1. Digression : characters and pseudo-characters (bis)

If $T : G \to A$ is a pseudo-character of dimension n and $f : A \to B$ is a ring homomorphism, then we define $T \otimes_A B : G \to B$ as $f \circ T$. It is clearly a B-valued pseudo-character of dimension n.

THEOREM 1.1. *Let A be a henselian (e.g. complete) local ring with residue field k and let $T : G \to A$ be a pseudo-character. Assume $T \otimes_A k$ is the trace of an absolutely irreducible representation $\bar{\rho} : G \to \mathrm{GL}_n(k)$. Then there is a unique (up to isom.) representation $\rho : G \to \mathrm{GL}_n(A)$ whose trace is T. Actually, $A[G]/\mathrm{CH(T)} \simeq \mathrm{M_n(A)}$. If $A \in \mathcal{C}$, then T is continuous if and only if ρ is continuous.*

This result is due independently to Nyssen, Rouquier and Procesi (for the uniqueness, we also find in the litterature an argument by Carayol and Serre). If $A \in \mathcal{C}$ let us precise that we say that T is continuous if it is as a map.

We now prove the Theorem for $n = 2$. Denote again by T the A-linear extension of T to $A[G]$ and view $\bar{\rho}$ as a surjective A-algebra homomorphism $A[G] \to M_n(k)$ which is surjective by assumption. As $T \otimes_A k = \mathrm{trace}(\bar{\rho})$ and as trace $: M_n(k) \to k$ is Cayley-Hamilton, we have the following inclusion of two-sided ideal of $A[G]$: $\mathrm{CH(T)} \subset \mathrm{Ker}\bar{\rho}$. In particular, if $R = A[G]/\mathrm{CH(T)}$ then we have a surjective A-algebra homomorphism

$$R \to R/J \simeq M_2(k)$$

that "commutes with trace mod m_A" and the left-hand side is Cayley-Hamilton. Pick $x \in R$ mapping to a non-trivial idempotent $\bar{e} \in M_2(k)$. The ring $A[x] \subset R$ is a finite A-algebra by the Cayley-Hamilton identity and we have a surjective A-algebra homomorphism

$$A[x] \to k[\bar{e}] \simeq k \times k$$

so the idempotent $\bar{e}$ lifts as an idempotent $e \in A[x] \subset R$ by the henselian property (or by Hensel lemma if A is complete).[1]

We also may pick $x \in eR(1-e)$ and $y \in (1-e)Re$ such that $T(xy) \in A^{\times}$: lift anyhow generators the elementary matrices $E_{1,2}$ and $E_{2,1}$ in $M_2(k)$. The last lemma of the previous lecture ensures then that $R \simeq M_2(A)$ as an A-algebra. We conclude the existence of ρ using the tautological morphism $G \to R^{\times} \simeq \mathrm{GL}_n(A)$.

For the uniqueness, remark that if $\rho' : A[G] \to M_n(A)$ is a representation with trace T, then $\rho'(\mathrm{CH(T)}) = 0$ so it induces an A-algebra homomorphism

$$A[G]/\mathrm{CH(T)} \longrightarrow \mathrm{M_n(A)},$$

but any A-algebra homomorphism $M_n(A) \to M_n(A)$ is automatically an isomorphism, and induced by the conjugation by some $P \in \mathrm{GL}_n(A)$ (check this as an exercise).

If ρ is continuous then so is T, when $A \in \mathcal{C}$. If T is continuous, as $\rho(A[G]) = M_n(A)$ we may find finitely many elements $g_i \in G$, $i \in I$, such that the $\rho(g_i)$ generate

---

[1] We can argue here as follows : if $Q = X^2 - T(x)X + (T(x)^2 - T(x^2))/2 \in A[X]$ is the "characteristic polynomial of x", then $Q \bmod m_A = X^2 - X \in k[X]$ by assumption. As X and $X - 1$ are coprime in $k[X]$, Hensel lemma ensures that $Q = (X - a)(X - b) \in A[T]$ for some unique $a, b \in A$, with $a \in m_A$ and $b \equiv 1 \bmod m_A$. Then $e := (x - a)/(b - a) \in A[X]$ lifts $\bar{e}$ and $1 - e = (b - x)/(b - a)$, so $e^2 = e$.

$M_n(A)$ as A-module. The linear map

$$M_n(A) \to A^I$$

$x \mapsto (T(xg_i))$ is injective, hence a homeomorphism onto its image (a property of finite type modules over complete local noetherian rings). If T is continuous, then so are the maps $g \mapsto T(g^{\pm 1}g_i)$, and so is ρ by the previous assertion. $\square$

2. Pseudo-deformations and representability

Let G be a profinite group, $k = \mathcal{O}/p\mathcal{O}$ as in the first section of lecture 3, $n! \in k^\times$ (that is $p > n$) and let

$$\overline{T} : G \to k$$

be a continuous pseudo-character of dimension n. Define the *pseudo-deformation functor* of $\overline{T}$ as the functor

$$F_{\overline{T}} : \mathcal{C} \to \mathrm{Sets}$$

where $F_{\overline{T}}(A)$ is the set of continuous pseudo-characters $T_A : G \to A$ of dimension n such that $T_A \otimes_A k = \overline{T}$ via the augmentation map $A \to k$. Of course, if $A \to B$ is a morphism in $\mathcal{C}$ and $T_A \in F_{\overline{T}}(A)$, we set $F_{\overline{T}}(T_A) = T_A \otimes_A B$.

THEOREM 2.1. (i) *There is a unique local pro-artinian ring $R(\overline{T})$ with residue field k such that $F_{\overline{T}} \simeq F_{R(\overline{T})}$.*
  (ii) *If $\overline{T} = \mathrm{trace}(\bar{\rho})$ where $\bar{\rho} : G \to \mathrm{GL}_n(k)$ is absolutely irreducible, then $\rho_A \mapsto \mathrm{trace}(\rho_A)$ induces an isomorphism $F_{\bar{\rho}} \simeq F_{\overline{T}}$.*
  (iii) *If $(*G)$ holds then $R(\overline{T})$ is noetherian and $F_{\overline{T}}$ is representable.*

The combination of (i), (ii) and (iii) concludes the proof of Mazur's theorem when $p > n$.

Proof — Consider the abstract $\mathcal{O}$-algebra

$$R_0 = \mathcal{O}[\{T_g, g \in G\}]/J$$

where J is the ideal generated by the relations $T_1 - n$, $T_{gh} - T_{hg}$ for all $g, h \in G$, as well as the abstract pseudo-character relation : for instance when $n = 2$ we add the relations

$$T_{gg'g''} + T_{gg''g'} - T_g T_{g'g''} - T_{g'}T_{gg''} - T_{g''}T_{gg'} + T_g T_{g'}T_{g''}$$

for all g, g', g'' in G. By definition, the map

$$T : G \to R_0, g \mapsto T_g,$$

is a R_0-valued pseudo-character of dimension n which is universal in the following sense: for any $\mathcal{O}$-algebra A and any pseudo-character $T_A : G \to A$ of dimension n, there is a unique ring $\mathcal{O}$-algebra homomorphism $R_0 \to A$ such that $T \otimes_{R_0} A = T_A$. Indeed, all we have to do is to send $T_g \in R_0$ to $T_A(g) \in A$.

In particular, $\overline{T}$ defines a surjective $\mathcal{O}$-algebra morphism $R_0 \to k$ and we shall denote by m its kernel (a maximal ideal). Let $\mathcal{I}$ be the set of ideals $I \subset m$ of R_0 such that R_0/I is artinian and such that the pseudocharacter $T \otimes_{R_0} R_0/I$ is continuous. Note that $\mathcal{I}$ is stable by finite intersections (why?). Define R as the completion of R_0 with respect to $\mathcal{I}$:

$$R(\overline{T}) = \mathrm{projlim}_{I \in \mathcal{I}} R_0/I.$$

It is a pro-artinian local ring.[2] Unravelling the definitions, it is obvious that $(R(\overline{T}), T \otimes_{R_0} R(\overline{T}))$ represents $F_{\overline{T}} : \mathcal{C} \to$ Sets. This proves (i).

Part (ii) is a reformulation of Theorem 1.1 of Nyssen-Rouquier-Procesi.

We shall only prove (iii) when $\overline{T}$ is the trace of an absolutely irreducible representation $G \to \mathrm{GL}_n(k)$. In this case,

$$F_{\bar\rho} \simeq F'_{\bar\rho} \simeq F_{\overline{T}}$$

hence the tangent spaces of these three functors coincide and are finite dimensional over k, as the one of $F'_{\bar\rho}$ is as we have seen in lecture 3. It follows that $R(\overline{T})$ is actually noetherian by a Prop. of lecture 3 as well, hence that the three functors above are actually representable.

$\square$

The following corollary is useful in the applications to Galois representations, and follows at once from the construction above and from the equality $R(\overline{T}) = R(\bar\rho)$:

COROLLARY 2.2. *(Under the assumptions of Mazur's theorem) Let* $t : G \to \mathcal{O}$ *be the Teichmuller lift of the function* $\mathrm{trace}(\bar\rho) : G \to k$. *The* $\mathcal{O}$-*algebra* $R(\bar\rho)$ *is topologically generated by the elements* $\mathrm{trace}(\rho^u(g)) - t(g)$, *for* $g \in G$.

Remarks. Assume (*G), $n = 2$ and $p > 2$.

(i) If $\overline{T} = \chi_1 + \chi_2$ for two distinct continuous characters $\chi_i : G \to k^\times$. One can show that there is an exact sequence

$$0 \to H^1(G, k)^2 \to F_{\overline{T}}(k[\varepsilon]) \to H^1(G, \chi_1/\chi_2) \otimes_k H^1(G, \chi_2/\chi_1).$$

(see my book with Bellaiche chapter 1, as well as Bellaiche's paper "Pseudodeformations".)

(ii) $\overline{T} = 2\chi$ for $\chi : G \to k^\times$ a continuous character, one can show that there is an exact sequence

$$0 \to H^1(G, k) \oplus \mathrm{Sym}^2(H^1(G, k)) \to F_{\overline{T}}(k[\varepsilon]) \to \Lambda^3(H^1(G, k)).$$

(ask me if you want to know the proof of this.)

Remark. Thanks to some work of Vaccarino and others, it is actually possible to modify the definition of a pseudocharacter in such a way that the assumption $n! \in k^\times$ is not necessary anymore : see my paper "The p-adic analytic space of pseudocharacters of a profinite group, and pseudorepresentations over arbitrary rings".

3. Formally smooth deformation functors

A covariant functor $F : \mathcal{C} \to$ Sets is said *formally smooth* (over $\mathcal{O}$) if for each object $A \in \mathcal{C}$ and any ideal $I \subset A$ such that $m_A I = 0$, the natural map

$$F(A) \to F(A/I)$$

is surjective.

---

[2]If for any $I \in \mathcal{I}$ we denote by $I' \subset R(\overline{T})$ the kernel of $R(\overline{T}) \to R_0/I$, then $(I \cap J)' = I' \cap J'$ and the natural map

$$R(\overline{T}) \to \mathrm{projlim}_{I \in \mathcal{I}} R(\overline{T})/I'$$

is injective with dense image, hence an isomophism as the left-hand side is compact.

PROPOSITION 3.1. *Let $R \in \mathcal{C}$. Then F_R is formally smooth if and only if $R \simeq \mathcal{O}[[X_1, \ldots, X_n]]$ (necessarily, $n = \dim_k F_R(k[\varepsilon])$).*

Proof — If R is a power series ring as in the statement, then $\varphi \mapsto (\varphi(X_i))_i$ induces a bijection

$$\mathrm{Hom}_{\mathcal{C}}(R, A) \to A^n$$

for all $A \in \mathcal{C}$, thus F_R is trivially formally smooth (the surjectivity property even holds for any $I \subset m_A$). Conversely, let $x_1, \ldots, x_n \in m_R$ wose image in m_R/m_R^2 form a k-basis. Consider $S := \mathcal{O}[[X_1, \ldots, X_n]]$ and the natural morphism in $\mathcal{C}$ sending X_i on x_i :

$$\varphi : S \to R.$$

This morphism is surjective (by an argument actually already explained) and we want to show that its kernel J vanishes. Consider the tautological exact sequence

$$0 \to J/m_S J \to S/m_S J \to R = S/J \to 0.$$

Applying the formal smoothness of F_R (note that m_S kills $J/m_S J$) we may lift the identity map of R to a morphism $R \to S/m_S J$, so that the above sequence admits a section. It follows that

$$S/m_S J = R \oplus J/m_S J$$

hence that $m_S/m_S^2 = m_R/m_R^2 \oplus J/m_S J$. As m_R/m_R^2 and m_S/m_S^2 both have dimension n over k by construction, it follows that $J/m_S J = 0$ hence that $J = 0$ by Nakayama's lemma. $\qquad\square$

We now investigate when Mazur's functor $F'_{\bar{\rho}}$ is fomally smooth.

PROPOSITION 3.2. *(Unobstructed deformation functor) If $H^2(G, \mathrm{ad}(\bar{\rho})) = 0$ then $F'_{\bar{\rho}}$ is formally smooth.*

Proof — Let $A \to A/I$ a morphism in $\mathcal{C}$ with $m_A I = 0$. Consider the exact sequence of profinite groups

$$1 \to M_n(I) \to \mathrm{GL}_n(A) \to \mathrm{GL}_n(A/I) \to 1.$$

The theory of (profinite) group extensions with abelian kernel associates to the extension above a continuous cohomology class

$$c \in H^2(\mathrm{GL}_n(A/I), M_n(I)).$$

If $\rho : G \to \mathrm{GL}_n(A/I)$ is a continous morphism, the same theory says that we may lift ρ to a continuous group homomorphism in $\mathrm{GL}_n(A)$ if and only if the restricted class

$$c_{|G} \in H^2(G, M_n(I))$$

defined by $\rho : G \to \mathrm{GL}_n(A/I)$, vanishes. But the k-representation $M_n(I)$ of G is $\mathrm{ad}(\bar{\rho}) \otimes_k I$ (trivial action on I), whose H^2 vanishes by assumption. $\qquad\square$

An immediate corollary of these two propositions is the following:

COROLLARY 3.3. *Under the assumptions of Mazur's theorem, if $H^2(G, \mathrm{ad}(\bar{\rho})) = 0$ then $R(\bar{\rho}) \simeq \mathcal{O}[[X_1, \ldots, X_m]]$ where $m = \dim_k H^1(G, \mathrm{ad}(\bar{\rho}))$.*

In this case, the situation is especially pleasant, as we have a nice continuous

$$\rho^u : G \to \mathrm{GL}_n(\mathcal{O}[[X_1, \ldots, X_m]]).$$

The homomorphisms $R(\bar{\rho}) \to \mathcal{O}$, which parametrises via ρ^u the isomorphism classes of lifts of $\bar{\rho}$ to $\mathcal{O}$, are in bijection with $(p\mathcal{O})^n$ via $X_i \mapsto x_i \in p\mathcal{O}$. In other words, "the open unit disc in $\mathcal{O}^n$ parametrises the set of $\mathcal{O}$-lifts of $\bar{\rho}$".

4. Galois cohomology of number fields

As we have seen, the most basic properties of Mazur's deformation functors are governed by some cohomology groups. In order to make some computations in the case $G = G_{F,S}$ for number fields, we need to recall the important results regarding the computation of Galois cohomology of number fields. Let F be a number field and let $S \subset S(F)$ be a finite set.

PROPOSITION 4.1. $G_{F,S}$ *satisfies (*G) for any prime p.*

Proof — Indeed, let H be an open subgroup of $G_{F,S}$. Then $H = G_{F',S'}$ where F' is a finite extension of F in F^S and S' is the set of all the places of F' above some place of S. The results then follows from Hermite's theorem recalled in lecture 1. $\square$

Fix a prime p and let k be a finite field of characteristic p. Assume that S contains all the primes of F above p and ∞. Let ρ be a Galois representation of $G_{F,S}$ on a finite dimensional k-vector space V. Recall that $V^\vee = \mathrm{Hom}_k(V, k)$ denotes the dual representation and $V(1)$ is the twist of V by the cyclotomic character mod p of $G_{F,S}$.

For $i \geq 0$, recall the continuous cohomology groups

$$H^i(G_{F,S}, V)$$

(Recall that continuous cohomology is defined following Tate as the cohomology of the complex of continuous cochains in V). These spaces are finite dimensional and vanish for $i > 2$ if $p > 2$ or if F is totally complex : it is clear for H^0, it follows from the inflation-restriction exact sequence and (*G) for $i = 1$ and we admit it for $i > 1$. For each place $v \in S(F)$ we have a natural k-linear map

$$\mathrm{res}_v : H^i(G_{F,S}, V) \to H^i(G_{F_v}, V)$$

defined by restricting cochains by means of one of the morphims $G_{F_v} \to G_{F,S}$ (to see that the map on cohomology "does not depend" on the chosen $G_{F_v} \to G$ apply Prop. VII.3 of Serre "Corps locaux"). It is customary to set

$$\text{Ш}_S^i(G_{F,S}, V) = \mathrm{Ker}\ H^i(G_{F,S}, V) \overset{(\mathrm{res}_v)_{v \in S}}{\longrightarrow} \prod_{v \in S} H^i(G_{F_v}, V).$$

For W a finite G_{F_v}-module, we also set $\widetilde{H}^0(F_v, W) = H^0(F_v, W)$ if $F_v \neq \mathbb{R}$ and $\widetilde{H}^0(G_\mathbb{R}, W) = W^{c=1}/(1 + c)W$ otherwise, where c is the generator of $G_\mathbb{R}$. We take the following result as a black box.

THEOREM 4.2. *(Poitou-Tate theorems)*

(i) *(Euler characteristic formula)*

$$\sum_{i=0}^{2} (-1)^i \dim_k H^i(G_{F,S}, V) = -(|S_{\mathbb{C}}| + |S_{\mathbb{R}}|) \dim_k(V) + \sum_{v \in S_{\mathbb{R}}} \dim_k H^0(G_{F_v}, V).$$

(ii) *(Hasse's principle) There is a natural exact sequence*

$$0 \longrightarrow \text{III}_S^2(G_{F,S}, V) \xrightarrow{can} H^2(G_{F,S}, V) \xrightarrow{(\text{res}_v)} \prod_{v \in S} H^2(G_{F_v}, V) = \prod_{v \in S} \widetilde{H}^0(G_{F_v}, V^\vee(1))^\vee$$

$$\xrightarrow{(\text{res}_v^\vee)} H^0(G_{F,S}, V^\vee(1))^\vee \longrightarrow 0$$

where equality in the middle is the local duality theorem of Tate.

(iii) *(Poitou-Tate duality) There is a canonical perfect pairing*

$$\text{III}^1(G_{F,S}, V^\vee(1)) \times \text{III}^2(G_{F,S}, V) \to k.$$

These theorems are due to Tate and Poitou. For proofs, which are difficult, see for instance Neukirch, Schmidt, Wingberg "Cohomology of number fields" Ch. 8 or Milne "Arithmetic Duality theorems" Ch. I.

A quick look at these formulas shows that they are not enough to compute $H^1(G_{F,S}, V)$ and $H^2(G_{F,S}, V)$ in general. They rather give $\dim_k H^1 - \dim_k H^2$ and reduce the computation of $\dim_k H^2$ to that of $\dim_k \text{III}_S^1(G_{F,S}, V^\vee(1))$. This latter space is difficult to control in practice, however it frequently vanishes.

PROPOSITION 4.3. *Let F'/F be the number field cut-out by V. If the ideal class group of $\mathcal{O}_{F'}$ has order prime to p and if $H^1(\text{Gal}(F'/F), V) = 0$, then*

$$\text{III}_S^1(G_{F,S}, V) = 0.$$

Proof — If V is a trivial $G_{F,S}$-module, then $F' = F$ and

$$H^1(G_{F,S}, V) = \text{Hom}(G_{F,S}, V)$$

(continuous group homomorphisms to the vector space V) so $\text{III}_S^1(G_{F,S}, V)$ is the space of homomorphisms $G_{F,S} \to V$ that vanish on the image of $G_{F_v} \to G_{F,S}^{\text{ab}}$ for each $v \in S$. By global class-field theory (see the description of $G_{F,S}^{\text{ab}}$ in lecture 1), such a homomorphism factors through the quotient $\text{Cl}(\mathcal{O}_F)$ of $G_{F,S}^{\text{ab}}$ (and even through the quotient of $\text{Cl}(\mathcal{O}_F)$ by the subgroup generated by the prime ideals in S_f). The proposition follows in this case. In general, the inflation restriction sequence writes

$$0 \to H^1(\text{Gal}(F'/F), V) \to H^1(G_{F,S}, V) \to H^1(G_{F',S'}, V),$$

where S' is the set of places of F' above some place in S. Under vanishing of the left-hand side, it follows that the restriction induces an injection

$$0 \to \text{III}_S^1(G_{F,S}, V) \to \text{III}_{S'}^1(G_{F',S'}, V)$$

and we are reduced to the previous case. $\qquad\square$

5. Deformation theory of regular Galois representations.

We assume from now on that $F = \mathbb{Q}$ to fix ideas. Fix

$$\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_n(\mathbb{F}_q)$$

an absolutely irreducible Galois representation. We still assume that S contains ∞, p and we assume as well that p is odd. In particular, the conjugacy class of complex conjugations $c \in \mathrm{G}_{\mathbb{Q}}$ has the form

$$\bar{\rho}(c) \sim (1, \ldots, 1, -1, \ldots, -1)$$

with $i(c) = \dim \mathrm{Ker}(\rho(c) - \mathrm{id})$ times the eigenvalue 1 (hence $n - i(c)$ times -1).

Recall the associated representation $\mathrm{ad}(\bar{\rho})$ by conjugation on $M_n(\mathbb{F}_q)$. We say that $\bar{\rho}$ is *regular*, or S-*regular* to emphasize the S, if $H^2(G_{\mathbb{Q},S}, \mathrm{ad}(\bar{\rho})) = 0$. (These are not standard terminologies.)

PROPOSITION 5.1. *If $\bar{\rho}$ is regular then $R(\bar{\rho}) \simeq \mathbb{Z}_q[[X_1, \ldots, X_r]]$ where $r = 1 + 2i(c)(n - i(c))$.*

In this case, $\bar{\rho}(c)$ is a scalar if and only if $R(\bar{\rho}) \simeq \mathbb{Z}_q[[T]]$. Moreover, if $n = 2$ and $\bar{\rho}$ is odd then $R(\bar{\rho}) \simeq \mathbb{Z}_q[[X, Y, Z]]$.

Proof —   Indeed, $\dim \mathrm{ad}(\bar{\rho}) = n^2$. Moreover, $\mathrm{ad}(\bar{\rho}(c))$ is diagonalisable with $i(c)^2 + (n - i(c))^2$ times the eigenvalue 1, so that the right-hand side of the Euler-characteristic formula is $-2i(c)(n - i(c))$. As

$$H^0(G_{\mathbb{Q},S}, \mathrm{ad}(\bar{\rho})) \subset M_n(\mathbb{F}_q)$$

is the centralizer of $\bar{\rho}$, hence the scalar matrices as $\bar{\rho}$ is absolutely irreducible, it has dimension 1, and we are done. $\square$

When $\bar{\rho}$ is not assumed regular, the structure of $R(\bar{\rho})$ is presumably extremely complicated in general, and essentially unknown. By argument similar to the ones explained in this lecture, Mazur has shown that the Krull-dimension of $R(\bar{\rho})/(p)$ is always at least $1 + 2i(c)(n - i(c))$

OPEN PROBLEM : Is is true that, in all cases, $R(\bar{\rho})/(p)$ has dimension $1 + 2i(c)(n - i(c))$?

When $n = 1$, we have $\mathrm{ad}(\bar{\rho}) = \mathbb{F}_q$ (trivial representation), so $H^1(G_{\mathbb{Q},S}, \mathbb{F}_q)$ is the space of continuous homomorphisms $G_{\mathbb{Q},S}^{\mathrm{ab}} \to \mathbb{F}_q$. By the Euler characteristic formula applied to $V = \mathbb{F}_q$, $\bar{\rho}$ is regular if and only if this space has dimension 1. By the Kronecker-Weber theorem,

$$G_{\mathbb{Q},S}^{\mathrm{ab}} \simeq \prod_{\ell \in S} \mathbb{Z}_\ell^\times$$

so $\bar{\rho}$ is regular if and only if $\ell \not\equiv 1 \bmod p$ for all finite prime ℓ in S (this is independent of $\bar{\rho}$). In this case, we have $R(\bar{\rho}) \simeq \mathbb{Z}_q[[T]]$.

REMARK 5.2. *Actually, we have not explained it but it is easy to describe $R(\bar{\rho})$ directly for any one-dimensional $\bar{\rho} : G \to k^\times$, for any group G satisfying (*G) : it is simply the completed group ring $\mathcal{O}[[\Delta]]$ where Δ is the maximal abelian and pro-p-quotient of G, the universal character being the natural map $G \to \mathcal{O}[[\Delta]]^\times$.*

Under the assumption on G, $\Delta \simeq \mathbb{Z}_p^r \times \Delta'$ for some finite abelian p-group Δ', and it is well-known that (Iwasawa)

$$\mathcal{O}[[\Delta]] \simeq \mathcal{O}[[T_1, \ldots, T_r]][\Delta'].$$

In particular, $\mathcal{O}[[\Delta]] \in \mathcal{C}$ and it is formally smooth over $\mathcal{O}$ iff Δ is torsion free. To check the claim above, note that twisting by the inverse of a Teichmüller lift $G \to \mathbb{Z}_q^\times$ of $\bar{\rho}$, we have $R(\bar{\rho}) \simeq R(1)$ so that we may assume $\bar{\rho} = 1$. The result follows then easily as $1 + m_A$ is an abelian pro-p-group for any $A \in \mathcal{C}$.

When $\bar{\rho}(c)$ is a scalar matrix and $\bar{\rho}$ is regular and even, we get a universal deformation ring isomorphic to $\mathbb{Z}_q[[T]]$. Actually, it is easy to check that if we fix some lift $\rho_0 : G_{\mathbb{Q},S} \to \mathrm{GL}_n(\mathcal{O})$ of $\bar{\rho}$ (which exists by the assumed formal smoothness property of $F_{\bar{\rho}}$, i.e. by the regularity of $\bar{\rho}$) then the universal deformation ring $R(\bar{\rho})$ "essentially" coincides with the twist of ρ_0 by the universal character deforming 1 (this is stricly true if n is prime to p). It follows that this case is not very interesting ! The first really interesting case is thus $n = 2$ and $\bar{\rho}$ odd.

6. Some explicit examples of odd regular $\bar{\rho}$ of dimension 2

We will actually look for an example of odd regular $\bar{\rho}$ on the p-torsion points of an elliptic curve over $\mathbb{Q}$. Fix $E/\mathbb{Q}$ such an elliptic curve and let $\bar{\rho}$ be the Galois representation on $E[p]$ where $E[p] = E(\overline{\mathbb{Q}})[p] \simeq \mathbb{F}_p^2$ (so $k = \mathbb{F}_p$ from now on). As we know, we have $\det(\bar{\rho}) = \mathbb{F}_p(1)$, so that $\det(\bar{\rho}(c)) = -1$ and $\bar{\rho}$ is indeed odd.

As $\bar{\rho}$ has dimension 2, then $\bar{\rho}^\vee \simeq \bar{\rho} \otimes \det(\bar{\rho})^{-1}$ (because it is so for the representation of $\mathrm{GL}_2(k)$ over k^2) and we have a decomposition

$$\mathrm{ad}(\bar{\rho}) = \bar{\rho} \otimes \bar{\rho}^\vee \simeq \mathbb{F}_q \oplus V, \quad V = \mathrm{Sym}^2(\bar{\rho}) \otimes \det(\bar{\rho})^{-1} = \mathrm{Sym}^2 E[p](-1).$$

We have already seen above that the vanishing of $H^2(G_{\mathbb{Q},S}, \mathbb{F}_q)$ is equivalent to the fact that S does not contain any prime $\ell \equiv 1 \bmod p$. We shall therefore concentrate on the other term $H^2(G_{\mathbb{Q},S}, \mathrm{Sym}^2 E[p](-1))$. The following criterion is a direct consequence of the theorems of Poitou and Tate part (ii) and (iii) :

LEMMA 6.1. *For any finite $\mathbb{F}_p[G_{\mathbb{Q},S}]$-module V, $H^2(G_{\mathbb{Q},S}, V) = 0$ is equivalent to the following two properties:*

(R1) $H^0(G_{\mathbb{Q},S}, V^\vee(1)) \to \prod_{v \in S} H^0(G_{\mathbb{Q}_v}, V^\vee(1))$ is an isomorphism.
(R2) $\mathrm{III}_S^1(G_{\mathbb{Q},S}, V^\vee(1)) = 0$.

In our case,

$$V^\vee(1) = (\mathrm{Sym}^2(\bar{\rho}) \otimes \det(\bar{\rho})^{-1})^\vee(1) = \mathrm{Sym}^2 E[p].$$

Note that (R1) is a local (usually easier) check whereas (R2) is a global (usually much harder) problem, essentially the "vanishing of a piece of the class group of the number field cut out by $V^\vee(1)$" as shown by proposition 4.3. Below we denote for short $E[p]$ for $E(\overline{F})[p]$ if E is an elliptic curve over F.

LEMMA 6.2. *Assume that E is an elliptic curve over $\mathbb{Q}_\ell$ with split multiplicative reduction, and say $\ell \neq p$. Assume $p \neq 2$, $\ell^2 \not\equiv 1 \bmod p$ and that $v_\ell(j(E))$ is prime to p. Then $H^0(G_{\mathbb{Q}_\ell}, \mathrm{Sym}^2 E[p]) = 0$.*

Proof —   Indeed, as $v_\ell(j(E))$ is prime to p, Tate's theorem recalled in lecture 2 ensures that there is a non split exact sequence of $\mathbb{F}_p[G_{\mathbb{Q}_\ell}]$-modules

$$0 \to \mathbb{F}_p(1) \to E[p] \to \mathbb{F}_p \to 0.$$

As $p > 2$, it follows that $\mathrm{Sym}^2 E[p]$ has a unique $G_{\mathbb{Q}_\ell}$-stable line, on which it acts by $\mathbb{F}_p(2)$, so frob_ℓ acts by $\ell^2 \neq 1$ on this line.   □

Actually, if E has non-split multiplicative reduction, the same criterion holds as $E[p]$ contains as unique $G_{\mathbb{Q}_\ell}$-stable line $\mathbb{F}_p(1)$ twisted by the unramified character sending ℓ to -1, whose square is still $\mathbb{F}_p(2)$. The criterion also holds when $\ell = p$ if $p > 3$ (exercise).

LEMMA 6.3. *Assume that E is an elliptic curve over $\mathbb{Q}_p$ with good reduction, $p > 2$, and let $a = p + 1 - |\overline{E}(\mathbb{F}_p)|$. If $a \not\equiv 0, \pm 1 \bmod p$ then $H^0(G_{\mathbb{Q}_p}, \mathrm{Sym}^2 E[p]) = 0$.*

Proof —   As a is prime to p, E has good ordinary reduction and as we have recalled in lecture 2 in this case there is an exact sequence of $\mathbb{F}_p[G_{\mathbb{Q}_p}]$-modules:

$$0 \to \psi^{-1}(1) \to E[p] \to \psi \to 0$$

where $\psi : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ is the unramified character sending $\mathrm{frob}_{\mathbb{Q}_p}$ to $a \bmod p$. The semi-simplification of $\mathrm{Sym}^2 E[p]$ is then $\psi^{-2}(2) \oplus \mathbb{F}_p(1) \oplus \psi^2$ and none of these three characters is trivial by assumption on a.   □

Actually, if E has good reduction and $a \equiv 0 \bmod p$ (supersingular reduction), then $H^0(G_{\mathbb{Q}_p}, \mathrm{Sym}^2 E[p]) = 0$ as well. Moreover, even if $a \equiv \pm 1 \bmod p$ but if $E[p]$ is not split (which occurs most probably in practice), then $\mathbb{F}_p(2)$ is the unique stable line in $\mathrm{Sym}^2 E[p]$ hence non-trivial as long as $\mathbb{F}_p(2) \neq \mathbb{F}_p$, i.e. $p > 3$.

These two simple facts will be enough to check (R1) in the explicit example considered below. As already said, it is actually much more difficult to check condition (R2), namely the vanishing of $\mathrm{III}^1_S(G_{\mathbb{Q},S}, \mathrm{Sym}^2 E[p])$, essentially because there is a part of mystery in this cohomology group (it is a special case of the "Tamagawa number conjecture"). We shall assume from now on that $\bar{\rho}$ *is surjective*, so that the number field $\mathbb{Q}(\bar{\rho})$ that it cuts out is a Galois extension of $\mathbb{Q}$ with Galois group $\simeq \mathrm{GL}_2(\mathbb{F}_p)$.

LEMMA 6.4. *If $p > 3$ and if the class group of $\mathbb{Q}(\bar{\rho})$ has order prime to p, then (R2) holds.*

Proof —   Indeed, $H^1(\mathrm{GL}_2(\mathbb{F}_p), \mathrm{Sym}^2(\mathbb{F}_p^2)) = 0$ as the center $\mathbb{F}_p^\times$ of $\mathrm{GL}_2(\mathbb{F}_p)$ has order prime to p and acts via the non-trivial character $\lambda \mathrm{id} \mapsto \lambda^2$ ($p > 3$).   □

This naive criterion is however not reasonable to check with a computer as $|\mathrm{GL}_2(\mathbb{F}_p)|$ is too big even for $p = 3$. Another simple, slightly more reasonable, criterion is the following. Let $B \subset \mathrm{GL}_2(\mathbb{F}_p)$ be the subgroup of upper-triangular matrices and let $\chi : B \to \mathbb{F}_p^\times$ be the character of B occuring as a quotient of the natural representation over $\mathbb{F}_p^2$. Let $F = \mathbb{Q}(\rho)^B$ and $F \subset F' \subset \mathbb{Q}(\bar{\rho})$ the extension of F cut out by the character χ^2 of B. If $p > 2$, note that $[F' : \mathbb{Q}] = (p^2 - 1)/2$.

LEMMA 6.5. *If $p > 3$ and if the class group of F' has order prime to p, then (R2) holds.*

Proof — By Frobenius reciprocity we have a non-zero $\mathbb{F}_p[\mathrm{GL}_2(\mathbb{F}_p)]$-morphism

$$\mathrm{Sym}^2(\mathbb{F}_p^2) \to \mathrm{Ind}_B^{\mathrm{GL}_2(\mathbb{F}_p)} \chi^2.$$

This morphism is injective as $p > 2$ (so the left hand-side is irreducible) and its cokernel does not contain the trivial representation of $\mathrm{GL}_2(\mathbb{F}_p)$ as $p > 3$ (we leave this as an exercise to the reader. The cokernel is actually isomorphic to a twist of $\mathrm{Sym}^{p-3}(\mathbb{F}_p^2)$ and is irreducible). As $\bar{\rho}$ is surjective, the cohomology exact sequence gives an injection

$$0 \to H^1(G_{\mathbb{Q},S}, \mathrm{Sym}^2(E[p])) \to H^1(G_{\mathbb{Q},S}, \mathrm{Ind}_F^{\mathbb{Q}} \chi^2) = H^1(G_{F,S}, \chi^2)$$

(use Shapiro's lemma, here and below we still denote by S the set of places of F or F' dividing a place of S). Inflation-restriction gives as well an injection (as $[F' : F]$ is prime to p)

$$H^1(G_{F,S}, \chi^2) \to H^1(G_{F',S}, \mathbb{F}_p).$$

If we follow these two injections, we obtain an injection

$$\mathrm{III}_S^1(G_{\mathbb{Q},S}, \mathrm{Sym}^2 E[p]) \to \mathrm{III}_S^1(G_{F',S}, \mathbb{F}_p)$$

and the last group vanishes by assumption on $\mathrm{Cl}(\mathcal{O}_{F'})$ by Prop. 4.3. $\qquad\square$

There should be an explicit formula taking an elliptic curve say over $\mathbb{Q}$ and giving equations for the field F' (or for the extension of F cut out by $\mathrm{Ker}(\chi)$), however I have not been able to find such a routine on Pari GP (http://pari.math.u-bordeaux.fr/ or on Sage (http://www.sagemath.org/). It would be nice to implement one.

We can however circumvent this problem by first computing the field $K \subset \mathbb{Q}(\bar{\rho})$ which is fixed by the subgroup H of matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ of the form

$$\begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix}$$

Indeed, as the abscissa of a non-zero $P \in E(\overline{\mathbb{Q}})$ uniquely determines $\pm P$, the field K is generated by the abscissa of a nonzero point of p-torsion, that is a splitting field of the x-coordinate of the p-th division polynomial of the elliptic curve E (use e.g. the elldivpol routine by Cremona). By Galois theory the field F' (just as K) is a subfield of degree $(p^2 - 1)/2$ of $K(\cos(2\pi/p))$ and it would not be difficult to characterize it. This gives a way to find F' explicitely, and then to compute its class number. In practice, Pari can for instance compute such a class number for $p = 5$ (the extension F' has degree 12). Already for $p = 7$, Pari will compute it in general only assuming GRH ! We shall actually apply this below when $p = 5$ in which case there are just 3 subfields of degree 12 in $K(\cos(2\pi/5)) : K$, F' and another one with the specific property that it contains $\mathbb{Q}(\cos(2\pi/5)) = \mathbb{Q}(\sqrt{5})$. This gives a way to find F' explicitely, and then to compute its class number.

EXAMPLE: Let E be the elliptic curve $y^2 + xy + y = x^3 - x^2 - x$. This curve have discriminant 17 and $j(E) = \frac{3^3.11^3}{17}$. It has thus good reduction outside 17 and multiplicative reduction at 17, actually split : if $Y = y + x/2 + 1/2$ and $X = x - 2$, then $Y^2 = X^2(X + 1)$ modulo 17. The reduction mod 2 has $4 = 3 - (-1)$ points in $\mathbb{F}_2$ and $X^2 + X + 2$ is irreducible mod 5. We take $p = 5$ and $S = \{\infty, 5, 17\}$. It follows that $\bar{\rho}$ is surjective by an argument similar to the one explained in lecture 2. Let us check (R1):

(i) At ∞ it is automatic as $p \neq 2$ (recall the convention on $H^0(G_\mathbb{R}, -)$).

(ii) At 17 this follows from lemma 6.2 as $17^2 = -1 \mod 5$.

(iii) The reduction mod 5 of E has $7 = 5 - (-2)$ points in $\mathbb{F}_5$, so that $a = -2 \not\equiv 0, \pm 1 \mod 5$ and we conclude by lemma 6.3.

To check (R2) we compute first the 5-division polynomial (in abscissa), which is

$$5x^{12} - 15x^{11} - 22x^{10} + 125x^9 - 240x^8 + 240x^7 - 45x^6 - 123x^5 + 100x^4 - 30x^3 + 10x^2 - 5x + 1$$

This allows to compute the field F' as explained above and we find that $F' = \mathbb{Q}(z)$ where

$$z^{12} - 2z^{11} - 11z^{10} + 30z^9 + 10z^8 - 49z^7 - 37z^6 + 49z^5 + 10z^4 - 30z^3 - 11z^2 + 2z + 1 = 0.$$

Pari tells us that the class group of this number field is actually trivial, and we are done ! As an exercise, the reader can check by the same argument that the 5-torsion of the elliptic curve $y^2 + y = x^3 + x^2 + x$ (so $\Delta = -19$) is regular as well. $\square$

As we have seen, it is rather painful to check a condition like (R2), although it is likely to be satisfied rather often as the method above may suggest. This is reminescent to the fact that a positive density of primes should be regular in the sense of Kummer. However, the sufficient class number condition described above is by no mean necessary as we mostly forgot the Galois structure of class group of $\mathbb{Q}(\bar{\rho})$ and the part related to (R2), that is the $\mathrm{Sym}^2 E[p]$-isotypic component of $\mathrm{Cl}(\mathbb{Q}(\bar{\rho}))/(p)$, may vanish even if the class group itself does not modulo p. The following result of Flach (*A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math. 109 (1992), pp. 307–327.) actually beautifully solves the problem in a completely different way:

THEOREM 6.6. *(Flach) Let E be an elliptic curve over $\mathbb{Q}$, $p > 3$ a prime of good reduction and S the set of primes above $p\infty$ or of bad reduction of E. If $\bar{\rho}$ surjective and p does not divide the degree of a modular parametrisation of E then* $\mathrm{III}_S^1(\mathrm{G}_{\mathbb{Q},S}, \mathrm{Sym}^2 E[p]) = 0$.

A modular parametrisation of E is a finite morphism $X_0(N) \to E$. That such a morphism always exists is a consequence of Taniyama-Shimura-Weil + Falting's isogeny theorem. For instance, the curve $X_0(17)$ is already an elliptic curve (hence has trivially modular degree 1). It is isogenous to the curve $y^2 + xy + y = x^3 - x^2 - x$ treated above. As $\bar{\rho}$ is surjective mod 5 in this case such an isogeny has order prime to 5 and we are done ! (Actually it can be shown that the only non-trivial isogenies of this curve have degree a power of 2). In general, the result of Flach (combined with a result of Serre and the modularity results above) shows that if E has no CM then for all but finitely many p we have $\mathrm{III}_S^1(\mathrm{G}_{\mathbb{Q},S}, \mathrm{Sym}^2 E[p]) = 0$. It is not difficult to check how (R1) varies with p, and one can actually shows that :

THEOREM 6.7. *(Mazur) If E is a non-CM elliptic curve, then for a subset of primes p with Dirichlet density one the Galois representation on $E[p]$ is regular.*

See Mazur's paper *An infinite fern in the deformation space of Galois representations* Corollary 2. The result of Flach has been generalized to any modular Galois representations by Diamond-Flach-Guo, which allowed Weston to give a variant of Mazur's result for all the modular Galois representations (see his paper "Unobstructed modular deformation problems", there is also related work by Yamagami).

For instance, Weston shows that if Δ is Ramanujan 's cuspform of weight 12 and level 1, then $\bar{\rho}_{\Delta,p}$ is unobstructed for all prime $p > 13$ and $p \neq 691$.