The prime-to-adjoint principle and unobstructed Galois deformations in the Borel case

Gebhard BÖCKLE

Lehrstuhl für Mathematik, Prof. Pink

Universität Mannheim

D7, 27

68131 Mannheim

Germany

e-mail: boeckle@math.uni-mannheim.de

Ariane MÉZARD

Institut Fourier

UMR 5582 CNRS-UJF

B.P. 74

38402 Saint-Martin d'Hères Cedex

France

e-mail: ariane.mezard@ujf-grenoble.fr

1991 Math. subject classification : 13D10, 11R23, 11G05, 11R18.

Proposed running head: Deformations of Borel type representations

Address to which proofs should be sent:

Gebhard Böckle

Lehrstuhl für Mathematik, Prof. Pink

Universität Mannheim

D7, 27

68131 Mannheim

Germany

Abstract

For a given odd two-dimensional representation $\bar{\rho}$ over $\mathbf{F}_p$ of the absolute Galois group G_E of a totally real field E which is unramified outside a finite set of places S, Mazur defined a universal deformation ring $R_{G_S}(\bar{\rho})$. By obstruction theory, the group $Ш^2_S(E, \mathrm{ad}\bar{\rho})$ measures to what extend $R_{G_S}(\bar{\rho})$ is determined by local relations.

Using devissage on $\mathrm{ad}\bar{\rho}$, we give criteria for the vanishing of $Ш^2_S(E, \mathrm{ad}\bar{\rho})$ in terms of vanishing of S-class groups, in terms of Iwasawa invariants and in terms of special values of p-adic L-functions.

If S is the set of places above p and ∞, the condition $Ш^2_S(E, \mathrm{ad}\bar{\rho}) = 0$ implies that $R_{G_S}(\bar{\rho})$ is free of dimension $2[E : \mathbf{Q}] + 1$. In this case, we obtain a reformulation of Vandiver's conjecture and asymptotic connections between Greenberg's conjecture and the freeness of $R_{G_S}(\bar{\rho})$.

For larger S, we relate the freeness of the universal deformation ring for minimal deformations to the vanishing of a modified obstruction group $Ш^2_{S,S_p}(E, \mathrm{ad}\bar{\rho})$. Based on this, we can calculate non-free rings $R_{G_S}(\bar{\rho})$ for some explicit reducible $\bar{\rho}$ coming from the action of $G_{\mathbf{Q}}$ on p-torsion points of elliptic curves.

Key words : Galois representations, deformation theory, Vandiver's conjecture, class groups, Iwasawa theory, L-functions, elliptic curves.

1 Introduction

Let p be an odd prime number. Let $\bar{\rho} : \mathrm{Gal}(\bar{E}/E) \to \mathrm{GL}_2(\mathbf{F}_p)$ be a fixed odd continuous Galois representation, unramified outside a finite set $S(E)$ of primes of the number field E containing the set of archimedean places, the set of places above p and the set of places where $\bar{\rho}$ ramifies. Then $\bar{\rho}$ factors through $G_S(E) = \mathrm{Gal}(E_S/E)$ where E_S is the maximal extension of E unramified outside $S(E)$.

We study deformations of such representations $\bar{\rho}$ and the universal deformation ring $R_{G_S}(\bar{\rho})$ attached to this problem, as defined in [16]. There are several motivations for being interested in $R_{G_S}(\bar{\rho})$. First $R_{G_S}(\bar{\rho})$ parametrizes all deformations of $\bar{\rho}$ to complete noetherian $\mathbf{Z}_p$-algebras. Its p-torsion free components parametrize all lifts to characteristic zero. Its Krull dimension measures the wealth of deformations (for fixed $S(E)$). As remarked by Mazur in [16], the Krull dimension of $R_{G_S}(\bar{\rho})$ is related to the Leopoldt conjecture for E. Finally for $E = \mathbf{Q}$, the universal deformation ring $R_{G_S}(\bar{\rho})$ might be related to the Hecke algebra of p-adic modular forms with residual representation $\bar{\rho}$ ([10], [28], [33]).

It is a well known property –but not a thoroughly understood one– that the structure of $R_{G_S}(\bar{\rho})$ is intimately related to the $G_S(E)$-cohomology of the adjoint representation $\mathrm{ad}\bar{\rho}$ of $\bar{\rho}$. The dimension $d = \dim_{\mathbf{F}_p} H^1(G_S(E), \mathrm{ad}\bar{\rho})$ is the minimal number of generators in a presentation of $R_{G_S}(\bar{\rho}) = \mathbf{Z}_p[[T_1, \ldots, T_d]]/I$. For a minimal presentation the ideal I of relations is related by obstruction theory to $H^2(G_S(E), \mathrm{ad}\bar{\rho})$. One knows that

$$\dim_{\mathbf{F}_p} I/(I\mathfrak{m}_{\mathbf{Z}_p[[T_1,\ldots,T_d]]}) \leq \dim_{\mathbf{F}_p} H^2(G_S(E), \mathrm{ad}\bar{\rho}) \tag{1}$$

so that I vanishes whenever $H^2(G_S(E), \mathrm{ad}\bar{\rho}) = 0$. If moreover $\bar{\rho}$ is irreducible, one conjectures that equality holds in (1).

The usual local-to-global methods allow us to divide the study of $H^2(G_S(E), \mathrm{ad}\bar{\rho})$ into two parts:
- the study of the semi-local part $\oplus_{v \in S(E)} H^2(\mathrm{Gal}(\bar{E}_v/E_v), \mathrm{ad}\bar{\rho})$, which can in principle be com-

puted (see [3]) using Tate local duality,

- that of the purely global part, the localization kernel $Ш^2_S(E, \mathrm{ad}\bar{\rho})$ of the Tate-Poitou sequence, which can be considered as the main difficulty of the deformation problem.

We say that the deformation problem is **cohomologically unobstructed** (or **globally unobstructed**) if $H^2(G_S(E), \mathrm{ad}\bar{\rho}) = 0$ (or $Ш^2_S(E, \mathrm{ad}\bar{\rho}) = 0$, resp.). We seek conditions under which either $R_{G_S}(\bar{\rho})$ is free (namely under which the deformation problem is unobstructed), or I is completely controlled by local equations (the deformation problem being globally unobstructed). In a more general fashion, we would like to unravel the arithmetical information contained in $G_S(E)$ that determines the ideal of relations of a presentation of the universal deformation ring $R_{G_S}(\bar{\rho})$.

It is easy to see that $R_{G_S}(\bar{\rho})$ is free of relative dimension $2[E : \mathbf{Q}] + 1$ if and only if $\bar{\rho}$ is cohomologically unobstructed. There are no examples known, and maybe there aren't any, where $R_{G_S}(\bar{\rho})$ is free, but of relative dimension greater then $2[E : \mathbf{Q}] + 1$ (it cannot be smaller), i.e., where not at the same time $\bar{\rho}$ is cohomologically unobstructed.

Unobstructed deformations are not rare: Mazur has proved in [17] that for a given modular elliptic curve $\mathcal{E}$ over $\mathbf{Q}$ without complex multiplication, the set of prime p for which $H^2(G_S(\mathbf{Q}), \mathrm{ad}\bar{\rho}) = 0$ has density 1. The non obstruction can arise from:

- the arithmetical properties of the field E: for example if $H^2(G_S(E(\mu_p)), \mathbf{F}_p) = 0$ (which means that the maximal pro-p quotient of $G_S(E(\mu_p))$ is free) then the problem is unobstructed. The cyclotomic case (§3.3), where $E = \mathbf{Q}$ and $\mathbf{Q}(\mu_p)$ satisfies Vandiver's conjecture, is a subtler unobstructed deformation problem.

- the arithmetical properties of the representation $\bar{\rho}$: Flach, for instance, studies the representations $\bar{\rho} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(\mathcal{E}[p])$ associated to the p-torsion points of an elliptic curve $\mathcal{E}$ having good reduction at p. In [8, Theorem 2], Flach gives a list of conditions that imply the unobstructedness of the deformation problem. These conditions include $p \geq 5$, the surjectivity of $\bar{\rho}$,

and an assumption on a special value of a Hasse-Weil L-function.

In our paper, we propose to disentangle the interaction between $G_S(E)$ and $\bar{\rho}$ by using the prime-to-adjoint principle introduced in [5] and developed in [2]. It investigates consequences from the condition that $\mathrm{ad}\bar{\rho}$ and some localization kernel $Ш^2_S(F, \mathbf{F}_p)$ (where F is a certain splitting field associated to $\bar{\rho}$) have no common irreducible component as $\mathbf{F}_p[\mathrm{Gal}(F/E)]$-modules (§3.1, §3.2).

Here we shall restrict our analysis to **Borel type representations**, i.e. representations for which $\mathrm{Im}\bar{\rho}$ is contained in the set of upper triangular matrices –at least after conjugation. Representations of Borel type appear naturally as representations on the group of p-torsion points of elliptic curves having a rational p-torsion point, or at least a rationally defined subgroup of order p of p-torsion points. Such representations can also arise as mod p representations associated to modular (cusp) forms [24].

In the Borel case, we shall see that prime-to-adjointness is directly related to components of class groups (§3.2), to Iwasawa modules (§3.4) and to p-adic L-functions (§3.5). As a consequence, we shall be able to give a reformulation of Vandiver's conjecture in terms of the freeness of $R_{G_S}(\bar{\rho})$ where $E = \mathbf{Q}$ (§3.3). For general totally real E, we summarize in Theorem 3.4.6 the connections, which are generally of an asymptotic type, between the freeness of rings $R_{G_S}(\bar{\rho})$ and Greenberg's conjecture.

With some devissage hypotheses (which are verified for $\mathbf{Q}$, see §3.3) the prime-to-adjoint principle allows us to annihilate $Ш^2_S(E, \mathrm{ad}\bar{\rho})$ without too restrictive hypotheses on the arithmetical properties of E. We derive from this in a systematic way new classes of (globally) unobstructed deformations. Based on a local to global principle from [1], we describe also some unobstructed minimal deformation problems (a notion similar to that introduced by Wiles [33]) and exhibit some explicit universal deformation rings of Galois representations associated to elliptic curves. Finally in §5, we discuss a partial reciprocal, namely sufficient conditions under which the (global) non obstruction implies the prime-to-adjointness.

Acknowledgements: Our warmest thanks go to Professeur Nguyen Quang Do for many interesting discussions and suggestions that lead to the improvement of the original manuscript. We both benefited greatly from this and enjoyed his interest in our work. Furthermore, we are grateful to the Institut Henri Poincaré where this work was initiated when the authors met in spring 1997. The first author would also like to thank the Institut für Experimentelle Mathematik, for the stimulating atmosphere during his stay as a post-doctoral fellow with Professor Frey. The second author would like to thank Professor Gillard for his encouragements. Finally we would like to thank the referee for several suggestions to the improvement of the original manuscript.

2 Notations

Let $\bar{\rho} : \mathrm{Gal}(\bar{E}/E) \to \mathrm{GL}_2(\mathbf{F}_p)$ be an odd Galois representation of Borel type, i.e

$$\mathrm{Im}\bar{\rho} \subset \begin{pmatrix} * & * \\ & \\ 0 & * \end{pmatrix} \text{ and } \det\bar{\rho}(c) = -1$$

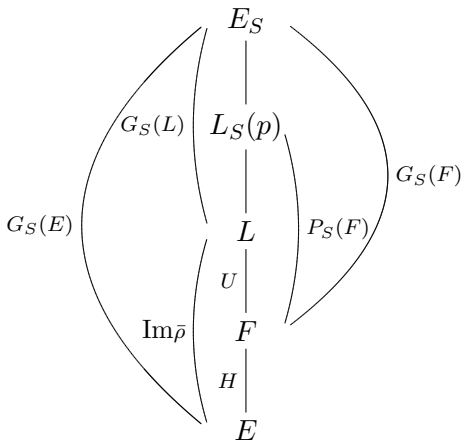
for all complex conjugations c. By definition E is totally real. We shall also assume that the centralizer of $\bar{\rho}$ inside $\mathrm{GL}_2(\mathbf{F}_p)$ is the set of scalars –this is relevant for the representability of the deformation functor we shall consider. In particular $\mathrm{Im}\bar{\rho}$ is not abelian. Let $S(E)$ be a finite set of places of E containing the set $S_\infty = S_\infty(E)$ of archimedean primes, the set $S_p = S_p(E)$ of places above p and the set $\mathrm{Ram}(\bar{\rho})$ of places where $\bar{\rho}$ ramifies. By L we denote the subfield of $\bar{E}$ fixed by $\ker\bar{\rho}$. By definition one has $\mathrm{Gal}(L/E) \cong \mathrm{Im}\bar{\rho}$.

Let E_S be the maximal extension of E unramified outside $S(E)$. We define $G_S(E) = \mathrm{Gal}(E_S/E)$. In particular $\bar{\rho}$ and all deformations of it factor through $G_S(E)$. When no confusion arises, we will write S for $S(E)$ or $S(L)$.

Let F be the subextension of L such that $U = \mathrm{Gal}(L/F)$ is the Sylow-p-subgroup of $\mathrm{Gal}(L/E)$. We shall assume throughout that F is a CM field. We now fix a complex conjugation c. Then all complex conjugations will behave like c under $\det(\bar{\rho})$. Let $\widetilde{F} = F(\mu_p)$ and $\widetilde{H} = \mathrm{Gal}(\widetilde{F}/E)$.

As the quotient $H = \mathrm{Gal}(F/E)$ of $\mathrm{Gal}(L/E)$ is of order prime to p, we shall consider H as a subgroup of $\mathrm{Gal}(L/E)$. Without loss of generality we can assume that U is the set of matrices of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, and H is the set of all matrices of the form $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ inside $\mathrm{Im}\bar{\rho}$.

The field E_S is also the maximal extensions of F and L unramified outside $S(F)$ and $S(L)$, resp. Let $G_S(F) = \mathrm{Gal}(E_S/F)$, $G_S(L) = \mathrm{Gal}(E_S/L)$. Let $L_S(p)$ be the maximal pro-p-extension of L unramified outside $S(L)$ and $P_S(F) = \mathrm{Gal}(L_S(p)/F)$. The following diagram summarizes our notation.



For a field K, we denote by $\mu_p(K)$ (resp. $\mu(K)$) the set of p-th roots of unity in K (resp. the set of roots of unity in K of p-power order). The algebraic closure of K is denoted by $\bar{K}$, and $G_K = \mathrm{Gal}(\bar{K}/K)$. The quotient of the p-class group $\mathrm{Cl}(K)$ of K by the class of prime ideals corresponding to finite places of $S(K)$ is denoted by $\mathrm{Cl}_S(K)$. For $v \in S(K)$, K_v is the v-completion of K.

For M a $G_S(E)$-module, its Pontryagin dual is denoted by $M^* = \mathrm{Hom}_{\mathbf{Z}_p}(M, \mathbf{Q}_p/\mathbf{Z}_p)$, and for a morphism $\gamma : M \to N$ between $G_S(E)$-modules, γ^* denotes the induced morphism from N^* to M^*. By M^+ (resp. M^-) we will denote the submodule of elements of M on which the complex conjugation c acts by $+1$ (resp. -1). For all integers i, $M(i)$ is the module M twisted i times by the cyclotomic character (also called 'Tate twist' of M).

Let $\widehat{H}$ be the group of characters of H. Let ω be the Teichmüller character of $G_S(E)$. For a

character $\varphi \in \widehat{H}$, e_φ denotes the associated idempotent in $\mathbf{Z}_p[H]$, which exists because p is prime to the order of H. For a $\mathbf{Z}_p[H]$-module M, we define $M_\varphi = e_\varphi M$. This is the largest submodule of M on which H acts via the character φ. Similarly we define for $\mathcal{V} = \{\varphi_1, \ldots, \varphi_k\} \subset \widehat{H}$

$$M_{\mathcal{V}} = M_{\varphi_1,\ldots,\varphi_k} = \oplus_{i=1}^{k} M_{\varphi_i}$$

We also denote by $\mathbf{F}_p^\varphi$ (resp. $\mathbf{Z}_p^\varphi$) the $\mathbf{F}_p[H]$-module $\mathbf{F}_p$ (resp. the $\mathbf{Z}_p[H]$-module $\mathbf{Z}_p$) with the action of H given by φ. Let $M^\varphi = M \otimes_{\mathbf{Z}_p} \mathbf{Z}_p^\varphi$. The above definitions imply $M_{\varphi^{-1}} = (M^\varphi)^H$.

For any pro-p group P and any finite $\mathbf{F}_p[P]$-module M, we define

$$h^i(P, M) = \dim_{\mathbf{F}_p} H^i(P, M)$$

and for any integer $n \geq 0$, the partial Euler-Poincaré characteristic

$$\chi_{(n)}(P, M) = \sum_{i=0}^{n} (-1)^i h^i(P, M)$$

The global Euler-Poincaré characteristic (if finite) is $\chi(P, M) = \sum_{i=0}^{\infty} (-1)^i h^i(G, M)$. It is multiplicative, i.e. $\chi(Q, M) = [P : Q]\chi(P, M)$ for any subgroup Q of finite index in P, c.f. [27].

By $\mathrm{ad}\bar{\rho}$ (resp. $\mathrm{ad}^0\bar{\rho}$) we denote the representation of $G_S(E)$ or of G_E on $\mathrm{M}_2(\mathbf{F}_p)$ (resp. on the trace zero matrices in $\mathrm{M}_2(\mathbf{F}_p)$), obtained by composing $\bar{\rho}$ with the adjoint action of $\mathrm{GL}_2(\mathbf{F}_p)$ on $\mathrm{M}_2(\mathbf{F}_p)$. Then $\mathrm{ad}\bar{\rho} \cong \mathbf{F}_p \oplus \mathrm{ad}^0\bar{\rho}$.

We denote by $\mathcal{C}$ the category of complete noetherian local $\mathbf{Z}_p$-algebras with residue field $\mathbf{F}_p$ where the morphisms are morphisms of local rings inducing the identity on residue fields. For R an object of $\mathcal{C}$, we denote by $\mathfrak{m}_R$ its maximal ideal.

We recall that a deformation of $\bar{\rho}$ to an object R of $\mathcal{C}$ is an equivalence class $[\rho]$ of representations $\rho : G_S(E) \to \mathrm{GL}_2(R)$ (unramified outside S) such that for the canonical surjection $\pi : R \to \mathbf{F}_p$ the equality $\pi \circ \rho = \bar{\rho}$ holds. Two representations ρ and ρ' are equivalent if there exists $M \in \Gamma_2(R) = \ker(\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbf{F}_p))$ such that $\rho = M\rho' M^{-1}$. Mazur's deformation functor is the functor Def from $\mathcal{C}$ to the category Set of sets defined by

$$\mathrm{Def}(R) = \{\text{deformations } [\rho] \text{ of } \bar{\rho} \text{ to } R\}$$

Following Ramakrishna [23] Theorem 1.1, we know that the functor Def is representable since $\mathrm{M}_2(\mathbf{F}_p)^{\mathrm{Im}\bar{\rho}} = \mathbf{F}_p\mathrm{Id}$. We denote by $R_{G_S}(\bar{\rho})$ the object of $\mathcal{C}$ which represents this functor, and we call it the **universal deformation ring**.

3 Prime-to-adjoint principle

We define $\bar{\rho}$ as in the previous section. From obstruction theory one knows that the cohomology groups $H^i(G_S(E), \mathrm{ad}\bar{\rho}),\ i = 1, 2$ are relevant when one attempts a description of $R_{G_S}(\bar{\rho})$. We would like to relate those cohomology groups to $H^i(G_S(F), \mathbf{F}_p),\ i = 1, 2$. Boston's prime-to-adjoint principle [5] is a precise link between these cohomology groups for $i = 1$. In [1] this principle is generalized to the case $i = 2$. We now recall the prime-to-adjoint principle.

We fix lifts l_1, l_2 of H to $\mathrm{GL}_2(\mathbf{Z}_p)$ and to $\mathrm{Gal}(L_S(p)/E)$, resp. By the profinite version of the theorem of Schur-Zassenhaus these liftings exist. Indeed $P_S(F)$ and $\Gamma_2(\mathbf{Z}_p)$ are finitely generated pro-p groups. Using the morphisms $H \to \mathrm{GL}_2(\mathbf{Z}_p) \to \mathrm{GL}_2(R)$, H acts canonically via conjugation on $\mathrm{GL}_2(R)$ for all $R \in \mathcal{C}$. Similarly it acts via conjugation on the normal subgroup $P_S(F)$ of $\mathrm{Gal}(L_S(p)/E)$.

Since H is abelian of exponent dividing $p-1$, all the $\mathbf{F}_p[H]$-modules are semi-simple and can be decomposed into sums of irreducible $\mathbf{F}_p[H]$-modules of dimension 1. We denote by χ_1, χ_2 the diagonal characters which appear in $\bar{\rho} = \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$. Whence $\bar{\rho}_{|H} \sim \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$, and the irreducible components of $\mathrm{ad}\bar{\rho}$, restricted to H, are $\mathbf{F}_p, \mathbf{F}_p^{\psi}, \mathbf{F}_p^{\psi^{-1}}$, where $\psi = \chi_1^{-1}\chi_2$. We remark that ψ is odd since $\det\bar{\rho} = \chi_1\chi_2$ is odd.

We set $\mathcal{V} = \{\mathrm{triv}, \psi, \psi^{-1}\}$, and we say that a $G_S(E)$-module M is **prime-to-adjoint** if and only if its eigenspaces $M_\varphi = 0$ for all $\varphi \in \mathcal{V}$, that is, if $M_{\mathcal{V}} = 0$.

3.1 Prime-to-adjoint principle

We follow the strategy in §2 of [3]. We compare the deformation functor with a (simpler) functor, namely a modified functor of equivariant homomorphisms. The latter description shows more clearly the constraints on deformations imposed by the H-action on $P_S(F)$ and $\mathrm{GL}_2(R)$. We fix an element x_1 of $P_S(F)$ such that $\bar{\rho}(x_1) = \begin{pmatrix} 1 & 1 \\ & \\ 0 & 1 \end{pmatrix}$. Hence $\bar{\rho}(x_1)$ is a generator of U. By [2] the deformation functor Def is equivalent to the functor D_S from $\mathcal{C}$ to Sets, defined by

$$D_S(R) = \{\alpha \in \mathrm{Hom}_H(P_S(F), \widetilde{\Gamma}_2(R)),\ \alpha(x_1) = \begin{pmatrix} 1 & 1 \\ & \\ 0 & 1 \end{pmatrix},\ \alpha \cong \bar{\rho}_{|P_S(F)} \mathrm{mod}\ \mathfrak{m}_R\}$$

where $\widetilde{\Gamma}_2(R)$ denotes the subgroup of $\mathrm{GL}_2(R)$ generated by $\Gamma_2(R)$ and the matrices $\begin{pmatrix} 1 & r \\ & \\ 0 & 1 \end{pmatrix}$ for $r \in R$. Explicitly, the map $D_S(R) \to \mathrm{Def}(R)$ can be given as follows. Any $g \in \mathrm{Gal}(L_S(p)/E)$ can be written uniquely as $g = l_2(h)x$ with $h \in H$ and $x \in P_S(F)$. For $\alpha \in D_S(R)$ we define $\widetilde{\rho} : \mathrm{Gal}(L_S(p)/E) \to \mathrm{GL}_2(R)$ by $\widetilde{\rho}(g) = l_1(h)\alpha(x)$. By ρ we denote the composition of $\widetilde{\rho}$ with the map $G_S(E) \twoheadrightarrow \mathrm{Gal}(L_S(P)/E)$. Then $D_S(R) \to \mathrm{Def}(R)$ is the map that sends α to the equivalence class $[\rho]$.

We now explain the prime-to-adjoint principle which was expressed in [1, Prop. 8.2] for the tame case, but which can be adapted to the Borel case. To apply it to the deformation functor, it is indeed necessary to replace Def by the modified Hom-functor D_S. Let Γ_2 be any finitely generated pro-p-group with an H-action and with a filtration such that all subquotients are elementary p-abelian H-modules. We assume that all such subquotients M satisfy $M_\varphi = 0$ for $\varphi \notin \mathcal{V}$. This property is independent of the chosen filtration.

Let Π be a finitely presented pro-p-group with an H-action, which admits an H-equivariant presentation

$$1 \to \mathcal{R} \to \mathcal{F} \to \Pi \to 1$$

where $\mathcal{F}$ is a free pro-p-group. By a sequence of modifications, c.f. [1, 8], one can find a subgroup $\mathcal{R}'$ inside $\mathcal{F}$, which is invariant under the H-action, such that $\Pi' = \mathcal{F}/\mathcal{R}'$ satisfies

$$\mathrm{Hom}_H(\Pi, \Gamma_2) \cong \mathrm{Hom}_H(\Pi', \Gamma_2)$$

and $H^i(\Pi', \mathbf{F}_p)^* \cong (H^i(\Pi, \mathbf{F}_p)^*)_{\mathcal{V}}$ for $i = 1, 2$, [1, Cor. 8.3]. Furthermore the construction of Π' is independent of Γ_2; it only depends on $\mathcal{V}$.

By [5, §2], the pro-p-group $P_S(F)$ admits an H-equivariant presentation

$$1 \to \mathcal{R} \to \mathcal{F} \to P_S(F) \to 1$$

where $\mathcal{F}$ is a free pro-p group whose rank equals $h^1(P_S(F), \mathbf{F}_p)$ and where $\mathcal{R}$ is generated by $h^2(P_S(F), \mathbf{F}_p)$ elements. We set $\Pi = P_S(F)$ and $\Gamma_2 = \Gamma_2(R)$, of which one can check that it has the required properties, and so D_S is a subfunctor of $\mathrm{Hom}_H(\Pi, \Gamma_2)$ – this is the reason for replacing Def by D_S.

The **prime-to-adjoint principle** is the idea that the relevant information of $G_S(E)$ that determines $R_{G_S}(\bar{\rho})$ is 'contained' in $H^i(\Pi', \mathbf{F}_p)^* \cong (H^i(\Pi, \mathbf{F}_p)^*)_{\mathcal{V}}$ for $i = 1, 2$. Thus the prime-to-adjoint principle is relevant not only for controlling the generators, but also the relations (without controlling the relations it was already used and stated in [5]). In essence it says that one can erase all generators and all relations corresponding to elements in $(H^i(\Pi', \mathbf{F}_p)^*)_{\varphi}$ ($i = 1, 2$, resp.) whenever $\varphi \notin \mathcal{V}$. The fact that D_S is really a subfunctor of $\mathrm{Hom}_H(\Pi, \Gamma_2)$ is merely a minor technicality. To analyze $D_S(R)$, using the H-action, it suffices to consider those relation(s) in a presentation of $P_S(F)$ that come from $H^2(P_S(F), \mathbf{F}_p)_{\mathcal{V}}$. In §4 we use cohomological methods to further develop this idea. In this section we focus on the direct interpretation of $H^2(P_S(F), \mathbf{F}_p)_{\mathcal{V}}$.

Remark 3.1.1 For the above result, we used the description of Def as a modified Hom-functor. Such an interpretation is not known in the full case, i.e. when $\mathrm{SL}_2(\mathbf{F}_p) \subset \mathrm{Im}\bar{\rho}$. Hence our methods do not directly generalize to such cases. However the prime-to-adjoint principle as stated in [5] or [2] is still applicable.

3.2 Arithmetic interpretation of the prime-to-adjoint condition

We recall that $P_S(F) = \mathrm{Gal}(L_S(p)/F)$ and $\mathcal{V} = \{\mathrm{triv}, \psi, \psi^{-1}\}$. We now want to describe $H^2(P_S, \mathbf{F}_p)_{\mathcal{V}}$. We have $H^2(P_S(F), \mathbf{F}_p) \cong H^2(G_S(F), \mathbf{F}_p)$ where the isomorphism is compatible with the H action. This follows by applying the Hochschild-Serre spectral sequence to

$$1 \to \mathrm{Gal}(E_S/L_S(p)) \to G_S(F) \to P_S(F) \to 1,$$

upon observing that $H^i(\mathrm{Gal}(E_S/L_S(p)), \mathbf{F}_p) = 0$ for all $i > 0$, because $\mathrm{Gal}(E_S/L_S(p))$ has no finite p-group quotients, by its very definition, and its cohomology can be computed as the direct limit of the cohomologies of all finite quotients. Hence we may write the Poitou-Tate exact sequence of $\mathbf{F}_p[H]$-modules:

$$0 \to Ш^2_S(F, \mathbf{F}_p) \to H^2(P_S(F), \mathbf{F}_p) \to \coprod_{v \in S(F)} H^2(G_{F_v}, \mathbf{F}_p) \to H^0(G_S(F), \mathbf{F}_p^*(1))^* \to 0$$

The two rightmost terms are easy to calculate, only $Ш^2_S(F, \mathbf{F}_p)$ is mysterious. Provided that $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint (for the definition see §3.1), we can easily describe $H^2(P_S(F), \mathbf{F}_p)_{\mathcal{V}}$. In that case we only need to consider the relations coming from local relations.

We shall look for arithmetical conditions under which

$$Ш^2_S(F, \mathbf{F}_p)_\varphi = (Ш^2_S(F, \mathbf{F}_p)^{\varphi^{-1}})^H = 0, \ \varphi \in \mathcal{V}$$

Proposition–Definition 3.2.1 *The* **prime-to-adjoint condition** *is defined as one of the following equivalent properties:*

(i) $Ш^2_S(F, \mathbf{F}_p)$ *is prime-to-adjoint, that is* $Ш^2_S(F, \mathbf{F}_p)_{\mathcal{V}} = 0$

(ii) $Ш^2_S(F, \mathbf{F}_p^\varphi)^H = 0, \ \varphi \in \mathcal{V}$

(iii) $Ш^2_S(E, \mathbf{F}_p^\varphi) = 0, \ \varphi \in \mathcal{V}$

PROOF: Since F trivializes the action of ψ, (i) and (ii) are obviously equivalent. To descend to E, we note that $Ш^2_S(L,M)^\Delta \cong Ш^2_S(E,M)$ for any finite Galois extension L of E such that p does not divide the order of $\Delta = \mathrm{Gal}(L/E)$. We can apply this to F and $H = \mathrm{Gal}(F/E)$. ∎

That the $Ш^2_S(E,\mathbf{F}_p)^\varphi$, $\varphi \in \mathcal{V}$ are the relevant obstruction groups, can also be seen by observing that the Jordan-Hölder decomposition factors of $\mathrm{ad}\bar{\rho}$ are the three modules $\mathbf{F}_p^\varphi,\ \varphi \in \mathcal{V}$.

Remark 3.2.2 If $\psi = \omega^i$ then the condition $Ш^2_S(E,\mathbf{F}_p^{\omega^i}) = Ш^2_S(E,\mathbf{F}_p(i)) = 0$ is implied by the so called (p,i)-regularity of E, c.f. [13, p. 54], that is $H^2(G_S(E),\mathbf{F}_p(i)) = 0$.

Using class field theory, we now discuss the prime-to-adjoint condition. We can apply the proof of Proposition–Definition 3.2.1 to $\widetilde{F}$ and $\widetilde{H}$, defined near the beginning of Section 2. Here the characters of $\mathcal{V}$ are considered as characters on $\widetilde{H}$ also. Then the prime-to-adjoint condition is equivalent to

$$Ш^2_S(\widetilde{F},\mathbf{F}_p^\varphi)^{\widetilde{H}} = 0,\ \varphi \in \mathcal{V}$$

Since $\mathbf{F}_p = \mu_p^{\omega^{-1}}$, by global Poitou-Tate duality we have

$$Ш^2_S(\widetilde{F},\mathbf{F}_p) = Ш^1_S(\widetilde{F},\mu_p)^*, \text{ where}$$

$$0 \to Ш^1_S(\widetilde{F},\mu_p) \to H^1(G_S(\widetilde{F}),\mu_p) \to \mathrm{Ш}_{v\in S(\widetilde{F})} H^1(G_{\widetilde{F}_v},\mu_p)$$

with $G_S(\widetilde{F}) = \mathrm{Gal}(E_S/\widetilde{F})$. Recall that by definition $\mu_p \subset \widetilde{F}$. Since the action of $G_S(\widetilde{F})$ on μ_p is trivial, by class field theory and Kummer theory we obtain

$$Ш^1_S(\widetilde{F},\mu_p) = \mathrm{Hom}(\mathrm{Cl}_S(\widetilde{F}),\mu_p) = \mathrm{Hom}(\mathrm{Cl}_S(\widetilde{F}),\mathbf{F}_p)(1)$$

Hence

$$Ш^2_S(\widetilde{F},\mathbf{F}_p) = \mathrm{Hom}(\mathrm{Cl}_S(\widetilde{F}),\mathbf{F}_p)(1)^* = (\mathrm{Cl}_S(\widetilde{F})/(p))^{\omega^{-1}}$$

Thus

$$Ш^2_S(\widetilde{F},\mathbf{F}_p^\varphi) = (\mathrm{Cl}_S(\widetilde{F})/(p))^{\omega^{-1}\varphi^{-1}}$$

Moreover, as $\mathrm{Cl}_S(\widetilde{F})$ is a p-group, we obtain

Theorem 3.2.3 *Let $\mathcal{V} = \{\mathrm{triv}, \psi, \psi^{-1}\}$, then $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint if and only if $\mathrm{Cl}_S(F(\mu_p))_{\omega\mathcal{V}} = 0$.*

Remark 3.2.4 Skinner and Wiles use stronger conditions on the class groups in order to obtain that some ordinary Borel type Galois representations are modular, c.f. [28]. Their conditions on the vanishing of odd parts of the class group imply by 'Spiegelung' the vanishing of certain even parts of the class group, too.

Remark 3.2.5 The three conditions for the characters in $\mathcal{V}$ on $Ш^2_S(F, \mathbf{F}_p)$ to be prime-to-adjoint are not of the same nature and will not be treated by the same methods; see §3.4 below. Proposition 3.2.1 admits a more 'economical' formulation, thanks to

Lemma 3.2.6 *For all $\varphi \in \widehat{\widehat{H}}$, one has*

$$e_\varphi(\mathrm{Cl}_S(\widetilde{F})) \cong e_\varphi(\mathrm{Cl}_S(E(\varphi)))$$

where $E(\varphi)$ is the fixed field by $\ker\varphi$.

PROOF: This is well known. Similar results were discussed in [29, Rem. II.1 and Prop. II.1]. ∎

Example 3.2.7 Let $F = \mathbf{Q}(\zeta_p, \sqrt{d})$, ($\zeta_p$ is a primitive p-root of unity and d a positive square free integer) and $E = \mathbf{Q}$. The (even) quadratic character associated to $\sqrt{d}$ is denoted by χ. Let $p = 3$ and $\psi = \omega\chi$. Using Lemma 3.2.6 the prime-to-adjoint condition is satisfied if

$$\mathrm{Cl}_S(\mathbf{Q}(\sqrt{-3}))_\omega = 0, \quad \mathrm{Cl}_S(\mathbf{Q}(\sqrt{d}))_\chi = \mathrm{Cl}_S(\mathbf{Q}(\sqrt{d})) = 0$$

The first condition is satisfied since the ring of integers of $\mathbf{Q}(\sqrt{-3})$ is principal. If $S = S_p \cup S_\infty$ and $p = 3$ is inert, then

$$\mathrm{Cl}_S(\mathbf{Q}(\sqrt{d})) = \mathrm{Cl}(\mathbf{Q}(\sqrt{d}))$$

Using tables of class numbers of quadratic fields or a package like 'pari', one can easily construct many examples with a prime-to-adjoint $Ш^2_S(F, \mathbf{F}_p)$.

3.3 Prime-to-adjoint condition and Vandiver's conjecture

We now specialize to the situation $E = \mathbf{Q}$ and $F = \mathbf{Q}(\zeta_p)$, where we formulate a link between the prime-to-adjoint condition and Vandiver's conjecture. Later we develop an analogous link for more general fields, Vandiver's conjecture being replaced by Greenberg's conjecture.

Let $\bar{\rho} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p)$ be a continuous odd representation of Borel type unramified outside $S(\mathbf{Q}) = \{p, \infty\}$ with $E = \mathbf{Q}$, $F = \mathbf{Q}(\zeta_p)$ and $\det\bar{\rho} = \omega$. Such representations appear in the study of elliptic curves, c.f. [26, §5.5]. Since $S(\mathbf{Q}) = \{p, \infty\}$ the representation $\bar{\rho}$ is only ramified in p. Whence the diagonal characters of $\bar{\rho}$ are ω^i and ω^j with $i + j \equiv 1 \bmod p - 1$.

Proposition 3.3.1 *In the Borel case, if the centralizer in* $\mathrm{GL}_2(\mathbf{F}_p)$ *of* $\mathrm{Im}\bar{\rho}$ *is the set of homotheties, if* $F = \mathbf{Q}(\zeta_p)$ *and if Vandiver's conjecture holds (this is the case for* $p < 1 + 4 \cdot 10^6$*), then*

$$R_{G_S}(\bar{\rho}) = \mathbf{Z}_p[[Y_1, Y_2, Y_3]]$$

Proof: By Theorem 3.2.3, the prime-to-adjoint condition of $Ш^2_S(F, \mathbf{F}_p)$ is equivalent to

$$\mathrm{Cl}_S(F)_\omega = 0, \quad \mathrm{Cl}_S(F)_{\omega^{2j}} = 0, \quad \mathrm{Cl}_S(F)_{\omega^{2-2j}} = 0$$

Here $\mathrm{Cl}_S(F) = \mathrm{Cl}(F)$. The last two conditions follow from Vandiver's conjecture which we assume to hold. The field $E = \mathbf{Q}$ is $(p, 0)$-regular, and so by Remark 3.2.2, the first condition holds. For $\varphi \in \{\mathrm{triv}, \psi, \psi^{-1}\}$ by considering the Poitou-Tate sequence

$$0 \to H^2(G_S(F), \mathbf{F}_p)_\varphi \to H^2(G_{F_\mathfrak{p}}, \mathbf{F}_p)_\varphi \to (H^0(G_S(F), \mu_p)^*)_\varphi \to 0$$

it follows that $H^2(G_S(F), \mathbf{F}_p)_\varphi = 0$. By devissage and by the long exact sequence of cohomology one easily finds $H^2(G_S(\mathbf{Q}), \mathrm{ad}\bar{\rho}) = 0$. The deformation problem is thus unobstructed, and the proposition follows from [16]. ∎

If p is an irregular prime, the above proposition provides an example of an unobstructed deformation problem for which $Ш^2_S(F, \mathbf{F}_p) \neq 0$.

Remark 3.3.2 In [18, Prop. 7.5.2], it was only shown that the universal deformation ring of $\bar{\rho} : \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p)$ admits a presentation

$$R_{G_S}(\bar{\rho}) = \mathbf{Z}_p[[Y_1, Y_2, Y_3]]/I$$

with $I \equiv (0) \bmod Y_3$ if Vandiver's conjecture holds for p, and $I = (0)$ if p is a regular prime.

Remark 3.3.3 The hypotheses of Proposition 3.3.1 are unnecessarily restrictive. The following two parts of Vandiver's conjecture are sufficient:

$$\mathrm{Cl}_S(F)_{\omega^{2j}} = 0, \quad \mathrm{Cl}_S(F)_{\omega^{2-2j}} = 0$$

Using K-theory, Kurihara has shown that Vandiver's conjecture for the ω^{p-3}-component, c.f. [15].

Remark 3.3.4 In order to prove that $\mathrm{Cl}(\mathbf{Q}(\mu_p))_\omega$ is zero, one usually applies Stickelberger's theorem, c.f. [31, Thm. 6.16]. We used the cohomological argument of the $(p, 0)$-regularity of $\mathbf{Q}$ anticipating generalizations in the following subsections to a broader context.

We have the following converse to the above result.

Corollary 3.3.5 *Vandiver's conjecture holds if and only if for all Borel representations*

$$\bar{\rho} : \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \text{ with } S = \{p, \infty\} \text{ and } \bar{\rho} = \begin{pmatrix} \omega^i & * \\ 0 & \omega^j \end{pmatrix}$$

where $i + j \equiv 1 \mod p - 1$ and $*$ is not identically zero, the universal deformation ring $R_{G_S}(\bar{\rho})$ is isomorphic to $\mathbf{Z}_p[[T_1, T_2, T_3]]$, i.e., all such $\bar{\rho}$ are cohomologically unobstructed.

Proof: By Proposition 3.3.1, it suffices to show that if $R_{G_S}(\bar{\rho}) = \mathbf{Z}_p[[T_1, T_2, T_3]]$ for all representations $\bar{\rho}$ as above, then Vandiver's conjecture holds. By [16], this is equivalent to proving Vandiver's conjecture assuming that $H^2(G_S(E), \mathrm{ad}\bar{\rho}) = 0$ for all $\bar{\rho}$ as above.

From the long exact sequence of cohomology applied to the surjection $\mathrm{ad}\bar{\rho} \twoheadrightarrow \mathbf{F}_p^{\psi}$ it follows that $H^2(G_S(E), \mathbf{F}_p^{\psi}) = 0$ where $\psi = \omega^{j-i} = \omega^{2j-1}$, hence $Ш_S^2(\mathbf{Q}, \mathbf{F}_p^{\psi}) = 0$. Let $F = \mathbf{Q}(\zeta_p)$ and $H = \mathrm{Gal}(F/\mathbf{Q})$. From the Poitou-Tate sequence together with Theorem 3.2.3 and $\mathrm{Cl}(F) = \mathrm{Cl}_S(F)$, this implies $\mathrm{Cl}(F)_{\omega^{2j}} = 0$.

The only thing left to do, is to construct a Borel type representation for each even integer $2j$ in the interval $[2, p-1]$ as above, where the $(1,2)$-entry $*$ is non-trivial, and such that $\bar{\rho}$ is unramified outside $\{p, \infty\}$. To construct such a $\bar{\rho}$, we merely need to show that $\bar{P}_S(F) = P_S(F)/[P_S(F), P_S(F)]P_S(F)^p$ satisfies $(\bar{P}_S(F))_{\psi} \neq 0$.

Recall that by [7], Proposition 3.2, in our situation $\bar{P}_S(F) = \coprod_{k \text{ odd}} \mathbf{F}_p^{\omega^k} \oplus \mathbf{F}_p \oplus Ш_S^2(F, \mathbf{F}_p)^*$. Hence for each given j, there is a k such that $k = j - i = 2j - 1$. We construct $\bar{\rho}$ from this component of $\bar{P}_S(F)$. By the above we know that for all even integers in $[2, p-1]$ the corresponding component of $\mathrm{Cl}(F)[p]$ is trivial, whence Vandiver's conjecture follows. ∎

Similarly one can prove the following result where we consider residual representations that are of Borel type and ordinary at p in the sense of [16].

Corollary 3.3.6 *Vandiver's conjecture holds if and only if for all Borel representations*

$$\bar{\rho} : \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \text{ with } S = \{p, \infty\} \text{ and } \bar{\rho} = \begin{pmatrix} 1 & * \\ 0 & \omega^j \end{pmatrix},$$

where j is odd and $*$ is not identically zero, the universal deformation ring is isomorphic to $\mathbf{Z}_p[[T_1, T_2, T_3]]$.

If the universal deformation ring for ordinary deformations of $\bar{\rho}$ with fixed determinant is isomorphic to $\mathbf{Z}_p$, and if $\omega^j \neq \omega$, then $\mathrm{Cl}(\mathbf{Q}(\zeta_p))_{\omega^{j+1}} = 0$.

The proof of the first part is analogous to that of Corollary 3.3.5. The second part follows from [17, Main Prop.] and [2, §9].

Remark 3.3.7 If $\omega^j = \omega$ in Corollary 3.3.6 it is unlikely to expect that the universal ordinary ring with fixed determinant is isomorphic to $\mathbf{Z}_p$, see [1].

It would be nice if one could relate the above to the theory of modular forms in a similar way as in the proof of Fermat's last theorem, [33]. However for reducible Galois representations there seem to be no conjectures about them being related to modular forms. Unlike in the absolutely irreducible case, given a residual representation $\bar{\rho}$ it seems unclear how to guess the prime-to-p level of a modular form whose associated mod p representation gives rise to $\bar{\rho}$. Also if any minimal prime to p level is non-trivial but $\bar{\rho}$ is unramified outside p, the corresponding universal deformation ring would not be the one above. Thus it is not clear how in such a situation one should be able to interpret the above universal ring as some Hecke algebra of modular forms.

In [24], Ribet constructs modular forms for representations similar to the $\bar{\rho}$ above, under the assumption that an odd part of the class group of $\mathbf{Q}(\zeta_p)$ is non-trivial. Thus if one takes Ribet's $\bar{\rho}$, and if one could establish, via a correspondence between Hecke algebras and universal deformation rings of ordinary deformations with fixed determinant, that the corresponding universal ring is $\mathbf{Z}_p$, then this would imply that Vandiver's conjecture holds for ω^{1-i} whenever $\mathrm{Cl}(\mathbf{Q}(\zeta_p))_{\omega^i} = 0$, for i odd. For progress towards such a correspondence, see [28].

3.4 Iwasawa-theoretic interpretation of the prime-to-adjoint condition

Here we generalize the previous discussion about Vandiver's conjecture. We recall that $G_S(F) = \mathrm{Gal}(E_S/F)$ and $\mathcal{V} = \{\mathrm{triv}, \psi, \psi^{-1}\}$. We want to discuss the hypotheses of Theorem 3.2.3,

$$\mathrm{Cl}_S(F(\mu_p))_{\omega\mathcal{V}} = 0$$

in terms of Iwasawa modules, in order to obtain precise criteria for the prime-to-adjointness of $Ш^2_S(F, \mathbf{F}_p)$ in terms of p-adic L-functions. It is well known that the Main Conjecture of Iwasawa theory allows us to deal with the even part of $Ш^2_S(F, \mathbf{F}_p)$ (which is related to the odd part of the class group). The odd part of $Ш^2_S(F, \mathbf{F}_p)$ (the even part of the class group) is usually expressed

in terms of indices of cyclotomic units or universal norms, c.f. [14], which are much more difficult to treat. To avoid this difficulty we introduce a condition on certain Iwasawa modules, which implies the prime-to-adjoint condition (Proposition 3.4.3). For this we formulate an assumption of non decomposition :

$(*)$ There is a place v of F above p for which $\mu_{p^\infty}(F) \cong \mu_{p^\infty}(F_v)$.

For M a $G_S(E)$-module, $M[p]$ denotes the submodule of elements annihilated by p.

Lemma 3.4.1 *Assume* $(*)$*, then the following natural morphism:*

$$Ш^2_S(F, \mathbf{Z}_p)/(p) \to Ш^2_S(F, \mathbf{F}_p)$$

is surjective.

PROOF: The exactness of

$$0 \to \mu_p \to \mu_{p^\infty} \xrightarrow{p} \mu_{p^\infty} \to 0$$

gives the two horizontal short exact sequences from long exact cohomology sequences in the following diagram

$$\begin{array}{ccccc}
0 & & Ш^1_S(F, \mu_p) & & Ш^1_S(F, \mu_\infty)[p] \\
\downarrow & & \downarrow & & \downarrow \\
H^0(G_S(F), \mu_{p^\infty})/(p) & \hookrightarrow & H^1(G_S(F), \mu_p) & \twoheadrightarrow & H^1(G_S(F), \mu_{p^\infty})[p] \\
\downarrow & & \downarrow & & \downarrow \\
Ш_{v\in S} H^0(G_{F_v}, \mu_{p^\infty})/(p) & \hookrightarrow & Ш_{v\in S} H^1(G_{F_v}, \mu_p) & \twoheadrightarrow & Ш_{v\in S}\, H^1(G_{F_v}, \mu_{p^\infty})[p]
\end{array}$$

The middle and right vertical sequences come from the definition of $Ш^1_S$. The injectivity of the left vertical map follows from $(*)$. Hence the induced map

$$Ш^1_S(F, \mu_p) \hookrightarrow Ш^1_S(F, \mu_{p^\infty})[p]$$

is injective. Taking the Pontryagin duals, one obtains the lemma. ∎

We deduce a sufficient condition under which $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint:

$$\forall \varphi \in \mathcal{V},\ Ш^2_S(F, \mathbf{Z}_p)_\varphi = 0$$

We can discuss this condition in terms of Iwasawa modules. Let us recall some standard notations in Iwasawa theory. Let $F_\infty = \varinjlim F_n$ (resp. $\widetilde{F}_\infty = F(\mu_{p^\infty})$) be the cyclotomic $\mathbf{Z}_p$-extension of F (resp. of $\widetilde{F}$), $G_\infty = \mathrm{Gal}(\widetilde{F}_\infty/F)$, $\Delta = \mathrm{Gal}(\widetilde{F}/F) \cong \mathrm{Gal}(\widetilde{F}_\infty/F_\infty)$ and $\Gamma = \mathrm{Gal}(\widetilde{F}_\infty/\widetilde{F})$. Let $X' = X'(\widetilde{F})$ be the Galois group over $\widetilde{F}_\infty$ of the maximal abelian pro-p extension of $\widetilde{F}_\infty$ that is unramified and completely split at all finite places of S (hence X' depends on S), and similarly $X(\widetilde{F})$ that of the maximal abelian unramified pro-p extension of $\widetilde{F}_\infty$. Analogously one defines $X'(K), X(K)$ for any number field K and not just $\widetilde{F}$. The following is a consequence of Tate's Lemma for $\mathbf{Q}_p/\mathbf{Z}_p(m)$, $m \neq 1$, c.f. [14] or [25, §6, Lemma 1].

Lemma 3.4.2 *For $m \neq 1$,*

$$Ш^2_S(F, \mathbf{Z}_p(m)) \cong (X'(m-1))_{G_\infty}$$

Lemma 3.4.3 *For all $m \neq 1$, $\varphi \in H$, we have*

$$Ш^2_S(F, \mathbf{Z}_p(m))_\varphi = 0 \Longleftrightarrow X'_{\omega^{1-m}\varphi} = 0$$

In particular the condition $(*)$ and $X'_{\omega\mathcal{V}} = 0$ together imply that $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint. Conversely if $Ш^2_S(F_n, \mathbf{F}_p)$ is prime-to-adjoint for all sufficiently large n, then $X'_{\omega\mathcal{V}} = 0$.

Proof: By Lemma 3.4.2 and Nakayama's Lemma,

$$Ш^2_S(F, \mathbf{Z}_p(m))_\varphi = 0 \Leftrightarrow ((X'(m-1))_{G_\infty})_\varphi/(p) = 0$$

Since p does not divide the order of $\widetilde{H}$ and $\mathrm{Gal}(\widetilde{F}_\infty/E)$ is abelian,

$$((X'(m-1)_{G_\infty})_\varphi)/(p) \cong (((X'/(p))^{\omega^{m-1}})_{\Gamma\times\Delta})_\varphi \cong ((X'^{\omega^{m-1}})^\Delta_\varphi)_\Gamma/(p)$$

The latter is isomorphic to $((X'^{\omega^{m-1}\varphi^{-1}})^{\widetilde{H}})_\Gamma/(p) \cong (X'_{\omega^{1-m}\varphi})_\Gamma/(p)$, since φ is trivial on G_F. Again by Nakayama's Lemma we conclude that

$$Ш^2_S(F, \mathbf{Z}_p(m))_\varphi = 0 \Longleftrightarrow X'_{\omega^{1-m}\varphi} = 0$$

This finishes the proof of the first part of the lemma. The other parts are rather straight forward using Lemma 3.4.1 for the second part and the simple observation that $\mathrm{Cl}_S(\widetilde{F}_n)_{\omega\mathcal{V}} = 0$ for all n implies that $X'_{\omega\mathcal{V}} = 0$ for the last part. ∎

In order to explain in what sense the above results are generalizations of the relation between Vandiver's conjecture and the freeness of certain universal deformation rings, we assume $S = S_p \cup S_\infty$ and we recall two more lemmas.

For $\widetilde{F}_\infty = \varinjlim \widetilde{F}_n$, we denote

$$\mathrm{Cap}_\infty(\widetilde{F}) = \ker(\mathrm{Cl}_S(\widetilde{F}_m) \to \varinjlim \mathrm{Cl}_S(\widetilde{F}_n))$$

for $m \gg 0$ (for the stabilization of this kernel see [12]). We recall the arithmetic interpretation of the condition $X'_{\omega\psi} = 0$ given by Fleckinger and Nguyen Quang Do in [FlNg], Proposition 3.10.

Lemma 3.4.4 *The following properties are equivalent:*

(i) $X'_{\omega\varphi} = (0)$.

(ii) $(\mathrm{Cap}_\infty(\widetilde{F}))_{\omega\varphi} = (0)$ *and* $\lambda'_{\omega\varphi} = \mu'_{\omega\varphi} = 0$ *where* $\lambda'_{\omega\varphi}$, $\mu'_{\omega\varphi}$ *are the Iwasawa invariants associated to the* Λ*-torsion module* $X'_{\omega\varphi}$.

These equivalent properties imply that for all $n \geq 1$, *all cyclic p-extensions* $F'_n/\widetilde{F}_n$ *that are unramified and completely split at all the places above p, and for which H acts on* $\mathrm{Gal}(F'_n/\widetilde{F}_n)$ *by* φ^{-1}, *are contained in a* $\mathbf{Z}_p$*-extension of* $\widetilde{F}_n$.

As in [31, Prop. 13.22], one can show the following.

Lemma 3.4.5 *Let K be a number field with a unique prime $\mathfrak{p}$ above p such that this prime is totally ramified in K_∞/K. Then $X(K)_\Gamma = \mathrm{Cl}(K)$ and $X'(K)_\Gamma = \mathrm{Cl}_{S_p}(K)$, and so in particular $X'(K)_{\omega\varphi} = 0$ if and only if $\mathrm{Cl}_{S_p}(K)_{\omega\varphi} = 0$.*

Thus Vandiver's conjecture is equivalent to the vanishing of $X'(\mathbf{Q}(\zeta_p)^+)$ – or equivalently to the vanishing of $X(\mathbf{Q}(\zeta_p)^+)$. A natural generalization of this is Greenberg's conjecture that predicts that $X(K)$ is finite for any totally real field K. However there maybe some torsion in $X(K)$. Such torsion isn't necessarily visible on the level of K by which we mean that one might well have $\mathrm{Cl}_{S_p}(K) = 0$ and $X'(K) \neq 0$. Only if the latter condition holds all along the cyclotomic $\mathbf{Z}_p$-tower, one must have $X'(K) = 0$. Even worse, in general $X'(K) = 0$ doesn't even imply that $\mathrm{Cl}_{S_p}(K) = 0$. The relation between $\mathrm{Cl}(K) = 0$ and $X(K) = 0$ is similar.

Assuming Leopoldt's conjecture for all K_n, one also knows that the finiteness of $X'(K)$ is equivalent to that of $X(K)$. Furthermore for abelian fields K it is known that the μ-invariant is zero and that Leopoldt's conjecture holds. Concerning the $(p,0)$-regularity of a totally real field E, it is known that it implies the $(p,0)$-regularity for all fields E_n in the cyclotomic tower provided that none of the local field E_v, $v \in S_p$ contains p-th roots of unity, see [19]. Finally if the capitulation is trivial, then $X'(K)$ contains no finite subgroups.

We call a representation $\bar{\rho}^* : G_S(E) \to \mathrm{GL}_2(\mathbf{F}_p)$ a dual of $\bar{\rho}$ if $\bar{\rho}^* \sim \begin{pmatrix} \chi_2 & * \\ 0 & \chi_1 \end{pmatrix}$ and $*$ is non-trivial. Such a dual always exists (see the proof of Corollary 3.3.5); it may however not be unique. If $\bar{\rho}$ arises from a cusp form f, then there is a naturally defined dual obtained by choosing a suitable sublattice inside the associated p-adic representation of f. If one generalizes the proof of Corollary 3.3.5 to arbitrary totally real fields E, and takes Example 4.1.4 into account, we can summarize the above discussion in the following theorem.

Theorem 3.4.6 *Let $S = S_p \cup S_\infty$. Assume that $\bar{\rho} : G_S(E) \to \mathrm{GL}_2(\mathbf{F}_p)$ is of Borel type, $M_2(\mathbf{F}_p)^{\mathrm{Im}\bar{\rho}} = \mathbf{F}_p$, and that F is a CM field. Then one has the following implications.*

(i) *If $\bar{\rho}$ and any dual representation $\bar{\rho}^*$ are cohomologically unobstructed, then $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint. Similarly if $\bar{\rho}_{|G_S(E_n)}$ and any dual are cohomologically unobstructed, then $Ш^2_S(F_n, \mathbf{F}_p)$ is prime-to-adjoint.*

(ii) *$Ш^2_S(F_n, \mathbf{F}_p)$ is prime-to-adjoint for all sufficiently large $n \Leftrightarrow X'_{\omega\mathcal{V}} = 0$.*

(iii) *Here we assume that $\mu_p(E_\nu) = \{1\}$ for any $\nu \in S$, and that for each $s \in \{\pm 1\}$, there is at most one $\nu \in S$ such that $p|\#\bar{\rho}(G_{E_\nu})$ and $\psi_{|G_{E_\nu}} = \omega^s_{|G_{E_\nu}}$; if such a ν exists, then we require that $\omega_{|G_{E_\nu}}$ and $\omega_{|G_S(E)}$ have the same order. Under these conditions, if $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint, then $\bar{\rho}$ and any dual are cohomologically unobstructed. Moreover under the same conditions, if $Ш^2_S(F_n, \mathbf{F}_p)$ is prime-to-adjoint for sufficiently large n, then $\bar{\rho}_{|G_S(E_n)}$ and any dual of it are cohomologically unobstructed for all sufficiently large n. (The above condition remains unchanged if we replace E by E_n.)*

(iv) *Assuming that F has trivial capitulation (at least for the $\omega\psi^{\pm 1}$ components), the following holds. Greenberg's conjecture for the $\omega\psi^{\pm 1}$ components of $X(\widetilde{F})$ and the condition that E is $(p, 0)$-regular imply that $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint, and similarly in the limit if the fields E_n are $(p, 0)$-regular for sufficiently large n. For the statement in the limit, the converse is true, too, provided one assumes Leopoldt's conjecture for the fields $\widetilde{F}_n$.*

Under more restrictive hypothesis, e.g. if F is abelian, or if the hypothesis of Lemma 3.4.5 are satisfied, one can draw further conclusions, which we leave up to the reader.

3.5 Links with p-adic L-functions

We interpret the sufficient conditions of Proposition 3.4.3 in terms of p-adic L-functions. As seen in the cyclotomic case (Remark 3.3.3), the prime-to-adjoint condition relies on the assumption that $Ш^2_S(F, \mathbf{F}_p)_\varphi = 0$ for $\varphi = \psi, \psi^{-1}$, ψ an odd character, and $Ш^2_S(F, \mathbf{F}_p)_{\mathrm{triv}} = 0$ for the even character triv. At the basis of such an interpretation are the results of Wiles in [32], relating

p-adic L-functions to characteristic polynomials of Iwasawa modules. The explicit results we need are taken from [14] and [20].

First we consider the case of odd characters. Since E is totally real, we can express the conditions $X'_{\omega\psi} = X'_{\omega\psi^{-1}} = 0$ in terms of p-adic L-functions. Let R_m^χ be the Soulé p-adic regulator, that is the order of the cokernel of the homomorphism of localization

$$R_m^\chi = \#\left(\mathrm{Coker}\Big(\frac{H^1(G_S(F), \mathbf{Z}_p(m))_\chi}{\mathrm{tor}_{\mathbf{Z}_p} H^1(G_S(F), \mathbf{Z}_p(m))} \to \underset{v\in S}{\oplus} \frac{H^1(G_{F_v}, \mathbf{Z}_p(m))_\chi}{\mathrm{tor}_{\mathbf{Z}_p} H^1(G_{F_v}, \mathbf{Z}_p(m))_\chi}\Big)\right)$$

Let $w_m^\chi(F_v) = \#H^0(G_{F_v}, \mathbf{Q}_p/\mathbf{Z}_p(m))_\chi$. We recall [14, Thm. 4.3].

Theorem 3.5.1 *Assume F is a CM field and finite abelian over E, a totally real field. Let χ be a character of H. Let $m \neq 0, 1$ be an integer such that $\chi(c) = (-1)^{1-m}$, and for which $H^2(G_S(F), \mathbf{Q}_p/\mathbf{Z}_p(1-m)) = 0$. Then*

$$L_p(E, \chi\omega^{1-m}, m) \sim_p \#Ш_S^2(F, \mathbf{Z}_p(m))_\chi \cdot R_m^\chi \cdot \prod_{v\in S} w_m^\chi(F_v).$$

Here $a \sim_p b$ means that a/b is a p-adic unit.

We want to apply this theorem in our situation. We note that $H^2(G_S(F), \mathbf{Q}_p/\mathbf{Z}_p(m')) = 0$ for all $m' \geq 2$, c.f. [14, 6.1]. We obtain

Corollary 3.5.2 *With the notation of Theorem 3.5.1*

$$Ш_S^2(F, \mathbf{Z}_p)_\psi = 0 \Longleftrightarrow \frac{L_p(E, \psi\omega^p, 1-p) R_{1-p}^{\psi\omega^{1-p}} \cdot \prod_{v\in S} w_{1-p}^{\psi\omega^{1-p}}(F_v)}{\sim}_p 1$$

Proof: Since ω has exponent $p-1$, we have

$$X'_{\omega\psi} = 0 \Longleftrightarrow X'_{\omega^p\psi} = 0$$

Using Lemma 3.4.3 we obtain

$$Ш_S^2(F, \mathbf{Z}_p)_\psi = 0 \Longleftrightarrow Ш_S^2(F, \mathbf{Z}_p(1-p))_\psi = 0$$

Then we apply Theorem 3.5.1 for $m = 1-p$ and $\chi = \psi$. ∎

If $(*)$ holds, by Lemma 3.4.1 $Ш^2_S(F, \mathbf{Z}_p)_\psi = 0$ implies $Ш^2_S(F, \mathbf{F}_p)_\psi = 0$. Thus Corollary 3.5.2 gives a sufficient condition for having $Ш^2_S(F, \mathbf{F}_p)_\psi = 0$ in terms of special values of p-adic L-functions and regulators.

For the even character triv we use [20, Prop. 2.1]. Let $w_1(E_v) = \#H^0(G_{E_v}, \mathbf{Q}_p/\mathbf{Z}_p(1))$.

Lemma 3.5.3 *Assume that Leopoldt's conjecture holds for E, then*

$$\#Ш^2_S(F, \mathbf{Z}_p)_{\mathrm{triv}} \sim_p \frac{w_1(E(\mu_p))h(E)R}{\sqrt{d} \cdot \prod_{v\in S} w_1(E_v)} \prod_{v\in S}(1 - (Nv)^{-1})$$

where d is the absolute value of the discriminant of E, $h(E)$ is the class number of E and R is the p-adic regulator of Leopoldt of E.

Hence one obtains

Theorem 3.5.4 *Assume there exists $v|p$ such that $\mu(F) = \mu(F_v)$ and Leopoldt's conjecture holds for E. A sufficient condition for having $Ш^2_S(F, \mathbf{F}_p)$ prime-to-adjoint is that the p-adic integers*

$$\frac{L_p(E, \psi\omega^p, 1-p)}{R_{1-p}^{\psi\omega^{1-p}} \cdot \prod_{v\in S} w_{1-p}^{\psi\omega^{1-p}}(F_v)}, \quad \frac{L_p(E, \psi^{-1}\omega^p, 1-p)}{R_{1-p}^{\psi^{-1}\omega^{1-p}} \cdot \prod_{v\in S} w_{1-p}^{\psi^{-1}\omega^{1-p}}(F_v)}, \quad \frac{w_1(E(\mu_p))h(E)R}{\sqrt{d} \cdot \prod_{v\in S} w_1(E_v)} \prod_{v\in S}(1-(Nv)^{-1})$$

are p-adic units.

According to Theorem 3.5.1 it suffices to replace $m = 1 - p$ by any negative $m = -l(p-1)$ to obtain another criterion for having $Ш^2_S(F, \mathbf{F}_p)$ prime-to-adjoint. This can be viewed as further evidence for the validity of Greenberg's conjecture.

4 From the prime-to-adjoint condition to global unobstructedness

We now further investigate the relation between $H^2(G_S(E), \mathrm{ad}\bar{\rho})$ and $H^2(P_S(F), \mathbf{F}_p)_\mathcal{V}$. Clearly the decomposition factors of $\mathrm{ad}\bar{\rho}$ as a $G_S(E)$-module are the modules $\mathbf{F}_p^\varphi$ where $\varphi \in \mathcal{V} =$

$\{\mathrm{triv}, \psi, \psi^{-1}\}$. We recall the Poitou-Tate exact sequence

$$0 \to Ш^2_S(E, \mathrm{ad}\bar{\rho}) \to H^2(G_S(E), \mathrm{ad}\bar{\rho}) \to \coprod_{v \in S} H^2(G_{E_v}, \mathrm{ad}\bar{\rho}) \to H^0(G_S(E), \mathrm{ad}\bar{\rho}^*(1))^* \to 0$$

In §4.1 we shall use a devissage argument to derive sufficient conditions for $Ш^2_S(E, \mathrm{ad}\bar{\rho}) = 0$ and for $H^2(G_S(E), \mathrm{ad}\bar{\rho}) = 0$. In §4.2, we discuss deformation problems that are possibly ramified outside $S_p \cup S_\infty$. For this we introduce the concept of a minimal deformation problem analogous to the definition in [33] and we give conditions for it to be unobstructed. If $S = S_p \cup S_\infty \cup \mathrm{Ram}(\bar{\rho})$ then the local to global principle in [1] often allows an explicit description of $R_{G_S}(\bar{\rho})$ provided that $Ш^2_S(E, \mathrm{ad}\bar{\rho}) = 0$. Based on this, in §4.3 we give examples related to elliptic curves.

4.1 Devissage of $H^2(G_S(E), \mathrm{ad}\bar{\rho})$

We shall now establish general conditions under which $Ш^2_S(E, \mathrm{ad}\bar{\rho}) = 0$ provided that we know that $Ш^2_S(E, \mathbf{F}_p^{\varphi}) = 0$ for $\varphi \in \mathcal{V}$. To achieve this we shall investigate conditions on short exact sequences of $G_S(E)$-modules for which the induced sequence of $Ш^2_S$-terms is middle exact or right exact, or exact. The conditions will be conditions on global or local H^0-terms of the Galois modules in the sequence, as those terms are the only objects that can be reasonably calculated. Before looking at the general case, we shall discuss the most basic example that will explain the definitions and lemmas to come. For this let

$$0 \to M' \to M \to M'' \to 0 \tag{2}$$

be a short exact sequence of $G_S(E)$-modules. From Poitou-Tate and the long exact sequences of

Galois cohomology we obtain the following diagram.

$$\begin{array}{ccccccc}
0 \to Ш^1_S(E,M'') & \to & H^1(G_S(E),M'') & \to & \coprod_{v\in S} H^1(G_{E_v},M'') & \to & H^1(G_S(E),M''^*(1))^* \\
& & \downarrow \beta'' & & \downarrow \gamma'' & & \downarrow \delta'' \\
0 \to Ш^2_S(E,M') & \to & H^2(G_S(E),M') & \xrightarrow{\varepsilon} & \coprod_{v\in S} H^2(G_{E_v},M') & \xrightarrow{\varepsilon'} & H^0(G_S(E),M'^*(1))^* \to 0 \\
& & \downarrow \beta & & \downarrow \gamma & & \downarrow \delta \\
0 \to Ш^2_S(E,M) & \to & H^2(G_S(E),M) & \xrightarrow{\eta} & \coprod_{v\in S} H^2(G_{E_v},M) & \xrightarrow{\eta'} & H^0(G_S(E),M^*(1))^* \to 0 \\
& & \downarrow \beta' & & \downarrow \gamma' & & \downarrow \delta' \\
0 \to Ш^2_S(E,M'') & \to & H^2(G_S(E),M'') & \to & \coprod_{v\in S} H^2(G_{E_v},M'') & \to & H^0(G_S(E),M''^*(1))^* \to 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & & 0 & & 0
\end{array}$$

One can now apply the snake lemma to the two central vertical columns after modding out the images of β'' and γ'', respectively, to obtain the following lemma on the induced sequence of $Ш^2_S$ applied to (2).

Lemma 4.1.1 *The sequence obtained by applying $Ш^2_S$ to (2) is right exact if and only if the following sequence is exact.*

$$0 \to Ш^2_S(E,M')/(Ш^2_S(E,M') \cap \mathrm{Im}(\beta'')) \to \ker(\beta') \to \ker(\gamma') \to \ker(\delta') \to 0$$

More precisely, one has.

(i) $Ш^2_S(E,M') \to Ш^2_S(E,M)$ *is injective if and only if* $Ш^2_S(E,M') \cap \mathrm{Im}(\beta'') = 0$*, where the intersection is taken inside* $H^2(G_S(E),M')$*.*

(ii) $Ш^2_S(E,M') \to Ш^2_S(E,M) \to Ш^2_S(E,M'')$ *is exact (in the middle) if and only if*

$$0 \to Ш^2_S(E,M')/(Ш^2_S(E,M') \cap \mathrm{Im}(\beta'')) \to \ker(\beta') \to \ker(\gamma')$$

is left exact.

(iii) $Ш^2_S(E,M) \to Ш^2_S(E,M'')$ *is surjective if and only if*

$$\ker(\beta') \to \ker(\gamma') \to \ker(\delta') \to 0$$

is right exact.

Corresponding to the three cases above, we shall say that $Ш^2_S$ applied to (2) is injective on the left, middle exact, or surjective on the right, resp. Some further diagram chases together and Tate local duality prove the following Lemma.

Lemma 4.1.2 *For* $Ш^2_S$ *applied to (2), the following hold.*

(i) It is surjective on the right $\iff \varepsilon'(\ker(\gamma)) \cong \ker(\delta) \iff \mathrm{Im}(\gamma^*) \cap \mathrm{Im}(\varepsilon'^*) = \mathrm{Im}(\varepsilon'^*\delta^*)$.

(ii) It is exact in the middle if $\ker(\gamma)$ *maps injectively under* ε' *to* $\ker(\delta)$. *The latter is equivalent to* $\mathrm{Im}(\gamma^*) + \mathrm{Im}(\varepsilon'^*) = \coprod_{v\in S} H^0(G_{E_v}, M'^*(1))$.

(iii) If β'' *is zero, then the statement in (ii) is an equivalence, and furthermore* $Ш^2_S$ *is automatically injective on the left.*

For conditions (i) and (ii) the relevant diagram to consider is

$$\begin{array}{ccc} \coprod_{v\in S} H^0(G_{E_v}, M'^*(1)) & \overset{\varepsilon'^*}{\leftarrow} & H^0(G_S(E), M'^*(1)) \\ \uparrow \gamma^* & & \uparrow \delta^* \\ \coprod_{v\in S} H^0(G_{E_v}, M^*(1)) & \overset{\eta'^*}{\leftarrow} & H^0(G_S(E), M^*(1)) \end{array}$$

Let W_0 be a finite, indecomposable $\mathbf{F}_p[G_S(E)]$-module with a filtration

$$0 = W_n \subset \cdots \subset W_1 \subset W_0$$

such that all $W_{i-1}/W_i = V_i$ are irreducible $\mathbf{F}_p[G_S(E)]$-modules for $1 \le i \le n$. We say that the filtration is **good** for $Ш^2$ on $S' \subset S$, if for all $i = 1, \ldots, n-1$, in the diagram

$$\begin{array}{ccc} \coprod_{v\in S'-S_\infty} H^0(G_{E_v}, W_i^*(1)) & \overset{\varepsilon'^*_i}{\leftarrow} & H^0(G_S(E), W_i^*(1)) \\ \uparrow \gamma_i^* & & \uparrow \delta_i^* \\ \coprod_{v\in S'-S_\infty} H^0(G_{E_v}, W_{i-1}^*(1)) & \overset{\varepsilon'^*_{i-1}}{\leftarrow} & H^0(G_S(E), W_{i-1}^*(1)) \end{array} \tag{3}$$

the inclusion $\mathrm{Im}(\gamma_i^*) + \mathrm{Im}(\varepsilon_i'^*) \subset \coprod_{v \in S'-S_\infty} H^0(G_{E_v}, W_i^*(1))$ is an equality, and if furthermore $S_p \cup S_\infty \subset S'$, and if all the V_i are unramified outside S'.

Remark 4.1.3 By a simple inductive argument, the condition $H^2(G_S(E), V_i) = 0$ for $i = 2, \ldots, n$ implies that the filtration of W_0 is good for Ш^2 on S. By Poitou-Tate, this condition is equivalent to Ш$^2_S(E, V_i) = 0$ together with the condition that

$$H^0(G_S(E), V_i^*(1)) \to \Pi_{v \in S-S_\infty} H^0(G_{E_v}, V_i^*(1))$$

is an isomorphism. As primarily we seek for conditions under which the vanishing of the Ш$^2_S(E, V_i)$ implies that of Ш$^2_S(E, W_0)$, this provides us with a condition purely in terms of the V_i. However, as one can easily convince oneself, it is a lot more restrictive than the above condition of 'good filtration'.

Example 4.1.4 An important example of such an $\mathbf{F}_p[G_S(E)]$-module is $W_0 = \mathrm{ad}\bar{\rho}^0$. Its filtration is defined by the exact sequences

$$0 \to V_3 = \mathbf{F}_p^{\psi^{-1}} \to W_1 \to V_2 = \mathbf{F}_p \to 0$$

$$0 \to W_1 \to \mathrm{ad}^0\bar{\rho} \to V_1 = \mathbf{F}_p^{\psi} \to 0$$

where $W_1 \cong \left\{ \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix},\ a, b \in \mathbf{F}_p \right\}$. In this situation, one finds the following two conditions, one from each of the short exact sequences, for the filtration to be good for Ш^2 on the a set $S' \subset S$. First, we need that there is at most one $\nu \in S'$ for which $p | \#\bar{\rho}(G_{E_\nu})$ and $\psi_{|G_{E_\nu}} = \omega^{-1}_{|G_{E_\nu}}$, and for this prime, one must have that the order of ω as a character of G_{E_ν} and as a character of $G_S(E)$ is the same. Second, we need that for all places $\nu \in S'$ $\mu_p(E_\nu) = \{1\}$.

We specialize this to the representation $\bar{\rho}$ of §3.3, i.e. $E = \mathbf{Q}$, $F = \mathbf{Q}(\zeta_p)$, $S' = S = \{p, \infty\}$. Thus ψ, ψ^{-1}, ω factor through $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong \mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$. Hence their orders are the same if considered as a character of $G_S(E)$, or as a character of G_{E_ν} where here $\nu = p$. From this

it is obvious, that the conditions we found above are satisfied, and therefore that the (unique) filtration (by irreducibles) of W_0 is good for $Ш^2$ on S'.

From the discussion before the definition of 'good filtration', by a simple induction argument, we obtain the following lemma.

Lemma 4.1.5 *With the above notation, if* $Ш^2_S(E, V_i) = 0$ *for all* i*, and if* W_0 *has a good filtration for* $Ш^2$ *on* S*, then* $Ш^2_S(E, W_0) = 0$ *and thus* $H^2(G_S(E), W_0)$ *is dual to the cokernel of*

$$H^0(G_S(E), W_0^*(1)) \to \coprod_{v \in S' - S_\infty} H^0(G_{E_v}, W_0^*(1))$$

In Section 4.2, we shall need a slight variant of the above result for which we introduce some further notation. By Poitou-Tate, one has the following description of $Ш^2_S(E, M)$ for any finite $G_S(E)$-module M

$$0 \to Ш^2_S(E, M)^* \to H^1(G_S(E), M^*(1)) \to \coprod_{v \in S} H^1(G_{E_v}, M^*(1))$$

We now define a larger obstruction group $Ш^2_{S,S'}(E, M)$ for a subset S' of S, that contains all places of S_p and S_∞, by

$$0 \to Ш^2_{S,S'}(E, M)^* \to H^1(G_S(E), M^*(1)) \to \coprod_{v \in S'} H^1(G_{E_v}, M^*(1)) \oplus \coprod_{v \in S - S'} H^1(I_v, M^*(1))^{G_{E_v}}$$

As M is a $G_S(E)$-module, S contains all places where the representation of G_E on M ramifies. One can easily verify the following simple properties. If one has $S' \subset S'' \subset S$ in the notation above, then $Ш^2_{S,S'}(E, M)$ is a quotient of $Ш^2_{S,S''}(E, M)$. Moreover if Δ_S is a set of places disjoint from S, then

$$Ш^2_{S,S'}(E, M) \supset Ш^2_{S \cup \Delta_S, S'}(E, M) = Ш^2_{S \cup \Delta_S, S' \cup \Delta_S}(E, M)$$

Lemma 4.1.6 *We assume that we are given a filtration of* $G_S(E)$*-modules* W_i *as above. We suppose that for a fixed place* $v \in S - (S_p \cup S_\infty)$*, the canonical map* $W_{i-1} \to V_i$ *induces an*

isomorphism $(V_i^*(1))^{I_v} \xrightarrow{\sim} (W_{i-1}^*(1))^{I_v}$ *of invariants under the inertia group* I_v *of* G_{E_v}*. Then one has an injection*

$$H^1(I_v, V_i^*(1))^{G_{E_v}} \to H^1(I_v, W_{i-1}^*(1))^{G_{E_v}}$$

PROOF: Our assumption implies that the canonical maps

$$H^0(G_{E_v}/I_v, (V_i^*(1))^{I_v}) \to H^0(G_{E_v}/I_v, (W_{i-1}^*(1))^{I_v})$$

$$H^0(G_{E_v}, V_i^*(1)) \to H^0(G_{E_v}, W_{i-1}^*(1))$$

are isomorphisms. This explains the zeros on the top in the following diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & H^0(G_{E_v}/I_v, (W_i^*)^{I_v}(1)) & \to & H^0(G_{E_v}, W_i^*(1)) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 \to & & H^1(G_{E_v}/I_v, (V_i^*)^{I_v}(1)) & \to & H^1(G_{E_v}, V_i^*(1)) & \to & H^1(I_v, V_i^*(1))^{G_{E_v}} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 \to & & H^1(G_{E_v}/I_v, (W_{i-1}^*)^{I_v}(1)) & \to & H^1(G_{E_v}, W_{i-1}^*(1)) & \to & H^1(I_v, W_{i-1}^*(1))^{G_{E_v}} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 \to & & H^1(G_{E_v}/I_v, (W_i^*)^{I_v}(1)) & \to & H^1(G_{E_v}, W_i^*(1)) & \to & H^1(I_v, W_i^*(1))^{G_{E_v}} & \to & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

The rows are inflation-restriction exact sequences, and the columns are parts of long exact sequences of cohomology. The map between the H^0 terms is an isomorphism. Hence by the snake lemma, the asserted injectivity follows. ∎

One can now prove the following lemma by the same devissage technique as in the proof of Lemma 4.1.5.

Lemma 4.1.7 *Let S' be a fixed set of places such that $S_p \cup S_\infty \subset S' \subset S$. We assume that we are given a good filtration for $Ш^2$ on S' of the $G_S(E)$-module W_0 (as above), that for all places $v \in S - (S' \cup S_\infty)$ and for all $i \geq 1$ the canonical map $W_{i-1} \to V_i$ induces an isomorphism $(V_i^*(1))^{I_v} \to (W_{i-1}^*(1))^{I_v}$, that the V_i are unramified outside S', and that $Ш^2_{S'}(E, V_i) = 0$ for all i. Then $Ш^2_{S,S'}(E, W_0) = 0$.*

We omit the proof.

We now return to the case $W_0 = \mathrm{ad}\bar{\rho}^0$. Its filtration is defined in Example 4.1.4. We have the following corollary of Lemma 4.1.5

Corollary 4.1.8 *If $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint and the filtration of $\mathrm{ad}^0\bar{\rho}$ is good for $Ш^2$ on S, then the deformation problem is globally unobstructed, that is $Ш^2_S(E, \mathrm{ad}\bar{\rho}) = 0$.*

Proof: Recall that as $\mathbf{F}_p[G_S(E)]$-module, we have $\mathrm{ad}\bar{\rho} = \mathbf{F}_p \oplus \mathrm{ad}^0\bar{\rho}$. The order of H is prime to p and $Ш^2_S(F, \mathbf{F}_p)_{\mathrm{triv}} = 0$, thus

$$Ш^2_S(E, \mathbf{F}_p) = Ш^2_S(F, \mathbf{F}_p)^H = 0.$$

We have $Ш^2_S(E, \mathbf{F}_p^\varphi) = Ш^2_S(F, \mathbf{F}_p^\varphi)^H = 0$, for all $\varphi \in \mathcal{V}$. By Lemma 4.1.5, $Ш^2_S(E, \mathrm{ad}^0\bar{\rho}) = 0$ and

$$Ш^2_S(E, \mathrm{ad}\bar{\rho}) = Ш^2_S(E, \mathrm{ad}^0\bar{\rho}) \oplus Ш^2_S(E, \mathbf{F}_p) = 0. \quad \blacksquare$$

4.2 Minimal deformations

We now consider a representation

$$\bar{\rho} : \mathrm{Gal}(\bar{E}/E) \to \mathrm{GL}_2(\mathbf{F}_p) \text{ where } \bar{\rho} = \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} \text{ and } \psi = \chi_2\chi_1^{-1} \text{ is odd.}$$

We assume that ψ is unramified outside p, and we let $S = S_p \cup S_\infty \cup \mathrm{Ram}(\bar{\rho})$. By twisting $\bar{\rho}$ by a suitable character, one can achieve that $\mathrm{Ram}(\psi) = \mathrm{Ram}(\chi_1) \cup \mathrm{Ram}(\chi_2)$. Thus we shall

henceforth assume this to hold. In particular this means that the $(1,2)$ entry $*$ of $\bar{\rho}$ is ramified at all places in $S-(S_p \cup S_\infty)$, but neither χ_1 nor χ_2 are ramified at any of these places. This also implies that $\mathrm{Ram}(\bar{\rho}) = \mathrm{Ram}(\mathrm{ad}\bar{\rho})$. We shall again impose

$$\mathrm{Cl}_{S_p}(F(\mu_p))_{\omega\mathcal{V}} = 0, \text{ for } \mathcal{V} = \{\mathrm{triv}, \psi, \psi^{-1}\}.$$

Under this hypotheses we are able to apply the local-to-global principle from [1], in particular the results from §7, to calculate more general universal deformation rings $R_{G_S}(\bar{\rho})$. Lemma 4.1.7 will be needed for the devissage of $\mathrm{ad}\bar{\rho}^0$. Even if the deformation problem is obstructed, we can compute the universal deformation ring $R_{G_S}(\bar{\rho})$. Our hypotheses on $\bar{\rho}$ imply that the relations of $R_{G_S}(\bar{\rho})$ come from tame relations of local Galois groups that can be given explicitly (§4.2, §4.3).

We need to introduce some more notation. First we define a minimal universal deformation ring, following the example of Wiles in [33], with however no restriction at the places above p. The corresponding universal deformation ring will turn out to be smooth. Hence the minimal deformation problem will be a good substitute for the above deformation problems (§3.3).

To motivate the definition of a minimal deformation functor, we briefly describe $\bar{\rho}_{|I_v}$ for ramified places $v \in S-(S_p \cup S_\infty)$, where I_v is the inertia subgroup of G_{E_v}. The group $\bar{\rho}(I_v)$ is a subquotient of the tame inertia quotient of G_{E_v}. It follows that $\bar{\rho}(I_v)$ is an abelian subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$ independently of $\bar{\rho}$ and v. So either $\bar{\rho}(I_v)$ consists entirely of matrices of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ and of homotheties, or it is inside a conjugate of H. The latter situation is impossible under our assumption that χ_1, χ_2 are unramified outside p. We want our minimal deformations to have as little ramifications as possible at places not above p or ∞.

A **minimal deformation** of $\bar{\rho}$ is a deformation ρ satisfying the additional condition:

$$\text{If } v \notin S_p \cup S_\infty \text{ and if } \bar{\rho}(I_v) = U, \text{ then } \rho_{|I_v} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \tag{4}$$

So for places $v \in \mathrm{Ram}(\bar{\rho}) - (S_p \cup S_\infty)$, i.e. places where p divides $\bar{\rho}(I_v)$, we do allow ramification,

but of a very special type. For example if the universal deformation ring is of characteristic zero, at such a place v there is infinite ramification. Let $\bar{\mathbf{Z}}_p$ denote the ring of integers of $\bar{\mathbf{Q}}_p$. Our condition (4) might seem surprising at first, as there are elements in $\mathrm{GL}_2(\bar{\mathbf{Z}}_p)$ of order p whose reduction modulo p is $\begin{pmatrix} 1 & 1 \\ & \\ 0 & 1 \end{pmatrix}$. The problem with such elements though is, that they are not defined over $\mathbf{Z}_p$, but only over a ramified extension of it. As we do not want to enlarge the universal deformation ring superficially, we choose to use, as is also done in [33], the word **minimal** for a type of deformation that does impose no additional condition on the universal deformation ring. 'Minimal' can also be interpreted in the sense that the set of tangential deformations is as small as possible without restricting the deformations at places above p.

We define the functor of minimal deformations of $\bar{\rho}$

$$\mathcal{F} : \mathcal{C} \to \mathrm{Set},\ R \mapsto \{\text{minimal deformations of } \bar{\rho} \text{ to } R\}$$

One can verify that if $(M_2(\mathbf{F}_p))^{\mathrm{Im}\bar{\rho}} = \mathbf{F}_p$, then $\mathcal{F}$ is representable. We denote by $(R^{\mathrm{min}}_{G_S}(\bar{\rho}), \rho^{\mathrm{min}}_U)$ the universal pair of $\mathcal{F}$.

Local deformations are deformations of the residual representation $\bar{\rho}_{|G_{E_v}}$. For all but a few ramified places the local deformation functors have only a versal hull. As it turns out, the equations defining this hull determine under suitable assumptions the ideal of relations of the universal deformation ring, see [1]. Our goal is to make use of this.

Let

$$\mathcal{L}_v^{\mathrm{nr}} = H^1(G_{E_v}/I_v, \mathrm{ad}\bar{\rho}^{I_v}) \text{ and } \mathcal{L}_v = H^1(G_{E_v}, \mathrm{ad}\bar{\rho})$$

For a ring $R \in \mathcal{C}$ one defines its mod p tangent space as $t_R = \mathfrak{m}_R/(\mathfrak{m}_R^2, p)$. Then $(\mathcal{L}_v^{\mathrm{nr}})^*$ is canonically isomorphic to the mod p tangent space of local unramified deformations of $\bar{\rho}_{|G_{E_v}}$. Moreover $(\mathcal{L}_v)^*$ is canonically isomorphic to the mod p tangent space of local unrestricted deformations of

$\bar{\rho}_{|G_{E_v}}$. Let

$$\mathcal{L}_v^{\min} = \begin{cases} \mathcal{L}_v & \text{if } v \in S_p \cup S_\infty \\ \mathcal{L}_v^{\mathrm{nr}} & \text{otherwise} \end{cases} \qquad \mathcal{L}_v^{S} = \begin{cases} \mathcal{L}_v & \text{if } v \in S \\ \mathcal{L}_v^{\mathrm{nr}} & \text{otherwise} \end{cases}$$

Then $t_{R^{\min}_{G_S(\bar{\rho})}}$ is isomorphic to the kernel of

$$H^1(G_S(E), \mathrm{ad}\bar{\rho}) \to Ш_{v\in S} H^1(G_{E_v}, \mathrm{ad}\bar{\rho})/\mathcal{L}_v^{\min}$$

and $t_{R_{G_S}(\bar{\rho})}$ is isomorphic to the kernel of

$$H^1(G_S(E), \mathrm{ad}\bar{\rho}) \to Ш_{v\in S} H^1(G_{E_v}, \mathrm{ad}\bar{\rho})/\mathcal{L}_v,$$

see [2]. Using the perfect pairing

$$H^1(G_{E_v}, \mathrm{ad}\bar{\rho}) \times H^1(G_{E_v}, \mathrm{ad}\bar{\rho}^*(1)) \to H^2(G_{E_v}, \mathbf{F}_p(1))$$

induced by the cup product, one defines $\mathcal{L}_v^{\perp}$ (resp. $\mathcal{L}_v^{\mathrm{nr}\perp}$) as the annihilator under this pairing of $\mathcal{L}_v$ (resp. of $\mathcal{L}_v^{\mathrm{nr}}$). One can check that for v not above p

$$\mathcal{L}_v^{\mathrm{nr}\perp} = H^1(G_{E_v}/I_v, (\mathrm{ad}\bar{\rho}^*(1))^{I_v})$$

If $\mathrm{ad}\bar{\rho}$ is unramified at v, this can be found in [27, II.5.5]. For $v \in S - (S_p \cup S_\infty)$, this could be shown by an analogous argument. Thus one defines

$$\mathcal{L}_v^{\min\perp} = \begin{cases} \mathcal{L}_v^{\perp} & \text{if } v \in S_p \cup S_\infty \\ \mathcal{L}_v^{\mathrm{nr}\perp} & \text{otherwise} \end{cases} \qquad \mathcal{L}_v^{S\perp} = \begin{cases} \mathcal{L}_v^{\perp} & \text{if } v \in S \\ \mathcal{L}_v^{\mathrm{nr}\perp} & \text{otherwise} \end{cases}$$

Lemma 4.2.1 *If* $\mathrm{Cl}_{S_p}(F(\mu_p))_{\omega\mathcal{V}} = 0$ *and if the filtration of* $\mathrm{ad}\bar{\rho}^0$ *is good for* $Ш^2$ *on* $S_p \cup S_\infty$, *then the kernel of*

$$H^1(G_S(E), \mathrm{ad}\bar{\rho}^*(1)) \to Ш_{v\in S} H^1(G_{E_v}, \mathrm{ad}\bar{\rho}^*(1))/\mathcal{L}_v^{\min\perp}$$

is zero.

PROOF: By definition, the above kernel is $Ш^2_{S,S_p}(E, \mathrm{ad}\bar{\rho}^*(1))$. To analyze it, one decomposes $\mathrm{ad}\bar{\rho} = \mathbf{F}_p^{\mathrm{triv}} \oplus \mathrm{ad}\bar{\rho}^0$. The triviality of $Ш^2_{S,S_p}(E, \mathbf{F}_p^*(1))$ is immediate from the remarks above Lemma 4.1.6. The triviality of $Ш^2_{S,S_p}(E, \mathrm{ad}\bar{\rho}^{0*}(1))$ is a consequence of Lemma 4.1.7, applied to $S' = S_p \cup S_\infty$ and $W = \mathrm{ad}\bar{\rho}^0$. ∎

From Poitou-Tate, as described in [33], one now computes the dimensions of the mod p tangent spaces of $R_{G_S}(\bar{\rho})$ and $R^{\min}_{G_S}(\bar{\rho})$:

$$\dim_{\mathbf{F}_p} t_{R^{\min}_{G_S}(\bar{\rho})} = 3 \quad \dim_{\mathbf{F}_p} t_{R_{G_S}(\bar{\rho})} = 3 + r \text{ where } r = \sum_{v \in S - S_p} h^2(G_{E_v}, \mathrm{ad}\bar{\rho})$$

From the first form of the local to global principle in [1], Theorem 5.2 and the remark thereafter, it follows that $R_{G_S}(\bar{\rho})$ has a presentation as a quotient of $\mathbf{Z}_p[[X_1, X_2, X_3, T_1, \ldots, T_r]]$ by r local equations. These equations come from the local deformation problems for the ramified primes different from p. Their explicit shape we will be described below.

Let $v \in S - (S_p \cup S_\infty)$. Since $\mathrm{Ram}(\bar{\rho}) = \mathrm{Ram}(\mathrm{ad}\bar{\rho})$, we find $h^1(G_{E_v}, \mathrm{ad}\bar{\rho}^0) = 1$. The variables of the versal hull of the local deformation problem at v that correspond to ramification of the local versal deformation are called **local ramified variables**. By [3] the relations of the local deformation versal hull at v are equations involving only local ramified variables.

As r is the difference of the dimensions of $t_{R_{G_S}(\bar{\rho})}$ and $t^{\min}_{R_{G_S}(\bar{\rho})}$, we can assume that the variables T_i are images of the local ramified variables under the local to global map, c.f. [1]. So if we denote by $f_i = 0$ the equation satisfied by the local variable mapping to T_i, then we have globally the equation $f_i(T_i) = 0$.

Furthermore the minimal deformation problem corresponds to choosing for each T_i a certain solution in $p\mathbf{Z}_p$ of $f_i(T_i) = 0$. From this discussion we find

Theorem 4.2.2 *Let* $\bar{\rho} = \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ *be an odd representation where* $\chi_1^{-1}\chi_2$ *is unramified outside*

S_p. If $\mathrm{Cl}_{S_p}(F(\mu_p))_{\omega\mathcal{V}} = 0$, and if the filtration of $\mathrm{ad}\bar{\rho}^0$ is good for $Ш^2$ on $S_p \cup S_\infty$, then

$$R_S^{\min}(\bar{\rho}) = \mathbf{Z}_p[[T_1, T_2, T_3]]$$

If further $\mathrm{Ram}(\bar{\rho}) = \mathrm{Ram}(\mathrm{ad}\bar{\rho})$ then

$$R_{G_S}(\bar{\rho}) = \mathbf{Z}_p[[X_1, X_2, X_3, T_1, \ldots, T_r]]/(f_1(T_1), \ldots, f_r(T_r))$$

where $S = S_p \cup S_\infty \cup \mathrm{Ram}(\bar{\rho})$, $r = \sum_{v \in S - S_p} h^2(G_{E_v}, \mathrm{ad}\bar{\rho})$ and the relations f_i are as described below.

It remains to explain what the equations $f_i = 0$ are. Let $v \in S$ be a place above $l \neq p$. The number of local relations for v is $h^2(G_{E_v}, \mathrm{ad}\bar{\rho})$, which is zero, one or two in our situation. This is the same as the number of local ramified variables for this place. There are two kinds of equations, those corresponding to a local deformation problem of fixed determinant, see [1], and those corresponding to a deformation of the determinant. The latter are obtained using class field theory and were implicitly described in [16]. We now recall in detail these equations.

If E_v contains p-th roots of unity, then there is one ramified variable T describing the deformations of the determinant. The corresponding equation is $(1+T)^{p^n} - 1 = 0$, where p^n is the order of the p-Sylow subgroup of the roots of unity of E_v, i.e. $|\mu(E_v)|$. One can instead take the p-Sylow subgroup of the multiplicative group of the residue field of E_v.

We now describe the relation of the local versal hull for deformations with fixed determinant. Since $\mathrm{Ram}\bar{\rho} = \mathrm{Ram}(\mathrm{ad}\bar{\rho})$, $\bar{\rho}(I_v) \cong U$. Let $p^n = |\mu(F_v)|$. Then the local equation at v is $Tg_{p^n}(T) = 0$, where g_{p^n} is the following polynomial

$$g_{p^n}(T) = \sum_{k=0}^{(p^n-1)/2} b_{p^n,k} T^k \quad \text{with} \quad b_{p^n,k} = \frac{p^n}{(2k+1)!} \prod_{j=0}^{k-1} \left(p^{2n} - (2j+1)^2\right)$$

Thus g_{p^n} is a Weierstrass polynomial of degree $(p^n-1)/2$, [1, Lemma 3.10].

Remark 4.2.3 By the same method, one can treat intermediate functors between Def and $\mathcal{F}$, imposing various conditions on the local deformations at $v \in S - (S_p \cup S_\infty)$.

One can also increase S by unramified primes v such that the image under $\bar{\rho}$ of a corresponding Frobenius element has distinct eigenvalues.

4.3 Examples associated to an elliptic curve

We now give a few examples of explicit universal deformation rings $R_{G_S}(\bar{\rho})$ for Borel type representations $\bar{\rho}$ associated to the action of $G_{\mathbf{Q}}$ on p-torsion points of elliptic curves.

Let $\mathcal{E}$ denote an elliptic curve over $E = \mathbf{Q}$. We consider the action of $G_{\mathbf{Q}}$ on p-torsion points, i.e. $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$. In all our examples we have $F = \mathbf{Q}(\zeta_p)$ and $\bar{\rho} = \begin{pmatrix} 1 & * \\ & \\ 0 & \omega \end{pmatrix}$, i.e. E has a p-torsion point. We recall, Example 4.1.4, that in this case the filtration of $\mathrm{ad}^0_{\bar{\rho}}$ is good for $Ш^2$ on $S_p \cup S_\infty = \{p, \infty\}$. By l we denote a prime different from p for which $p \mid \#\bar{\rho}(I_l)$. The set S shall be the set of places where $\bar{\rho}$ ramifies. In all examples one can verify that $\mathrm{Ram}(\bar{\rho}) = \mathrm{Ram}(\mathrm{ad}\bar{\rho})$. For $l \neq p$ one finds

$$\begin{aligned} H^2(G_{\mathbf{Q}_l}, \mathrm{ad}\bar{\rho}^0)^* &\cong H^0(G_{\mathbf{Q}_l}, \mathrm{ad}\bar{\rho}^{0*}(1)) \cong H^0(G_{\mathbf{Q}_l}, \mathbf{F}_p^{\omega^{1-1}}) \cong \mathbf{F}_p \\ H^2(G_{\mathbf{Q}_l}, \mathbf{F}_p)^* &\cong H^0(G_{\mathbf{Q}_l}, \mathbf{F}_p^{\omega}) \end{aligned}$$

Thus the dimension of the first group is always one, and that of the latter is one precisely when $l \equiv 1 (\mathrm{mod}\ p)$ and zero otherwise. Correspondingly, the number of ramified variables at l is two or one.

We use examples from [26] and take the numbering from there.

• First one assumes $\mathcal{E}$ is given by $y^2 + y = x^3 - x^2$, this is [26, 5.5.1]. For $p = 5$ the curve $\mathcal{E}$ has a five torsion point. The discriminant is $\Delta = -11$ and the 11-adic valuation of the j-invariant of $\mathcal{E}$ is negative. Thus there is multiplicative reduction at $l = 11$. As $5 \nmid v_{11}(\Delta)$, 5 divides $\#\bar{\rho}(I_{11})$. Clearly $11 \equiv 1 (\mathrm{mod}\ 5)$ so $r = 2$. The order of the 5-Sylow subgroup of $\mathbf{F}_{11}^*$ is 5. One computes $g_5(T) = 5 + 20T + 16T^2$. We let $S = \{5, 11, \infty\}$.

From the above, one obtains

$$R_{G_S}(\bar{\rho}) \cong \mathbf{Z}_5[[T_1, T_2, T_3, T_4, T_5]]/(T_4 g_5(T_4), (1+T_5)^5 - 1)$$

• In the next example $\mathcal{E}$ is given by $y^2 + xy + y = x^3 - x$, [26, 5.5.3]. Here $\Delta = -2^2 7$ and we take $p = 3$. Then $\bar{\rho}$ has the same shape as above, only with 3 replacing 5. For l we can take 2 as well as 7. As j is odd, both places satisfy $H^2(G_{\mathbf{Q}_v}, \mathrm{ad}\bar{\rho}^0) \neq 0$. One computes the 3-Sylow groups of $\mathbf{F}_l^*(\zeta_3)$ for $l = 2, 7$. Their orders are three in both cases. Here $g_3(T) = 3 + 4T$. With $S = \{2, 3, 7, \infty\}$ one has

$$R_{G_S}(\bar{\rho}) \cong \mathbf{Z}_3[[T_1, T_2, T_3, T_4, T_5, T_6]]/(T_4 g_3(T_4), T_5 g_3(T_5), (1+T_6)^3 - 1)$$

• Similarly one can treat the curve [26, 5.7.4] for $p = 3$. (For $p = 5$ that curve is not interesting for our purposes as 5 is then the only prime where $\bar{\rho}_5$ ramifies).

• Finally let $\mathcal{E}$ be given by $y^2+xy+y = x^3-x^2-3x+3$, [26, 5.5.4]. Here $p = 7$ and $S = \{7, 13, \infty\}$ (as $7|v_2(\Delta)$, there is no ramification at 2). One calculates $g_7(T) = 7 + 56T + 112T^2 + 64T^3$ and obtains

$$R_{G_S}(\bar{\rho}) \cong \mathbf{Z}_7[[T_1, T_2, T_3, T_4]]/(T_4 g_7(T_4))$$

5 From global unobstructedness to the prime-to-adjoint condition

In §4.1 we have shown that if $Ш^2_S(F, \mathbf{F}_p)$ is prime-to-adjoint and if some local conditions hold then the deformation problem is globally unobstructed, i.e. $Ш^2_S(E, \mathrm{ad}\bar{\rho}) = 0$. In §5.1 we establish sufficient conditions under which the globally unobstructed deformation problem implies the prime-to-adjoint condition. Then we interpret these conditions (§5.2).

5.1 Partial reciprocal

We use the same notation as in Section 4.1. By L (resp. L^i) we denote the fixed field of the kernel of the representation W_0 (resp. V_i). Let $G_S(L) = \mathrm{Gal}(E_S/L)$ and $G_S(L^i) = \mathrm{Gal}(E_S/L^i)$. We recall that W_0 was unramified outside S.

Lemma 5.1.1 *If all maps* $\mathrm{res} : H^2(G_S(L^i), \mathbf{F}_p) \to H^2(G_S(L), \mathbf{F}_p)$ *are injective and if the groups* $\mathrm{Gal}(L^i/E)$ *have orders prime to* p*, then the following sequences are exact*

$$0 \to H^2(G_S(E), W_i) \to H^2(G_S(E), W_{i-1}) \to H^2(G_S(E), V_i) \to 0 \; i = 1, \ldots, n-1.$$

Proof: We compare the long exact sequence of cohomology coming from the split exact sequence

$$0 \to W_i \to W_{i-1} \to V_i \to 0 \tag{5}$$

for $G_S(E) = \mathrm{Gal}(E_S/E)$ and $G_S(L) = \mathrm{Gal}(E_S/L)$ under restriction and obtain

$$\begin{array}{ccccccc} 0 \to & H^2(G_S(L), W_i) & \to & H^2(G_S(L), W_{i-1}) & \to & H^2(G_S(L), V_i) & \to 0 \\ & \uparrow & & \uparrow & & \uparrow & \\ & H^2(G_S(E), W_i) & \to & H^2(G_S(E), W_{i-1}) & \to & H^2(G_S(E), V_i) & \to 0 \end{array}$$

The exactness of the top row can be seen as follows. As L is the fixed field of $\ker W_0$ the involved L action on the modules is trivial, so the top sequence is the same as tensoring the sequence (5) with the group $H^2(G_S(L), \mathbf{F}_p)$. We claim that by decreasing induction on i starting with $i = n-1$ the bottom sequence is exact, and that all vertical arrows are injections.

For $i = n-1$ the two outer vertical arrows are injections. This follows from

$$H^2(G_S(E), V_i) \cong H^2(G_S(L^i), V_i)^{\mathrm{Gal}(L^i/E)} \subset H^2(G_S(L^i), V_i) \to H^2(G_S(L), V_i)$$

which holds for all i, where the first isomorphism comes from the Hochschild-Serre spectral sequence, and the last injection from our injectivity hypotheses, as by definition of L^i (and hence also of L) one simply has $H^2(G_S(L^i), V_i) \cong H^2(G_S(L^i), \mathbf{F}_p) \otimes V_i$. It follows that the bottom

sequence must be exact and that the middle arrow must be an injection. Now we proceed by downward induction using the same argument for all i. ∎

We can now combine the results of Lemma 4.1.2 with the Lemma above to obtain the following proposition by a simple induction argument.

Proposition 5.1.2 *We keep the assumptions of Lemma 5.1.1. Furthermore we assume that for* $i = 1, \ldots, n-1$, *in diagram 3 we have* $\mathrm{Im}(\gamma_i^*) \cap \mathrm{Im}(\varepsilon_i'^*) = \mathrm{Im}(\varepsilon_i'^* \delta_i^*)$. *Then, if* $Ш_S^2(E, W_0) = 0$, *it follows that* $Ш_S^2(E, V_i) = 0$ *for* $i = 1, \ldots, n$.

Remark 5.1.3 One can also combine the conditions of parts (i) and (ii) to obtain the following result. If one assumes the conditions of Lemma 5.1.1 and if one assumes for $i = 1, \ldots, n-1$ in the diagram (3) that $\varepsilon_i'^*$ induces an isomorphism between the cokernels of γ_i^* and δ_i^*, then the vanishing of $Ш_S^2(E, W_0) = 0$ is equivalent to that of $Ш_S^2(E, V_i)$ for all $i = 1, \ldots, n$.

In the special case of $\mathrm{ad}_{\bar{\rho}}^0$, the condition that the diagram (3) satisfies the above property is equivalent to the conditions stated in example 4.1.4 and the further condition in the case $\omega = \psi$ (as characters of $G_S(E)$), that there is a place ν in S above p for which $p | \#\bar{\rho}(G_{E_\nu})$. (For $\omega \neq \psi$ no further condition is necessary.)

Corollary 5.1.4 *Assume that* $H^2(G_S(F), \mathbf{F}_p) \to H^2(G_S(L), \mathbf{F}_p)$ *is injective and that the filtration of* $\mathrm{ad}_{\bar{\rho}}^0$ *satisfies the conditions of example 4.1.4 and the condition of the previous remark. Then* $Ш_S^2(E, \mathrm{ad}^0 \bar{\rho}) = 0$ *if and only if* $Ш_S^2(F, \mathbf{F}_p)$ *is prime to adjoint.*

The conditions on the filtration of $\mathrm{ad}_{\bar{\rho}}^0$ *are satisfied in particular, if* $H^0(G_{E_\nu}, \mathbf{F}_p^{\varphi^*}(1)) = 0$ *for all* $\nu \in S - S_\infty$ *and for* $\varphi \in \{\psi, \mathrm{triv}\}$.

5.2 Interpretation of the injectivity condition

We now give an interpretation of the injectivity condition on

$$\mathrm{res} : H^2(G_S(L^i), \mathbf{F}_p) \to H^2(G_S(L), \mathbf{F}_p)$$

used in Lemma 5.1.1, in the case where $\mathrm{Gal}(L/L^i)$ is a p-group. This is the interesting case, as for extensions of order prime to p, the injectivity always holds. Let $P_S(L^i) = \mathrm{Gal}(L_S(p)/L^i)$. As $\mathrm{Gal}(L/L^i)$ is a p-group, as the kernel of $G_S(L^i) \twoheadrightarrow P_S(L^i)$ admits no finite p-group quotients, when computing cohomology groups, we can replace $G_S(L^i)$ by $P_S(L^i)$, and similarly $G_S(L)$ by the open subgroup $P_S(L) = \mathrm{Gal}(L_S(p)/L)$ of $P_S(L^i)$.

We give two interpretations of the injectivity condition on $\mathrm{res} : H^2(P_S(L^i), \mathbf{F}_p) \to H^2(P_S(L), \mathbf{F}_p)$. The first one is in terms of presentation of $P_S(L^i)$ and $P_S(L)$ by generators and relations. The second one is in terms of multiplicativity of λ-invariants of some classical Iwasawa modules.

We consider the following presentations.

$$\begin{array}{ccccccc}
1 \longrightarrow & \mathcal{R} & \longrightarrow & \mathcal{F} & \xrightarrow{\tau} & P_S(L^i) & \to 0 \\
 & \uparrow & & \uparrow & & \uparrow & \\
0 \longrightarrow & \mathcal{R} & \longrightarrow & \mathcal{F}' = \tau^{-1}(P_S(L)) & \longrightarrow & P_S(L) & \to 0 \\
 & \uparrow & & \gamma \uparrow & & \uparrow & \\
0 \longrightarrow & \mathcal{R}' & \longrightarrow & \mathcal{F}'' & \longrightarrow & P_S(L) & \to 0
\end{array}$$

The top row is a presentation of $P_S(L^i)$ where $\mathcal{F}$ is a free pro-p group of minimal rank. The middle row is the presentation of $P_S(L)$ induced from that of $P_S(L^i)$, by restricting the former to the free open subgroup $\mathcal{F}' = \tau^{-1}(P_S(L))$ of $\mathcal{F}$. However the middle row is not necessarily a minimal presentation. To obtain such a presentation, we choose a subset of a set of generators of $\mathcal{F}'$ whose image generates $P_S(L^i)$ and whose cardinality is the rank of $P_S(L)$. We call $\mathcal{F}''$ the subgroup generated by them inside $\mathcal{F}'$. Again it is a free pro-p group. For $\mathcal{R}'$ we take $\mathcal{R} \cap \mathcal{F}''$. We obtain maps

$$\mathcal{R}'/[\mathcal{R}', \mathcal{F}'']\mathcal{R}'^p \to \mathcal{R}/[\mathcal{R}, \mathcal{F}']\mathcal{R}^p \to \mathcal{R}/[\mathcal{R}, \mathcal{F}]\mathcal{R}^p$$

where the second one is clearly surjective and the composite of the two maps is the dual of the map res : $H^2(P_S(L^i), \mathbf{F}_p) \to H^2(P_S(L), \mathbf{F}_p)$. The following result is essentially due to Tsvetkov [30].

Lemma 5.2.1 *Assume* $\mathrm{Gal}(L/L^i)$ *is a p-group* ($p > 2$)*, then the following are equivalent*

(i) res : $H^2(P_S(L^i), \mathbf{F}_p) \to H^2(P_S(L), \mathbf{F}_p)$ *is injective.*

(ii) The map $\mathcal{R}'/[\mathcal{R}', \mathcal{F}'']\mathcal{R}'^p \to \mathcal{R}/[\mathcal{R}, \mathcal{F}']\mathcal{R}^p$ *is surjective.*

(iii) $\mathcal{R}$ *is contained in the Frattini subgroup* $\Phi(\mathcal{F}') := \mathcal{F}'^p[\mathcal{F}', \mathcal{F}']$.

(iv) $h^1(P_S(L), \mathbf{F}_p) - 1 = \#\mathrm{Gal}(L/L^i)(h^1(P_S(L^i), \mathbf{F}_p) - 1)$.

(v) $h^2(P_S(L), \mathbf{F}_p) = [L : L^i]h^2(P_S(L^i), \mathbf{F}_p)$.

Proof: The equivalence of the first two conditions was remarked above. The equivalence of conditions (iii) and (iv) is as follows. If (iii) holds, then the minimal number of generators of $P_S(L)$ is that of $\mathcal{F}'$. So we need to show that

$$h^1(\mathcal{F}, \mathbf{F}_p) - 1 = [\mathcal{F} : \mathcal{F}'](h^1(\mathcal{F}', \mathbf{F}_p) - 1)$$

This follows from the multiplicativity of the Euler-Poincaré characteristic and the fact that $\chi = \chi_{(1)}$ for free pro-p groups. Conversely, if (iv) holds, then none of the generators of $\mathcal{F}'$ can be superfluous in the presentation of $P_S(L)$. Thus $\mathcal{R}$ must lie inside $\Phi(\mathcal{F})$. For the equivalence of (iv) and (v) we note that $\mathrm{cd}_p G_S(L^i)$, $\mathrm{cd}_p G_S(L) \leq 2$. Thus the partial Euler-Poincaré characteristic $\chi_{(2)}$ is multiplicative, and hence $\chi_{(1)}$ is multiplicative if and only if h^2 is so, which proves the equivalence of (iv) and (v).

To see that (i) implies (iii), one reasons as follows. A 2-cocycle in $H^2(P_S(L^i), \mathbf{F}_p)$ can be thought of as a linear functional on $\mathcal{R}/[\mathcal{R}, \mathcal{F}]\mathcal{R}^p$. If $\bar{\tau} : \mathcal{R} \to \mathcal{F}'/\Phi(\mathcal{F}')$ is non-trivial, then we choose a non-zero linear functional f whose kernel contains the kernel of $\bar{\tau}$. The image of $\mathcal{R}'$ is contained

in $\Phi(\mathcal{F}')$, and thus f vanishes on the image of $\mathcal{R}'/[\mathcal{R}', \mathcal{F}'']\mathcal{R}'^p$ in $\mathcal{R}/[\mathcal{R}, \mathcal{F}']\mathcal{R}^p$. This means that f gets mapped to zero in $H^2(P_S(L), \mathbf{F}_p)$, contradicting the injectivity of res. Thus $\bar{\tau}$ is the trivial map. This means precisely that $\mathcal{R} \subset \Phi(\mathcal{F}')$. The converse is rather obvious, as (iii) implies that $\mathcal{F}' = \mathcal{F}''$ which directly implies (ii). ∎

Remark 5.2.2 If $P_S(L^i)$ is a Demuškin group, and $P_S(L)$ any proper open subgroup of it, one can show by an explicit calculation that the map on cohomology groups is trivial. So the condition of injectivity is closely related to the depth in which the relations that are used to describe $P_S(L^i)$ occur and possibly (not so in the Demuškin case), to the depth of the relations of subgroup corresponding to L.

For examples in which $P_S(L^i)$ is a Demuškin group, we refer the reader to [3] where however the groups $P_S(L^i)$ are local Galois groups. The calculations there clearly demonstrate that in the Demuškin situation the implication of Lemma 5.1.1 does not hold. In [3], the sequences on the H^2 level, arising through devissage, are not necessarily short exact sequences.

We now turn to a second type of interpretation of the equivalent conditions of Lemma 5.2.1, namely in terms of a multiplicativity condition (in an obvious sense) for the λ-invariant of some classical Iwasawa modules. Using this interpretation, it will be easy to construct explicit examples of fields L^i, L for which res is injective. We need some more notations.

Let M be any number field. Let $\mathcal{X}(M)$ be the Galois group over M_∞ of the maximal abelian unramified outside p pro-p extension of M_∞. We denote $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(M_\infty/M)]]$. Let $\lambda_\infty(M)$ be the λ-invariant of $\mathrm{tor}_\Lambda \mathcal{X}(M)$. For a finite extension N of M, let $\mathrm{Cap}(N_\infty/M) = \ker(K_2(M) \to K_2(N_\infty))$ where K_2 is the Milnor functor. Thanks to [21, Thm. 2.1], we have

Lemma 5.2.3 *Assume that $\mu_{2p} \subset M$, M has trivial μ-invariant and N/M is a p-extension unramified outside p such that* $\mathrm{Cap}(N_\infty/M) = 0$. *Then*

$$\lambda_\infty(N) = \lambda_\infty(M)[N_\infty : M_\infty]$$

Let $L_\infty^i = \varinjlim L_n^i$ (resp. $L_\infty = \varinjlim L_n$) be the cyclotomic $\mathbf{Z}_p$-extension of L^i (of L resp.). Let $r_n = h^2(\mathrm{Gal}(E_S/L_n^i), \mathbf{F}_p)$. It is known that the sequence r_n increases, and that it is stationary if and only if the μ-invariant of L^i is zero. In this case $r_\infty := \lim r_n \leq \lambda_\infty(L^i)$, with equality if and only if $F_\Lambda \mathcal{X}(L^i) = \mathcal{X}(L^i)/\mathrm{tor}_\Lambda \mathcal{X}(L^i)$ is a free Λ-module, that is if $\mathrm{Cap}_\infty(L^i) = 0$, see [22, Rem. 2.6]. Then for $n \gg 0$, if $\mathrm{Cap}_\infty(L^i) = \mathrm{Cap}_\infty(L) = 0$,

$$h^2(\mathrm{Gal}(E_S/L_n^i), \mathbf{F}_p) = \lambda_\infty(L^i) \quad \text{and} \quad h^2(\mathrm{Gal}(E_S/L_n), \mathbf{F}_p) = \lambda_\infty(L)$$

For sufficiently large n, $[L_\infty : L_\infty^i] = [L_n : L_n^i]$. If $\mu_{2p} \subset L^i$, it is known that the triviality of $\mathrm{Cap}(L_\infty/L^i)$ implies that of $\mathrm{Cap}_\infty(L^i)$, e.g. [21, proof of Lemma 2.2]. Thus if we apply Lemma 5.2.3 to L_n^i and L_n, we obtain the following

Corollary 5.2.4 *If* $\mathrm{Cap}(L_\infty/L^i) = \mathrm{Cap}_\infty(L) = 0$*, then for* n *large enough, it follows that*

$$h^2(\mathrm{Gal}(E_S/L_n^i), \mathbf{F}_p) = [L_n : L_n^i] h^2(\mathrm{Gal}(E_S/L_n), \mathbf{F}_p)$$

which means that condition (v) of Lemma 5.2.1 holds. Hence, at least asymptotically, the hypotheses of Proposition 5.1.2 are satisfied.

References

[1] G. Böckle, A local to global principle for deformations of Galois representations, Preprint no. 6 (1998), Institut für Experimentelle Mathematik, Uni GH Essen.

[2] G. Böckle, The generic fiber of the universal deformation space associated to a tame Galois representation, to appear in *Manuscripta Math.*

[3] G. Böckle, Demuškin groups with group actions and applications to deformations of local Galois representations, Preprint no. 4 (1998), Institut für Experimentelle Mathematik, Uni GH Essen.

[4] G. Böckle, Explicit Deformations of Even Galois Representations, to appear in *Math. Nachr.*

[5] N. Boston, Explicit deformation of Galois representations, *Invent. Math.* **103** (1991), 181-196.

[6] N. Boston, Families of Galois Representations – Increasing the Ramification, *Duke Math. Journ.* **66** vol. 3 (1992), 357-367.

[7] N. Boston and S.V. Ullom, Representations related to CM elliptic curves, *Math. Proc. Camb. Phil. Soc.* **113** (1993), 71-85.

[8] M. Flach, A finiteness theorem for the symmetric square of an elliptic curve, *Invent. Math.* **109** (1992), 307-327.

[9] V. Fleckinger and T. Nguyen Quang Do, Bases normales, unités et conjecture faible de Leopoldt, *Manuscripta Math.* **71** (1991), 183-195.

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

[11] R. Greenberg, On the Iwasawa invariants of totally real fields, *Amer. J. Math.* **96** (1976), 263-284.

[12] K. Iwasawa, On $\mathbf{Z}_l$-extensions of Algebraic Number Fields, *Ann. of Math.* **98** (1973), 246-326.

[13] M. Kolster, Remarks on étale K-theory and Leopoldt's conjecture, *Séminaire de Théorie des Nombres Paris* 91-92 (1992), 37-62.

[14] M. Kolster, T. Nguyen Quang Do and V. Fleckinger, Twisted S-units, p-adic class number formulas and the Lichtenbaum conjectures, *Duke Math. Journ.* **84** (1996), 679-717.

[15] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbf{Z}$, *Comp. Math.* **81** (1992), 223-236.

[16] B. Mazur, Deforming Galois representations, in: "Galois groups over $\mathbf{Q}$", Y. Ihara, K. Ribet, J.-P. Serre eds., MSRI Publ. **16**, 385-437, Springer-Verlag, New-York, Berlin, Heidelberg, 1987.

[17] B. Mazur, An "infinite fern" in the universal deformation space of Galois representations, Proceedings of the *Journées Arithmétiques*, Barcelona, 1995.

[18] A. Mézard, Computation of a universal deformation ring in the Borel case, to appear in *Math. Proc. Camb. Phil. Soc.*

[19] A. Movahhedi, Sur les p-extensions des corps p-rationnels, *Math. Nachr.* **149** (1990), 163-176.

[20] T. Nguyen Quang Do, Sur la $\mathbf{Z}_p$-torsion de certains modules galoisiens, *Ann. Inst. Fourier* **36** (1986), 27-46.

[21] T. Nguyen Quang Do, K_3 et formules de Riemann-Hurwitz p-adiques, *K-Theory* **7** (1993), 429-441.

[22] T. Nguyen Quang Do, Sur la cohomologie de certains modules galoisiens p-ramifiés, in: "Théorie des nombres – Number Theory", J.M De Koninck, C. Levesque eds., 740-754, 1989.

[23] R. Ramakrishna, On a variation of Mazur's deformation functor, *Comp. Math.* **87** (1993), 269-286.

[24] K. Ribet, A Modular Construction of Unramified p-Extensions of $\mathbf{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.

[25] P. Schneider, Über gewisse Galoiskohomologiegruppen, *Math. Zeit.* **168** (1979), 181-205.

[26] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[27] J.-P. Serre, "Cohomologie galoisienne", LNM 5, Springer Verlag, 1973.

[28] C. Skinner and A. Wiles, Ordinary representations and modular forms, *Proc. Nat. Acad. Sci. USA* **94** (1997), 10520–10527.

[29] D. Solomon, On the class group of imaginary abelian fields, *Ann. Inst. Fourier* **40** (3) (1990), 467–492.

[30] V. M. Tsvetkov, Euler-Poincaré characteristic of pro-p-groups, *Math. Inst. Steklov* **71** (1977), 256-258.

[31] L. C. Washington, "Introduction to cyclotomic fields", Springer-Verlag, 1997.

[32] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131** (1990), 493–540.

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