L'objet de ce cours est une introduction à la théorie des déformations de représentations galoisiennes p-adiques : représentations locales et globables, déformations, déformations cadrées, représentabilité, espaces tangents, calculs via la cohomologie galoisienne...
La théorie des déformations permet d'étudier les relèvements d'objets de la caractéristique $p > 0$ à la caractéristique zéro et d'en déterminer les propriétés universelles.

1 Anneau des vecteurs de Witt

Soit p un nombre premier. Il s'agit de généraliser la construction des entiers p-adiques

$$\mathbf{Z}_p = \lim_{\leftarrow} \mathbf{Z}/p^n\mathbf{Z}$$

notamment pour relever les éléments d'un corps fini $\mathbf{F}_q$.

1.1 Rappels d'algèbre commutative

Un *foncteur* F de la catégorie $\mathcal{C}$ dans la catégorie $\mathcal{C}'$ est une loi qui à chaque objet A de $\mathcal{C}$ associe un objet $F(A)$ de $\mathcal{C}'$ et à chaque morphisme $f : A \longrightarrow B$ de $\mathcal{C}$ associe un morphisme $F(f) : F(A) \longrightarrow F(B)$ de $\mathcal{C}'$ de sorte que :
- pour tout objet A de $\mathcal{C}$, $F(\mathrm{Id}_A) = \mathrm{Id}_{F(A)}$,
- pour tous morphismes $f : A \longrightarrow B$ et $g : B \longrightarrow C$: $F(g \circ f) = F(g) \circ F(f)$.

Limite projective.
Soit I un ensemble ordonné. Soit $(A_i)_i \in I$ un système projectif d'anneaux : pour tous $i, j, k \in I$ avec $i \leq j \leq k$, on a des morphismes d'anneaux $\varphi_{i,j} : A_j \to A_i$, tels que $\varphi_{i,i} = Id$, $\varphi_{i,j} \circ \varphi_{j,k} = \varphi_{i,k}$. La *limite projective* de $(A_i)_i \in I$ est l'anneau A

$$A = \{(g_i) \in \Pi A_i, \forall i \leq j, g_i = \varphi_{i,j}(g_j)\}.$$

Il peut être défini par la propriété universelle suivante : si Y anneau avec morphismes compatibles dans les A_i, alors il existe un morphisme de $Y \to A$ qui induit tout.

Exemple 1.1.1 *Soit p un nombre premier pour $i \leq j$, la réduction modulo p^i définit un morphisme d'anneaux $\mathbf{Z}/p^j\mathbf{Z} \to \mathbf{Z}/p^i\mathbf{Z}$ et fait de $(\mathbf{Z}/p^n\mathbf{Z})_{n\in\mathbf{N}^*}$ un système projectif. L'anneau des entiers p-adiques $\mathbf{Z}_p$ est la limite projective des $(\mathbf{Z}/p^n\mathbf{Z})_{n\in\mathbf{Z}^*}$.*

De la même façon, on définit les notions de limite projective de groupes ou de modules et de limite inductive.

Groupe profini.(voir §.1 [Se2]).
Nous appelons *groupe profini* un groupe topologique obtenu comme limite projective de groupes finis (munis chacun de la topologie discrète). Un tel groupe est compact et totalement discontinu, i.e. il n'existe pas de partie connexe non triviale (et réciproquement, car alors G possède une base de voisinages de 1 formé par les sous-groupes ouverts distingués U et $G = \mathrm{proj}\lim G/U$). Les groupes profinis forment une catégorie, les morphismes étant les morphismes continus de groupes.
Un pro-p-groupe est une limite projective de p-groupes finis. Un p-Sylow d'un groupe profini G est un sous-pro-p-groupe fermé maximal pour l'inclusion des pro-p-sous-groupes de G.

Exemple 1.1.2 *Soit E/F une extension galoisienne de corps. Le groupe de Galois* $\mathrm{Gal}(E/F)$ *de cette extension, est un groupe profini, comme limite projective des groupes de Galois* $\mathrm{Gal}(E_i/F)$ *des extensions galoisiennes finies E_i/F contenues dans E/F.*

Exemple 1.1.3 *Le groupe $\mathbf{Z}_p$ est un pro-p-groupe.*

Exemple 1.1.4 *Si M est un groupe discret abelien de torsion, son dual $M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$ muni de la topologie de la convergence simple est un groupe profini commutatif (en effet, M est la limite inductive de ses sous-groupes finis N donc M^* est la limite projective des groupes finis N^*). Nous obtenons ainsi une anti-équivalence de catégories, dite dualité de Pontryagin, entre la catégorie des groupes abeliens discrets de torsion et la catégorie des groupes profinis commutatifs.*
De même, le dual d'un groupe abelien profini G est le groupe discret de torsion constitué des homomorphismes continus $\mathrm{Hom}_{\mathrm{cont}}(G, \mathbf{Q}/\mathbf{Z})$.

Exemple 1.1.5 *Soit K un corps p-adique (extension finie de $\mathbf{Q}_p$). Soit $\overline{K}$ une cloture algébrique de K, K_{nr} son extension maximale non ramifiée de K dans $\overline{K}$ et K^{mr} l'extension maximale modérément ramifiée de K_{nr}. Soit $U = \mathrm{Gal}(\overline{K}/K_{\mathrm{nr}})$ le groupe d'inertie. La théorie des groupes de ramification établit que $U_p = \mathrm{Gal}(\overline{K}/K^{\mathrm{mr}})$ est l'unique p-Sylow de U.*

Anneaux artiniens, noetheriens.
Sauf mention explicite du contraire, tous les anneaux considérés dans ce cours sont commutatifs et unitaires.
Un anneau *artinien* est un anneau dans lequel toute suite décroissante d'idéaux est stationnaire.
Un anneau *noetherien* est un anneau dans lequel toute suite croissante d'idéaux est stationnaire. En particulier, les anneaux artiniens sont noethériens (voir exercice).

Exemple 1.1.6 *Soit k un corps. Les anneaux suivants sont artiniens : k, $k[X]/(X^2)$, $k[X]/(X^n)$, $\mathbf{Z}_p[X,Y]/(p^n, X^iY^{n-i}, 0 \leq i \leq n)$. Les quotients de $\mathbf{Z}_p[[X_1, \ldots, X_n]]$ sont noetheriens.*

Remarque 1.1.7 *Un anneau (commutatif unitaire) est artinien si et seulement si il est noetherien et tous ses idéaux premiers sont maximaux (voir exercice).*

Complétion d'un anneau par rapport à un idéal.(voir §.3 [Bo])
Soit A un anneau, I un idéal de A. On appelle *topologie I-adique*, l'unique topologie sur A compatible avec sa structure d'anneau dont un système de voisinage de 0 soit l'ensemble I^ℓ, $\ell \geq 0$. La topologie obtenue est séparée si $\cap I^\ell = \{0\}$. Elle est complète si pour toute famille $(a_\ell \in I_\ell)_{\ell \in \mathbf{N}}$, il existe $a \in A$ tel que pour tout $k \in \mathbf{N}$, $a - \sum_{\ell<k} a_\ell \in I^k$. Le séparé complèté de A muni de la topologie I-adique est $\hat{A} = \operatorname{proj\,lim} A/I^\ell$.

1.2 Définition des vecteurs de Witt

Soit A un anneau (commutatif et unitaire). Notons $W(A)$ l'ensemble $A^{\mathbf{N}}$ des suites infinies à valeurs dans A. Les éléments de $W(A)$ sont dits *vecteurs de Witt* à coefficients dans A. A chaque morphisme d'anneaux $f : A \to B$, nous associons l'application d'ensembles $W(f) : W(A) \to W(B)$, $(a_k)_{k\in\mathbf{N}} \mapsto (f(a_k))_{k\in\mathbf{N}}$. Ainsi W définit un foncteur de la catégorie des anneaux commutatifs dans la catégorie des ensembles.
A chaque vecteur $x = (x_k)_k$ de $W(A)$, nous associons la suite $x^* = (x^{(k)})_k$ de $A^{\mathbf{N}}$ définie par :

$$\forall k \geq 0, x^{(k)} = x_0^{p^k} + px_1^{p^{k-1}} + \cdots + p^k x_k.$$

Les coefficients $x^{(k)}, k \geq 0$ de la suite x^* sont dits *composantes fantômes* de x.

Nous définissons l'application

$$g_A : W(A) \to A^{\mathbf{N}}, \quad x \mapsto x^* \quad (x_k)_k \mapsto (x^{(k)})_k$$

Proposition 1.2.1 *Si l'anneau A contient le corps $\mathbf{Q}$ des nombres rationnels, l'application g_A est bijective.*

Preuve : On a $x_0 = x^{(0)}$ et $x_1 = (x^{(1)} - x^{(0)^p})/p$. En suite pour $k \geq 1$, nous avons :

$$x_k = \frac{1}{p^k}\Big(x^{(k)} - \sum_{0\leq d\leq k-1} p^d x_d^{p^{n-d}}\Big).$$

Ainsi chaque composante x_k s'écrit comme combinaison linéaire des $x^{(d)}$ avec $0 \leq d \leq k$ à coefficients rationnels. Donc g_A est bijective. ∎

Si A contient $\mathbf{Q}$, l'application g_A est bijective et nous posons

$$\forall a, b \in W(A) \;\; a\hat{+}b = g_A^{-1}(a^* + b^*) \text{ et } a\hat{\times}b = g_A^{-1}(a^* \times b^*).$$

Plus précisément, la somme et le produit sont définis comme les vecteurs de Witt dont les composantes fantômes sont données par :

$$\forall k \geq 0, (a\hat{+}b)^{(k)} = a^{(k)} + b^{(k)}, \;\; (a\hat{\times}b)^{(k)} = a^{(k)} \cdot b^{(k)}.$$

C'est en particulier le cas pour $R_{\mathbf{Q}} = \mathbf{Q}[X_0, X_1, \dots, Y_0, Y_1, \dots]$. Nous allons montrer que l'addition et la multiplication définies sur $W(R_{\mathbf{Q}})$ n'utilisent que des coefficients entiers : soit $X = (X_0, X_1, \dots)$ et $Y = (Y_0, Y_1, \dots)$ deux vecteurs de Witt particuliers dans $W(R_{\mathbf{Q}})$, notons

$$(X\hat{+}Y)_k = S_k(X_0, X_1, \dots, Y_0, Y_1, \dots), \text{ et } (X\hat{\times}Y)_k = P_k(X_0, X_1, \dots, Y_0, Y_1, \dots)$$

les composantes des vecteurs de Witt $X\hat{+}Y$ et $X\hat{*}Y$.

Remarque 1.2.2 *On peut définir une version généralisée des vecteurs de Witt ([?] § VI) $W'(A) = A^{\mathbf{N}}$ en associant à $z = (z_k)_k \in W'(A)$ la suite $z_* = (z_{(k)})_k$ de $A^{\mathbf{N}}$, définie par les composantes "fantômes généralisées"*

$$\forall k \geq 0, z_{(k)} = \sum_{d|k} d z_d^{k/d}$$

et donc une addition $\hat{\hat{+}}$ et une multiplication $\hat{\hat{\times}}$ sur $W'(S_{\mathbf{Q}} = \mathbf{Q}[Z_0, Z_1, \dots, Z'_0, Z'_1, \dots])$. La projection

$$W'(S_{\mathbf{Q}}) \to W(S_{\mathbf{Q}}) = W(R_{\mathbf{Q}}), Z_\ell \mapsto \begin{cases} X_k & si\ \ell = p^k \\ 0 & sinon \end{cases}$$

est un morphisme d'anneaux.

Proposition 1.2.3 *Pour tout $k \geq 0$, $S_k, P_k \in \mathbf{Z}[X_0, \dots, X_k, Y_0, \dots, Y_k]$.*

Preuve : Considérons la série formelle

$$f_{\underline{Z}}(t) = \Pi_{k \geq 0}(1 - Z_k t^k)$$

où $(Z_\ell)_{\ell^i n \mathbf{N}}$ est un ensemble d'indéterminées. Nous avons

$$-t f'_{\underline{Z}}(t)/f_{\underline{Z}}(t) = \sum_{k \geq 0} g_k(\underline{Z}) t^k \text{ avec } g_k(\underline{Z}) = \sum_{d|k} d Z_d^{k/d}.$$

Notons $\underline{Z'} = (Z'_\ell)_{\ell \in \mathbf{N}}$ un autre ensemble d'indéterminées et $\underline{Z''} = (Z''_\ell)_{\ell \in \mathbf{N}}$ défini par

$$\underline{Z''} = (\underline{Z} \hat{+} \underline{Z'}).$$

En comparant les dérivées et les valeurs prises en 0 des séries $f_Z(t) f_{Z'}(t)$ et $f_{Z''}(t)$, nous montrons que

$$f_Z(t) f_{Z'}(t) = f_{Z''}(t)$$

En identifiant les coefficients des t^{p^k}, et en appliquant la projection de $W'(S_{\mathbf{Q}}) \to W(R_{\mathbf{Q}})$, on obtient $S_k \in \mathbf{Z}[X_0, \dots, X_k, Y_0, \dots Y_k]$. On obtient de façon analogue le résultat annoncé pour P_k. ∎

Nous allons définir une addition et une multiplication sur $a, b \in W(A)$ pour A anneau commutatif. Pour cela, posons $R_{\mathbf{Z}} = \mathbf{Z}[X_0, X_1, \dots, Y_0, Y_1, \dots]$ et introduisons l'unique homomorphisme d'anneaux

$$\phi_{ab} : R_{\mathbf{Z}} \to A, X_k \mapsto a_k, Y_k \mapsto b_k, \forall k \in \mathbf{N}.$$

Définition 1.2.4 *Soit A un anneau. Pour tous $a, b \in W(A)$, notons*

$$a \hat{+} b = W(\phi_{ab})(X \hat{+} Y),\ a \hat{\times} b = W(\phi_{ab})(X \hat{\times} Y)$$

Exemple 1.2.5

$$(a + b) = (a_0 + b_0, a_1 + b_1 - \sum_{k=1}^{p-1} 1/p \binom{p}{k} a_0^k b_0^{p-k}, \cdots)$$

$$(ab) = (a_0 b_0, a_1 b_0^p + a_0^p b_1 + p a_1 b_1, \dots)$$

Nous avons la propriété fonctorielle

Proposition 1.2.6 *Soit A un anneau. Pour tous vecteurs de Witt a, b dans $W(A)$, les relations suivantes sont satisfaites :*

$$g_A(a \hat{+} b) = g_A(a) + g_A(b),\ g_A(a \hat{\times} b) = g_A(a) g_A(b).$$

En d'autres termes, pour tous $a, b \in W(A)$, il existe un unique vecteur de Witt dans $W(A)$ noté $a \hat{+} b$ (resp. $a \hat{\times} b$) dont les composantes fantômes sont $a^{(k)} + b^{(k)}$ (resp. $a^{(k)} b^{(k)}$).

PREUVE : Nous avons le diagramme commutatif

$$\begin{array}{ccc} W(A_{\mathbf{Z}}) & \stackrel{W(\phi_{a,b})}{\longrightarrow} & W(A) \\ \downarrow g_{A_{\mathbf{Z}}} & & \downarrow g_A \\ A_{\mathbf{Z}}^{\mathbf{N}} & \stackrel{\phi_{a,b}^{\mathbf{N}}}{\longrightarrow} & A^{\mathbf{N}} \end{array}$$

Or pour tous $X, Y \in W(A_{\mathbf{Z}})$, il existe un unique vecteur de Witt dans $W(A_{\mathbf{Z}})$ noté $X\hat{+}Y$ dont les composantes fantômes sont $X^{(k)} + Y^{(k)}$ et le morphisme $\phi_{a,b}^{\mathbf{N}}$ est additif. Ainsi

$$\begin{array}{rcc} g_A(a\hat{+}b) & = & g_A \circ W(\phi_{ab})(X\hat{+}Y) \\ & = & \phi_{a,b}^{\mathbf{N}} \circ g_{A_{\mathbf{Z}}}(X\hat{+}Y) \\ & = & \phi_{a,b}^{\mathbf{N}}(g_{A_{\mathbf{Z}}}(X) + g_{A_{\mathbf{Z}}}(Y)) \\ & = & \phi_{a,b}^{\mathbf{N}} \circ g_{A_{\mathbf{Z}}}(X) + \phi_{a,b}^{\mathbf{N}} \circ g_{A_{\mathbf{Z}}}(Y) \\ & = & g_A(a) + g_A(b) \end{array}$$

De même, nous montrons $g_A(a\hat{\times}b) = g_A(a) \cdot g_A(b)$. ∎

Remarque 1.2.7 *La proposition 1.2.6 ne suffit pas, en général à définir des lois d'addidtion et de multiplication sur $W(A)$. Ce sera l'objet du théorème 1.2.9. Par exemple si p n'est pas inversible dans A, l'application g_A n'est plus bijective car deux vecteurs de Witt distincts peuvent avoir les mêmes composantes fantômes. Si A contient $\mathbf{Q}$, g_A définit un isomorphisme d'anneaux. Dans le cas général, $A^{\mathbf{N}}$ et $W(A)$ se correspondent uniquement en tant qu'ensembles. Par exemple, si l'anneau A est de caractéristique $p > 0$, $A^{\mathbf{N}}$ aussi, mais $W(A)$ est de caractéristique 0. Ces anneaux ne peuvent pas être isomorphes.*

Proposition 1.2.8 *Soit A, B deux anneaux. Si $f : A \to B$ est un morphisme d'anneaux, alors l'application induite :*

$$W(f) : W(A) \to W(B)$$

est additive et multiplicative pour les lois $\hat{+}$ et $\hat{\times}$.

PREUVE :

$$W(f)(a\hat{+}b) = W(f \circ \phi_{ab})(X\hat{+}Y) = W(\phi_{W(f)(a),W(f)(b)})(X\hat{+}Y)$$

$$= W(\phi_{W(f)(a),W(f)(b)})(X)\hat{+}W(\phi_{W(f)(a),W(f)(b)})(Y) = W(f)(a) + W(f)(b)$$

de même pour le produit. ∎

Théorème 1.2.9 *Soit A un anneau. Notons 0,1 ses éléments neutres pour l'addition et la multiplication. Alors l'ensemble $W(A)$ muni de $\hat{+}$ et $\hat{\times}$ est un anneau d'élément neutre $(0,0,\dots)$ et d'unité $(1,0,\dots)$.*

PREUVE : Si A contient $\mathbf{Q}$, l'application g_A est bijective, additive, multiplicative donc transfère la structure d'anneau commutatif de $(A^{\mathbf{N}},+,\times)$ à $(W(A),\hat{+},\hat{\times})$.
Si A est un sous-anneau d'un anneau contenant $\mathbf{Q}$, $W(A)$ est encore un anneau. C'est en particulier le cas pour $R_{\mathbf{Z}} = \mathbf{Z}[X_0,X_1,\dots,Y_0,Y_1,\dots,Z_0,Z_1,\dots]$ dans lequel nous notons X,Y et Z les vecteurs de Witt $(X_0,X_1,\dots)$, $(Y_0,Y_1,\dots)$ et $(Z_0,Z_1,\dots)$.
Sinon, soit $a,b,c \in W(A)$. Notons $\phi_{abc} : R_{\mathbf{Z}} \to A$ l'homomorphisme d'anneaux qui envoie les composantes X_k (resp. Y_k, Z_k) sur a_k (resp. b_k, c_k) pour tout entier $k \geq 0$. L'application ϕ_{abc} est additive, multiplicative, elle transporte donc les relations d'associativité, distributivité et commutativité de l'anneau $W(R_{\mathbf{Z}})$ dans l'ensemble $W(A)$ pour les lois $\hat{+}$, $\hat{\times}$. Ainsi $W(A)$ est muni d'une structure d'anneau commutatif.
Les éléments neutre et unité : c'est trivial quand $\mathbf{Q} \subset A$ et une preuve analogue à la précédente conclut. ∎

Nous en déduisons alors :

Corollaire 1.2.10 *Soient A,B deux anneaux. Pour tout morphisme d'anneaux $f : A \to B$, l'application induite $W(f) : W(A) \to W(B)$ est un morphisme d'anneaux.*

Remarque 1.2.11 *Nous avons ainsi défini un foncteur de la catégorie des anneaux dans la catgorie des anneaux.*

Définition 1.2.12 *Pour tout entier $n \geq 1$, nous notons $W_n(A)$ l'ensemble des vecteurs de Witt de $W(A)$ tronqués $(x_0,x_1,\dots,x_{n-1})$ de longueur n*

Ainsi $W_n(A),\hat{+},\hat{\times}$ est un anneau commutatif, quotient de $W(A)$. Pour $n \geq m \geq 1$, nous notons le morphisme de troncation

$$t_{nm} : W_n(A) \to W_m(A), (x_0,\dots,x_{n-1}) \mapsto (x_0,\dots,x_{m-1}).$$

Théorème 1.2.13 *Soit A un anneau. L'anneau des vecteurs Witt $W(A)$ est isomorphe à la limite projective du système $(W_n,t_{nm})_{(n,m)\in\mathbf{N}^2}$:*

$$W(A) = \lim_{\leftarrow} W_n(A).$$

PREUVE : Les morphismes de troncation t_{nm} sont des morphismes d'anneaux, la limite projective $\text{proj lim}\, W_n(A)$ a une structure d'anneau. Montrons l'existence d'un isomorphisme d'anneaux entre $W(A)$ et $\text{proj lim}\, W_n(A)$. Pour $n \in N^*$, notons π_n la projection

$$\pi_n : \text{proj lim}\, W_n(A) \longrightarrow W_n(A)$$

Comme les applications de troncation sont surjectives les projections π_n aussi. La propriété universelle des limites projectives appliqués aux morphismes compatibles $t_n : W(A) \to W_n(A)$ induit l'existence d'une unique application (qui est donc un morphisme d'anneaux) $\theta : W(A) \to \text{proj lim}\, W_n(A)$ qui factorise les t_n à travers π_n : $t_n = \theta \circ \pi_n$.
Montrons que θ est bijectif. Il est clairement injectif. Soit $z = (z^1, z^2, \dots) \in \text{proj lim}\, W_n(A)$, on cherche $x \in W(A)$ tel que $\theta(x) = z$. Or

$$\theta(x) = z \Longleftrightarrow \forall n \geq 1, \pi_n \circ \theta(x) = \pi_n(z) \Longleftrightarrow \forall n \geq 1, t_n(x) = z^n \Longleftrightarrow \forall n \geq 1, \forall k \leq n-1, x_k = (z^n)_k$$

Pour $n \geq m$, $t_{nm} \circ \pi_n(z) = \pi_m(z)$ (système projectif). Donc Pour $n \geq m$ et $k \in \{0, \dots, m-1\}$, $(z^n)_k = (z^m)_k$. Ainsi pour $k \geq 0$ et $n \geq k+1$ les coefficients $(z^n)_k$ sont constants et égaux à $(z^{k+1})_k$. Alors le vecteur de Witt x de $W(A)$ défini par ses coefficients :

$$\forall k \geq 0, x_k = (z^{k+1})_k$$

satisfait

$$\forall n \geq 0, \forall k \leq n-1, (x)_k = (z^{(n)})_k.$$

Donc $\theta(x) = z$ et θ est surjectif. ∎

Corollaire 1.2.14 *Si A est un anneau topologique, l'anneau des vecteurs de Witt $W(A)$ est naturellement muni d'une topologie induite du produit $\Pi_n W_n(A)$, où chaque anneau $W_n(A)$ a la topologie induite de A^n.*

Nous concluons ce paragraphe par une description des unités de $W(A)$.

Lemme 1.2.15 *Pour tout entier $n \geq 1$, un vecteur tronqué $(x_0, \dots, x_{n-1})$ de $W_n(A)$ est une unité de $W_n(A)$ si et seulement si x_0 est une unité de A.*

PREUVE : Si $x = (x_0, \dots, x_{n-1}) \in W_n^*(A)$, alors il existe $y = (y_0, \dots, y_{n-1}) \in W_{n-1}(A)$ tel que $xy = (1, 0 \dots)$ donc $x_0 y_0 = 1$ et $x_0 \in A^*$.
Réciproquement si $x_0 \in A^*$. Soit $y = (y_0^{-1}, 0, \dots,) \in W_n(A)$. Ainsi

$$xy = (1, *, \dots, *) = (1, 0, \dots, 0) - (0, *, \dots, *) = 1 - Vz$$

pour $z \in W_n(A)$. Ainsi il existe $h \in W_n(A)$ tel que pour $y' = y(1 + Vh)$, $xy' = 1 - V^2 z'$ pour $z' \in W_n(A)$ et par récurrence, on obtient $\tilde{y}, \tilde{z} \in W_n(A)$ avec $x\tilde{y} = 1 - V^n \tilde{z} = 1$, donc $x \in W_n(A)^*$. ∎

Proposition 1.2.16 *Les unités de l'anneau de Witt $W(A)$ sont les vecteurs de Witt dont la première composante est une unité de A.*

PREUVE :

$$\begin{aligned} x \in W(A)^* &\iff \exists y \in W(A), x \cdot y = 1 \\ &\iff \exists y \in W(A), \forall n, t_n(x \cdot y) = 1 \\ &\iff \exists y \in W(A), \forall n, t_n(x) \cdot t_n(y) = 1 \\ &\iff \forall n, t_n(x) = (x_0, \dots, x_{n-1}) \text{ est une unité de} W_n(A) \\ &\iff x_0 \text{ est une unité de } A. \end{aligned}$$

■

1.3 Catégorie d'anneaux noetheriens

L'objet de ce paragraphe est l'introduction de notations et de notions d'algèbre commutative qui nous seront utiles pour définir nos foncteurs de déformations.
Soit $\mathbf{F}$ un corps fini de caractéristique p, $W(\mathbf{F})$ l'anneau des vecteurs de Witt de $\mathbf{F}$. Pour R un anneau local, on note $\mathfrak{m}_R$ son idéal maximal.

Définition 1.3.1 *On note $\widehat{\mathcal{C}}$ la catégorie des $W(\mathbf{F})$-algèbres locales noetheriennes, complets (et séparés) de corps résiduel $\mathbf{F}$. Les morphismes sont les morphismes continus d'anneaux locaux.*

Définition 1.3.2 *On appelle espace cotangent de R objet de $\widehat{\mathcal{C}}$ le $R/\mathfrak{m}_R$-module $t_R^* = \mathfrak{m}_R/(\mathfrak{m}_R^2 + pR)$. C'est un $\mathbf{F}$-espace vectoriel de dimension finie car R est noetherien. On note $t_R = \mathrm{Hom}(t_R^*, \mathbf{F})$ son espace dual, appelé espace tangent.*
Si $R \to S$ est un morphisme de $\widehat{\mathcal{C}}$, on pose $t_{S/R}^* = \mathfrak{m}_S/(\mathfrak{m}_S^2 + \mathfrak{m}_R S)$.

Lemme 1.3.3 *Soit R un objet de $\widehat{\mathcal{C}}$ et un morphisme de $\phi : S \longrightarrow T$ de $\widehat{\mathcal{C}}$. On suppose de plus que ϕ est un morphisme de R-algèbres. Alors ϕ est surjectif si et seulement si l'application induite $t_{S/R}^* \longrightarrow t_{T/R}^*$ est surjective.*

PREUVE : Si $S \to T$ est surjective alors l'application induite $t_{S/R}^* \longrightarrow t_{T/R}^*$ est surjective.

Si $R \to S$ est un morphisme de $\widehat{\mathcal{C}}$, S est engendré comme R-algèbre par l'image de R dans S et par l'idéal maximal $\mathfrak{m}_S$ (S et R ont même corps résiduel $\mathbf{F}$). L'application $\mathfrak{m}_R/\mathfrak{m}_R^2 \to \mathfrak{m}_R S/(\mathfrak{m}_R S \cap \mathfrak{m}_S^2)$ est surjective.

Si $S \longrightarrow T$ est un morphisme de $\widehat{\mathcal{C}}$ et de R-algèbres, on a un diagramme commutatif avec des suites exactes

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathfrak{m}_R S/(\mathfrak{m}_R S \cap \mathfrak{m}_S^2) & \longrightarrow & \mathfrak{m}_S/\mathfrak{m}_S^2 & \longrightarrow & t^*_{S/R} & \longrightarrow 0 \\ & \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & \\ 0 \longrightarrow & \mathfrak{m}_R T/(\mathfrak{m}_R T \cap \mathfrak{m}_T^2) & \longrightarrow & \mathfrak{m}_T/\mathfrak{m}_T^2 & \longrightarrow & t^*_{T/R} & \longrightarrow 0 \end{array}$$

L'application f^1 est surjective. Si l'application f_3 est surjective alors f_2 aussi et $S \to T$ est surjective. ∎

Soit R un objet de $\widehat{\mathcal{C}}$ et $x_1, \ldots, x_n$ une $\mathbf{F}$-base de t_R. Soit $r_1, \ldots r_n$ une famille de relèvement des x_i dans $\mathfrak{m}_R$. Alors le morphisme de $W(\mathbf{F})$-algèbres

$$W(\mathbf{F})[[X_1, \ldots, X_n]] \longrightarrow R,\ X_i \mapsto r_i$$

est surjectif. Ainsi $R = W(\mathbf{F})[[X_1, \ldots, X_n]]/I$ avec $n = \dim_{\mathbf{F}} t_R$, la difficulté se concentre dans la description de I.
Dans la suite, nous allons nous interesser à des foncteurs

$$F : \widehat{\mathcal{C}} \longrightarrow \text{Ens}$$

où Ens désigne la catégorie des ensembles. Etre représentable pour un tel foncteur est lié à la propriété de conservation du produit fibré. Cependant pour avoir stabilité par produit fibré, on doit se placer sur une sous-catégorie de $\widehat{\mathcal{C}}$.

Soit $\alpha : R \longrightarrow S$ et $\beta : T \longrightarrow S$ des morphismes d'anneaux locaux. Le produit fibré $R \times_S T$ est défini par

$$R \times_S T = \{(r, t) \in R \times T, \alpha(r) = \beta(t)\}.$$

Exemples 1.3.4 *Soit* $R = \mathbf{F}[[X, Y]] \times_{\mathbf{F}[[X]]} \mathbf{F}$ *où* $\mathbf{F} \to \mathbf{F}[[X]]$ *est l'inclusion et* $\mathbf{F}[[X, Y]] \to \mathbf{F}[[X]]$, $Y \mapsto 0$. *Alors* R *s'identifie au sous-anneau de* $\mathbf{F}[[X, Y]]$ *:*

$$R = \Big\{ a + YP(X, Y), a \in \mathbf{F} P \in \mathbf{F}[[X, Y]] \Big\}.$$

Ainsi $\dim_{\mathbf{F}} \mathfrak{m}_R/\mathfrak{m}_R^2$ *est infinie et* R *n'est pas noetherien. Donc* $\widehat{C}$ *n'est pas stable par produit fibré.*

Définition 1.3.5 *Soit* $\mathcal{C}$ *la catégorie des anneaux locaux* A *artiniens complets de corps résiduel* $\mathbf{F}$. *Les morphismes sont les morphimes d'anneaux locaux.*

Pour tout object R de $\widehat{\mathcal{C}}$, R est homéomorphe à la limite des objets $R/\mathfrak{m}_R^n$ de $\mathcal{C}$. La catégorie $\mathcal{C}$ est stable par produit fibré. Dans la suite, nous allons définir des foncteurs $F : \mathcal{C} \to \text{Ens}$ et les étendre par continuité à $\widehat{\mathcal{C}}$ via

$$F(R) = \operatorname{proj}\lim_n F(R/\mathfrak{m}_R^n).$$

Définition 1.3.6 *On dit qu'un foncteur $F : \widehat{\mathcal{C}} \to$ Ens est continu si pour chaque R de $\widehat{\mathcal{C}}$, $F(R) \to \operatorname{proj}\lim F(R/\mathfrak{m}_R^n)$ est bijectif. Un tel foncteur est donc déterminé par sa restriction à $\mathcal{C}$.*

Comme la limite projective commute avec le foncteur $\text{Hom}(A, \bullet)$, pour tout R objet de $\mathcal{C}$, le foncteur $\text{Hom}(R, \bullet) : \widehat{\mathcal{C}} \longrightarrow$ Ens est continu.

Définition 1.3.7 *Un foncteur $F : \widehat{\mathcal{C}} \longrightarrow$ Ens est représentable s'il existe un objet R de $\widehat{\mathcal{C}}$ et un isomorphisme $F \simeq \text{Hom}(R, \bullet)$. Un foncteur $F : \mathcal{C} \to$ Ens est dit pro-représentable s'il existe $R \in \widehat{\mathcal{C}}$ tel que $F \simeq \text{Hom}(R, \bullet)$.*

Ainsi les foncteurs de déformations que nous allons définir dans la suite et qui seront représentables seront continus.

Définition 1.3.8 *Soient deux foncteurs $F, G : \mathcal{C} \longrightarrow$ Ens tels que $F(\mathbf{F})$ et $G(\mathbf{F})$ soient réduits à un élément. On prolonge par continuité ces deux foncteurs à $\widehat{\mathcal{C}}$. On dit qu'un morphisme de foncteur $F \longrightarrow G$ est lisse lorsque pour toute surjection $A \to B$ dans $\mathcal{C}$, l'application naturelle suivante est surjective*

$$F(A) \longrightarrow F(B) \times_{G(B)} G(A).$$

Voyons ce que signifie être lisse dans le cas de foncteurs représentables.

Proposition 1.3.9 *Soit $R \to S$ un morphisme de $\widehat{\mathcal{C}}$. Alors $Hom(S, \bullet) \longrightarrow \text{Hom}(R, \bullet)$ est lisse si et seulement si S est un anneau de séries formelles sur R. On dit que S est lisse sur R.*

Preuve : Si S est un anneau de séries formelles sur R, le morphisme de foncteur est lisse. Réciproquement soit $x_1, \ldots, x_n$ des éléments de S qui induisent une base de $t^*_{S/R} = \mathfrak{m}_S/(\mathfrak{m}_S^2 + \mathfrak{m}_R S)$. Soit $T = R[[X_1, \ldots, X_n]]$. Nous avons un morphisme de R-algèbre locale $u_1 : S \longrightarrow T/(\mathfrak{m}_T^2 + \mathfrak{m}_R T)$ en envoyant x_i sur l'image de X_i.
Par lissité, u_1 se relève en $u_2 : S \longrightarrow T/\mathfrak{m}_T^2$, puis en $u_3 : S \longrightarrow T/\mathfrak{m}_T^3$... Ainsi, on obtient $u : S \longrightarrow T$ qui induit un isomorphisme de $t^*_{S/R}$ avec $t^*_{T/R}$ (vu le choix de u_1) donc u est une surjection.
Soit $y_i \in S$ tels que $u(y_i) = X_i$; en posant $vX_i = y_i$, on obtient un morphisme local $v : T \longrightarrow S$ de R-algèbres tel que $uv = 1_T$. Donc v est injective. Or v induit une bijection sur les espaces cotangents donc v est surjective et S est isomorphe à T. ∎

2 Cohomologie galoisienne

Dans la suite, nous nous interessons essentiellement à la cohomologie des groupes profinis suivants :
- soit $\mathbf{F}$ une extension finie de $\mathbf{F}_p$, $\overline{\mathbf{F}}$ une clôture algébrique de $\mathbf{F}$ et G est le groupe de Galois $G = \mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})$,
- soit ℓ un nombre premier, L une extension finie de $\mathbf{Q}_\ell$, $\overline{L}$ une clôture algébrique de L et G est le groupe de Galois local $G = \mathrm{Gal}(\overline{L}/L)$,
- soit F un corps de nombres (i.e. une extension finie de $\mathbf{Q}$), S un ensemble fini de places de F et $F_S \subset \overline{\mathbf{Q}}$ la plus grande extension de F non ramifiée en dehors de S, G est le groupe de Galois global $G = \mathrm{Gal}(F_S/F)$.

Nous commençons par rappeler les résultats de cohomologie des groupes profinis qui nous seront utiles dans ce cours. Voir [Se2] §1. et 2. pour les démonstrations détaillées des résultats rappelés ici.

2.1 Cohomologie d'un groupe profini

Avant de commencer, rappelons la construction classique de la cohomologie pour des complexes de R-modules où R est un anneau. Un complexe $A^\bullet$ de R-modules est une suite d'homomorphismes de R-modules

$$d^i : A^i \to A^{i+1}, i \in \mathbf{Z}$$

telle que $d^{i+1} \circ d^i = 0$ pour tout i. Le i-ème groupe de cohomologie du complexe $A^\bullet$ est

$$H^i(A^\bullet) = \ker d^i / \operatorname{im} d^{i-1}, i \in \mathbf{Z}.$$

Un morphisme de complexes $A^\bullet \to B^\bullet$ est une collection d'homomorphismes $\phi^i : A^i \to B^i$, $i \in \mathbf{Z}$ tels que le diagramme suivant est commutatif

$$\begin{array}{ccc} A^i & \longrightarrow & A^{i+1} \\ \phi^i \downarrow & & \downarrow \phi^{i+1} \\ B^i & \longrightarrow & B^{i+1} \end{array}$$

Un morphisme de complexes induit donc des applications $H^i(A^\bullet) \to H^i(B^\bullet)$ pour $i \in \mathbf{Z}$. Une suite exacte de complexes est une suite de morphismes de complexes

$$0 \longrightarrow A^\bullet \longrightarrow B^\bullet \longrightarrow C^\bullet \longrightarrow 0$$

telle que pour tout $i \in \mathbf{Z}$, la suite de R-modules suivantes est exacte :

$$0 \longrightarrow A^i \longrightarrow B^i \longrightarrow C^i \longrightarrow 0.$$

On rappelle le lemme du serpent :

Lemme 2.1.1 *Etant donné un diagramme commutatif de R-modules*

$$\begin{array}{ccccccc} & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow 0 \\ & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & \\ 0 \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \end{array}$$

avec des lignes exactes, alors il existe une suite exacte

$$\ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma \longrightarrow \mathrm{Coker}\,\alpha \longrightarrow \mathrm{Coker}\,\beta \longrightarrow \mathrm{Coker}\,\gamma.$$

Preuve : La construction des applications de la suite exacte est immédiate sauf pour δ : $\ker\gamma \to \mathrm{Coker}\,\alpha$. Soit $c \in \ker\gamma$ et b un relèvement de c dans B. Par commutativité du diagramme, $\beta(b)$ s'envoie sur 0 dans C' donc provient d'un unique $a' \in A'$. On définit $\delta(c)$ comme l'image de a' dans $\mathrm{Coker}\,\alpha$. Deux choix de relèvements b, b' diffèrent par un élément $a \in A$ qui s'envoie sur 0 dans $\mathrm{Coker}\,\alpha$ donc δ est bien défini. Il suffit alors de vérifier l'exactitude de la suite obtenue. ∎

Proposition 2.1.2 *Soit*

$$0 \longrightarrow A^\bullet \longrightarrow B^\bullet \longrightarrow C^\bullet \longrightarrow 0$$

une suite exacte de complexes de R-modules. Alors on a une suite exacte longue de cohomologie

$$\cdots \longrightarrow H^i(A^\bullet) \longrightarrow H^i(B^\bullet) \longrightarrow H^i(C^\bullet) \longrightarrow H^{i+1}(A^\bullet) \longrightarrow H^{i+1}(B^\bullet) \longrightarrow \cdots$$

Preuve : Il suffit d'applique le lemme du serpent au diagramme

$$\begin{array}{ccccccc} & A^i/\operatorname{im} d_A^{i-1} & \longrightarrow & B^i/\operatorname{im} d_B^{i-1} & \longrightarrow & C^i/\operatorname{im} d_C^{i-1} & \longrightarrow 0 \\ & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & \\ 0 \longrightarrow & \ker d_A^{i+1} & \longrightarrow & \ker d_B^{i+1} & \longrightarrow & \ker d_C^{i+1} & \end{array}.$$

∎

Soit G un groupe profini. Un G-module A est un groupe abelien discret sur lequel G opère continûment, i.e. pour tout $x \in A$, $g \mapsto g \cdot x$ est continue de G dans A, i.e. le fixateur de tout point est ouvert, i.e. $A = \cup A^U$ où U parcourt l'ensemble des sous-groupes discrets de G. La cohomologie de G définie ici est à valeurs dans les G-modules. Soit A un tel G-module. Nous notons $C^n(G, A)$ le n-ième groupe (des cochaines continues) des applications continues (localement constantes) de G^n dans A. Pour $n = 0$, $C^0(G, A) = \{G^0 = \{1\} \to A\}$. Nous définissons le cobord

$$d^n : C^n(G, A) \to C^{n+1}(G, A)$$

par la formule

$$d^n f(g_1, \dots, g_{n+1}) = g_1 \cdot f(g_2, \dots, g_n) + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1} f(g_1, \dots, g_n).$$

Nous vérifions facilement que $d^2 = 0$. Nous obtenons ainsi un complexe $C^*(G, A)$ dont les groupes de cohomologie permettent de définir $H^n(G, A) = \ker d^n / \operatorname{im} d^{n-1}$ $n \geq 0$ $(d^{-1} = 0)$.

Exemple 2.1.3 *Par définition*

$$H^0(G, A) = A^G = \{a \in A, ga = a \ \ \forall g \in G\}.$$

$$H^1(G, A) = \frac{\{f : G \to A, f(g_1 g_2) = g(g_1) + g_1 g(g_2), \forall g_1, g_2 \in G\}}{\{f : G \to A, \exists a \in A, f(g) = ga - a, \forall g \in G\}}.$$

Remarque 2.1.4 *Il est important de prendre la topologie de G et de A en compte. En effet pour $G = \mathrm{Gal}(L/K)$ extension finie, le groupe de cohomologie algébrique (sans topologie) $H^1(G, A) = \mathrm{Hom}(G, A)$ classifie habituellement les sous-extensions $K \subset K' \subset L$ telle que $\mathrm{Gal}(K'/K)$ est isomorphe à un sous-groupe de A. D'après la théorie de Galois infinie, seuls les sous-groupes fermés de $\mathrm{Gal}(L/K)$ correspondent aux sous-extensions $K \subset K' \subset L$.*

La cohomologie profinie est fonctorielle en ses coefficients : si $A \to A'$ est un morphisme de G-modules, on a des morphismes $H^n(G, A) \longrightarrow H^n(G, A')$. Si on a une suite exacte de modules topologiques et qu'il existe une section continue $A'' \to A$ (d'ensembles pas de modules), alors

$$0 \longrightarrow C^n(G, A'') \longrightarrow C^n(G, A) \longrightarrow C^n(G, A'') \longrightarrow 0$$

est exacte pour tout n et on a une suite exacte longue de cohomologie

$$\cdots \longrightarrow H^n(G, A') \longrightarrow H^n(G, A) \longrightarrow H^n(G, A'') \longrightarrow H^{n+1}(G, A') \longrightarrow \cdots .$$

Si A et B sont deux G-modules, $A \otimes_{\mathbf{Z}} B$ est un G-module via $g(a \otimes b) = ga \otimes gb$, $g \in G$, $(a, b) \in A \times B$. On en déduit une application bilinéaire au niveau des cochaînes

$$C^p(G, A) \times C^q(G, B) \longrightarrow C^{p+q}(G, A \otimes B),$$

$$\phi \cup \psi(g_1, \dots, g_p, g_{p+1}, \dots, g_{p+q}) = \phi(g_1, \dots, g_p) \otimes \psi(g_{p+1}, \dots, g_{p+q}).$$

Proposition 2.1.5 *L'application $\cup$ induit une application bilinéaire*

$$H^p(G,A) \times H^q(G,B) \longrightarrow^{\cup} H^{p+q}(G, A \otimes B)$$

notée encore $\cup$ et appelée cup-produit.

PREUVE : Il suffit de vérifier la formule

$$d(a \cup b) = (da) \cup b + (-1)^p (a \cup db).$$

Or

$$d(a \cup b)(g_0, \dots, g_{p+q+1}) = \sum_{i=0}^{p} (-1)^i a(g_0, \dots, \hat{g}_i, \dots, g_{p+1}) \otimes b(g_{p+1}, \dots, g_{p+q+1})$$
$$+ \sum_{i=p+1}^{p+q+1} (-1)^i a(g_0, \dots, g_p) \otimes b(g_p, \dots, \hat{g}_i, \dots, g_{p+q+1})$$

$$(da \cup b)(g_0, \dots, g_{p+q+1}) = \sum_{i=0}^{p} (-1)^i a(g_0, \dots, \hat{g}_i, \dots, g_{p+1}) \otimes b(g_{p+1}, \dots, g_{p+q+1})$$

$$(a \cup db)(g_0, \dots, g_{p+q+1}) = \sum_{i=0}^{q+1} (-1)^i a(g_0, \dots, g_p) \otimes b(g_p, \dots, \hat{g}_{i+p}, \dots, g_{p+q+1})$$

On obtient alors le résultat annoncé. ∎

Plus gnralement, s'il existe des applications continues de G-modules $M \to P$, $N \to P$, on peut définir de même un cup-produit $H^p(G,M) \times H^1(G,N) \to H^{p+q}(G,P)$.

Proposition 2.1.6 *Soit (G_i) un système projectif de groupes profinis ; soit (A_i) un système inductif de G_i-modules discrets, les flêches de transition étant compatibles avec celles de (G_i). Soit $G = \operatorname{proj\,lim} G_i$ et $A = \lim_{\leftarrow} A_i$. Alors pour tout $q \in \mathbf{N}$,*

$$H^q(G,A) = \lim_{\leftarrow} H^q(G_i, A_i).$$

PREUVE : Il suffit de montrer que les homomorphismes canoniques

$$\lim_{\leftarrow} C^q(G_i, A_i) \longrightarrow H^q(G,A)$$

sont des isomorphismes. L'injectivité : si $\varphi \in \lim_{\leftarrow} C^q(G_i^q \longrightarrow A_i)$ induit une fonction nulle de G^q dans A, alors les valeurs de φ (qui sont en nombre fini par continuité) s'annulent toutes dans A_j pour $j \geq i$. Donc l'image de φ dans $C^q(G_j, A_j)$ est nulle donc aussi son image dans la limite inductive.

La surjectivité : soit $f : G \longrightarrow A$ continue, f est localement constante. Comme G est compact et possède une base de voisinage de 1 constituée de sous-groupes distingués fermés (car G totalement discontinu), la fonction f se factorise à travers un quotient fini G/U qui est un quotient G_j/U_n de l'un des G_j. En particulier l'application induite $\overline{f} : G/U \longrightarrow A$ provient d'un homomorphisme $f_j : G_j/U_j \longrightarrow A_i$. On peut supposer $i \geq j$ donc f provient de $f_i : G_i \longrightarrow A_i$ composée de $G_i \longrightarrow G_j$ avec $f_j : G_j/U_j \longrightarrow A_i$. ∎

On déduit de cette proposition un corollaire important car il permet de se ramener à des groupes finis pour démontrer des résultats sur les groupes de cohomologie. Lorsque les groupes sont finis, la continuité des appplications $C^q(G, A)$ est immédiate. Il faut juste faire attention, pour les propriétés faisant intervenir un sous-groupe H de G, à se restreindre aux sous-groupes fermés de G, de manière à rester dans la catégorie des groupes profinis.

Corollaire 2.1.7 *Soit A un G-module discret. Alors*

$$H^q(G, A) = \lim_{\leftarrow U} H^q(G/U, A^U)$$

où U parcourt l'ensemble des sous-groupes ouverts distingués de G.

Soit G un groupe profini, A un G-module et H un sous-groupe fermé. L'injection canonique $f : H \longrightarrow G$ permet de munir A d'une structure de H-module :

$$h \cdot a = f(h) \cdot a, a \in A, h \in H$$

et donc des morphismes de restriction Res : $H^q(G, A) \to H^q(H, A)$, $q \geq 0$. Par ailleurs, si H est normal, le groupe-quotient G/H agit sur A^H et l'inclusion $A^H \to A$ est compatible avec la surjection canonique $G \longrightarrow G/H$. On a donc des morphismes d'inflation

$$\inf : H^q(G/H, A^H) \longrightarrow H^q(G, A), \quad q \geq 0.$$

Proposition 2.1.8 *Soit H un sous-groupe normal fermé de G.*
On a une suite d'inflation-restriction

$$0 \longrightarrow H^1(G/H, A^H) \longrightarrow^{\text{Inf}} H^1(G, A) \longrightarrow^{\text{Res}} H^1(H, A)$$

Preuve : On démontre ce résultat pour G fini. Montrons d'abord l'injectivité de l'inflation. Soit $f : G/H \longrightarrow A^H$ un 1-cocycle cohomologue à 0 dans $H^1(G, A)$. Ainsi f s'identifie à une application de G dans A constante sur chaque classe modulo H. Il existe $a \in A$ tel que $f(s) = s \cdot a - a$, pour tout $s \in G$. Pour tout $t \in H$, $f(t) = f(1) = 0 = t \cdot a - a$, donc $a \in A^H$ et la classe de f dans $H^1(G/H, A^H)$ est nulle.

Montrer qu'un élement de $\ker \mathrm{Res}$ est dans $\Im \mathrm{Inf}$. Soit $f : G \to A$ un 1-cocycle. Si $\mathrm{Res}(f) = 0$ alors il existe $a \in A$ tel que $f(t) = t \cdot a - a$, $t \in H$. Quitte à remplacer f par le cocycle cohomologue $G \longrightarrow A$, $t \mapsto f(t) - (t \cdot a - a)$ et supposer $f(t) = 0$ pour tout $t \in H$. Or pour tout $s, t \in G$, $f(st) = f(s) + s \cdot f(t)$, donc f se factorise en une application $\bar{f} : G/H \to A$. Pour tout $s \in H$ les classes de st et t sont les mêmes

■

Remarque 2.1.9 *Plus généralement, pour G groupe profini, M discret et H sous-groupe normal de G, on a une suite spectrale $H^p(G/H, H^q(H, M)) \longrightarrow H^{p+q}(G, M)$ car les groupes de cohomoloie $H^q(G, M)$ sont des foncteurs dérivés de $M \mapsto M^G$ et que ce foncteur est la composition de $M \mapsto M^H$ avec $M^G \mapsto (M^H)^{G/H}$. En particulier les termes de bas degrés de la suite spectrale donne la suite exacte de Hochschild-Serre dite d'inflation-restriction*

$$0 \to H^1(G/H, M^H) \to^{\mathrm{inf}} H^1(G, M) \to^{\mathrm{res}} H^1(H, M)^{G/H} \to H^2(G/H, M^H) \to^{\mathrm{inf}} H^2(G, M).$$

Pour U un sous-groupe ouvert distingué de G, on définit la norme $N_{G/U} : A^U \longrightarrow A^G$ par $N_{G/U} : a \mapsto_{s \in G/U} sa$. On définit également par limite inductive, le groupe de cohomologie modifié :

$$\hat{H}^0(G, A) = \lim_{\leftarrow} \hat{H}^0(G/U, A^U)$$

où pour U sous-groupes distingués de G, $\hat{H}^0(G/U, A^U) = A^G/N_{G/U}A^U$ et pour $V \subset U$ deux sous-groupes ouverts distingu{es de G, l'inclusion $N_{G/V}A^V \subset N_{G/U}A^U$, obtenue en regroupant les éléments de G/V en classes selon U/V, induit $\hat{H}^0(G/V, A^V) \longrightarrow \hat{H}^0(G/U, A^U)$.

2.2 Compléments de cohomologie des groupes

2.2.1 Lemme de Shapiro

La cohomologie des groupes finis, s'obtient de façon plus abstraite par résolution projective. C'est un moyen efficace pour obtenir des résultats sur la cohomologie des groupes finis, qui, par passage, à la limite donnent des résultats sur la cohomologie de groupes profinis.

Définition 2.2.1 *Soit R un anneau. Un R-module est dit projectif si pour toute surjection $\alpha : A \to B$, l'application naturelle $\mathrm{Hom}(P, A) \to \mathrm{Hom}(P, B)$ est surjective.*
Soit A un R-module, une résolution projective $P_\bullet$ de A est une suite exacte infinie

$$\cdots \longrightarrow P_2 \longrightarrow P_1, \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

avec P_i projectif.

Si G est un groupe fini, A un G-module et $P_\bullet$ une résolution projective du G-module trivial $\mathbf{Z}$, alors $\mathrm{Hom}_G(P_\bullet, A)$ est un complexe de groupes abeliens et on a

$$H^i(G, A) = H^i(\mathrm{Hom}_G(P_i, A)).$$

Il s'agit de voir d'une part que cette construction ne dépend pas de la résolution projective choisie, d'autre part que la suite de cochaînes introduite dans ce cours correspond à une résolution projective (dite standard).

Définition 2.2.2 *Soit G un groupe fini, H un sous-groupe et A un H-module. Le G-module $\mathbf{Z}[G]$, vu comme H-module permet d'associer à A le G-module*

$$I_H^G(A) = \mathrm{Hom}_H(\mathbf{Z}[G], A)$$

où $\sigma \in G$ agit sur le H-homomorphisme $\phi : \mathbf{Z}[G] \to A$ par $(\sigma\phi)(g) = \phi(g\sigma)$ pour g élément de la base de $\mathbf{Z}[G]$.

Lemme 2.2.3 *Soit G un groupe fini, H un sous-groupe, A un H-module, M un G-module. On a l'isomorphisme*

$$\mathrm{Hom}_G(M, I_H^G(A)) \simeq \mathrm{Hom}_H(M, A), \quad (m \mapsto \phi_m) \mapsto (m \mapsto \phi_m(1)).$$

Preuve : La réciproque s'obtient de la façon suivante : soit $\psi \in \mathrm{Hom}_H(M, A)$, soit $\psi_m \in \mathrm{Hom}_H(\mathbf{Z}[G], A)$, $\psi_m(g) = \psi(gm)$. Ainsi $m \mapsto \psi_m$ définit un élément de $\mathrm{Hom}_G(M, \mathrm{Hom}_H(\mathbf{Z}[G], A))$.
∎

En appliquant ce lemme aux termes d'une $\mathbf{Z}[G]$-résolution projective de $\mathbf{Z}$ (qui est une résolution projective de H-modules car $\mathbf{Z}[G]$ est libre comme $\mathbf{Z}[H]$-module), on obtient plus généralement

Proposition 2.2.4 *(Lemme de Shapiro) On a des isomorphismes canoniques*

$$H^q(G, I_H^G(A)) \to H^q(H, A), \quad q \geq 0.$$

2.2.2 Cohomologie des pro-p-groupes

Citons un résultat de Serre qui permet de comprendre mieux comment les groupes de cohomologie donnent des informations précise sur la structure des groupes. Soit G un pro-p-groupe, on note $H^i(G) = H^i(G, \mathbf{Z}/p\mathbf{Z})$ où G agit trivialement sur $\mathbf{Z}/p\mathbf{Z}$.

Définition 2.2.5 *Soit I un ensemble et soit $L(I)$ le groupe discret libre engendré par des éléments x_i indexés par I. On considère la famille X de sous-groupes distingués M de $L(I)$ tels que $L(I)/M$ est un p-groupe fini et M contient presque tous les x_i. Le pro-p-groupe libre engendré par I est défini par $F(I) = \operatorname{proj\,lim} L(I)/M$.*
Lorsque I est de cardinal n, on note $F(n)$ le pro-p-groupe libre à n générateurs.

Définition 2.2.6 *Soit G un groupe profini. On dit que des éléments $g_1, \ldots, g_n$ de G engendrent G si le sous-groupe qu'ils engendrent (au sens algébrique) est dense dans G, i.e. pour tout U normal ouvert, le quotient G/U est engendré par les g_i.*

Lemme 2.2.7 *Soit $f : G_1 \to G_2$ un morphisme de pro-p-groupes. Le morphisme f est surjectif si et seulement si $H^1(G_2) \to H^1(G_1)$ est injectif.*

PREUVE : Le sens direct est clair. Réciproquement, supposons que f n'est pas surjective. Alors il existe un quotient fini P_2 de G_2 tel que l'image P_1 de $f(G_1)$ dans P_2 soit distincte de P_2. Il existe alors un sous-groupe distingué de P_2 d'indice p contenant P_1. Donc il existe un morphisme non nul $\pi : P_2 \to \mathbf{Z}/p\mathbf{Z}$ qui envoie P_1 sur 0. L'image de $\pi \in H^1(G_2)$ dans $H^1(G_1)$ est nulle. Donc $H^1(G_2) \to H^1(G_1)$ n'est pas injective. ∎

Corollaire 2.2.8 *Si G est un pro-p-groupe, on note $G^* = G^p\overline{[G,G]}$. Un morphisme $G_1 \to G_2$ est surjectif si et seulement si $G/G_1^* \to G_2/G_2^*$ l'est.*

PREUVE : En effet G^* s'identifie au sous-groupe de G intersection des noyaux des homomorphismes continus $\pi : G \to \mathbf{Z}/p\mathbf{Z}$. Les groupes G/G^* et $H^1(G)$ sont donc duaux l'un de l'autre.
∎

Corollaire 2.2.9 *Soit $g_1, \ldots, g_n$ des éléments d'un pro-p-groupe G. Montrer l'équivalence entre :*
i. les g_i engendrent G,
ii. l'homomorphisme $F(n) \to G$ défini par les g_i est surjectif,
iii. Les images des g_i dans G/G^* engendre ce groupe,
iv. Tout $\pi \in H^1(G)$ qui s'annule sur les g_i est égal à 0.

Proposition 2.2.10 *Soit G un pro-p-groupe tel que $H^1(G)$ et $H^2(G)$ soient finis. Alors*
i. Le nombre minimum de générateurs $x_1, \dots, x_n$ de G est égal à la dimension de $H^1(G)$.
ii. Le nombre des relations entre les x_i est égal à la dimension de $H^2(G)$.

PREUVE : i. Comme les homomorphismes de $G \to \mathbf{Z}/p\mathbf{Z}$ s'annulent sur $G^* = G^p[G,G]$, on a $H^1(G) = H^1(G/G^*)$. On a vu que $g_1, \dots, g_n$ engendrent G si et seulement si leurs images engendrent G/G^*.
ii. Soit G un pro-p groupe admettant une présentation à $n = \dim H^1(G)$ générateurs, $F = F(n)$

$$0 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 0.$$

Comme on a une bijection $H^1(G) \to H^1(F)$, l'application $t : H^1(R)^G \to H^2(G)$ est injective. Le groupe F est libre, donc $H^2(F) = 0$. Donc t surjective donc bijective.
Il s'agit alors de voir que $\dim H^1(R)^{F/R}$ est le nombre minimal de générateurs de R comme sous groupe fermé distingué de F (les conjugués des générateurs engendrent (au sens algébrique) un sous-groupe dense de R). Or pour que les r_i engendrent R, il faut et il suffit que tout élément $\pi \in H^1(R)^{F/R}$ qui s'annule sur les r_i soit nul (exercice). Donc $\dim H^1(R)^{F/R}$ est le nombre minimal de générateurs de R. ∎

Citons l'exemple des pro-p-groupes dit de Demuskin qui admettent des présentations par générateurs et relations très simples et qui sont caractérisés par leurs propriétés cohomologiques.

Définition 2.2.11 *Un pro-p-groupe est dit de Demuskin s'il vérifie les propriétés suivantes*
i. $H^2(G)$ est de dimension 1 sur $\mathbf{Z}/p\mathbf{Z}$,
ii. $H^1(G)$ est de dimension finie et le cup-produit

$$H^1(G) \times H^1(G) \to H^2(G) = \mathbf{Z}/p\mathbf{Z}$$

est une forme bilinéaire non dégénérée.

Notons $n = \dim H^1(G)$. Un groupe de Demuskin est donc engendré par n éléments et une relation. Il s'agit de déterminer cette relation. Pour cela, notons $G' = G/\overline{[G,G]}$, c'est un quotient de $\mathbf{Z}_p^n$ par un sous-groupe isomorphe à $\mathbf{Z}_p$ ou réduit à 0. Comme $H^1(G') = H^1(G)$ est de dimension n, on a $G' = (\mathbf{Z}_p)^n$ ou $\mathbf{Z}/q\mathbf{Z} \times (\mathbf{Z}_p)^{n-1}$ avec $q = p^f$.

Théorème 2.2.12 *(exercice) Soit G un groupe de Demuskin d'invariant $q \neq 0, 2$. Alors G est isomorphe au groupe engendré par n générateurs $x_1, \dots, x_n$ liés par la relation*

$$x_1^q [x_1, x_2] \cdots [x_{n-1}, x_n] = 1.$$

Remarque 2.2.13 *Le cas $q = 2$ (et n pair) est exceptionnel, les invariants n et q ne suffisent plus à déterminer la structure de G.*

PREUVE : (esquisse) Soit $G = F/(r)$ un groupe de Demuskin d'invariants n, q avec $q \neq 0, 2$ et $p \neq 2$, quotient du groupe libre F à n générateurs et une relation r.
On considère la filtration (F_i) du pro-p-groupe F :

$$F_0 = F,\ F_{i+1} = F_i^q[F, F_i], i \geq 1.$$

On introduit le gradué $\mathrm{gr}(F) = F_i/F_{i+1}$ de F. On constate que $r \in F_2$ et $\mathrm{gr}_2(F)$ admet une $\mathbf{Z}/q\mathbf{Z}$-base dans laquelle on écrit $\bar{r} \in F_2/F_3$. On relie l'écriture obtenue au cup-produit et par approximation successive modulo F_h, on construit une famille de générateurs $x_1, \ldots, x_n$ de G qui satisfont la relation de Demuskin. ∎

2.3 Cohomologie galoisienne

Dans ce paragraphe, K un corps, $\overline{K}$ une clôture séparable et $G_K = \mathrm{Gal}(\overline{K}/K)$. Le groupe abelien $\overline{K}^*$ est muni d'une action naturelle de G_K-module discret. Notons μ_n le groupes des racines n-ième de $\overline{K}^*$.
Dans la suite de ce cours, on va s'interesser à la cohomologie de groupes de Galois sur K à valeurs dans des $\mathbf{F}$-espaces vectoriels ($\mathbf{F}$ corps fini) de dimension finie. Pour K, corps fini, les calculs sont élémentaires. Pour un corps local, l'étude de la structure du groupe de Galois absolu permet de déterminer ces groupes de cohomologie. Pour un corps de nombres, ces calculs sont plus mystérieux et sont liés à plusieurs conjectures classiques de théorie algébrique des nombres. Un premier moyen pour déterminer ces groupes de cohomologie est d'utiliser des résultats de passage local/global.

2.3.1 Premiers calculs de cohomologie galoisienne

L'objet de ce paragraphe est de présenter quelques stratégies classiques de calculs de cohomologie galoisienne en spécifiant les hypothèses et les résultats sur le corps de base K.

Lemme 2.3.1 *On a*

$$H^0(G_K, \overline{K}^*) = K^*,\ \ H^0(G_K, \mu_n) = \mu_n \cap K.$$

Lemme 2.3.2 *On a $H^q(G_K, \overline{K}) = 0$ pour $q > 0$.*

PREUVE : Soit L une extension finie galoisienne de K, le $\mathrm{Gal}(L/K)$-module L est isomorphe à $\mathbf{Z}[\mathrm{Gal}(L/K)] \otimes_{\mathbf{Z}} K$. Le résultat est une application immédiate du lemme de Shapiro. On conclut par passage à la limite inductive sur les groupes de cohomologie. ∎

On en déduit le résultat suivant pour la cohomologie des corps finis (Artin-Schreier):

Proposition 2.3.3 *Soit K un corps de caractéristique p et $\phi : \overline{K} \to \overline{K}$, $x \mapsto x^p - x$. Alors $H^1(G_K, \mathbf{Z}/p\mathbf{Z}) = K/\phi(K)$ et $H^q(G_K, \mathbf{Z}/p\mathbf{Z}) = 0$ pour $q \geq 2$.*

PREUVE : L'application ϕ est un morphisme ($\overline{K}$ est de caractéristique p de G_K-modules surjectif car pour tout $a \in \overline{K}$, le polynôme $X^p - X - a$ est séparable et $\overline{K}$ est algébriquement clos. Le noyau de ϕ est un sous-corps premier de $\overline{K}$ donc $\mathbf{Z}/p\mathbf{Z}$. On a donc la suite exacte de G_K-module

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow \overline{K} \longrightarrow^{\phi} \overline{K} \longrightarrow 0$$

et en utilisant la suite exacte longue associée, on en déduit $H^q(G_K, \overline{K}) = 0$ pour tout $q > 0$. ∎

Le théorème d'Hilbert 90 donne un résultat important sur les H^1 :

Théorème 2.3.4 *Soit L une extension finie de K et $G_L = \mathrm{Gal}(L/K)$. Alors*

$$H^1(G_L, L^*) = 0 \text{ et } H^1(G_K, \overline{K}^*) = 0.$$

PREUVE : Soit $s \mapsto a_s$ un cocycle de $\ker d^1 \subset C^1(G, L^*)$. D'après le théorème d'indépendance linéaire de Dedekind, il existe $c \in L^*$ tel que

$$b = \sum_{t \in G} a_t t(c)$$

soit non nul. Alors

$$\forall s \in G, s(b) = \sum_{t \in G} s(a_t) \cdot (st)(c) = \sum_{t \in G} a_s^{-1} a_{st} \cdot (st)(c) = a_s^{-1} b.$$

Donc $a_s = s(b^{-1})/b^{-1}$ est un cobord. ∎

La suite exacte longue de cohomologie associée à

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^* \longrightarrow^n \overline{K}^* \longrightarrow 1$$

donne alors le corollaire suivant :

Corollaire 2.3.5 *Soit n inversible dans K, $H^1(G_K, \mu_n) = K^*/K^{*n}$.*

2.3.2 Quelques résultats locaux

Dans ce paragraphe K désigne une extension finie de $\mathbf{Q}_p$. Notons $\hat{\mathbf{Z}} = \Pi_p \mathbf{Z}_p$. D'après la théorie du corps de classes locale, le groupe de Galois $G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ de K^{ab} la limite projective des extensions abeliennes E/K dans $\overline{K}$: $G_K^{\mathrm{ab}} \simeq \hat{\mathbf{Z}} \times \mathcal{O}_K^*$. Ainsi

Proposition 2.3.6 *Soit K une extension finie de $\mathbf{Q}_p$*
i. $H^0(G_K, \mu_n) = \mu_n \cap K$,
ii. $H^1(G_K, \mu_n) = K^*/(K^*)^n$,
iii. $H^2(G_K, \mu_n) = \mathbf{Z}/n\mathbf{Z}$,
iv. $H^i(G_K, \mu_n) = 0$, $i \geq 3$.

Remarque 2.3.7 *Soit K une extension finie de $\mathbf{Q}_p$ et A est un G_K-module fini, alors on peut également montrer que $H^n(G_K, A)$ est fini pour tout $n \geq 0$.*

Nous disposons du résultat de dualité de Tate (admis).

Théorème 2.3.8 *Soit K une extension finie de $\mathbf{Q}_p$, A un G_K-module fini de cardinal n et $A' = \mathrm{Hom}(A, \mu_n)$ (le groupe A' est muni d'une action de G_K via $(ga^*)(a) = g(a^*(g^{-1}a))$.) Alors pour $0 \leq i \leq 2$, le cup-produit induit un accouplement parfait*

$$H^i(G_K, A) \times H^{2-i}(G_K, A') \to H^2(G_K, \mu_n) = \mathbf{Z}/n\mathbf{Z}.$$

Ce résultat de dualité local est essentiel, non seulement pour déterminer la structure des groupes de Galois locaux mais aussi pour établir le lien entre cohomologie locale et globale. D'après l'étude de la cohomologie des pro-p-groupes et grâce à la dualité de Tate, pour K extension finie de $\mathbf{Q}_p$ de degré d, on dispose d'une présentation par générateurs et relations de $G_K(p) = \mathrm{Gal}(K(p)/K)$ pour $K(p)$ la plus grande extension galoisienne de K dans $\overline{K}$ dont le groupe de Galois soit un pro-p-groupe.

Corollaire 2.3.9 *Soit q la plus grande puissance de p telle que K contienne les racines q-ièmes de l'unité.*
Si K ne contient pas les racines p-ièmes de l'unité ($q = 1$), $G_K(p)$ est un pro-p-groupe libre à $d+1$ générateurs.
Si $q \geq 2$, le groupe $G_K(p)$ est un groupe de Demushkin d'invariants $(d+2, q)$. En particulier si $q \geq 3$, $G_K(p)$ est défini par $d+2$ générateurs liés par la relation

$$x_1^q [x_1, x_2] \cdots [x_{d+1}, x_{d+2}] = 1$$

2.3.3 Théorème de Poitou-Tate

On dispose enfin de résultats fins de cohomologie galoisienne permettant de comparer la cohomologie des groupes locaux et globaux. On présente ici sans preuve la suite exacte de Poitou-Tate (voir [Mi]).

Notons K un corps de nombres algébriques, i.e. une extension finie de $\mathbf{Q}$. Une place de K est une classe d'équivalence de valeurs absolues de K; l'ensemble des places est noté V. Si $v \in V$, le complété de K pour la topologie associée à v est noté K_v ; si v est archimédienne, K_v est isomorphe à $\mathbf{R}$ ou $\mathcal{C}$; sinon, K_v est un corps p-adique.
Il est souvent utile pour les applications de travailler non plus avec le groupe de Galois absolu G_K mais avec des quotients G_S associés à des sous-ensembles non vides de V. Soit $S \subset V$ contenant toutes les places archimédiennes, K_S la plus grande extension de K incluse dans une clotûre algébrique $\bar{K}$ fixée de K. On pose $G_S = \mathrm{Gal}(K_S/K)$.

Si $v \in S$, on note $G_v \subset G_K$ le sous-groupe de décomposition en v, il s'identifie au groupe de Galois absolu du complété K_v. Pour tout G_S-module, on a donc des applications de restriction $\mathrm{Res} : H^i(G_S, M) \longrightarrow H^i(G_v, M)$ et donc des applications locales/globales :

$$H^i(G_S, M) \longrightarrow \oplus_{s \in S} H^i(G_v, M), i \geq 0$$

La suite exacte de Poitou-Tate insère ses applications dans une suite exacte, via des résultats de dualité de Tate.

Pour le corps des nombres réels, la dualité de Tate est beaucoup plus simple :

Proposition 2.3.10 *Soit A un $G_{\mathbf{R}}$-module fini. Notons $\hat{H}^0(G_{\mathbf{R}}, A) = A^{G_{\mathbf{R}}}/N_{G_{\mathbf{R}}}A$ et $\hat{H}^i(G_{\mathbf{R}}, A) = H^i(G_{\mathbf{R}}, A)$ pour $i = 1, 2$. Alors le cup-produit*

$$\hat{H}^i(G_{\mathbf{R}}, A) \times \hat{H}^{2-i}(G_{\mathbf{R}}, A') \to H^2(G_{\mathbf{R}}, \mathbf{C}^*) = \mathbf{Z}/2\mathbf{Z}$$

est une dualité parfaite de groupes finis de 2-torsion pour $0 \leq i \leq 2$.

Preuve : Le groupe de Galois $G_{\mathbf{R}}$ est d'ordre 2, on peut supposer que M est de torsion 2-primaire et par récurrence sur l'ordre de M, on se ramène au cas où M est simple, donc $A = \mathbf{Z}/2\mathbf{Z}$ avec action triviale ($A_{\mathbf{R}}^G \neq \{0\}$, équation aux classes). pour $A = \mathbf{Z}/2\mathbf{Z}$ tous les groupes de cohomologie considérés sont égaux à $\mathbf{Z}/2\mathbf{Z}$. ∎

Définition 2.3.11 *Soit K un corps de nombre et v une place de K. Nous notons $H^i(K_v, M)$ le groupe $H^i(G_v, M)$ sauf pour $i = 0$ et v archimédienne auquel cas $H^0(K_v, M)$ est nul si v est complexe et $M^{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}/N_{\mathrm{Gal}(\mathbf{C}/\mathbf{R})}M$ si v est réelle.*

Théorème 2.3.12 *Soit S un ensemble fini de places contenant les places archimédienne de K et les places v avec $v(|M|) \neq 0$. Soit M un G_S module fini. Alors*
i. la suite suivante est exacte :

$$0 \longrightarrow H^0(G_S, M) \longrightarrow \oplus_{s\in S} H^0(K_v, M) \longrightarrow H^2(G_S, M')^*$$
$$\longrightarrow H^1(G_S, M) \longrightarrow \oplus_{s\in S} H^1(K_v, M) \longrightarrow H^1(G_S, M')^*$$
$$\longrightarrow H^2(G_S, M) \longrightarrow \oplus_{s\in S} H^2(K_v, M) \longrightarrow H^0(G_S, M')^* \longrightarrow 0$$

où G^* désigne le dual au sens de Pontryagin du groupe localement compact G et $M' = \mathrm{Hom}(M, \mathbf{G}_m)$.
ii. Posons $Ш^1_S(G_k, M) = \ker(H^1(G_S, M) \to \oplus_{s\in S} H^1(K_v, M))$. Alors les groupes $Ш^1_S(G_k, M')$ et $Ш^1_S(G_k, M)$ sont finis et duaux.

Corollaire 2.3.13 *Soit S un ensemble fini de places (avec $p \neq 2$ si K a des places réelles) et A un G_S-module fini, alors les groupes $H^r(G_S, A)$ sont finis pour $0 \leq r \leq 2$.*

3 Foncteur de déformations

3.1 Définition du foncteur de déformations

Définition 3.1.1 *Une surjection $A' \to A$ dans $\mathcal{C}$ est dite abelienne si son noyau $\mathfrak{a}$ vérifie $\mathfrak{a}\mathcal{M}_{A'} = 0$. Si de plus $\mathfrak{a}$ est principal, la surjection (ou extension) est dite petite. Remarquons que toute extension abelienne dans $\mathcal{C}$ est composée de petites surjections.*

Définition 3.1.2 *Soit A un objet de $\widehat{\mathcal{C}}$. Une représentation de G sur A est un A-module libre V_A de type fini avec une action A-linéaire et continue de G (pour la topologie produit sur $V_A \simeq A^n$).*

Définition 3.1.3 *On note $V_{\mathbf{F}}$ un $\mathbf{F}$-espace vectoriel de dimension finie n muni d'une action continue de G. Soit A un object de $\widehat{\mathcal{C}}$. Un relèvement V_A de $V_{\mathbf{F}}$ à A est un A-module libre fini muni d'une action continue de G et d'un G-isomorphisme : $V_A \otimes_A \mathbf{F} \simeq V_{\mathbf{F}}$.*
Une déformation de $V_{\mathbf{F}}$ à A est une classe d'isomorphisme de relèvements de $V_{\mathbf{F}}$ à A.
Pour une $\mathbf{F}$-base β de $V_{\mathbf{F}}$ fixée, une déformation cadrée de V_A à A est une classe d'isomorphisme de relèvements de $V_{\mathbf{F}}$ à A munis de relèvements de la base β en une A-base de V_A.

Définition 3.1.4 *Le foncteur de déformations est le foncteur*

$$D_{V_{\mathbf{F}}} : \widehat{\mathcal{C}} \longrightarrow \mathrm{Ens}, A \to \{\textit{déformations de } V_{\mathbf{F}} \textit{ à } A\}$$

Le foncteur des déformations cadrées est le foncteur

$$D^{\square}_{V_{\mathbf{F}}} : \widehat{\mathcal{C}} \longrightarrow \mathrm{Ens}, A \to \{\textit{déformations cadrées de } V_{\mathbf{F}} \textit{ à } A\}.$$

Pour alléger les notations et en absence d'ambiguïté, nous notons D pour $D_{V_{\mathbf{F}}}$ et $D^{\square}$ pour $D^{\square}_{V_{\mathbf{F}}}$.

Remarque 3.1.5 *Le morphism $D^{\square} \longrightarrow D$ est formellement lisse (voir plus loin).*

Remarque 3.1.6 *Le choix d'une base β permet de voir $V_{\mathbf{F}}$ comme une représentation*

$$\bar{\rho} : G \to \mathrm{GL}_n(\mathbf{F}).$$

Ainsi $D^{\square}_{V_{\mathbf{F}}}$ est l'ensemble des relèvements de $\bar{\rho}$:

$$\rho : G \to \mathrm{GL}_n(A).$$

Par ailleurs, $D_{V_{\mathbf{F}}}(A)$ est l'ensemble de ces relèvements modulo $\ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbf{F}))$ *agissant par conjugaison. Dans ce contexte, nous notons $D_{\bar{\rho}}$ pour $D_{V_{\mathbf{F}}}$ et $D^{\square}_{\bar{\rho}}$ pour $D^{\square}_{V_{\mathbf{F}}}$.*

Le foncteur $F : \widehat{\mathcal{C}} \to \mathrm{Ens}$ est dit représentable s'il existe un couple $(R, \rho_{\mathrm{univ}})$ où R est un objet de $\widehat{\mathcal{C}}$ et $\rho_{\mathrm{univ}} \in F(R)$ tel que l'application canonique de foncteurs :

$$\rho_{\mathrm{univ}} : \mathrm{Hom}(R, \cdot) \to F$$

induise une équivalence. Le coupe $(R, \rho_{\mathrm{univ}})$ est alors unique à un unique isomorphisme. Le foncteur F admet alors une déformation universelle, l'anneau R est dit anneau de déformation universel et ρ_{univ} est dite déformation universelle.
Le foncteur F admet une déformation verselle s'il existe un objet R de $\widehat{\mathcal{C}}$ et un élément $\xi \in F(R)$ tel que le morphisme de foncteur $\xi : h_R \longrightarrow F$ est formellement lisse.
Ces définitions sont dûes à Mazur [Ma]: la déformation universelle est *uni*que, ce que n'est pas la déformation verselle.

Le critère de Schlessinger (§4) est un critère d'existence d'une déformation (uni)verselle. Pour le foncteur de déformation cadrée, la preuve est élémentaire.

Lemme 3.1.7 *Soit G un groupe fini d'unité e. Le foncteur $D^{\square}$ admet une déformation universelle.*

PREUVE : Soit $\Lambda[G,n]$ la Λ-algèbre commmutative donnée par :
- générateurs : X_{ij}^g, $g \in G, 1 \leq i,j \leq n$;
- relations : pour $g,h \in G$, $1 \leq i,j \leq n$

$X_{ij}^{gh} = \sum_{\ell=1}^n X_{i\ell}^g X_{\ell i}^h$,

$X_{ij}^e = \begin{cases} 1 & \text{si } i=j \\ 0 & \text{si } i \neq j \end{cases}$

Pour toute Λ-algèbre A, nous avons une bijection canonique

$$\mathrm{Hom}_{\Lambda-\mathrm{alg}}(\Lambda[G,n],A) \simeq \mathrm{Hom}_{gp}(G,\mathrm{GL}_n(A)), \quad f \longrightarrow \Big(g \mapsto (f(X_{ij}^g))_{i,j}\Big) \tag{1}$$

Par la bijection (1), l'homomorphisme $\bar{\rho} : G \longrightarrow \mathrm{GL}_n(\mathbf{F})$ donne un morphisme d'algèbres $\Lambda[G,n] \to \mathbf{F}$. Son noyau est un idéal maximal $\mathfrak{m}_{\bar{\rho}}$. Soit $\tilde{R}$ la complétion de $\Lambda[G,n]$ par rapport à $\mathfrak{m}_{\bar{\rho}}$. Alors $\tilde{R}$ est un objet de $\widehat{\mathcal{C}}$. L'application canonique $\Lambda[G,n] \longrightarrow \tilde{R}$ donne un morphisme $\tilde{\rho} \in D^{\square}_{V_{\mathbf{F}}}(\tilde{R})$. Soit A un object de $\widehat{\mathcal{C}}$ et $\rho \in D^{\square}_{V_{\mathbf{F}}}(A)$. Par (1), il existe un unique morphisme de Λ-algèbres $f : \Lambda[G,n] \longrightarrow A$ tel que $\rho_f = \rho$ et nous avons $f(\mathfrak{m}_{\bar{\rho}}) \subset \mathfrak{m}_A$. L'application $\Lambda[G,n] \to A \to A/\mathfrak{m}_A^m$ est continue pour la topologie $\mathfrak{m}_{\bar{\rho}}$-adique sur $\Lambda[G,n]$ pour tout $m \geq 0$. Nous obtenons ainsi un homomorphisme de Λ-algèbres $\tilde{f} : \tilde{R} \to A$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} G & \longrightarrow^{\tilde{\rho}} & \mathrm{GL}_n(\tilde{R}) \\ \downarrow^{\mathrm{Id}} & & \downarrow^{\tilde{f}} \\ G & \longrightarrow^{\rho} & \mathrm{GL}_n(A) \end{array}$$

Comme les éléments $\tilde{f}(X_{ij}^g)$ sont déterminés par ρ, et les X_{ij}^g engendrent une sous-Λ-algèbre dense de $\tilde{R}$, l'application $\tilde{f}$ est uniquement déterminée par la condition de continuité et la commutativité du diagramme.
L'unicité du couple universel $(\tilde{R},\tilde{\rho})$ se déduit enfin de la propriété universelle. ∎

Proposition 3.1.8 *Supposons que G satisfait la propriété de finitude (Φ_p). Alors le foncteur $D^{\square}$ admet une déformation universelle.*

PREUVE : Comme G est profini, nous pouvons écrire $G = \lim_{\leftarrow} H$, où H parcourt les quotients discrets de G tels que la représentation $\bar{\rho} : G \longrightarrow \mathrm{GL}_n(\mathbf{F})$ se factorise à travers l'application $\bar{\rho}_H : H \longrightarrow \mathrm{GL}_n(\mathbf{F})$. Pour un tel groupe fini H, le lemme 3.1.7 donne un anneau $\tilde{R}_H$ et un homomorphisme de groupe $\tilde{\rho}_H \in D^{\square}_{\bar{\rho}_H}(\tilde{R}_H)$. Les anneaux $(\tilde{R}_H)_H$ dans $\widehat{\mathcal{C}}$ forment un système projectif (qui admet une limite dans $\hat{\mathcal{C}}$ car G satisfait (Φ_p) ; on pourrait perdre la propriété "noetherien" par passage à la limite). Nous définissons alors $\tilde{R} = \lim_{\leftarrow} \tilde{R}_H$. Montrons que

$\tilde{R}$ est l'objet universel. Pour A objet de $\widehat{\mathcal{C}}$, écrivons $A = \lim_{\leftarrow} A_i$ où A_i quotients discrets artiniens. Nous avons les isomorphismes canoniques :

$$D_{\bar{\rho}}^{\square}(A) = \lim_{\rightarrow i} D_{\bar{\rho}}^{\square}(A_i) = \lim_{\rightarrow i} \lim_{\leftarrow H} D_{\bar{\rho}_H}^{\square}(A_i)$$

$$= \lim_{\rightarrow i} \lim_{\leftarrow H} \mathrm{Hom}_{\Lambda-\mathrm{alg}}(\tilde{R}_H, A_i) = \lim_{\rightarrow i} \mathrm{Hom}_{\Lambda-\mathrm{alg}}(\tilde{R}, A_i) = \mathrm{Hom}_{\Lambda-\mathrm{alg}}(\tilde{R}, A).$$

■

Remarque 3.1.9 *Si $F : \widehat{\mathcal{C}} \longrightarrow$ Ens est représentable par R object de $\widehat{\mathcal{C}}$, alors,*
i. $F(\mathbf{F}) = \mathrm{Hom}_{W(\mathbf{F})}(R, \mathbf{F})$ est réduit à un élément,
ii. F commute avec le produit fibré dans $\mathcal{C}$,
iii. $F(A) \longrightarrow \mathrm{proj\,lim}\, F(A/\mathcal{M}_A^n)$ est bijective,
iv. $F(\mathbf{F}[\varepsilon]) = \mathrm{Hom}(\mathcal{M}_R/(\mathcal{M}_R^2, p), \mathbf{F})$ est un espace vectoriel de dimension d, où d est le nombre minimal de générateurs de R.

4 Critère de Schlessinger

L'objet de cette partie est d'établir l'existence de la déformation (uni)verselle du foncteur de déformation. Précisément

Théorème 4.0.10 *Le foncteur de déformation $D_{V_{\mathbf{F}}}$ admet une déformation verselle. Si, de plus $End_{\mathbf{F}[G]} V_{\mathbf{F}} = \mathbf{F}$, la déformation verselle est universelle.*

Remarque 4.0.11 *Kisin a donné une preuve directe de la pro-représentatibilité du foncteur $D_{V_{\mathbf{F}}}$ en identifiant le spectre formel* Spf $R_{V_{\mathbf{F}}}$ *au quotient* Spf $R_{V_{\mathbf{F}}}^{\square}/\widehat{\mathrm{PGL}_n}$ *où $\widehat{PGL}_n$ est la complétion du groupe* PGL_n *sur $W(\mathbf{F})$ le long de sa section identité ([Ki]).*

4.1 Énoncé

Rappelons le théorème 2.1.1 [Sc], dit critère de Schlessinger :

Théorème 4.1.1 *Soit un foncteur $F : \widehat{\mathcal{C}} \longrightarrow$ Ens tel que $F(k) = \{*\}$ (un singleton). Pour deux morphismes dans $\mathcal{C}$, $u_1 : A' \to A$, $u_2 : A'' \to A$, considérons*

$$\theta : F(A' \times_A A'') \longrightarrow F(A') \times_{F(A)} F(A'')$$

le morphisme canonique.
1. Le foncteur F admet une déformation verselle si et seulement si F vérifie les propriétés

suivantes :
H1. Pour tout $u_2 : A'' \to A$, petite extension, θ est surjectif ;
H2. si $A = \mathbf{F}$, $A'' = \mathbf{F}[\varepsilon]$, alors θ est bijectif ;
H3. $\dim_{\mathbf{F}} F(\mathbf{F}[\varepsilon]) < \infty$.
2. Le foncteur F admet une déformation universelle si et seulement si F vérifie les propriétés H1. H2. H3. et
H4. si $u_1 : A' \to A$ est une petite extension, alors

$$\theta : F(A' \times_A A') \longrightarrow F(A') \times_{F(A)} F(A')$$

est bijective.

Remarque 4.1.2 *Schéma grossier de la preuve de Schlessinger: (preuve détaillée plus loin)*
La condition H2. permet de munir $F(\mathbf{F}[\varepsilon])$ d'une structure de $\mathbf{F}$-espace vectoriel. On note $d = \dim_{\mathbf{F}} F(\mathbf{F}[\varepsilon])$. Posons $S = \Lambda[[X_1, \dots, X_d]]$ et $\mathfrak{m}_S$ son idéal maximal. On montre que l'anneau (uni)versel de déformation est de la forme S/J pour un idéal J de relations construit par recurrence.
On pose d'abord $J_1 = \mathfrak{m}_S^2 + (\mu)$ (où μ est une uniformisante de Λ) et $R_1 = S/J_1$. Alors, grâce à l'hypothèse H1., on montre l'existence d'une déformation $\xi_1 \in F(\mathbf{F}[\varepsilon])$ qui induit un isomorphisme $\mathrm{Hom}_{\mathcal{C}}(R_1, \mathbf{F}[\varepsilon]) \to F(\mathbf{F}[\varepsilon])$.
Supposons que l'on ait défini un couple (R_q, ξ_q) avec $R_q = S/J_q$ (pour un idéal convenable J_q de S) et $\xi_q \in F(R_q)$ (hypothèse d'universalité à préciser). D'après H1, il existe un idéal J_{q+1} de S tel que $\mathfrak{m}_S J_q \subset J_{q+1} \subset J_q$ et un relèvement $\xi_{q+1} \in F(S/J_{q+1})$ de ξ_q (hypothèse d'universalité à préciser).
Enfin, on pose $J = \cap_{q \in \mathbf{N}} J_q$ et $R = S/J$ et on vérifie que $(R, \lim_{\leftarrow q \in \mathbf{N}} \xi_q)$ est une déformation verselle (resp. universelle si F satisfait H4.)

La preuve du critère de Schlessinger montre que l'anneau R admet une présentation minimale de la forme

$$R = \Lambda[[t_1, \dots, t_d]]/I$$

avec $d = \dim_{\mathbf{F}} F(\mathbf{F}[\varepsilon])$. Pour décrire R, il suffit donc de déterminer la dimension de l'espace tangent et de décrire l'idéal des relations I, ce qui est difficile en général.

4.2 Espace tangent

Pour connaitre la dimension de l'espace tangent, nous l'identifions à un groupe de cohomologie. Considérons le foncteur $D_{\bar{\rho}}$ de déformation de la représentation $\bar{\rho} : G \to \mathrm{GL}(V_{\mathbf{F}}) = \mathrm{GL}_n(\mathbf{F})$

pour une base β fixée. Pour déterminer l'espace tangent $D_{\bar\rho}(\mathbf{F}[\varepsilon])$, introduisons la suite exacte suivante

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Id}+\varepsilon\Theta & \longrightarrow & \mathrm{GL}_n(\mathbf{F}[\varepsilon]) & \longrightarrow & \mathrm{GL}_n(\mathbf{F}) \longrightarrow 0 \\ & & & & & & \uparrow{\scriptstyle \bar\rho} \\ & & & & & & G \end{array}$$

Le noyau $\mathrm{Id}+\varepsilon\Theta$ est un sous-groupe distingué, muni par composition d'une action de G. Précisement, Θ est la représentation adjointe $\mathrm{ad}\,\bar\rho$ (noté également suivant le contexte $\mathrm{ad}\,V_{\mathbf{F}}$), c'est-à-dire $M_n(\mathbf{F})$ avec l'action du groupe de Galois G définie par conjugaison par $\bar\rho$ ($gA = \bar\rho(g)^{-1}A\bar\rho(g)$). Un relèvement ρ de $\bar\rho$ à $\mathrm{GL}_n(\mathbf{F}[\varepsilon])$ s'écrit

$$\rho = \bar\rho \circ (\mathrm{Id}+\varepsilon c) \text{ avec } c : G \to \mathrm{ad}\,\bar\rho.$$

La condition de composition $\rho(gh) = \rho(g)\rho(h)$, $g, h \in G$ permet d'identifier c à un cocyle $c \in Z^1(G, \mathrm{ad}\,\bar\rho)$. En effet

$$\rho(gh) = \bar\rho(gh) \circ (\mathrm{Id}+\varepsilon c(gh)) \;\; \rho(g)\rho(h) = \bar\rho(g) \circ (\mathrm{Id}+\varepsilon c(g))\bar\rho(h) \circ (\mathrm{Id}+\varepsilon c(h))$$

d'où $c(gh) = \bar\rho(h)^{-1}c(g)\bar\rho(h) + c(h)$, $\forall g, h \in G$ et $c \in Z^1(G, \mathrm{ad}\,\bar\rho)$. Enfin en considérant la classe de conjugaison de ρ, nous obtenons

$$\rho = \bar\rho \circ (\mathrm{Id}+\varepsilon c) \equiv \rho' = \bar\rho \circ (\mathrm{Id}+\varepsilon c')$$

si et seulement si il existe $P \in M_n(\mathbf{F})$ telle que $\rho = (Id + \varepsilon P)\rho'(Id - \varepsilon P)$ i.e. c et c' diffèrent d'un cobord : $c = c' + \bar\rho^{-1}P\bar\rho - P$.

Lemme 4.2.1 *On a un isomorphisme canonique*

$$D(\mathbf{F}[\varepsilon]) \simeq H^1(G, \mathrm{ad}\,\bar\rho).$$

Si, de plus, G satisfait la condition de finitude (Φ_p), alors $D_{V_{\mathbf{F}}}(\mathbf{F}[\varepsilon])$ est un $\mathbf{F}$-espace vectoriel de dimension finie et

$$\dim_{\mathbf{F}} D^{\square}_{V_{\mathbf{F}}}(\mathbf{F}[\varepsilon]) = \dim_{\mathbf{F}} D_{V_{\mathbf{F}}}(\mathbf{F}[\varepsilon]) + n^2 - \dim_{\mathbf{F}}(\mathrm{ad}\,\bar\rho)^G = n^2 + \dim_{\mathbf{F}} H^1(G, \mathrm{ad}\,\bar\rho) - \dim_{\mathbf{F}} H^0(G, \mathrm{ad}\,\bar\rho)$$

Preuve : Supposons que G satisfait la condition (Φ_p). Soit $G' = \ker\bar\rho$. C'est un sous-groupe fermé de G. La suite d'inflation restriction induit la suite exacte :

$$0 \longrightarrow H^1(G/G', \mathrm{ad}\,\bar\rho) \to H^1(G, \mathrm{ad}\,\bar\rho) \longrightarrow \mathrm{Hom}(G', \mathbf{F}_p) \otimes_{\mathbf{F}_p} \mathrm{ad}\,\bar\rho)^{G/G'}.$$

Le terme de gauche est fini car G/G' et $\mathrm{ad}\,\bar\rho$ sont finis. Le terme de droite est fini car la condition (Φ_p) est satisfaite.

Établissons l'égalité concernant les dimensions des espaces tangents. Fixons une déformation $V_{\mathbf{F}[\varepsilon]}$ de $V_{\mathbf{F}}$ à $\mathbf{F}([\varepsilon])$. L'ensemble des $\mathbf{F}([\varepsilon])$-bases de $V_{\mathbf{F}[\varepsilon]}$ relevant une base fixée de $V_{\mathbf{F}}$ est un $\mathbf{F}$-espace vectoriel de dimension n^2. Soient β', β'' deux telles bases relevées. Alors on a un isomorphisme de déformations cadrées

$$(V_{\mathbf{F}[\varepsilon]}, \beta'') \simeq (V_{\mathbf{F}[\varepsilon]}, \beta')$$

si et seulement si il existe un automorphisme de $V_{\mathbf{F}[\varepsilon]}$ qui se réduit sur l'identité modulo ε et qui envoie β'' sur β'. Par conséquent les fibres de

$$D^{\square}_{V_{\mathbf{F}}}(\mathbf{F}[\varepsilon]) \to D_{V_{\mathbf{F}}}(\mathbf{F}[\varepsilon])$$

sont un espace homogènes sous $\operatorname{ad}\bar{\rho}/(\operatorname{ad}\bar{\rho})^G$. ∎

Définition 4.2.2 *Un morphisme $\phi : D' \to D$ de foncteurs de $\mathcal{C} \to$ Ens est dit formellement lisse si pour toute surjection $A \to A'$ de $\mathcal{C}$, l'application $D'(A) \longrightarrow D'(A') \times_{D(A')} D(A)$ est surjective.*

Corollaire 4.2.3 *La transformation naturelle $D^{\square}_{V_{\mathbf{F}}} \longrightarrow D_{V_{\mathbf{F}}} : (V_A, \beta_A) \mapsto V_A$ est formellement lisse. Ainsi si $R_{V_{\mathbf{F}}}$ est représentable alors $R^{\square}_{V_{\mathbf{F}}}$ est un anneau de séries formelles sur $R_{V_{\mathbf{F}}}$ de dimension relative $d^2 - \dim_{\mathbf{F}} H^0(G, \operatorname{ad}\bar{\rho})$.*

4.3 Identification des obstructions

Préciser l'idéal des relations, c'est effectuer l'analyse des obstructions à relever $[\rho] \in D_{V_{\mathbf{F}}}(A)$ en $[\rho'] \in D_{V_{\mathbf{F}}}(A')$ pour $\pi : A' \to A$ une extension abélienne de noyau I de $\mathcal{C}$. Comme $\mathcal{M}_{A'} I = 0$, l'idéal I est naturellement muni d'une structure de $\mathbf{F}$-espace vectoriel. Considérons l'extension

$$\begin{array}{ccccccc} 0 \longrightarrow N_{A'/A} & \longrightarrow & \mathrm{GL}_n(A') & \longrightarrow & \mathrm{GL}_n(A) \to 0 \\ & & & & \uparrow \rho \\ & & & & G \end{array}$$

avec $N_{A'/A} \simeq I \otimes_{\mathbf{F}} \operatorname{ad}\bar{\rho}$, la structure de G-module étant triviale sur I. Supposons que ρ soit un représentant d'une déformation de $\bar{\rho}$ à A. Pour relever ρ à A', pour tout $\sigma \in G$, nous relevons ρ_σ en $\rho^*_\sigma \in \mathrm{GL}_n(A')$. L'application ρ^* ainsi définie n'est pas forcément un morphisme de groupes. L'égalité

$$\rho^*_\sigma \rho^*_\tau = \varphi(\sigma, \tau) \rho^*_{\sigma\tau}, \quad \sigma, \tau \in G$$

définit un élément $\varphi(\sigma, \tau) \in N_{A'/A}$. Une déformation de ρ à A' est une classe d'équivalence de tels éléments ρ^*, donc (faire le calcul !) $\{\varphi(\sigma, \tau)\}$ représente une classe d'équivalence

$\mathrm{obs}_\rho(\pi) \in H^2(G, \mathrm{ad}\,\bar{\rho}) \otimes_{\mathbf{F}} I$, dite classe d'obstruction à relever ρ à A'. Rappelons que toute extension abélienne s'obtient par composition de petites extensions. Nous pouvons alors définir le groupe des obstructions :

Définition 4.3.1 *Le groupe des obstructions* $\mathrm{Obs}(\bar{\rho})$ *est le sous-groupe de* $H^2(G, \mathrm{ad}\,\bar{\rho})$ *engendré par tous les éléments* $\mathrm{obs}_\rho(\pi)$ *avec* ρ *représentant d'une déformation de* $\bar{\rho}$ *à un objet* A *de* $\mathcal{C}$ *et* $\pi : A' \to A$ *petite extension de* $\mathcal{C}$.

Remarque 4.3.2 *Si le groupe de 2-cohomologie* $H^2(G, \mathrm{ad}\,\bar{\rho})$ *associé au problème de déformation est nul, le problème de déformation est dit cohomologiquement non obstrué. En effet dans ce cas, le groupe des obstructions est réduit à 0, le problème de déformation est non obstrué, l'anneau de déformation (uni)versel est un anneau de séries formelles* $\Lambda[[X_1, \ldots, X_d]]$ *à* d *variables.*

Rappelons deux lemmes utiles de fonctorialité des obstructions.

Lemme 4.3.3 *Soit le diagramme de* $\mathcal{C}$

$$\begin{array}{ccc} A' & \xrightarrow{u'} & B' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ A & \xrightarrow{u} & B \end{array}$$

où π, π' *sont des extensions abéliennes de noyaux respectifs* I, I'. *Soit* ρ *un relèvement de* $\bar{\rho}$ *à* A. *Alors par l'application* $1 \otimes u' : H^2(G, \mathrm{ad}\,\bar{\rho}) \otimes_{\mathbf{F}} I \longrightarrow H^2(G, \mathrm{ad}\,\bar{\rho}) \otimes_{\mathbf{F}} I'$, *nous avons*

$$(1 \otimes u')(\mathrm{obs}_\rho(\pi)) = \mathrm{obs}_{u(\rho)}(\pi').$$

Lemme 4.3.4 *Soit* $\pi : A \longrightarrow B$ *une extension abélienne de noyau* I *et* J *un sous-*$\mathbf{F}$*-espace vectoriel de* I, *notons* $\pi' : A \longrightarrow C = A/J$ *et* $\pi'' : C \longrightarrow B$. *Soit* $[\rho] \in D_{\bar{\rho}}(B)$, *alors*

$$\pi'(\mathrm{obs}_\rho(\pi)) = \mathrm{obs}_\rho(\pi'').$$

4.4 Définition de la n-versalité

Nous rappelons dans ce paragraphe les notations et les définitions de [Vi].

Définition 4.4.1 *Soit* $n \geq 1$, *un objet* A *de* $\mathcal{C}$ *est dit d'ordre* $\leq n$ *si*

$$\mathfrak{m}_A^{n+1} = 0 = \mu\mathfrak{m}_A^{n-1} = 0$$

où μ *désigne une uniformisante de* Λ. *La catégorie* $\mathcal{C}_n$ *est la sous-catégorie pleine de* $\mathcal{C}$ *dont les objets sont d'ordre* $\leq n$.

Remarque 4.4.2 *Si A est un objet de $\mathcal{C}_n$, I idéal de A, alors A/I est un objet de $\mathcal{C}_n$. Donc si $u : A' \longrightarrow A$ est une surjection de $\mathcal{C}_n$, alors nous pouvons factoriser u en une succession de surjections élémentaires du type $v : C' \longrightarrow C$, avec C, C' objets de $\mathcal{C}_n$, $\mathcal{M}_{C'} \ker v = 0$ (v extension abélienne) ; nous pouvons imposer de plus $\dim_{\mathbf{F}} \ker v = 1$ (v petite extension).*

Définition 4.4.3 *Pour A objet de $\widehat{\mathcal{C}}$, nous définissons le tronqué d'ordre $\leq n$ de A, l'objet défini par*

$$\tau_{\leq n}(A) = A/(\mathfrak{m}_A^{n+1} + \mu\mathfrak{m}_A^{n-1}).$$

Exemple 4.4.4 *Les objets de $\mathcal{C}_1$ sont les objets A de $\widehat{\mathcal{C}}$ tels que $\mathcal{M}_A^2 = \mu A = 0$, i.e., $A = \mathbf{F} \oplus V$, $V = \mathcal{M}_A$ avec la structure d'idéal de carré nul. Ainsi la catégorie $\mathcal{C}_1$ est équivalente à la catégorie des $\mathbf{F}$-espaces vectoriels de dimension finie. Nous identifions ces deux catégories. Nous avons un isomorphisme fonctoriel*

$$D_{V_{\mathbf{F}}}(A) \xrightarrow{\sim} t_{D_{V_{\mathbf{F}}}} \otimes_{\mathbf{F}} V$$

où $t_{D_{V_{\mathbf{F}}}}$ est le $\mathbf{F}$-espace vectoriel tangent $D_{V_{\mathbf{F}}}(\mathbf{F}[\varepsilon])$. Cet isomorphisme est conséquence des axiomes de Schlessinger :

$$\dim_{\mathbf{F}} t_{D_{\mathbf{F}}} < \infty \text{ et } D_{\mathbf{F}}((\mathbf{F} \oplus V) \times_{\mathbf{F}} (\mathbf{F} \oplus W)) \longrightarrow^{\simeq} D_{\mathbf{F}}(\mathbf{F} \oplus V) \times D_{\mathbf{F}}(\mathbf{F} \oplus W)$$

pour V, W deux $\mathbf{F}$-espaces vectoriels. De plus, nous avons $t_{D_{\mathbf{F}}} \otimes V = \mathrm{Hom}(t^*_{D_{V_{\mathbf{F}}}}, V)$ pour $t^*_{D_{V_{\mathbf{F}}}}$ $\mathbf{F}$-espace vectoriel dual de $t_{D_{V_{\mathbf{F}}}}$.
Si A est un objet de $\mathcal{C}$,

$$\tau_{\leq 1}(A) = A/\mathcal{M}_A^2 + \mu A) \simeq \mathbf{F} \oplus t_A^*$$

avec t_A^* espace co-tangent à A, $t_A^* = \mathcal{M}_A/(\mathcal{M}_A^2 + \mu A)$.

Définition 4.4.5 *Si $[\rho] \in D_{V_{\mathbf{F}}}(A)$ avec A objet de $\mathcal{C}$, nous notons encore $\tau_{\leq n}([\rho])$ la classe d'équivalence de l'image de ρ par $\tau_{\leq n}$.*
Soit R objet de $\widehat{\mathcal{C}}$ et $\xi \in D_{V_{\mathbf{F}}}(R)$. Pour $n \geq 1$, le coupe (R, ξ) est dit n-versel si
- le morphisme de $\mathcal{C}_n$, $\tau_{\leq n}(\xi) : h_{\tau_{\leq n}(R)} \to D_{V_{\mathbf{F}}}$ est lisse,
- et $(\tau_{\leq 1}(R), \tau_{\leq 1}(\xi))$ est la déformation 1-universelle de $D_{V_{\mathbf{F}}}$; ce qui signifie que si A est un objet de $\mathcal{C}_1$ et $\alpha \in D_{V_{\mathbf{F}}}(A)$, le morphisme $f : \tau_{\leq 1}(R) \longrightarrow A$ tel que $D_{V_{\mathbf{F}}}(f)(\tau_{\leq 1}(\xi)) = \alpha$ est déterminé de manière unique.

Exemple 4.4.6 *Reprenons l'exemple 4.4.4. Soit ξ_1 l'élément de $D_{V_{\mathbf{F}}}(t^*_{D_{V_{\mathbf{F}}}}) \simeq \mathrm{Hom}(t_{D_{V_{\mathbf{F}}}}, t_{D_{V_{\mathbf{F}}}})$ correspondant à $\mathrm{Id}_{t_{D_{V_{\mathbf{F}}}}}$. Ainsi $(\mathbf{F} \oplus t_{D_{V_{\mathbf{F}}}}, \xi_1)$ est un couple 1-versel.*

Remarque 4.4.7 *Le tronqué d'ordre n d'un anneau R de n-versel est unique à isomorphisme près. En effet, soit (R,ξ) et (R',ξ') deux couples n-versels. Par n-versalité, il existe des morphismes*

$$f : \tau_{\leq n}(R) \longrightarrow \tau_{\leq n}(R'), f' : \tau_{\leq n}(R') \longrightarrow \tau_{\leq n}(R)$$

qui induisent des bijections au niveau des espaces tangents. Ainsi pour $R_n = \tau_{\leq n}(R)$ $g = f' \circ f : R_n \longrightarrow R_n$ est un homomorphisme avec $g^* : \mathcal{M}_{R_n}/\mathcal{M}_{R_n}^2 \longrightarrow \mathcal{M}_{R_n}/\mathcal{M}_{R_n}^2$ surjective, donc $\mathcal{M}_{R_n}^k/\mathcal{M}_{R_n}^{k+1} \longrightarrow \mathcal{M}_{R_n}^k/\mathcal{M}_{R_n}^{k+1}$ est surjective et g est un isomorphisme. Ainsi $f \circ f'$, $f' \circ f$, f et f' sont des isomorphismes.

Lemme 4.4.8 *Soit $n \geq 1$.*
i. Le coupe (R,ξ) est n-versel si et seulement si $(\tau_{\leq n}(R), \tau_{\leq n}(\xi))$ est n-versel.
ii. Si $m \leq n$ et (R,ξ) est n-versel, alors il est m-versel.

PREUVE : Si A est un objet de $\mathcal{C}_n$, tout morphisme $u : R \to A$ se factorise par $\tau_{\leq n}(R)$ car $u(\mathcal{M}_R^{n+1} + \mu\mathcal{M}_R^{n-1}) = 0$. La propriété *ii* s'obtient alors en observant que $\tau_{\leq 1}(\tau_{\leq \ell}(R)) = \tau_{\leq 1}(R)$ pour tout $\ell \geq 1$. ∎

4.5 Construction de l'idéal des relations

Nous présentons ici l'adapation à la caractéristique mixte de la preuve détaillée de Vistoli [Vi] du critère de Schlessinger pour un foncteur de déformation. Posons $S = \Lambda[[t_1, \ldots, t_d]]$ où $(t_i)_{1\leq i\leq d}$ est une base de $t^*_{D_{V_{\mathbf{F}}}}$. Notons $r = \dim_{\mathbf{F}} H^2(G, V_{\mathbf{F}})$. Soit $\mathcal{N} = \mu S + \sum_{i=1}^d t_i S$ l'idéal maximal de S. Posons $J_0 = S$, $I_1 = J_1 = \mathcal{N}^2 + \mu S$ et $J_n = \mathcal{N}^{n-1} J_1$ pour $n \geq 2$. Ainsi

$$J_0/J_1 \simeq \mathbf{F}[[t_1, \ldots, t_d]]/(t_1, \ldots, t_d)^2 \simeq \oplus_{i=1}^d \mathbf{F} t_i \simeq t^*_{D_{V_{\mathbf{F}}}} \text{ et } J_n = \mathcal{N}^{n+1} + \mu\mathcal{N}^{n-1}.$$

Plus généralement, nous avons

Lemme 4.5.1 *Pour tout $\ell \geq 2$,*

$$\frac{J_{\ell-1}}{J_\ell} \simeq \mathrm{Sym}^\ell(t^*_{D_{V_{\mathbf{F}}}}) \oplus \Big(\oplus_{j=1}^{\ell-1} \frac{\mu^j}{\mu^{j+1}} \otimes \mathrm{Sym}^{\ell-j-1}(t^*_{D_{V_{\mathbf{F}}}}) \Big).$$

PREUVE : Par définition, nous avons

$$\frac{J_{\ell-1}}{J_\ell} = \frac{\mathcal{N}^\ell + \mu\mathcal{N}^{\ell-2}}{\mathcal{N}^{\ell+1} + \mu\mathcal{N}^{\ell-1}}.$$

Un élément ϕ de $\mathcal{N}^\ell$ s'écrit

$$\phi = \sum_{i=0}^{\ell} \mu^{\ell-i} g_i(t), \text{ avec } g_i(t) \in (t_1, \dots, t_d)^i$$

où t désigne le système de variables $t_1, \dots, t_d$. Ainsi pour $i \leq \ell - 1$, $\mu^{\ell-i} g_i(t) \in \mu\mathcal{N}^{\ell-1}$, donc modulo $\mathcal{N}^{\ell+1} + \mu\mathcal{N}^{\ell-1}$ un élément de $\mathcal{N}^\ell + \mu\mathcal{N}^{\ell-2}$ s'écrit

$$\bar{\phi} = f_\ell(t) + \mu\Big(\sum_{j=1}^{\ell-1} \mu^{j-1} f_{\ell-j-1}(t) \Big)$$

avec $f_{\ell-j-1}(t) \in (t_1, \dots, t_d)^{\ell-j-1}$ et $f_\ell(t) = g_\ell(t) \in (t_1, \dots, t_d)^\ell$. Nous pouvons alors définir une application

$$\frac{J_{\ell-1}}{J_\ell} \longrightarrow \mathrm{Sym}^\ell(t^*_{D_{V_{\mathbf{F}}}}) \oplus \Big(\oplus_{j=1}^{\ell-1} \frac{\mu^j}{\mu^{j+1}} \otimes \mathrm{Sym}^{\ell-j-1}(t^*_{D_{V_{\mathbf{F}}}}) \Big),\ \bar{\phi} \mapsto (\overline{f}_\ell, \{\overline{f}_{\ell-j-1}\})$$

où $\bar{f}_i$ est f_i dont nous prenons la classe modulo μS des coefficients, puis la classe de la série obtenue modulo $(t_1, \dots, t_d)^{i+1}$. Cette application est bien définie et bijective : pour cela, il suffit de prendre deux écritures différentes de $\bar{\phi}$

$$\bar{\phi} = f_\ell(t) + \sum_{j=1}^{\ell-1} \mu^j f_{\ell-j-1}(t) = f'_\ell(t) + \Big(\sum_{j=1}^{\ell-1} \mu^j f'_{\ell-j-1}(t) \Big).$$

Puis en prenant successivement les images de ces égalités modulo μS, $(t_1, \dots, t_d)^i$ pour i variant de $\ell + 1$ à 1, nous constatons que l'image de $\bar{\phi}$ est définie de manière unique. ∎

Le lemme 4.5.1 est la principale modification nécessaire à l'adaptation des résultats de Vistoli ([Vi] §7) au cadre des déformations en caractéristique mixte. Nous rappelons dans ce paragraphe les différentes étapes de sa démonstration qui sont encore valables ici.
Pour tout $n \geq 1$, nous allons construire par récurrence une suite de couples (R_n, ξ_n) avec $R_n = S/I_n$ où $I_n = J_n + < F_1^{(n)}, \dots, F_r^{(n)} >$ pour $F_j^{(n)} \in S$, $1 \leq j \leq r$ et $\xi_n \in D_{V_{\mathbf{F}}}(R_n)$ tels que
- par la surjection $S \to S/J_{n-1}$, $\tau_{\leq n-1}(F_j^{(n)})$ et $F_j^{(n-1)}$ ont les mêmes images pour tout $1 \leq j \leq r$,
- (R_n, ξ_n) est n-versel et $D_{V_{\mathbf{F}}}(\tau_{\leq n-1})(\xi_n) = \xi_{n-1}$.
Pour $n = 1$, nous avons vu dans l'exemple 4.4.6 que $R_1 = \mathbf{F} \oplus t^*_{D_{V_{\mathbf{F}}}} = S/J_1$ et ξ_1 définissent un couple 1-versel. Posons $F_j^{(0)} = 0$, $1 \leq j \leq r$.
Supposons avoir construit (R_n, ξ_n) n-versel comme indiqué. Considérons l'extension abélienne

$$\pi_n : R_n^* = S/\mathcal{N}I_n \to R_n = S/I_n.$$

L'obstruction au relèvement de ξ_n à R_n^* est un élément de $H^2(G, V_{\mathbf{F}}) \otimes_{\mathbf{F}} I_n/\mathcal{N}I_n$. Fixons une $\mathbf{F}$-base $(w_1, \ldots, w_r)$ de $H^2(G, \operatorname{ad} V_{\mathbf{F}})$; ainsi l'obstruction s'écrit

$$\operatorname{obs}_{\xi_n}(\pi_n) = \sum_{j=1}^{r} w_j \otimes u_j, \text{ avec } u_j \in I_n/\mathcal{N}I_n, 1 \leq j \leq r.$$

Nous posons alors $I_{n+1} = \mathcal{N}I_n + < u_j >$ et $R_{n+1} = S/I_{n+1}$. Constatons que $J_{n+1} \subset J_n\mathcal{N} \subset I_{n+1}$, donc R_{n+1} est un objet de $\mathcal{C}_{n+1}$. Par fonctorialité des obstructions, ξ_n se relève à R_{n+1} ; soit ξ_{n+1} un tel relèvement.

Lemme 4.5.2 *Supposons (R_n, ξ_n) n-versel. Soit A un objet de $\mathcal{C}_n$, $\alpha \in D_{V_{\mathbf{F}}}(A)$ et une surjection $\mathfrak{p} : A \to R_n$ telle que $D_{V_{\mathbf{F}}}(\mathfrak{p})(\alpha) = \xi_n$ et $\mathfrak{p}$ induit un isomorphisme $d\mathfrak{p} : t_A^* \simeq t_{R_n}^*$. Alors $\mathfrak{p}$ est un isomorphisme.*

Preuve : Par versalité de (R_n, ξ_n), il existe $\sigma : R_n \to A$ avec $D_{V_{\mathbf{F}}}(\sigma)(\xi_n) = \alpha$. Ainsi pour $\mathfrak{q} = \mathfrak{p} \circ \sigma : R_n \to R_n$ nous avons $D_{V_{\mathbf{F}}}(\mathfrak{q})(\xi_n) = \xi_n$. Par unicité de l'anneau n-versel à isomorphisme près, $\mathfrak{q}$ est un isomorphisme et comme $d\mathfrak{p}$ en est un, $d\sigma$ aussi. Ainsi $d\sigma$ est surjectif, σ est surjectif donc bijectif et $\mathfrak{p}$ est bijectif. ∎

Lemme 4.5.3 *Nous avons $I_n = J_n + I_{n+1}$.*

Preuve : Le morphisme $R_{n+1} \to R_n = S/I_n$ se factorise à travers $A = S/(J_n + I_{n+1})$

$$R_{n+1} \xrightarrow{\mathfrak{q}} A \xrightarrow{\mathfrak{p}} R_n.$$

Or A est un objet de $\mathcal{C}_n$ et ξ_n se relève à R_{n+1} donc à A. Par conséquent, pour $D_{V_{\mathbf{F}}}(\mathfrak{q})(\xi_{n+1}) = \alpha \in D_{V_{\mathbf{F}}}(A)$, alors $D_{V_{\mathbf{F}}}(\mathfrak{p})(\alpha) = \xi_n$. Comme $d\mathfrak{p} : t_A^* \sim t_{R_n}^*$, nous pouvons appliquer le lemme 4.5.2 et ainsi

$$I_n = J_n + I_{n+1}.$$

∎

Lemme 4.5.4 *Le couple (R_{n+1}, ξ_{n+1}) est $n+1$-versel.*

PREUVE : Par construction et comme $I_n = J_n + I_{n+1}$,

$$\tau_{\leq n}(R_{n+1}) = R_{n+1}/J_n R_{n+1} = R_n \text{ et } \tau_{\leq 1}(R_{n+1}) = \tau_{\leq 1}(R_n).$$

Il s'agit de montrer que le morphisme de $\mathcal{C}_{n+1}$ $\tau_{\leq n+1}(\xi_{n+1}) : h_{\tau_{\leq n+1}(R_{n+1})} \to D_{V_{\mathbf{F}}}$ est lisse, autrement dit pour toute surjection de $\mathcal{C}_{n+1}$, $u : A \longrightarrow B$ de noyau $\mathfrak{a}$, $\alpha \in D(A)$, $\beta = D(u)(\alpha)$ et $g : R_{n+1} \longrightarrow B$ tel que $D(g)(\xi_{n+1}) = \beta$. Nous pouvons $f : R_{n+1} \longrightarrow A$ tel que $u \circ f = g$ et $D(f)(\xi_{n+1}) = \alpha$.
Supposons d'abord que $\mathfrak{a} \in \mathcal{M}_A^{n+1}$. On a $\tau_{\leq n}(A) = \tau_{\leq n}(B)$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & a & \longrightarrow & A & \longrightarrow & B & \longrightarrow & 0 \\ & & & & \uparrow f_S & & g \uparrow & & \\ 0 & \longrightarrow & I_{n+1} & \longrightarrow & S & \longrightarrow & R_{n+1} & \longrightarrow & 0 \end{array}$$

Nous pouvons relever g en $f_S : S \longrightarrow A$ en relevant les images de t_i dans B à A. On a $f_S(\mathcal{N}I_n) \subset \mathcal{M}_A(\mathcal{M}_A^{n+1} + \mathfrak{a}) = 0$ donc f_S se factorise par $R_n^* = S/\mathcal{N}I_n$ et induit $f_{R_n^*} = S/\mathcal{N}I_n \longrightarrow A$. Comme l'obstruction à relever ξ_{n+1} à R_{n+1} est nulle, $f_{R_n^*}$ se factorise par R_{n+1} et nous obtenons $f : R_{n+1} \to A$ qui relève g. Comme $D(g)(\xi_{n+1}) = D(u)D(f)(\xi_n) = \beta$ et $D(u)(\alpha) = \beta$, $D(f)(\xi_{n+1}) = \alpha$ relève β.
Pour traiter le cas $\mathfrak{a} \notin \mathcal{M}_A^{n+1}$, nous factorisons la surjection $u : A \longrightarrow B$ par

$$A \longrightarrow^{\pi} A/(\mathcal{M}_A^{n+1} \cap \mathfrak{a}) \longrightarrow^{\pi'} B.$$

Si on peut relever le morphisme $g : R_{n+1} \to B$ à $\tilde{f} : R_{n+1} \to A/(\mathcal{M}_A^{n+1} \cap \mathfrak{a})$ qui induit la déformation, comme noyau de π est inclu dans $\mathcal{M}_A^{n+1}$, nous pouvons alors appliquer la démonstration précédente pour conclure à l'existence d'un relèvement $f : R_{n+1} \longrightarrow A$ qui induit la déformation. Puis $A/(\mathcal{M}_A^{n+1} \cap \mathfrak{a})$ s'identifie au produit fibré

$$A/(\mathcal{M}_A^{n+1} \cap \mathfrak{a}) = B \times_{B_{\tau \leq n}} A_{\tau \leq n}.$$

La propriété (H1) du critère de Schlessinger permet alors de conclure. ∎

Nous voudrions écrire I_{n+1} sous la forme

$$I_{n+1} = J_{n+1} + (F_1^{(n+1)}, \ldots, F_r^{(n+1)})$$

avec les propriétés annoncées précédemment sur les $F_j^{(n+1)}$, $1 \leq j \leq r$. Pour alléger les notations, posons $< F_i^{(n+1)} >= (F_1^{(n+1)}, \ldots, F_r^{(n+1)})$. Établissons

Lemme 4.5.5 *Nous avons $I_n = J_n + < u_i >$ et $I_{n+1} = J_{n+1} + < u_i >$.*

PREUVE : D'après le lemme 4.5.3, $I_n = J_n + I_{n+1}$. Ainsi

$$I_n = J_n + \mathcal{N} I_n + < u_i >= J_n + \mathcal{N} J_n + \mathcal{N} < F_i^{(n)} > + < u_i >$$

$$= J_n + \mathcal{N} < F_i^{(n)} > + < u_i >= J_n + < F_i^{(n)} > .$$

Or pour tout j, nous pouvons écrire

$$F_j^{(n)} = h_j + \sum_{\ell=1}^{r} \alpha_{\ell j} F_\ell^{(n)} + \sum_{m=1}^{r} \beta_{mj} u_m$$

avec $h_j \in J_n, \alpha_{\ell j} \in \mathcal{N}$ et $\beta_{mj} \in S$. Sous forme matricielle, ces égalités s'écrivent

$$(\mathrm{Id} - \alpha) F^{(n)} = h + \beta \cdot u$$

avec $\mathrm{Id} - \alpha$ matrice inversible ; donc nous pouvons écrire

$$F_j^{(n)} = \sum_{\ell}^{r} \lambda_{\ell j} h_\ell + \sum_{q=1}^{r} \lambda'_{qj} u_q$$

avec $\lambda_{\ell j}, \lambda'_{qj} \in S$. Donc $F_j^{(n)} \in J_n + < u_i >$ et $I_n = J_n + < u_i >$. De plus

$$I_{n+1} = \mathcal{N} + < u_i >= \mathcal{N} J_n + \mathcal{N} < u_i > + < u_i >= J_{n+1} + < u_i > .$$

■

Comme $I_{n+1} = J_{n+1} + < u_i >$, les images des u_i et $F_j^{(n)}$ engendrent le même idéal dans J_n/J_{n+1}. Puis nous avons

Lemme 4.5.6 *Soit $\mathcal{O}$ un anneau local et M un $\mathcal{O}$-module de type fini. Soient $(\alpha_1, \ldots, \alpha_r)$ et $(\beta_1, \ldots, \beta_r)$ deux systèmes de générateurs de M. Alors il existe une matrice $X = (X_{ij})_{1 \le i,j \le r} \in \mathrm{GL}_r(\mathcal{O})$ telle que $\beta_i = \sum_{j=1}^{r} X_{ij} \alpha_j$, $\forall i \in [1, r]$.*

PREUVE : Les systèmes de générateurs (α_i) et (β_i) définissent deux surjections $\mathfrak{p}, \mathfrak{q}$ de $\mathcal{O}^r$ sur M. Pour démontrer le lemme, il suffit de trouver $X \in \mathrm{GL}_r(\mathcal{O})$ tel que $\mathfrak{q} = \mathfrak{p}X$. C'est clair si $\mathcal{O}$ est un corps car alors M est un espace vectoriel. Sinon nous passons au corps résiduel de $\mathcal{O}$ et nous relevons la matrice obtenue, nous avons alors $X \in \mathrm{GL}_r(\mathcal{O})$ telle que $\mathfrak{q} = \mathfrak{p}X$ modulo l'idéal maximal $\mathcal{M}_\mathcal{O}$ de $\mathcal{O}$, ainsi pour tout i,

$$\beta_i = \sum_{j=1}^{r} X_{ij} \alpha_j + \sum_{j=1}^{r} y_{ij} \alpha_j$$

avec $\forall i, j \in \{1, \ldots, r\}$, $y_{ij} \in \mathcal{M}_\mathcal{O}$. Notons $Y = (y_{ij})_{1 \le i,j \le r}$. Il suffit alors de remplacer X par $X + Y$ pour obtenir le lemme. ■

Par conséquent, il existe $X \in \mathrm{GL}_r(S)$ telle que $F_j^{(n)} \equiv \sum_{i=1}^r X_{ji} u_i, \mod J_n$. Alors un relèvement $(F_j^{(n+1)})_{1 \leq j \leq r}$ à S^r du système $(\sum_{i=1}^r X_{ji} u_i)_{1 \leq j \leq r}$ défini modulo J_{n+1} convient.

Corollaire 4.5.7 *Le nombre minimal de relations de l'anneau universel de déformations est inférieur ou égal à la dimension* $r = \dim_{\mathbf{F}} H^2(G, \mathrm{ad}\, V_{\mathbf{F}})$.

Remarque 4.5.8 *Il existe différents problèmes de déformations pour lesquels, l'inégalité du Corollaire 4.5.7 est stricte (notamment pour les déformations de certains revêtements galoisiens entre courbes algébriques). En revanche, pour les déformations de représentations galoisiennes impaires irréductibles, la conjecture de Mazur [Ma] sur la dimension de Krull de l'anneau universel de déformation impose que le nombre minimal de relations soit égal à* $\dim_{\mathbf{F}} H^2(G, \mathrm{ad}\, V_{\mathbf{F}})$. *Plus précisément, si* $G = G_{F,S}$ *pour un corps de nombre* F *et un ensemble fini de places* S *contenant les places au-dessus de* p *et l'infini, si* $\mathrm{End}_{F[G]}(V_{\mathbf{F}}) = \mathbf{F}$ *alors* $R_{V_{\mathbf{F}}}$ *est un anneau d'intersection complète plat sur* $W(\mathbf{F})$ *de dimension relative* $h^1(G, \mathrm{ad}\, V_{\mathbf{F}}) - h^0(G, \mathrm{ad}\, V_{\mathbf{F}}) - h^2(G, \mathrm{ad}\, V_{\mathbf{F}})$.

Remarque 4.5.9 *Soit* $f = \sum a_n q^n$ *une forme nouvelle de poids* $k \geq 2$, *niveau* N *et caractère* ω. *Soit* S *un ensemble fini de places de* $\mathbf{Q}$ *conteant les places infinies et les places au-dessus des premiers divisant* N. *Soit* K *le corps de nombres engendré par les* a_n. *D'après les travaux de Eichler, Shimura, Deligne et Serre, pour tout premier* p *de* K, *on a une représentation galoisienne* V_p *semisimple de dimension 2*

$$\rho_{f,p} : G_{\mathbf{Q},S \cup \{p\}} \longrightarrow \mathrm{GL}_2(\mathbf{F})$$

où $\mathbf{F}$ *est le corps résiduel de* K. *On montre que la représentation* V_p *est absolument irréductible. D'après Weston [Wes], si* $k \geq 3$, V_p *est non obstruée pour presque tous les places premières* p. *Si* $k = 2$, *alors* V_p *est non obstruée en dehors d'un ensemble de densité nulle.*

5 Représentations galoisiennes

5.1 Généralités

Définition 5.1.1 *Soit V une $\mathbf{F}$-représentation de dimension finie de $G_K = \mathrm{Gal}(\overline{K}/K)$.*
Si K est un corps de nombres, la représentation V est dite galoisienne globale.
Si K est un corps p-adique, la représentation est dite galoisienne locale. Si, de plus, $\mathbf{F}$ est une extension finie de $\mathbf{Q}_\ell$ avec $\ell \neq p$, la représentation est dite ℓ-adique ; si $\ell = p$, la représentation est dite p-adique.

Remarque 5.1.2 *Les représentations ℓ-adique et p-adique sont de nature très différentes. En effet, le groupe d'inertie sauvage étant un pro-p-groupe, il est d'image finie dans le cas ℓ-adique mais pas forcément dans le cas p-adique.*

Exemples 5.1.3 *Soit K un corps de caractéristique 0. Le groupe G_K agit sur*

$$\mathbf{Z}_p \simeq \operatorname{proj}\lim_n \mu_{p^n}(\overline{K}^*) = T_p(\overline{K}^*)$$

et permet de définir le caractère cyclotomique

$$\chi_p : G_K \to \mathrm{Aut}(T_p(\overline{K}^*)) \simeq \mathbf{Z}_p^* = \mathrm{GL}_1(\mathbf{Z}_p) \to \mathrm{GL}_1(\mathbf{Q}_p).$$

Pour $K = \mathbf{Q}$, χ_p est un caractère non ramifié en toute place $\ell \neq p$. Pour $\xi \in \mu_{p^n}(\overline{\mathbf{Q}}^*)$ et $\sigma \in G_{\mathbf{Q}}$, on a $\sigma(\xi) = \xi^{\chi_p(\sigma)}$.

Définition 5.1.4 *Soit V une $\mathbf{F}$-représentation de G. On dit que V est absolument irréductible si $V \otimes_{\mathbf{F}} K$ est un $K[G]$-module simple pour toute extension K de $\mathbf{F}$.*

Enfin une version profinie de l'existence d'un vecteur invariant ([**?**]) sous l'action d'un p-groupe G d'une G-représentation V en caractéristique p.

Proposition 5.1.5 *Soit E un corps de caractéristique p. Soit P un pro-p-groupe, $\pi : P \to \mathrm{Aut}_E(V)$ une représentation (éventuellement de dimension infinie) lisse (i.e tout $v \in V$ a un stabilisateur ouvert dans P) non nulle de P. Alors il existe un vecteur non nul de V qui est fixe sous l'action de P.*

Preuve : Soit $v \in V - \{0\}$. Soit ρ le sous $E[P]$-module de V engendré par v. Par lissité, le stabilisateur $\mathrm{Stab}_P(v)$ est un sous-groupe ouvert du pro-p-groupe P, donc d'indice fini et ρ est une représentation de dimension finie. Soit $v_1, \ldots, v_d$ une base de ρ sur E et $H = \cap_{i=1}^d \mathrm{Stab}_P(v_i)$ est un groupe d'indice fini inclu dans le sous-groupe normal $\ker \rho$. L'action de ρ se factorise à travers un p-groupe fini. Le résultat résulte alors de sa version sur l'action des p-groupes sur des espaces de dimension finie en caractéristique p. ∎

5.2 Représentations p-adiques locales modulo p

Dans ce paragraphe, on donne une classification des représentations p-adiques locales modulo p de dimension 2 (voir §2.1 [Br]). Il s'agit d'illustrer le fait qu'en caractéristique p les représentations galoisiennes locales sont faciles à décrire.

Soit F une extension finie de $\mathbf{Q}_p$, $\mathcal{O}_F$ l'anneau des entiers de F, $\mathfrak{m}_F$ son idéal maximal, π_F une uniformisante et $\mathbf{F}_q = \mathbf{F}_{p^f}$ son corps résiduel. L'action de $G_F = \mathrm{Gal}(\overline{\mathbf{Q}}_p/F)$ sur $\overline{\mathbf{Q}}_p$ stabilise $\overline{\mathbf{Z}_p}$ et son idéal maximal. Elle induit donc une action de $\overline{\mathbf{F}}_p$ fixant $\mathbf{F}_p$ et donc un morphisme de groupes $G_F \to \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_q)$. On vérifie que ce morphisme est surjectif et on note $I_F = I(\overline{\mathbf{Q}}_p/F)$ son noyau, dit sous-groupe d'inertie. Pour résumer, on a la suite exacte :

$$0 \to I_F \to G_F \to \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_q) \to 0$$

Le groupe d'inertie sauvage est P_F le plus grand pro-p-sous-groupe de I_F.

Définition 5.2.1 *Soit k un corps topologique. Une représentation galoisienne locale $\rho : G_F \to \mathrm{GL}_n(k)$ est dite*
- non ramifiée si $\rho(I_F) = \mathrm{Id}$,
- modérément ramifiée si $\rho(P_F) = \mathrm{Id}$.

Le sous-groupe d'inertie I_F s'identifie au groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}_p/F^{\mathrm{nr}})$ de la plus grande extension F^{nr} non ramifiée de F dans $\overline{\mathbf{Q}}_p$, i.e l'extension de F obtenue en ajoutant toutes les racines m-ième d'élements de $\mathcal{O}_F^*$ pour tous les m premiers à p.
Soit m premier à p et F^m l'extension de F^{nr} obtenue en ajoutant toutes les racines m-ième de π_F. Alors,

$$I_F/P_F \simeq \operatorname{proj\,lim}_m \mathrm{Gal}(F^m/F^{\mathrm{nr}})$$

la limite projective étant définie par les applications de restriction. Le lemme suivant donne une description utile de ce quotient.

Lemme 5.2.2 *On a un isomorphisme de groupes topologiques*

$$I_F/P_F \simeq \operatorname{proj\,lim} \mathbf{F}_{p^n}^*$$

où la limite projective est prise pour les applications normes $\mathbf{F}_{p^{nm}}^* \to \mathbf{F}_{p^n}^*$.

Preuve : Pour $n \geq 1$, l'application de $I_F \to \mathbf{F}_{p^n}^*$ qui envoie $g \in I_F$ dans l'image de

$$\frac{g(\sqrt[p^n-1]{\pi_F})}{\sqrt[p^n-1]{\pi_F}} \in \mu_{p^n-1}(\overline{\mathbf{Z}}_p)$$

dans $\overline{\mathbf{F}}_p^* = (\overline{\mathbf{Z}}_p/\mathfrak{m}_{\overline{\mathbf{Z}}_p})^*$ est bien définie. En effet, $g \mapsto \frac{g(\sqrt[p^n-1]{\pi_F})}{\sqrt[p^n-1]{\pi_F}}$ induit un isomorphisme de groupes $\mathrm{Gal}(F^m/F^{\mathrm{nr}}) \simeq \mu_m(\overline{\mathbf{Z}_p})$ qui est indépendant du choix de l'uniformisante et de la racine $\sqrt[m]{\pi_F}$ (les racines m-ième d'un élément de $\mathcal{O}_F^*$ sont dans F^{nr} donc l'action de I_F est triviale sur ces éléments.)
Comme m est premier à p, la réduction modulo $\mathfrak{m}_{\overline{\mathbf{Z}}_p}$ induit un isomorphisme de groupes (d'après le lemme de Hensel appliqué à $P(x) = x^m - 1$)

$$\mu_m(\overline{\mathbf{Z}_p}) \simeq \mu_m(\overline{\mathbf{F}}_p).$$

Ainsi, on a

$$I_F/P_F \simeq \operatorname*{proj\,lim}_m \mu_m(\overline{\mathbf{F}}_p)$$

où les applications de transition sont $\mu_{mm'}(\overline{\mathbf{F}}_p) \to \mu_{m'}(\overline{\mathbf{F}}_p), \mu \mapsto \mu^m$. Mais tout entier m premier à p divise un entier de la forme $p^n - 1$ pour n convenable. Il suffit donc de prendre la limite projective sur les entiers de la forme $p^n - 1$. Le résultat résulte donc de $\mu_{p^n-1}(\overline{\mathbf{F}}_p) = \mathbf{F}_{p^n}^* \subset \overline{\mathbf{F}}_p^*$. ∎

On commence par décrire les caractères continus $\theta : I_F \to \overline{\mathbf{F}}_p^*$, puis ceux qui se prolongent à G_F. Ce travail conduit à une classification des représentations continues $\rho : G_F \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_p)$.

Définition 5.2.3 *Un caractère fondamental de niveau $n > 0$ est un caractère $\theta : I_F \to \overline{\mathbf{F}}_p^*$ qui se factorise à travers $I_F \to \mathbf{F}_{p^n}^* \to \overline{\mathbf{F}}_p^*$.*

Lemme 5.2.4 *Soit $\theta : I_F \to \overline{\mathbf{F}}_p^*$ un caractère continu. Alors il existe $n > 0$ tel que θ soit un caractère fondamental de niveau n.*

Preuve : Le caractère θ est continu pour la topologie discrète sur $\overline{\mathbf{F}}_p$. Donc l'image inverse du sous-groupe ouvert $\{1\} \subset \overline{\mathbf{F}}_p^*$ est un sous-groupe ouvert U de I_F et θ se factorise à travers le quotient fini I_F/U. L'image de P_F dans I_F/U est un p-groupe fini. Or $\overline{\mathbf{F}}_p^*$ ne contient aucun p-groupe de torsion non trivial donc $\theta(P_F) = \{1\}$ i.e. $P_F \subset U$. Ainsi θ se factorise à travers un quotient fini de I_F/P_F donc à travers un $\mathbf{F}_{p^n}^*$ d'après le lemme 5.2.2. ∎

Fixons un plongement $\iota : \mathbf{F}_{p^n} \to \overline{\mathbf{F}}_p$ et notons ω_n le caractère fondamental $I_F \to \mathbf{F}_{p^n}^* \to \overline{\mathbf{F}}_p^*$ induit par ι. Alors si θ est un caractère fondamental de niveau n, il existe $0 \leq i_j \leq p-1$ tels que

$$\theta = \omega_n^{i_0 + p i_1 + \cdots + p^{n-1} i_{n-1}}.$$

Si m divise n alors

$$\omega_n^{1+p^m+p^{2m}+\cdots+p^{(n/m-1)m}} = \omega_m$$

d'après le lemme 5.2.2 et $N_{\mathbf{F}_{p^n}/\mathbf{F}_{p^m}}(x) = x^{1+p^m+p^{2m}+\cdots+p^{(n/m-1)m}}$.

Lemme 5.2.5 *Le caractère ω_n s'étend de I_F à G_F si et seulement si n divise $f = [W(k_F)[1/p]/\mathbf{Q}_p]$.*

PREUVE : Le groupe de Galois $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_q)$ est topologiquement engendré par le Frobenius $\mathrm{Frob}^f : x \mapsto x^q$. Les corps $F(\sqrt[p^n-1]{\pi_F})$ et F ont même corps résiduel $\mathbf{F}_q$. Donc on a une surjection de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/F(\sqrt[p^n-1]{\pi_F})) \to \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_q)$. Ainsi on peut relever Frob^f en $s \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/F(\sqrt[p^n-1]{\pi_F}))$. Le noyau I_F de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/F) \to \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_q)$ est un sous-groupe normal de G_F. Donc $sgs^{-1} \in I_F$ pour tout $g \in I_F$. Comme $s(\sqrt[p^n-1]{\pi_F}) = \sqrt[p^n-1]{\pi_F}$ et $s(\sqrt[p^n-1]{1}) = (\sqrt[p^n-1]{1})^q$ (car $\mu_{p^n-1}(\overline{\mathbf{Z}}_p) \simeq \mu_{p^n-1}(\overline{\mathbf{F}}_p)$). On a pour tout $g \in I_F$,

$$\omega_n(sgs^{-1}) = \frac{sgs^{-1}(\sqrt[p^n-1]{\pi_F})}{\sqrt[p^n-1]{\pi_F}} = s\Big(\frac{g(\sqrt[p^n-1]{\pi_F})}{\sqrt[p^n-1]{\pi_F}}\Big) = \Big(\frac{g(\sqrt[p^n-1]{\pi_F})}{\sqrt[p^n-1]{\pi_F}}\Big)^q = \omega_n(g)^q.$$

Si ω_n s'étend à G_F, alors $\omega_n(sgs^{-1}) = \omega_n(s)\omega_n(g)\omega_n(s^{-1}) = \omega_n(g)$. Donc $\omega_n(g) = \omega_n(g)^q$ pour tout $g \in I_F$. Donc $\omega_n^{q-1} = 1$ et n divise f.
Si n divise f, alors pour toute racine $\sqrt[q-1]{\pi_F}$ de π_F et tout $g \in G_F$, l'élément

$$\frac{g(\sqrt[q-1]{\pi_F})}{\sqrt[q-1]{\pi_F}} \in \mu_{q-1}(\overline{\mathbf{Z}}_p)$$

ne dépend pas du choix de la racine $\sqrt[q-1]{\pi_F}$ et induit un caractère $G_F \to \mathbf{F}_q^*$ qui est ω_f en restriction à I_F. Il suffit alors de prendre $\omega_f^{1+p^n+\cdots+p^{(f/n-1)n}}$. ∎

Proposition 5.2.6 *Soit $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}_p/F) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ une représentation continue. Alors,*
i. Si ρ est réductible alors il existe des entiers m_1, m_2 tels que

$$\rho_{|I_F} \simeq \begin{pmatrix} \omega_f^{m_1} & * \\ 0 & \omega_f^{m_2} \end{pmatrix},$$

ii. Si ρ est irréductible, il existe m entier non divisible par $q-1$ tel que

$$\rho_{|I_F} \simeq \begin{pmatrix} \omega_{2f}^{m} & 0 \\ 0 & \omega_{2f}^{qm} \end{pmatrix}.$$

PREUVE : i. Si ρ est réductible, $\rho_{|I_F} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$, pour des caractères continus $\chi_1, \chi_2 : I_F \to \overline{\mathbf{F}}_p^*$ qui s'étendent à G_F. Donc il existe $n_i \geq 0$ minimal, $m_i \geq 0$ tels que $\chi_i = \omega_{n_i}^{m_i}$, $i = 1, 2$. Commes ces caractères s'étendent à G_F, n_i divise f, donc $n_1 = n_2 = f$.

ii. On suppose ρ irréductible. Soit ρ^{P_F} le sous-espace de ρ sur lequel P_F agit trivialement. Pour $v \in \rho^{P_F}$, $g \in G_F$, $w \in P_F$,

$$wgv = g(g^{-1}wg)v = gv$$

car $g^{-1}wg \in P_F$, donc $gv \in \rho^{P_F}$ et ρ^{P_F} est G_F-stable. Donc $\rho^{P_F} \neq 0$. Or ρ est irréductible. Donc $\rho = \rho^{P_F}$ et P_F agit trivialement, donc $\rho_{|I_F}$ se factorise à travers I_F/P_F. Or I_F/P_F est abelien, premier à p donc $\rho_{|I_F}$ est la somme de deux caractères fondamentaux $\chi_1 \oplus \chi_2$. En raisonnant comme dans la preuve du lemme 5.2.5, on a $\chi(sgs^{-1}) = \chi(g)^q$ pour $g \in I_F$ et $s \in G_F$ relèvement de Frob^f. Comme la représentation $\rho^s = \rho(s \cdot s^{-1})$ est isomorphe (car conjuguée) à ρ, on a $\{\chi_1, \chi_2\} = \{\chi_1^q, \chi_2^q\}$. Si $\chi_1 = \chi_1^q$, alors $\chi_2 = \chi_2^q$ et les caractères χ_i s'étendent à G_F donc ρ est réductible. Donc $\chi_1 = \chi_2^q \neq \chi_1^q$ et $\chi_i^{q^2} = \chi_i$. ∎

Corollaire 5.2.7 *Soit $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ une représentation continue. Il existe un caractère η de I_F qui s'étend à G_F tel que*
i. Si ρ est réductible alors il existe des entiers r_i avec $-1 \leq r_i \leq p-2$ et $(r_0, \ldots, r_{f-1}) \neq (p-2, \ldots, p-2)$ tels que

$$\rho_{|I_F} \simeq \begin{pmatrix} \omega_f^{\sum_{i=0}^{f-1}(r_i+1)p^i} & * \\ 0 & 1 \end{pmatrix} \otimes \eta,$$

ii. Si ρ est irréductible, alors il existe des entiers r_i avec $0 \leq r_0 \leq p-1$ et $-1 \leq r_i \leq p-2$ pour $i > 0$ et $(r_0, \ldots, r_{f-1}) \neq (p-1, p-2, \ldots, p-2)$ tels que

$$\rho_{|I_F} \simeq \begin{pmatrix} \omega_{2f}^{\sum_{i=0}^{f-1}(r_i+1)p^i} & 0 \\ 0 & \omega_{2f}^{q\sum_{i=0}^{f-1}(r_i+1)p^i} \end{pmatrix} \otimes \eta.$$

Définition 5.2.8 *Soit $\rho : G_F \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ une représentation irréductible. On dit que ρ est générique, si dans l'écriture ii. du Corollaire 5.2.7, $1 \leq r_0 \leq p-1$ et $0 \leq r_i \leq p-3$, $1 \leq i \leq f-1$.*

Remarque 5.2.9 *Dans l'écriture ii. du corollaire 5.2.7, on peut remplacer $(r_0, \ldots, r_{f-1})$ et η par $(p-1-r_0, p-3-r_1, \ldots, p-3-r_{f-1})$ et $\eta\omega_f^{r_0+\sum_{i=1}^{f-1} p^i(r_i+1)}$.*

Définition 5.2.10 *Soit $\rho : G_F \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ une représentation irréductible. L'ensemble des poids de Diamond associé à ρ est l'ensemble des $(r'_0, \ldots, r'_{f-1}), \eta'$ tels qu'il existe $(q_i)_{0 \leq i \leq f-1} \in \{p^i, qp^i\}_{0 \leq i \leq f-1}$ avec*

$$\rho_{|I_F} \simeq \begin{pmatrix} \omega_{2f}^{\sum_{i=0}^{f-1}(r'_i+1)q_i} & 0 \\ 0 & \omega_{2f}^{q\sum_{i=0}^{f-1}(r'_i+1)q_i} \end{pmatrix} \otimes \eta'.$$

Remarque 5.2.11 *Si ρ est générique, l'ensemble des poids de Diamond associés à ρ est de cardinal 2^f.*

Exemples 5.2.12 *Les poids de Diamond associés à*

$$\rho_{I_{\mathbf{Q}_{p^2}}} \simeq \begin{pmatrix} \omega_4^{(r_0+1)+(r_1+1)p} & 0 \\ 0 & \omega_4^{(r_0+1)p^2+(r_1+1)p^3} \end{pmatrix}$$

sont

$$\{(r_0,r_1),(r_0-1,p-2-r_1)\omega_2^{p(r_1+1)},(p-1-r_0,p-3-r_1)\omega_2^{r_0+p(r_1+1)},(p-2-r_0,r_1+1)\omega_2^{r_0+p(p-1)}\}.$$

En effet

$$\begin{pmatrix} \omega_4^{(r_0+1)+(r_1+1)p} & 0 \\ 0 & \omega_4^{(r_0+1)p^2+(r_1+1)p^3} \end{pmatrix} = \begin{pmatrix} \omega_4^{r_0+(p-1-r_1)p^3} & 0 \\ 0 & \omega_4^{r_0p^2+(p-1-r_1+1)p} \end{pmatrix} \otimes \omega_2^{p(r_1+1)}$$

$$= \begin{pmatrix} \omega_4^{(p-r_0)p^2+(p-2-r_1)p^3} & 0 \\ 0 & \omega_4^{(p-r_0)+(p-2-r_1)p} \end{pmatrix} \omega_2^{r_0+p(r_1+1)}$$

$$= \begin{pmatrix} \omega_4^{(p-1-r_0)p^2+(r_2+1)p} & 0 \\ 0 & \omega_4^{(p-1-r_0)+(r_1+1)p^3} \end{pmatrix} \omega_2^{r_0+p(p-1)}.$$

6 Déformations de représentations globales

L'objet de ce chapitre est de présenter les premiers calculs d'anneaux de déformations universels de représentations galoisiennes globales ([Bo]) afin d'illustrer les stratégies mises en place pour les déterminer. Ils reposent sur des résultats décrivant la structure des groupes de galois (Théorie du corps de classes et théorie d'Iwasawa).

Pour X un groupe $x \in X$, on note $\overline{X} = X/\overline{X^p[X,X]}$ et $\bar{x}$ l'image de x dans $\bar{X}$. On suppose p impair. Soit F une extension totalement complexe ($r_1(F) = 0$ et $r_2(F) = [F : \mathbf{Q}]/2$) finie d'ordre premier à p de $\mathbf{Q}$, S un ensemble fini de places de F contenant les places au-dessus de p, L la plus grande pro-p-extension de F dans $\overline{\mathbf{Q}}$ non ramifiée en dehors de S, $P = \mathrm{Gal}(L/F)$. On rappelle (ou on admet) quelques résultats de théorie du corps de classes qui s'établissent via une version $A = \mathrm{Gal}(F/\mathbf{Q})$-équivariante de la suite de Poitou-Tate. Comme $\mathbf{F}_p[A]$-modules, on a l'identification

$$\overline{P} = \mathrm{Ind}_{A_\infty}^{A} \tilde{\mathbf{F}}_p \oplus \mathbf{F}_p \oplus \mathrm{Coker}\left(\mu_p(F) \longrightarrow \oplus_{v\in S'}\mu_p(F_v)\right) \oplus B_S$$

où $B_S = Ш^2_S(F, \mathbf{F}_p)^*$, A_∞ est un sous-groupe de A d'ordre 2 engendré par le choix d'une conjugaison complexe, $\tilde{\mathbf{F}}_p$ est le $\mathbf{F}_p[A_\infty]$-module irréductible non trivial. De plus la suite de $\mathbf{F}_p[A]$-module suivante est exacte

$$0 \longrightarrow \mathrm{Coker}\left(\mu_p(F) \longrightarrow \oplus_{v\in S'}\mu_p(F_v)\right) \longrightarrow H^2(P, \mathbf{F}_p)^* \longrightarrow Ш^2_S(F, \mathbf{F}_p)^* \longrightarrow 0.$$

De cette présentation de $\overline{P}$ comme $\mathbf{F}_p[A]$-module, nous allons pouvoir déduire des informations sur le pro-p-groupe P muni de l'action de A. Pour cela, nous devons besoin de résultats supplémentaires concernant les pro-p-groupes avec opérateurs ([Gr]).

6.1 Pro-p-groupes avec opérateurs

On rappelle l'énoncé du théorème de Schur-Zassenhaus pour les groupes finis :

Théorème 6.1.1 *Si G est un groupe fini et N est un sous-groupe normal de G tel que les ordres $|N|$ et $n = |G/N|$ soient premiers entre eux, alors il existe un sous-groupe H de G d'ordre n, tel que $G = N| \times H$ et deux tels sous-groupes H, H' sont conjugués.*

Nous en déduisons une version profinie :

Proposition 6.1.2 *Soit G un groupe profini, N un pro-p-groupe normal de G d'indice fini premier à p. Alors G contient un sous-groupe H tel que $G = HN$ et $H \cap N = \{e_G\}$. De plus tous les sous-groupes satisfaisants ces propriétés sont conjugués. Autrement dit $G = N| \times H$ et si H et H' sont deux tels sous-groupes alors il existe $n \in N$ tel que $H' = nHn^{-1}$.*

Nous rappelons les résultats vus avant suivants (dit lemme de Burnside)

Lemme 6.1.3 *Soit P un pro-p-groupe admettant un nombre fini de générateurs topologiques.*
i. La famille $\{x_1, \ldots, x_n\}$ engendre P si et seulement si $\{\bar{x}_1, \ldots, \bar{x}_n\}$ engendre $\overline{P}$.
ii. Le groupe $\ker\left(\mathrm{Aut}_{\mathbf{F}_p} P \longrightarrow \mathrm{Aut}_{\mathbf{F}_p} \bar{P}\right)$ *est un pro-p-groupe.*

Nous pouvons ainsi établir

Lemme 6.1.4 *Soit A un groupe fini d'ordre premier à p, Γ un pro-p-groupe libre admettant un nombre fini de générateurs et $\psi : A \longrightarrow \mathrm{Aut}_{\mathbf{F}_p} \overline{\Gamma}$ un homomorphisme. Alors il existe un relèvement $\varphi : A \longrightarrow \mathrm{Aut}_{\mathbf{F}_p} \Gamma$ de ψ.*

Preuve : Il s'agit d'abord de montrer que tout automorphisme $\bar{\alpha} \in \mathrm{Aut}_{\mathbf{F}_p} \overline{\Gamma}$ se relève en un automorphisme continu $\alpha \in \mathrm{Aut}_{\mathbf{F}_p} \Gamma$. Autrement dit l'application

$$f : \mathrm{Aut}_{\mathbf{F}_p} \Gamma \longrightarrow \mathrm{Aut}_{\mathbf{F}_p} \overline{\Gamma} \tag{2}$$

est surjective. Comme Γ est libre, on peut relever $\bar{\alpha}$ en un homomorphisme continu $\alpha : \Gamma \longrightarrow \Gamma$. Cet homomorphisme est surjectif d'après le lemme de Burnside. La suite d'inflation-restriction et la nullité de $H^2(\Gamma, \mathbf{F}_p) = 0$ implique que $H^1(\ker\alpha, \mathbf{F}_p) = 0$. Comme $\ker\alpha$ est un pro-p-groupe, on en déduit que $\ker\alpha$ est trivial donc α est injective. Il suffit alors d'établir que α^{-1} est continu.
Soit $G \subset \mathrm{Aut}_{\mathbf{F}_p}\Gamma$ l'image inverse de $\psi(A)$ par f et $N = \ker f$. Alors $N \subset G$ et $G/N \simeq \psi(A)$. Comme $\psi(A)$ est d'ordre premier à p, d'après le théorème de Schur-Zassenhaus, G contient un sous groupe H isomorphe à $\psi(A)$ tel que $G = N| \times H$. Ainsi on a une application surjective $A \to H$ qui induit $\psi : A \to G/N \to \mathrm{Aut}_{\mathbf{F}_p}\bar{\Gamma}$. ∎

Définition 6.1.5 *Soit A un groupe fini d'ordre premier à p. Un pro-p groupe P ayant un nombre fini de générateurs muni d'un homomorphisme $A \longrightarrow \mathrm{Aut}_{\mathbf{F}_p} P$ est dit A-groupe.*

Proposition 6.1.6 *Soit A un groupe fini d'ordre premier à p, Γ, P des pro-p-A-groupes ayant un nombre fini de générateurs. On suppose de plus que Γ est libre et qu'il existe un A-homomorphisme surjectif*

$$\tau : \overline{\Gamma} \longrightarrow \bar{P}$$

Alors il existe un A-homomorphisme surjectif $\sigma : \Gamma \longrightarrow P$ tel que $\bar{\sigma} = \tau$.

Preuve : Introduisons les notations suivantes pour les morphismes induisant les structures de (pro-)p-A-groupes.

$$\phi : A \longrightarrow \mathrm{Aut}\,\Gamma, \psi : A \longrightarrow \mathrm{Aut}\,\overline{\Gamma}$$

$$\kappa : A \longrightarrow \mathrm{Aut}\,P, \lambda : A \longrightarrow \mathrm{Aut}\,\overline{P}$$

Ainsi $\tau \circ \psi(\alpha) = \lambda(\alpha) \circ \tau$ pour tout $\alpha \in A$. Notons $H = \phi(A)$ et $J = \kappa(A)$.
Commençons par supposer que τ est un isomorphisme. Il induit un isomorphisme entre $\mathrm{Aut}\,\overline{\Gamma}$ et $\mathrm{Aut}\,\overline{P}$ donc entre H et J. D'après le théorème de Burnside, il existe un homomorphisme continu surjectif $\delta : \Gamma \longrightarrow P$ tel que $\overline{\delta} = \tau$. Notons $\Delta = \ker\delta$ et $\mathrm{Aut}_\Delta\,\Gamma$ le sous-groupe des automorphismes continus de Γ qui fixe le sous-groupe δ. Ainsi

$$g : \mathrm{Aut}_\Delta\,\Gamma \longrightarrow \mathrm{Aut}\,P$$

est surjectif de noyau $N' \subset N = \ker(Aut\Gamma \to \mathrm{Aut}\,\overline{\Gamma})$ un pro-p sous-groupe de $\mathrm{Aut}_\Delta\,\Gamma$. Soit $G' = g^{-1}(J)$. D'après le lemme de Schur Zassenhaus $G' = H'N'$ avec action de H' isomorphe à J et l'application $\kappa : A \to J$ détermine l'application $\varphi : A \to H'$. Ainsi pour Γ, A-groupe via l'application φ (au lieu de ϕ), δ est un A-homomorphisme de Γ dans P.
Or ϕ et φ induisent ψ, la même application ψ de A dans $\mathrm{Aut}\,\overline{\Gamma}$. Notons G l'image inverse de

$\psi(A)$ par $Aut\Gamma \to \mathrm{Aut}\,\overline{\Gamma}$. On a $H' \subset G$ et $G = H'N$. Donc H et H' sont conjugués, il existe $\eta \in N$ tel que $H' = \eta H \eta^{-1}$. Ainsi pour $\alpha \in A$, $\varphi(\alpha) \circ \eta = \eta \circ \phi(\alpha)$ donc η induit l'identité sur $\overline{Gamma}$. Donc $\sigma = \delta \circ \eta : \Gamma \longrightarrow P$ est un A-homomorphisme surjectif et $\overline{\sigma}$ coincide avec $\tau : \overline{\Gamma} \longrightarrow \overline{P}$.
Si τ n'est pas injectif, définissons l'isomorphisme

$$\tau_1 : \overline{\Gamma} \longrightarrow \overline{P} \times \ker(\tau)$$

et appliquons le résultat précédent à $P_1 = P \times \ker(\tau)$. ∎

Corollaire 6.1.7 *Supposons que A est abelien et tous ces éléments ont un ordre divisant $p-1$. Soit χ un caractère de A et z un élément de $\overline{P}$ sur lequel A agit via χ. Alors il existe un élément $x \in P$ tel que $\overline{x} = z$.*

Preuve : L'hypothèse sur A implique que les $\mathbf{F}_p$-représentations irréductibles de A peuvent être identifiées aux caractères $\widehat{A} = \mathrm{Hom}(A, \mathbf{F}_p^*)$. Soit $\chi \in \widehat{A}$, el le composant vace l'homomorphisme canonique $\mathbf{F}_p^* \to \mathbf{Z}_p^*$, on obtient un caractère $\chi \in \mathrm{Hom}(A, \mathbf{Z}_p^*)$ que l'on note de la même façon. On choisit une $\mathbf{F}_p[A]$-base de $\overline{\Gamma} = \overline{P}$ (avec action via des caractères). On la relève dans Γ, puis on applique la proposition précédente. ∎

6.2 Généralités

Définition 6.2.1 *Supposons qu'il existe un plongement $\tau_\infty : K \to \mathbf{R}$. Soit c la conjugaison complexe dans $\mathcal{C}$. Alors pour tout plongement $\tau : \overline{\mathbf{Q}} \to \mathcal{C}$ prolongeant τ_∞, l'application $\tau^{-1} \circ c \circ \tau$ définit un élément de G_K dit conjugaison complexe. Ainsi toutes les conjugaisons complexes sont conjuguées*

Définition 6.2.2 *Soit K un corps de nombres et E un corps topologique. La représentation $\rho : G_K \to \mathrm{GL}_n(E)$ est dite impaire si l'image de toutes conjugaison complexe est de déterminant -1 (et paire sinon).*

Soit $\bar{\rho} : G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p)$ un représentation impaire de groupe $G_{\mathbf{Q},S}$ de la plus grande extension algébrique de $\mathbf{Q}$ non ramifiée en dehors d'un ensemble fini de places S. On note K le sous-corps de $\mathbf{Q}_S$ fixe par $\ker \bar{\rho}$ et L la plus grande pro-p-extension de K non ramifiée aux places au-dessus de S. On note $P = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(K/\mathbf{Q})$. On note S' l'ensemble des places de F au-dessus de S.

Définition 6.2.3 *Soit H un sous-groupe de $\mathrm{GL}_n(\mathbf{F})$ et $\mathrm{ad}_{|H}$ le $\mathbf{F}[H]$-module adjoint correspondant. Un $\mathbf{F}[H]$-module V est dit premier à l'adjoint s'il existe un sous-groupe A de H d'ordre premier à p tel que V et $\mathrm{ad}_{|H}$ sont premiers entre eux comme $\mathbf{F}[A]$-module (comme A est d'ordre premier à p, $\mathbf{F}[A]$ est semi-simple, V et $\mathrm{ad}_{|H}$ sont premiers entre eux signifie qu'ils n'ont pas de sous-représentation irréductible en commun). Les générateurs de V sont alors dit premiers à l'adjoint.*

Lemme 6.2.4 *Soit R un objet de $\widehat{C}$. Alors*
i. $\Gamma_n(R) = \ker(\mathrm{GL}_n(R) \longrightarrow \mathrm{GL}_n(\mathbf{F}))$ est un pro-p-groupe,
ii. Soit X un sous-groupe de type fini de $\Gamma_n(R)$ et A un sous-groupe de $\mathrm{GL}_n(R)$ d'ordre premier à p qui normalise X. Si le $\mathbf{F}_p[A]$-module $\overline{X} = X/X^p[X,X]$ est premier à l'adjoint, alors X est trivial.

PREUVE : i. Le groupe $\ker(\Gamma_n(R/\mathfrak{m}_R^r)\Gamma_n(R/\mathfrak{m}_R^{r-1}))$ est un p-groupe abelien et $\Gamma_n(R) = \mathrm{proj\,lim}\,\Gamma_n(R/\mathfrak{m}_R^r)$ est un pro-p-groupe.
ii. Raisonnons par l'absurde et supposons que X n'est s trivial. Soir r minimal tel que X n'est pas inclus dans $K_r = \ker(\Gamma_n(R) \to \Gamma_n(R/\mathfrak{m}_R^r))$. Alors $X/(X \cap K_r) = XK_r/K_r$ est un sous-groupe non trivial de K_{r-1}/K_r qui est un multiple de la représentation $\mathrm{ad}_{|A}$ (calcul). ∎

Nous disposons du résultat de théorie des groupes suivants ([Sw]) qui nous permet de différentier trois situations :

Remarque 6.2.5 *Il y a trois possibilités pour l'image de $\bar{\rho}$:*
- ordre premier à p, $\bar{\rho}$ est dite modérée,
- contenant $\mathrm{SL}_2(\mathbf{F}_p)$, dans ce cas $\bar{\rho}$ est absolument irréductible et est dite pleine,
- résoluble d'ordre divisible par p et dans ce cas $\bar{\rho}$ est réductible.

6.3 Le cas modéré

Ici $H = \mathrm{Gal}(K/\mathbf{Q})$ est d'ordre premier à p. Il existe donc un relèvement $\sigma : H \longrightarrow \mathrm{GL}_n(\mathbf{Z}_p)$ de $\overline{\rho}_{|H}$ à $\mathbf{Z}_p$ et deux relèvements sont équivalents. Pour tout R de $\mathcal{C}$, H agit sur $\Gamma_2(R)$ via σ et le morphisme $\mathbf{Z}_p \to R$. On définit le foncteur

$$E : \mathcal{C} \longrightarrow \mathrm{Ens}, \quad E(R) = \mathrm{Hom}_H(P, \Gamma_2(R)).$$

Proposition 6.3.1 *Si $\overline{\rho}$ est modérée absolument irréductible non triviale, $E \longrightarrow D_{\bar{\rho}}$ est un isomorphisme de foncteurs.*

PREUVE : Tout élément de $E(R)$ définit un homomorphisme de G (produit semi-direct de P et de H) dans $\mathrm{GL}_2(R)$. L'application $E(R) \longrightarrow D_{\bar{\rho}}$ est surjective car tout relèvement de $\bar{\rho}$ se factorise à travers G et s'obtient de cette façon une fois fixé l'homomorphisme $H \longrightarrow \mathrm{GL}_2(R)$ (deux tels homomorphismes laissent invariant la classe de conjugaison).
Pour l'injectivité, il s'agit de déterminer les éléments de $\Gamma_2(R)$ qui fixe l'homomorphisme $H \longrightarrow \mathrm{GL}_2(R)$. Comme $\bar{\rho}$ est absolument irréductible non triviale, ce sont les homothéties. Les homothéties agissent trivialement de P sur $\Gamma_2(R)$. D'où l'injectivité. ∎

Définition 6.3.2 *Une représentation modérée est dite régulière si elle est absolument irréductible, impaire et si* $V = \mathrm{Coker}(\mu_p(K) \longrightarrow \oplus_{s\in S}\mu_p(K_v))$ *et* B_S *sont premiers à l'adjoint.*

Remarque 6.3.3 *l'hypothèse régulière correspond à des hypothèses favorables pour effectuer les calculs. En effet on a la présentation comme* $\mathbf{F}_p[H]$*-module :*

$$\overline{P} = \mathrm{Ind}_{H_\infty}^{H} \tilde{\mathbf{F}}_p \oplus \mathbf{F}_p \oplus \mathrm{Coker}\left(\mu_p(F) \longrightarrow \oplus_{v\in S'}\mu_p(F_v)\right) \oplus B_S$$

Donc si $\bar{\rho}$ *est régulière,* $\overline{P}$ *est engendré comme* $\mathbf{F}_p[H]$*-module par les générateurs spéciaux suivants :* $\overline{x}, \overline{y}$ *et des générateurs premiers à l'adjoint avec* $h \cdot \bar{x} = \bar{x}$, $h \in H$ *et* $\sigma \cdot \bar{y} = \bar{y}^{-1}$ *pour* σ *une conjugaison complexe. De plus le sous-groupe engendré par* x, y *dans* P *est libre car les hypothèses premier-à-l'adjoint imposent* $H^2(G_{K,S}, \mathrm{ad}) = H^2(P, \mathrm{ad})^H = 0$ *donc* $H^2(P, \mathbf{F}_p)^H = 0$ *(car* $\mathrm{ad} = \mathrm{ad}^0 + \mathbf{F}_p$*). De plus* $\dim_{\mathbf{F}_p} H^1(G_{K_S}, ad) = 3$*. Nous verrons dans la suite que ce ne sont pas des hypothèses vides. Par exemple, elles sont satisfaites pour les corps p-réguliers ([Gr]). Par ailleurs, augmenter l'ensemble des places* S*, peut permettre d'annuler la composante* B_S*.*

Proposition 6.3.4 *Soit* $\bar{\rho} : G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p)$ *modérée et régulière. Alors* $R_{\bar{\rho}} = \mathbf{Z}_p[[X_1, X_2, X_3]]$ *et la déformation universelle est donnée par*

$$x \mapsto \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_1 \end{pmatrix},$$

$$y \mapsto \begin{pmatrix} (1+T_2T_3)^{1/2} & T_2 \\ T_3 & (1+T_2T_3)^{1/2} \end{pmatrix},$$

et les autres gén'erateurs spéciaux s'envoient sur l'identité

PREUVE : D'après l'hypothèse régulière

$$\dim_{\mathbf{F}_p} H^1(G, \mathrm{ad}) = 3, \quad \dim_{\mathbf{F}_p} H^2(G, \mathrm{ad}) = 0$$

donc $R_{\bar{\rho}} = \mathbf{Z}_p[[T_1, T_2, T_3]]$.
Par unicité de la structure du produit semi-direct, G est isomorphe au produit semi-direct de H et de P. Il existe des relèvements $x, y \in P$ avec $h \cdot x = x$, $h \in H$ et $\sigma \cdot y = y^{-1}$. Le groupe P est engendré par x, y et d'autres éléments premiers à l'adjoint. Or $D_{\bar{\rho}}(R) = \mathrm{Hom}_H(P, \Gamma_2(R))$ donc toute déformation est déterminée par l'image de x et de y. Ces images sont de la forme

$$\begin{pmatrix} 1+X_1 & X_2 \\ X_3 & 1+X_4 \end{pmatrix}$$

avec $X_i \in R$. Comme $\bar{\rho}$ est absulument irréductible et x est invariant par H, donc l'image de x est scalaire. L'égalité $\sigma \cdot y = y^{-1}$ impose l'image de y en écrivant les égalités matricielles correspondantes :

$$\begin{aligned} \rho(\sigma \cdot y) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1+X_1 & X_2 \\ X_3 & 1+X_4 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= (\det(\rho(y)))^{-1} \begin{pmatrix} 1+X_4 & -X_2 \\ -X_3 & 1+X_1 \end{pmatrix} = \rho(y)^{-1}. \end{aligned}$$

■

6.4 Le cas plein

Dans le cas modéré, le foncteur de déformations s'identifie à un foncteur simple $\mathrm{Hom}_H(P, \Gamma_2(\cdot))$. Si la représentation $\bar{\rho}$ n'est pas modérée, $\rho(P) \not\subset \Gamma_2(R)$ mais pour calculer la déformation universelle, nous procédons par analogie. On fait agir un sous-groupe A de $H = \mathrm{Gal}(K/\mathbf{Q})$ d'ordre premier à p sur un pro-p-sous-groupe de Sylow P de $G = \mathrm{Gal}(K_{S,p}/\mathbf{Q})$. Il convient alors de connaître $\rho(A)$, $\mathrm{Hom}_A(P, \Gamma_2(R))$, $\rho(K/F)$ (où F est le sous-corps de $\mathbf{Q}_{S,p}$ fixe par P et K le sous-corps fixe par $\ker \bar{\rho}$)...
Soit a un générateur de $\mathbf{F}_p^*$. Soit A le sous-groupe de H engendré par

$$\alpha = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \gamma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Le groupe A est d'ordre premier à p. Il s'identifie à un sous groupe de $G = \mathrm{Gal}(K_{S,p}/\mathbf{Q})$.

Définition 6.4.1 *Une représentation pleine est dite régulière si les conditions suivantes sont satisfaites :*
i. elle est impaire,
ii. elle admet un relèment à $\mathbf{Z}_p$,
iii. $\overline{P}$ *est engendré comme* $\mathbf{F}_p[A]$*-module par* $\overline{x}$ *et des générateurs premiers à l'adjoint où* $\overline{x}$ *engendre l'image de* $\mathbf{F}_p[A]$ *dans* $\overline{P}$.

Proposition 6.4.2 *On suppose $p > 3$. Si $\bar{\rho}$ est pleine et régulère, alors $R_{\bar{\rho}} = \mathbf{Z}_p[[T_1, T_2, T_3]]$ et la déformation universelle est donnée sur les générateurs spéciaux par*

$$s \mapsto \begin{pmatrix} 1 & 1+T \\ 0 & 1 \end{pmatrix}$$

$$x \mapsto \begin{pmatrix} 1+U_1 & U_2 \\ U_3 & 1+U_4 \end{pmatrix}$$

et les autres s'envoient sur l'identité. Les $U_1, \ldots, U_i$ s'obtiennent à partir d'une permutation de T_1, T_2, T_3 et d'une série formelle de $R_{\bar{\rho}}$ et $T \in R_{\bar{\rho}}$.

PREUVE : L'hypothèse de régularité impose $R_{\bar{\rho}} = \mathbf{Z}_p[[T_1, T_2, T_3]]$. Soit Q le pro-p-sous-groupe de Sylow de G tel que $\bar{\rho}(Q) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Le sous-groupe $\langle \alpha \rangle$ de A agit sur Q par conjugaison. Donc il existe $s \in Q$ tel que $\bar{\rho}(s) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\alpha \cdot s = s^{a^2}$ (où $a \in \mathbf{Z}_p$ est une notation abusive pour le relèvement de Teichmüller de $a \in \mathbf{F}_p$). De plus s^p, $(\gamma s)^3 \in P$. Dans $R_{\bar{\rho}}[[T, U_1, U_2, U_3, U_4]]$, les images de x et s s'écrivent de la façon la plus générale possible donnée par l'énoncé. En effet, il s'agit d'effectuer des calculs élémentaires du type

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1+X_1 & 1+X_2 \\ X_3 & 1+X_4 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1+X_1 & a^2(1+X_2) \\ a^{-2}X_3 & 1+X_4 \end{pmatrix}$$

$$\begin{pmatrix} 1+X_1 & 1+X_2 \\ X_3 & 1+X_4 \end{pmatrix} \begin{pmatrix} 1+X_1 & 1+X_2 \\ X_3 & 1+X_4 \end{pmatrix} = \begin{pmatrix} (1+X_1)^2 + X_3(1+X_2) & (1+X_2)(2+X_1+X_4) \\ X_3(2+X_2+X_4) & (1+X_4)^2 + X_3(1+X_2) \end{pmatrix}$$

pour montrer que $s \mapsto \begin{pmatrix} 1 & 1+T \\ 0 & 1 \end{pmatrix}$. Or

$$s^p \mapsto \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$$

$$(\gamma s)^3 \mapsto \begin{pmatrix} 1+T & 2T \\ -2T & 1-T \end{pmatrix}$$

en terme d'image de x elles sont toutes les deux de la forme

$$\begin{pmatrix} 1+\sum a_i U_i & \sum b_i U_i \\ \sum c_i U_i & 1+\sum d_i U_i \end{pmatrix} \mod \mathfrak{m}_{R_{\bar{\rho}}}.$$

On obtient donc deux équations de la forme $T \equiv \sum a_i U_i \mod \mathfrak{m}_R^2$ et $p \equiv \sum b_i U_i \mod \mathfrak{m}_R^2$. La première équation montre que T est une série formelle en les U_i, la deuxième montre que l'un des U_i s'exprime en fonction des autres car $p \equiv 0 \mod \mathfrak{m}_R^2$ est exclu par l'existence d'un relèvement à $\mathbf{Z}_p$. ∎

6.5 Le cas résoluble

L'objet de ce paragrahe est d'illustrer qur un exemple le sens arithmétique des hypothèses premier-à-l'adjoint qui pouvaient sembler artificielles dans les des exemples de calculs précédents. On suppose à présent $\bar{\rho} : G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p)$ avec $S = \{\infty, p\}$ et

$$\bar{\rho} \subset \begin{pmatrix} \omega^i & * \\ 0 & \omega^j \end{pmatrix}$$

avec ω caratère cyclotomique, $i + j \equiv 1 \mod p - 1$ et le centralisateur de $\mathrm{im}\,\bar{\rho}$ dans $\mathrm{GL}_2(\mathbf{F}_p)$ est le groupe des homothéties. Notons K le sous-corps de $\mathbf{Q}_S$ fixe par $\ker \bar{\rho}$, $G = \mathrm{Gal}(K_{S,p}/\mathbf{Q})$, P le pro-p-groupe de Sylow de G, $A = G/P = \mathrm{Gal}(F/\mathbf{Q})$ où ici $F = \mathbf{Q}(\zeta_p)$.
Pour ν un caractère de A et M un $\mathbf{F}_p[A]$-module, on note M_ν le plus grand qouq-mosule de M sur lequel A agit par ν. On note $\mathbf{F}_p^\nu$ le $\mathbf{F}_p[A]$-module sur lequel A agit par ν. Enfin on note $M(1)$ le module M tordu par l'action du caractère cyclotomique. Ainsi la représentation adjointe ad se décompose comme $\mathbf{F}_p[A]$ module sous

$$0 \longrightarrow \mathrm{ad}^0 \longrightarrow \mathrm{ad} \longrightarrow \mathbf{F}_p \longrightarrow 0$$

où ad^0 désigne les matrices de trace nulle, l'action par conjugaison de A laisse invariant la trace. La $\mathbf{F}_p[A]$-représentation ad^0 admet la décomposition

$$0 \longrightarrow W_1 \longrightarrow \mathrm{ad}^0 \longrightarrow \mathbf{F}_p^\psi \longrightarrow 0$$

$$0 \longrightarrow \mathbf{F}_p^{\psi^{-1}} \longrightarrow W_1 \longrightarrow \mathbf{F}_p \longrightarrow 0$$

où $W_1 = \left\{ \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}, a, b \in \mathbf{F}_p \right\}$ et $\psi = \omega^{j-i}$ (faire les calculs élémentaires de conjugaison par les éléments de A).

Lemme 6.5.1 *Les conditions suivantes sont équivalentes :*
i. $Ш_S^2(F, \mathbf{F}_p)$ *est premier à l'adjoint,*
ii. $Ш_S^2(F, \mathbf{F}_p^\nu)^A = 0$, $\nu \in \{\mathrm{Id}, \psi, \psi^{-1}\}$,
ii. $Ш_S^2(\mathbf{Q}, \mathbf{F}_p^\nu) = 0$, $\nu \in \{\mathrm{Id}, \psi, \psi^{-1}\}$.

PREUVE : $i \Leftrightarrow ii$ car le corps F trivialise l'action de A. Pour l'équivalence avec le iii, il suffit de revenir à la définition des groupes de Shafarevich pour voir $Ш^2_S(F, \mathbf{F}_p^\nu)^A = Ш^2_S(\mathbf{Q}, \mathbf{F}_p^\nu)$ car A est d'ordre premier à p. ∎

Remarque 6.5.2 *Si $\mu_p \subset F$, le groupe de Safarevich*

$$Ш^2_S(F, \mathbf{F}_p^\nu) = \ker(H^1(\mathrm{Gal}(F_S/F), \mu_p) \longrightarrow \oplus_{s\in S} H^1(\mathrm{Gal}(\overline{F_v}/F_v, \mu_p))$$

permet de comprendre le défaut d'unicité de la factorisation en éléments premiers dans $F^*/F^{*}p$, donc de comprendre les unités et le groupe des classes de F. En utilisant la théorie de Kummer et la théorie du corps de classe, on peut identifier $Ш^1_S(F, \mu_p) = \mathrm{Hom}(\mathrm{Cl}_S(F), \mu_p)$ où $\mathrm{Cl}_S(F)$ est le p-groupe des S-classes de F.

Proposition 6.5.3 *Le groupe $Ш^2_S(F, \mathbf{F}_p)$ est premier à l'adjoint si et seulement si $\mathrm{Cl}_S(F)_{\omega\nu} = 0$ pour $\nu \in \{\mathrm{Id}, \psi, \psi^{-1}\}$.*

PREUVE : Comme $\mathbf{F}_p = \mu_p^{\omega^{-1}}$, d'après la dualité du théorème de Poitou-tate,

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

. Or $Ш^1_S(F, \mu_p) = \mathrm{Hom}(\mathrm{Cl}_S(F), \mu_p)$. L'action de $\mathrm{Gal}(\mathbf{Q}_S/F)$ sur μ_p est triviale, donc

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

Ainsi, vu que $\mathrm{Cl}_S(F)$ est un p-groupe,

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

et

$$Ш^2_S(F, \mathbf{F}_p) = (\mathrm{Cl}_S(F))^{\omega^{-1}\nu^{-1}})^A = (\mathrm{Cl}_S(F))_{\omega\nu}.$$

∎

La conjecture de Vandiver prédit que

$$\mathrm{Cl}_S(\mathbf{Q}(\zeta_p))_{\omega^{2j}} = 0, 2j \in [2, p-1],$$

avec $S = \{\infty, p\}$.

Remarque 6.5.4 *les ω^{2j+1}-parties du groupe des classes sont beaucoup moins mystérieuses et leur nullité est reliée à la divisibilité par p des numérateurs de noombre de Bernouilli (voir [?], [?]). En particulier, on a $\mathrm{Cl}_S(\mathbf{Q}(\zeta_p))_\omega = 0$.*

Proposition 6.5.5 *La conjecture de Vandiver est vraie si et seulement si pour toute représentation non diagonale*

$$\bar{\rho} : G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \text{ avec } S = \{p, \infty\} \text{ et } \bar{\rho} \subset \begin{pmatrix} \omega^i & * \\ 0 & \omega^j \end{pmatrix}$$

$i + j \equiv 1 \mod p - 1$ *et le centralisateur de* $\mathrm{im}\,\bar{\rho}$ *dans* $\mathrm{GL}_2(\mathbf{F}_p)$ *est le groupe des homothéties, l'anneau de déformations universel est* $\mathbf{Z}_p[[T_1, T_2, T_3]]$.

Preuve : Supposons que la conjecture de Vandiver soit vraie. Prenons une représentation $\bar{\rho}$ de la forme de l'énoncé. La condition premier-à-l'adjoint pour $Ш^2_S(F, \mathbf{F}_p)$ est équivalente à

$$\mathrm{Cl}_S(F)_\omega = 0, \mathrm{Cl}_S(F)_{\omega^{i-j+1}} = 0, \mathrm{Cl}_S(F)_{\omega^{j-i+1}} = 0$$

conditions satisfaites ici. Pour $\nu \in \{\mathrm{Id}, \omega^{i-j}, \omega^{j-i}\}$, on a la suite de Poitou-Tate

$$0 \longrightarrow H^2(\mathrm{Gal}(\mathbf{Q}_S/F), \mathbf{F}_p)_\nu \longrightarrow H^2(G_{F_v}, \mathbf{F}_p)_\nu \longrightarrow (H^0(\mathrm{Gal}(\mathbf{Q}_S/F, \mu_p)^*)_\nu \longrightarrow 0.$$

Donc (utiliser la dualité locale) $H^2(G_S(F), \mathbf{F}_p)_\nu) = 0$. Par dévissage et avec la suite exacte longue de cohomologie, on en déduit $H^2(G_{\mathbf{Q},S}, \mathrm{ad}) = 0$. Ainsi $R_{\bar{\rho}} = \mathbf{Z}_p[[T_1, \ldots, T_r]]$ avec $r = \dim_{\mathbf{F}_p} H^1(G_{\mathbf{Q},S}, \mathrm{ad})$. Or comme $\mathbf{F}_p[A]$ (A diagonal) module,

$$\overline{P} = \mathrm{Ind}_{A_\infty}^{A} \tilde{\mathbf{F}}_p \oplus \mathbf{F}_p \oplus \mathrm{Coker}\left(\mu_p(F) \longrightarrow \mu_p(F_v)\right) \oplus B_S$$

et ici $S = \{p, \infty\}$, $\mathrm{Coker}\left(\mu_p(F) \longrightarrow \mu_p(F_v)\right) = 0$. Or B_S est premier à l'adjoint donc $r = 3$. Réciproquement si $\mathrm{Cl}_S(F)_{\omega^{2j}} \neq 0$, on peut construire une représentation $\bar{\rho}$ de la forme de l'énoncé pour laquelle $\dim_{\mathbf{F}_p} H^1(G_S, \mathrm{ad}) = d \leq 4$ (définir $\bar{\rho}$ à l'aide des gńérateurs spéciaux de $\overline{P}$), donc

$$R_{\bar{\rho}} = \mathbf{Z}_p[[T_1, \ldots, T_d]]/I$$

avec $d \geq 4$ et $I \subset (T_i T_j, pT_j, 1 \leq i \leq d)$ donc $R_{\bar{\rho}} \neq \mathbf{Z}_p[[T_1, T_2, T_3]]$. ∎

7 Comparaison local/global

7.1 Comparaison local-global

Dans ce paragraphe K désigne un corps de nombres, S est un ensemble fini de places contenant les places $v|p$ et $v|\infty$. Le groupe de Galois de la plus grande extension K_S de K dans $\overline{K}$ non

ramifiée en dehors de S est noté G_S. On note $\Sigma \subset S$ un sous-ensemble de places.
Pour toute place v de K, on note $G_v = \mathrm{Gal}(\overline{K}_v/K_v)$. Pour tout v, on fixe un homomorphisme $\overline{K} \to \overline{K}_v$ qui prolonge $K \subset K_v$. Ainsi pour $v \in S$, on a un homomorphisme de groupes $G_v \to G_S$.

Soit $G_S \to \mathrm{GL}(V_{\mathbf{F}})$ une G_S-représentation. On note ad la représentation adjointe et ad^0 la sous-représentation des matrices de trace nulle. Si p ne divise pas la dimension de $V_{\mathbf{F}}$, $\mathrm{ad} = \mathrm{ad}^0 \oplus \mathbf{F}$ ce que nous supposons dans ce paragraphe (ce qui exclut par exemple le cas $p = 2$ et $n = 2$).
Les foncteurs de déformations sont définis sur la catégorie des λ-algèbres locales artiniennes (complètes) de corps résiduel $\mathbf{F}$, pour Λ l'anneau des entiers d'une extension totalement ramifiée de $W(\mathbf{F})[1/p]$. On fixe $\psi : G_S \to \Lambda^*$ un relèvement de $\det V_{\mathbf{F}}$. Le lemme suivant est une application directe du critère de Schlessinger :

Lemme 7.1.1 *Soit D^ψ (resp. $D^{\square,\psi}$ le sous-foncteur de D des déformations de $V_{\mathbf{F}}$ à déterminant fixé :*

$$D^\psi(A) = \{[\xi] \in D(A), \det \xi : G_S \to A^* \text{ se factorise à travers } \psi\}.$$

Les foncteurs $D^{\square,\psi}$ et D^ψ satisfont les hypothèses du critère de Schlessinger. L'espace tangent $D^\psi(\mathbf{F}[\varepsilon]$ est isomorphe à $H^1(G_S, \mathrm{ad}^0)$ et on a une suite exacte

$$0 \longrightarrow \mathrm{ad}^0 / H^1(G_S, \mathrm{ad}^0) \longrightarrow D^{\psi,\square}(\mathbf{F}[\varepsilon]) \longrightarrow D^\psi(\mathbf{F}[\varepsilon]) \longrightarrow 0.$$

Nous supposons que les seuls endomorphismes de $V_{\mathbf{F}}$ comme G_v-représentation, v$\in \Sigma$ et G_S-représentation sont les homothéties. On note alors R_v^ψ et $R_{F,S}^\psi$ les anneaux de déformations universels et $\mathfrak{m}_\Sigma$, $\mathfrak{m}_{F,S}$ leurs idéaux maximaux.

Remarque 7.1.2 *Lorsque ces hypothèses ne sont pas satisfaites, il faut passer aux déformations cadrées. Pour tout $v \in \Sigma$, on fixe une base β_v de $V_{\mathbf{F}}$ et on note $D_v^{\square,\psi}$ le foncteur des déformations cadrées de base β_v de déterminant fixé et $R_v^{\square,\psi}$ son anneau de déformations universel. On note $D_\Sigma^{\square,\psi}$, le foncteur de déformations V_A cadrées munies d'une base β qui relève toutes les bases β_v en $v \in \Sigma$. On note $R_\Sigma^{\square,\psi}$ son anneau de déformations universel. Dans la suite, on se limite aux foncteurs de déformations (non cadrées). Les énoncés analogues pour les déformations cadrées se démontrent de façon similaire.*

Soit $R_\Sigma^\psi = \hat{\otimes}_{\Lambda, v\in\Sigma} R_v^\psi$, l'anneau qui représente le produit des foncteurs représentés par les R_v^ψ (voir sur les points artiniens où le produit tensoriel complété coïncide avec le produit tensoriel habituel). Par propriété universelle des anneaux de déformations et du produit tensoriel, l'anneau $R_{F,S}^\psi$ hérite d'une structure naturelle de R_Σ^ψ-algèbre. On rappelle l'énoncé suivant établi lors de la première séance d'exercices.

Lemme 7.1.3 *Si $f : G \longrightarrow H$ est un homomorphisme continu entre groupes profinis, alors il existe une section continue.*

Théorème 7.1.4 *Nous avons un isomorphisme de R^{ψ}_{Σ}-algèbres*

$$R^{\psi}_{F,S} = R^{\psi}_{\Sigma}[[x_1, \dots, x_r]]/(f_1, \dots, f_{r+s})$$

où $r = \dim_{\mathbf{F}} \ker \Big(H^1(G_S, \mathrm{ad}^0) \to \Pi_{v\in\Sigma} H^1(G_v, \mathrm{ad}^0) \Big)$, $s = c + h_2 - r$ *avec*

$$c = \dim_{\mathbf{F}} \mathrm{Coker} \Big(H^1(G_S, \mathrm{ad}^0) \to \Pi_{v\in\Sigma} H^1(G_v, \mathrm{ad}^0) \Big),$$

$$h_2 = \dim_{\mathbf{F}} \ker \Big(H^2(G_S, \mathrm{ad}^0) \to \Pi_{v\in\Sigma} H^2(G_v, \mathrm{ad}^0) \Big).$$

Preuve : On a une surjection entre anneaux complets de $\hat{\mathcal{C}}$

$$S = R^{\psi}_{\Sigma}[[x_1, \dots, x_r]] \longrightarrow R^{\psi}_{F,S}$$

pour $r = \dim_{\mathbf{F}} \mathrm{Coker} \Big(\mathfrak{m}_{\Sigma}/(\mathfrak{m}^2_{\Sigma}, \mu) \to \mathfrak{m}_{F,S}/(\mathfrak{m}^2_{F,S}, \mu) \Big)$. Et

$$r = \dim_{\mathbf{F}} \ker \Big(\mathrm{Hom}_{\mathbf{F}}(\mathfrak{m}_{F,S}/(\mathfrak{m}^2_{F,S}, \mu), \mathbf{F}) \to \mathrm{Hom}_{\mathbf{F}}(\mathfrak{m}_{\Sigma}/(\mathfrak{m}^2_{\Sigma}, \mu), \mathbf{F}) \Big)$$

$$r = \dim_{\mathbf{F}} \ker \Big(H^1(G_S, \mathrm{ad}^0) \to \Pi_{v\in\Sigma} H^1(G_v, \mathrm{ad}^0) \Big),$$

car l'espace tangent d'un produit est le produit des espaces tangents.
Notons $\mathfrak{m}$ l'idéal maximal de S et $J = \ker(S \to R^{\psi}_{F,S})$. On peut relever $\rho : G_S \longrightarrow \mathrm{GL}_n(R^{\psi}_{F,S})$ en tant qu'application entre ensembles en $\tilde{\rho} : G_S \to \mathrm{GL}_n(S/\mathfrak{m}J)$ mais pas forcément en tant qu'homomorphisme continu. On peut supposer cependant déjà supposer que $\det \tilde{\rho} \cong \psi$ mod $\mathfrak{m}J$. Soit $\pi : S/\mathfrak{m}J \longrightarrow R^{\psi}_{F,S}$ et $\mathrm{obs}_{\pi}(\rho) \in H^2(G_S, \mathrm{ad}^0) \otimes J/\mathfrak{m}J$.
Pour la restriction de $\rho_{|G_v}$, on a un relèvement par universalité de ρ_v :

$$G_v \longrightarrow^{\rho_v} \mathrm{GL}_n(R^{\psi}_v) \to \mathrm{GL}_n(R^{\psi}_{\Sigma}) \longrightarrow \mathrm{GL}_n(S)$$

ainsi $\mathrm{obs}_{\pi}(\rho)_{|G_v} \in H^2(G_v, \mathrm{ad}^0) \otimes J/\mathfrak{m}J$ est nulle. Ainsi on a une application $\mathbf{F}$-linéaire

$$\Phi : \mathrm{Hom}_{\mathbf{F}}(J/\mathfrak{m}J, \mathbf{F}) \to \ker \Big(H^2(G_S, \mathrm{ad}^0) \longrightarrow \Pi_{v\in\Sigma} H^2(G_v, \mathrm{ad}^0) \Big)$$

Il s'agit de montrer que $\dim_k \ker \Phi \leq c$. En effet

$$h_2 = \dim_{\mathbf{F}} \ker H^2(G_S, \mathrm{ad}^0) \longrightarrow \Pi_{v\in\Sigma} H^2(G_v, \mathrm{ad}^0)$$

et $\dim_{\mathbf{F}} J/\mathfrak{m}J \leq h_2 + c$. Or $\dim_{\mathbf{F}} J/\mathfrak{m}J$ est le nombre de relations de J, quite à rajouter des relations nulles si $\dim_{\mathbf{F}} \ker \Phi < c$, on peut supposer que le nombre de relations est $h_2 + c$.
Soit $I = \ker\Big(\mathfrak{m}_\Sigma/(\mathfrak{m}_\Sigma^2 + \mu) \longrightarrow \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2 + \mu)\Big)$. Ainsi, par dualité,

$$\mathrm{Hom}_{\mathbf{F}}(I, \mathbf{F}) \simeq \mathrm{Coker}\Big(H^1(G_S, \mathrm{ad}^0) \to \Pi_{v\in\Sigma} H^1(G_v, \mathrm{ad}^0)\Big).$$

Il suffit donc de construire une injection $\mathbf{F}$-linéaire $\ker\Phi \to \mathrm{Hom}_{\mathbf{F}}(I, \mathbf{F})$. On observe d'abord que

$$I = \ker\Big(\mathfrak{m}/(\mathfrak{m}^2, \mu) \longrightarrow \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \mu)\Big)$$

car on a envoyé les x_i sur une base du conoyau des espaces tangents

$$\mathrm{Coker}\Big(\mathfrak{m}_\Sigma/(\mathfrak{m}_\Sigma^2, \mu) \longrightarrow \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \mu)\Big)$$

Aucun des éléments en plus de $\mathfrak{m}$ ne s'annule quand on l'envoie dans $\mathfrak{m}_{F,S}$.
Ensuite montrons que $J/\mathfrak{m}J$ se surjecte dans I. On a par définition,

$$0 \longrightarrow J \longrightarrow \mathfrak{m} \longrightarrow \mathfrak{m}_{F,S} \longrightarrow 0,$$

donc on a la surjection

$$J/\mathfrak{m}J \longrightarrow \ker\Big(\mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathfrak{m}_{F,S}/\mathfrak{m}_{F,S}^2\Big).$$

Soit $x \in I \subset \mathfrak{m}/(\mathfrak{m}^2, \mu)$. On peut relever x en $\tilde{x} \in \mathfrak{m}/\mathfrak{m}^2$. Comme x s'envoie sur 0 dans $\mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \mu)$, $\tilde{x}$ s'envoie sur $r\mu \mod \mathfrak{m}_{F,S}^2$ pour $r \in R_{F,S}^{\psi}$. On peut relever r en $\tilde{r} \in S$. tel que $\tilde{r} = r \mod J$. En remplaçant $\tilde{x}$ par $\tilde{x} - (\tilde{r}\mu \mod \mathfrak{m}^2)$, on peut supposer que l'image de $\tilde{x}$ est nulle dans $\mathfrak{m}_{F,S}/\mathfrak{m}_{F,S}^2$. Donc $\tilde{x} \in \Big(\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}_{F,S}/\mathfrak{m}_{F,S}^2\Big)$. Donc $\tilde{x}$ est dans l'image de $J/\mathfrak{m}J$ dans $\mathfrak{m}/gm^2$ et on a donc construit une surjection (que l'on peut rendre $\mathbf{F}$-linéaire) $J : \mathfrak{m}J \to I$ et ainsi une injection $\mathrm{Hom}_{\mathbf{F}}(I, \mathbf{F}) \to \mathrm{Hom}_{\mathbf{F}}(J/\mathfrak{m}J, \mathbf{F})$.
Il s'agit enfin de montrer que $\ker\Phi \subset \mathrm{Hom}_{\mathbf{F}}(I, \mathbf{F})$. Or $\Phi : u \mapsto \mathrm{obs}_\pi(\rho)$. Si $\mathrm{obs}_\pi(\rho) = 0$, on veut donc montrer que u se factorise par I, autrement dit s'annule sur $K = \ker(J : \mathfrak{m}J \to I)$. Or $K = J \cap (\mathfrak{m}^2, \mu)$. En effet $I \subset \mathfrak{m}/(\mathfrak{m}^2, \mu)$ donc $J \cap (\mathfrak{m}^2, \mu) \subset K$ et par définition

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J & \longrightarrow & \mathfrak{m} & \longrightarrow & \mathfrak{m}_{F,S} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I & \longrightarrow & \mathfrak{m}/(\mathfrak{m}^2, \mu) & \longrightarrow & \mathfrak{m}_{F,S}/(\mathfrak{m}_{F,S}^2, \mu) & \longrightarrow & 0
\end{array}$$

Donc $K \subset \ker(\mathfrak{m}/(\mathfrak{m}^2, \mu)$ donc $K \subset (\mathfrak{m}^2, \mu)$ et $K \subset J$ donc $K \subset J \cap (\mathfrak{m}^2, \mu)$. On doit donc montrer $J \cap (\mathfrak{m}^2, \mu) \subset \ker u$ (on indetifie $\ker u$ avec $\ker(J \to J/\mathfrak{m}J \to^y \mathbf{F})$. Comme $\mathrm{obs}_\pi(\rho) = 0$, on a un morphisme

$$S = R_\Sigma^{\psi}[[x_1, \ldots, x_r]]/J \to R_\Sigma^{\psi}[[x_1, \ldots, x_r]]/\ker u,$$

x_i s'envoie sur $x_i + a_i$ avec $a_i \in J$ car les x_i s'envoie sur une base de $\ker\Big(H^1(G_{F,S}, \mathrm{ad}^0) \longrightarrow \Pi_{v\in\Sigma} H^1(G_v, \mathrm{ad}^0)\Big)$. Un élément $g \in (\mathfrak{m}^2, \mu) \cap J$ s'écrit $g = g_0 + \sum g_i x_i + O(\mathfrak{m}^2)$ avec $g_i \in \mu R^{\psi}_{\Sigma}$ et a pour image

$$g = g_0 + \sum g_i x_i + O(\mathfrak{m}^2) \mapsto g_0 + \sum g_i (x_i + a_i) + O(\mathfrak{m}^2)$$

or $g_i x_i \in \mathfrak{m}J \subset \ker u$ et de même les termes de plus haut degré qui diffèrent de g s'annulent modulo $\ker u$. D'où $J \cap (\mathfrak{m}^2, \mu) \subset \ker u$.

∎

Ce théorème est le point de départ de la méthode de recollement, *Patching method* de Taylor-Wiles-Kisin pour prouver des résultats de modularité ([Ki]). D'une part, on agrandit l'ensemble des places Σ pour annuler la coposante $Ш^2_{\Sigma}(F, \mathrm{ad})$ purement globale du $H^2(G_{F,\Sigma}, \mathrm{ad})$. Ainsi les relations sont de nature locale et $R^{\psi}_{F,\Sigma}$ est lisse sur $\mathbf{R}^{\psi}_{\Sigma}$. D'autre part, on met des conditions supplémentaires sur les déformations de représentations locales en p de nature géométrique (c'est l'objet de la théorie de Hodge p-adique). Il s'agit alors de construire par induction un isomorphisme entre l'anneau de déformations universel (dont on contrôle les composantes locales) et une certaine algèbre de Hecke (Théorème $R = T$).

References

[Bl] J. Blondeau, *Déformations des extensions peu ramifiés en p*, Thèse 2011.

[Br] C. Breuil, *Representations of Galois and of Gl_2 in characteristic p*, Cours à Columbia 2007.

[Bo] N. Bourbaki, Algèbre commutative.

[Gr] R. Greenberg, *Galois representations with open image*, preprint 2013.

[GS] P. Gille et T. Szamuely, Central simple algebras and Galois cohomology, Cambridge studies in advanced mathematics.

[Ki] M. Kisin, *Lectures on deformations of Galois representations.*

[Ma] B. Mazur, *An introduction to the Deformation Theory of Galois Representations*, dans Modular Forms and Fermat's Last theorem, G. Cornell, J.H. Silverman et G. Stevens eds, Springer-Verlag (1997).

[Mi] J. Milne, Arithmetic duality theorems, Acad. Press, Boston (1986).

[Th] L. Thomas, *Arithmétique des extensions d'Artin-Schreier-Witt*, Thèse 2005.

[Sc] M. Schlessinger, *Functors of Artinians rings.* Transactions of the American Mathematical Society, Vol. 130 No. 2 (1968), p.208–222.

[Se1] J.-P. Serre, Corps locaux.

[Se2] J.-P. Serre, Cohomologie galoisienne.

[Sw] P. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*. Lecture Notes in Math. 350 (1973), 1–55.

[Ta] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), p.257–274.

[Vi] A. Vistoli, *The deformation theory of local complete intersection.*

[Wa] L. Washington, it Galois cohomology, dans Modular Forms and Fermat's Last theorem, G. Cornell, J.H. Silverman et G. Stevens eds, Springer-Verlag (1997).

[Wes] T. Weston, *Unobstrued modular deformations problems*, Amer. Journ. Math. **126** (2004),1237–1252.