UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL ATOMIC ENERGY AGENCY
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.1004/12

SUMMER SCHOOL ON ELLIPTIC CURVES

(11- 29 August 1997)

Deformations of Galois Representations

G. Böckle
Institute for Experimental Mathematics
University of Essen
Ellernstrasse 29
D-45326 Essen
Germany

These are preliminary lecture notes, intended only for distribution to participants

MAIN BUILDING STRADA COSTIERA, 11 TEL. 2240111 TELEFAX 224163 TELEX 460392 ADRIATICO GUEST HOUSE VIA GRIGNANO, 9 TEL. 224241 TELEFAX 224531 TELEX 460449
MICROPROCESSOR LAB. VIA BEIRUT, 31 TEL. 2249911 TELEFAX 224600 TELEX 460392 GALILEO GUEST HOUSE VIA BEIRUT, 7 TEL. 2240311 TELEFAX 2240310 TELEX 460392
ENRICO FERMI BUILDING VIA BEIRUT, 6 (TELEPHONE, FAX AND TELEX THROUGH MAIN BUILDING)

Deformations of Galois Representations

Gebhard Böckle

August 27, 1997

Introduction

The goal here will be to give an introduction to the theory of deformations of Galois representations. In the first part we shall discuss some conjectures of Gouvêa and Mazur concerning families of modular forms and congruences and their consequences. Then we shall explain the transition from modular forms to Galois representations. The next step is to introduce the concept of a deformation of a given Galois representation. Families of modular forms satisfying congruences can then be naturally interpreted in this context.

As a starting point for our own investigations we shall state a main theorem in the subject, namely the existence of a universal deformation space. The main goal will be to discuss conjectures and properties of the universal deformation space. Our main theorem will discuss ring-theoretic properties of it, namely we will give fairly general conditions under which the underlying ring is flat over $\mathbb{Z}_p$, a complete intersection and of relative dimension three, or respectively more general conditions under which the ring modulo p is a complete intersection of Krull dimension three. In order to establish this, we shall state a local-to-global theorem for deformations and discuss local deformation functors.

1 Families of modular forms (and congruences)

A reference for this and for further details is [GoMa1]. We fix levels $N \geq 1$ and Np where N and p are relatively prime, and p is a prime, $p > 2$. By k we shall denote weights of spaces of modular forms, by L an extension of $\mathbb{Q}_p$ inside $\mathbb{C}_p$. We fix a valuation v on $\mathbb{C}_p$ such that $v(p) = 1$. For such an L we define

$$S_k(L) := S_k(\Gamma_0(Np), \mathbb{Q}) \otimes_{\mathbb{Q}} L.$$

We will now decompose this space in p-old and p-new forms,

$$S_k(L) = S_k(L)^{p-old} \oplus S_k(L)^{p-new}.$$

The space $S_k(K)^{p-old}$ is defined to be the span of the image of $S_k(\Gamma_0(N), L)$ under the maps B_1^* and B_p^*, i.e. sending $f = \sum a_n q^n \in S_k(\Gamma_0(N), L)$ to itself inside $S_k(L)$, or to $\sum a_n q^{pn}$ inside $S_k(L)$. This can all be done over $\mathbb{Q}$, and so the space S_k^{p-new} could be defined as the orthogonal complement via the Petersson inner product. Equivalently, and this avoids the analytic structure, we define it to be the subspace inside $S_k(L)$ that is in the $\bar{\mathbb{Q}}_p$ linear span of the eigenforms of $S_k(\bar{\mathbb{Q}}_p)$ that satisfy $f = -p^{1-k/2} T_{p,Np} W_p f$. Here W_p denotes the Atkin-Lehner involution and the index p, Np of the Hecke operator means that we consider the operator T_p acting on $S_k(\Gamma_0(Np), L)$, in order to distinguish it from the operator T_p acting on $S_k(\Gamma_0(N), L)$ which we denote by $T_{p,N}$.

1.1 DEFINITION. For a normalized eigenform $f \in S_k(\mathbb{C}_p)$, we define the slope of f to be

$$\alpha(f) := v(a_p(f)),$$

$a_p(f)$ being the p-th Fourier coefficient of f.

We now have the following easy proposition concerning slopes.

1.2 PROPOSITION. *Let f be a normalized eigenform in $S_k(\mathbb{C}_p)$. Then $\alpha(f) \geq 0$ and we have the following cases.*

(i) f is p-old. Then there exists a unique twin $\tilde{f}$, i.e. a p-old form that satisfies $a_q(f) = a_q(\tilde{f})$ for all primes $q \neq p$, such that $\alpha(f) + \alpha(\tilde{f}) = k-1$. In particular $\alpha(f) \in [0, k-1]$.

(ii) f is p-new. Then $\alpha(f) = k/2 - 1$.

PROOF: Part (ii) simply follows from our above characterisation of p-new eigenforms, on observing that for such forms $W_p f = \pm f$.

To see (i), note that as f is p-old, there is a unique oldform g, an eigenform, such that $a_q(g) = a_q(f)$ for all primes $q \neq p$ and such that f is in the span of $B_1^* g$ and $B_p^* g$. If $g = \sum a_n q^n$, then the two forms are given by $\sum a_n q^n$ and $\sum a_n q^{pn}$. It is easy to see that the Hecke operator $T_{p,Np}$ on the span of these two forms is given as

$$T_{p,Np} = \begin{pmatrix} T_{p,N} & -p^{k-1} \\ 1 & 0 \end{pmatrix}.$$

Diagonalizing this and calculating the corresponding eigenvectors and eigenvalues, gives f and its twin and their respective p-th Fourier coefficients. ∎

We can now state a conjecture of Gouvêa and Mazur - for more conjectures and examples see [GoMa1].

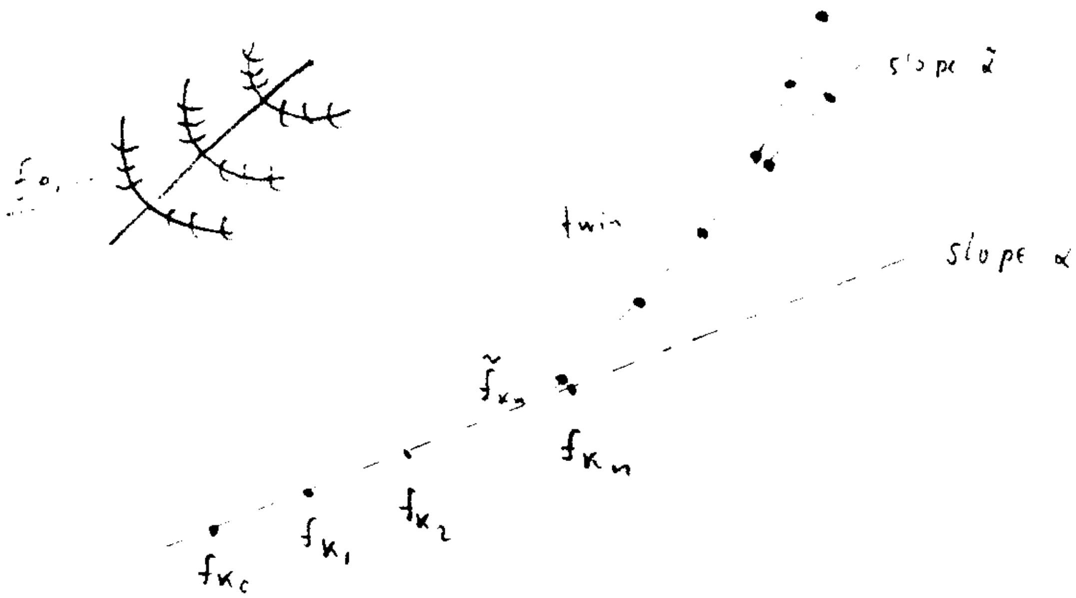
1.3 CONJECTURE. Suppose for some k_0 and some α such that $0 \leq \alpha < k_0 - 1$ there exists a unique normalized eigenform $f_{k_0} \in S_k(\bar{\mathbb{Q}}_p)$ of slope α. Then there exists an integer $n \geq \alpha$ and an arithmetic progression $\mathcal{K} = \{k_0 + mp^n(p-1) : m \in \mathbb{N}_0\}$ such that in each of the spaces $S_k(\bar{\mathbb{Q}}_p)$ there is a unique normalized eigenform f_k of slope α. Furthermore the functions f_k satisfy

$$f_k \equiv f_{k_0} \pmod{p^{n+1}},$$

i.e. $a_q(f) \equiv a_q(f_{k_0}) \pmod{p^{n+1}}$ for all $k \in \mathcal{K}$ and primes q.

If we assume the conjecture, and if we are given f_{k_0} as in it of slope α, we can construct the following 'fern' of eigenforms congruent modulo p^{n_0+1} where n_0 is the least integer greater as α.

First there is the arithmetic progression of slope α, $f_{k_0}, f_{k_1}, f_{k_2}, \ldots$. We follow it, say to f_{k_n} where $k_n/2 - 1 > \alpha$. At this point we must have a p-oldform by the above proposition - for p-newforms one must have $k_n/2 - 1 = \alpha$. So there is a twin $\tilde{f}_{k_n}$ of slope $\tilde{\alpha} = k - 1 - \alpha > \alpha$. But then we can use it to start a new family. We can move along this family and then do the same thing again, etc. So we constructed a huge family of modular forms f for which we have $a_q(f) \equiv a_q(f_{k_0})$ modulo p^{n_0+1} for all $q \neq p$. Translating this to the associated Galois representation will make the congruences even nicer!



2 From modular forms to Galois Representations

Let f be a normalized eigenform in $S_k(L)$, where $L/\mathbb{Q}_p$ is finite. $\mathcal{O}_L$ shall denote its ring of integers, π_L a uniformizing parameter. One has the following theorem due to Eichler, Shimura, Deligne and Serre.

2.1 THEOREM. *For any normalized eigenform $f \in S_k(L)$ there is a unique representation $\rho_f : G_{\mathbb{Q},S} \to \mathrm{GL}_2(L)$, where S is the set of all places of $\mathbb{Q}$ dividing Np enlarged by infinity, $G_{\mathbb{Q},S}$ is the Galois group of the maximal outside S unramified extension of $\mathbb{Q}$, and ρ_f satisfies*

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_q)) = a_q(f) \quad \forall q \not| Np \tag{1}$$

$$\det(\rho_f(\mathrm{Frob}_q)) = q^{k-1} = \chi_p^{k-1}(q) \quad \forall q \not| Np. \tag{2}$$

Note that this means that the representation is unramified outside S. Also note that ρ_f applied to any complex conjugation in $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ gives a matrix conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. We call such representations odd.

It is possible to choose an $\mathcal{O}_L$ lattice in L^2 stable under the Galois action, so that one has up to base change a representation $\rho_f : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_L)$, and by reduction modulo π_L, if we denote $\mathcal{O}_L/\pi_L$ by $\mathbf{F}$, a representation $\bar{\rho}_f : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbf{F})$. If $\bar{\rho}_f$

is absolutely irreducible, then the representation to $\mathcal{O}_L$ is unique up to isomorphism, i.e. for all Galois stable lattices one obtains the same representation. We will also denote it by ρ_f.

By the Cebotarov density theorem it is not hard to see that in fact the images of the Frobenius elements for all primes $q \not| Np$ determine ρ_f completely in the case that $\bar{\rho}_f$ is absolutely irreducible. So now we can interprete the fern construction in a different way. We assume that f_{k_0} is as in the fern construction and that further $\bar{\rho}_{f_{k_0}}$ is absolutely irreducible. Then each element f in the fern gives rise to a $\rho_f : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ and so that all the representations agree modulo p^{n_0+1}! This motivates the definition of a deformation in the following section.

3 A good environment to grow ferns

We assume that we are given the following data, S a finite set of places of $\mathbb{Q}$ containing $\{p, \infty\}$, $\mathbf{F}$ a finite field of characteristic p, $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbf{F})$ an odd absolutely irreducible Galois representation, $W(\mathbf{F})$ the ring of Witt vectors of $\mathbf{F}$.

Let $\mathcal{C}$ be the category of complete noetherian local $W(\mathbf{F})$-algebras $(R, \mathfrak{m}_R)$ with a given surjective map $R \to \mathbf{F}$, and where the homomorphisms are local homomorphisms that induce the identity on $\mathbf{F}$. We define the following functor.

3.1 DEFINITION.

$$\mathrm{Def}_{\bar{\rho},S} : \mathcal{C} \to (Sets) : R \mapsto \{\text{lifts } \rho : G_{\mathbb{Q},S} \to \mathrm{GL}_2(R) \text{ of } \bar{\rho}\}/\cong$$

where $\cong$ stands for strict equivalence. We say that two lifts ρ, ρ' are strictly equivalent iff there exists an M in the kernel of the map from $\mathrm{GL}_2(R)$ to $\mathrm{GL}_2(\mathbf{F})$ such that $\rho = M^{-1}\rho' M$. We call the elements in $\mathrm{Def}_{\bar{\rho},S}(R)$ deformations from of $\bar{\rho}$ to R.

We note that one can make this definition under much more general assumptions over arbitrary number fields instead of $\mathbb{Q}$ and without the assumption that $\bar{\rho}$ is odd, or absolutely irreducible.

The following will be crucial for the investigations to come.

3.2 THEOREM. *Under the assumptions made in this section, the functor* $\mathrm{Def}_{\bar{\rho},S}$ *is representable. By* $([\rho_S], R_S)$ *we shall denote a pair representing it, in particular this means that* $\rho_S : G_{\mathbb{Q},S} \to \mathrm{GL}_2(R_S)$.

Again we note that this can be done much more generally. The main hypothesis is that the centralizer of the image of $\bar{\rho}$ in $\mathrm{GL}_2(\mathbf{F})$ is the set of homotethies. This is clearly satisfied if $\bar{\rho}$ is absolutely irreducible.

We apply this to the case where $\bar{\rho} = \bar{\rho}_{f_{k_0}}$ is as in the previous section, generating a fern. Then any f in the fern gives rise to a representation $\rho_f \in \mathrm{Def}_{\bar{\rho},S}(\bar{\mathbb{Q}}_p)$. Note that as the representations are all congruent to each other certainly modulo p, one can always take the same residue field $\mathbf{F}$. Also

$$\mathrm{Def}_{\bar{\rho},S}(\bar{\mathbb{Q}}_p) \cong Hom_{W(\mathbf{F})\text{-algebras}}(R_S, \bar{\mathbb{Q}}_p) \cong \text{closed points of } \mathrm{Spec}(R_S[1/p]).$$

and so the modular points correspond to prime ideals of R_S, i.e. elements of $\mathrm{Spec}(R_S)$.

Using recent results of Coleman and the infinite fern construction Gouvêa and Mazur were able to prove the following [GoMa2].

3.3 THEOREM. *If f is as the f_{k_0} in the fern construction, if $\rho = \bar{\rho}_f$ is absolutely irreducible, $N = 1$, $S = \{p, \infty\}$ and $\mathrm{Def}_{\bar{\rho},S}$ is unobstructed - which we will define below -, then the set of modular points is Zariski dense in Spec(R_S), where $R_S \cong W(\mathbf{F})[[X_1, X_2, X_3]]$.*

Furthermore they show that the above R_S can be viewed naturally as a certain Hecke algebra.

We will now turn the attention to properties of R_S which is our main interest of study.

4 Properties of R_S

We assume that we are given $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbf{F})$ as at the beginning of the previous section.

A The basic theorem and conjecture

We define $\mathrm{ad}_{\bar{\rho}}$ as the representation of $G_{\mathbb{Q},S}$ on $M_2(\mathbf{F})$ defined as the composite of $\bar{\rho}$ with the conjugation action of $\mathrm{GL}_2(\mathbf{F})$ on $M_2(\mathbf{F})$. $\mathrm{ad}^0_{\bar{\rho}}$ is the subrepresentation on trace zero matrices.

We define $\delta^i = \dim_{\mathbf{F}} H^i(G_{\mathbb{Q},S}, \mathrm{ad}_{\bar{\rho}})$. Note that the δ^i depend on S. We call $\bar{\rho}$ unobstructed (for S) if $\delta^2 = 0$.

4.1 THEOREM. *In all cases one has a presentation*

$$0 \to \bar{I} \to \mathbf{F}[[X_1, \ldots, X_{\delta^1}]] \to R_S/(p) \to 0$$

where $\bar{I}$ is generated by at most δ^2 elements, and $\delta^1 - \delta^2 = 3$.

If $\bar{\rho}$ is unobstructed, then $R_S \cong W(\mathbf{F})[[X_1, X_2, X_3]]$.

If $\bar{\rho}$ is tame, i.e. the order of the image of $\bar{\rho}$ is not divisible by p, then on has a presentation

$$0 \to I \to W(\mathbf{F})[[X_1, \ldots, X_{\delta_{S,1}}]] \to R_S \to 0$$

where I is generated by at most δ^2 elements.

The first two claims are shown in [Maz1], the third one follows from the material presented below and can be found in [Boe2].

We now want to discuss the following conjecture by Mazur

4.2 CONJECTURE. $R_S/(p)$ is flat over $W(\mathbf{F})$, and dim $R_S/(p) = 3$.

What we shall prove is the following theorem, which in some cases has been sketched by Mazur in [Maz2, Maz3] and a full prove is given in [Boe3].

4.3 THEOREM. *If $\bar{\rho}$ is ordinary - to be defined below -, and if $\bar{\rho}$ is modular, i.e. equal to some $\bar{\rho}_f$ for some cusp eigenform f, then*

(i) If $\bar{\rho}$ is tame, then R_S is flat over $W(\mathbf{F})$, of relative dimension three and a complete intersection.

(ii) If $\det(\bar{\rho})$ is ramified at p, then $\dim R_S/(p) = 3$.

B Fixing the determinant

In a first step, we decompose R_S by splitting off the part that is related to the determinant, i.e. to abelian representations and thus to class field theory.

We suppose that we are given $\rho_0 \in \mathrm{Def}_{\bar{\rho},S}(W(\mathbf{F}))$ (or $\rho_0 \in \mathrm{Def}_{\bar{\rho},S}(K)$, K a finite totally ramified extension of $W(\mathbf{F})$), and define $\eta = \det(\rho_0)$. Note that if $\bar{\rho}$ is tame, then such a ρ_0 always exists. We can define a functor $\mathrm{Def}^{\eta}_{\bar{\rho},S}$ by

$$\mathrm{Def}^{\eta}_{\bar{\rho},S}(R) = \{[\rho] \in \mathrm{Def}_{\bar{\rho},S}(R) : \det(\rho) = \eta\}.$$

4.4 PROPOSITION. *$\mathrm{Def}^{\eta}_{\bar{\rho},S}$ is again representable. If the representing ring is called R^{η}_S, then one has*

$$R_S \cong R^{\eta}_S \hat{\otimes} W(\mathbf{F})[[\Gamma^{ab}_S]].$$

Here Γ^{ab}_S is the Galois group of the maximal abelian pro-p extension of $\mathbb{Q}$ unramified outside S, and from class field theory it follows easily that $W(\mathbf{F})[[\Gamma^{ab}_S]]$ is finite flat over some appropriately defined $W(\mathbf{F})[[X]]$.

We note that this decomposition may seem unnatural if one thinks of modular forms, as fixing the determinant means that one fixes the weight and hence one should expect at most a finite set of modular forms for given weight. Yet for our deformation theoretic studies this decomposition is well-suited.

C Ordinary deformations

Next we define ordinary representations.

4.5 DEFINITION. A representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ for $R \in \mathcal{C}$ is called ordinary if the restriction of $\rho|_{I_p}$, I_p a chosen inertia group at p, can be conjugated to lie inside the set of matrices of the type $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, and if further $(\rho \pmod{\mathfrak{m}_R})|_{I_p}$ is not the trivial representation.

If $\bar{\rho}$ is ordinary, we can define a deformation functor for ordinary deformations (and for ordinary deformations with fixed determinant, if one has a ρ_0 as above). This functor is representable and the deformation ring will be called R^{ord}_S (resp. $R^{ord,\eta}_S$). The following theorem which was crucial in the proof of Fermat's last theorem can be found in [Wil], [TaWi], and [Dia].

4.6 THEOREM. *If $\bar{\rho}$ is modular, absolutely irreducible and ordinary, then $R^{ord,\eta}_S$ is finite flat over $W(\mathbf{F})$ for some appropriate η.*

D Local deformation problems

In the next step we shall consider local deformation problems, i.e. deformations of a given $\bar{\tau} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbf{F})$ where l is any prime equal to p or not. Usually $\bar{\tau}$ will be $\bar{\rho}|_{G_{\mathbb{Q}_l}}$.

We note that in any case $\bar{\tau}$ will have solvable image, and as we think of it as a restriction of $\bar{\rho}$ to $G_{\mathbb{Q}_l}$, the image will usually be rather small. So the crucial condition for the representability of the deformation functor, $C_{\mathrm{GL}_2(\mathbf{F})}(\mathrm{Im}(\tau))$ equals the set of homotethies will usually not be satisfied. This problem can be remedied by defining a slightly different local deformation functor $\tilde{\mathrm{Def}}_l$ of which one can show that there is a map $\mathrm{Def}_{\bar{\rho},S} \to \tilde{\mathrm{Def}}_l$, if $\tau = \bar{\rho}|_{G_{\mathbb{Q}_l}}$.

We indicate the definition of $\tilde{\mathrm{Def}}_l$. By U we denote the unique p-Sylow subgroup of $\mathrm{Im}(\tau)$ - it could be trivial. We let H be the quotient of $\mathrm{Im}(\tau)$ modulo U. One can show there is a section and so we shall also regard H inside $\mathrm{Im}(\tau)$. As H is prime to p, one can choose a lift of $H \subset \mathrm{Im}(\tau) \subset \mathrm{GL}_2(\mathbf{F})$ to $\mathrm{GL}_2(W(\mathbf{F}))$.

We denote by F the fixed field of $\bar{\tau}^{-1}(U)$ and by $G_F(p)$ the Galois group of the maximal pro-p extension of F. By $g_1, \ldots, g_i$ we shall denote elements of $G_F(p)$ whose images under $\bar{\tau}$ generate U as a group. We shall assume without loss of generality that U is inside the matrices of type $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, that g_1 maps to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and the other g_i to $\begin{pmatrix} 1 & x_i \\ 0 & 1 \end{pmatrix}$. Now we define

$$\begin{aligned} \tilde{\mathrm{Def}}_l(R) \quad := \quad & \{\alpha \in Hom_H(G_F(p), \Gamma_2(R)) : \alpha(g_1) \text{ has } (1,2) \text{ entry equal to } 1, \\ & \alpha(g_i) \equiv \begin{pmatrix} 1 & x_i \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{m}} \text{ for all } i\} \end{aligned}$$

The following theorem is a combination of [Bos], [Boe1] and [Boe2] for the cases $l \neq p$ and can be found in [Boe3] for the cases $l = p$. Special cases for $l = p$ were treated in [Maz2].

4.7 THEOREM. *The local functors $\tilde{\mathrm{Def}}_l$ are representable, and so are their variants $\tilde{\mathrm{Def}}_l^{\eta}$, $\tilde{\mathrm{Def}}_p^{ord}$, $\tilde{\mathrm{Def}}_p^{ord,\eta}$. The respective rings will be denoted by $R_l^?$. Furthermore one has presentations*

$$0 \to I_l \to W(\mathbf{F})[[X_1, \ldots, X_{n_l}]] \to R_l \to 1$$

where $n_l = \dim_{\mathbf{F}} H^1(G_{\mathbb{Q}_l}, \mathrm{ad}_{\bar{\tau}})$, I_l is generated by exactly $\dim_{\mathbf{F}} H^2(G_{\mathbb{Q}_l}, \mathrm{ad}_{\bar{\tau}})$ elements, and the rings R_l are finite flat over $W(\mathbf{F})$ and complete intersection. One has similar presentations for R_l^{η} with $\mathrm{ad}^0_{\bar{\tau}}$ replacing $\mathrm{ad}_{\bar{\tau}}$. Finally the kernel of the surjective map $R_p^{\eta} \to R_p^{ord,\eta}$ is generated by at most two elements.

E A local-to-global principle

The next fact we need is a local-to-global principle. Here we shall make the assumption that

$$H^2(G_{\mathbb{Q},S}, \mathrm{ad}_{\bar{\rho}}) \to \coprod_{q \in S} H^2(G_{\mathbb{Q}_l}, \mathrm{ad}_{\bar{\rho}})$$

is injective. This is not necessary and one can use auxiliary primes as in [TaWi] to overcome this problem. Under our assumption however one has the following.

4.8 THEOREM. *Let $\mathcal{O} = W(\mathbf{F})$ if $\bar\rho$ is tame and $\mathcal{O} = \mathbf{F}$ otherwise. Let*

$$\mathcal{O}[[X_1, \ldots, X_n]] \to R_S \otimes \mathcal{O}$$

be a surjection with kernel I'. Then there is a map

$$\coprod_{q \in S} W(\mathbf{F})[[X_1, \ldots, X_{n_q}]] \to \mathcal{O}[[X_1, \ldots, X_n]]$$

such that I is the ideal generated by the images of the I_q for $q \in S$. The same theorem holds for R_S^η where the numbers n_l have to be replaced by the respective numbers for R_l^η and the I_l by the ideals in a presentation for R_l^η.

This and the previous theorem prove easily the missing part in theorem 4.1.

F The proof of theorem 4.3 in the case that $\bar\rho$ is tame

By the the first fixing the determinant, it suffices to show that R_S^η is flat over $W(\mathbf{F})$ of relative dimension 2, and a complete intersection, where $\eta = \det(\rho_f)$. By theorem 4.1, adjusted to R_S^η, we have a presentation

$$0 \to I' \to W(\mathbf{F})[[X_1, \ldots, X_n]] \to R_S^\eta \to 0$$

where I' is generated by at most $n-2$ elements, call them $r_1, \ldots, r_{n-2}$ where we allow $r_i = 0$ if I' is generated by less then $n-2$ elements.

From the local considerations concerning $R_p^{ord,\eta}$ and R_p^η it is easy to see that the kernel of the surjection $R_S^\eta \to R_S^{ord,\eta}$ is generated by at most two elements, call them r_{n-1}, r_n.

By theorem 4.6, R_S^η is finite flat over $W(\mathbf{F})$. Hence the elements $r_1, \ldots, r_n$ must form a regular sequence, and by flatness of the latter ring, also the elements $r_1, \ldots, r_n, p$. So the same is true for any permutation and any subsequence, as $W(\mathbf{F})[[X_1, \ldots, X_n]]$ is local. Hence $r_1, \ldots, r_{n-2}, p$ form a regular sequence. This easily implies the result in the tame case in theorem 4.3.

4.9 REMARK. Similar results based on the work of Fujiwara, [Fuji], instead of Diamond, Taylor, Wiles can be obtained for totally odd representations over certain totally real fields instead of $\mathbb{Q}$. Also the local to global principle and the local considerations work in general for arbitrary number fields respectively local fields - though certain explicit numbers we gave will obviously differ in the general cases.

References

[Boe1] G. Böckle, *Explicit Deformations of Even Galois Representations*, accepted by Math. Nachr.

[Boe2] G. Böckle, *The generic fiber of the universal deformation space associated to a tame Galois representation*, preprint.

[Boe3] G. Böckle, *Demushkin groups with group actions and application to deformations of Galois representations*, preprint.

[Bos] N. Boston, *Explicit Deformations of Galois Representations*, Invent. Math. 103 (1990), p. 181–196.

[Dia] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. **144** (1996), 137–166.

[Fuji] K. Fujiwara *Deformation rings and Hecke algebras in the totally real case*, preprint, July 9, 1996.

[GoMa1] F. Gouvêa, B. Mazur, *Families of modular eigenforms*, Math. Comp. **58** (1992), 793–806.

[GoMa2] F. Gouvêa, B. Mazur, *On the density of modular representations*, preprint 1996.

[Maz1] B. Mazur, *Deforming Galois Representations*, in Galois Groups over $\mathbb{Q}$, Springer-Verlag 1987.

[Maz2] B. Mazur, *Two-dimensional p-adic Galois representations unramified away from p*, Comp. Math. **74** (1990), 115–133.

[Maz3] B. Mazur, *An "infinite fern" in the universal deformation space of Galois representations*, to appear in the proceedings of the *Journées Arithméthiques*, Barcelona, 1995.

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

[Wil] A. Wiles *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **142** (1995), 443–551.