Astérisque

JOSEPH OESTERLÉ

Travaux de Wiles (et Taylor, ...), partie II

Astérisque, tome 237 (1996), Séminaire Bourbaki,
exp. n° 804, p. 333-355

<http://www.numdam.org/item?id=SB_1994-1995__37__333_0>

Séminaire BOURBAKI
47ème année, 1994-95, n° 804

Juin 1995

TRAVAUX DE WILES (ET TAYLOR, ...), PARTIE II

par **Joseph OESTERLÉ**

Cet exposé fait suite à celui de J.-P. Serre, auquel nous référerons par [S]. On note ℓ un nombre premier ≥ 3 et $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$. Pour toute sous-extension K de $\overline{\mathbf{Q}}$, on pose $G_K = \mathrm{Gal}(\overline{\mathbf{Q}}/K)$. On note $\chi_\ell : G_{\mathbf{Q}} \to \mathbf{Z}_\ell^\times$ le caractère cyclotomique via lequel $G_{\mathbf{Q}}$ opère sur les racines de l'unité de $\overline{\mathbf{Q}}$ d'ordre une puissance de ℓ. Par abus, si A est une $\mathbf{Z}_\ell$-algèbre, on note encore χ_ℓ l'homomorphisme composé $G_{\mathbf{Q}} \xrightarrow{\chi_\ell} \mathbf{Z}_\ell^\times \to A^\times$.

Pour tout nombre premier p, on note D_p le groupe de décomposition d'une place de $\overline{\mathbf{Q}}$ au-dessus de p, I_p son groupe d'inertie, $\mathrm{Frob}_p \in D_p$ un élément de Frobenius arithmétique et $\overline{\mathbf{Q}}_p$ la fermeture algébrique de $\mathbf{Q}_p$ dans le complété de $\overline{\mathbf{Q}}$ en la place choisie.

Soient A l'anneau des entiers d'une extension de degré fini de $\mathbf{Q}_\ell$, $\mathfrak{m}$ son idéal maximal et ρ un homomorphisme continu de $G_{\mathbf{Q}}$ dans $\mathbf{GL}_2(A)$, non ramifié en dehors d'un ensemble fini de nombres premiers. Choisissons un plongement de $A/\mathfrak{m}$ dans une clôture algébrique $\overline{\mathbf{F}}_\ell$ de $\mathbf{F}_\ell$ et notons $\overline{\rho} : G_{\mathbf{Q}} \to \mathbf{GL}_2(\overline{\mathbf{F}}_\ell)$ la représentation déduite de ρ par réduction mod $\mathfrak{m}$. Le théorème suivant fournit des conditions suffisantes pour que ρ soit modulaire (au sens de [S], 2.3) lorsque $\overline{\rho} : G_{\mathbf{Q}} \to \mathbf{GL}_2(\overline{\mathbf{F}}_\ell)$ est modulaire (au sens de [S], 2.2). Il résout en partie une conjecture de Fontaine et Mazur ([6]).

THÉORÈME 1.— *Supposons satisfaite l'une des deux conditions suivantes :*

a) *Le $\mathbf{Z}_\ell$-module A^2, muni de l'action de D_ℓ définie par ρ, est isomorphe au module de Tate d'un groupe ℓ-divisible sur $\mathbf{Z}_\ell$, et $\det\rho$ coïncide avec χ_ℓ dans I_ℓ.*

b) *La restriction de ρ à D_ℓ est conjuguée à $\begin{pmatrix} \varphi & * \\ 0 & \psi \end{pmatrix}$, où ψ est un caractère non ramifié de D_ℓ, φ est un caractère de D_ℓ dont la restriction à un sous-groupe d'indice fini de I_ℓ est χ_ℓ^{k-1} pour un entier $k \geq 2$, et $\varphi \not\equiv \psi \bmod \mathfrak{m}_A$.*

Si $\overline{\rho}$ est modulaire et que sa restriction à $G_{\mathbf{Q}(\sqrt{\ell^*})}$ (où $\ell^* = (-1)^{(\ell-1)/2}\ell$) est irréductible, ρ est modulaire.

Ce théorème est démontré par Wiles [16], complété par Taylor-Wiles [15], sous l'hypothèse restrictive suivante : pour tout nombre premier $p \equiv -1 \bmod \ell$ tel que $\overline{\rho}_{|I_p}$ soit réductible, $\overline{\rho}_{|D_p}$ l'est aussi. Dans [4], Diamond montre comment s'affranchir de cette hypothèse.

Nous ne traiterons ici que le cas particulier du th. 1 utilisé par Serre dans son exposé ([S], 2.4), pour démontrer la conjecture de Taniyama-Weil pour les courbes elliptiques semi-stables : celui où l'on a $\det\rho = \chi_\ell$ et où, pour tout nombre premier $p \neq \ell$, le groupe $\rho(I_p)$ est unipotent, *i.e.* conjugué d'un sous-groupe de $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. On trouvera un exposé détaillé de la preuve de Wiles dans ce cas dans [2'] ; nous en résumerons les grandes lignes.

Le principe de la démonstration est le suivant. On part d'une représentation continue ρ_0 de $G_{\mathbf{Q}}$, de degré 2 sur un corps fini F de caractéristique ℓ, qui est semi-stable (n° 1) et vérifie des conditions convenables d'irréductibilité. À chaque ensemble fini Σ de nombres premiers est associé un type de déformations de ρ_0 (n° 2). Il existe une déformation universelle de ρ_0 de type Σ, définie sur un anneau R_Σ (*loc. cit.*). Les représentations galoisiennes associées aux formes modulaires fournissent, lorsque ρ_0 est supposée modulaire, une déformation de ρ_0 de type Σ à un anneau $\mathbf{T}_\Sigma$ construit à partir des algèbres de Hecke (n° 3 et 4). On déduit de la propriété universelle de R_Σ un homomorphisme d'anneaux $\pi_\Sigma : R_\Sigma \to \mathbf{T}_\Sigma$ (n° 5) ; il est surjectif. Soit Σ_1 l'ensemble formé de ℓ et des nombres premiers $p \neq \ell$ en lesquels ρ_0 est non ramifiée. Pour traiter le cas particulier du th. 1 considéré ci-dessus, il suffit de prouver π_Σ est bijectif pour tout sous-ensemble fini Σ de Σ_1. Deux critères pour qu'un homomorphisme d'anneaux soit un isomorphisme entre anneaux d'intersection complète sont énoncés dans l'appendice III. Le premier, appliqué au n° 6, permet de prouver d'une part que $\pi_\varnothing$ est bijectif, d'autre part que $\mathbf{T}_\varnothing$ est un anneau d'intersection complète. (C'est dans la preuve de ces énoncés que se trouvait le "trou" de la démonstration initiale de Wiles, comblé par Taylor-Wiles.) La variation de certains invariants numériques des anneaux locaux R_Σ et $\mathbf{T}_\Sigma$ en fonction de Σ est décrite au n° 7. Leur comparaison permet en appliquant le second critère de conclure par récurrence que, pour tout sous-ensemble fini Σ de Σ_1, π_Σ est bijectif et $\mathbf{T}_\Sigma$ est un anneau d'intersection complète, ce qui termine la démonstration.

1. REPRÉSENTATIONS SEMI-STABLES

Soient F un corps fini de caractéristique ℓ et ρ une représentation continue de $G_{\mathbf{Q}}$ dans un espace vectoriel V de dimension 2 sur F. Soit $\overline{\rho} : G_{\mathbf{Q}} \to \mathbf{GL}_2(\overline{\mathrm{F}})$ une représentation déduite de ρ par choix d'une base de V et extension des scalaires à une clôture algébrique de F. Le triplet associé à $\overline{\rho}$ dans le n° 2.2 de [S] ne dépend que de ρ ; nous le noterons $\big(\mathrm{N}(\rho), k(\rho), \varepsilon(\rho)\big)$. Nous dirons que ρ est *modulaire* si $\overline{\rho}$ est modulaire au sens de *loc. cit.*.

Nous dirons que ρ est *bonne en* ℓ si le D_ℓ-module V provient d'un schéma en groupes fini et plat sur $\mathbf{Z}_\ell$ et que $\det\rho$ coïncide avec χ_ℓ dans I_ℓ. Nous dirons que ρ est *semi-stable en* ℓ si elle est bonne en ℓ ou que $\rho_{|\mathrm{I}_\ell}$ s'écrit $\begin{pmatrix} \chi_{\ell|\mathrm{I}_\ell} & * \\ 0 & 1 \end{pmatrix}$ dans une base convenable de V. Pour que ρ soit bonne (resp. semi-stable) en ℓ, il faut et il suffit d'après [14] que $k(\rho)$ soit égal à 2 (resp. à 2 ou à $\ell+1$).

Soit p un nombre premier distinct de ℓ. Nous dirons que ρ est *bonne en* p si elle est non ramifiée en p. Nous dirons que ρ est *semi-stable* en p si $\rho(\mathrm{I}_p)$ est un sous-groupe unipotent de $\mathbf{GL}(\mathrm{V})$; il est alors d'ordre 1 ou ℓ.

Nous dirons que la représentation ρ est *semi-stable* si elle est semi-stable en tout nombre premier. Pour cela, il faut et il suffit que $k(\rho)$ soit égal à 2 ou $\ell+1$, que $\mathrm{N}(\rho)$ soit sans facteurs carrés et que $\varepsilon(\rho)=1$. Si ρ est semi-stable, on a $\det\rho=\chi_\ell$. Notons alors $\overline{\mathrm{N}}(\rho)$ le produit des nombres premiers en lesquels ρ n'est pas bonne : on a $\overline{\mathrm{N}}(\rho)=\mathrm{N}(\rho)$ si ρ est bonne en ℓ, et $\overline{\mathrm{N}}(\rho)=\ell\mathrm{N}(\rho)$ sinon.

Remarque 1. — Si ρ est irréductible et de déterminant χ_ℓ, elle est absolument irréductible ([14], 3.3). Si de plus ρ est semi-stable en ℓ et $\ell \geq 5$, la restriction de ρ à $\mathrm{H}=\mathrm{G}_{\mathbf{Q}(\sqrt{\ell^*})}$ (où $\ell^*=(-1)^{(\ell-1)/2}\ell$) est absolument irréductible. Il résulte en effet de [14] que $\overline{\rho}(\mathrm{I}_\ell)$ est contenu dans un sous-groupe de Borel de $\mathbf{GL}_2(\overline{\mathrm{F}})$ et qu'un élément au moins de $\overline{\rho}(\mathrm{I}_\ell\cap\mathrm{H})$ a deux valeurs propres distinctes. On en déduit que toute droite stable par $\overline{\rho}(\mathrm{I}_\ell\cap\mathrm{H})$ est aussi stable par $\overline{\rho}(\mathrm{I}_\ell)$. Le groupe d'inertie I_ℓ n'est pas contenu dans H ; on a donc $\mathrm{G}_{\mathbf{Q}}=\mathrm{I}_\ell\mathrm{H}$. S'il existait une droite stable par $\overline{\rho}(\mathrm{H})$, elle serait aussi stable par $\overline{\rho}(\mathrm{G}_{\mathbf{Q}})$, ce qui est absurde.

Pour $k\geq 2$ et $\mathrm{N}\geq 1$, notons $\mathrm{S}(\mathrm{N},k,1)_{\overline{\mathrm{F}}}$ l'espace vectoriel des formes modulaires paraboliques de type $(\mathrm{N},k,1)$ à coefficients dans $\overline{\mathrm{F}}$, au sens de [14], 3.1.

PROPOSITION 1.— *Supposons ρ semi-stable et irréductible. Si $\ell=3$, supposons de plus que la restriction de ρ à $\mathrm{G}_{\mathbf{Q}(\sqrt{-3})}$ soit absolument irréductible. Alors, si ρ est modulaire, elle est associée au sens de* [S], 2.1, *à une forme modulaire $f\in\mathrm{S}(\overline{\mathrm{N}}(\rho),2,1)_{\overline{\mathrm{F}}}$, fonction propre des opérateurs de Hecke T_p pour $p\not|\,\ell\overline{\mathrm{N}}(\rho)$.*

C'est là un résultat difficile, qui a requis les efforts combinés de nombreux mathématiciens. On prouve d'abord que ρ est associée à une forme modulaire $g \in S(N(\rho), k(\rho), 1)_{\overline{F}}$, fonction propre des opérateurs T_p pour $p \nmid \ell\overline{N}(\rho)$ (cf. [5], cor. 1.2 du th. 1.1 où sont récapitulés les travaux cités dans [S], 2.2, remarque 2). La prop. 1 en résulte si $k(\rho) = 2$. Si $k(\rho) = \ell + 1$ et $\ell \geq 5$, on utilise le fait que, pour tout entier $N \geq 1$ premier à ℓ, les éléments de $S(N, \ell+1, 1)_{\overline{F}}$ coïncident avec ceux de $S(\ell N, 2, 1)_{\overline{F}}$ possédant un relèvement en caractéristique 0 dont la trace de $\Gamma_0(\ell N)$ à $\Gamma_0(N)$ est nulle (pour $N = 1$, voir [13], 3.3 ; le cas général est analogue). Le cas où $k(\rho) = \ell + 1$ et $\ell = 3$, plus subtil, est traité dans [5], th. 5.1 et lemme 2.1.

Remarque 2. — La forme modulaire f est en fait unique à un scalaire multiplicatif près et est fonction propre de tous les opérateurs de Hecke T_n ($n \geq 1$). Pour tout nombre premier p, la valeur propre a_p de T_p associée à f est la trace de Frob_p opérant sur le plus grand quotient de V non ramifié en p.

2. DÉFORMATIONS D'UNE REPRÉSENTATION SEMI-STABLE

Soient F un corps fini de caractéristique ℓ et ρ_0 une représentation continue de $G_{\mathbf{Q}}$ de degré 2 sur F, qui est *semi-stable* (cf. n° 1) et irréductible (donc absolument irréductible, d'après la remarque 1 du n° 1) ; rappelons que son déterminant est χ_ℓ.

Soient A un anneau local noethérien complet de corps résiduel F et ρ une déformation de ρ_0 à A (*i.e.* une représentation continue de $G_{\mathbf{Q}}$ dans un A-module M_ρ libre de rang 2, dont la représentation résiduelle est isomorphe à ρ_0 ; cf. App. II, n° 2). Supposons son déterminant égal à χ_ℓ. Nous dirons que ρ est *bonne en* ℓ si, pour tout idéal $\mathfrak{a}$ d'indice fini de A, le D_ℓ-module $M_\rho/\mathfrak{a}M_\rho$ provient d'un schéma en groupes fini et plat sur $\mathbf{Z}_\ell$. Nous dirons que ρ est *ordinaire en* ℓ si $\rho_{|I_\ell}$ s'écrit $\begin{pmatrix} \chi_{\ell|I_\ell} & * \\ 0 & 1 \end{pmatrix}$ dans une base convenable de M_ρ ; il suffit pour cela qu'il existe un sous-groupe fermé M' de M_ρ, stable par I_ℓ, tel que I_ℓ opère par χ_ℓ sur M' et par 1 sur M_ρ/M'. Nous dirons que ρ est *semi-stable en* ℓ si elle est bonne ou ordinaire en ℓ.

Remarques. — 1) Il arrive que ρ soit à la fois bonne et ordinaire en ℓ. Plus précisément, supposons ρ ordinaire en ℓ. Le $A[I_\ell]$-module M_ρ est alors isomorphe à une extension

$$0 \to A(1) \xrightarrow{\iota} E \xrightarrow{\pi} A \to 0$$

de A (muni de l'action triviale de I_ℓ) par $A(1) = A \otimes_{\mathbf{Z}_\ell} \varprojlim \mu_{\ell^n}$. Associons à ρ un idéal principal $\mathfrak{a}_\rho$ de A la manière suivante. Si l'anneau A est fini, l'extension E est

caractérisée par sa classe de cohomologie $\xi_E \in H^1(I_\ell, A(1))$ (c'est la classe commune des cocycles $\sigma \mapsto \sigma(x) - x$, où $x \in \pi^{-1}(1)$), et $H^1(I_\ell, A(1))$ s'identifie par la théorie de Kummer à $(Q_\ell^{nr})^\times \otimes_{\mathbf{Z}} A$ (où Q_ℓ^{nr} est l'extension non ramifiée maximale de Q_ℓ dans $\overline{Q}_\ell$). À multiplication près par un élément de $A^\times$, ξ_E ne dépend que de ρ. Par définition, $\mathfrak{a}_\rho$ est l'idéal de A engendré par $(v \otimes 1_A)(\xi_E)$, où $v : (Q_\ell^{nr})^\times \to \mathbf{Z}$ est la valuation ℓ-adique. Lorsque A n'est pas fini, on applique ce qui précède aux quotients finis de A et on définit $\mathfrak{a}_\rho$ par passage à la limite projective. Pour que ρ soit bonne en ℓ, il faut et il suffit que l'on ait $\mathfrak{a}_\rho = 0$.

2) Supposons ρ semi-stable en ℓ. Alors ρ est ordinaire en ℓ si ρ_0 est ordinaire en ℓ.

Soit Σ un ensemble fini de nombres premiers. Disons qu'une déformation ρ de ρ_0 est *de type* Σ si son déterminant est χ_ℓ, qu'elle est semi-stable en ℓ et qu'elle a le même type de propriétés que ρ_0 en dehors de Σ, à savoir :

— si $\ell \notin \Sigma$ et que ρ_0 est bonne en ℓ, ρ est bonne en ℓ ;

— si $p \notin \Sigma \cup \{\ell\}$ et que ρ_0 est non ramifiée en p, ρ est non ramifiée en p ;

— si $p \notin \Sigma \cup \{\ell\}$ et que ρ_0 est ramifiée en p, $\rho_{|I_p}$ s'écrit $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ dans une base convenable de M_ρ. (Il suffit pour cela qu'il existe un sous-groupe fermé M' de M_ρ, stable par I_p, tel que I_p opère trivialement sur M' et M_ρ/M'.)

Une déformation de ρ_0 de type Σ est non ramifiée en dehors de l'ensemble fini des nombres premiers qui divisent $\ell N(\rho_0)$ ou appartiennent à Σ. Une déformation de ρ_0, non ramifiée en dehors d'un ensemble fini S de nombres premiers, de déterminant χ_ℓ et semi-stable en ℓ, est de type $S \cup \{\ell\}$.

PROPOSITION 2.— *Il existe un anneau local noethérien complet* R_Σ, *de corps résiduel* F, *et une déformation* ρ_Σ *de type* Σ *de* ρ_0 *à* R_Σ, *possédant la propriété universelle suivante : pour tout anneau local noethérien complet* A, *de corps résiduel* F, *et toute déformation* ρ *de type* Σ *de* ρ_0 *à* A, *il existe un unique homomorphisme d'anneaux* $u : R_\Sigma \to A$, *induisant l'identité sur les corps résiduels, tel que* ρ *soit isomorphe à* $\rho_\Sigma \otimes_{R_\Sigma} 1_A$.

Compte tenu des définitions précédentes et de la remarque 2, c'est un cas particulier de la situation considérée dans la prop. 2 et la remarque 1 de l'appendice II, n° 2.

Le couple (R_Σ, ρ_Σ) est unique à isomorphisme unique près. Nous dirons que R_Σ est *l'anneau universel de déformation de type* Σ *de* ρ_0 et que ρ_Σ est *la déformation universelle de type* Σ *de* ρ_0. Soit Σ' un sous-ensemble de Σ. Il existe d'après la

prop. 2 un unique homomorphisme d'anneaux $u_{\Sigma'\Sigma} : R_\Sigma \to R_{\Sigma'}$, induisant l'identité sur les corps résiduels, tel que $\rho_{\Sigma'}$ soit isomorphe à $\rho_\Sigma \otimes_{R_\Sigma} R_{\Sigma'}$; cet homomorphisme est *surjectif* (App. II, n° 1, remarque 2).

Remarque 3. — Soit V l'espace de la représentation ρ_0 et soit $\mathfrak{sl}(V)$ le $G_{\mathbf{Q}}$-module formé des endomorphismes de V de trace nulle (cf. App. II, n° 2, remarque 2). Les classes d'isomorphisme de déformations de ρ_0 à $k[\varepsilon]$ de déterminant χ_ℓ correspondent bijectivement aux éléments de $H^1\big(G_{\mathbf{Q}}, \mathfrak{sl}(V)\big)$ (*loc. cit.*). Celles des déformations de type Σ correspondent aux éléments d'un sous-groupe $H^1_\Sigma\big(G_{\mathbf{Q}}, \mathfrak{sl}(V)\big)$ (*loc. cit.*), qui est en fait un groupe de Selmer (cf. App. IV), défini par une famille $\mathcal{L}_\Sigma = (L_{\Sigma,p})$, où, pour chaque p, $L_{\Sigma,p}$ est un sous-groupe de $H^1\big(D_p, \mathfrak{sl}(V)\big)$ qui reflète les exigences locales en p imposées à une déformation de type Σ. (Nous ne parlons pas de la place à l'infini, car le groupe de cohomologie local correspondant est nul.) Pour $p \neq \ell$, par exemple, $L_{\Sigma,p}$ est égal à $H^1\big(D_p, \mathfrak{sl}(V)\big)$ si $p \in \Sigma$ et à $H^1_{nr}\big(D_p, \mathfrak{sl}(V)\big)$ si $p \notin \Sigma$.

3. ALGÈBRES DE HECKE ET REPRÉSENTATIONS GALOISIENNES ASSOCIÉES

Soit N un entier ≥ 1. Notons $S = S(N, 2, 1)$ l'espace vectoriel sur $\mathbf{C}$ des formes modulaires paraboliques de type $(N, 2, 1)$, $\mathbf{T} = \mathbf{T}(N)$ l'anneau d'endomorphismes de S engendré par les opérateurs de Hecke T_n $(n \geq 1)$ et $\mathbf{T}' = \mathbf{T}'(N)$ celui engendré par les opérateurs T_n pour n premier à ℓN. L'anneau $\mathbf{T}$ est commutatif et libre de rang fini sur $\mathbf{Z}$; son sous-anneau $\mathbf{T}'$ est réduit. On définit une application $\mathbf{T}$-linéaire bijective de $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{T}, \mathbf{C})$ sur S par $u \mapsto \sum_{n=1}^{\infty} u(T_n) q^n$. Par cette bijection, les formes modulaires $f \in S$ qui sont fonctions propres de tous les opérateurs de Hecke correspondent aux homomorphismes d'anneaux de $\mathbf{T}$ dans $\mathbf{C}$; les formes modulaires dont le développement à l'infini est à coefficients dans un sous-anneau R de $\mathbf{C}$ correspondent aux éléments de $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{T}, R)$.

PROPOSITION 3.— *Soit* $\mathfrak{m}$ *un idéal maximal de* $\mathbf{T}'$, *de caractéristique résiduelle* ℓ.

a) *Il existe une représentation continue semi-simple* $\tilde{\rho}_{\mathfrak{m}}$ *de degré* 2 *de* $G_{\mathbf{Q}}$ *sur le corps* $\mathbf{T}'/\mathfrak{m}$, *non ramifiée en dehors de* ℓN, *telle que* $\mathrm{Tr}\,\tilde{\rho}_{\mathfrak{m}}(\mathrm{Frob}_p) = T_p$ *et* $\det \tilde{\rho}_{\mathfrak{m}}(\mathrm{Frob}_p) = p$ *pour* $p \nmid \ell N$. *Une telle représentation est unique à isomorphisme près.*

b) *Supposons* $\tilde{\rho}_{\mathfrak{m}}$ *irréductible. Notons* $\mathbf{T}'_{\mathfrak{m}}$ *le complété* $\mathfrak{m}$*-adique de* $\mathbf{T}'$. *Il existe une représentation continue* $\rho_{\mathfrak{m}}$ *de degré* 2 *de* $G_{\mathbf{Q}}$ *sur l'anneau* $\mathbf{T}'_{\mathfrak{m}}$, *non ramifiée en dehors de* ℓN, *telle que* $\mathrm{Tr}\,\rho_{\mathfrak{m}}(\mathrm{Frob}_p) = T_p$ *et* $\det \rho_{\mathfrak{m}}(\mathrm{Frob}_p) = p$ *pour* $p \nmid \ell N$. *Une telle représentation est unique à isomorphisme près.*

Soit $\mathbf{F}$ une clôture algébrique du corps fini $\mathbf{T}'/\mathfrak{m}$. L'homomorphisme canonique $\mathbf{T}' \to \mathbf{T}'/\mathfrak{m}$ se prolonge en un homomorphisme d'anneaux $u : \mathbf{T} \to \mathbf{F}$, et $f = \sum u(\mathrm{T}_n)q^n$ est un élément de $\mathrm{S}(\mathrm{N}, 2, 1)_{\mathbf{F}}$ (avec les notations du n° 1) ; toute représentation semi-simple de $\mathrm{G}_{\mathbf{Q}}$ de degré 2 sur $\mathbf{F}$ associée à f au sens de [S], 2.1, possède les propriétés de a), et est réalisable sur $\mathbf{T}'/\mathfrak{m}$ ([3], lemme 6.13). Cela prouve l'existence de $\tilde{\rho}_{\mathfrak{m}}$. L'unicité résulte de la prop. 1 de l'appendice I.

Le groupe $\mathrm{G}_{\mathbf{Q}}$ opère continûment sur le module de Tate $\mathbb{T}_\ell\big(\mathrm{J}_0(\mathrm{N})\big)$ de la jacobienne de $\mathrm{X}_0(\mathrm{N})$, et $\mathbb{T}_\ell\big(\mathrm{J}_0(\mathrm{N})\big) \otimes_{\mathbf{Z}} \mathbf{Q}$ est un $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$-module libre de rang 2, d'où une représentation linéaire continue ρ_ℓ de degré 2 de $\mathrm{G}_{\mathbf{Q}}$ sur $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$. Cette représentation est non ramifiée en dehors de $\ell\mathrm{N}$, et l'on a $\operatorname{Tr} \rho_\ell(\mathrm{Frob}_p) = \mathrm{T}_p$ et $\det \rho_\ell(\mathrm{Frob}_p) = p$ pour $p \nmid \ell\mathrm{N}$, d'après les relations d'Eichler-Shimura. Notons $\rho_{\ell,\mathfrak{m}}$ la représentation déduite de ρ_ℓ par extension des scalaires de $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$ à $\mathbf{T}_{\mathfrak{m}} \otimes_{\mathbf{Z}} \mathbf{Q}$. L'homomorphisme canonique $\mathbf{T}'_{\mathfrak{m}} \to \mathbf{T}_{\mathfrak{m}} \otimes_{\mathbf{Z}} \mathbf{Q}$ est injectif et la trace de $\rho_{\ell,\mathfrak{m}}$ prend ses valeurs dans $\mathbf{T}'_{\mathfrak{m}}$ d'après le théorème de Cebotarev. Supposons la représentation $\tilde{\rho}_{\mathfrak{m}}$ irréductible. Elle est alors absolument irréductible puisque son déterminant est impair, et $\rho_{\ell,\mathfrak{m}}$ provient par extension des scalaires d'une représentation $\rho_{\mathfrak{m}}$ de $\mathrm{G}_{\mathbf{Q}}$ de degré 2 sur $\mathbf{T}'_{\mathfrak{m}}$ (App. I, prop. 2 et remarque). Une telle représentation $\rho_{\mathfrak{m}}$ est nécessairement continue et satisfait aux conditions de b). Son unicité à isomorphisme près résulte de *loc. cit.*, prop. 1.

Remarques. — 1) Sous les hypothèses de b), la représentation résiduelle de $\rho_{\mathfrak{m}}$ est isomorphe à $\tilde{\rho}_{\mathfrak{m}}$ (App. I, cor. de la prop. 1), et il existe un sous-$\mathbf{T}'_{\mathfrak{m}}$-module libre de rang 2 de $\mathbb{T}_\ell\big(\mathrm{J}_0(\mathrm{N})\big)_{\mathfrak{m}}$, stable par $\mathrm{G}_{\mathbf{Q}}$, qui fournit un modèle de $\rho_{\mathfrak{m}}$.

2) Conservons les notations de la prop. 2. Soit N_1 un multiple de N. On dispose d'une application de restriction $r : \mathbf{T}'(\mathrm{N}_1) \to \mathbf{T}'(\mathrm{N})$ qui applique T_n sur T_n pour $n \geq 1$ premier à $\ell\mathrm{N}_1$. Posons $\mathfrak{m}_1 = r^{-1}(\mathfrak{m})$; c'est un idéal maximal de $\mathbf{T}'(\mathrm{N}_1)$. La représentation $\tilde{\rho}_{\mathfrak{m}}$ provient (à isomorphisme près) de $\tilde{\rho}_{\mathfrak{m}_1}$ par l'extension des scalaires $\mathbf{T}(\mathrm{N}_1)/\mathfrak{m}_1 \to \mathbf{T}(\mathrm{N})/\mathfrak{m}$ (App. I, cor. de la prop. 1). Si $\tilde{\rho}_{\mathfrak{m}}$ est irréductible, la représentation $\rho_{\mathfrak{m}}$ provient (à isomorphisme près) de $\rho_{\mathfrak{m}_1}$ par l'extension des scalaires $\hat{r} : \mathbf{T}(\mathrm{N}_1)_{\mathfrak{m}_1} \to \mathbf{T}(\mathrm{N})_{\mathfrak{m}}$ (*loc. cit.*) ; on en déduit, en considérant les traces de ces représentations, que $\hat{r}$ est surjectif. (On peut démontrer mieux : le conoyau de r est un 2-groupe fini ; il est réduit à un élément si $2 \nmid \mathrm{N}_1$ ou si $2 \mid \mathrm{N}$.)

4. DÉFORMATIONS DE HECKE D'UNE REPRÉSENTATION SEMI-STABLE

Soient F un corps fini de caractéristique ℓ et ρ_0 une représentation continue de $\mathrm{G}_{\mathbf{Q}}$, de degré 2 sur F, *semi-stable, modulaire et irréductible* (cf n° 1). Si $\ell = 3$,

on suppose que la restriction de ρ_0 à $G_{\mathbf{Q}(\sqrt{-3})}$ est absolument irréductible. Soit $\overline{N} = \overline{N}(\rho_0)$ le produit des nombres premiers p en lesquels ρ_0 n'est pas bonne(*loc.cit.*).

PROPOSITION 4.— *Il existe un unique homomorphisme d'anneaux* $a : T'(\overline{N}) \to F$ *qui applique* T_p *sur* $\mathrm{Tr}\,\rho_0(\mathrm{Frob}_p)$ *pour tout nombre premier* p *tel que* $p \nmid \ell\overline{N}$. *Soit* $\mathfrak{m}$ *son noyau. C'est un idéal maximal de* $T'(\overline{N})$, *et la représentation* ρ_0 *est isomorphe à celle déduite de* $\widetilde{\rho}_{\mathfrak{m}}$ (cf. n° 3) *par l'extension des scalaires* $T'(\overline{N})/\mathfrak{m} \to F$.

C'est une autre formulation de la prop. 1 du n° 1. En effet, soit $f \in S(\overline{N}, 2, 1)_{\overline{F}}$ une forme modulaire, fonction propre des opérateurs de Hecke T_p pour $p \nmid \ell\overline{N}$, satisfaisant les conclusions de cette proposition. Soit $a : T'(\overline{N}) \to \overline{F}$ l'homomorphisme d'anneaux tel que $T(f) = a(T)f$ pour $T \in T'(\overline{N})$. On a alors $a(T_p) = \mathrm{Tr}\,\rho_0(\mathrm{Frob}_p)$ pour tout nombre premier p tel que $p \nmid \ell\overline{N}$. Cela prouve l'existence de a ; son unicité est claire. La dernière assertion de la prop. 4 résulte de la prop. 1 de l'appendice I.

Pour tout ensemble fini Σ de nombres premiers, notons $N_\Sigma(\rho_0)$, ou simplement N_Σ, l'entier $\prod p^{n_p}$, où n_p est l'exposant de p dans $\overline{N}$ si $p \notin \Sigma$, est 2 si $p \in \Sigma$ et $p \neq \ell$, et 1 si $p \in \Sigma$ et $p = \ell$. On a $N_\varnothing = \overline{N}$. Notons m_Σ l'idéal maximal de $T'(N_\Sigma)$, image réciproque de $\mathfrak{m}$ (cf. prop. 4) par l'application de restriction $T'(N_\Sigma) \to T'(\overline{N})$.

PROPOSITION 5.— *Soient* A *un anneau local noethérien complet de corps résiduel* F, ρ *une déformation de* ρ_0 *à* A, *et* Σ *un ensemble fini de nombres premiers. Les conditions suivantes sont équivalentes :*

a) *La représentation* ρ *est non ramifiée en dehors de* ℓN_Σ *et il existe un homomorphisme d'anneaux* $\alpha : T'(N_\Sigma) \to A$ *tel que* $\mathrm{Tr}\,\rho(\mathrm{Frob}_p) = \alpha(T_p)$ *pour* $p \nmid \ell N_\Sigma$.

b) *Il existe un homomorphisme d'anneaux* $\widehat{\alpha} : T'(N_\Sigma)_{\mathfrak{m}_\Sigma} \to A$ *tel que* ρ *soit isomorphe à la représentation déduite de* $\rho_{\mathfrak{m}_\Sigma}$ (cf. n° 3) *par l'extension des scalaires* $\widehat{\alpha}$.

Lorsqu'elles sont satisfaites, a) détermine α *de façon unique,* $\widehat{\alpha}$ *est le prolongement continu de* α, *et* ρ *est une déformation de* ρ_0 *de type* Σ (cf. n° 2).

Supposons la condition b) satisfaite. La condition a) l'est alors aussi, avec pour α la restriction de $\widehat{\alpha}$, et l'homomorphisme $\widehat{\alpha}$ est local, donc continu. Il résulte de la remarque 1 du n° 3, des propriétés des modules de Tate des variétés abéliennes semi-stables sur un corps local, et du fait que $J_0(N_\Sigma)$ a bonne réduction en un nombre premier p si $p \nmid N$ et réduction semi-stable en p si $p^2 \nmid N$, que ρ est une déformation de type Σ de ρ_0.

Supposons la condition a) satisfaite. Elle détermine α de façon unique, et les applications composées $T'(N_\Sigma) \xrightarrow{\alpha} A \to F$ et $T'(N_\Sigma) \to T'(\overline{N}) \xrightarrow{a} F$ (avec a comme dans la prop. 4) sont égales. Il en résulte que $\alpha(\mathfrak{m}_\Sigma)$ est contenu dans

l'idéal maximal de A, donc que α se prolonge par continuité en un homomorphisme $\widehat{\alpha} : \mathbf{T}'(\mathrm{N}_\Sigma)_{\mathfrak{m}_\Sigma} \to \mathrm{A}$. Celui-ci satisfait b) (App. I, cor. de la prop. 1).

Nous dirons qu'une déformation de ρ_0 satisfaisant les conditions a) et b) de la prop. 5 est une *déformation modulaire de type* Σ *de* ρ_0.

Soit F_0 le sous-corps de F engendré par $\mathrm{Tr}\,\rho_0(\mathrm{G}_\mathbf{Q})$. Il s'identifie au corps résiduel de $\mathfrak{m}_\Sigma$, de sorte que $\mathbf{T}'(\mathrm{N}_\Sigma)_{\mathfrak{m}_\Sigma}$ est une algèbre sur l'anneau des vecteurs de Witt $\mathrm{W}(\mathrm{F}_0)$. Notons $\mathbf{T}_\Sigma(\rho_0)$, ou simplement $\mathbf{T}_\Sigma$, l'anneau $\mathbf{T}'(\mathrm{N}_\Sigma)_{\mathfrak{m}_\Sigma} \otimes_{\mathrm{W}(\mathrm{F}_0)} \mathrm{W}(\mathrm{F})$. Il est local noethérien et complet, son corps résiduel est F, et la représentation déduite de $\rho_{\mathfrak{m}_\Sigma}$ par extension des scalaires à $\mathbf{T}_\Sigma$ est une déformation modulaire de type Σ de ρ_0. Notons-là ρ_Σ^{Hecke}. La prop. 5 peut s'interpréter en disant que le couple $(\mathbf{T}_\Sigma, \rho_\Sigma^{Hecke})$ possède la propriété universelle suivante.

PROPOSITION 6.— *Pour tout anneau local noethérien complet* A *de corps résiduel* F *et toute déformation modulaire de type* Σ *de* ρ_0 *à* A, *il existe un unique homomorphisme d'anneaux* $v : \mathbf{T}_\Sigma \to \mathrm{A}$, *induisant l'identité sur les corps résiduels, tel que* ρ *soit isomorphe à* $\rho_\Sigma^{Hecke} \otimes_{\mathbf{T}_\Sigma} 1_\mathrm{A}$.

Nous dirons que $\mathbf{T}_\Sigma$ est *l'anneau universel de déformation modulaire de type* Σ *de* ρ_0 et que ρ_Σ^{Hecke} est *la déformation de Hecke de type* Σ *de* ρ_0. Soit Σ' un sous-ensemble de Σ. Il existe d'après la prop. 6 un unique homomorphisme d'anneaux $v_{\Sigma'\Sigma} : \mathbf{T}_\Sigma \to \mathbf{T}_{\Sigma'}$, induisant l'identité sur les corps résiduels, tel que $\rho_{\Sigma'}^{Hecke}$ soit isomorphe à $\rho_\Sigma^{Hecke} \otimes_{\mathbf{T}_\Sigma} \mathbf{T}_{\Sigma'}$; cet homomorphisme est *surjectif* (n° 3, remarque 2).

Remarque. — L'anneau $\mathbf{T}'(\mathrm{N}_\Sigma)$ est réduit et libre de rang fini sur $\mathbf{Z}$. Il en résulte que l'anneau $\mathbf{T}_\Sigma$ est réduit et libre de rang fini sur $\mathrm{W}(\mathrm{F})$.

5. ÉNONCÉ DU THÉORÈME PRINCIPAL

Soient F un corps fini de caractéristique ℓ et ρ_0 une représentation continue de $\mathrm{G}_\mathbf{Q}$, de degré 2 sur F, *semi-stable, modulaire et irréductible* (cf n° 1). Si $\ell = 3$, on suppose que la restriction de ρ_0 à $\mathrm{G}_{\mathbf{Q}(\sqrt{-3})}$ est absolument irréductible. Soit Σ un ensemble fini de nombres premiers. Rappelons que ρ_0 possède une déformation universelle ρ_Σ de type Σ à un anneau R_Σ (n° 2, prop. 2) et une déformation de Hecke ρ_Σ^{Hecke} de type Σ à un anneau $\mathbf{T}_\Sigma$ (n° 4, prop. 6). Les anneaux R_Σ et $\mathbf{T}_\Sigma$ sont locaux ; ce sont des $\mathrm{W}(\mathrm{F})$-algèbres, et leurs corps résiduels s'identifient canoniquement à F. Il existe un unique homomorphisme d'anneaux $\pi_\Sigma : \mathrm{R}_\Sigma \to \mathbf{T}_\Sigma$, induisant l'identité sur les corps résiduels, tel que ρ_Σ^{Hecke} se déduise (à isomorphisme près) de ρ_Σ par l'extension des scalaires π_Σ (n° 2, prop. 2). L'homomorphisme π_Σ

est surjectif : en effet la $W(F)$-algèbre T_Σ est engendrée par les opérateurs de Hecke T_p, pour p nombre premier qui ne divise pas ℓN_Σ, et T_p est l'image par π_Σ de la trace de $\rho_\Sigma(\mathrm{Frob}_p)$. Notons Σ_1 l'ensemble formé de ℓ et des nombres premiers $p \neq \ell$ en lesquels ρ_0 n'est pas ramifiée.

THÉORÈME 2.— *Si* $\Sigma \subset \Sigma_1$, *l'homomorphisme* $\pi_\Sigma : R_\Sigma \to T_\Sigma$ *est bijectif et* T_Σ *est un anneau d'intersection complète* (cf. App. III, n° 1).

COROLLAIRE.— *Si* $\Sigma \subset \Sigma_1$, *toute déformation de* ρ_0 *de type* Σ (cf. n° 2) *est une déformation modulaire de type* Σ (cf. n° 4).

Indiquons comment le th. 1 (dans le cas particulier considéré dans l'introduction) se déduit du th. 2. La représentation ρ dans ce cas particulier est par hypothèse de déterminant χ_ℓ. Elle peut être considérée comme une déformation de sa représentation résiduelle $\widetilde{\rho}$. Pour tout $p \neq \ell$, le groupe $\widetilde{\rho}(I_p)$ est supposé unipotent : cela signifie que $\widetilde{\rho}$ est semi-stable en p. Sous chacune des hypothèses a) et b) du th. 1, $\widetilde{\rho}$ et ρ sont semi-stables en ℓ. Soit S l'ensemble des nombres premiers en lesquels ρ est ramifiée et $\widetilde{\rho}$ non ramifiée. L'ensemble $\Sigma = \{\ell\} \cup S$ est fini et contenu dans Σ_1, et ρ est une déformation de type Σ de $\widetilde{\rho}$. D'autre part, $\widetilde{\rho}$ est irréductible et, si $\ell = 3$, sa restriction à $G_{\mathbf{Q}(\sqrt{-3})}$ est absolument irréductible. D'après le cor. du th. 2, ρ est une déformation modulaire de $\widetilde{\rho}$ de type Σ. Elle satisfait donc la condition a) de la prop. 5, ce qui prouve qu'elle est une représentation modulaire au sens de [S],2.3.

Remarque. — Soit $\mathcal{O}$ un anneau de valuation discrète, libre de rang fini sur $W(F)$. Notons $\pi_{\Sigma,\mathcal{O}} : R_{\Sigma,\mathcal{O}} \to T_{\Sigma,\mathcal{O}}$ l'homomorphisme d'anneaux déduit de π par extension des scalaires de $W(F)$ à $\mathcal{O}$. Pour que T_Σ soit un anneau d'intersection complète, il faut et il suffit que $T_{\Sigma,\mathcal{O}}$ en soit un ; pour que π_Σ soit un isomorphisme, il faut et il suffit que $\pi_{\Sigma,\mathcal{O}}$ en soit un. Lorsque $\mathcal{O} = W(F')$, où F' est une extension finie de F, $R_{\Sigma,\mathcal{O}}$ et $T_{\Sigma,\mathcal{O}}$ s'identifient aux anneaux universels de déformations associés à $\rho_0 \otimes_F 1_{F'}$ (App. II, n° 1, remarque 4). Lorsque le corps résiduel de $\mathcal{O}$ est F, $R_{\Sigma,\mathcal{O}}$ et $T_{\Sigma,\mathcal{O}}$ possèdent des propriétés universelles analogues à celles des anneaux R_Σ et T_Σ pour les déformations de ρ aux $\mathcal{O}$-algèbres locales noethériennes complètes de corps résiduel F.

6. LE THÉORÈME 2 DANS LE CAS MINIMAL

6.1. Étude locale de certaines déformations

Soient F un corps fini de caractéristique ℓ et q un nombre premier congru à 1 mod ℓ. Soient A un anneau local noethérien complet, de corps résiduel F et ρ une

représentation continue du groupe de décomposition D_q dans un A-module libre M de rang n.

LEMME.— *Si la représentation résiduelle $\widetilde{\rho}$ de ρ est non ramifiée et que $\rho_0(\mathrm{Frob}_q)$ est diagonalisable, à valeurs propres simples, il existe une base de* M *sur* A *dans laquelle ρ se diagonalise. Dans cette base, $\rho_{|I_q}$ s'écrit $\mathrm{diag}(\chi_1, \ldots, \chi_n)$ où les $\chi_i : I_q \to A^\times$ sont d'ordre une puissance de ℓ qui divise $q-1$.*

D'après le lemme de Hensel, il existe une base de M sur A dans laquelle $\rho(\mathrm{Frob}_q)$ opère par une matrice diagonale $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Soit $x \in I_q$. La matrice de $\rho(x)$ dans la base précédente est de la forme $I_n + (a_{ij})$, avec les a_{ij} dans l'idéal maximal $\mathfrak{m}$ de A. Comme $\widetilde{\rho}$ est non ramifiée et $q \neq \ell$, ρ est modérément ramifiée ; par suite

$$\rho(\mathrm{Frob}_q)\rho(x)\rho(\mathrm{Frob}_q)^{-1} = \rho(x^q) = \rho(x)^q. \tag{1}$$

Soit $\mathfrak{a}$ l'idéal de A engendré par les a_{ij} pour $i \neq j$. On déduit de (1) que, pour $i \neq j$, on a $\lambda_i a_{ij} \lambda_j^{-1} \equiv q a_{ij} \equiv a_{ij} \bmod \mathfrak{m}\mathfrak{a}$ et par suite $a_{ij} \in \mathfrak{m}\mathfrak{a}$. Mais alors on a $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$, d'où $\mathfrak{a} = 0$ (lemme de Nakayama). Cela prouve que $\rho(x)$, et par suite tout élément de $\rho(D_q)$, opère diagonalement dans la base considérée. La relation (1) s'écrit alors $\rho(x) = \rho(x)^q$, de sorte que les caractères χ_i sont d'ordre fini divisant $q-1$; comme ils sont congrus à 1 modulo $\mathfrak{m}$, leurs ordres sont des puissances de ℓ.

Remarque. — Soit Δ_q le plus grand quotient de $(\mathbf{Z}/q\mathbf{Z})^\times$ d'ordre une puissance de ℓ. Par l'application composée $I_q \to G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\mu_q)/\mathbf{Q}) \to (\mathbf{Z}/q\mathbf{Z})^\times \to \Delta_q$, il s'identifie à un quotient de I_q. La dernière assertion du lemme signifie que les caractères χ_i se factorisent par Δ_q. À chaque valeur propre de $\widetilde{\rho}(\mathrm{Frob}_q)$ est canoniquement associé l'un des caractères χ_i, et donc un homomorphisme de Δ_q dans $A^\times$.

6.2. Construction d'ensembles auxiliaires de nombres premiers

Soient F un corps fini de caractéristique ℓ et ρ_0 une représentation continue de $G_{\mathbf{Q}}$, de degré 2 sur F, de déterminant χ_ℓ, dont la restriction à $G_{\mathbf{Q}(\sqrt{\ell^*})}$, où $\ell^* = (-1)^{(\ell-1)/2}\ell$, est absolument irréductible (cette dernière condition est automatiquement satisfaite lorsque $\ell \geq 5$ et que ρ_0 est semi-stable et irréductible ; cf. n° 1, remarque 1).

Notons V l'espace de la représentation ρ_0, et $\mathfrak{sl}(V)$ l'espace vectoriel des endomorphismes de V de trace nulle, muni de l'action adjointe de $G_{\mathbf{Q}}$ (cf. App. II, n° 2, remarque 2). On définit un isomorphisme canonique du $G_{\mathbf{Q}}$-module $\mathfrak{sl}(V)(1) = \mathfrak{sl}(V) \otimes \mu_\ell$ (où μ_ℓ désigne le groupe des racines ℓ-ièmes de l'unité de $\overline{\mathbf{Q}}$) sur le

$G_{\mathbf{Q}}$-module $\mathfrak{sl}(V)^* = \mathrm{Hom}_{\mathbf{Z}}(V, \overline{\mathbf{Q}}^{\times})$ (cf. App. IV) en associant à $x \otimes \zeta$ l'homomorphisme $y \mapsto \zeta^{t(xy)}$, où $t = \mathrm{Tr}_{F/\mathbf{F}_\ell} \circ \mathrm{Tr}$.

Fixons un entier $n \geq 1$.

PROPOSITION 7.— *Soit $\sigma \to a_\sigma$ un 1-cocycle continu de $G_{\mathbf{Q}}$ dans $\mathfrak{sl}(V)(1)$, non cohomologue à 0. Il existe $g \in G_{\mathbf{Q}}$ tel que :*

a) *les racines ℓ^n-ièmes de l'unité de $\overline{\mathbf{Q}}$ soient fixées par g ;*

b) *$\rho_0(g)$ ait deux valeurs propres distinctes dans $\overline{\mathrm{F}}$;*

c) *on ait $a_{g^m} \neq 0$, en notant m l'ordre de $\rho_0(g)$.*

C'est un exercice de théorie des groupes qui utilise la classification des images possibles de $G_{\mathbf{Q}}$ dans $\mathbf{PGL}(V)$ et que nous ne reproduirons pas ici.

Notons Q_n l'ensemble des nombres premiers $q \equiv 1 \bmod \ell^n$ tels que ρ_0 soit non ramifiée en q et que $\rho_0(\mathrm{Frob}_q)$ ait deux valeurs propres distinctes dans $\overline{\mathrm{F}}$.

COROLLAIRE 1.— *Il existe une infinité de nombres premiers $q \in Q_n$ tels que la restriction au groupe de décomposition D_q du cocyle $\sigma \to a_\sigma$ ne soit pas cohomologue à 0.*

Cela résulte de la prop. 1, d'après le théorème de densité de Cebotarev.

Remarque. — Si $q \in Q_n$, les espaces vectoriels $H^1_{nr}(D_q, \mathfrak{sl}(V))$ et $H^1_{nr}(D_q, \mathfrak{sl}(V)(1))$ (cf. App. IV) sont de dimension 1 sur F. Ils sont en effet isomorphes (D_q opère trivialement sur μ_ℓ puisque $q \equiv 1 \bmod \ell$) et leur dimension est égale à celle de $H^0(D_q, \mathfrak{sl}(V))$ puisque q est premier à l'ordre de $\mathfrak{sl}(V)$ (*loc. cit.*). Mais $H^0(D_q, \mathfrak{sl}(V))$ se compose des endomorphismes de V de trace nulle qui commutent à $\rho_0(\mathrm{Frob}_q)$; il est de dimension 1 puisque les deux valeurs propres de $\rho_0(\mathrm{Frob}_q)$ dans $\overline{\mathrm{F}}$ sont distinctes.

COROLLAIRE 2.— *Soit H un sous-espace vectoriel de $H^1(G_{\mathbf{Q}}, \mathfrak{sl}(V)(1))$ de dimension finie d. Il existe un sous-ensemble Q de Q_n, de cardinal d, tel que l'application $H \to \prod_{q \in Q} H^1_{nr}(D_q, \mathfrak{sl}(V)(1))$ déduite des applications de restriction soit bijective.*

Notons S l'ensemble des nombres premiers q tels que l'image de H dans $H^1(D_q, \mathfrak{sl}(V)(1))$ ne soit pas contenue dans $H^1_{nr}(D_q, \mathfrak{sl}(V)(1))$; il est fini (App. IV). Posons $Q'_n = Q_n - S$. L'application $H \to \prod_{q \in Q'_n} H^1_{nr}(D_q, \mathfrak{sl}(V)(1))$ déduite des applications de restriction est injective (cor.1) et $H^1_{nr}(D_q, \mathfrak{sl}(V)(1))$ est de dimension 1 pour tout $q \in Q'_n$ (remarque). Il existe donc un sous-ensemble Q de Q'_n, de cardinal d, tel que l'application $H \to \prod_{q \in Q} H^1_{nr}(D_q, \mathfrak{sl}(V)(1))$ soit bijective.

COROLLAIRE 3.— *Supposons que* ρ_0 *soit semi-stable* (cf. n° 1). *Soit* d *la dimension de* $H^1_{\varnothing}(G_{\mathbf{Q}}, \mathfrak{sl}(V))$ (cf. n° 2, remarque 3) *sur* F. *Il existe un sous-ensemble* Q *de* Q_n, *de cardinal* d, *tel que l'application canonique* $H^1_{\varnothing}(G_{\mathbf{Q}}, \mathfrak{sl}(V)) \to H^1_{Q}(G_{\mathbf{Q}}, \mathfrak{sl}(V))$ *soit bijective.*

Le groupe $H^1_{\varnothing}(G_{\mathbf{Q}}, \mathfrak{sl}(V))$ est le groupe de Selmer associé à une famille $\mathcal{L} = (L_p)$ de sous-groupes des groupes de cohomologie locaux, avec $L_p = H^1_{nr}(D_p, \mathfrak{sl}(V))$ pour $p \neq \ell$ (*loc. cit.*). Le groupe $H^1_{Q}(G_{\mathbf{Q}}, \mathfrak{sl}(V))$ est le groupe de Selmer associé à la famille $\mathcal{L}' = (L'_p)$, où $L'_p = L_p$ pour $p \notin Q$ et $L'_p = H^1(D_p, \mathfrak{sl}(V))$ pour $p \in Q$ (*loc. cit.*). Identifions $\mathfrak{sl}(V)^*$ à $\mathfrak{sl}(V)(1)$, notons H le sous-groupe de Selmer de $H^1(G_{\mathbf{Q}}, \mathfrak{sl}(V)(1))$ associé à la famille $\mathcal{L}^{\perp}$ (cf. App. IV) et d' sa dimension. Il existe un sous-ensemble Q de Q_n, de cardinal d', satisfaisant les conditions du cor. 2 pour H. Dans la suite exacte de la remarque de l'App. IV, appliquée au $G_{\mathbf{Q}}$-module $\mathfrak{sl}(V)$, l'application γ est duale de l'application $H \to \prod_{q \in Q} H^1_{nr}(D_q, \mathfrak{sl}(V)(1))$, donc est injective ; par suite l'application canonique $H^1_{\varnothing}(G_{\mathbf{Q}}, \mathfrak{sl}(V)) \to H^1_{Q}(G_{\mathbf{Q}}, \mathfrak{sl}(V))$ est bijective.

Il reste à prouver que l'on a $d = d'$. Or la formule (1) de l'App. IV s'écrit $d - d' = d_0 - d'_0 - d_+ + d_\ell$, avec $d_0 = \dim H^0(G_{\mathbf{Q}}, \mathfrak{sl}(V))$, $d'_0 = \dim H^0(G_{\mathbf{Q}}, \mathfrak{sl}(V)(1))$, $d_+ = \dim H^0(D_\infty, \mathfrak{sl}(V))$ et $d_\ell = \dim L_\ell - \dim H^0(D_\ell, \mathfrak{sl}(V))$. On a $d_0 = 0$ car ρ_0 est absolument irréductible, $d'_0 = 0$ car la restriction de ρ_0 à $G_{\mathbf{Q}(\sqrt{\ell^*})}$ est absolument irréductible, et $d_+ = 1$ car 1 est valeur propre simple de la conjugaison complexe opérant dans $\mathfrak{sl}(V)$. Le calcul de d_ℓ, plus compliqué, utilise la théorie de Fontaine-Lafaille qui établit une équivalence entre la catégorie des schémas en groupes fini et plat sur $\mathbf{Z}_\ell$ et une catégorie "concrète", relevant de l'algèbre linéaire. On trouve que d_ℓ est égal à 1. On a donc bien $d = d'$.

6.3. Fin de la démonstration du théorème 2 dans le cas minimal

Soient F un corps fini de caractéristique ℓ et ρ_0 une représentation continue de $G_{\mathbf{Q}}$ de degré 2 sur F, satisfaisant les hypothèses du th.2. On se propose de démontrer ce théorème lorsque Σ est l'ensemble vide. Quitte à étendre les scalaires (n° 5, remarque), on peut supposer que les valeurs propres des éléments de $\rho_0(G_{\mathbf{Q}})$ appartiennent à F. Posons alors $d = dim\, H^1_{\varnothing}(G_{\mathbf{Q}}, \mathfrak{sl}(V))$. Soit n un entier ≥ 1. Choisissons un ensemble Q de nombres premiers, de cardinal d, satisfaisant les conditions du cor. 3 de la prop. 7 et, pour chaque $q \in Q$, choisissons une des deux valeurs propres de $\rho_0(\mathrm{Frob}_q)$, ce qui définit (cf. 6.1, remarque), un homomorphisme de $\Delta_Q = \prod_{q \in Q} \Delta_q$ dans l'anneau $R^{\times}_Q$ de déformation universel de ρ_0 de type Q. Cela munit R_Q, et par suite son quotient T_Q, de structures de $W(F)[\Delta_Q]$-algèbres.

Notons $\mathfrak{a}_Q$ l'idéal d'augmentation de $W(F)[\Delta_Q]$. Pour qu'une déformation de type Q de ρ_0 à un anneau local noethérien complet A soit non ramifiée en les $q \in Q$, il faut et il suffit, par construction, que le noyau de l'homomorphisme associé $R_Q \to A$ contienne $\mathfrak{a}_Q R_Q$. L'homomorphisme canonique $R_Q \to R_\varnothing$ définit donc par passage au quotient un isomorphisme de $R_Q/\mathfrak{a}_Q R_Q$ sur $R_\varnothing$.

Nous utiliserons le résultat suivant (th. 3.13 de [2']), voisin du th. 2 de [15].

PROPOSITION 8.— *T_Q est un $W(F)[\Delta_Q]$-module libre et l'homomorphisme canonique $T_Q \to T_\varnothing$ définit par passage au quotient un isomorphisme de $T_Q/\mathfrak{a}_Q T_Q$ sur $T_\varnothing$.*

Définissons alors un homomorphisme u de l'anneau $A = W(F)[[S_1, \ldots, S_d]]$ dans $W(F)[\Delta_Q]$ en ordonnant les éléments $q_1, \ldots, q_d$ de Q et en envoyant $1 + S_i$ sur un générateur du groupe Δ_{q_i}. Son noyau $\mathfrak{b}$ est engendré par les $(1 + S_i)^{l^{n(i)}} - 1$, où $l^{n(i)}$ est l'ordre de Δ_{q_i}. Il est contenu dans l'idéal $\mathfrak{m}_A^n(S_1, \ldots, S_d)$ de A. Il résulte des propriétés décrites ci-dessus que le diagramme

$$\begin{array}{ccc} R_Q & \xrightarrow{\pi_Q} & T_Q \\ \downarrow & & \downarrow \\ R_\varnothing & \xrightarrow{\pi_\varnothing} & T_\varnothing \end{array}$$

est une $\mathfrak{b}$-structure pour $\pi_\varnothing$, au sens de l'App. III, n° 2. Il existe a fortiori une $\mathfrak{m}_A^n(S_1, \ldots, S_d)$-structure pour $\pi_\varnothing$. Comme ceci est le cas pour tout $n \geq 1$, l'application $\pi_\varnothing$ est bijective et $T_\varnothing$ est un anneau d'intersection complète (*loc. cit.*).

7. LE THÉORÈME 2 DANS LE CAS GÉNÉRAL

Les hypothèses et notations sont celles du th. 2. Choisissons un homomorphisme d'anneaux de $T_\varnothing$ dans l'anneau des entiers $\mathcal{O}$ d'une extension finie de $\mathbf{Z}_\ell$. Cela munit la $\mathcal{O}$-algèbre $T_{\varnothing,\mathcal{O}}$ d'une augmentation $\varepsilon_\varnothing : T_{\varnothing,\mathcal{O}} \to \mathcal{O}$. Par composition avec la surjection canonique $T_{\Sigma,\mathcal{O}} \to T_{\varnothing,\mathcal{O}}$, on en déduit une augmentation $\varepsilon_\Sigma : T_{\Sigma,\mathcal{O}} \to \mathcal{O}$ pour tout ensemble fini Σ de nombres premiers. Notons $\mathfrak{t}_\Sigma$ son noyau et $\mathfrak{r}_\Sigma$ l'image réciproque de $\mathfrak{t}_\Sigma$ par la surjection canonique $R_{\Sigma,\mathcal{O}} \to T_{\Sigma,\mathcal{O}}$. La $\mathcal{O}$-algèbre $R_{\Sigma,\mathcal{O}}$ est locale, noethérienne et complète, et la $\mathcal{O}$-algèbre $T_{\Sigma,\mathcal{O}}$ est libre de rang fini sur $\mathcal{O}$ et réduite. Notons a_Σ la longueur du $\mathcal{O}$-module $\mathfrak{r}_\Sigma/\mathfrak{r}_\Sigma^2$ et b_Σ celle du $\mathcal{O}$-module

$T_{\Sigma,\mathcal{O}}/(t_\Sigma + \mathrm{Annt}_\Sigma)$ (où l'annulateur de t_Σ est pris dans $T_{\Sigma,\mathcal{O}}$). Compte tenu de l'App. III, n° 3, prop. 2 et cor., et de la remarque du n° 5, les conditions suivantes sont équivalentes :

a) $\pi_\Sigma : R_\Sigma \to T_\Sigma$ est une bijection et T_Σ est un anneau d'intersection complète.

b) $\pi_{\Sigma,\mathcal{O}} : R_{\Sigma,\mathcal{O}} \to T_{\Sigma,\mathcal{O}}$ est une bijection et $T_{\Sigma,\mathcal{O}}$ est un anneau d'intersection complète.

c) On a $a_\Sigma \leq b_\Sigma$.

d) On a $a_\Sigma = b_\Sigma$.

Elles sont satisfaites pour $\Sigma = \varnothing$ (n° 6). On les démontre pour tout $\Sigma \subset \Sigma_1$ par récurrence sur le cardinal de Σ. Pour cela, il suffit de prouver que, si Σ est un sous-ensemble fini de Σ_1 et p un élément de $\Sigma_1 - \Sigma$, il existe un nombre c_p tel que l'on ait, en posant $\Sigma' = \Sigma \cup p$,

$$(*) \qquad a_{\Sigma'} \leq a_\Sigma + c_p \qquad\qquad b_{\Sigma'} \geq b_\Sigma + c_p.$$

En fait, on peut prendre pour c_p la longueur de $\mathcal{O}/\varepsilon_\Sigma(\gamma_p)$, où γ_p est un élément convenable de T_Σ (par exemple $\gamma_p = (p-1)(T_p^2 - (p+1)^2)$ si $p \neq \ell$).

Les premières des inégalités (*) sont démontrées dans [2'] en donnant des groupes t_Σ/t_Σ^2 une interprétation cohomologique analogue à celle donnée dans l'App. II, n° 2, remarque 2. Les secondes font l'objet de la prop. 3.16 de [2'] (énoncée sous des hypothèses plus restrictives que dans [2]). Des énoncés voisins, dans un cadre plus général, sont démontrés dans le chapitre 2 de [16].

Appendice I. REPRÉSENTATIONS D'UN GROUPE SUR UN ANNEAU LOCAL (d'après Carayol [1])

Soient A un anneau local commutatif, k son corps résiduel, G un groupe et ρ une représentation de G de degré n sur A (*i.e.* dans un A-module libre M_ρ de rang n). La *trace* de ρ est l'application $g \mapsto \mathrm{Tr}\,\rho(g)$ de G dans A. Pour toute A-algèbre A', on note $\rho_{(A')}$ la représentation déduite de ρ par extension des scalaires de A à A'. On appelle *représentation résiduelle de* ρ la représentation $\rho_{(k)}$.

PROPOSITION 1.— *Supposons la représentation résiduelle de ρ absolument irréductible.*

a) *Le commutant de ρ est réduit aux homothéties.*

b) *Toute représentation de G de degré n sur A, de même trace que ρ, est isomorphe à ρ.*

Soit $u : A[G] \to \mathrm{End}_A(M_\rho)$ l'application A-linéaire qui prolonge ρ. Comme la représentation $\rho_{(k)}$ est absolument irréductible, l'application $u_{(k)}$ est surjective (théorème de Jacobson). L'application u est donc surjective (lemme de Nakayama), d'où a). Pour l'assertion b), voir [1], th. 1.

COROLLAIRE.— *Soient u un homomorphisme local de A dans un anneau local commutatif A' et ρ' une représentation de G de degré n sur A'. Pour que ρ' soit isomorphe à $\rho_{(A')}$, il faut et il suffit que l'on ait $\mathrm{Tr}\rho' = u \circ \mathrm{Tr}\rho$.*

PROPOSITION 2.— *Supposons l'anneau local A hensélien. Soient A' un anneau commutatif contenant A et ρ' une représentation de degré n de G sur A' telle que :*

a) *la trace de ρ' prenne ses valeurs dans A ;*

b) *la réduction modulo $\mathfrak{m}_A$ de $\mathrm{Tr}\rho'$ soit la trace d'une représentation absolument irréductible ρ_0 de degré n de G sur k.*

Il existe alors une représentation ρ de G de degré n sur A de même trace que ρ'. Sa représentation résiduelle est isomorphe à ρ_0.

C'est une variante du th. 2 de [1]. Considérons les applications A-linéaires $u : A[G] \to \mathrm{End}_{A'}(M_{\rho'})$ et $u_0 : A[G] \to \mathrm{End}_k(M_{\rho_0})$ prolongeant ρ' et ρ_0. La seconde est surjective (théorème de Jacobson). Il existe donc un sous-ensemble S de G, de cardinal n^2, que ρ_0 applique sur une base de $\mathrm{End}_k(M_{\rho_0})$. La matrice $(\mathrm{Tr}\,\rho'(st))_{(s,t)\in S\times S}$ de $M_{n^2}(A)$ est inversible car sa réduction modulo $\mathfrak{m}_A$ l'est. Par suite, $(\rho'(s))_{s\in S}$ est une base de $\mathrm{End}_{A'}(M_{\rho'})$ sur A'. Soit B l'image de u ; c'est une A-algèbre. On a $\mathrm{Tr}(\rho'(gt)) \in A$ pour $g \in G$, $t \in S$, d'où, par les formules de Cramer, $\rho'(g) \in \sum_{s\in S} A\rho'(s)$ pour $g \in G$. Il en résulte que $(\rho'(s))_{s\in S}$ est une base de B sur A.

Soit $x \in \mathrm{Ker}\,u$. Pour $t \in S$, on a $\mathrm{Tr}\big(u(x)\rho'(t)\big) = 0$, d'où $\mathrm{Tr}\big(u_0(x)\rho_0(t)\big) = 0$ par réduction modulo $\mathfrak{m}_A$; on a par suite $u_0(x) = 0$. Il existe donc un homomorphisme de A-algèbres $B \to \mathrm{End}_k(M_{\rho_0})$ qui applique $\rho'(s)$ sur $\rho_0(s)$ pour tout $s \in S$; on en déduit que la k-algèbre $B \otimes_A k$ est isomorphe à $\mathrm{End}_k(M_{\rho_0})$. Comme l'anneau A est hensélien, B est, d'après un théorème d'Azumaya, isomorphe à l'algèbre des endomorphismes d'un A-module libre M de rang n. Identifions B à une telle algèbre. L'application $\rho : g \to \rho'(g)$ de G dans B est alors une représentation linéaire de G dans M. Par dualité de Morita, on sait que le $B \otimes_A A'$-module $M_{\rho'}$ est isomorphe à $M \otimes_A N$, où N est un A'-module. Puisque M et $M_{\rho'}$ sont libres de rang n sur A et A' respectivement, le A'-module N est projectif de rang 1. Il en résulte que l'on a $\mathrm{Tr}\,\rho(g) = \mathrm{Tr}\,\rho'(g)$ pour tout $g \in G$. La dernière assertion de la prop. 2 résulte du

cor. de la prop. 1.

Remarque. — On prendra garde que ρ' n'est pas nécessairement isomorphe à $\rho_{(A')}$. Il résulte de la démonstration qu'elle est isomorphe à $\rho \otimes_A 1_N$, où N est un A′-module projectif de rang 1 ; elle est donc isomorphe à $\rho_{(A')}$ lorsque l'anneau A′ est local (ou même semi-local).

Appendice II. DÉFORMATIONS DE REPRÉSENTATIONS GALOISIENNES

1. Le critère de représentabilité de Schlessinger

Soit k un corps fini de caractéristique p. Notons $\mathcal{A}_k$ la catégorie dont les objets sont les anneaux locaux noethériens complets (commutatifs) de corps résiduel k et dont les morphismes sont les homomorphismes d'anneaux induisant l'identité par passage aux corps résiduels. Tout objet de $\mathcal{A}_k$ est canoniquement muni d'une structure d'algèbre sur l'anneau des entiers de Witt $W(k)$.

Soit $\mathcal{F}$ un foncteur covariant de la catégorie $\mathcal{A}_k$ dans celle des ensembles. On dit que $\mathcal{F}$ est *représenté* par un couple (R, r), où R est un objet de $\mathcal{A}_k$ et r un élément de $\mathcal{F}(R)$ si, pour tout objet A de $\mathcal{A}_k$ et tout $a \in \mathcal{F}(A)$, il existe un unique morphisme $u : R \to A$ tel que $\mathcal{F}(u)$ applique r sur a. On dit que $\mathcal{F}$ est *représentable* s'il existe un couple (R, r) qui le représente ; ce couple est alors unique à isomorphisme unique près. Le critère de représentabilité suivant est un cas particulier d'un théorème de Schlessinger ([11]).

PROPOSITION 1.— *Pour que $\mathcal{F}$ soit représentable, il faut et il suffit qu'il possède les propriétés suivantes :*

a) *L'ensemble $\mathcal{F}(k)$ est réduit à un élément.*

b) *Si A, B, C sont des anneaux artiniens de corps résiduel k, $u : A \to C$ un morphisme et $v : B \to C$ un morphisme surjectif, l'application canonique de $\mathcal{F}(A \times_C B)$ dans $\mathcal{F}(A) \times_{\mathcal{F}(C)} \mathcal{F}(B)$ est bijective.* (Noter que sous les hypothèses faites, le produit fibré $A \times_C B$ est un anneau local artinien de corps résiduel k.)

c) *Soit A un objet de $\mathcal{A}_k$; l'application canonique $\mathcal{F}(A) \to \varprojlim \mathcal{F}(A/\mathfrak{m}_A^n)$ est bijective.*

d) *L'ensemble $\mathcal{F}(k[\varepsilon])$, où $k[\varepsilon]$ est l'algèbre des nombres duaux sur k, est fini.*

Remarques. — Supposons que $\mathcal{F}$ soit représenté par un couple (R, r). Alors :

1) L'ensemble $\mathcal{F}(k[\varepsilon])$ s'identifie au dual du k-espace vectoriel $\mathfrak{m}_R/(\mathfrak{m}_R^2 + pR)$.

2) Soient $\mathcal{F}'$ un sous-foncteur représentable de $\mathcal{F}$ et (R', r') un couple qui le représente. L'homomorphisme $u : R \to R'$ tel que $\mathcal{F}(u)(r) = r'$ est surjectif. En

effet, d'après 1), l'application $\mathfrak{m}_R/(\mathfrak{m}_R^2 + pR) \to \mathfrak{m}_{R'}/(\mathfrak{m}_{R'}^2 + pR')$ déduite de u est surjective, et donc aussi l'application $\mathfrak{m}_R/\mathfrak{m}_R^2 \to \mathfrak{m}_{R'}/\mathfrak{m}_{R'}^2$; comme les anneaux locaux R et R′ sont noethériens et complets et ont même corps résiduel, l'application u est surjective.

3) Si pour tout anneau artinien A de corps résiduel k et tout idéal $\mathfrak{a}$ de carré nul de A, l'application canonique $\mathcal{F}(A) \to \mathcal{F}(A/\mathfrak{a})$ est surjective, R est isomorphe à une algèbre de séries formelles en un nombre fini d'indéterminées à coefficients dans $W(k)$.

4) Soit k' une extension de degré fini de k. Si A est un objet de $\mathcal{A}_{k'}$, notons A_* l'anneau formé des $a \in A$ qui se réduisent modulo $\mathfrak{m}_A$ en un élément de k. C'est un objet de $\mathcal{A}_k$. Le foncteur $\mathcal{F}' : A \mapsto \mathcal{F}(A_*)$ de la catégorie $\mathcal{A}_{k'}$ dans celle des ensembles est représenté par $\big(R \otimes_{W(k)} W(k'), \mathcal{F}(u)(r)\big)$, où $u : R \to \big(R \otimes_{W(k)} W(k')\big)_*$ est le morphisme canonique.

2. Déformations universelles de représentations galoisiennes

Soient k un corps fini de caractéristique p, n un entier ≥ 1 et ρ_0 une représentation continue de $G_{\mathbf{Q}}$ de degré n sur k. Soit A un anneau local noethérien complet de corps résiduel k. Appelons *déformation de* ρ_0 *à* A une représentation continue ρ de $G_{\mathbf{Q}}$ dans un A-module M_ρ libre de rang n, dont la représentation résiduelle $\widetilde{\rho} = \rho \otimes 1_k$ est isomorphe à ρ_0.

PROPOSITION 2 (Mazur [9] et Ramakrishna [10]).— *Supposons* ρ_0 *absolument irréductible. Soit* $\mathcal{C}$ *une catégorie de* $G_{\mathbf{Q}}$*-modules finis, stable par produits finis, sous-objets et quotients, et dont* $\mathbf{Z}/p\mathbf{Z}$*, muni de l'action triviale de* $G_{\mathbf{Q}}$*, est un objet. Soit* S *un ensemble fini de nombres premiers contenant ceux en lesquels* ρ_0 *est ramifiée. Pour tout anneau local noethérien complet* A *de corps résiduel* k*, notons* $\mathcal{F}(A)$ *l'ensemble des classes d'isomorphisme de déformations* ρ *de* ρ_0 *à* A*, non ramifiées en dehors de* S *et telles que, pour tout idéal* $\mathfrak{a}$ *d'indice fini de* A*, le* $G_{\mathbf{Q}}$*-module* $M_\rho/\mathfrak{a}M_\rho$ *soit un objet de* $\mathcal{C}$*. Le foncteur* $\mathcal{F}$ *ainsi défini, de la catégorie* $\mathcal{A}_k$ (cf. n° 1) *dans celle des ensembles, est représentable.*

Il suffit de vérifier que les conditions a), b), c), d) du critère de Schlessinger sont satisfaites. Pour a) et c), c'est facile. Pour b), cela résulte de ce que le commutant de toute déformation de ρ_0 est réduit aux homothéties (App. I, prop. 1). Enfin d) résulte de ce que $\mathbf{Q}$ ne possède dans $\overline{\mathbf{Q}}$ qu'un nombre fini d'extensions de degré donné non ramifiées en dehors de S.

Remarques. — 1) Soit $\chi : G_{\mathbf{Q}} \to W(k)^\times$ un relèvement de $\det \rho_0$ à l'anneau des vecteurs de Witt de k. La prop. 1 reste valable si l'on se restreint aux déformations

de ρ_0 de déterminant χ.

2) Soit V l'espace de la représentation ρ_0. Notons $\mathfrak{gl}(V)$ le k-espace vectoriel des endomorphismes de V, sur lequel $G_{\mathbf{Q}}$ opère par la représentation adjointe $(g, M) \mapsto \rho_0(g) M \rho_0(g^{-1})$. Il existe une bijection canonique ι de $H^1\big(G_{\mathbf{Q}}, \mathfrak{gl}(V)\big)$ sur l'ensemble des classes d'isomorphisme de déformations de ρ_0 à la k-algèbre des nombres duaux $k[\varepsilon]$: à la classe de cohomologie d'un 1-cocycle $a : G_{\mathbf{Q}} \mapsto \mathfrak{gl}(V)$ correspond la classe d'isomorphisme de la déformation obtenue en faisant opérer $G_{\mathbf{Q}}$ sur $V \otimes_k k[\varepsilon]$ par $\sigma \mapsto \big(1 + a(\sigma) \otimes \varepsilon\big) \circ \big(\rho_0(\sigma) \otimes 1\big)$.

Sous les hypothèses de la prop. 2, notons $H^1_{\mathcal{C}}\big(G_{\mathbf{Q}}, \mathfrak{gl}(V)\big)$ l'image réciproque de $\mathcal{F}(k[\varepsilon])$ par ι. C'est un sous-k-espace vectoriel de $H^1\big(G_{\mathbf{Q}}, \mathfrak{gl}(V)\big)$. Si (R, r) représente le foncteur $\mathcal{F}$, la bijection de $H^1_{\mathcal{C}}\big(G_{\mathbf{Q}}, \mathfrak{gl}(V)\big)$ sur le dual du k-espace vectoriel $\mathfrak{m}_R/\mathfrak{m}_R^2 + pR$, déduite de ι modulo l'identification de la remarque 1 du n° 1, est k-linéaire. Par suite, R est isomorphe à un quotient de $W(k)[[X_1, \ldots, X_n]]$, où $n = \dim_k H^1_{\mathcal{C}}\big(G_{\mathbf{Q}}, \mathfrak{gl}(V)\big)$.

Tout ce qui précède reste valable lorsqu'on se restreint aux déformations de déterminant fixé (cf. remarque 1), à condition de remplacer $\mathfrak{gl}(V)$ par l'espace vectoriel $\mathfrak{sl}(V)$ des endomorphismes de V de trace nulle.

Appendice III. ANNEAUX D'INTERSECTION COMPLÈTE

1. Définition

Un anneau local noethérien complet (commutatif) Λ est isomorphe au quotient d'un anneau local noethérien régulier et complet A par un idéal $\mathfrak{a}$. On dit que Λ est un *anneau d'intersection complète* si $\mathfrak{a}$ est engendré par une suite régulière d'éléments de A, *i.e.* une suite finie $(a_1, \ldots, a_n)$ telle que l'homothétie de rapport a_i dans $A/(a_1A + \ldots + a_{i-1}A)$ soit injective pour $1 \leq i \leq n$; cette définition ne dépend pas du couple $(A, \mathfrak{a})$ choisi ([8], th. 21.2).

2. Premier critère d'isomorphisme

Soient $\mathcal{O}$ un anneau de valuation discrète complet à corps résiduel fini et $\pi : R \to T$ un homomorphisme de $\mathcal{O}$-algèbres. Soit r un entier ≥ 0. Posons $A = \mathcal{O}[[S_1, \ldots, S_r]]$. Considérons R et T comme des A-algèbres en faisant opérer les S_i par 0. Soit $\mathfrak{a}$ un idéal de A contenu dans $\sum AS_i$. Appellons $\mathfrak{a}$-structure pour π la donnée de deux A-algèbres R′ et T′ et d'un diagramme commutatif

d'homomorphismes surjectifs de A-algèbres

$$\begin{array}{ccc} R' & \xrightarrow{\pi'} & T' \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ R & \xrightarrow{\pi} & T \end{array}$$

satisfaisant les conditions suivantes :

a) en tant que $\mathcal{O}$-algèbre, R' est isomorphe à un quotient de $\mathcal{O}[[X_1, \ldots, X_r]]$;

b) pour tout idéal $\mathfrak{b}$ de A contenant $\mathfrak{a}$, $T'/\mathfrak{b}T'$ est une $A/\mathfrak{b}$-algèbre fidèle ;

c) le noyau de α est $\sum S_i R'$ et celui de β est $\sum S_i T'$.

Notons que lorsqu'une telle structure existe, R et T sont des anneaux locaux, noethériens et complets.

PROPOSITION 1.— *Supposons que* T *soit libre de rang fini sur* $\mathcal{O}$. *Soit* $(\mathfrak{a}_n)_{n\geq 0}$ *une suite décroissante d'idéaux de* A, *d'intersection nulle. S'il existe pour tout* $n \geq 0$ *une* $\mathfrak{a}_n$*-structure pour* π, T *est un anneau d'intersection complète et* π *est bijectif.*

Pour la démonstration, on pourra consulter [2'] (th. 3.20 prouvé en 5.10).

3. Deuxième critère d'isomorphisme

Soient $\mathcal{O}$ un anneau de valuation discrète complet et T une $\mathcal{O}$-algèbre locale, libre de rang fini sur $\mathcal{O}$, munie d'une augmentation, *i.e.* d'un homomorphisme de $\mathcal{O}$-algèbres $\varepsilon : T \to \mathcal{O}$. Posons $\mathfrak{t} = \operatorname{Ker}\varepsilon$ et supposons que $\mathfrak{t}/\mathfrak{t}^2$ soit de longueur finie sur $\mathcal{O}$ (ce qui signifie que $V(\mathfrak{t})$ est une composante irréductible de multiplicité 1 de Spec T) ; cette condition est satisfaite par exemple lorsque l'anneau T est réduit.

PROPOSITION 2.— *La longueur sur* $\mathcal{O}$ *de* $T/(\mathfrak{t} + \operatorname{Ann}_T \mathfrak{t})$ *est inférieure à celle de* $\mathfrak{t}/\mathfrak{t}^2$, *et l'on a égalité si et seulement si* T *est un anneau d'intersection complète.*

Wiles démontre cette proposition dans [16] en supposant que l'anneau T est de Gorenstein. Cette hypothèse est superflue, comme le remarque Lenstra ([7], formule (6) et cor. 10), auquel nous renvoyons pour la démonstration.

COROLLAIRE.— *Soit* R *une* $\mathcal{O}$*-algèbre locale noethérienne et complète et soit* $\pi : R \to T$ *un homomorphisme surjectif de* $\mathcal{O}$*-algèbres. Posons* $\mathfrak{r} = \pi^{-1}(\mathfrak{t})$. *Si la longueur sur* $\mathcal{O}$ *de* $\mathfrak{r}/\mathfrak{r}^2$ *est inférieure à celle de* $T/(\mathfrak{t} + \operatorname{Ann}_T \mathfrak{t})$, π *est bijectif et* T *est un anneau d'intersection complète.*

L'application $u : \mathfrak{r}/\mathfrak{r}^2 \to \mathfrak{t}/\mathfrak{t}^2$ déduite de π est surjective. La longueur de $\mathfrak{t}/\mathfrak{t}^2$ est donc inférieure à celle de $\mathfrak{r}/\mathfrak{r}^2$. D'après la prop. 2, ces longueurs sont égales, *i.e.* u est bijective, et l'anneau T est d'intersection complète. Choisissons des relèvements $r_1, \ldots, r_n$ dans $\mathfrak{r}$ de générateurs du $\mathcal{O}$-module $\mathfrak{r}/\mathfrak{r}^2$. L'homomorphisme de $\mathcal{O}$-algèbres $\psi : \mathcal{O}[[X_1, \ldots, X_n]] \to R$ qui applique X_i sur r_i est surjectif. Comme T est un anneau d'intersection complète de dimension 1, $\mathrm{Ker}(\pi \circ \psi)$ est engendré par une suite régulière $(f_1, \ldots, f_n)$ d'éléments de $\mathcal{O}[[X_1, \ldots, X_n]]$. Ces éléments sont sans terme constant. Soient $f_i^{(1)} = \sum a_{ij} X_j$ leurs composantes homogènes de degré 1. Le $\mathcal{O}$-module $\mathfrak{t}/\mathfrak{t}^2$ s'identifie à $\sum \mathcal{O}X_j / \sum \mathcal{O} f_i^{(1)}$; comme il est de longueur finie, on a $\det(a_{ij}) \neq 0$. On a $\pi(\sum a_{ij} r_j) \in \mathfrak{t}^2$, d'où $\sum a_{ij} r_j \in \mathfrak{r}^2$ puisque l'application u est injective. Il existe donc des éléments $g_i \in \mathcal{O}[[X_1, \ldots, X_n]]$, sans terme constant et de mêmes composantes homogènes de degré 1 que les f_i, tels que $\psi(g_i) = 0$. Ils appartiennent au noyau de $\pi \circ \psi$, donc s'écrivent $\sum h_{il} f_l$, avec les h_{il} dans $\mathcal{O}[[X_1, \ldots, X_n]]$. En comparant les composantes homogènes de degré 1, on constate que l'on a $a_{ij} = \sum h_{il}(0) a_{lj}$ quels que soient i et j. Cela implique, puisque $\det(a_{ij}) \neq 0$, que $\big(h_{ij}(0)\big)$ est la matrice unité et par suite que la matrice (h_{ij}) est inversible. Ainsi les f_i appartiennent au noyau de ψ, d'où $\mathrm{Ker}(\pi \circ \psi) = \mathrm{Ker}\, \psi$; cela prouve que l'homomorphisme π est injectif.

Appendice IV. GROUPES DE SELMER

Soient K un corps de nombres, $\overline{K}$ une clôture algébrique de K, et M un groupe abélien fini sur lequel $G = \mathrm{Gal}(\overline{K}/K)$ opère continûment. Notons M^* le G-module $\mathrm{Hom}(M, \overline{K}^\times)$.

Choisissons au-dessus de chaque place v de K une place de $\overline{K}$, et notons D_v son groupe de décomposition. Le groupe (de cohomologie continue) $H^1(D_v, M)$ est fini. On obtient, en composant le cup-produit et le plongement canonique de $H^2(D_v, \overline{K}^\times)$ dans $\mathbf{Q}/\mathbf{Z}$, une forme $\mathbf{Z}$-bilinéaire inversible (dualité de Tate locale)

$$H^1(D_v, M) \times H^1(D_v, M^*) \to \mathbf{Q}/\mathbf{Z}.$$

Si v est une place finie de K, on note I_v le sous-groupe d'inertie de D_v et $H^1_{nr}(D_v, M)$ le noyau de l'application de restriction $H^1(D_v, M) \to H^1(I_v, M)$; l'ordre de $H^1_{nr}(D_v, M)$ est égal à celui de $H^0(D_v, M)$. Lorsque la caractéristique résiduelle de v ne divise pas l'ordre de M, l'orthogonal (pour la dualité de Tate locale) de $H^1_{nr}(D_v, M)$ est $H^1_{nr}(D_v, M^*)$.

Les images x_v d'un élément $x \in H^1(G, M)$ par les applications de restriction $H^1(G, M) \to H^1(D_v, M)$ appartiennent à $H^1_{nr}(D_v, M)$ pour presque toute place finie v de K. (Pour tout cela, voir [12], ch. II, §6.)

Supposons donné, pour chaque place v de K, un sous-groupe L_v de $H^1(D_v, M)$, égal pour presque toute place finie v à $H^1_{nr}(D_v, M)$. L'ensemble des éléments $x \in H^1(G, M)$ tels que $x_v \in L_v$ pour tout v s'appelle le *groupe de Selmer associé à la famille* $\mathcal{L} = (L_v)$; notons-le $H^1_{\mathcal{L}}(G, M)$. Soit $\mathcal{L}^\perp$ la famille $(L_v^\perp)$, où $L_v^\perp$ est l'orthogonal de L_v dans $H^1(D_v, M^*)$. Les groupes de Selmer $H^1_{\mathcal{L}}(G, M)$ et $H^1_{\mathcal{L}^\perp}(G, M^*)$ sont finis et leurs ordres sont liés par relation

$$\frac{|H^1_{\mathcal{L}}(G, M)|}{|H^1_{\mathcal{L}^\perp}(G, M^*)|} = \frac{|H^0(G, M)|}{|H^0(G, M^*)|} \prod_v \frac{|L_v|}{|H^0(D_v, M)|}. \tag{1}$$

Cette formule se déduit des théorèmes de Poitou-Tate : on pourra consulter [2], th. 2.14 où est traité le cas $K = \mathbf{Q}$, qui nous suffira ; le cas général est similaire.

Remarque. — Soit $\mathcal{L}' = (L'_v)$ une autre famille de sous-groupes des $H^1(D_v, M)$, telle que L_v soit contenu dans L'_v pour tout v et égal à L'_v pour presque tout v. On déduit de la suite exacte de Poitou-Tate une suite exacte

$$0 \to H^1_{\mathcal{L}}(G, M) \xrightarrow{\alpha} H^1_{\mathcal{L}'}(G, M) \xrightarrow{\beta} \prod_v L'_v/L_v \xrightarrow{\gamma} H^1_{\mathcal{L}^\perp}(G, M^*)^\vee \xrightarrow{\delta} H^1_{\mathcal{L}'^\perp}(G, M^*)^\vee \to 0$$

où α est l'injection canonique, β se déduit des applications de restriction, $X^\vee$ désigne pour tout groupe fini X le groupe $\mathrm{Hom}(X, \mathbf{Q}/\mathbf{Z})$ et δ, γ se déduisent des applications analogues à α et β par dualité. Cette suite exacte montre que la validité de la formule (1) ne dépend pas du choix de $\mathcal{L}$.

BIBLIOGRAPHIE

[S] J-P. SERRE, *Travaux de Wiles (et Taylor, ...), partie I*, Séminaire Bourbaki 1994/95, exposé 803.

[1] H. CARAYOL, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, Contemporary Math. **165** (1994), 213-237.

[2] H. DARMON, F. DIAMOND et R. TAYLOR, *Fermat's Last Theorem*, Current Developments in Math. 1995, International Press, Cambridge MA.

[2'] H. DARMON, F. DIAMOND et R. TAYLOR, *Fermat's Last Theorem*, Current Developments in Math., International Press, Cambridge MA, version révisée et complétée, à paraître.

[3] P. DELIGNE et J-P. SERRE, *Formes modulaires de poids* 1, Ann. Sci. E.N.S. **7** (1974), 507-530.

[4] F. DIAMOND, *On deformation rings and Hecke rings*, Ann. of Math., à paraître.

[5] F. DIAMOND, *The refined conjecture of Serre*, Conference on Elliptic Curves, Hong-Kong 1993, International Press, Cambridge MA (1995), 22-37.

[6] J-M. FONTAINE et B. MAZUR, *Geometric Galois representations*, Conference on Elliptic Curves, Hong-Kong 1993, International Press, Cambridge MA (1995), 41-78.

[7] H. W. LENSTRA Jr, *Complete intersections and Gorenstein rings*, Conference on Elliptic Curves, Hong-Kong 1993, International Press, Cambridge MA (1995), 99-109.

[8] H. MATSUMURA, *Commutative ring theory*, Cambridge studies in advanced mathematics, Cambridge Univ. Press, 1986.

[9] B. MAZUR, *Deforming Galois representations*, in : Galois groups over $\mathbf{Q}$, MSRI Publ. **16**, (1989), 385-437.

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

[11] M. SCHLESSINGER, *Functors of Artin rings*, Trans. A.M.S. **130**, (1968), 208–222.

[12] J-P. SERRE, *Cohomologie galoisienne*, Lecture Notes in Math. **5**, Springer-Verlag. 1973.

[13] J-P. SERRE, *Formes modulaires et fonctions zêta p-adiques*, Lect. Notes in Math **350**, 1973, Springer-Verlag, 191-268.

[14] J-P. SERRE, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179-230.

[15] R. TAYLOR et A. WILES, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553-572.

[16] A. WILES, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443-551.

Joseph OESTERLÉ
Institut Henri Poincaré
11, rue Pierre et Marie Curie
F-75005 PARIS