (R, D) satisfies statement (1) of the theorem. Let W be a representation of G over a ring A in $\mathcal{C}$ for which $W \otimes_A k \cong_{k[G]} V$. Choosing a basis of W as in the argument before (2.5), one can give the G-action on W by a continuous homomorphism $\rho \in \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A))$. By (2.5) there is a $\mathcal{C}$-morphism

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

$f_b\colon R_b \to A$ such that the composite map $G \xrightarrow{\rho_b} \mathrm{GL}_n(R) \xrightarrow{f_b} \mathrm{GL}_n(A)$ is equal to ρ. Then the restriction $f\colon R \to A$ of f_b has the property that $f_*(D)$ is the $A[G]$-isomorphism class of W.

The trace of an element of G in some representation of G depends only on the representation up to isomorphism. Given $f_*(D)$ the map f is therefore uniquely determined on the traces of $\rho_b(g)$ for all $g \in G$. But the $\mathcal{O}$-algebra generated by these traces is dense in R, and f is continuous, so f is uniquely determined. This proves the universal property (1) in (2.3) once we know (2.5) and (2.6).

3. Lifting homomorphisms to matrix groups

In this section we prove (2.5). The last statement in (2.5) follows by the usual uniqueness argument.

Suppose first that G is finite, and denote its identity element by e. We define $\mathcal{O}[G,n]$ to be the commutative $\mathcal{O}$-algebra given by

$$\begin{array}{lll} \text{generators:} & X_{ij}^{g} & \text{for } g \in G \text{ and } 1 \le i,j \le n; \\ \text{relations:} & X_{ij}^{e} = \begin{cases} 1 \\ 0 \end{cases} & \begin{array}{l} \text{if } i = j, \\ \text{if } i \ne j; \end{array} \\ & X_{ij}^{gh} = \displaystyle\sum_{l=1}^{n} X_{il}^{g} X_{lj}^{h} & \text{for } g,h \in G \text{ and } 1 \le i,j \le n. \end{array}$$

For example, $\mathcal{O}[G,1]$ is just the group ring of the largest abelian quotient of G over $\mathcal{O}$.

For every $\mathcal{O}$-algebra A we have a canonical bijection

$$\mathrm{Hom}_{\mathcal{O}\text{-Alg}}(\mathcal{O}[G,n], A) \cong \mathrm{Hom}(G, \mathrm{GL}_n(A)), \tag{3.1}$$

where an $\mathcal{O}$-algebra homomorphism $f\colon \mathcal{O}[G,n] \to A$ corresponds to the group homomorphism ρ_f that sends $g \in G$ to the matrix $(f(X_{ij}^{g}))_{i,j}$.

By (3.1) the homomorphism $\overline{\rho}\colon G \to \mathrm{GL}_n(k)$ gives rise to an $\mathcal{O}$-algebra homomorphism $\mathcal{O}[G,n] \to k$. Its kernel is a maximal ideal, which we denote by $\mathfrak{m}_{\overline{\rho}}$. Now let R_b be the completion of $\mathcal{O}[G,n]$ at $\mathfrak{m}_{\overline{\rho}}$. Certainly R_b is noetherian and lies in $\mathcal{C}$. The canonical map $\mathcal{O}[G,n] \to R_b$ gives by (3.1) a map $\rho_b\colon G \to \mathrm{GL}_n(R_b)$ such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\rho_b} & \mathrm{GL}_n(R_b) \\ \| & & \downarrow \\ G & \xrightarrow{\overline{\rho}} & \mathrm{GL}_n(k) \end{array}$$

commutes.

To prove that the map in (2.5) is a bijection, let A be a ring in $\mathcal{C}$ and let $\rho \in \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A))$. By (3.1), there is a unique $\mathcal{O}$-algebra

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

homomorphism $f\colon \mathcal{O}[G,n] \to A$ such that $\rho_f = \rho$. The fact that ρ_f reduces to $\overline{\rho}$ modulo $\mathfrak{m}_A$ implies that $f(\mathfrak{m}_{\overline{\rho}}) \subset \mathfrak{m}_A$. The topology on A is given by open ideals $\mathfrak{a}$ for which $A/\mathfrak{a}$ is artinian, and the map $\mathcal{O}[G,n] \to A \to A/\mathfrak{a}$ is continuous for the $\mathfrak{m}_{\overline{\rho}}$-adic topology on $\mathcal{O}[G,n]$ for each such $\mathfrak{a}$. We therefore obtain a continuous $\mathcal{O}$-algebra homomorphism $\hat{f}\colon R_b \to A$ for which the diagram

$$\begin{array}{ccc} G & \xrightarrow{\rho_b} & \mathrm{GL}_n(R_b) \\ \| & & \downarrow \hat{f} \\ G & \xrightarrow{\rho} & \mathrm{GL}_n(A) \end{array}$$

commutes. Since the elements $\hat{f}(X_{ij}^g)$ are determined by ρ, and the X_{ij}^g generate a dense sub-$\mathcal{O}$-algebra of R_b, the map $\hat{f}$ is uniquely determined by the conditions that it be continuous and that the diagram commute. This finishes the proof of (2.5) in the case that G is finite.

For the general case, write G as $G = \varprojlim H$, with H ranging over those discrete quotients of G for which the representation $\overline{\rho}\colon G \to \mathrm{GL}_n(k)$ factors through a map $\overline{\rho}_H\colon H \to \mathrm{GL}_n(k)$. Each H is finite, so the construction above produces a ring R_H in $\mathcal{C}$ with a group homomorphism $H \to \mathrm{GL}_n(R_H)$ that reduces to $\overline{\rho}_H\colon H \to \mathrm{GL}_n(k)$. Using (2.5) for each H we get a projective system $(R_H)_H$ in $\mathcal{C}$.

Now let $R_b = \varprojlim R_H$. We have a continuous map $\rho_b\colon G \to \mathrm{GL}_n(R_b)$ induced by the composite maps $G \to H \to \mathrm{GL}_n(R_H)$. For fixed H, the images of the defining generators of $\mathcal{O}[H,n]$ generate each discrete artinian quotient of R_H over $\mathcal{O}$. But these images are contained in the image of R_b, so R_b surjects to each discrete artinian quotient of R_H. Moreover, each discrete artinian quotient of R_b arises in this way. In particular it follows that R_b lies in $\mathcal{C}$.

Let $A = \varprojlim A_i$ be a ring in $\mathcal{C}$ written as a projective limit of its discrete artinian quotients. We now have canonical isomorphisms

$$\begin{aligned} \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A)) &\cong \varprojlim_i \ \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A_i)) \\ &\cong \varprojlim_i \ \varinjlim_H \ \mathrm{Hom}_{\overline{\rho}_H}(H, \mathrm{GL}_n(A_i)) \\ &\cong \varprojlim_i \ \varinjlim_H \ \mathrm{Hom}_{\mathcal{C}}(R_H, A_i) \\ &\overset{(*)}{\cong} \varprojlim_i \ \mathrm{Hom}_{\mathcal{C}}(R_b, A_i) \\ &\cong \mathrm{Hom}_{\mathcal{C}}(R_b, A). \end{aligned}$$

For $(*)$ we use that a continuous homomorphism $R_b \to A_i$ factors over some artinian quotient R' of R_b, and that R' can be chosen to be an artinian quotient of some R_H. This proves (2.5).

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

4. The condition of absolute irreducibility

In this section we show (2.6). Let $V = W \otimes_A k$. The G-action on V gives an $\mathcal{O}$-algebra homomorphism $\overline{\rho}\colon k[G] \to \mathrm{End}_k(V)$. The irreducibility of V implies that $D = \mathrm{End}_{k[G]}(V)$ is a division ring, and since V is absolutely irreducible, the tensor product $D \otimes_k K = \mathrm{End}_{K[G]}(V \otimes_k K)$ is also a division ring for any field extension K of k. This implies that $D = k$. By Wedderburn's theorem [7, chap. XVII, 3.5] one then deduces that $k[\overline{\rho}(G)] = \mathrm{End}_k(V)$.

Choosing a k-basis of V we may identify the k-algebra $\mathrm{End}_k(V)$ with the ring $M_n(k)$ of $n \times n$-matrices over k. Let $\bar{e}_1, \ldots, \bar{e}_{n^2}$ be a k-basis of $\mathrm{End}_k(V)$ for which each matrix $\bar{e}_i$ has exactly one non-zero entry. We denote the trace of an endomorphism f of a finitely generated free module over a ring R by $\mathrm{Tr}_R(f)$. An easy computation shows that the determinant of the matrix $(\mathrm{Tr}_k(\bar{e}_i\bar{e}_j))_{i,j} \in M_{n^2}(k)$ does not vanish.

Let B be the sub-A'-algebra of $\mathrm{End}_A(W)$ generated by the image of G. Denote the natural map $\mathrm{End}_A(W) \to \mathrm{End}_k(V)$ by φ. Then we have $\varphi(B) = k[\overline{\rho}(G)] = \mathrm{End}_k(V)$, so we can choose $e_i \in B$ such that $\varphi(e_i) = \bar{e}_i$. Since φ induces an isomorphism $\mathrm{End}_A(W) \otimes_A k \xrightarrow{\sim} \mathrm{End}_k(V)$, it follows from Nakayama's lemma that the e_i form an A-basis of $\mathrm{End}_A(W)$. We claim that they also form an A'-basis of B. Indeed, if we write an element $b \in B$ on this basis as $b = \sum_i a_i e_i$ with $a_i \in A$, then we have

$$\sum_{i=1}^{n^2} a_i \,\mathrm{Tr}_A(e_i e_j) = \mathrm{Tr}_A(b e_j) \in A',$$

because $\mathrm{Tr}_A(B) \subset A'$. The coefficient matrix $(\mathrm{Tr}_A(e_i e_j))_{i,j} \in M_{n^2}(A')$ is invertible, because it is invertible modulo $\mathfrak{m}_{A'}$. Therefore all a_i lie in A', which proves our claim. It follows that $B \otimes_{A'} A = \mathrm{End}_A(W)$.

Choose an idempotent $\bar{\eta}$ in the ring $\mathrm{End}_k(V)$ that generates a minimal left-ideal; e.g., take a matrix with one diagonal entry equal to 1 and all other entries equal to 0. We claim that there exists $\eta \in B$ such that $\eta^2 = \eta$ and $\varphi(\eta) = \bar{\eta}$. If $x \in B$ and $l \geq 1$ are such that $x \equiv x^2 \bmod \mathfrak{m}_{A'}^l B$, then it is easy to check that $f(x) = 3x^2 - 2x^3$ satisfies $f(x) \equiv x \bmod \mathfrak{m}_{A'}^l B$ and $f(x)^2 \equiv f(x) \bmod \mathfrak{m}_{A'}^{2l} B$. Now choose any $\eta_0 \in B$ with $\varphi(\eta_0) = \bar{\eta}$ and consider the sequence η_0, $f(\eta_0)$, $f(f(\eta_0))$, $\cdots$. This is clearly a Cauchy sequence for the $\mathfrak{m}_{A'}$-adic topology on B. But A' is a projective limit of artinian rings, so its $\mathfrak{m}_{A'}$-adic topology is at least as strong as the given topology on A', for which it is complete. This means that the sequence is a Cauchy sequence for the product topology on the free A'-module B, so that the sequence converges to a limit η in B. This η satisfies our conditions.

We have $B\eta \oplus B(1-\eta) = B$, and B is a free A'-module. It follows that the B-module $W' = B\eta$ is also free over A', and from $\varphi(\eta) = \bar{\eta}$ we see that its rank over A' equals $\dim_k(\mathrm{End}_k(V)\bar{\eta}) = n$. Choose an element w_0 of W whose image v_0 in V satisfies $\bar{\eta} v_0 \neq 0$. Then we have

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

$\mathrm{End}_k(V)\bar{\eta}v_0 = V$, so Nakayama's lemma implies that the $\mathrm{End}_A(W)$-linear map $W' \otimes_{A'} A = \mathrm{End}_A(W)\eta \to W$ sending σ to σw_0 is surjective. By checking A-ranks one sees that it is an isomorphism. It follows that W and $W' \otimes_{A'} A$ are isomorphic over $B \otimes_{A'} A$, and in particular they are $A[G]$-isomorphic. It also follows that the G-action on W' is continuous. □

The following result will be needed for the proof of part (3) of (2.3).

(4.1) Lemma. *Let A be a local ring with residue field k and let G be a group. Let $\overline{\rho}: G \to \mathrm{GL}_n(k)$ be a group homomorphism that makes k^n into an absolutely irreducible $k[G]$-module. Then two elements $\rho, \rho' \in \mathrm{Hom}_{\overline{\rho}}(G, \mathrm{GL}_n(A))$ define isomorphic $A[G]$-module structures on A^n if and only if there is a matrix $M \in \mathrm{GL}_n(A)$ reducing to the identity matrix in $\mathrm{GL}_n(k)$ such that $\rho(g) = M\rho'(g)M^{-1}$ for all $g \in G$.*

Proof. The only non-trivial point is the following: if there exists $M \in \mathrm{GL}_n(A)$ such that $\rho(g) = M\rho'(g)M^{-1}$ for all $g \in G$, then M can be chosen so that its reduction $\overline{M} \in \mathrm{GL}_n(k)$ is the identity matrix. Note that $\overline{M}$ lies in $\mathrm{Aut}_{k[G]}(k^n)$, which by the first paragraph of the proof above is just k^*. But the scalar matrix $\overline{M}$ can then be lifted to a scalar matrix T in $\mathrm{GL}_n(A)$, and we can now replace M by MT^{-1}. □

5. Projective limits

In this section we show (2.4) and statement (3) of (2.3).

Let A be a ring in $\mathcal{C}$ which is given as a projective limit $\varprojlim A_i$ of a collection of discrete artinian quotients, where i ranges over some directed index set. We let $\mathfrak{m}$ and $\mathfrak{m}_i$ be the maximal ideals of A and A_i.

(5.1) Lemma. *Suppose that we have a sequence of projective systems*

$$(M_i^1) \to (M_i^2) \to (M_i^3)$$

which for each i is an exact sequence of finitely generated A_i-modules. Assume also that for each $i' \leq i$ and $j = 1, 2, 3$, the transition map $M_i^j \to M_{i'}^j$ is A_i-linear. Then the induced sequence

$$\varprojlim_i M_i^1 \longrightarrow \varprojlim_i M_i^2 \xrightarrow{\varphi} \varprojlim_i M_i^3$$

is an exact sequence of A-modules.

Proof. The projective limits are A-modules by the condition on the transition maps. It is clear that the maps between them are A-linear, and that the composition of the two maps is zero.

Suppose that $(x_i)_i$ is an element in the kernel of φ. Let

$$E_i = \{x \in M_i^1 : x \mapsto x_i\}.$$

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

We need to show that $\varprojlim E_i$ is non-empty. In the case that k is finite one can see this by remarking that $\prod_i E_i$ is compact, and that $\varprojlim E_i$ is the intersection of a collection of closed subsets with the property that any finite subcollection has a non-empty intersection.

For the general case the reader is referred to the criterion for projective limits to be non-empty given in Bourbaki [2, III.7.4, Théorème 1]. To apply this criterion one lets $\mathfrak{S}_i$ be the set of subsets of E_i of the form $x + N$, where $x \in E_i$ and where N is a sub-A_i-module of the kernel of the map $M_i^1 \to M_i^2$ (see also [2, loc. cit., Example II]). □

(5.2) Remark. With a similar argument we will show the following, which will be used in Section 6. If X is a collection of open ideals I of A which is closed under taking finite intersections, then the canonical map $\varphi\colon A \to A' = \varprojlim_{I\in X} A/I$ induces a topological isomorphism $A/F \xrightarrow{\sim} A'$, where $F = \bigcap_{I\in X} I$. Clearly, φ is continuous, and $\operatorname{Ker}\varphi = F$. Suppose first that k is finite. Then A and A' are compact and $\varphi(A)$ is a dense compact subset of A', so φ is surjective. A continuous bijection between compact Hausdorff spaces is a homeomorphism, so our claim follows.

Let us sketch the argument for general k. For $I \in X$ let A_i^I be the cokernel of the map $I \to A_i$. Since A_i is artinian, it surjects to $\varprojlim_I A_i^I$, and by (5.1) the ring A surjects to $\varprojlim_i \varprojlim_I A_i^I = \varprojlim_I \varprojlim_i A_i^I$. Since I is open we have $\varprojlim_i A_i^I = A/I$, and it follows that φ is surjective. In the same way one shows that the image in A' of any open ideal $\mathfrak{a}$ of A is $\varprojlim_I (\mathfrak{a}+I)/I$, which is open in A' because by (5.1) it is the kernel of the continuous map from A' to the discrete ring $\varprojlim_I A/(\mathfrak{a}+I)$. Thus, φ is an open map, and the map $A/F \to A'$ is a homeomorphism.

(5.3) Proposition. *The following two statements are equivalent:*

(1) *A is noetherian;*
(2) $\dim_k(\mathfrak{m}_i/\mathfrak{m}_i^2)$ *is a bounded function of i.*

If they hold, then the following are also true:

(3) $\mathfrak{m}^a = \varprojlim \mathfrak{m}_i^a$ *for all $a \geq 0$;*
(4) *the topology on A is the $\mathfrak{m}$-adic topology.*

This proposition implies (2.4). To obtain the last statement of (2.4), write $A' = \varprojlim A_i'$ with A_i' artinian and note that for each i the map $A \to A' \to A_i'$ is continuous in the $\mathfrak{m}$-adic topology on A. We already used this argument to show (2.5) in the case that G is finite.

Proof. Suppose that A is noetherian. Then $\mathfrak{m}$ can be generated as an A-ideal by a finite number d of elements of $\mathfrak{m}$. Since $\mathfrak{m}$ surjects to $\mathfrak{m}_i$ we have $\dim_k(\mathfrak{m}_i/\mathfrak{m}_i^2) \leq d$ for each i, so (1) implies (2).

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Now assume that (2) holds. We need to show (1), (3) and (4). We start with (3). The statement is trivial for $a = 0$, and we will proceed by induction on a. Assume (3) holds for a and consider the sequence of projective systems

$$0 \longrightarrow \mathfrak{m}_i^{a+1} \longrightarrow \mathfrak{m}_i^a \longrightarrow \mathfrak{m}_i^a/\mathfrak{m}_i^{a+1} \longrightarrow 0.$$

Assumption (2) implies that $\mathfrak{m}_i^a/\mathfrak{m}_i^{a+1}$ also has bounded dimension, so the system on the right stabilizes, i.e., all transition maps for $j \geq i$ are isomorphisms if i is large enough. This implies that its limit is a finite dimensional k-vector space N. By (5.1) and the induction hypothesis we have a short exact sequence

$$(*) \qquad 0 \longrightarrow \varprojlim_i \mathfrak{m}_i^{a+1} \longrightarrow \mathfrak{m}^a \longrightarrow N \longrightarrow 0.$$

Choose elements $b_1, \ldots, b_l$ of $\mathfrak{m}^a$ whose images in N form a basis of N over k. For each i we have a surjection $A_i^l \to \mathfrak{m}_i^a$, sending $(x_1, \ldots, x_l)$ to $x_1 b_1 + \cdots + x_l b_l$. Taking limits we deduce from (5.1) and the induction hypothesis that $\mathfrak{m}^a$ is generated by $b_1, \ldots, b_l$ as an A-ideal. We now have $l \geq \dim_k(\mathfrak{m}^a/\mathfrak{m}^{a+1}) \geq \dim_k(N) = l$, so $\mathfrak{m}^{a+1}$ is equal to the kernel of the map $\mathfrak{m}^a \to N$. By the sequence $(*)$ above, this gives the induction step. This shows (3).

Applying (5.1) to the sequence

$$0 \longrightarrow \mathfrak{m}_i^a \longrightarrow A_i \longrightarrow A_i/\mathfrak{m}_i^a \longrightarrow 0$$

and using (3) we get $A/\mathfrak{m}^a = \varprojlim A_i/\mathfrak{m}_i^a$. Again with (2) one sees that this system stabilizes. But this means that the map $A \to A/\mathfrak{m}^a$ factors through A_i for some i, so that $\mathfrak{m}^a$ is open in A. We already mentioned in Section 4 that the $\mathfrak{m}$-adic topology on a ring in $\mathcal{C}$ is at least as strong as the given topology, so in this case the two topologies coincide. This shows (4).

We now know that A is $\mathfrak{m}$-adically complete, and that $\mathfrak{m}$ is a finitely generated A-ideal. To prove that A is noetherian we use a standard argument, which also goes into the proof that a completion of a noetherian ring is noetherian. The graded ring $\mathrm{G}(A) = \bigoplus_{m \geq 0} \mathfrak{m}^m/\mathfrak{m}^{m+1}$ is a finitely generated k-algebra, which is noetherian by Hilbert's basis theorem. By [1, (10.25)] this implies that A is noetherian. This shows (1). □

Proof of part (3) of (2.3). We consider deformations of V in the ring $A = k[\epsilon]$ with $\epsilon^2 = 0$. Write R as a projective limit of its discrete artinian quotients R_i. Let $\mathfrak{m}_i$ be the maximal ideal of R_i. One easily sees that

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(R, k[\epsilon]) &= \varinjlim_i \mathrm{Hom}_{\mathcal{O}\text{-Alg}}(R_i, k[\epsilon]) \\ &= \varinjlim_i \mathrm{Hom}_k(\mathfrak{m}_i/(\mathfrak{m}_i^2 + \mathfrak{m}_{\mathcal{O}} R_i), k). \end{aligned}$$

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Let us denote the rightmost set by T, and note that T is a vector space over k. Recall that $\mathcal{O}$ is noetherian, so that the k-dimension d of $\mathfrak{m}_{\mathcal{O}}/\mathfrak{m}_{\mathcal{O}}^2$ is finite. Clearly $\dim_k(\mathfrak{m}_i/(\mathfrak{m}_i^2+\mathfrak{m}_{\mathcal{O}}R_i))$ and $\dim_k(\mathfrak{m}_i/\mathfrak{m}_i^2)$ differ by at most d. Since the transition maps in the injective limit are injective, the dimension of T is finite if and only if the dimension of $\mathfrak{m}_i/\mathfrak{m}_i^2$ is bounded, which by (5.3) is equivalent to R being noetherian.

By part (1) of (2.3) the set $\mathrm{Def}(V,k[\epsilon])$ can be identified with T, so after choosing a basis of V over k one gets a surjection

$$\mathrm{CHom}_{\overline{\rho}}(G,\mathrm{GL}_n(k[\epsilon]))\to T.$$

We have $\mathrm{GL}_n(k[\epsilon])=\mathrm{GL}_n(k)\oplus M_n(k)\epsilon$, and one easily checks that the homomorphisms on the left are exactly the maps $g\mapsto(1+c(g)\epsilon)\overline{\rho}(g)$ for which $c\colon G\to M_n(k)$ is a continuous 1-cocycle. Moreover, it follows from (4.1) that two 1-cocycles give the same deformation in $k[\epsilon]$ if and only if they differ by a coboundary, so that we get a bijection $H^1(G,\mathrm{End}_k(V))\xrightarrow{\sim}T$. In the case that k is finite, statement (3) follows at once. For the general case one checks that this bijection is k-linear, so that the same conclusion holds. □

6. Restrictions on deformations

In this section a class of additional properties of deformations is identified for which one gets a representable sub-functor of the deformation functor.

Suppose that for each ring A in $\mathcal{C}$ a subset $S(A)$ of $\mathrm{Def}(V,A)$ is given such that for each A in $\mathcal{C}$ and $D\in\mathrm{Def}(V,A)$ the following hold:

(1) we have $D\in S(A)$ if and only if $D/\mathfrak{a}D\in S(A/\mathfrak{a})$ for all open ideals $\mathfrak{a}\neq A$ in A;
(2) if $\mathfrak{a}$ and $\mathfrak{b}$ are open ideals $\neq A$ of A such that $D/\mathfrak{a}D\in S(A/\mathfrak{a})$ and $D/\mathfrak{b}D\in S(A/\mathfrak{b})$, then $D/(\mathfrak{a}\cap\mathfrak{b})D\in S(A/(\mathfrak{a}\cap\mathfrak{b}))$;
(3) if $A\subset A'$ is an inclusion of artinian rings in $\mathcal{C}$, then $D\in S(A)$ if and only if $D\otimes_A A'\in S(A')$.

(6.1) Proposition. *For any $\mathcal{C}$-morphism $f\colon A\to A'$ we have $f_*(S(A))\subset S(A')$. If V is absolutely irreducible, then there is a closed ideal $\mathfrak{a}$ of the universal deformation ring R such that the map* $\mathrm{Hom}_{\mathcal{C}}(R,A)\xrightarrow{\sim}\mathrm{Def}(V,A)$ *in* (2.3) *induces a bijection* $\mathrm{Hom}_{\mathcal{C}}(R/\mathfrak{a},A)\xrightarrow{\sim}S(A)$.

Proof. Let A be a ring in $\mathcal{C}$ and $D\in\mathrm{Def}(V,A)$. Using (5.2) one deduces from conditions (1) and (2) above that there is a unique closed ideal $\mathfrak{a}_S^D$ of A such that for every open ideal $\mathfrak{a}$ of A we have $D/\mathfrak{a}D\in S(A/\mathfrak{a})$ if and only $\mathfrak{a}\supset\mathfrak{a}_S^D$. By condition (1) we have $D\in S(A)$ if and only if $\mathfrak{a}_S^D=0$.

Now let $f\colon A\to A'$ be a $\mathcal{C}$-morphism and put $D'=D\otimes_A A'$, where the tensor product is taken via f. Let $\mathfrak{a}'$ be an open A'-ideal and write $\mathfrak{a}=f^{-1}(\mathfrak{a}')$. By condition (3) we have $D'/\mathfrak{a}'D'\in S(A'/\mathfrak{a}')$ if and only if $D/\mathfrak{a}D\in S(A/\mathfrak{a})$. Therefore, $\mathfrak{a}_S^{D'}\subset\mathfrak{a}'$ if and only if $f(\mathfrak{a}_S^D)\subset\mathfrak{a}'$. In particular, $D'\in S(A')$ if and only if $\mathrm{Ker}\,f$ contains $\mathfrak{a}_S^D$.

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

The first statement of the proposition now follows at once, and by taking $\mathfrak{a} = \mathfrak{a}_S^D \subset R$, where D is the universal deformation, we obtain the second statement. □

(6.2) Ordinary deformations. Suppose that I is a closed subgroup of G. A 2-dimensional representation W of G over a ring A in $\mathcal{C}$ is said to be *ordinary* if the sub-A-module W^I of I-invariants is a direct summand of W of A-rank 1 (cf. [8, 1.7]). Suppose that V is 2-dimensional, absolutely irreducible, and ordinary. We want to show that the ordinary deformations form a representable functor on $\mathcal{C}$.

Using the fact that V is ordinary one can see that $D \in \mathrm{Def}(V, A)$ is ordinary if and only if the I-action on D is given by matrices $\left(\begin{smallmatrix}1 & * \\ 0 & *\end{smallmatrix}\right)$ on a suitable A-basis of D, and if and only if D^I contains an element z not mapping to 0 in V. Now choose an element $g_0 \in I$ that does not act trivially on V. Then one checks that D is ordinary if and only if D is annihilated by the elements $(g-1)(g_0 - \det_D(g_0)) \in A[G]$ with $g \in I$ (for the if-part, choose $z = (g_0 - \det_D(g_0))y$ for suitable y). It is easy to verify that conditions (1)–(3) hold for this latter property.

(6.3) Flat deformations. Assume that k is a finite field of characteristic p. Let K be finite field extension of the field $\mathbb{Q}_p$ of p-adic numbers, let $\mathcal{O}_K$ be its ring of integers, and let $G = \mathrm{Gal}(\overline{K}/K)$, where $\overline{K}$ is an algebraic closure of K. We say that a $\mathbb{Z}[G]$-module of finite cardinality is *flat* if it is G-isomorphic to the group of points in $\overline{K}$ of a finite flat group scheme over $\mathcal{O}_K$. The flatness property is preserved under passing to finite products, submodules, and quotients [11; 4]. Let us sketch the argument. For products it is clear. Suppose that $X' \subset X$ are $\mathbb{Z}[G]$-modules and that $X = \mathcal{G}(\overline{K})$ for a finite flat group scheme $\mathcal{G} = \operatorname{Spec} A$ over $\mathcal{O}_K$. Let I be the kernel of the map $A \to \prod_{x \in X'} \overline{K}$. The comultiplication $m^*\colon A \to A \otimes A$ induces a comultiplication on $A' = A/I$ and on $A'' = \{x \in A\colon m^*(x) \equiv x \otimes 1 \bmod A \otimes I\}$. Then $\mathcal{G}' = \operatorname{Spec} A'$ and $\mathcal{G}'' = \operatorname{Spec} A''$ are finite flat group schemes over $\mathcal{O}_K$ and one checks that $\mathcal{G}'(\overline{K}) \cong X'$ and $\mathcal{G}''(\overline{K}) \cong X/X'$.

A deformation of V in an artinian ring A in $\mathcal{C}$ is said to be flat if it is flat as a $\mathbb{Z}[G]$-module. Use condition (1) to define flatness for deformations to arbitrary rings A in $\mathcal{C}$. Then one easily checks (2) and (3). For (3) one notes that D' contains D as a sub-$\mathbb{Z}[G]$-module, and that D' is a quotient of a finite product of copies of D. Thus, the flat deformation functor on $\mathcal{C}$ is representable if V is absolutely irreducible and flat.

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

7. Relaxing the absolute irreducibility condition

In this section we will show that our main result already holds when $\mathrm{End}_{k[G]}(V) = k$. We saw in Section 4 that this is a weaker condition on V than absolute irreducibility. This improved result will not be needed in the rest of this book.

(7.1) Proposition. *If* $\mathrm{End}_{k[G]}(V) = k$ *then statements* (1)–(4) *of* (2.3) *hold.*

Proof. We will use the same construction as before, but we need to pass to a different subring of R_b: we may need more elements than the traces of the actions of the group elements. In order to describe a suitable set of elements we explain Faltings's notion of "well-placed" representations.

We choose a basis for V over k, so that the G-action on V is given by a continuous group homomorphism $\overline{\rho}\colon G \to \mathrm{GL}_n(k)$. Since $M_n(k)$ is finite-dimensional over k, we can choose a finite number of elements $g_1, \ldots, g_r$ in G such that the only matrices in $M_n(k)$ commuting with all $\overline{\rho}(g_i)$ are the scalar matrices. Let a lift $E_i \in M_n(\mathcal{O})$ of each $\overline{\rho}(g_i)$ be chosen. For any ring A in $\mathcal{C}$ we let $M_n^0(A)$ be the matrix ring $M_n(A)$ modulo scalars; this is a free A-module of rank n^2-1. By Nakayama's lemma one sees that we have a split injection $i_A\colon M_n^0(A) \to M_n(A)^r$ given by $M \mapsto (ME_i - E_iM)_{i=1}^r$. We now choose a splitting $\pi_{\mathcal{O}}$ of $i_{\mathcal{O}}$ once and for all. We have a canonical isomorphism $M_n^0(A) \cong M_n^0(\mathcal{O}) \otimes_{\mathcal{O}} A$, and $\pi_A = \pi_{\mathcal{O}} \otimes \mathrm{id}_A$ is a splitting of i_A. Consider the composite map

$$(7.2) \qquad \begin{array}{ccccc} \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A)) & \longrightarrow & M_n(A)^r & \xrightarrow{\pi_A} & M_n^0(A). \\ \rho & \mapsto & (\rho(g_i))_{i=1}^r & & \end{array}$$

We say that ρ is *well-placed* if its image in $M_n^0(A)$ is $\pi_{\mathcal{O}}(E_1, \ldots, E_r) \otimes 1$.

(7.3) Lemma (Faltings). *For every* $\rho \in \mathrm{CHom}_{\overline{\rho}}(G, \mathrm{GL}_n(A))$ *there is a matrix* $M \in \mathrm{GL}_n(A)$ *reducing to* $1 \in \mathrm{GL}_n(k)$ *so that* $M\rho M^{-1}$ *is well-placed. This matrix* M *is determined uniquely modulo* $1 + \mathfrak{m}_A$.

Proof. Put $\mathfrak{m} = \mathfrak{m}_A$. By induction on m we first show the lemma under the hypothesis that $\mathfrak{m}^m = 0$. For $m = 1$ this is clear. To make the induction step for $m \geq 2$ we can assume by the induction hypothesis that ρ is well-placed modulo $\mathfrak{m}^{m-1}$. We are done if we show that $(1+M)\rho(1+M)^{-1}$ is well-placed for a unique $M \in M_n^0(\mathfrak{m}^{m-1}) = \mathfrak{m}^{m-1}M_n^0(A)$, and this follows from the fact that the maps in (7.2) respect suitable actions of $M_n^0(\mathfrak{m}^{m-1})$: we let $M \in M_n^0(\mathfrak{m}^{m-1})$ act by conjugation with $1+M$ on the leftmost set, by translation with $i_A(M)$ on the middle group, and by translation with M on $M_n^0(A)$.

To obtain the general case one refines the conjugating matrix modulo increasing powers of $\mathfrak{m}$ (recall that an $\mathfrak{m}$-adic Cauchy sequence in A converges to a unique limit in A even if A has a coarser topology). □

pp. 313–326 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

We apply the lemma to the deformation ρ_b of Proposition (2.5), and we let ρ be the well-placed conjugate of ρ_b. Define R to be the smallest closed sub-$\mathcal{O}$-algebra of R_b that contains all entries of $\rho(g)$ for all $g \in G$. Then ρ defines a deformation D of V in R, and we claim that properties (1)–(4) of Theorem (2.3) now hold. The map $\mathrm{Hom}_{\mathcal{C}}(R, A) \to \mathrm{Def}(V, A)$ in (1) is again surjective. To see injectivity, suppose that for $f_1, f_2 \in \mathrm{Hom}_{\mathcal{C}}(R, A)$ the well-placed composite maps

$$\rho_1, \rho_2\colon G \xrightarrow{\rho} \mathrm{GL}_n(R) \xrightarrow{f_1, f_2} \mathrm{GL}_n(A)$$

give the same deformation of V in A. By the argument of (4.1) together with the uniqueness statement in (7.3) it follows that $\rho_1 = \rho_2$, and by the definition of R this implies that $f_1 = f_2$. The proofs of (2) and (4) are as before. For (3) we just remark that the argument at the end of Section 5 showing that $H^1(G, \mathrm{End}_k(V)) \cong T$, only uses that $\mathrm{End}_{k[G]}(V) = k$. This proves (7.1). □

References

1. M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.
2. N. Bourbaki, *Théorie des ensembles*, Hermann, Paris, 1970.
3. H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, pp. 213–237 in: B. Mazur and G. Stevens (eds), *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture*, Contemp. Math. **165**, Amer. Math. Soc., Providence, 1994.
4. B. Conrad, *The flat deformation functor*, Chapter XIV in this volume.
5. H. Darmon, F. Diamond, and R. Taylor, *Fermat's Last Theorem*, pp. 1–107 in: R. Bott, A. Jaffe, and S. T. Yau (eds), *Current developments in mathematics, 1995*, International Press, Cambridge, Mass., 1995.
6. A. Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique, II*, Sém. Bourbaki **12** (1959/60), n° 195.
7. S. Lang, *Algebra*, 3rd ed., Addison-Wesley, Reading, Mass., 1993.
8. B. Mazur, *Deforming Galois representations*, pp. 385–437 in: Y. Ihara, K. Ribet, and J-P. Serre (eds), *Galois groups over* $\mathbb{Q}$, MSRI Publications **16**, Springer-Verlag, New York, 1989.
9. C. Procesi, *Rings with polynomial identities*, Marcel Dekker, New York, 1973.
10. C. Procesi, *Deformations of representations*, preprint, December 1995.
11. R. Ramakrishna, *On a variation of Mazur's deformation functor*, Compositio Math. **87** (1993), 269–286.
12. M. Schlessinger, *Functors of Artin rings*, Trans. Amer. Math. Soc. **130** (1968), 208–222.
13. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. (2) **141** (1995), 443–551.