
UNE ESTIMATION DE LA DIMENSION DE KRULL DES ANNEAUX DE DÉFORMATIONS EN RAMIFICATION INCOMPLÈTE

par

Christian Maire

Résumé. — Nous étudions la dimension de Krull des anneaux de déformations de représentations galoisiennes quand la ramification en p peut-être incomplète. Sous certaines conditions, nous donnons une minoration non triviale de cette dimension.

Abstract. — We study the Krull dimension of deformation rings associated to Galois representation, with ramification restricted to (not necessarily all) places above p . Under some conditions we give a non trivial minoration of this dimension.

Table des matières

Introduction	129
1. Sur l'importance du multiplicateur de Schur	132
2. Quelques structures galoisiennes	133
3. Sur la dimension de Krull de l'anneau R_S^T	137
4. Détail d'un exemple	138
Références	141

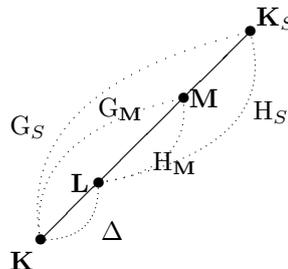
Introduction

Soient \mathbf{K} un corps de nombres et S un ensemble fini de places finies de \mathbf{K} . Pour simplifier, supposons que S ne contient que des places au-dessus de p .

Après s'être fixé une clôture algébrique $\bar{\mathbf{K}}$ de \mathbf{K} , soit

$$\bar{\rho} : \text{Gal}(\bar{\mathbf{K}}/\mathbf{K}) \rightarrow \text{GL}_2(\mathbf{F}_p)$$

une représentation continue du groupe de Galois $G_S := \text{Gal}(\bar{\mathbf{K}}_S/\mathbf{K})$ de la plus grande extension galoisienne $\bar{\mathbf{K}}_S$ de \mathbf{K} pour laquelle les places finies en dehors de S y sont non-ramifiées. Notons par \mathbf{L} l'extension galoisienne maximale de \mathbf{K} fixée par $\ker(\bar{\rho})$; $\text{Gal}(\mathbf{L}/\mathbf{K}) \simeq \Delta = \text{Im}(\bar{\rho})$.



Classification mathématique par sujets (2000). — Primary 11R37; Secondary 11R34 .

Mots clefs. — ramification restreinte, anneaux de déformations galoisiennes.

Ce travail a été rédigé lors de mon séjour à l'École Polytechnique de Lausanne, durant l'été 2004. Je remercie Éva Bayer pour son invitation. Je remercie également Christophe Delaunay et Thong Nguyen Quang Do pour leurs remarques.

Pour une extension galoisienne \mathbf{M} de \mathbf{K} contenue dans \mathbf{K}_S et contenant \mathbf{L} , posons $H_{\mathbf{M}} = \text{Gal}(\mathbf{M}/\mathbf{L})$ et $G_{\mathbf{M}} = \text{Gal}(\mathbf{M}/\mathbf{K})$. La surjection canonique $G_S \rightarrow G_{\mathbf{M}}$ permet alors à la représentation $\bar{\rho}$ de se factoriser à travers $G_{\mathbf{M}}$.

Soit \mathcal{C} la catégorie des anneaux locaux (R, \mathfrak{m}_R) noetherien complet de corps résiduel \mathbb{F}_p . Si R est un élément de \mathcal{C} et $\rho : G_{\mathbf{M}} \rightarrow \text{Gl}_2(R)$ une représentation continue de $G_{\mathbf{M}}$, on dit que celle-ci est un relèvement de la représentation $\bar{\rho}$ si le diagramme suivant est commutatif

$$\begin{array}{ccc} G_{\mathbf{M}} & \xrightarrow{\rho} & \text{Gl}_2(R) \\ & \searrow \bar{\rho} & \downarrow \text{mod } \mathfrak{m}_R \\ & & \text{Gl}_2(\mathbb{F}_p) \end{array}$$

Si $\rho' : G_{\mathbf{M}} \rightarrow \text{Gl}_2(R)$ est une autre représentation de $G_{\mathbf{M}}$, les représentations ρ et ρ' sont dites strictement équivalentes si elles sont conjuguées par un élément de $\ker \left(\text{Gl}_2(R) \xrightarrow{\text{mod } \mathfrak{m}_R} \text{Gl}_2(\mathbb{F}_p) \right)$. Une classe de conjugaison d'une telle représentation ρ est appelée une déformation de $\bar{\rho}$ à R .

Comme S est fini, des travaux de Mazur [15] montrent l'existence d'un élément $R_{\mathbf{M}}$ de \mathcal{C} et d'une représentation verselle $\rho_{\mathbf{M}} : G_{\mathbf{M}} \rightarrow \text{Gl}_2(R_{\mathbf{M}})$ relevant la représentation $\bar{\rho}$. Tout relèvement $\rho' : G_{\mathbf{M}} \rightarrow \text{Gl}_2(R)$ de $\bar{\rho}$, avec $R \in \mathcal{C}$, se factorise à travers $\rho_{\mathbf{M}}$, c'est à dire qu'il existe un morphisme d'anneau local $\varphi : R_{\mathbf{M}} \rightarrow R$ où la composée $\varphi \circ \rho_{\mathbf{M}}$ produit un relèvement de $\bar{\rho}$ strictement équivalent à ρ' . L'anneau $R_{\mathbf{M}}$ est unique, et est appelé anneau de déformation de la représentation $\bar{\rho}$ (associée à l'extension \mathbf{M}/\mathbf{K}). Lorsque $\bar{\rho}$ est absolument irréductible (non triviale) la représentation $\rho_{\mathbf{M}}$ est de plus universelle, c'est à dire que la donnée de $\rho_{\mathbf{M}}$ détermine φ .

Si l'on note par Ad la représentation adjointe associée à $\bar{\rho}$, Mazur a montré que la dimension de Krull de l'anneau $R_{\mathbf{M}}/pR_{\mathbf{M}}$ est minorée par la quantité $d_p H^1(G_{\mathbf{M}}, \text{Ad}) - d_p H^2(G_{\mathbf{M}}, \text{Ad})$. En fait, l'anneau de déformation $R_{\mathbf{M}}$ est de la forme $\mathbb{Z}_p[[T_1, \dots, T_r]]/I$, où $r = \dim_{\mathbb{F}_p} H^1(G_{\mathbf{M}}, \text{Ad})$. L'idéal I est trivial dès lors que le groupe de cohomologie $H^2(G_{\mathbf{M}}, \text{Ad})$ l'est. Si tel est le cas (i.e. $I = (0)$), on dit que la déformation $\rho_{\mathbf{M}}$ est sans obstruction.

Remarquons que comme le noyau de la restriction $\text{Gl}_2(R) \rightarrow \text{Gl}_2(\mathbb{F}_p)$ est un pro- p -groupe (voir par exemple [1]), tout relèvement de $\bar{\rho} : G_{\mathbf{M}} \rightarrow \text{Gl}_2(\mathbb{F}_p)$ se factorise à travers la plus grande pro- p -extension $\mathbf{M}(p)$ de \mathbf{L} contenue dans \mathbf{M} .

Fixons T un second ensemble fini de places finies de \mathbf{K} . Assurons-nous que T et S sont disjoints. Nous nous intéressons au cas où le corps \mathbf{M} correspond à $\mathbf{L}_S^T(p)$, où $\mathbf{L}_S^T(p)$ est la plus grande extension de \mathbf{L} contenue dans \mathbf{K}_S pour laquelle l'ensemble des places au-dessus des places de T y sont totalement décomposées. Nous noterons par R_S^T son anneau de déformation et par $\rho_S^T : \text{Gal}(\mathbf{L}_S^T(p)/\mathbf{K}) \rightarrow \text{Gl}_2(R_S^T)$ une déformation verselle de $\bar{\rho}$ associée à cette extension. Posons $P_S^T = H_{\mathbf{L}_S^T(p)} = \text{Gal}(\mathbf{L}_S^T(p)/\mathbf{L})$ le groupe de Galois de l'extension $\mathbf{L}_S^T(p)/\mathbf{L}$.

Lorsque S contient l'ensemble des places au-dessus de p , grâce à la dualité de Poitou-Tate (cf. par exemple [9], [17]), Mazur a montré comment obtenir une minoration de la dimension de Krull de l'anneau R_S . Ce point de départ a ensuite été utilisé par de nombreux auteurs (Mazur [15], Boston [3], Boston et Mazur [4], Ramakrishna [18], Böckle [1] [2], Böckle et Mézard [16], Gouvêa [6], ...). Dans ce cas (ici $T = \emptyset$), la différence $d_p H^1(G_S, \text{Ad}) - d_p H^2(G_S, \text{Ad})$ est parfaitement connue. Avant d'en donner une évaluation, donnons une définition.

Définition 0.1. — Une place infinie v de \mathbf{K} est dite *impaire* (relativement à $\bar{\rho}$) si le déterminant de $\bar{\rho}(s_v)$ est -1 , où s_v est un générateur du sous-groupe de décomposition Δ_v de v dans Δ .

La place v est dite *paire* sinon.

Notons par κ_1 le nombre de places infinies v de \mathbf{K} en lesquelles la représentation $\bar{\rho}|_{\Delta_v}$ est impaire et par κ_0 le nombre de places infinies de \mathbf{K} en lesquelles la représentation $\bar{\rho}|_{\Delta_v}$ est paire. Il vient :

$$\begin{aligned} d_p H^1(G_S, \text{Ad}) - d_p H^2(G_S, \text{Ad}) &= d_p H^0(G_S, \text{Ad}) + 4(r_1 + 2r_2) \\ &\quad - 4\kappa_0 - 2\kappa_1 \\ &\geq 1 + 4(r_1 + 2r_2) - 4\kappa_0 - 2\kappa_1 \\ &= 1 + 2\kappa_1 + 4r_2, \end{aligned}$$

où (r_1, r_2) est la signature du corps \mathbf{K} (à noter que le G_S -module Ad contient au moins un sous-espace non réduit à $\{0\}$ avec action triviale, les matrices diagonales).

Malheureusement, une telle démarche n'est plus possible dès que S ne contient plus à priori toutes les places au-dessus de p (c'est ce que l'on appelle la situation p -ramification incomplète). Néanmoins, lorsque $(\#\Delta, p) = 1$, nous donnons ici une minoration non triviale de la dimension de Krull de l'anneau R_S^T/pR_S^T dès lors que le poids δ_S de S est suffisamment grand.

Définition 0.2. — Nous définissons le *poids* δ_S de S comme étant la quantité

$$\delta_S = \sum_{v \in S} [\mathbf{K}_v : \mathbb{Q}_p].$$

Définition 0.3. — Supposons Δ d'ordre premier à p . Soit v une place de \mathbf{K} . Notons par Δ_v le groupe de décomposition de v dans \mathbf{L}/\mathbf{K} . Soit $\bar{\rho}_v := \bar{\rho}|_{\Delta_v}$ la restriction de $\bar{\rho}$ à Δ_v . Notons alors par τ_v le nombre de fois qu'apparaît la représentation triviale dans la décomposition du Δ_v -module Ad . Ou encore : $\tau_v = \langle \text{Ad}, \mathbf{1} \rangle_{\Delta_v}$. Posons $\kappa_v = 4 - \tau_v$, puis pour Σ un ensemble de places de \mathbf{K} ,

$$\kappa_\Sigma = \sum_{v \in \Sigma} \kappa_v.$$

Remarque 0.4. — Notons par Pl_∞ l'ensemble des places archimédiennes de \mathbf{K} . Alors $\kappa_{Pl_\infty} = 2\kappa_1$.

Démonstration. — En effet, une place v est impaire si et seulement si $\tau_v = 2$. Sinon $\tau_v = 4$. \diamond

On en arrive à l'énoncé du résultat principal.

Théorème 0.5. — *Supposons $\#\Delta$ premier à p et $\delta_S \geq r_1 + r_2 + |T|$. Alors*

$$\dim_{\text{krull}}(R_S^T/pR_S^T) \geq 1 + 2\kappa_1 + \kappa_T + 4(\delta_S - (r_1 + r_2 + |T|)).$$

(Si $\text{Im}(\bar{\rho})$ est un sous-groupe de Cartan l'inégalité est stricte.)

Corollaire 0.6. — *Plaçons nous sous les conditions du théorème précédent. Supposons de plus que pour toute place v de T , $\Delta_v = \{1\}$. Alors*

$$\dim_{\text{krull}}(R_S^T/pR_S^T) \geq 1 + 2\kappa_1 + 4(\delta_S - (r_1 + r_2 + |T|)).$$

(Si $\text{Im}(\bar{\rho})$ est un sous-groupe de Cartan l'inégalité est stricte.)

Notons que la condition $\delta_S \geq r_1 + r_2 + |T|$ implique l'existence d'une \mathbb{Z}_p -extension de \mathbf{L} contenue dans $\mathbf{L}_S^T(p)/\mathbf{L}$.

Le théorème 0.5 se montre en utilisant l'action semi-simple de Δ sur les groupes de cohomologie $H^i(P_S^T, \text{Ad})$, $i = 1, 2$. Nous explicitons cette action galoisienne dans le paragraphe 3. Dans le paragraphe 4, nous montrons le théorème principal. Enfin, le dernier paragraphe est consacré à l'étude d'un exemple se situant dans la lignée de l'exemple étudié par Mazur dans [15].

À noter qu'ici nous ne regardons l'anneau R_S^T que sous un angle purement arithmétique.

Notations. Pour un \mathbb{Z}_p -module de type fini M , nous désignerons par

$$\text{Tor}(M) = \{m \in M, \exists k \in \mathbb{Z}_p, m^k = 1\}$$

le sous-module de torsion de M , et par

$$\text{Tor}_p(M) = \{m \in M, m^p = 1\},$$

le sous-module de p -torsion de M .

Pour un corps \mathbf{F} , $\mu_p(\mathbf{F})$ désignera le groupe des racines p -èmes de l'unité contenues dans \mathbf{F} et pour un groupe abélien localement compact G , son dual de Pontryagin sera noté G^* .

1. Sur l'importance du multiplicateur de Schur

Nous allons montrer le rôle crucial que joue le multiplicateur de Schur dans le calcul de la dimension de Krull de l'anneau R_M . Commençons par un premier lemme :

Lemme 1.1. — *La suite exacte $1 \rightarrow H_M \rightarrow G_M \rightarrow \Delta \rightarrow 1$ fournit l'isomorphisme de Δ -modules suivant :*

$$H^i(H_M, \text{Ad}) \simeq H^i(H_M, \mathbb{F}_p) \otimes \text{Ad}.$$

Démonstration. — Il suffit de noter que H_M agit trivialement sur Ad , \mathbb{F}_p -espace vectoriel de dimension 4, puis que l'isomorphisme souhaité est obtenu via la composition des isomorphismes suivants :

$$H^i(H_M, \mathbb{F}_p) \otimes \text{Ad} \xrightarrow{\sim} \bigoplus_{j=1}^4 H^n(H_M, \mathbb{F}_p) e_j \xrightarrow{\sim} H^n(H_M, \text{Ad})$$

et que ceux-ci sont bien des isomorphismes de Δ -modules (où (e_1, \dots, e_4) est une \mathbb{F}_p -base de Ad).

◇

Lemme 1.2. — *Soit G un pro- p -groupe de type fini. Alors*

$$d_p H^1(G, \mathbb{F}_p) - d_p H^2(G, \mathbb{F}_p) = d_p \text{Fr}_{\mathbb{Z}_p} G - d_p H_2(G, \mathbb{Z}_p),$$

où $\text{Fr}_{\mathbb{Z}_p} G$ désigne la partie \mathbb{Z}_p -libre de G^{ab} . Si de plus $H_2(G, \mathbb{Z}_p)$ est trivial alors, $H^2(G, \mathbb{F}_p) \simeq \text{Tor}_p(G^{ab})$.

Démonstration. — C'est bien connu, cela résulte de la suite exacte courte :

$$1 \rightarrow \mathbb{F}_p \rightarrow \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p \rightarrow 1.$$

◇

Lemme 1.3. — Supposons $\#\Delta$ premier à p .

(i) On a, pour tout $i \geq 1$, $H^i(\mathbf{G}_M, \text{Ad}) \simeq [H^i(\mathbf{H}_M, \mathbb{F}_p) \otimes \text{Ad}]^\Delta$.

(ii) $H^1(\mathbf{G}_M, \text{Ad}) \simeq [(H_M^{ab})^* \otimes \text{Ad}]^\Delta$, où $H_M^{ab} := \mathbf{H}_M/[\mathbf{H}_M, \mathbf{H}_M]$.

(iii) Si le groupe $H^2(\mathbf{H}_M, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial, il vient alors :

$$H^2(\mathbf{G}_M, \text{Ad}) \simeq [(\text{Tor}_p(H_M^{ab}))^* \otimes \text{Ad}]^\Delta.$$

Démonstration. — (i) Comme $\#\Delta$ est premier à p , la suite spectrale au niveau supérieur donne l'isomorphisme entre $H^i(\mathbf{G}_M, A)$ et $H^i(\mathbf{H}_M, A)^\Delta$ et ce pour tout \mathbf{G}_M -module discret p -primaire de torsion A . Il suffit ensuite d'utiliser le lemme 1.1.

(ii) C'est un cas particulier du point précédent.

(iii) Sous l'hypothèse $H^2(\mathbf{H}_M, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, on a $\text{Tor}_p(H_M^{ab}) \simeq H_2(\mathbf{H}_M, \mathbb{F}_p)$. Il suffit ensuite d'utiliser le point (i). \diamond

Ainsi, ces trois lemmes montrent que pour avoir une minoration non triviale de la dimension de Krull de \mathbf{R}_M , il est souhaitable que d'une part le corps \mathbf{L} ait au moins une \mathbb{Z}_p -extension contenue dans \mathbf{M}/\mathbf{L} (ou encore que $\text{Fr}_{\mathbb{Z}_p}\mathbf{H}_M$ soit non trivial) et que d'autre part l'on puisse contrôler le multiplicateur de Schur $H_2(\mathbf{H}_M, \mathbb{Z}_p)$ du groupe \mathbf{H}_M .

Quand S contient l'ensemble des places au-dessus de p et pour $\mathbf{M} = \mathbf{L}_S(p)$, ces deux quantités sont intimement liées. En fait, la conjecture de Leopoldt pour le couple (\mathbf{L}, p) , donne exactement le rang de $\text{Fr}_{\mathbb{Z}_p}\mathbf{H}_S$, et cette conjecture équivaut à la trivialité du multiplicateur de Schur du groupe $\text{Gal}(\mathbf{L}_S(p)/\mathbf{L})$.

Maintenant, lorsque S ne contient pas toutes les places au-dessus de p , il est quand même possible d'obtenir des informations sur ce multiplicateur de Schur. Comme pour le cas où S contient l'ensemble des places au-dessus de p , nous verrons (cf. corollaire 2.4) que le multiplicateur de Schur de ce groupe $\text{Gal}(\mathbf{L}_S(p)/\mathbf{L})$ est aussi dans ce cas lié à un problème d'indépendance p -adique.

2. Quelques structures galoisiennes

Pour toute la suite, nous supposons que l'ensemble S est non vide et qu'il ne contient que des places finies v au-dessus de p .

2.1. Les notations. — Pour une place v de \mathbf{K} , notons par $\Delta_v = \Delta_w$ le groupe de décomposition dans \mathbf{L}/\mathbf{K} d'une place quelconque w de \mathbf{L} au-dessus de v . Pour un ensemble E de places de \mathbf{K} , nous notons par $E(\mathbf{L})$ l'ensemble des places \mathbf{L} au-dessus des places de E .

Soit

$$\text{III}_S^T(\mathbf{L}) = \{x \in \mathbf{L}^\times, v_w(x) \equiv 0 \pmod{p}, \forall w \notin T(\mathbf{L}); x \in \mathbf{L}_w^p, \forall w \in S(\mathbf{L})\}/\mathbf{L}^{\times p}$$

le groupe de Shafarevich du corps \mathbf{L} associé aux ensembles S et T .

Pour w une place finie de \mathbf{L} , notons \mathfrak{U}_w le sous-groupe des unités principales du complété \mathbf{L}_w de \mathbf{L} en w . Soit $\mathfrak{U}_S = \prod_{w \in S(\mathbf{L})} \mathfrak{U}_w$ et soit

$$\Psi_S^T = \mathbb{Z}_p \otimes E_{\mathbf{L}}^T \rightarrow \mathfrak{U}_S$$

le plongement des $T(\mathbf{L})$ -unités $E_{\mathbf{L}}^T$ de \mathbf{L} dans le produit des complétés des places de $S(\mathbf{L})$ (qui rappelons-le sont toutes au-dessus de p).

Fixons \mathbb{C}_p le complété d'une clôture algébrique de \mathbb{Q}_p . Lorsque w est une place de $S(\mathbf{L})$, notons par \log_w le logarithme p -adique associé à la place w . Pour $x = (x_1, \dots, x_s) \in \mathfrak{U}_S$, nous posons

$$\text{Log}(x) = (\log_{w_1}(x_1), \dots, \log_{w_s}(x_s)) \in \mathbb{C}_p^s.$$

2.2. Les principales estimations. —

Supposons $\#\Delta$ premier à p .

Pour un $\mathbb{Z}_p[\Delta]$ -module M et un caractère $\mathbb{C}_p[\Delta]$ -irréductible φ , M_φ désignera la φ -partie de ce module et $r_\varphi(M)$ le φ -rang de M . Rappelons que M_φ est vu comme module sur l'anneau local $\mathbb{Z}_p[\varphi]$. Si ψ et ψ' sont deux caractères de $\mathbb{Z}_p[\Delta]$, nous noterons par $\langle \psi, \psi' \rangle$ le produit scalaire entre ceux-ci. Si M est un $\mathbb{Z}_p[\Delta]$ -module, on identifiera M avec son caractère. Ainsi, par exemple, si φ est \mathbb{C}_p -irréductible, $r_\varphi(M) = \langle M, \varphi \rangle$.

Pour un sous-groupe H de Δ et un H -module M , $\text{Ind}_H^\Delta(M)$ désignera le Δ -module induit de H à Δ obtenu à partir de M . On rappelle la formule de réciprocity :

$$\langle M, \text{Ind}_H^\Delta N \rangle = \langle M, N \rangle_{|H}.$$

Si χ est le caractère du Δ -module M , le caractère du dual M^* de M sera noté χ^* . On rappelle que pour tout σ de Δ , on a $\chi^*(\sigma) = \chi(\sigma^{-1})$.

Nous noterons par $\mathbf{1}$ le caractère de la représentation triviale (ou unité) : $\mathbf{1}(\sigma) = 1$, pour tout $\sigma \in \Delta$.

Soit donc $P_S^T = \text{Gal}(\mathbf{L}_S^T(p)/\mathbf{L})$. La structure du Δ -module $P_S^{T,ab} := P_S^T/[P_S^T, P_S^T]$ est parfaitement connue :

Proposition 2.1 (Gras [7]). — *Soit φ un caractère \mathbb{C} -irréductible de Δ . Alors*

$$r_\varphi(P_S^{T,ab}) = r_\varphi(\text{III}_S^T(\mathbf{L})) - r_\varphi(\mathbf{E}_\mathbf{L}^T) + \sum_{v \in S} \delta_v r_\varphi \text{Ind}_{\Delta_v}^\Delta \mu_p(\mathbf{L}_v) + \varphi(1)(\delta_S + \delta_{2,p} r_1(\mathbf{L})),$$

où $\delta_S = \sum_{v \in S} [\mathbf{K}_v : \mathbb{Q}_p]$, où $\delta_v = \delta_w = 1$ si \mathbf{L}_w contient les racines p -èmes de l'unité, 0 sinon, où $r_1(\mathbf{L})$ est le nombre de places réelles de \mathbf{L} et où $\delta_{2,p}$ est le symbole de Kronecker.

En ce qui concerne le φ -rang du Δ -module $H_2(P_S^T, \mathbb{F}_p)$, il est possible d'en donner une majoration :

Proposition 2.2. — *Soit φ un caractère \mathbb{C} -irréductible de Δ . Alors*

$$r_\varphi(H_2(P_S^T, \mathbb{F}_p)) \leq r_\varphi(\text{III}_S^T(\mathbf{L})) - r_\varphi \mu_p(\mathbf{L}) + \sum_{v \in S} \delta_v r_\varphi \text{Ind}_{\Delta_v}^\Delta \mu_p(\mathbf{L}_v) + \delta_{2,p} \varphi(1) r_1(\mathbf{L}).$$

Démonstration. — On reprend la preuve classique permettant de donner une majoration du p -rang de $H^2(P_S^T, \mathbb{F}_p)$ tout en faisant ressortir l'action de Δ (voir [12], [11], [7], [13] ...)

Pour commencer un lemme (cf. [12], [17]) :

Lemme 2.3. — *Soit $\overline{G}_\mathbf{L}(p)$ (respectivement $\overline{G}_w(p)$) le plus grand pro- p -quotient du groupe de Galois absolu $\overline{G}_\mathbf{L}$ (resp. \overline{G}_w) de \mathbf{L} (resp. \mathbf{L}_w). On a la suite de Δ -modules :*

$$1 \longrightarrow H^2(\overline{G}_\mathbf{L}(p), \mathbb{F}_p) \xrightarrow{\text{Loc}} \oplus_w H^2(\overline{G}_w(p), \mathbb{F}_p) \longrightarrow \left((\mu_p)^{\overline{G}_\mathbf{L}(p)} \right)^* \longrightarrow 1.$$

Ensuite, on sait qu'il existe un Δ -morphisme

$$\ker \left(H^2(P_S^T, \mathbb{F}_p) \xrightarrow{\text{Inf}} H^2(\overline{G}_\mathbf{L}(p), \mathbb{F}_p) \right) \hookrightarrow (\text{III}_S^T(\mathbf{L}))^*$$

obtenu à partir du symbole de réciprocity local (cf. [12]). Ainsi,

$$\ker(\text{Loc} \circ \text{Inf}) \hookrightarrow (\text{III}_S^T(\mathbf{L}))^*,$$

où $\text{Inf} : H^2(\mathbf{P}_S^T, \mathbb{F}_p) \rightarrow H^2(\overline{\mathbf{G}}_{\mathbf{L}}(p), \mathbb{F}_p)$. Comme les places en dehors de S et de l'infini sont non ramifiées dans $\mathbf{L}_S^T(p)/\mathbf{L}$,

$$\text{Loc} \circ \text{Inf}(H^2(\mathbf{P}_S^T, \mathbb{F}_p)) = \text{Loc}_{S'} \circ \text{Inf}(H^2(\mathbf{P}_S^T, \mathbb{F}_p)),$$

où $\text{Loc}_{S'}$ est la projection de Loc sur les composantes en $S(\mathbf{L})$ et en les places réelles de \mathbf{L} . D'autre part le morphisme

$$\bigoplus_{w \in S(\mathbf{L}) \cup Pl_\infty} H^2(\overline{\mathbf{G}}_w(p), \mathbb{F}_p) \xrightarrow{\Sigma_{S'}} \mu_p(\mathbf{L})^*$$

est surjectif (se rappeler que par hypothèse, S est non vide) et $\Sigma_{S'} \circ \text{Loc} \circ \text{Inf} = 0$. En résumé :

$$\begin{aligned} r_\varphi H^2(\mathbf{P}_S^T, \mathbb{F}_p) &= r_\varphi \ker(\text{Loc} \circ \text{Inf}) + r_\varphi \text{Im}(\text{Loc} \circ \text{Inf}) \\ &\leq r_\varphi (\text{III}_S^T(\mathbf{L}))^* + r_\varphi \text{Loc}(\text{Inf}(H^2(\mathbf{P}_S^T, \mathbb{F}_p))) \\ &= r_\varphi (\text{III}_S^T(\mathbf{L}))^* + r_\varphi \text{Loc}_{S'}(\text{Inf}(H^2(\mathbf{P}_S^T, \mathbb{F}_p))) \\ &\leq r_\varphi (\text{III}_S^T(\mathbf{L}))^* + r_\varphi \ker \Sigma_{S'} \\ &= r_\varphi (\text{III}_S^T(\mathbf{L}))^* + r_\varphi \left(\bigoplus_{w \in S(\mathbf{L}) \cup Pl_\infty} H^2(\overline{\mathbf{G}}_w(p), \mathbb{F}_p) \right) - r_\varphi \mu_p(\mathbf{L})^*. \end{aligned}$$

Notons ensuite

$$\bigoplus_{w \in S(\mathbf{L}) \cup Pl_\infty} H^2(\overline{\mathbf{G}}_w(p), \mathbb{F}_p) = \bigoplus_{v \in S \cup Pl_\infty} \text{Ind}_{\Delta_v}^\Delta H^2(\overline{\mathbf{G}}_v(p), \mathbb{F}_p)$$

où, dans la seconde somme, on a privilégié le choix d'une place w de \mathbf{L} au-dessus de v et posé $\overline{\mathbf{G}}_v(p) = \overline{\mathbf{G}}_w(p)$.

Pour les places w de \mathbf{L} en lesquelles le groupe $\mu_p(\mathbf{L}_w)$ est trivial, on sait que le pro- p -groupe $\overline{\mathbf{G}}_w(p)$ est libre c'est à dire que $H^2(\overline{\mathbf{G}}_w(p), \mathbb{F}_p) = 0$. Pour les autres places w , $\overline{\mathbf{G}}_w(p)$ agit trivialement sur $\mu_p(\mathbf{L}_w)$, et ainsi (à l'aide de la suite exacte de Kummer)

$$\begin{aligned} H^2(\overline{\mathbf{G}}_w(p), \mathbb{F}_p) \otimes \mu_p(\mathbf{L}_w) &\simeq H^2(\overline{\mathbf{G}}_w(p), \mu_p(\mathbf{L}_w)) \\ &\simeq H^2(\overline{\mathbf{G}}_w, \mu_p(\mathbf{L}_w)) \\ &\simeq \text{Tor}_p(\text{Br}(\mathbf{L}_w)) \simeq \mathbb{Z}/p\mathbb{Z}, \end{aligned}$$

où $\text{Tor}_p(\text{Br}(\mathbf{L}_w))$ est la p -torsion du groupe de Brauer $\text{Br}(\mathbf{L}_w)$ de \mathbf{L}_w . Tout ceci étant des isomorphismes de Δ_w -modules.

Au total, on obtient :

$$r_\varphi H^2(\mathbf{P}_S^T(p), \mathbb{F}_p) \leq r_\varphi (\text{III}_S^T(\mathbf{L}))^* + \sum_{v \in S} \delta_v r_\varphi \text{Ind}_{\Delta_v}^\Delta \mu_p(\mathbf{L}_v)^* + \varphi(1) r_1(\mathbf{L}) \delta_{2,p} - r_\varphi \mu_p(\mathbf{L})^*$$

ou encore

$$r_\varphi H_2(\mathbf{P}_S^T, \mathbb{F}_p) \leq r_\varphi \text{III}_S^T(\mathbf{L}) + \sum_{v \in S} r_\varphi \text{Ind}_{\Delta_v}^\Delta \mu_p(\mathbf{L}_v) + \varphi(1) r_1(\mathbf{L}) \delta_{2,p} - r_\varphi \mu_p(\mathbf{L}).$$

◇

Ces propositions permettent d'en déduire le corollaire suivant :

Corollaire 2.4. — (i) $r_\varphi (H_2(\mathbf{P}_S^T, \mathbb{Z}_p)) \leq r_\varphi (\ker(\Psi_S^T))$.

En particulier, le groupe $H^2(\mathbf{P}_S^T, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial dès lors que Ψ_S^T est injectif.

(ii) $r_\varphi (\text{Tor}_p(\mathbf{P}_S^{T,ab})) \leq r_\varphi (H_2(\mathbf{P}_S^T, \mathbb{F}_p)) \leq r_\varphi (\text{Tor}_p(\mathbf{P}_S^{T,ab})) + r_\varphi (\ker(\Psi_S^T))$.

Ainsi, lorsque Ψ_S^T est injectif, $\text{Tor}_p(\mathbf{P}_S^{T,ab}) \simeq H_2(\mathbf{P}_S^T, \mathbb{F}_p)$, isomorphisme de Δ -modules.

Démonstration. — La suite exacte

$$1 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p\mathbb{Z}_p \longrightarrow 1$$

fournit immédiatement l'égalité

$$r_\varphi(H_2(\mathbb{P}_S^T, \mathbb{Z}_p)/p) = r_\varphi(H_2(\mathbb{P}_S^T, \mathbb{F}_p)) - r_\varphi(\mathrm{Tor}_p(\mathbb{P}_S^{T,ab})).$$

(Noter qu'ici tous les \mathbb{Z}_p -modules sont de type fini.)

La torsion de $\mathbb{P}_S^{T,ab}$ étant finie, il vient

$$\begin{aligned} r_\varphi(\mathrm{Tor}_p(\mathbb{P}_S^{T,ab})) &= r_\varphi\left(\mathrm{Tor}(\mathbb{P}_S^{T,ab})/\left(\mathrm{Tor}(\mathbb{P}_S^{T,ab})\right)^p\right) \\ &= r_\varphi(\mathrm{Tor}(\mathbb{P}_S^{T,ab})) \\ &= r_\varphi(\mathbb{P}_S^{T,ab}) - \delta_S \varphi(1) + r_\varphi(\mathrm{Im}(\Psi_S^T)) \\ &= r_\varphi(\mathrm{III}_S^T(\mathbf{L})) - r_\varphi(\mathbf{E}_\mathbf{L}^T) + \sum_{v \in S} \delta_v r_\varphi \mathrm{Ind}_{\Delta_v}^\Delta \mu_p(\mathbf{L}_v) \\ &\quad + \varphi(1) \delta_{2,p} r_1(\mathbf{L}) + r_\varphi(\mathrm{Im}(\Psi_S^T)). \end{aligned}$$

Par conséquent

$$r_\varphi(H_2(\mathbb{P}_S^T, \mathbb{Z}_p)) \leq r_\varphi(\mathrm{Im}(\Psi_S^T)) + r_\varphi(\mathbf{E}_\mathbf{L}^T) - r_\varphi \mu_p(\mathbf{L}) = r_\varphi(\ker(\Psi_S^T))$$

d'où (i). Le second point s'en déduit immédiatement. \diamond

2.3. Les premières conséquences. — Reprenons les notations introduites précédemment.

Proposition 2.5. — *Supposons $\#\Delta$ premier à p . Lorsque le groupe $H^2(\mathbf{G}_\mathbf{M}, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial, la représentation $\rho_\mathbf{M}$ est sans obstruction dès lors que le Δ -module $\mathrm{Tor}(\mathbf{H}_\mathbf{M}^{ab})$ est premier au Δ -module Ad .*

En particulier, si le morphisme Ψ_S^T est injectif et si le Δ -module $\mathrm{Tor}(\mathbb{P}_S^{T,ab})$ est premier au Δ -module Ad , la représentation ρ_S^T est sans obstruction (c'est ce que l'on peut appeler la situation "prime-to-adjoint").

Démonstration. — C'est le lemme 1.3 associé au corollaire 2.4.

\diamond

Comme nous l'avons vu, quand le groupe $H^2(\mathbf{H}_\mathbf{M}, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial, le groupe de cohomologie $H^2(\mathbf{G}_\mathbf{M}, \mathrm{Ad})$ s'interprète à partir de la torsion de $\mathbf{H}_\mathbf{M}^{ab}$. Lorsque $\mathbf{M} = \mathbf{L}_S^T(p)$, ce groupe de torsion a déjà beaucoup été étudié.

Proposition 2.6 (Gras [8], Théorème 2.6 page 261). — *Si la p -partie $\mathrm{Cl}_\mathbf{L}^T(p)$ du groupe des T -classes de \mathbf{L} est triviale, alors l'application d'Artin permet d'obtenir l'isomorphisme suivant :*

$$\mathrm{Tor}(\mathbb{P}_S^{T,ab}) \simeq \mathrm{Tor}(\mathfrak{A}_S/\Psi_S^T(\mathbb{Z}_p \otimes \mathbf{E}_\mathbf{L}^T)).$$

Corollaire 2.7 (Gras [8] Théorème 2.6 page 261 et lemme 4.2.4 page 295)

Le pro- p -groupe $\mathbb{P}_S^{T,ab}$ est sans torsion dès lors que $\mathrm{Cl}_\mathbf{L}^T$ est d'ordre premier à p , que $\sum_{v \in S} \mu_v/\mu_\mathbf{L} = 0$ et que $\mathrm{Tor}(\mathrm{Log}(\mathfrak{A}_S)/\mathbb{Z}_p \mathrm{Log}(\Psi_S^T(\mathbf{E}_\mathbf{L}^T))) = 0$.

Pour être complet, citons la remarque suivante :

Remarque 2.8 (Wingberg, [19]). — Pour que le groupe $H^2(\mathbb{P}_S, \mathbb{F}_p)^\Delta$ soit trivial, il est nécessaire que l'extension $\mathbf{K}_S(p)/\mathbf{K}$ soit pro- p -libre.

3. Sur la dimension de Krull de l'anneau R_S^T

3.1. Cas où $\#\Delta$ est une puissance de p . —

Proposition 3.1. — *Supposons que Δ est un p -groupe et que pour toute place v de T , $\Delta_v = \{1\}$. Alors*

$$\dim_{\text{krull}}(R_S^T/pR_S^T) \geq 1 + 4(\delta_S - (r_1 + r_2 + |T|)).$$

Démonstration. — Si pour un groupe profini G , l'on dénote par $\chi_2(G)$ sa caractéristique d'Euler-Poincaré tronquée à l'ordre 2, il est bien connu que

$$\chi_2(G, A) \leq \#A \cdot \chi_2(G, \mathbb{F}_p),$$

où A est un G -module fini.

Ensuite (cf. [7], [14], ... ou propositions 2.1 et 2.2)

$$\chi_2(G_S^T(p), \mathbb{F}_p) \leq r_1 + r_2 + |T| - \delta_S,$$

où $G_S^T(p) = \text{Gal}(\mathbf{K}_S^T(p)/\mathbf{K})$. Comme $\mathbf{L}_S^T(p) = \mathbf{K}_S^T(p)$, il vient

$$\dim_{\text{krull}}(R_S^T/pR_S^T) \geq 1 + 4(\delta_S - (r_1 + r_2 + |T|)),$$

R_S^T étant l'anneau de déformation associé à l'extension $\mathbf{L}_S^T(p)/\mathbf{K}$. \diamond

3.2. Situation modérée (preuve du théorème 0.5). — Les propositions 2.1 et 2.2 permettent de montrer l'inégalité suivante :

$$r_\varphi(H^1(P_S^T, \mathbb{F}_p)^*) - r_\varphi(H^2(P_S^T, \mathbb{F}_p)^*) \geq \langle \mathbf{1}, \varphi \rangle + \delta_S \varphi(1) - \sum_{v \in T \cup Pl_\infty} r_\varphi(\text{Ind}_{\Delta_v}^\Delta \mathbf{1}).$$

Notons ensuite l'identité suivante :

$$\begin{aligned} & \delta_S \varphi(1) - \sum_{v \in T \cup \infty} \langle \text{Ind}_{\Delta_v}^\Delta \mathbf{1}, \varphi \rangle \\ &= (\delta_S - (r_1 + r_2 + |T|))\varphi(1) + \sum_{v \in T \cup Pl_\infty} \langle \varphi, (\text{Ind}_{\Delta_v}^\Delta \text{Ind}_{\{1\}}^{\Delta_v} \mathbf{1} - \text{Ind}_{\Delta_v}^\Delta \mathbf{1}) \rangle. \end{aligned}$$

Comme $\text{Ind}_{\{1\}}^{\Delta_v} \mathbf{1}$ contient la représentation triviale, la quantité

$$\sum_{v \in T \cup Pl_\infty} \langle \varphi, (\text{Ind}_{\Delta_v}^\Delta \text{Ind}_{\{1\}}^{\Delta_v} \mathbf{1} - \text{Ind}_{\Delta_v}^\Delta \mathbf{1}) \rangle$$

est positive.

Ainsi sous la condition $\delta_S \geq (r_1 + r_2 + |T|)$, il vient pour tout caractère \mathbb{C}_p -irréductible φ l'inégalité suivante :

$$r_\varphi(H^1(P_S^T, \mathbb{F}_p)^*) - r_\varphi(H^2(P_S^T, \mathbb{F}_p)^*) \geq 0.$$

Regardons maintenant les termes locaux.

Pour $v|_\infty$ décomposée dans \mathbf{L}/\mathbf{K} , il vient

$$\text{Ind}_{\Delta_v}^\Delta \text{Ind}_{\{1\}}^{\Delta_v} \mathbf{1} - \text{Ind}_{\Delta_v}^\Delta \mathbf{1} = 0.$$

Pour $v|_\infty$ paire, non-décomposée dans \mathbf{L}/\mathbf{K} , il vient

$$\text{Ind}_{\{1\}}^{\Delta_v} \mathbf{1} = \mathbf{1} + \chi_v,$$

où χ_v est l'unique caractère irréductible non trivial de Δ_v . Et ainsi, pour cette même place,

$$\langle \text{Ind}_{\Delta_v}^\Delta \chi_v, \text{Ad} \rangle = \langle \chi_v, \text{Ad} \rangle_{|\Delta_v} = \langle \chi_v, 4 \cdot \mathbf{1} \rangle_{|\Delta_v} = 0.$$

Pour $v|_\infty$ impaire :

$$\langle \text{Ind}_{\Delta_v}^\Delta \chi_v, \text{Ad} \rangle = \langle \chi_v, \text{Ad} \rangle_{|\Delta_v} = \langle \chi_v, 2 \cdot \mathbf{1} + 2 \cdot \chi_v \rangle_{|\Delta_v} = 2.$$

Notons par $\sum_{\varphi} \alpha_{\varphi} \varphi$ la décomposition de la représentation adjointe Ad en somme de caractères $\mathbb{C}_p[\Delta]$ -irréductibles. Pour v impaire, il vient finalement

$$\sum_{\varphi} \alpha_{\varphi} \langle \varphi, \chi_v \rangle_{|\Delta_v} = 2.$$

En regroupant tout ceci, on obtient alors

$$\begin{aligned} & \langle \sum_{\varphi} (r_{\varphi}(H^1(\mathbb{P}_S^T, \mathbb{F}_p)^*) - r_{\varphi}(H^2(\mathbb{P}_S^T, \mathbb{F}_p)^*)) \varphi, \text{Ad} \rangle \\ &= \langle \sum_{\varphi} (r_{\varphi}(H^1(\mathbb{P}_S^T, \mathbb{F}_p)^*) - r_{\varphi}(H^2(\mathbb{P}_S^T, \mathbb{F}_p)^*)) \varphi, \sum_{\varphi} \alpha_{\varphi} \varphi \rangle \\ &\geq \left(\sum_{\varphi} \alpha_{\varphi} (\langle \mathbf{1}, \varphi \rangle + (\delta_S - r_1 + r_2 + |T|)\varphi(1)) \right) + \\ &\sum_{T \cup Pl_{\infty}} \sum_{\varphi} \alpha_{\varphi} \langle \varphi, \text{Ind}_{\Delta_v}^{\Delta} \text{Ind}_{\mathbf{1}}^{\Delta_v} \mathbf{1} - \text{Ind}_{\Delta_v}^{\Delta} \mathbf{1} \rangle \\ &= \left(\sum_{\varphi} \alpha_{\varphi} (\langle \mathbf{1}, \varphi \rangle + (\delta_S - r_1 + r_2 + |T|)\varphi(1)) \right) + \\ &\sum_{v|\infty, \Delta_v \neq \mathbf{1}} \sum_{\varphi} \alpha_{\varphi} \langle \chi_v, \varphi \rangle_{|\Delta_v} + \sum_{v \in T} \left(\langle \text{Ad}, \text{Ind}_{\{1\}}^{\Delta} \mathbf{1} \rangle - \langle \text{Ad}, \text{Ind}_{\Delta_v}^{\Delta} \mathbf{1} \rangle \right) \\ &= a_1 + (\delta_S - (r_1 + r_2 + |T|)) \sum_{\varphi} \alpha_{\varphi} \varphi(1) + 2\kappa_1 + \sum_{v \in T} \kappa_v \\ &= a_1 + 4(\delta_S - (r_1 + r_2 + |T|)) + 2\kappa_1 + \kappa_T. \end{aligned}$$

Pour conclure, on a le lemme suivant :

Lemme 3.2. — Soient M et N deux $\mathbb{Z}_p[\Delta]$ -modules. Alors le p -rang de $(M \otimes N)^{\Delta}$ est égal au produit scalaire $\langle M^*, N \rangle$.

En effet, le p -rang de $(M \otimes N)^{\Delta}$ est égal exactement au nombre de fois qu'apparaît la représentation triviale dans $M \otimes N$. Ainsi, si $M = \sum_{\psi} \beta_{\psi} \psi$ et $N = \sum_{\varphi} \beta'_{\varphi} \varphi$ sont les décompositions de M et N en caractères \mathbb{C}_p -irréductibles, il vient :

$$\begin{aligned} \langle \mathbf{1}, M \otimes N \rangle &= \sum_{\varphi, \psi} \beta_{\psi} \beta'_{\varphi} \langle \mathbf{1}, \varphi \psi \rangle \\ &= \sum_{\varphi, \psi} \beta_{\psi} \beta'_{\varphi} \langle \varphi^{-1}, \psi \rangle \\ &= \langle M^*, N \rangle \end{aligned}$$

On obtient de tout ceci une minoration de la dimension de Krull de $\mathbb{R}_S^T/p\mathbb{R}_S^T$ dès lors que l'on aura noté que celle-ci vaut au moins

$$\sum_{\varphi} \langle (r_{\varphi}(H^1(\mathbb{P}_S^T, \mathbb{F}_p)^*) - r_{\varphi}(H^2(\mathbb{P}_S^T, \mathbb{F}_p)^*)) \varphi, \text{Ad} \rangle$$

(car chaque terme est positif).

En remarque, notons que $a_1 \geq 1$ et que si $\text{Im}(\bar{\rho})$ est un sous-groupe de Cartan, la représentation adjointe Ad contient au moins deux fois la représentation unité $\mathbf{1}$ (et donc que $a_1 > 1$). \diamond

Corollaire 3.3. — Supposons que S contient l'ensemble des places au-dessus de p et prenons $T = \emptyset$. Alors

$$\dim_{\text{krull}}(\mathbb{R}_S) \geq 1 + 2\kappa_1 + 4r_2.$$

4. Détail d'un exemple

Comme indiqué dans l'introduction, l'exemple suivant s'inspire de l'exemple décortiqué par Mazur dans [15].

Fixons un plongement $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Soit un entier $a > 0$. Soit le polynôme irréductible $P(x) = x^3 + ax + 1$ de discriminant $d = -4a^3 - 27$ (que l'on souhaite sans facteur carré) et ayant pour groupe de Galois S_3 .

Considérons les corps suivants : $\mathbf{K} = \mathbb{Q}(\sqrt{d})$; $\mathbf{F} = \mathbb{Q}(\theta)$, où θ est la racine réelle de P ; $\mathbf{L} = \mathbb{Q}(\sqrt{d}, \theta)$. Soit θ' une seconde racine de P .

L'extension \mathbf{L}/\mathbf{K} est non-ramifiée, en particulier \mathbf{L} est contenue dans \mathbf{K}_S/\mathbf{K} , et ce pour tout ensemble S .

Soit $\bar{\rho} : \Delta \hookrightarrow \mathrm{Gl}_2(\mathbb{F}_p)$ une représentation injective de Δ dans $\mathrm{Gl}_2(\mathbb{F}_p)$, pour un certain nombre premier p . L'image $\bar{\rho}(\Delta)$ est un sous-groupe de Cartan (qui est déployé si et seulement si, 3 divise $p - 1$). Nous souhaitons caractériser des situations où l'anneau de déformation de $\bar{\rho}$ est sans obstruction.

Commençons par regarder les unités du corps \mathbf{L} .

Lemme 4.1. — (i) L'élément θ (resp. θ') est une unité fondamentale de \mathbf{F} (resp. de $\mathbb{Q}(\theta')$).
(ii) Pour $p > 3$, la famille $\{\theta, \theta'\}$ forme une \mathbb{Z}_p -base de $\mathbf{E}_{\mathbf{L}}$.

Démonstration. — (i) Soit $a > 1$ (le cas $a = 1$ se traite directement).

Soit $\mathrm{Reg}(\mathbf{F})$ le régulateur du groupe des unités $\mathbf{E}_{\mathbf{F}}$ de \mathbf{F} . Notons par $\mathrm{Reg}(\theta) = |\log |\theta||$ le régulateur du sous réseau $\theta^{\mathbb{Z}}$ de $\mathbf{E}_{\mathbf{F}}$.

D'après Cusick [5], on connaît une minoration de $\mathrm{Reg}(\mathbf{F})$:

$$\mathrm{Reg}(\mathbf{F}) \geq \frac{1}{3} \log((4a3 + 27)/27)$$

car $4a3 + 27$ est sans facteur carré.

Ainsi

$$[E_{\mathbf{F}} : \langle \pm\theta \rangle] = \mathrm{Reg}(\theta)/\mathrm{Reg}(\mathbf{F}) = \frac{3|\log |\theta||}{\log((4a3 + 27)/27)}.$$

On note ensuite que $\theta \in [-1/a; -1/a2]$ et est d'autant plus proche de $-1/a$ que a est grand. Il vient alors facilement que $\mathrm{Reg}(\theta)/\mathrm{Reg}(\mathbf{F}) < 2$ et donc que $\mathbf{E}_{\mathbf{F}} = \langle \pm\theta \rangle$.

(ii) Remarquons tout d'abord, d'après (i), que si θ est divisible alors nécessairement $\mathbf{L} = \mathbf{F}(\sqrt{\pm\theta})$. Comme $\mathbf{L} = \mathbf{F}(\sqrt{-4a3 - 27})$, par la théorie de Kummer,

$$\pm\theta(-4a3 - 27)^{-1} \in \mathbf{F}2,$$

ce qui est impossible (la contradiction est apportée par un premier l divisant $4a3 + 27$).

Ainsi θ n'est pas divisible. Soit alors $\{\theta, \xi\}$ une \mathbb{Z} -base de $\mathbf{E}_{\mathbf{L}}$. Ainsi $N_{\mathbf{L}/\mathbf{F}}\xi = \pm\theta^{\varepsilon+2n}$ avec $\varepsilon = 0$ ou 1 et $n \in \mathbb{Z}$. Par conséquent, $N_{\mathbf{L}/\mathbf{F}}(\xi\theta^{-n}) = \pm\theta^{\varepsilon}$. La famille $\{\theta, \xi\theta^{-n}\}$ formant également une base de $\mathbf{E}_{\mathbf{L}}$, on peut donc supposer que $N_{\mathbf{L}/\mathbf{F}}\xi = \pm\theta^{\varepsilon}$.

Écrivons ensuite θ' dans la base $\{\theta, \xi\}$. Il existe $\alpha, \beta \in \mathbb{Z}$, tels que $\theta' = \pm\theta^{\alpha}\xi^{\beta}$. Prenons la norme dans \mathbf{L}/\mathbf{F} de cette égalité :

$$-\theta^{-1} = N_{\mathbf{L}/\mathbf{F}}\theta' = \pm\theta^{2\alpha+\beta\varepsilon}$$

ainsi $\varepsilon = 1$ et il vient l'équation $-1 = 2\alpha + \beta$. Regardons la norme de θ' dans $\mathbf{L}/\mathbb{Q}(\theta')$:

$$\theta'2 = \pm\theta'^{-\alpha+\lambda\beta}$$

où $N_{\mathbf{L}/\mathbb{Q}(\theta')}\xi = \pm\theta'^{\lambda}$. D'où l'équation $2 = -\alpha + \lambda\beta$. De ces deux dernières équations, on en déduit

$$3 = \beta(1 + 2\lambda)$$

ainsi $\beta|3$ et le second point du lemme s'en déduit. \diamond

Choisissons un nombre premier $p > 3$ totalement décomposé dans \mathbf{F}/\mathbb{Q} (ou de façon équivalente totalement décomposé dans \mathbf{L}/\mathbf{K}). Assurons-nous que p est premier à l'ordre du groupe des classes de \mathbf{L} et que p ne divise pas d .

Soit $(x - u_1)(x - u_2)(x - u_3)$, avec $u_i \neq u_j$, la factorisation de P dans $\mathbb{F}_p[x]$.

Prenons $T = \emptyset$ et $S = \{v\}$, où v est l'une des deux places de \mathbf{K} au-dessus de p .

Dans ce contexte, le morphisme $\Psi_S : \mathbb{Z}_p \otimes E_L \rightarrow \mathfrak{U}_{S(\mathbf{L})}$ est injectif (cf. par exemple [10], [14]). Ainsi le groupe $H^2(P_S, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial (cf. corollaire 2.4).

Nous allons maintenant imposer des conditions afin que la torsion $\text{Tor}(P_S^{ab})$ de P_S^{ab} soit également triviale.

Soient $w_{(i)}$ les trois places de \mathbf{L} au-dessus de v .

Il est facile de noter que chaque premier de \mathbf{F} au-dessus de p donne lieu à une place de $S(\mathbf{L})$.

Assurons-nous que $\pi_i = \theta - u_i$ est une uniformisante de $\mathbf{L}_{w_{(i)}}$ (avec $u_i \in]0, p-1[$). Ceci se lit dans le corps \mathbf{F} .

Posons $e_i = \log_{w_i}(\theta)$. Alors $\text{Log } \mathfrak{U}_S = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 \oplus \mathbb{Z}_p e_3$ et $\text{Log}(\theta') = \sum_i \lambda_i e_i$, avec $\lambda_i \in \mathbb{Z}_p$.

Il est facile de voir que l'on peut s'arranger pour que θ' vérifie :

$$\begin{cases} \theta' &= u_3 + \pi_1 \\ \theta' &= u_1 + \pi_2 \\ \theta' &= u_2 + \pi_3 \end{cases}$$

Soit donc $y = \sum_i y_i e_i$ un élément de p -torsion de $\text{Log}(\mathfrak{U}_S)/\text{Log}(E_L)$. Il existe $a, b \in \mathbb{Z}_p$ tels que

$$p(y_1 e_1 + y_2 e_2 + y_3 e_3) = a(e_1 + e_2 + e_3) + b(\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3),$$

d'où le système linéaire

$$\begin{cases} py_1 &= a + b\lambda_1 \\ py_2 &= a + b\lambda_2 \\ py_3 &= a + b\lambda_3 \end{cases}$$

Ainsi, et c'est notre dernière condition sur p , s'il existe i, j tels que $\lambda_i \not\equiv \lambda_j \pmod{p}$, il vient immédiatement $b \equiv a \equiv 0 \pmod{p}$, c'est à dire $y \in \Psi_S(E_L)$ et de ce fait la p -torsion de $\mathfrak{U}_S/\Psi_S(E_L)$ est triviale.

Interprétons un peu plus précisément cette condition. On a

$$\begin{aligned} \lambda_1 &= \log_{w_1}(\theta') / \log_{w_1}(\theta) \\ &= \frac{u_1}{u_3} \pmod{\pi_1} \end{aligned}$$

$$\lambda_2 = \frac{u_2}{u_1} \pmod{\pi_2}$$

$$\lambda_3 = \frac{u_3}{u_2} \pmod{\pi_3}$$

De ce fait la p -torsion de $\mathfrak{U}_S/\Psi_S(E_L)$ est triviale dès lors que pour un triplet (i, j, k) , i, j, k deux à deux différents, on a

$$u_i u_j \neq u_k^2$$

Si tel est le cas, le corollaire 2.7 s'applique. Le pro- p -groupe P_S^{ab} est sans torsion.

Comme $H^2(P_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, on en déduit que P_S est libre et par conséquent $H^2(P_S, \text{Ad}) = 0$. L'anneau R_S est sans obstruction.

Le nombre minimal de générateurs de R_S est exactement égal à la dimension sur \mathbb{F}_p de $H^1(G_S, \text{Ad})$, et $H^1(G_S, \text{Ad}) \simeq [P_S^{ab*} \otimes \text{Ad}]^\Delta$. Or Δ agit trivialement sur $P_S^{ab} \simeq \mathbb{Z}_p$ et Ad contient deux fois le caractère trivial $\mathbf{1}$. Par conséquent $R_S = \mathbb{Z}_p[[T_1, T_2]]$.

Le groupe P_S , isomorphe à \mathbb{Z}_p , est engendré par un élément x . Alors $\text{Gal}(\mathbf{L}_S(p)/\mathbf{K}) \simeq \Delta \times \langle x \rangle$ et ρ_S peut être définie par :

$$\rho_S(x) = \begin{pmatrix} 1 + T_1 & 0 \\ 0 & 1 + T_2 \end{pmatrix}.$$

Ceci, par exemple, s'applique aux couples

$$(a, p) = (2, 17), (2, 71), \dots, (4, 71), (4, 73), (4, 83), \dots, (5, 19), (5, 29), (5, 73), \dots$$

Références

- [1] G. Böckle, *Explicit universal deformations of even Galois representations*, Math. Nachr. **206** (1999), 85-110.
- [2] G. Böckle, A. Mézard, *The prime-to-adjoint principle and unobstructed Galois deformations in the Borel case*, Journal of Number Theory **78** (1999), 167-203.
- [3] N. Boston, *Explicit deformation of Galois representations*, Invent. math. **103** (1990), 181-186.
- [4] N. Boston, B. Mazur, *Explicit universal deformations of Galois representations*, Adv. Stud. Pure Math. **17** (1989), 1-21.
- [5] T.W. Cusick, *Lower bounds for regulators*, Number Theory Noordwijkerhout, Lecture Notes in Math. 1068, 1983.
- [6] F. Gouvêa, *Deforming Galois Representation : a survey*, Canadian Math. Society, Conference proceeding 17 (1995).
- [7] G. Gras, *Théorèmes de réflexion*, Journal Th. des Nombres de Bordeaux **10** (1988), 399-499.
- [8] G. Gras, *Class Field Theory, From Theory to practice*, Springer-Verlag, Berlin, 2003.
- [9] K. Haberland, *Galois cohomology of algebraic number fields*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.
- [10] J.-F. Jaulent, *Sur l'indépendance l -adique de nombres algébriques*, *J. Number Theory* **20** (1985), 149-158.
- [11] H. Kisilevsky, J. Labute, *On a sufficient condition for the p -class tower of a CM-field to be infinite*, Théorie des nombres (Quebec, PQ, 1987), 556-560, de Gruyter, Berlin, 1989.
- [12] H. Koch, *Galoissche Theorie des p -Erweiterungen*, VEB, Berlin, 1970.
- [13] C. Maire, *Compléments à un résultat de Shafarevich*, Math. Nachr. **198** (1999), 149-168.
- [14] C. Maire, *On \mathbb{Z}_l -rank of abelian extensions with restricted ramification*, Journal of Number Theory **92** (2002), 376-404.
- [15] B. Mazur, *Deforming Galois representations* In : Galois groups over \mathbb{Q} , Y. Ihara, K. Ribet, J.-P. Serre eds., MSRI Publ. **16**, Springer-Verlag, 1987, 385-437.
- [16] A. Mézard, *Computation of a universal deformation ring in the Borel case*, Math. Proc. Cambridge Philo. Soc. **126** (1999), 417-442.
- [17] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, GMW 323, Springer-Verlag Berlin Heidelberg, 2000.
- [18] R. Ramakrishna, *Deforming an even representation*, Invent. math. **132** (1998), 563-580.
- [19] K. Wingberg, *Free pro- p -extensions of number fields*, preprint 2005.

7 novembre 2006

CHRISTIAN MAIRE, Institut de Mathématiques de Toulouse, Université Toulouse Le Mirail, 5 allées Machado, 31058 Toulouse • E-mail : mair@univ-tlse2.fr