UFR Sciences et Techniques
Ecole doctorale Louis Pasteur
Université de Franche-Comté

Thèse de Doctorat

présentée par

Julien Blondeau

pour obtenir le grade de
Docteur de Mathématiques de l'Université de Franche-Comté

Déformation des extensions peu ramifiées en p

Thèse soutenue le 17 juin 2011, devant le jury composé de :

François Brunault	Maître de conférences à l'ENS de Lyon
Jean-Marc Couveignes (Rapporteur)	Professeur à l'Université Toulouse 2
Vincent Fleckinger	Professeur à l'Université de Franche-Comté
Ariane Mézard (Rapporteur)	Professeur à l'Université de Versailles St-Quentin
Christian Maire (Directeur)	Professeur à l'Université de Franche-Comté
Thong Nguyen Quang Do	Professeur à l'Université de Franche-Comté

UFR Sciences et Techniques
Ecole doctorale Louis Pasteur
Université de Franche-Comté

Thèse de Doctorat

présentée par

Julien Blondeau

pour obtenir le grade de
Docteur de Mathématiques de l'Université de Franche-Comté

Déformation des extensions peu ramifiées en p

Thèse soutenue le 17 juin 2011, devant le jury composé de :

François Brunault	Maître de conférences à l'ENS de Lyon
Jean-Marc Couveignes (Rapporteur)	Professeur à l'Université Toulouse 2
Vincent Fleckinger	Professeur à l'Université de Franche-Comté
Ariane Mézard (Rapporteur)	Professeur à l'Université de Versailles St-Quentin
Christian Maire (Directeur)	Professeur à l'Université de Franche-Comté
Thong Nguyen Quang Do	Professeur à l'Université de Franche-Comté

Remerciements

En écrivant ces remerciements, je pense déjà à Christian Maire qui m'a proposé un sujet de thèse passionnant et qui m'a guidé avec générosité en partageant ses idées et sa vision des mathématiques. Ses conseils, son aide, sa disponibilité infinie et sa patience ont rythmé mes années de travail à ses côtés. Merci Christian.

Je remercie chaleureusement Ariane Mézard et Jean-Marc Couveignes d'avoir accepté d'être rapporteurs. Ils ont apporté un regard précis sur mon travail me permettant ainsi d'améliorer véritablement le manuscrit. Merci pour vos remarques et vos encouragements, je vous en suis très reconnaissant.

François Brunault, Vincent Fleckinger et Thong Nguyen Quang Do ont accepté de composer mon jury. C'est pour moi un plaisir de les remercier, aussi bien pour leurs conseils que pour leurs questions.

Lors d'une conversation au Cirm avec Gabor Wiese, j'ai pu profiter de ses connaissances sur l'aspect modulaire de mon travail. Je tiens à le remercier pour son aide précieuse.
Pour l'intérêt qu'il a porté à mon travail à travers sa lecture attentive du second chapitre de ce manuscrit et pour son invitation à Heidelberg, je remercie Gebhard Böckle.
Je remercie également Mnacho pour son aide précieuse et sa disponibilité.

Durant ma thèse, j'ai eu la chance de participer au Trimestre Galoisien à l'IHP. Ces trois mois ont été d'une richesse absolue pour moi, je remercie les organisateurs ainsi que la Fondation Sciences Mathématiques de Paris.

Les années de thèse réservent des moments de doute et de déception. Parmi les personnes m'ayant permis de dépasser ces difficultés, je pense en particulier à Anthony et Mathilde. Merci à vous deux pour nos nombreuses discussions. Je n'oublie pas non plus Alexis, Emilie, Guillaume, Hendrik, Karine, Laetitia, Olivier, Ramla, Stéphane, Vanessa, Vésale...

En rentrant chez soi, on ne peut que rarement laisser son travail et ses préoccupations dans son bureau ou dans son ordinateur. Pour avoir su détourner mon regard de ces inquiétudes et sans aucun doute pour plein d'autres motifs, je remercie ma famille et mes amis. Ce travail doit beaucoup à Anwuli, merci de tout coeur.

TABLE DES MATIÈRES

Introduction 9

1. Déformations galoisiennes : rappels 21
Introduction 21
1.1. Préliminaire fonctoriel 23
1.2. Critère de Schlessinger 27
1.3. Le critère de Schlessinger revu par Mazur 29
1.4. Condition de déformation, foncteur relativement représentable 39
1.5. Représentations galoisiennes 42

2. Relèvement de représentations presque extraordinaires en p 49
Introduction 49
2.1. Deformation theory 51
2.2. Local-Global 53
2.3. The admissible pair (C_v^{neo}, L_v^{neo}) 58
2.4. Main Theorem 63
2.5. Applications, companion forms 68

3. Arithmétique des extensions peu ramifiées en p 71
Introduction 71
3.1. Théorie p-adique du corps de classes 73
3.2. Présentation des objets arithmétiques 76
3.3. Structures de $\mathbb{F}_p[H]$-modules semi-simples 79
3.4. Générateurs et relations de $\widetilde{G}_S^T$ 85
3.5. Déformation explicite, cadre 94
3.6. Méthode de Boston 95
3.7. Dimension de Krull de $\widetilde{R}_S^T/p$ 101

Bibliographie 107

Introduction

Dans ce travail, notre intérêt porte sur la théorie des déformations appliquée à la construction d'extensions galoisiennes à travers les déformations localement abéliennes, ou plus exactement presque extraordinaires.

Ce manuscrit est composé de trois chapitres. Le **chapitre 1** propose des rappels sur les déformations galoisiennes. Le **chapitre 2** est consacré aux déformations presque extraordinaires en p, ici p est un nombre premier. Notre théorème principal est un résultat de relèvement de représentations résiduelles presque extraordinaires (cf. théorème B). Comme conséquence, on montre l'existence, pour certains premiers p, d'extensions galoisiennes de $\mathbb{Q}(\mu_{p^\infty})$ non-ramifiées en p dont le groupe de Galois est isomorphe à $\mathrm{SL}_2(\mathbb{Z}_p)$ (cf. théorème C). Ici, $\mathbb{Q}(\mu_{p^\infty})$ est l'extension obtenue à partir de $\mathbb{Q}$ en ajoutant les racines de l'unité d'ordre une puissance de p.
La motivation initiale du **chapitre 3** est de décrire une pro-p-extension $\widetilde{K}_S^T/K$ dont la définition s'inspire du cas presque extraordinaire du **chapitre 2**. Le point de vue est purement arithmétique, la méthode aussi. On détermine le nombre minimal de générateurs et de relations du groupe de Galois de $\widetilde{K}_S^T/K$ (cf. théorème 3.4.1). Comme conséquence, on obtient des exemples nouveaux de pro-p-groupes de Galois libres à plusieurs générateurs. On donne également une application en déformant une représentation de $\mathrm{Gal}(\widetilde{K}_S^T/K)$. Les deux derniers chapitres sont indépendants, même si le cadre du **chapitre 3** s'inspire du **chapitre 2**.

Nous détaillons le contenu des chapitres en présentant le contexte général et les méthodes de démonstration de nos résultats.

Chapitre 1. Déformations galoisiennes : rappels

Commençons par présenter le contexte de notre travail. Soit p un nombre premier. On note respectivement $\overline{\mathbb{Q}}$ et $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}$ et de $\mathbb{Q}_p$. On fixe un plongement $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.
A chaque forme modulaire f parabolique, propre, normalisée de poids $k \geq 2$ et de niveau $N \geq 1$, on peut associer une représentation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ continue et non-ramifiée en dehors de pN grâce aux travaux de Deligne (cf. sous-section 1.5.3).
En réduisant ρ_f (et en semi-simplifiant), on obtient une représentation résiduelle $\bar{\rho}_f$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ continue, impaire et non-ramifiée en dehors de pN (cf. théorème 1.5.7).
Un problème inverse apparaît et porte sur l'existence de relèvement d'une représentation résiduelle $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ continue, irréductible, non-ramifiée en dehors d'un ensemble fini de premiers. Pour donner un sens précis à cette question, il s'agit de savoir ce que l'on entend par relèvement. Comme $\bar{\rho}$ est continue, elle prend ses valeurs dans un corps fini $\mathbb{F}$ de caractéristique p. On note $\widehat{\mathcal{C}}$ la catégorie des anneaux locaux, complets, Noetheriens de corps résiduel $\mathbb{F}$ (cf. sous-section 1.1.1). On regarde alors les représentations continues $\rho_R : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R)$ telles que $(\rho_R \mod m_R) = \bar{\rho}$, où $R \in \widehat{\mathcal{C}}$ et où m_R est l'idéal maximal de R. Les relèvements de $\bar{\rho}$ dont on parle par la suite sont de cette forme[(1)].
Ce chapitre est consacré à ce problème de rélèvement (cf. théorème 1.3.9). On rappelle la

[(1)] Dans[Hi 1], Hida construit des représentations à valeurs dans $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ à partir de formes ordinaires (p-adiques).

théorie de Schlessinger (cf. sections 1.2 et 1.1) ainsi que la théorie des déformations "à la Mazur" (cf. sections 1.3 et 1.4), l'exposition est classique et les démonstrations bénéficiant d'une référence précise dans la littérature ne sont pas reproduites. On termine par des rappels sur les formes compagnons (cf. sous-section 1.5.4).

Chapitre 2. Relèvement de représentations presque extraordinaires en p

Notre approche est motivée par le principe suivant : "les représentations galoisiennes associées aux formes modulaires ([DS]) permettent de construire des extensions galoisiennes, de décrire les groupes de Galois de ces extensions et d'en connaître la ramification". Le manière dont Ribet démontre le résultat ci-dessous illustre ce principe.

***Théorème 0.0.1* ([Ri], Th.1.2).** — *Soit $2 \leq k \leq p-3$ un entier pair. Supposons que le nombre premier p divise le k-ème nombre de Bernoulli B_k.*
Alors il existe une extension galoisienne $E/\mathbb{Q}$ contenant $\mathbb{Q}(\mu_p)$ telle que :
(a) $E/\mathbb{Q}(\mu_p)$ soit non-triviale et non-ramifiée,
(b) le groupe $H = \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ soit abélien de type $(p, \ldots, p)$,
(c) si $g \in G = \mathrm{Gal}(E/\mathbb{Q})$ et $h \in H$, alors : $ghg^{-1} = \chi_p(g)^{k-1} \cdot h$, où χ_p désigne le caractère cyclotomique.

Ribet exhibe une forme modulaire f dont les coefficients du q-développement vérifient des congruences héritées de l'hypothèse de divisibilité $p|B_k$ ([Ri], Th.3.7). On note $\bar{\rho}_{Ribet}$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ la réprésentaion associée à f, où $\mathbb{F}$ désigne un corps fini de caractéristique p.
La représentation $\bar{\rho}_{Ribet}$ est continue et non-ramifiée en dehors de p. De plus, $\bar{\rho}_{Ribet}$ est une extension non-triviale de la représentation associée à la puissance χ_p^{k-1} du caractère cyclotomique par la caractère trivial :

$$\bar{\rho}_{Ribet} \simeq \begin{pmatrix} 1 & * \\ 0 & \chi_p^{k-1} \end{pmatrix}$$

et la restriction de $\bar{\rho}_{Ribet}$ au sous-groupe de décomposition en p est diagonalisable ([Ri], Th.1.3). Le corps E du théorème ci-dessus est alors défini comme le sous-corps fixe par $\ker(\bar{\rho}_{Ribet})$.

Cas ordinaire. — Soit $\bar{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue, où $G_{\mathbb{Q},\{p\}}$ désigne le groupe de Galois de l'extension maximale de $\mathbb{Q}$ qui est non-ramifiée en dehors de p (nous n'imposons aucune condition sur les places archimédiennes). On suppose $\bar{\rho}$ absolument irréductible. Dans ce cas, il existe une déformation universelle $\boldsymbol{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(R(\bar{\rho}))$ de $\bar{\rho}$ (cf. théorème 1.3.9).

Nous accordons notre attention au cas où $\bar{\rho}$ est ordinaire[(2)] (sous-entendu en p). Cela signifie que la restriction de $\bar{\rho}$ au groupe de décomposition en p est isomorphe à

$$\begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

[(2)] Il arrive que la condition de ramification soit imposée à χ_2 au lieu de χ_1. On passe d'un cas à l'autre en remplaçant $\bar{\rho}$ par $\bar{\rho} \otimes \det(\bar{\rho})^{-1}$. Le problème de déformation est le même dans chacun des cas (cf. proposition 1.3.19).

avec χ_1 non-ramifié et χ_2 ramifié (cf. exemple 1.4.7). La représentation $\bar{\rho}_{Ribet}$ de Ribet est un exemple de représentation ordinaire en p. Mazur montre l'existence de la déformation universelle ordinaire de $\bar{\rho}$ ([Maz 2], §.30) notée par la suite :

$$\rho^o : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(R^o), \text{ où } R^o \text{ désigne l'anneau de déformation ordinaire de } \bar{\rho}.$$

L'anneau de déformation $R(\bar{\rho})$ se surjecte sur R^o (cf. théorème 1.4.5 et proposition 1.4.8). Sous l'hypothèse $\det(\bar{\rho}) \notin \{1, \chi_p^{\pm 1}, \chi_p^{(p-1)/2}\}$, Mazur décrit le noyau de cette surjection en mettant en évidence des générateurs particuliers des sous-groupes de décomposition et d'inertie ([Maz 3], §.3 et §.8) ; ce dévissage repose sur la méthode mise au point par Boston pour expliciter la déformation universelle grâce à la théorie des pro-p-groupes (cf. section 3.6).

On rappelle maintenant une façon d'obtenir des représentations résiduelles $\bar{\rho}$ ordinaires. Soit $f = \sum_n a_n q^n \in \mathrm{S}_k(\Gamma_1(1), \overline{\mathbb{F}}_p)(\varepsilon)$ une forme parabolique modulo p, propre pour les opérateurs de Hecke et normalisée (cf. section 1.5.3). On suppose f ordinaire, i.e. $a_p \neq 0$. Si $\bar{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ est associée à la forme f[3] (et si le poids de f vérifie $2 \leq k \leq p+1$), alors la représentation $\bar{\rho}$ est ordinaire (cf. théorème 1.5.10). On choisit de travailler avec la réprésentation $\bar{\rho}$ associée à la forme ordinaire f. Dans ce cadre, l'anneau R^o possède une description dans laquelle l'anneau de déformation Λ[4] du caractère

$$\det(\bar{\rho}) : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_1(\mathbb{F}_p)$$

joue un rôle central.

On sait que Λ est isomorphe à l'algèbre d'Iwasawa $\mathbb{Z}_p[[X]]$ (cf. exemple 1.3.22). Comme R^o induit une déformation du caractère $\det(\bar{\rho})$, l'anneau R^o est naturellement muni d'une structure de Λ-module. Par ailleurs, l'algèbre de Hecke $\mathbf{T}$, définie dans [Maz 3] (§.6) et introduite par Hida[5], est de type fini et plate sur Λ si $p \geq 5$ ([Hi 2]). Lorsque $p \geq 5$, il existe une déformation de $\bar{\rho}$ à $\mathbf{T}$, notée :

$$\rho_{Hida} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbf{T}).$$

Cela provient de la théorie de Hida ([Go 2], Th.4) et signifie que toute déformation de $\bar{\rho}$ attachée à une forme p-adique ordinaire sa factorise grâce à ρ_{Hida}. Par conséquent, il existe une application

$$R^o \to \mathbf{T}$$

qui est conjecturalement un isomorphisme[6] ([Maz 3]). On sait que cette application est surjective. La conjecture "$R^o \simeq \mathbf{T}$" implique que

$$\rho^o \simeq \rho_{Hida}$$

et possède par conséquent une interprétation en termes de déformation. Elle signifie qu'une déformation ordinaire est modulaire, autrement dit chaque déformation ordinaire de $\bar{\rho}$ se trouve associée à une forme modulaire p-adique ordinaire ([Go 2]).

---

[3] Au lieu de considérer une forme f modulo p, on pourrait prendre une forme f classique. Dans ce cas, c'est la condition "a_p est un unité p-adique" qui assure que la représentation $\bar{\rho}_f$ est ordinaire ([Maz 3]).
[4] On devrait le noter $R(\det(\bar{\rho}))$ selon la convention adoptée pour les anneaux de déformation universel.
[5] Dans [Hi 2], cette algèbre est définie comme un localisé de h_∞^{ord}.
[6] Si $p \geq 5$ et si la restriction de $\bar{\rho}$ à $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$ est une représentation absolument irréductible, alors la conjecture "$R^o \simeq \mathbf{T}$" est vérifiée ([Wi], Th.3.3).

Supposons, jusqu'à la fin de cette introduction, que $R^o \simeq \mathbf{T}$ et que $\mathbf{T} \simeq \Lambda$. Il en résulte que $R(\bar{\rho})$ est isomorphe à l'algèbre des séries formelles à trois indéterminées sur $\mathbb{Z}_p$ ([Maz 3]). Pour la suite, on suppose que le caractère ε de la forme f associée à $\bar{\rho}$ est le caractère trivial. Dans cette situation, le déterminant de la représentation ρ^o, connu grâce à la théorie de Hida ([Hi 1], §.2 ou [GV], §.3), s'exprime de la façon suivante

$$\begin{array}{rccc} \det(\rho^o) & : & G_{\mathbb{Q},\{p\}} & \to & \Lambda^\times \\ & & \sigma & \mapsto & [\chi_p(\sigma)]^{k-1}\left(\frac{1+T}{1+p}\right)^{s(\sigma)}, \end{array}$$

où $[\chi_p]$ est le relèvement de Teichmüller du caractère cyclotomique mod p et où l'application s provient de la théorie du corps de classes :

$$\begin{array}{ccc} G_{\mathbb{Q},\{p\}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) & \simeq & (1+p\mathbb{Z}_p) \\ \sigma & \mapsto & (1+p)^{s(\sigma)}. \end{array}$$

On en vient à présent à décrire l'extension $\mathbb{Q}(\rho^o)$ qui désigne le sous-corps fixe par ρ^o. Puisque l'on dispose de l'expression de $\det(\rho^o)$, on s'appuie sur le sous-corps $\mathbb{Q}(\det(\rho^o))$ fixe par $\ker\det(\rho^o)$ pour étudier $\mathbb{Q}(\rho^o)$.
Si $(k-1)$ est premier avec $(p-1)$, alors il résulte de $\mathbb{Q}(\det(\rho^o)) \subseteq \mathbb{Q}(\rho^o)$ que

$$\mathbb{Q}(\mu_{p^\infty}) \subseteq \mathbb{Q}(\rho^o).$$

L'extension $\mathbb{Q}(\rho^o)/\mathbb{Q}$ est non-ramifiée en dehors de p. Pour connaître la ramification de $\mathbb{Q}(\rho^o)/\mathbb{Q}$, il suffit ainsi de regarder la ramification de l'extension $\mathbb{Q}(\rho^o)/\mathbb{Q}(\mu_{p^\infty})$. Or, lorsque $(k-1)$ est premier avec $(p-1)$, la restriction de ρ^o au sous-groupe d'inertie en p de $\mathbb{Q}(\rho^o)/\mathbb{Q}(\mu_{p^\infty})$ est isomorphe à

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

Dans la suite, le désir de tuer la ramification en p nous amène vers le cas où l'étoile "$*$" disparaît. Mais avant, voyons ce que l'on connaît de l'image de ρ^o.
Si l'image de $\bar{\rho}$ contient $\mathrm{SL}_2(\mathbb{F}_p)$ et si $\mathrm{pgcd}(k-1, p-1) = 1$, alors l'image de ρ^o contient $\mathrm{SL}_2(\Lambda)$ ([MW], Appendix, Prop.3) et donc :

$$\mathrm{Gal}(\mathbb{Q}(\rho^o)/\mathbb{Q}(\mu_{p^\infty})) \simeq \mathrm{SL}_2(\Lambda).$$

L'hypothèse concernant l'image de $\bar{\rho}$ est discutée dans la suite de l'introduction. Notons que si $p \geq 5$ et si $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \mathrm{im}\bar{\rho}$, alors la conjecture "$R^o \simeq \mathbf{T}$" est vérifiée d'après [Wi] (Th.3.3) car la restriction de $\bar{\rho}$ à $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ est absolument irréductible.

Cas extraordinaire et travail d'Ohtani. — On se souvient que la représentation $\bar{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ est associée à la forme ordinaire f et qu'elle est supposée absolument irréductible. Dans [Oh], Ohtani étudie le cas où $\bar{\rho}$ est extraordinaire en p, i.e. lorsque la restriction de $\bar{\rho}$ au groupe de décomposition en p est isomorphe à la somme de deux caractères

$$\chi_1 \oplus \chi_2,$$

avec χ_1 non-ramifié et χ_2 ramifié.

Avant de parler des déformations extraordinaires de $\bar{\rho}$, on rappelle comment obtenir des représentations résiduelles $\bar{\rho}$ extraordinaires. Grâce à un théorème de Gross (cf. théorème

1.5.14 et lemme 1.5.13), on sait que la représentation résiduelle attachée à f est extraordinaire en p si et seulement si f admet une forme compagnon. On remarque que si $\bar{\rho}' : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ est une représentation impaire[7] et absolument irréductible, alors on a l'équivalence : $\bar{\rho}'$ est extraordinaire si et seulement si $\bar{\rho}'$ est associée à une forme compagnon. Ceci est une conséquence de la conjecture de Serre ([Kh 2], pour le cas $N = 1$) combinée au théorème de Gross évoqué précédemment.

On suppose désormais que $\bar{\rho}$ est une réprésentation extraordinaire. Il existe une déformation extraordinaire $\rho^{eo} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(R^{eo})$ de $\bar{\rho}$ et comme une déformation extraordinaire est en particulier ordinaire, il existe une surjection $R^o \twoheadrightarrow R^{eo}$ (cf. proposition 1.4.8). Ohtani montre que si $\chi_1\chi_2^{-1} \neq \chi_p^{\pm 1}$, alors le noyau de la surjection $R^o \twoheadrightarrow R^{eo}$ est un idéal principal, que nous notons (b) (cf.[Oh], Coro.2.2). Comme on a supposé d'une part que $R^o \simeq \mathbf{T}$ et d'autre part que $\mathbf{T} \simeq \Lambda$, il vient :

$$R^{eo} \simeq \Lambda/(b'),$$

où (b') désigne l'image de (b) dans Λ. Dans ce contexte, Ohtani montre que la dimension de Krull de R^{eo} vaut 1, cela passe par la théorie des formes p-adiques à multiplication complexe ([Oh], Lem.3.3).

On en vient à décrire l'extension galoisienne construite grâce à ρ^{eo}, i.e. le corps $\mathbb{Q}(\rho^{eo})$ défini comme le sous-corps fixe par $\ker(\rho^{eo})$. Il se trouve que la déformation extraordinaire ρ^{eo} est localement abélienne, autrement dit l'image de chaque groupe de décomposition par ρ^{eo} est abélienne. Il en résulte, grâce à la théorie du corps de classes, que l'extension $\mathbb{Q}(\rho^{eo})/\mathbb{Q}(\mu_{p^\infty})$ est non-ramifiée. On termine cette description avec le résultat principal de [Oh] concernant le groupe de Galois de $\mathbb{Q}(\rho^{eo})/\mathbb{Q}(\mu_{p^\infty})$. Supposons que $p \geq 5$, que $\mathrm{SL}_2(\mathbb{F}_p)$ soit contenu dans l'image de $\bar{\rho}$ et que $\mathrm{pgcd}(k-1, p-1) = 1$. Alors le groupe de Galois de l'extension non-ramifiée $\mathbb{Q}(\rho^{eo})/\mathbb{Q}(\mu_{p^\infty})$ est isomorphe à

$$\mathrm{SL}_2(\Lambda/(b')) \text{ ([Oh], Th.0.1).}$$

Il ne manque qu'une seule information pour être en possession d'une description complète de $\mathbb{Q}(\rho^{eo})/\mathbb{Q}(\mu_{p^\infty})$. On sait que la dimension de Krull de R^{eo} vaut 1 et que $R^{eo} \simeq \Lambda/(b')$, mais on ne sait pas si b' est divisible par p[8]. Supposons un instant que $b' = X$. Alors la représentation

$$\rho^{eo} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(R^{eo})$$

est modulaire à twist près ; il s'agit d'une conséquence du théorème principal de [SW] combiné à la preuve de la conjecture de Serre par Khare-Wintenberger pour le niveau $N = 1$ ([Kh 2], Cor.1.4).

Nos résultats. — Déterminer si $p|b'$ constitue la motivation initiale de mon travail. On change de cadre en s'intéressant aux déformations de représentations presque extraordinaires[9], cela tient à la méthode employée. Car si les objets sont de même nature que ceux

[7] Je ne connais pas d'exemple naturel de représentation extraordinaire qui soit paire.

[8] Le théorème de préparation de Weierstrass indique de $(b') = (p^\mu P(X))$, où $\mu \in \mathbb{N}$ et P est un polynôme distingué de Λ ([Wa], Th.7.3).

[9] L'anneau de déformation presque extraordinaire R^{neo} existe ; avec les notations de [Oh], on sait que $R^{neo} \simeq R(\bar{\rho})/(b,c)$ et que $R^{eo} \simeq R(\bar{\rho})/(a-1,b,c)$ ([Oh], §.2). Le morphisme naturel qui va du foncteur de déformation extraordinaire vers le celui de déformation presque extraordinaire n'est pas lisse (cf. définition 1.2.2).

présentés précédemment, notre approche est différente puisqu'elle repose sur la méthode de Ramakrishna (cf [Ra 2]), formalisée par Taylor ([Ta 1]).

Soit $\bar{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue, impaire et absolument irréductible. On dit que $\bar{\rho}$ est presque extraordinaire si sa restriction au groupe de décomposition en p est isomorphe à la somme de deux caractères.

Dans la suite, indiquons deux différences avec les deux cas présentés précédemment :
• on oublie la condition associée à l'action de l'inertie en p. Cela présente l'avantage de pouvoir utiliser la méthode Taylor-Ramakrishna évoquée en fin d'introduction. Cependant, il y a un inconvénient : on ne peut pas aborder la question de modularité du relèvement.
• les déformations que l'on considère sont à déterminant fixé (cf. sous-section 2.1.2) ; cela revient à travailler avec des groupes de cohomologie à valeurs dans $\mathrm{Ad}^0(\bar{\rho})$ et non plus dans $\mathrm{Ad}(\bar{\rho})$. Cette seconde différence met à notre disposition un dévissage cohomologique (cf. lemme 2.4.1).
Jusqu'à la fin de l'introduction, les déformations sont supposées être à déterminant fixé.

Le résultat principal s'énonce :

Théorème A. — *Soit $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue, impaire et non-ramifiée en dehors de p, avec $p \geq 5$. On suppose $\bar{\rho}$ presque extraordinaire en p. De plus, supposons que $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \mathrm{im}(\bar{\rho})$.*
Alors il existe un relèvement $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ de $\bar{\rho}$ et un ensemble fini de premiers T contenant p tels que

$$\rho \text{ soit } T\text{-ramifiée et } \rho_{|G_{\mathbb{Q}_p}} \text{ soit isomorphe à la somme de deux caractères.}$$

Le théorème suivant est une conséquence du théorème A, il fait appel aux formes compagnons et s'obtient en reformulant le corollaire 2.5.4.

Théorème C. — *Soit $p \in \{107, 139, 271, 379\}$.*
Alors il existe une extension galoisienne $M/\mathbb{Q}(\mu_{p^\infty})$ non-ramifiée en dehors d'un ensemble fini de places ne contenant pas p et telle que

$$\mathrm{Gal}(M/\mathbb{Q}(\mu_{p^\infty})) \simeq \mathrm{SL}_2(\mathbb{Z}_p).$$

On donne les idées de la preuve du théorème C. L'extension M n'est rien d'autre que le corps $\mathbb{Q}(\rho)$ fixe par le noyau du relèvement ρ dont l'existence est assurée par le théorème A. Un résultat de relèvement de Serre indique que l'image de ρ contient $\mathrm{SL}_2(\mathbb{Z}_p)$ puisque celle de $\bar{\rho}$ contient $\mathrm{SL}_2(\mathbb{F}_p)$ (cf. proposition 2.5.2) ; ici nous n'utilisons pas le résultat de Boston évoqué dans le cas ordinaire ([MW], Appendix, Prop.3). Enfin, comme une déformation presque extraordinaire de $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ est localement abélienne, l'extension $M/\mathbb{Q}(\mu_{p^\infty})$ est non-ramifiée en p. On renvoie à la section 2.5 pour les détails.

Pour terminer, on discute des hypothèses et on donne le goût de la démonstration du théorème A. En réalité, on démontre un résultat plus général (cf. théorème B) ; comme les idées en jeu sont les mêmes, on expose le cas plus simple du théorème A.

La démonstration du théorème A repose sur la méthode de Taylor-Ramakrishna qui assure l'existence d'une déformation presque extraordinaire de $\bar{\rho}$ prenant ses valeurs dans $\mathbb{Z}_p$. De façon générale, en combinant des théorèmes de modularité avec la méthode de Taylor-Ramakrishna, on peut espérer que le relèvement fourni est modulaire ([Ta 1] et [Ge],

par exemple). Le cadre presque extraordinaire n'offre pas cette application puisque nous n'avons aucun contrôle sur l'image de l'inertie en p.
On peut résumer la méthode de Taylor-Ramakrishna de la façon suivante. On commence par montrer que les restrictions locales de $\bar{\rho}$ possèdent une déformation à valeurs dans $\mathbb{Z}_p$ (cf. définition 2.2.4 et section 2.3). Ensuite, on voit qu'un groupe de Selmer mesure l'obstruction à ce qu'une déformation extraordinaire de $\bar{\rho}$ à $\mathbb{Z}_p$ existe, il s'agit d'un principe local-global appliqué au foncteur de déformation presque extraordinaire de $\bar{\rho}$ (cf. propositions 2.2.9 et 2.2.10). Pour terminer, grâce au théorème de densité de Cebotarev, il existe un algorithme pour trivialiser le groupe de Selmer en question. Cela ajoute de la ramification, c'est de là que vient l'ensemble fini de places T (cf. proposition 2.4.4).
L'initialisation de l'algorithme impose à $\bar{\rho}$ d'être impaire (cf. corollaire 2.3.5). Par ailleurs, dans le cas extraordinaire, cette étape d'initialisation fait défaut (cf. sous-section 2.3.3) et c'est pour cette raison que nous travaillons avec des déformations presque extraordinaires plutôt qu'avec des déformations extraordinaires. Par ailleurs, supposer $p \geq 5$ implique que le groupe $\mathrm{PGL}_2(\mathbb{F}_p)$ n'est pas résoluble et que $H^1(\mathrm{SL}_2(\mathbb{F}_p), \mathrm{Ad}^0(\bar{\rho})) = (0)$ (cf. lemme 2.4.1). Ces deux points interviennent dans l'algorithme (cf. sous-section 2.4.2) sachant que l'image de $\bar{\rho}$ est supposée contenir $\mathrm{SL}_2(\mathbb{F}_p)$. Parlons de cette hypothèse concernant l'image de $\bar{\rho}$. Comme $\bar{\rho}$ est impaire, absolument irréductible et non-ramifiée en dehors de p, on sait qu'il existe une forme modulaire de niveau 1 à laquelle $\bar{\rho}$ est attachée ([Kh 2]). Or, dans ce cas, il n'y a qu'un nombre fini de premiers p pour lesquels $\mathrm{SL}_2(\mathbb{F}_p) \nsubseteq \mathrm{im}(\bar{\rho})$ ([Se 6], Th.10)[(10)]. Cette hypothèse sur l'image de $\bar{\rho}$ s'avère donc naturelle.

On propose de terminer cette introduction par un exemple. Dans le théorème C, les premiers p sont choisis de sorte qu'il existe une forme compagnon f modulo p de niveau $N = 1$, à caractère trivial, de poids k avec $\mathrm{pgcd}(k-1, p-1) = 1$ et $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \mathrm{im}(\bar{\rho})$, où $\bar{\rho}$ est attachée à f. L'hypotèse "$\mathrm{pgcd}(k-1, p-1) = 1$" n'est présente que pour s'assurer que $\mathbb{Q}(\det(\rho)) = \mathbb{Q}(\mu_{p^\infty})$ et permet d'énoncer un résultat uniforme.

Si p est différent de

$$2, 3, 5, 7, 11, 31, 59 \text{ et } 3617,$$

alors l'image de la représentation $\bar{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ attachée à Δ_{16} (la forme parabolique propre et normalisée de poids 16) contient le groupe $\mathrm{SL}_2(\mathbb{F}_p)$ ([Se 6], §.3.5). Des calculs menés par Elkies et Atkin (cf. sous-section 1.5.4) indiquent que Δ_{16} est une forme compagnon modulo 397, de niveau $N = 1$. On désigne par ρ le relèvement fourni par le théorème A. Alors l'extension $\mathbb{Q}(\rho)/\mathbb{Q}(\det(\rho))$ est non-ramifiée en p de groupe de Galois isomorphe à $\mathrm{SL}_2(\mathbb{Z}_p)$ et ici $\mathbb{Q}(\det(\rho)) \subset \mathbb{Q}(\mu_{p^\infty})$ car $\mathrm{pgcd}(k-1, p-1) = 3$, avec $k = 16, p = 397$.

Chapitre 3. Arithmétique des extensions peu ramifiées en p

Soit K un corps de nombres, soit S et T deux ensembles finis et disjoints de places de K avec T formé uniquement de places au-dessus de p. On note S_p l'ensemble des places de S

[(10)] Si l'image d'un représentation associée une forme modulaire ne contient pas $\mathrm{SL}_2(\mathbb{F}_p)$, alors cette image est contenue dans un sous-groupe de Borel, dans un normalisateur d'un sous-groupe de Cartan ou son image dans $\mathrm{PGL}_2(\mathbb{F}_p)$ est isomorphe au groupe symétrique S_4 ([Se 3], §.3.2). Khare a montré l'existence de relèvements à $\mathbb{Z}_p$ lorsque l'image est contenue dans un sous-groupe de Borel ([Kh 1], Th.2), mais sans contrôler le comportement local du relèvement.

au-dessus de p. On fixe $\overline{K}$ une clôture algébrique de K. Le couple $(r_1(K), r_2(K))$ désigne la signature de K. On note K^{cyc} la $\mathbb{Z}_p$-extension cyclotomique de K.
Par définition, $\widetilde{K}_S^T$ est la plus grande pro-p-extension de K^{cyc} non-ramifiée en dehors de S et totalement décomposée en T. Le pro-p-groupe de Galois de $\widetilde{K}_S^T/K$ est désigné par $\widetilde{G}_S^T$.
Notre désir d'étudier l'extension $\widetilde{K}_S^T/K$ trouve son origine dans le **chapitre 2** où des extensions de $\mathbb{Q}(\mu_{p^\infty})$ non-ramifiées en p sont exhibées grâce aux représentations associées aux formes compagnons. Dans le cas où $K = \mathbb{Q}, p \notin S$ et $T = \emptyset$, on peut voir une analogie entre une extension de $\mathbb{Q}(\mu_{p^\infty})$ non-ramifiée en p et une sous-extension de $\widetilde{K}_S^T$ qui contient K^{cyc}.
Quand Ω est un pro-p-groupe, on note $H^i(\Omega)$ le groupe de cohomologie $H^i(\Omega, \mathbb{F}_p)$, où $i = 1, 2$. On souhaite donc déterminer :
(i) $\dim_{\mathbb{F}_p} H^1(\widetilde{G}_S^T)$, i.e. le nombre minimal de générateurs de $\widetilde{G}_S^T$;
(ii) $\dim_{\mathbb{F}_p} H^2(\widetilde{G}_S^T)$, i.e. le nombre minimal de relations de $\widetilde{G}_S^T$;
(iii) la dimension cohomologique $\mathrm{cd}(\widetilde{G}_S^T)$.
En particulier, il est intéressant de savoir si l'inégalité $\mathrm{cd}(\widetilde{G}_S^T) \leq 1$ peut avoir lieu puisque cela équivaut à dire que le groupe $\widetilde{G}_S^T$ est pro-p-groupe libre.
Avant de présenter nos résultats concernant $\widetilde{G}_S^T$, on fait des rappels de résultats connus dans le cadre de la ramification restreinte au-dessus d'un corps de nombres. Les méthodes que nous employons pour étudier $\widetilde{G}_S^T$ s'inspirent de ce cadre.

Ramification restreinte au-dessus d'un corps de nombres. — Ici, $K_S(p)$ désigne la plus grande pro-p-extension S-ramifiée de K (nous n'imposons aucune condition sur les places archimédiennes). On note $G_S(p) = \mathrm{Gal}(K_S(p)/K)$. On peut ainsi faire varier K ou S. Rappelons deux cas simples, le premier est une conséquence du théorème de Hermite-Minkowski et le second du théorème de Kronecker-Weber :
– $K = \mathbb{Q}$, $S = \emptyset$: $\mathbb{Q}_\emptyset(p) = \mathbb{Q}$;
– $K = \mathbb{Q}$, $S = \{p\}$: $\mathbb{Q}_S(p) = \mathbb{Q}^{cyc}$ lorsque $p \geq 3$.
Dans le cas où $p = 2$, on suppose K totalement imaginaire. De cette façon, si v est une place de K telle que $Nv \not\equiv 0, 1 \mod p$, alors v ne se ramifie pas dans $K_S(p)/K$ (ici Nv désigne le cardinal du corps résiduel du complété K_v).

Le résultat suivant donne le nombre minimal de générateurs de $G_S(p)$ et fournit un majorant du nombre minimal de relations de $G_S(p)$. Dans les deux cas, le module de Kummer $V_S = (\mathcal{J}_K \prod_{v \notin S} \mathcal{U}_v) \cap \mathcal{R}_K$ intervient (cf. section 3.1 pour la définition des modules $\mathcal{J}_K, \mathcal{U}_v$ et $\mathcal{R}_K$).

Théorème 0.0.2 **([Ko], Th.11.5, Th.11.8).** — *Sous les conditions précédentes, on a :*

$$\dim_{\mathbb{F}_p} H^1(G_S(p)) = \dim_{\mathbb{F}_p}(V_S/\mathcal{R}_K^p)^* + \sum_{v \in S} \delta(\mu_p(K_v)) - \delta(\mu_p(K)) + 1 - r_1(K) - r_2(K) + \sum_{v \in S_p(K)} [K_v : \mathbb{Q}_p],$$

et

$$\dim_{\mathbb{F}_p} H^2(G_S(p)) \leq \dim_{\mathbb{F}_p}(V_S/\mathcal{R}_K^p)^* + \sum_{v \in S} \delta(\mu_p(K_v)) - \delta(\mu_p(K)) + \theta,$$

où θ vaut 1 si S est vide et si $\mu_p \subset K$, et vaut 0 sinon.

Le nombre minimal de générateurs de $G_S(p)$ se calcule grâce à la théorie p-adique du corps de classes (cf. section 3.1) puisque $H^1(G_S(p)) = \mathrm{Hom}(G_S(p)/G_S(p)^p[G_S(p), G_S(p)], \mathbb{F}_p)$. Pour le nombre minimal de relations, on fait appel à un principe local-global, ce qui explique la présence d'une inégalité. Plus précisément, il s'agit de comparer les relations locales et globales (sur le modèle du lemme 3.4.4) à l'aide du noyau de Shafarevich :

$$Ш_S = \ker\left[H^2(G_S(p)) \to \bigoplus_{v\in S} H^2(\widehat{G}_v)\right] \text{ (cf. section 3.2 pour la définition de } \widehat{G_v}).$$

Avant de revenir plus en détail sur cette stratégie dans la section 3.4, on énonce le théorème suivant motivant l'introduction du module $(V_S/\mathcal{R}_K^p)^*$.

***Théorème 0.0.3* ([Ko], Th.11.3).** — *Le noyau de Shafarevich s'injecte dans l'espace dual $(V_S/\mathcal{R}_K^p)^*$:*

$$Ш_S \hookrightarrow (V_S/\mathcal{R}_K^p)^*.$$

Le groupe abélien $Ш_S$ est donc fini.

Dans le théorème 0.0.2, la dimension $\dim_{\mathbb{F}_p} H^2(G_S(p))$ est estimée par une inégalité. Dans la sous-section qui suit, la dimension $\dim_{\mathbb{F}_p} H^2(G_S(p))$ est donnée par une égalité.

Cas où S contient les places au-dessus de p. —

***Théorème 0.0.4* ([NSW], Th.10.7.13).** — *Soit K un corps de nombres et S un ensemble fini de places de K contenant les places au-dessus de p. Lorsque $p = 2$, on suppose K totalement imaginaire. On note G_S le groupe de Galois de K_S/K où K_S est la plus grande extension de K non-ramifiée en dehors de S.*
Alors la caractéristique d'Euler-Poincaré tronquée à l'ordre deux est donnée par :

$$\chi_2(G_S(p)) = -r_2(K).$$

***Théorème 0.0.5* ([NSW], Cor.10.4.9, Prop.10.11.3).** — *Sous les mêmes hypothèses que dans le théorème qui précède, on a :*

$$\mathrm{cd}(G_S(p)) \leq \mathrm{cd}_p(G_S) = 2.$$

De plus, on dispose de l'inégalité suivante portant sur la dimension cohomologique stricte :

$$\mathrm{scd}(\mathrm{Gal}(K_S(p)/K^{cyc})) \leq 2.$$

La question se pose de savoir si des résultats analogues aux deux théorèmes précédents existent dans le cas où la ramification est incomplète en p, i.e. lorsque S ne contient pas toutes les places au-dessus de p.

Travaux de Labute et de Schmidt. — Labute a mis en évidence une classe de groupes dont la dimension cohomologique est 2, il s'agit des groupes mild ([La]). En arithmétique, certains groupes de Galois $G_S(p)$ se trouvent être mild pour des ensembles de places S ne contenant pas de place p-adique ; Labute en donne des exemples (cf. [La], §.1.2).
En se penchant sur le cas de la ramification restreinte avec des ensembles S ne contenant pas toutes les places au-dessus de p, Schmidt a montré dans [Sch] le théorème suivant ; le résultat principal de [Sch] comporte quatre points, nous reproduisons ici le premier d'entre eux.

Théorème 0.0.6 **([Sch], Th.1.1)**. — *Soit p un nombre premier différent de 2. On se donne S, T et M trois ensembles de places de K disjoints deux à deux, avec S et T finis et M de densité de Dirichlet nulle.*
Alors il existe un ensemble fini S_0 de places de K disjoint de $S \cup T \cup M$ pour lequel le groupe de Galois de la pro-p-extension maximale de K qui est $S \cup S_0$-ramifiée et T-décomposée, noté $G_{S\cup S_0}^T(p)$, est de dimension cohomologique 2 et tel que le cup-produit suivant soit surjectif :

$$H^1(G_{S\cup S_0}^T(p), \mathbb{F}_p) \otimes H^1(G_{S\cup S_0}^T(p), \mathbb{F}_p) \longrightarrow H^2(G_{S\cup S_0}^T(p), \mathbb{F}_p).$$

Schmidt montre même que le groupe $G_{S\cup S_0}^T(p)$ est mild selon la terminologie de Labute [La]. D'après [La], on sait qu'un groupe mild est de dimension cohomologique 2.
Tentons de résumer les grandes lignes des méthodes utilisées.
Il s'agit dans un premier temps de travailler avec un groupe $G_{S\cup S_0}^T(p)$ dont les relations sont purement locales ; on s'assure donc que le noyau de Shafarevich associé est trivial de sorte que le second groupe de cohomologie de $G_{S\cup S_0}^T(p)$ s'injecte dans la somme des seconds groupes de cohomologie locaux. Dans un second temps, on note la place tenue par le cup-produit grâce au théorème de Schmidt suivant.

Théorème 0.0.7 **([Sch], Th.6.2)**. — *Soit $p \neq 2$ un nombre premier et soit G un pro-p-groupe tel que $H^1(G) := H^1(G, \mathbb{F}_p)$ soit fini.*
Supposons $H^2(G) \neq (0)$ et qu'il existe une décomposition $H^1(G) = U \oplus V$ telle que :
1) le cup-produit $V \otimes V \to H^2(G)$ soit trivial,
2) le cup-produit $U \otimes V \to H^2(G)$ soit surjectif,
Alors le groupe G est (mild et en particulier) de dimension cohomologique 2.

Nos résultats. — Notre travail permet d'unifier le cas $T = \emptyset$ traité dans [Sa] ([Sa], Th. II.2.2 et 2.8) et le cas $T = Pl_p$ et $S = \emptyset$ traité dans [JM]. Remarquons aussi que lorsque $T = \emptyset$ et S contient les places au-dessus de p, l'extension $\widetilde{K}_S^T$ coïncide avec la pro-p-extension S-ramifiée de K. Nous nous sommes inspirés de ces travaux pour démontrer le résultat suivant.

Théorème 0.0.8. — *Le nombre minimal de générateurs $d_1(\widetilde{G}_S^T)$ et le nombre minimal de relations $d_2(\widetilde{G}_S^T)$ de $\widetilde{G}_S^T$ satisfont :*

$$d_1(\widetilde{G}_S^T) = \dim_{\mathbb{F}_p}(\widetilde{V}_S^T/\mathcal{R}_K^p) + 1 + |Pl_p - (S_p \cup T)| - r_1(K) - r_2(K) + \sum_{v\in S_p} [K_v : \mathbb{Q}_p]$$

$$+\sum_{v\in S}\delta(\mu_p(K_v))-\delta(\mu_p(K)).$$

et

$$d_2(\widetilde{G}_S^T)\leq \dim_{\mathbb{F}_p}(\widetilde{V}_S^T/\mathcal{R}_K^p)+|Pl_p-(S_p\cup T)|+\sum_{v\in S}\delta(\mu_p(K_v))-\delta(S)\delta(\mu_p(K)),$$

où $\delta(S)$ *vaut* 0 *si* $S=\emptyset$ *et* 1 *sinon.*
En notant $\chi_2(\widetilde{G}_S^T)$ *la caractéristique d'Euler-Poincaré de* $\widetilde{G}_S^T$ *tronquée à l'ordre* 2*, on a :*

$$\chi_2(\widetilde{G}_S^T)\leq r_1(K)+r_2(K)-\sum_{v\in S_p}[K_v:\mathbb{Q}_p].$$

Le résultat que nous démontrons est en fait plus précis puisqu'il concerne les modules $H^i(\widetilde{G}_S^T)$ pour $i=1,2$ vus comme des modules galoisiens après avoir fixé un sous-corps k de K tel que K/k soit galoisienne et d'ordre premier à p (cf. théorème 3.4.1).

Au cours de la preuve du théorème précédent, on montre l'inclusion suivante concernant le groupe de Shafarevich $Ш(\widetilde{G}_S^T):=\ker\left[H^2(\widetilde{G}_S^T)\longrightarrow\bigoplus_{v\in S}H^2(\widehat{G}_v)\oplus\bigoplus_{v\notin S\cup T}H^2(G_v^{cr})\right]$.

Proposition 0.0.9. — *(cf. proposition 3.4.19) Le groupe de Shafarevich vérifie l'inclusion :*

$$Ш(\widetilde{G}_S^T)\hookrightarrow(\widetilde{V}_S^T/\mathcal{R}_K^p)^*.$$

La présence de S *et* de T permet d'obtenir des situations où le groupe $\widetilde{G}_S^T$ est libre. On énonce la proposition :

Proposition 0.0.10. — *(cf. proposition 3.4.24) Soit* K *un corps de nombres ne contenant pas les racines p-èmes de l'unité. Supposons que :*
1) pour toute place $v\in S$ *:* $\zeta_p\notin K_v$*,*
2) $S\cup T=Pl_p(K)$*,*
3) toute p-extension de $K(\zeta_p)$ *non-ramifiée hors de* T *et totalement décomposée en* S *soit triviale.*
Alors le groupe $\widetilde{G}_S^T$ *est libre et possède* $1-r_1(K)-r_2(K)+\sum_{v\in S}[K_v:\mathbb{Q}_p]$ *générateurs.*

Nous souhaitons étudier la dimension cohomologique de $\widetilde{G}_S^T$ dans un prochain travail. Cette perspective s'inscrit dans le cadre dressé par Schmidt (cf. sous-section 3.4.4).

Les déformations extraordinaires en p nous ont conduits à définir le groupe $\widetilde{G}_S^T$. On termine avec une application du théorème 3.4.1 en théorie des déformations (cf. théorème 3.7.2). Ici, k est un corps de nombres et M_k est l'extension maximale de k contentant la $\mathbb{Z}_p$-extension cyclotomique k^{cyc} de k telle que M_k/k^{cyc} soit S-ramifiée et T-décomposée.
Soit

$$\bar{\rho}:\mathrm{Gal}(M_k/k)\to\mathrm{GL}_2(\mathbb{F}_p)$$

une représentation continue. Posons $K=(M_k)^{\ker\bar{\rho}}$. On note $Pl_\infty(k)^+$ l'ensemble des places pour lesquelles $\bar{\rho}$ est paire et $Pl_\infty(k)^-$ l'ensemble des places pour lesquelles $\bar{\rho}$ est impaire. Chaque déformation de $\bar{\rho}$ se factorise à travers le groupe $\mathrm{Gal}(\widetilde{K}_S^T/k)$ et on montre :

Théorème 0.0.11. — *Soit* $\bar{\rho} : \mathrm{Gal}(M_k/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ *une représentation continue. Soit* $\mathrm{Ad}(\bar{\rho})$ *la représentation adjointe de* $\bar{\rho}$. *Notons* $\widetilde{R}_S^T$ *l'anneau de déformation de* $\bar{\rho}$. *Alors*

$$\mathrm{dimKrull}(\widetilde{R}_S^T/p\widetilde{R}_S^T) \geq \mathrm{dim}_{\mathbb{F}_p}\mathrm{Ad}(\bar{\rho})^{\mathrm{Gal}(K/k)} + 4\sum_{v\in S_p}[k_v : \mathbb{Q}_p] - 4|Pl_\infty(k)^+| - 2|Pl_\infty(k)^-|,$$

où S_p *est formé des places de* S *qui sont au-dessus de* p.

CHAPITRE 1

DÉFORMATIONS GALOISIENNES : RAPPELS

Introduction

Ce chapitre est consacré à des rappels en théorie des déformations et en théorie des représentations galoisiennes. Ce choix est motivé par le **chapitre** 2 de ce travail dans lequel le formalisme des déformations est utilisé pour construire des extensions galoisiennes non-ramifiées (en p) au-dessus de la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$.
Jusqu'à la **section** 1.4, on propose un exposé de la théorie des déformations initiée par Mazur dans son article [Maz 1]. Le but est de trouver un objet universel paramétrant les déformations d'une représentation continue $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ d'un groupe profini Π, avec $\mathbb{F}$ un corps fini de caractéristique p. Mazur montre que le foncteur[(1)] associé à ce problème vérifie le critère de Schlessinger, i.e. les points *H1*, ..., *H4* dans [Sc]. On adopte ce point de vue par la suite. Signalons d'autres approches de ce problème, par exemple celle de Rouquier-Nyssen avec les pseudo-caractères ([Maz 2], §.7), celle de De Smit-Lenstra [deSL] et celle, plus géométrique, de Kisin avec les "framed" déformations [Ki 2].
Le travail de Schlessinger repose sur l'étude des nilpotents des anneaux locaux, Noetheriens (ou Artiniens), complets et de corps résiduel fixé $\mathbb{F}$. L'anneau des nombres duaux $\mathbb{F}[\varepsilon] := \mathbb{F}[X]/(X^2)$ permet de définir des $\mathbb{F}$-espaces vectoriels, les espaces tangents, qui jouent un rôle central notamment pour tester des propriétés de produit fibré. Schlessinger s'intéresse à un critère de (pro)représentabilité pour un foncteur $F : \mathcal{C} \to \mathrm{Ens}$, où $\mathcal{C}$ désigne la catégorie des anneaux Artiniens, locaux, complets de corps résiduel $\mathbb{F}$; autrement dit, on s'intéresse à l'existence d'un anneau R tel que $F \simeq \mathrm{Hom}(R, -)$. L'anneau R peut vivre dans la catégorie $\widehat{\mathcal{C}}$ (des anneaux locaux, complets, Noetherien de corps résiduel $\mathbb{F}$) plus grande que $\mathcal{C}$, c'est ce qui justifie la terminologie pro-représentable. On peut maintenant citer le théorème suivant dû à Grothendieck ([Maz 2], §.18).

Théorème 1.0.12 **(Grothendieck)**. — *Soit $F : \mathcal{C} \to \mathrm{Ens}$ un foncteur à valeurs dans la catégorie des ensembles tel que $F(\mathbb{F})$ soit réduit à un élément. Alors F est pro-représentable si et seulement si les deux propriétés suivantes sont satisfaites :*
1) Pour chaque couple $(A, \alpha), (B, \beta)$ avec $\alpha \in \mathrm{Hom}(A, C)$ et $\beta \in \mathrm{Hom}(B, C)$, l'application naturelle

$$F(A \times_C B) \to F(A) \times_{F(C)} F(B) \text{ est un isomorphisme.}$$

2) $F(\mathbb{F}[\varepsilon])$ est de dimension finie sur $\mathbb{F}$.

---

(1) Les foncteurs utilisés sont tous covariants.

Le critère de Schlessinger est analogue au théorème ci-dessus, il réduit le nombre de cas à tester dans le premier point. C'est là que $\mathbb{F}[\varepsilon]$ intervient.
Le fil conducteur est donc le foncteur $\mathrm{Hom}(R,-) : \mathcal{C} \to \mathrm{Ens}$, avec $R \in \widehat{\mathcal{C}}$. On remarque que $\mathrm{Hom}(R,-)$ est continu, respecte le produit fibré (i.e. $\mathrm{Hom}(R, A \times_C B) \simeq \mathrm{Hom}(R,A) \times_{\mathrm{Hom}(R,C)} \mathrm{Hom}(R,B)$ en gardant les notations du théorème ci-dessus) et que l'espace tangent $\mathrm{Hom}(R, \mathbb{F}[\varepsilon])$ est un $\mathbb{F}$-espace vectoriel de dimension finie. Ce sont ces trois propriétés qui tracent le chemin pour trouver une caractérisation des foncteurs représentables.

La **section** 1.5 s'articule en trois sous-sections. On présente d'abord des résultats classiques et bien connus concernant les représentations galoisiennes de dimension deux. Ensuite, la construction d'une représentation à partir des points de torsion d'une courbe elliptique est rappelée, ainsi que les résultats de Eichler-Shimura (lorsque $k = 2$), généralisés par Deligne (pour $k \geq 2$), qui associent une représentation galoisienne à une forme modulaire propre et normalisée. Pour terminer, on introduit les formes compagnons qui sont utilisées dans le **chapitre** 2 pour construire une extension non-ramifiée en p au-dessus de la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$.

Notations

p	un nombre premier.
$\mathbb{F}$	un corps fini de caractéristique p.
$\mathrm{W}(\mathbb{F})$	l'anneau des vecteurs de Witt de $\mathbb{F}$.
$\mathrm{Ad}(\bar{\rho})$	la représentation adjointe associée à $\bar{\rho}$.
$\mathrm{Ad}^0(\bar{\rho})$	la sous-représentation de $\mathrm{Ad}(\bar{\rho})$ formée des matrices de trace nulle.
$\mathcal{C}$	la catégorie des anneaux locaux complets et Artiniens de corps résiduel $\mathbb{F}$.
$\widehat{\mathcal{C}}$	la catégorie des anneaux locaux complets et Noetheriens de corps résiduel $\mathbb{F}$.
m_R	l'idéal maximal de l'anneau local R.
$\mathrm{dimKrull}(R)$	la dimension de Krull de l'anneau R.

1.1. Préliminaire fonctoriel

Soit p un nombre premier. Soit $\mathbb{F}$ un corps fini de caractéristique p et soit $\mathrm{W}(\mathbb{F})$ l'anneau des vecteurs de Witt de $\mathbb{F}$. On note m_R l'idéal maximal d'un anneau local R.

1.1.1. Anneaux Noetheriens et Artiniens. —

On appelle algèbre de coefficients un élément de la catégorie $\widehat{\mathcal{C}}$ des anneaux locaux (R, m_R) Noetheriens, complets et munis d'un isomorphisme $R/m_R \simeq \mathbb{F}$. On dit simplement que le corps résiduel de R est $\mathbb{F}$.
Les morphismes entre de tels anneaux sont des morphismes continus d'anneaux locaux qui induisent l'identité sur les corps résiduels. On note $\mathrm{Hom}(R, S)$ l'ensemble des morphismes $R \to S$, lorsque $R, S \in \widehat{\mathcal{C}}$.

Remarque 1.1.1. — Pour chaque anneau $R \in \widehat{\mathcal{C}}$, il existe une application naturelle

$$\varphi : R \to \varprojlim R/m_R^i \ .$$

Comme R est Noetherien, la topologie m_R-adique est séparée et φ est injective. La surjectivité provient du caractère complet de R. La topologie de R est celle donnée par la base de voisinage m_R^i de 0 et φ est un homéomorphisme.

1.1.1.1. Surjectivité, espace tangent. —

Définition 1.1.2. — On appelle espace cotangent (de Zariski) de $R \in \widehat{\mathcal{C}}$ le R/m_R-module suivant :

$$t_R^* = m_R/(m_R^2, p).$$

C'est ainsi un $\mathbb{F}$-espace vectoriel de dimension finie car R est Noetherien. On note

$$t_R = \mathrm{Hom}_{\mathbb{F}}(m_R/(m_R^2, p), \mathbb{F}) \text{ son espace dual, appelé l'espace tangent de } R.$$

On dispose de la caractérisation suivante :

Lemme 1.1.3 **([Sc], Lem.1.1)**. — *Soit $R, S \in \widehat{\mathcal{C}}$. Un morphisme $R \to S$ est surjectif si et seulement si l'application induite $t_R^* \to t_S^*$ est surjective.*

Chaque anneau $R \in \widehat{\mathcal{C}}$ est muni d'une structure naturelle de $\mathrm{W}(\mathbb{F})$-algèbre donnée par un morphisme naturel $\mathrm{W}(\mathbb{F}) \to R$. En effet, si on note $x_1, \ldots, x_n$ une base de t_R^* et $r_1, \ldots, r_n$ une famille qui la relève dans l'idéal maximal m_R, alors le morphisme d'anneaux

$$\mathrm{W}(\mathbb{F})[[X_1, ..., X_n]] \to R$$

qui associe r_i à X_i est surjectif d'après le lemme 1.1.3. Chaque $R \in \widehat{\mathcal{C}}$ est un quotient de $\mathrm{W}(\mathbb{F})[[X_1, ..., X_n]]$, où l'entier n est égal à $\dim_{\mathbb{F}} m_R/({m_R}^2, p)$, avec m_R l'idéal maximal de R. La difficulté se concentre sur l'idéal qui définit ce quotient.

Remarque 1.1.4. — Au départ, on peut adopter un point de vue plus général en se donnant un élément $\Lambda \in \widehat{\mathcal{C}}$ et en regardant la catégorie $\widehat{\mathcal{C}}_\Lambda$ formé des anneaux $R \in \widehat{\mathcal{C}}$ qui possèdent une structure d'algèbre sur Λ donnée par $\Lambda \to R$. On a choisi de se limiter à la

catégorie $\widehat{\mathcal{C}}$ vue comme $\widehat{\mathcal{C}}_{\mathrm{W}(\mathbb{F})}$. Dès que $R \in \widehat{\mathcal{C}}$, le produit complété $R \,\widehat{\otimes}_{\mathrm{W}(\mathbb{F})}\, \Lambda$ appartient à $\widehat{\mathcal{C}}_\Lambda$. Par définition, le complété $R \,\widehat{\otimes}_{\mathrm{W}(\mathbb{F})}\, \Lambda$ est la limite

$$\varprojlim_j \left(R \otimes_{\mathrm{W}(\mathbb{F})} \Lambda\right)/m^j,$$

avec $m := m_R \otimes_{\mathrm{W}(\mathbb{F})} \Lambda + R \otimes_{\mathrm{W}(\mathbb{F})} m_\Lambda$. De cette façon, on a bien $\left(R \,\widehat{\otimes}_{\mathrm{W}(\mathbb{F})}\, \Lambda\right) \in \widehat{\mathcal{C}}$, son idéal maximal étant la clôture de m.

Dans la suite, nous allons nous poser la question de la représentabilité de foncteurs

$$F : \widehat{\mathcal{C}} \longrightarrow \mathrm{Ens},$$

où Ens désigne la catégorie des ensembles. Être représentable pour un tel foncteur est lié à la propriété (dite de Mayer-Vietoris) de conservation du produit fibré. Pour pouvoir parler de produit fibré, il faut se placer dans une sous-catégorie de $\widehat{\mathcal{C}}$ comme le suggère l'exemple suivant.

Exemple 1.1.5. — Cet exemple dû à Conrad ([Maz 2] p.270) montre que $\widehat{\mathcal{C}}$ n'est pas stable par produit fibré. Considérons le produit

$$R = \mathbb{F}[[X,Y]] \times_{\mathbb{F}[[X]]} \mathbb{F},$$

où l'application $\mathbb{F} \to \mathbb{F}[[X]]$ est le morphisme naturel (et le seul possible) et l'autre application est définie par $Y \mapsto 0$. On peut voir R comme le sous-anneau

$$\{a + YP(X,Y) \mid a \in \mathbb{F} \text{ et } P \in \mathbb{F}[[X,Y]]\}$$

de $\mathbb{F}[[X,Y]]$ avec pour idéal maximal $m_R = (Y)$. Par conséquent $\dim_{\mathbb{F}} m_R/m_R^2$ est infinie et R n'est pas Noetherien, où m_R désigne l'idéal maximal de R.

1.1.1.2. Anneaux d'Artin, petite surjection. — La sous-catégorie de $\widehat{\mathcal{C}}$ formé des anneaux d'Artin est stable par produit fibré et les surjections entre deux anneaux d'Artin se factorisent grâce aux "petites surjections". C'est ce que nous présentons dans cette sous-section.

Définition 1.1.6. — On note $\mathcal{C}$ la catégorie des anneaux locaux (A, m_A) Artiniens, complets et munis d'un isomorphisme $A/m_A \simeq \mathbb{F}$. Les morphismes entre de tels anneaux sont des morphismes continus d'anneaux locaux qui induisent l'identité sur les corps résiduels.

Remarque 1.1.7. — 1) Tout idéal propre d'un anneau $A \in \mathcal{C}$ est nilpotent.
2) Lorsque $R \in \widehat{\mathcal{C}}$, on a vu dans la remarque 1.1.1 que R est homéomorphe à la limite projective de ses quotients R/m_R^n. Chaque quotient R/m_R^n appartient à $\mathcal{C}$.
3) Dire que A est Artinien équivaut à dire que A est Noetherien et $\dim\mathrm{Krull} A = 0$. Dans la suite, la dimension de Krull du quotient R/pR jouera un rôle important, lorsque $R \in \widehat{\mathcal{C}}$.

Cette catégorie $\mathcal{C}$ (qui est une sous-catégorie pleine de $\widehat{\mathcal{C}}$) est stable par produit fibré :

Lemme 1.1.8. — *Soit $A, B, C \in \mathcal{C}$ et soit $a : A \to C$ et $b : B \to C$ deux morphismes. Alors le produit $A \times_C B = \{(x,y) \in A \times B \mid a(x) = b(y)\}$ appartient à $\mathcal{C}$.*

Pour étudier une surjection entre deux anneaux de $\mathcal{C}$, on peut se limiter à étudier des petites surjections. C'est l'objet du lemme qui suit la définition :

Définition 1.1.9. — On appelle petite surjection $R \twoheadrightarrow S$ entre deux anneaux de $\widehat{\mathcal{C}}$ une surjection dont le noyau est un idéal principal (t) tel que $(t) \cdot m_R = (0)$.

Lemme 1.1.10. — *Soit $s : A \twoheadrightarrow B$ une surjection entre deux anneaux de $\mathcal{C}$. Alors la surjection s est la composée d'un nombre fini de petites surjections.*

Démonstration. — C'est de l'algèbre commutative élémentaire. On se donne $s : A \to A/I$ la surjection canonique avec I un idéal de A. Comme A est Noetherien, l'idéal I est engendré par un nombre fini d'éléments $(x_1, \ldots, x_n)$. Quitte à factoriser s par les quotients successifs $A \to A/(x_1) \to \ldots \to A/I$, on peut supposer I principal engendré par un élément noté x. Comme A est un anneau d'Artin, tous les idéaux propres sont nilpotents. Quitte à factoriser $A \to A/(x)$ par les quotients $A/(x)^i$, on peut supposer que $x^2 = 0$. L'idéal maximal m_A de A est engendré par un nombre fini d'éléments $(m_1, \ldots, m_g)$ et il existe un entier α tel que $m_A^\alpha = (0)$. La factorisation $A \to A/(xm_1^{\alpha-1}) \to A/(xm_1^{\alpha-1}, xm_2^{\alpha-1}) \to \ldots \to A/(x)$ permet de conclure. □

1.1.2. Continuité. — Remarquons que $\mathrm{W}(\mathbb{F}) \notin \mathcal{C}$. On souhaite pouvoir travailler avec des anneaux de $\widehat{\mathcal{C}}$. Dans la pratique, nous allons soit définir des foncteurs sur $\mathcal{C}$ et les étendre par continuité à $\widehat{\mathcal{C}}$, soit les définir sur $\widehat{\mathcal{C}}$ et vérifier qu'ils sont continus. On rappelle que l'idéal maximal de chaque anneau de $\mathcal{C}$ est nilpotent, et donc chaque foncteur $F : \mathcal{C} \to \mathrm{Ens}$ vérifie $F(A) = \varprojlim_n F(A/m_A^n)$, où $A \in \mathcal{C}$.

Définition 1.1.11. — 1) On étend un foncteur $F : \mathcal{C} \to \mathrm{Ens}$ par continuité en posant

$$F(R) = \varprojlim_n F(R/m_R^n), \text{ pour chaque } R \in \widehat{\mathcal{C}}.$$

2) On dit qu'un foncteur $F : \widehat{\mathcal{C}} \to \mathrm{Ens}$ est continu lorsque pour chaque $R \in \widehat{\mathcal{C}}$ le morphisme naturel

$$F(R) \to \varprojlim F(R/m_R^n) \text{ est bijectif.}$$

Un tel foncteur est donc déterminé par sa restriction à $\mathcal{C}$.

Il est bien connu que la limite projective commute avec le foncteur $\mathrm{Hom}(A, -)$, i.e. $\mathrm{Hom}(A, \varprojlim_i B_i) \simeq \varprojlim_i \mathrm{Hom}(A, B_i)$, avec A, B_i des anneaux commutatifs. En particulier, on a :

Lemme 1.1.12. — *Soit $R \in \widehat{\mathcal{C}}$. Alors le foncteur* $\mathrm{Hom}(R, -) : \widehat{\mathcal{C}} \to \mathrm{Ens}$ *est continu.*

Cette propriété de $\mathrm{Hom}(R, -)$ montre que les foncteurs représentables, définis dans la sous-section suivante, sont nécessairement continus.

1.1.3. Foncteur représentable. — Parmi les foncteurs $F : \mathcal{C} \to \mathrm{Ens}$ ou $F : \widehat{\mathcal{C}} \to \mathrm{Ens}$, on va s'intéresser à ceux qui sont (pro-)représentables, i.e. de la forme $\mathrm{Hom}(R, -)$ pour un $R \in \mathcal{C}$ ou $\widehat{\mathcal{C}}$. Enonçons la définition :

Définition 1.1.13. — 1) On dit d'un foncteur $F : \widehat{\mathcal{C}} \to \text{Ens}$ qu'il est représentable lorsqu'il existe $R \in \widehat{\mathcal{C}}$ tel qu'il existe un isomorphisme fonctoriel

$$F \simeq \text{Hom}(R, -).$$

De façon équivalente, dire que F est représentable signifie qu'il existe un couple (R, ρ) vérifiant :
(i) $R \in \widehat{\mathcal{C}}$ et $\rho \in F(R)$,
(ii) Pour tout $S \in \widehat{\mathcal{C}}$ et tout $\rho_S \in F(S)$, il existe un unique morphisme $r : R \to S$ tel que $F(r)$ applique ρ sur ρ_S.

2) On dit que $F : \mathcal{C} \to \text{Ens}$ est pro-représentable lorsqu'il existe $R \in \widehat{\mathcal{C}}$ tel que

$$F \simeq \text{Hom}(R, -).$$

1.1.4. Espace tangent. — Par la suite, on dit que

$$\mathbb{F}[\varepsilon] := \mathbb{F}[X]/(X^2) \text{ est l'anneau des nombres duaux de } \mathbb{F}.$$

L'anneau $\mathbb{F}[\varepsilon]$ est un $\mathbb{F}$-espace vectoriel de base $\{1, \varepsilon\}$, on écrit ses éléments sous la forme $x + y\varepsilon$ dans cette base, avec $x, y \in \mathbb{F}$.

Définition 1.1.14. — On dit que $F(\mathbb{F}[\varepsilon])$ est l'espace tangent du foncteur $F : \widehat{\mathcal{C}} \to \text{Ens}$.

Cette définition est motivée par le lemme suivant.

Lemme 1.1.15 **([Maz 2], Prop. p.271)**. — *Soit $R \in \widehat{\mathcal{C}}$. Il existe un isomorphisme naturel de $\mathbb{F}$-espaces vectoriels :*

$$t_R \simeq \text{Hom}(R, \mathbb{F}[\varepsilon]).$$

L'espace tangent du foncteur $\text{Hom}(R, -)$ est ainsi isomorphe en tant que $\mathbb{F}$-espace vectoriel à t_R. On souhaite munir d'une structure de $\mathbb{F}$-espace vectoriel l'espace tangent d'un foncteur. Pour cela, considérons les deux morphismes suivants :

$$\text{a} : \begin{cases} \mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon] \longrightarrow \mathbb{F}[\varepsilon] \\ (x + y\varepsilon, x + z\varepsilon) \mapsto x + (y + z)\varepsilon \end{cases}$$

et

$$\text{m}_\lambda : \begin{cases} \mathbb{F}[\varepsilon] \longrightarrow \mathbb{F}[\varepsilon] \\ x + y\varepsilon \mapsto x + (\lambda y)\varepsilon \end{cases}, \text{ où } \lambda \in \mathbb{F}.$$

On énonce une condition suffisante pour que $F(\mathbb{F}[\varepsilon])$ soit un espace vectoriel pour les lois induites par l'addition a et par la mutliplication m_λ par un scalaire.

Proposition 1.1.16 **([Sc], Lem.2.10.)**. — *Soit $F : \mathcal{C} \to \text{Ens}$ un foncteur tel que $F(\mathbb{F})$ soit réduit à un élément. Supposons que l'application naturelle suivante soit une bijection :*

$$\text{s}_\varepsilon : F(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]) \longrightarrow F(\mathbb{F}[\varepsilon]) \times F(\mathbb{F}[\varepsilon]).$$

Alors l'espace tangent $F(\mathbb{F}[\varepsilon])$ possède une structure de $\mathbb{F}$-espace vectoriel où l'addition et la multiplication (par $\lambda \in \mathbb{F}$) sont respectivement données par :

$$F(\mathbb{F}[\varepsilon]) \times F(\mathbb{F}[\varepsilon]) \xrightarrow{s_\varepsilon^{-1}} F(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]) \xrightarrow{F(\text{a})} F(\mathbb{F}[\varepsilon]) \quad \textit{et} \quad F(\mathbb{F}[\varepsilon]) \xrightarrow{F(\text{m}_\lambda)} F(\mathbb{F}[\varepsilon]) \ .$$

Si F est représentable, son espace tangent est un $\mathbb{F}$-espace vectoriel. On veut s'assurer en particulier que $\mathrm{s}_\varepsilon : F(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]) \longrightarrow F(\mathbb{F}[\varepsilon]) \times F(\mathbb{F}[\varepsilon])$ est bijective. Cela est précisé dans la section suivante (cf. propriété *H2* à venir).

1.2. Critère de Schlessinger

On énonce le critère de Schlessinger dans deux cas : lorsque le foncteur $F : \mathcal{C} \to \mathrm{Ens}$ est pro-représentable et lorsque F n'est pas pro-représentable, mais très proche de l'être. Dans le premier cas, on peut associer à F un anneau $R \in \widehat{\mathcal{C}}$ qui est unique à unique isomorphisme près, on parle d'anneau universel pour F. Dans le second cas, on attache également un anneau $R \in \widehat{\mathcal{C}}$ à F qui est unique mais pas à unique isomorphisme près, on parle d'anneau versel pour F.

1.2.1. Version universelle. — Ce critère s'énonce de la façon suivante.

Théorème 1.2.1 **([Sc], Th.2.11)**. — *Soit $F : \mathcal{C} \longrightarrow \mathrm{Ens}$ un foncteur. On suppose que $F(\mathbb{F})$ est réduit à un élément. Soient $a : A \to C$ et $b : B \to C$ deux morphismes dans $\mathcal{C}$. On note*

$$\mathrm{s} : \ F(A \times_C B) \to F(A) \times_{F(C)} F(B) \text{ l'application naturelle déduite des projections.}$$

Alors F est pro-représentable si et seulement si F satisfait les propriétés ci-dessous :

H1. L'application s *est surjective dès que $b : B \to C$ est une petite surjection.*
H2. L'application s *est bijective dès que $C = \mathbb{F}$ et $B = \mathbb{F}[\varepsilon]$.*
H3. L'espace tangent de F est de dimension finie : $\dim_{\mathbb{F}} F(\mathbb{F}[\varepsilon]) < \infty$.
H4. L'application s *est bijective dès que $A = B$, $a = b$ et $a : A \to C$ est une petite surjection.*

Les vérifications à effectuer pour utiliser le théorème ci-dessus reposent sur des petites surjections et sur l'espace tangent de F. D'après la proposition 1.1.16, l'hypothèse *H2* implique que l'espace tangent de F est un $\mathbb{F}$-espace vectoriel. Cela rend légitime la formulation de *H3*. Cette propriété *H3* assure que l'anneau qui représente F est bien Noetherien.

1.2.2. Version verselle. — Dans la sous-section précédente, une caractérisation est donnée pour les foncteurs $\mathcal{C} \to \mathrm{Ens}$ pro-représentables. Ici, on s'intéresse à des foncteurs qui sont assez proches des foncteurs représentables, i.e. qui possèdent un pro-hull (R, r) selon le vocable utilisé dans [Sc]. Pour de tels foncteurs F, on dispose d'un morphisme $\mathrm{Hom}(R, -) \to F$ (avec $R \in \widehat{\mathcal{C}}$) dit lisse. Mais à la différence du cas où le foncteur est représentable, on ne sait pas si le couple (R, r) est unique à isomorphisme unique près. C'est ce qui explique le titre de cette sous-section, l'objet (R, r) est dit versel pour F dans le cas où c'est un pro-hull de F. Commençons par définir la notion de morphisme lisse entre deux foncteurs et celle de "hull".

1.2.2.1. Morphisme lisse et hull. — On fixe deux foncteurs $F, G : \mathcal{C} \to \mathrm{Ens}$ tels que $F(\mathbb{F})$ et $G(\mathbb{F})$ soient réduits à un élément. On prolonge par continuité ces deux foncteurs à $\widehat{\mathcal{C}}$.

Définition 1.2.2. — On dit qu'un morphisme $F \to G$ est lisse lorsque pour toute surjection $A \twoheadrightarrow B$ dans $\mathcal{C}$, l'application naturelle suivante est surjective :

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

Remarque 1.2.3. — On peut reformuler cette définition de la façon suivante :
f : $F \to G$ est lisse lorsque pour toute surjection $A \twoheadrightarrow B$ dans $\mathcal{C}$, pour tout élément $b_1 \in F(B)$ et tout rélèvement a_2 de $b_2 = \mathrm{f}(B)(b_1)$ dans $G(A)$, il existe $a_1 \in F(A)$ tel que $\mathrm{f}(A)(a_1) = a_2$ et tel que a_1 soit un relèvement de b_1.

Voyons ce que signifie être lisse dans le cas simple où les deux foncteurs sont représentables :

Proposition 1.2.4 **([Sc], Prop.2.5)**. — *Soit $R \to S$ un morphisme d'éléments de $\widehat{\mathcal{C}}$. Alors* $\mathrm{Hom}(S, -) \to \mathrm{Hom}(R, -)$ *est lisse si et seulement si S est un anneau de séries formelles sur R.*
On dit alors que S est lisse sur R (ou relativement à R).

Dans la catégorie $\widehat{\mathcal{C}}$, dire que $R \to S$ est lisse revient à dire que S est un anneau de séries formelles sur R. On a donc étendu cette notion au niveau des morphismes de foncteurs.
La définition suivante formalise la notion d'être proche d'un foncteur représentable.

Définition 1.2.5. — On dit d'un couple (R, r) qu'il est un pro-hull pour le foncteur F si $R \in \widehat{\mathcal{C}}$ et si $r : \mathrm{Hom}(R, -) \to F$ est un morphisme de foncteurs qui est lisse et tel que l'application induite $t_R \to F(\mathbb{F}[\varepsilon])$ soit une bijection.

Remarque 1.2.6. — 1) Bien entendu, si F est pro-représentable par (R, r), alors ce couple est un pro-hull pour F.
2) Soit $S \twoheadrightarrow \mathbb{F}$ la réduction modulo m_S, avec $S \in \widehat{\mathcal{C}}$. Si (R, r) est un pro-hull pour F, alors l'application induite $\mathrm{Hom}(R, S) \to \mathrm{Hom}(R, \mathbb{F}) \times_{F(\mathbb{F})} F(S)$ est surjective. Dès que $F(S)$ est non-vide, on dispose donc d'une application (non-canonique) $R \to S$.

La question de l'unicité du pro-hull de F se pose, c'est l'objet de la proposition suivante.

Proposition 1.2.7 **([Sc], Prop.2.9)**. — *Soient (R, r) et (S, s) deux pro-hulls pour F. Alors il existe un isomorphisme $u : R \to S$ tel que $s = r \circ u^*$, où u^* est l'application* $\mathrm{Hom}(S, -) \to \mathrm{Hom}(R, -)$ *induite par u.*

La caractéristique du pro-hull R possède un véritable intérêt dans le cadre galoisien. En restant vague, si une représentation continue du groupe de Galois absolu de $\mathbb{Q}$ à valeurs dans $\mathrm{GL}_2(\mathbb{F}_p)$ possède certaines propriétés dites de modularités, on s'attend à ce que cette représentation possède un relèvement à $\mathrm{GL}_2(\mathbb{Z}_p)$, par exemple. C'est dans cet esprit que nous donnons la proposition suivante.

Proposition 1.2.8 **([Sc], Rem.2.10)**. — *Soit (R, r) un pro-hull pour F. Alors les deux points suivants sont équivalents :*
1) R est un anneau de séries formelles sur $\mathrm{W}(\mathbb{F})$.
2) Si $A \to B$ est surjective dans $\mathcal{C}$, alors $F(A) \to F(B)$ est surjective.

1.2.2.2. Critère de Schlessinger dans le cas versel. — On peut énoncer la version suivante du critère de Schlessinger.

Théorème 1.2.9 **([Sc], Th.2.11)**. — *Soit $F : \mathcal{C} \longrightarrow$ Ens un foncteur tel que $F(\mathbb{F})$ soit réduit à un élément. Soient $a : A \to C$ et $b : B \to C$ deux morphismes dans $\mathcal{C}$. On note*

$$\mathrm{s}: \ F(A \times_C B) \to F(A) \times_{F(C)} F(B) \text{ l'application naturelle déduite des projections.}$$

Alors F possède un pro-hull si et seulement si F satisfait les propriétés H1, H2 et H3 (du théorème 1.2.1).

Remarque 1.2.10. — 1) On peut trouver dans [Sc] l'isomorphisme canonique

$$F(R) \simeq \mathrm{Hom}(\mathrm{Hom}(R, -), F),$$

où $R \in \widehat{\mathcal{C}}$ et F est vu comme un foncteur $\mathcal{C} \to$ Ens dans le membre de droite. On a utilisé cette identification (du type Yoneda) pour énoncer la définition et la proposition précédente ; dans [Sc], l'élément r ci-dessus est vu dans $F(R)$.

2) Dans la preuve de la proposition ci-dessus, on exhibe deux morphismes $u : R \to S$ et $v : S \to R$ tels que $u \circ v$ induise un automorphisme de t_S, ainsi $u \circ v$ est surjectif (d'après le lemme 1.1.3). On sait enfin que que $u \circ v$ est bijectif car S est Noetherien.

1.3. Le critère de Schlessinger revu par Mazur

Soit $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ une représentation continue du groupe profini Π. On souhaite étudier des (classes de) relèvements de $\bar{\rho}$ et pouvoir les paramétrer par un anneau universel (ou versel selon les cas). Le problème est posé en termes fonctoriels à l'aide de $\mathbf{Def}^{\square}(\bar{\rho})$ et $\mathbf{Def}(\bar{\rho})$ (cf. la définition 1.3.2 à venir).
Mazur applique le critère de Schlessinger (version universelle ou verselle) avec $\mathbf{Def}(\bar{\rho})$, ce qui donne un anneau de déformation $R(\bar{\rho})$ pour lequel $\mathbf{Def}(\bar{\rho}) \simeq \mathrm{Hom}(R(\bar{\rho}), -)$ (version universelle) ou $\mathrm{Hom}(R(\bar{\rho}), -) \overset{\text{lisse}}{\longrightarrow} \mathbf{Def}(\bar{\rho})$ (version verselle). On donne ensuite des exemples simples en déformant des caractères de groupes de Galois dans le cas des corps locaux et des corps de nombres. Enfin, on rappelle la minoration de la dimension de Krull des quotients $R(\bar{\rho})/pR(\bar{\rho})$ obtenue grâce aux espaces tangents et à la théorie de l'obstruction, i.e. grâce à $H^i(\Pi, \mathrm{Ad}(\bar{\rho}))$, pour $i = 1, 2$ et $\mathrm{Ad}(\bar{\rho})$ la représentation adjointe.

1.3.1. Théorème de Mazur. — Pour chaque anneau $R \in \widehat{\mathcal{C}}$, on dispose de la réduction naturelle $\pi_R : \mathrm{GL}_n(R) \to \mathrm{GL}_n(\mathbb{F})$ modulo m_R. On définit alors le sous-groupe suivant :

$$\Gamma(R) = \ker[\mathrm{GL}_n(R) \xrightarrow{\pi_R} \mathrm{GL}_n(\mathbb{F})] = 1 + m_R \mathrm{M}_n(R).$$

Lemme 1.3.1. — *1) $\Gamma(R)$ est un pro-p-groupe.*
2) $\Gamma(R)$ agit de façon naturelle sur l'ensemble des relèvements $\rho_R : \Pi \to \mathrm{GL}_n(R)$ continus de $\bar{\rho}$ de la façon suivante :

$$\gamma \cdot \rho_R = \gamma \rho_R \gamma^{-1}, \ \textit{avec } \gamma \in \Gamma.$$

Démonstration. — 1) Il suffit de remarquer que le noyau est égal à $1+m_R\mathrm{M}_n(R)$, i.e. à la limite projective $\varprojlim_j 1+\mathrm{M}_n(m_R/m_R^j)$. Une récurrence immédiate montre que les groupes qui définissent cette limite sont des p-groupes. En effet, chacun de ces groupes multiplicatifs est isomorphe au groupe additif $\mathrm{M}_n(m_R/m_R^j)$ qui se dévisse grâce à $\mathrm{M}_n(m_R^{j-1}/m_R^j)$. Or, ce dernier est un $\mathbb{F}$-espace vectoriel, de dimension fini car R est Noetherien.
2) C'est immédiat. □

On définit le foncteur de déformation cadrée $\mathbf{Def}^{\square}(\bar{\rho})$ et le foncteur de déformation $\mathbf{Def}(\bar{\rho})$.

Définition 1.3.2. — Les foncteurs $\mathbf{Def}^{\square}(\bar{\rho}) : \widehat{\mathcal{C}} \longrightarrow \mathrm{Ens}$ et $\mathbf{Def}(\bar{\rho}) : \widehat{\mathcal{C}} \longrightarrow \mathrm{Ens}$ sont définis par :

$$\mathbf{Def}^{\square}(\bar{\rho})(R) = \{\rho_R : \Pi \to \mathrm{GL}_n(R) \text{ morphisme continu tel que } (\rho \mod m_R) = \bar{\rho}\}$$
$$\mathbf{Def}(\bar{\rho})(R) = \mathbf{Def}^{\square}(\bar{\rho})(R)/\Gamma(R).$$

Donnons une autre approche des foncteurs $\mathbf{Def}^{\square}(\bar{\rho})$ et $\mathbf{Def}(\bar{\rho})$.
On note $V_{\mathbb{F}}$ un $\mathbb{F}$-espace vectoriel de dimension n muni d'une action continue de Π. Soit $R \in \widehat{\mathcal{C}}$. On considère les R-modules libres V_R de rang n munis d'une action continue de Π et d'un isomorphisme Π-équivariant $\iota : V_R \otimes \mathbb{F} \simeq V_{\mathbb{F}}$, deux tels modules V_R et V_R' étant équivalents lorsqu'ils sont isomorphes en respectant ι et ι', avec des notation évidentes. Alors, $\mathbf{Def}(\bar{\rho})(R)$ correspond à l'ensemble des classes d'équivalence des V_R.
Pour $\mathbf{Def}^{\square}(\bar{\rho})$, fixons une base $\mathrm{b}_{\mathbb{F}}$ de $V_{\mathbb{F}}$. On considère les couples (V_R, b_R) avec V_R comme ci-dessus et b_R une base du R-module d'image $\mathrm{b}_{\mathbb{F}}$ via ι. Alors $\mathbf{Def}^{\square}(\bar{\rho})(R)$ correspond à l'ensemble des classes d'équivalence des couples (V_R, b_R).

Dans la suite, notre étude porte sur les déformations de $\bar{\rho}$ dont voici la définition.

Définition 1.3.3. — Soit $R \in \widehat{\mathcal{C}}$.
1) On appelle déformation cadrée de $\bar{\rho}$ à R un élément de $\mathbf{Def}^{\square}(\bar{\rho})(R)$. C'est la notion de "framed deformation" de Kisin (c'est de là que vient le $\square$, la base est fixée).
2) On appelle déformation de $\bar{\rho}$ à R un élément ρ_R de $\mathbf{Def}(\bar{\rho})(R)$. On dit aussi que (R, ρ_R) est une déformation de $\bar{\rho}$ à R.

On confondra la plupart du temps une déformation et un de ses représentants.

Remarque 1.3.4. — De façon générale, il est plus simple de montrer une propriété pour $\mathbf{Def}^{\square}(\bar{\rho})$ que pour $\mathbf{Def}(\bar{\rho})$. Pour s'en convaincre, il suffit de comparer la preuve du théorème 1.3.9 avec celle de la proposition 1.3.8.

Chacun des foncteurs $\mathbf{Def}^{\square}(\bar{\rho})$ et $\mathbf{Def}(\bar{\rho})$ est déterminé par sa restriction à $\mathcal{C}$, c'est ce que nous dit la proposition suivante.

Proposition 1.3.5. — *Les foncteurs* $\mathbf{Def}^{\square}(\bar{\rho})$ *et* $\mathbf{Def}(\bar{\rho})$ *sont continus.*

Démonstration. — La preuve pour $\mathbf{Def}^{\square}(\bar{\rho})$ est simple. En effet, il suffit de remarquer que $\mathrm{GL}_n(\varprojlim_i R/m_R^i) \simeq \varprojlim_i \mathrm{GL}_n(R/m_R^i)$ pour conclure à la continuité de $\mathbf{Def}^{\square}(\bar{\rho})$.
Pour la continuité de $\mathbf{Def}(\bar{\rho})$, nous renvoyons à ([Maz 2], §.20, Prop.1). □

Lemme 1.3.6. — *Les propriétés suivantes sont équivalentes :*

1) Le pro-p-complété $\varprojlim_N \Pi/N$ *de* Π *est topologiquement de type fini, où la limite projective est prise sur les sous-groupes fermés* N *distingués, d'indice une puissance finie de* p.
2) L'abélianisé du pro-p-complété de Π *est un* $\mathbb{Z}_p$*-module de type fini.*
3) Le quotient $\Pi/\Pi^p[\Pi,\Pi]$ *est fini, avec* $\Pi^p[\Pi,\Pi]$ *le sous-groupe distingué et fermé engendré par les puissances p-èmes et les commutateurs.*
4) L'ensemble des morphismes continus $\Pi \to \mathbb{F}_p$ *est fini.*

Démonstration. — Les implications $1 \Rightarrow 2 \Rightarrow 3$ sont immédiates. De plus, comme tout morphisme continu $\Pi \to \mathbb{F}_p$ se factorise via $\Pi/\Pi^p[\Pi,\Pi]$, on a l'équivalence entre les points 3 et 4. Enfin, le théorème de la base de Burnside ([Ro]) montre ici que $3 \Rightarrow 1$. □

Définition 1.3.7. — On dit que le groupe Π vérifie l'hypothèse de p-finitude lorsque tout sous-groupe ouvert de Π vérifie une des propriétés équivalentes du lemme ci-dessus.

Proposition 1.3.8 ([Ki 2]). — *Soit* $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ *une représentation continue d'un groupe profini* Π *qui vérifie l'hypothèse de p-finitude. Alors le foncteur* $\boldsymbol{Def}^{\square}(\bar{\rho})$ *est représentable.*

Démonstration. — On note $H = \ker(\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F}))$. Chaque relèvement $\rho_R : \Pi \to \mathrm{GL}_n(R)$ de $\bar{\rho}$ voit sa restriction $\rho_{R|H}$ prendre ses valeurs dans le pro-p-groupe (cf. lemme 1.3.1) $\Gamma(R)$. Ainsi $\rho_{R|H}$ se factorise à travers le pro-p-quotient maximal de H. Notons H' le sous-groupe distingué dans H tel que H/H' soit ce pro-p-quotient maximal. On peut voir H' comme l'intersection des noyaux $\ker(\rho_R)_{|H}$, avec R parcourant $\widehat{\mathcal{C}}$ et ρ_R parcourant les relèvements de $\bar{\rho}$ à R. Le groupe H' est donc distingué dans Π. L'hypothèse de p-finitude assure que H/H' est topologiquement de type fini et il en est de même pour G/H', car G/H est fini. Notons $x_1, \ldots, x_s$ les générateurs topologiques de G/H'. Alors $\mathbf{Def}^{\square}(\bar{\rho})$ est représentable par un quotient de $\mathrm{W}(\mathbb{F})[[X_{i,j,k}]]$ avec les entiers $i \in [1,s]$ et $j,k \in [1,n^2]$. □

On énonce le résultat principal concernant $\mathbf{Def}(\bar{\rho})$.

Théorème 1.3.9 ([Maz 1], **Prop.1**). — *Soit* $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ *une représentation continue d'un groupe profini* Π *qui vérifie l'hypothèse de p-finitude.*
1) Alors le foncteur $\boldsymbol{Def}(\bar{\rho})$ *possède un pro-hull, noté* $(R(\bar{\rho}), \boldsymbol{\rho})$ *et appelé déformation verselle de* $\bar{\rho}$.
2) Si de plus le commutant $\mathrm{C}(\bar{\rho}) = \mathbb{F}$*, alors* $\boldsymbol{Def}(\bar{\rho})$ *est représentable par l'anneau* $R(\bar{\rho})$. *On dit que* $(R(\bar{\rho}), \boldsymbol{\rho})$ *est la déformation universelle de* $\bar{\rho}$.

Remarque 1.3.10. — D'après la remarque 1.2.6, le premier point du théorème ci-dessus signifie, en particulier, que pour toute déformation (S, ρ_S) de $\bar{\rho}$, il existe un morphisme $R(\bar{\rho}) \to S$, pas nécessairement unique, tel que ρ_S soit induite par $\boldsymbol{\rho}$ via ce morphisme. Le second point du théorème assure l'unicité de $R(\bar{\rho}) \to S$.

Mazur ne donne pas tous les détails de la preuve de ce théorème dans [Maz 1], en particulier les lemmes 1.3.11 et 1.3.14 (cf. ci-dessous) sont juste énoncés. Ces détails sont bien connus et classiques. Cependant, pour le confort du lecteur, nous reproduisons l'intégralité de la preuve avec tous les détails. Enfin, le lemme 1.3.15 est dû à Ramakrishna sous cette forme (cf. [Ra 3]), Mazur utilisait l'hypothèse plus restrictive "$\bar{\rho}$ absolument irréductible" (le lemme de Schur nous dit que $\mathrm{C}(\bar{\rho}) = \mathbb{F}$ dès que $\bar{\rho}$ est absolument irréductible).

Démonstration. — On adopte les notations du théorème 1.2.1 et on s'intéresse donc à l'application naturelle

$$\mathrm{s}: \ \mathbf{Def}(\bar{\rho})(A \times_C B) \to \mathbf{Def}(\bar{\rho})(A) \times_{\mathbf{Def}(\bar{\rho})(C)} \mathbf{Def}(\bar{\rho})(B).$$

Il s'agit de s'assurer que $\mathbf{Def}(\bar{\rho})$ vérifie les propriétés *H1*, *H2*, *H3* (et *H4* lorsque $\mathrm{C}(\bar{\rho}) = \mathbb{F}$).

Lemme 1.3.11. — *Le foncteur $\boldsymbol{Def}(\bar{\rho})$ vérifie la propriété H1.*

Soit $B \twoheadrightarrow C$ une surjection dans $\mathcal{C}$. On note $([\rho_A], [\rho_B])$ un couple de $\mathbf{Def}(\bar{\rho})(A) \times_{\mathbf{Def}(\bar{\rho})(C)} \mathbf{Def}(\bar{\rho})(B)$. On se donne un couple de représentants (ρ_A, ρ_B) de $([\rho_A], [\rho_B])$. Ainsi, il existe une matrice $M \in \Gamma(C)$ telle que $\rho_A = M\rho_B M^{-1}$. Or, $\Gamma(B)$ se surjecte sur $\Gamma(C)$ grâce à l'application naturelle déduite de $B \twoheadrightarrow C$. Notons donc N un relèvement de M dans $\Gamma(B)$. Les représentations $N\rho_B N^{-1}$ et ρ_A ont même image dans $\Gamma(C)$, cela définit donc un élément ρ de $\mathbf{Def}^{\square}(\bar{\rho})(A \times_C B)$. La classe de ρ dans $\mathbf{Def}(\bar{\rho})(A \times_C B)$ est un antécédent de $([\rho_A], [\rho_B])$, ce qui montre la surjectivité. Remarquons au passage que nous n'avons pas besoin de supposer que $B \twoheadrightarrow C$ est une petite surjection.

Lemme 1.3.12. — *Le foncteur $\boldsymbol{Def}(\bar{\rho})$ vérifie la propriété H3.*

Soit ρ un relèvement de $\bar{\rho}$ à $\mathbb{F}[\varepsilon]$. Ce morphisme ρ détermine un morphisme de groupes $h_\rho : \ker \bar{\rho} \to \Gamma(\mathbb{F}[\varepsilon])$ et l'application $\rho \mapsto h_\rho$ est injective. Or $\Gamma(\mathbb{F}[\varepsilon])$ est un espace vectoriel sur $\mathbb{F}$, de dimension finie. Et donc, comme l'hypothèse de p-finitude est vérifiée, il n'y a qu'un nombre fini de morphismes $\ker \bar{\rho} \to \Gamma(\mathbb{F}[\varepsilon])$. Cela montre que $\mathbf{Def}(\bar{\rho})(\mathbb{F}[\varepsilon])$ est de dimension finie.

On note

$$G(\rho_R) = \{\gamma \in \Gamma(R) \mid \gamma\rho_R = \rho_R\gamma\},$$

avec $\rho_R \in \mathbf{Def}(\bar{\rho})(R)$. Par abus, dire que $\gamma\rho_R = \rho_R\gamma$ signifie que $\gamma\rho_R(g) = \rho_R(g)\gamma$, pour tout $g \in \Pi$.

Lemme 1.3.13. — *On rappelle que $B \twoheadrightarrow C$ est fixée.*
Si pour tout $\rho_B \in \boldsymbol{Def}(\bar{\rho})(B)$ d'image $\rho_C \in \boldsymbol{Def}^{\square}(\bar{\rho})(C)$, l'application $G(\rho_B) \to G(\rho_C)$ (induite par $B \twoheadrightarrow C$) est surjective, alors l'application

$$\mathrm{s}: \ \boldsymbol{Def}(\bar{\rho})(A \times_C B) \to \boldsymbol{Def}(\bar{\rho})(A) \times_{\boldsymbol{Def}(\bar{\rho})(C)} \boldsymbol{Def}(\bar{\rho})(B) \text{ est injective.}$$

Soient ρ et ρ' deux éléments de $\mathbf{Def}^{\square}(\bar{\rho})(A \times_C B)$ et soient leurs images respectives (ρ_A, ρ_B) et (ρ'_A, ρ'_B) dans $\mathbf{Def}^{\square}(\bar{\rho})(A) \times_{\mathbf{Def}^{\square}(\bar{\rho})(C)} \mathbf{Def}^{\square}(\bar{\rho})(B)$. On suppose que les couples (ρ_A, ρ_B) et (ρ'_A, ρ'_B) ont la même image dans $\mathbf{Def}(\bar{\rho})(A) \times_{\mathbf{Def}(\bar{\rho})(C)} \mathbf{Def}(\bar{\rho})(B)$. Autrement dit, il existe $(M_A, M_B) \in \Gamma(A) \times \Gamma(B)$ tel que $\rho_A = M_A\rho'_A M_A^{-1}$ et $\rho_B = M_B\rho'_B M_B^{-1}$. Comme ρ_A et ρ_B ont la même image ρ_C dans $\mathbf{Def}^{\square}(\bar{\rho})(C)$, on en déduit que l'image de $M_B^{-1}M_A$ dans $\Gamma(C)$ est un élément M_C de $G(\rho_C)$. On note $N \in G(\rho_B)$ un antécédent de M_C, qui

existe par hypothèse. Les matrices M_A et M_BN ont la même image dans $\Gamma(C)$. Ainsi le couple $(M_A, M_BN) \in \Gamma(A \times_C B)$, ce qui montre que ρ et ρ' ont la même image dans $\mathbf{Def}(\bar{\rho})(A \times_C B)$. L'injectivité est prouvée.

Lemme 1.3.14. — *Le foncteur* $\mathbf{Def}(\bar{\rho})$ *vérifie la propriété H2.*

Soient $C = \mathbb{F}$, $A = B = \mathbb{F}[\varepsilon]$. Il suffit de montrer que s est injective, on va utiliser le lemme précédent. En fait, on a $G(\rho_C) = \{1\}$ et donc $G(\rho_B) \to G(\rho_C)$ est surjective. On peut donc conclure avec le lemme 1.3.13.

Lemme 1.3.15. — *Si on suppose de plus que* $\mathrm{C}(\bar{\rho}) = \mathbb{F}$*, alors le foncteur* $\mathbf{Def}(\bar{\rho})$ *vérifie la propriété H4.*

La preuve de ce dernier lemme demande un peu de soin. Commençons par noter qu'il nous suffit de montrer que pour chaque petite surjection $B \twoheadrightarrow C$, dès que $G(\rho_C)$ est réduit à des homothéties, nécessairement il en va de même pour $G(\rho_B)$, avec ρ_B un relèvement de $\bar{\rho}$ à B et ρ_C son image dans C. En effet, pour chaque anneau $C \in \mathcal{C}$, la réduction naturelle modulo l'idéal maximal $C \to \mathbb{F}$ est la composée de petites surjections et par hypothèse $G(\bar{\rho}) = \{1\}$.

Soit $B \twoheadrightarrow C$ une petite surjection de noyau (t). Notons $\rho_B \in \mathbf{Def}^{\square}(\bar{\rho})(B)$ et ρ_C son image dans $\mathbf{Def}^{\square}(\bar{\rho})(C)$. Supposons que $G(\rho_C)$ est formé uniquement d'homothéties.
Soit $M \in G(\rho_B)$. L'image de M dans $G(\rho_C)$ est une homothétie et donc $M = M_1 + tM_2$, avec $M_1 \in \mathrm{M}_n(B)$ une homothétie et $M_2 \in \mathrm{M}_n(B)$. Comme M commute avec l'image de ρ_B et comme M_1 est une homothétie, on a $t(M_2\rho_B) = t(\rho_B M_2)$. Ici, la seule structure d'anneau ne suffit pas pour conclure puisque t est nilpotent ; on a besoin de voir l'égalité $t(M_2\rho_B) = t(\rho_B M_2)$ en termes d'algèbre linéaire. L'idéal (t) possède une structure naturelle de $\mathbb{F}$-espace vectoriel puisque $t \cdot m_B = (0)$. On a ainsi l'égalité

$$(M_2\rho_B \mod m_B) = (\rho_B M_2 \mod m_B).$$

Enfin, comme $\mathrm{C}(\bar{\rho}) = \mathbb{F}$, la matrice M_2 s'écrit comme la somme d'une homothétie et d'une matrice à coefficients dans m_B et donc $M = M_1 + tM_2$ est une homothétie (encore une fois car $t \cdot m_B = (0)$). □

Remarque 1.3.16. — L'hypothèse de p-finitude implique que l'espace $\mathbf{Def}(\bar{\rho})(\mathbb{F}[\varepsilon])$ est de dimension finie, ce qui implique que l'anneau universel (ou versel) est bien Noetherien. Les autres points de la preuve ne dépendent pas de cette hypothèse de p-finitude.

La théorie du corps de classes global et local donne deux types de groupes qui vérifient l'hypothèse de p-finitude. C'est l'objet de la proposition ci-desssous.

Proposition 1.3.17. — *1) On note* $G_{K,S}$ *le groupe de Galois de l'extension maximale* S*-ramifiée de* K *dans* $\overline{\mathbb{Q}}$*, avec* S *un ensemble fini de places du corps de nombres* $K/\mathbb{Q}$*. Alors* $G_{K,S}$ *vérifie l'hypothèse de p-finitude.*
1) Soit $K_v/\mathbb{Q}_l$ *un corps local, avec* l *un nombre premier. Alors le groupe de Galois absolu de* K_v *vérifie l'hypothèse de p-finitude.*

En conservant les notations de la proposition 1.3.17, on dispose du corollaire suivant.

Corollaire 1.3.18. — *Soit* $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ *une représentation continue et soit* $\Pi = G_{K,S}$ *ou* $\mathrm{Gal}(\overline{K}_v/K_v)$. *Alors le foncteur* $\boldsymbol{Def}(\bar{\rho})$ *possède une déformation (uni)verselle* $(R(\bar{\rho}), \boldsymbol{\rho})$.

1.3.2. Représentations de dimension 1. — D'après la proposition suivante, le twist par un caractère ne change pas le problème de déformation. En particulier, déformer une représentation de dimension 1 revient à déformer le caractère trivial. On donne ensuite la déformation universelle du caractère trivial, en l'illustrant lorsque Π est le groupe de Galois d'un corps local ou $G_{\mathbb{Q},S}$. Enfin, on termine cette sous-section en notant que chaque représentation induit grâce au déterminant une représentation de dimension 1, cela munit chaque anneau de déformation d'une nouvelle structure d'algèbre.

Proposition 1.3.19 **([Maz 1], §.1.2, Prop.1)**. — *Soit* $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ *continue telle que* $\mathrm{C}(\bar{\rho}) = \mathbb{F}$ *et soit* $\bar{\rho}' \simeq \chi \otimes \bar{\rho}$ *une représentation isomorphe au twist de* $\bar{\rho}$ *par le caractère* $\chi : \Pi \to \mathbb{F}^\times$.
Alors les anneaux de déformation universels de $\bar{\rho}$ *et* $\bar{\rho}'$ *sont isomorphes :*

$$R(\rho) \simeq R(\bar{\rho}').$$

1.3.2.1. La déformation universelle explicitée. — La proposition ci-dessus montre qu'une représentation $\bar{\rho} : \Pi \to \mathrm{GL}_1(\mathbb{F})$ de dimension 1 possède un anneau de déformation universel $R(\bar{\rho})$ ne dépendant que de Π et de $\mathbb{F}$; on propose de décrire l'anneau $R(\bar{\rho})$ et la déformation universelle de $\bar{\rho}$.
Le problème se ramène à déformer l'abélianisé de Π. Il faut considérer la partie première à p qui se traite grâce au Teichmüller et la partie en p qui se traite grâce à l'algèbre complétée de l'abélianisé du pro-p-complété de Π.
On note

$$[\bar{\rho}] : \Pi \to \mathrm{GL}_1(\mathrm{W}(\mathbb{F})) \text{ le relèvement de Teichmüller de } \bar{\rho}.$$

On définit Γ comme $\Pi^{ab,(p)} := \varprojlim_N \Pi^{ab}/N$, où N parcourt les sous-groupes fermés d'indice une puissance (finie) de p dans Π^{ab}. On note $\gamma : \Pi \twoheadrightarrow \Gamma$ la surjection canonique.
Notons l'algèbre complétée

$$\mathrm{W}(\mathbb{F})[[\Gamma]] := \varprojlim \mathrm{W}(\mathbb{F})[\Gamma/H],$$

où H parcourt les sous-groupes ouverts de Γ. On sait que Γ est un $\mathbb{Z}_p$-module de type fini (Π vérifie l'hypothèse de p-finitude), de rang noté r ; soit $(\gamma_1, \ldots, \gamma_r)$ un système de générateurs. L'algèbre $\mathrm{W}(\mathbb{F})[[\Gamma]]$ appartient à $\widehat{\mathcal{C}}$, c'est un quotient de $\mathrm{W}(\mathbb{F})[[X_1, \ldots, X_r]]$, où les éléments de torsion de Γ induisent l'idéal qui détermine ce quotient. On note encore

$$[\bar{\rho}] : \Pi \to (\mathrm{W}(\mathbb{F})[[\Gamma]])^\times$$

l'application déduite de $[\bar{\rho}]$ par le morphisme naturel $\mathrm{W}(\mathbb{F}) \to \mathrm{W}(\mathbb{F})[[\Gamma]]$.
Par ailleurs, il y a une injection naturelle $\Gamma \hookrightarrow \mathrm{W}(\mathbb{F})[[\Gamma]]^\times$ (construite par exemple grâce à $\gamma_i \mapsto 1 + X_i$) que l'on compose avec $\gamma : \Pi \to \Gamma$ pour obtenir l'application notée :

$$\lambda : \Pi \to (\mathrm{W}(\mathbb{F})[[\Gamma]])^\times .$$

On fait le bilan de ces observations dans la proposition suivante.

Proposition 1.3.20. — *L'anneau de déformation universelle de $\bar{\rho}$ est*

$$R(\bar{\rho}) \simeq \mathrm{W}(\mathbb{F})[[\Gamma]]$$

et la déformation universelle est donnée par :

$$\boldsymbol{\rho} : x \mapsto [\bar{\rho}](x) \cdot \lambda(x).$$

Démonstration. — Cette preuve est formelle. Il s'agit de montrer que le couple proposé est bien la déformation universelle de $\bar{\rho}$. Soit $\rho_S \in \mathbf{Def}^{\square}(\bar{\rho})(S)$, avec $S \in \widehat{\mathcal{C}}$. Comme le caractère $[\rho]^{-1}\rho_S$ prend ses valeurs dans le pro-p-groupe abélien $1 + m_S$ (où par abus on note encore $[\bar{\rho}] : \Pi \to S^{\times}$ le caractère obtenu comme composé du Teichmüller avec le morphisme naturel $\mathrm{W}(\mathbb{F}) \to S$), il se factorise à travers Γ et il en ressort un morphisme continu $\Gamma \to 1 + m_S$ donnant naissance à un morphisme d'algèbres $\mathrm{W}(\mathbb{F})[[\Gamma]] \to S$ qui transforme $\boldsymbol{\rho}$ en ρ_S. □

***Exemple 1.3.21* (Cas local)**. — Soit l un nombre premier et soit $K_v/\mathbb{Q}_l$ une extension finie de degré d. On note G_v le groupe de Galois absolu de K_v et q_v le cardinal du corps résiduel de K_v. On note encore α_v la plus grande puissance de p qui divise $q_v - 1$. Par la théorie du corps de classes, on sait que :

1) si $l \neq p$, alors $G_v^{ab,(p)} \simeq \mathbb{Z}_p \times \mu_{p^{\alpha_v}}$ si $q_v \equiv 1 \mod p$ et $G_v^{ab,(p)} \simeq \mathbb{Z}_p$ sinon.
2) si $l = p$, alors $G_v^{ab,(p)} \simeq \mathbb{Z}_p^{d+1} \times \mu_{p^\infty}(K_v)$, où $\mu_{p^\infty}(K_v)$ désigne les racines de l'unité dans K_v d'ordre une puissance de p. On note n le plus grand entier tel que $\mu_{p^n} \subseteq K_v$.

Ainsi, l'anneau de déformation universel $R(\bar{\rho})$ d'un caractère de G_v vérifie :

$$R(\bar{\rho}) \simeq \begin{cases} \mathrm{W}(\mathbb{F})[[X,Y]]/\left((1+Y)^{p^{\alpha_v}} - 1\right) & \text{si } l \neq p, \\ \mathrm{W}(\mathbb{F})[[X_1, \ldots, X_{d+1}, Y]]/\left((1+Y)^{p^n} - 1\right) & \text{si } l = p. \end{cases}$$

***Exemple 1.3.22* (Cas global)**. — Soit $p \geq 3$. On rappelle que $G_{\mathbb{Q},S}$ désigne le groupe de Galois de l'extension maximale de $\mathbb{Q}$ non-ramifiée hors de S. Par la théorie du corps de classes, on a $G_{\mathbb{Q},S}^{ab} \simeq \prod_{l \in S} \mathbb{Z}_l^{\times}$. On note I l'ensemble des premiers l de S qui vérifient $l \equiv 1 \mod p$; on confond un élément $l_i \in I$ et son indice i. On suppose que $p \in S$ (si ce n'est pas le cas, il suffit de ne pas faire figurer la variable T dans ce qui suit). Alors

$$R(\bar{\rho}) \simeq \mathrm{W}(\mathbb{F})[[X_i, T \mid i \in I]]/\left(\{(1+X_i)^{p^{\alpha_i}} - 1\}_{i \in I}\right),$$

où α_i désigne la plus grande puissance de p qui divise $l_i - 1$.

1.3.2.2. Le déterminant. — Soit $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ continue. La représentation

$$\det(\bar{\rho}) : \Pi \to \mathbb{F}^{\times}$$

possède une déformation universelle, notée (Λ, δ). Chaque déformation (R, ρ_R) de $\bar{\rho}$ induit une déformation de $\det(\bar{\rho})$, et donc par universalité, il existe une application naturelle $\Lambda \to R$ munissant ainsi R d'une structure de Λ-algèbre. Le problème de déformation de $\bar{\rho}$ peut être restreint à cette catégorie d'anneaux munis d'une structure d'algèbre supplémentaire. La proposition suivante présente ce cas.

Proposition 1.3.23 **([Maz 2], §.12)**. — *Soit* $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ *continue et telle que* $\mathrm{C}(\bar{\rho}) = \mathbb{F}$. *Soit* $\Lambda \in \widehat{\mathcal{C}}$. *Soit* $\widehat{\mathcal{C}}_\Lambda$ *la sous-catégorie de* $\widehat{\mathcal{C}}$ *formée des anneaux* R *munis d'une structure de* Λ*-algèbre donnée par un morphisme naturel* $\Lambda \to R$. *On note* $\boldsymbol{Def}(\bar{\rho})_\Lambda$ *le foncteur qui associe à chaque* $R \in \widehat{\mathcal{C}}_\Lambda$ *les déformations de* $\bar{\rho}$ *à* R. *Alors* $\boldsymbol{Def}(\bar{\rho})_\Lambda$ *est représentable par*

$$R(\bar{\rho}) \ \widehat{\otimes}_{\mathrm{W}(\mathbb{F})} \ \Lambda.$$

1.3.3. Espace tangent et obstruction. — On note $\mathrm{Ad}(\bar{\rho})$ la représentation adjointe de la représentation $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$, i.e. l'espace $\mathrm{M}_n(\mathbb{F})$ muni de l'action de GL_n par conjugaison via $\bar{\rho}$. Dans cette sous-section, on propose un survol de la théorie de l'obstruction et des espaces tangents dans le cadre des déformations. On termine avec des exemples de minoration des dimensions de Krull des anneaux de déformations provenant de représentations de $G_{K,S}$ (conséquence de la minoration de Mazur interprétée à l'aide de Poitou-Tate) et de groupes de Galois de corps locaux (exemples obtenus par Ramakrishna).

1.3.3.1. Le premier groupe de cohomologie. — Soit $\delta : \Pi \to \mathrm{GL}_n(\mathbb{F}[\varepsilon])$ une application qui relève $\bar{\rho}$, mais δ n'est pas un morphisme a priori.
Remarquons que le groupe $\mathrm{GL}_n(\mathbb{F})$ s'injecte de manière naturelle dans $\mathrm{GL}_n(\mathbb{F}[\varepsilon])$. On écrit δ sous la forme suivante : $\delta(g) = (1 + \varepsilon c(g))\bar{\rho}(g)$.
Formons alors

$$b(g,h) = \delta(gh)\delta(h)^{-1}\delta(g)^{-1}, \text{ avec } g, h \in \Pi.$$

L'application b mesure l'obstruction à ce que δ soit un morphisme de groupes. L'inverse de la matrice $1 + \varepsilon c(g)$ étant $1 - \varepsilon c(g)$, un calcul immédiat donne

$$b(g,h) = 1 - \varepsilon \left(\bar{\rho}(g)c(h)\bar{\rho}(g)^{-1} - c(gh) + c(g)\right).$$

Ainsi, δ est un morphisme de groupe si et seulement si l'application $c : \Pi \to \mathrm{Ad}(\bar{\rho})$ est un 1-cocycle. La correspondance linéaire $\varphi : \delta \mapsto c$ est donc une bijection entre l'espace tangent de $\mathbf{Def}^{\square}(\bar{\rho})$ et l'espace des 1-cocycles $Z^1(\Pi, \mathrm{Ad}(\bar{\rho}))$. Les images de δ et de δ' par φ diffèrent d'un 1-cobord si et seulement si $\delta' = M\delta M^{-1}$, avec $M \in \Gamma(\mathbb{F}[\varepsilon])$. On peut alors énoncer la proposition suivante, dont on vient de prouver le premier point.

Proposition 1.3.24 **([Maz 2], §.21, Prop.1)**. — *On désigne l'espace des* 1*-cocycles de* Π *dans* $\mathrm{Ad}(\bar{\rho})$ *par* $Z^1(\Pi, \mathrm{Ad}(\bar{\rho}))$.
1) Il y a un isomorphisme canonique entre les $\mathbb{F}$*-espaces vectoriels suivants*

$$\boldsymbol{Def}^{\square}(\bar{\rho})(\mathbb{F}[\varepsilon]) \simeq Z^1(\Pi, \mathrm{Ad}(\bar{\rho})) \quad \textit{et} \quad \boldsymbol{Def}(\bar{\rho})(\mathbb{F}[\varepsilon]) \simeq H^1(\Pi, \mathrm{Ad}(\bar{\rho})).$$

2) Supposons que Π *vérifie l'hypothèse de p-finitude.*
Alors les espaces tangents $\boldsymbol{Def}^{\square}(\bar{\rho})(\mathbb{F}[\varepsilon])$ *et* $\boldsymbol{Def}(\bar{\rho})(\mathbb{F}[\varepsilon])$ *sont de dimension finie et :*

$$\dim_{\mathbb{F}} \boldsymbol{Def}^{\square}(\bar{\rho})(\mathbb{F}[\varepsilon]) = \dim_{\mathbb{F}}(\boldsymbol{Def}(\bar{\rho})(\mathbb{F}[\varepsilon])) + \dim_{\mathbb{F}} \mathrm{Ad}(\bar{\rho}) - \dim_{\mathbb{F}} \mathrm{Ad}(\bar{\rho})^{\Pi}.$$

Démonstration. — Pour le second point, seule l'égalité portant sur la dimension de l'espace tangent $\mathbf{Def}^{\square}(\bar{\rho})(\mathbb{F}[\varepsilon])$ n'a pas été démontrée. Cela ne figure pas dans [Maz 2]. Il s'agit du cadre de Kisin [Ki 2]. Quoiqu'il en soit, la preuve est élémentaire. Comme un 1-cobord est de la forme $g \mapsto \bar{\rho}(g)M\bar{\rho}(g)^{-1} - M$, avec $M \in \mathrm{Ad}(\bar{\rho})$ fixée, il y a une bijection entre $\mathrm{Ad}(\bar{\rho})/\mathrm{Ad}(\bar{\rho})^{\Pi}$ et cet espace des 1-cobords. □

Remarque 1.3.25. — 1) On peut aussi voir que $\mathbf{Def}(\bar{\rho})(\mathbb{F}[\varepsilon])$ est en bijection avec $\mathrm{Ext}^1_\Pi(\bar{\rho},\bar{\rho})$ (par exemple dans [Maz 2]).
2) On suppose que $\mathrm{C}(\bar{\rho})=\mathbb{F}$. L'application naturelle $\mathbf{Def}^\square(\bar{\rho})\to\mathbf{Def}(\bar{\rho})$ induit $R^\square(\bar{\rho})\to R(\bar{\rho})$; cette application est lisse (cf. [Ki 1]) donc $R^\square(\bar{\rho})$ est un anneau de séries formelles sur $R(\bar{\rho})$. D'après la proposition précédente, il vient $R^\square(\bar{\rho})\simeq R(\bar{\rho})[[X_1,\dots,X_{n^2-1}]]$.

1.3.3.2. Le second groupe de cohomologie. — On se donne $R,S\in\widehat{\mathcal{C}}$ avec $R\twoheadrightarrow S$ une surjection de noyau I tel que $I\cdot m_R=(0)$. On voit I comme un $\mathbb{F}$-espace vectoriel.
Soit $\rho_S:\Pi\to\mathrm{GL}_n(S)$ une représentation continue. On note $\delta:\Pi\to\mathrm{GL}_n(R)$ une application telle que $(\delta \mod m_R)=\bar{\rho}_S$, ici on ne suppose pas que δ est un morphisme.
Formons alors

$$c(g,h):=\delta(gh)\delta(h)^{-1}\delta(g)^{-1},\ \text{avec } g,h\in\Pi.$$

Cette application c est telle que $c(g,h)\in 1+I\otimes\mathrm{M}_n(\mathbb{F})$. Un calcul (un peu long) nous indique que l'application

$$(g,h)\mapsto c(g,h)-1$$

est un 2-cocycle à valeurs dans $I\otimes\mathrm{Ad}(\bar{\rho})$. Un autre calcul (au moins aussi long que le précédent) montre que l'on passe de c au 2-cocycle c' associé à une autre application δ' (qui relève $\bar{\rho}_S$) grâce à un 2-cobord. De cette façon, on dispose d'un élément $\mathcal{O}(\rho_S)$ de $H^2(\Pi,\mathrm{Ad}(\bar{\rho}))\otimes_{\mathbb{F}} I$ qui dépend uniquement de $\bar{\rho}_S$. On dit que $\mathcal{O}(\rho_S)$ est la classe d'obstruction de ρ_S. Dire que cette classe $\mathcal{O}(\rho_S)$ est nulle signifie qu'il existe une représentation à valeurs de R qui relève ρ_S.

Remarque 1.3.26. — Avant ce commentaire sur l'obstruction, nous avons regardé le cas $R=\mathbb{F}[\varepsilon]$ et $S=\mathbb{F}$, avec $\rho_S=\bar{\rho}$. Le 2-cocycle associé à ce problème de relèvement est $(g,h)\mapsto\bar{\rho}(g)c(h)\bar{\rho}(g)^{-1}-c(gh)+c(g)$, qui est un 2-cobord. La classe $\mathcal{O}(\bar{\rho})$ est nulle ici, la représentation $g\mapsto\bar{\rho}(g)\in\mathrm{GL}_n(\mathbb{F}[\varepsilon])\subseteq\mathrm{GL}_n(\mathbb{F})$ est un relèvement de $\bar{\rho}$.

1.3.3.3. Dimension de Krull, déformation sans obstruction. — Donnons une idée de la preuve du théorème ci-dessous.
On a vu qu'un anneau $R\in\widehat{\mathcal{C}}$ admet une présentation donnée par

$$\mathrm{W}(\mathbb{F})[[X_1,\dots,X_n]]\to R\to 0.$$

En réduisant modulo p et en considérant $R(\bar{\rho})$, on a une suite exacte

$$0\to J\to F\to R(\bar{\rho})/pR(\bar{\rho})\to 0,$$

où $F=\mathbb{F}[[X_1,\dots,X_n]]$. Notons que le quotient $R(\bar{\rho})/pR(\bar{\rho})$ est l'anneau de déformation universel pour les déformations de $\bar{\rho}$ en caractéristique p. En considérant la suite exacte

$$0\to J/(m_F\cdot J)\to F/(m_F\cdot J)\to R(\bar{\rho})/pR(\bar{\rho})\to 0,$$

on voit que la dimension de Krull de $R(\bar{\rho})/pR(\bar{\rho})$ dépend du nombre minimal de générateurs de J. On note $\boldsymbol{\rho}_0$ la déformation de $\bar{\rho}$ à valeurs dans $R(\bar{\rho})/pR(\bar{\rho})$ induite par $\boldsymbol{\rho}$ et on forme la classe d'obstruction $\mathcal{O}(\boldsymbol{\rho}_0)\in H^2(\Pi,\mathrm{Ad}(\bar{\rho}))\otimes J/(m_F\cdot J)$. Mazur montre alors que l'application suivante est injective

$$\begin{array}{ccc}\mathrm{Hom}(J/(m_F\cdot J),\mathbb{F}) & \to & H^2(\Pi,\mathrm{Ad}(\bar{\rho}))\\ f & \mapsto & (1\otimes f)(\mathcal{O}(\boldsymbol{\rho}_0)).\end{array}$$

Le nombre minimal de générateurs de J est donc majoré par l'entier $\dim_{\mathbb{F}} H^2(\Pi, \mathrm{Ad}(\bar{\rho}))$. On peut alors énoncer :

Théorème 1.3.27 **([Maz 1], §.1.6, Prop.2)**. — *On suppose que* $\mathrm{C}(\bar{\rho}) = \mathbb{F}$. *Soit* $R(\bar{\rho})$ *l'anneau de déformation universel de* $\bar{\rho}$. *On note*

$$d_i = \dim_{\mathbb{F}} H^i(\Pi, \mathrm{Ad}(\bar{\rho})), \text{ avec } i = 1, 2.$$

Alors on a l'inégalité suivante :

$$\mathrm{dimKrull}\ R(\bar{\rho})/pR(\bar{\rho}) \geq d_1 - d_2.$$

Si $d_2 = 0$, *alors l'inégalité ci-dessus est une égalité et donc*

$$R(\bar{\rho}) \simeq \mathrm{W}(\mathbb{F})[[X_1, ..., X_{d_1}]].$$

On dit que le problème de déformation est sans obstruction lorsque d_2 *est nul.*
Dans tous les cas, l'anneau $R(\bar{\rho})$ *est de la forme :*

$$R(\bar{\rho}) \simeq \mathrm{W}(\mathbb{F})[[X_1, ..., X_{d_1}]]/I$$

avec $\mathrm{gen}(I) := \dim_{\mathbb{F}}(I/m_R I) \leq d_2$.

1.3.3.4. Cas Global. — En s'appuyant sur la suite exacte de Poitou-Tate (cf. [Se 3]), Mazur obtient la minoration suivante de la dimension de Krull. Comme le module $\mathrm{Ad}(\bar{\rho})$ est d'ordre une puissance de p, l'ensemble de places S autorisées à se ramifier doit contenir les places archimédiennes et les places au-dessus de p. On rappelle que $G_{K,S}$ désigne le groupe de Galois de l'extension maximale de K non-ramifiée en dehors de S.

Corollaire 1.3.28 **([Maz 1], §.1.10, Prop.5)**. — *Soit* $K/\mathbb{Q}$ *un corps de nombres de degré* d. *On se donne un ensemble fini* S *de places de* K *contenant les places archimédiennes* $Pl_\infty(K)$ *et les places au-dessus de* p. *On note* $\mathrm{Gal}(\overline{K}_v/K_v)$ *le groupe de Galois absolu du complété* K_v *de* K *en* $v \in Pl_\infty(K)$. *Soit* $\bar{\rho} : G_{K,S} \to \mathrm{GL}_n(\mathbb{F})$ *une représentation continue telle que* $\mathrm{C}(\bar{\rho}) = \mathbb{F}$. *On note* $R(\bar{\rho})$ *l'anneau de déformation universelle de* $\bar{\rho}$.
Alors

$$\mathrm{dimKrull}\ R(\rho)/R(\rho) \geq 1 + dn^2 - \sum_{v \in Pl_\infty(K)} H^0(\mathrm{Gal}(\overline{K}_v/K_v), \mathrm{Ad}(\bar{\rho})).$$

Dans la suite, on travaille avec des représentations de dimension deux. En distinguant les représentations paires et impaires, on peut préciser le corollaire ci-dessus lorsque $K = \mathbb{Q}$.

Définition 1.3.29. — Soit p différent de 2. On dit que $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ est impaire lorsque $\det\bar{\rho}(c) = -1$, où c est une conjugaison complexe. Sinon, on dit que $\bar{\rho}$ est paire.

En dimension deux avec $K = \mathbb{Q}$, le corollaire ci-dessus donne :

Corollaire 1.3.30. — *Soit* $p \geq 3$. *On conserve les mêmes hypothèses que dans le corollaire ci-dessus avec* $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$. *Alors*

$$\mathrm{dimKrull}\ R(\bar{\rho})/pR(\bar{\rho}) \geq \begin{cases} 3 \text{ si } \bar{\rho} \text{ est impaire,} \\ 1 \text{ si } \bar{\rho} \text{ est paire.} \end{cases}$$

Remarque 1.3.31. — On retrouve ce résultat dans le **chapitre** 3 dans le cas particulier $k = \mathbb{Q}$ (cf. Cor. 3.7.8).

Terminons en discutant du cas d'égalité dans le théorème 1.3.27, i.e. du cas où

$$\text{dimKrull } R(\bar{\rho})/pR(\bar{\rho}) = d_1 - d_2.$$

Mazur a conjecturé que cette égalité a toujours lieu dès que $\bar{\rho}$ est absolument irréductible. Il n'y a pas de contre-exemple, ni de preuve de ce fait pour le moment.

Notons que cette conjecture est une version de la conjecture de Leopoldt (qui dit que le nombre de $\mathbb{Z}_p$-extensions linéairement indépendantes d'un corps de nombres K de signatures (r_1, r_2) est égal à $1 + r_2$) en dimension n. Puisque $R(\bar{\rho}) \simeq \mathrm{W}(\mathbb{F})[[G_{K,S}^{ab,(p)}]]$ (d'après la proposition 1.3.20), la dimension de Krull de $R(\bar{\rho})/pR(\bar{\rho})$ est égale au $\mathbb{Z}_p$-rang de $G_{K,S}^{ab,(p)}$. Ainsi lorsque $n = 1$, dire que dimKrull $R(\bar{\rho})/pR(\bar{\rho}) = d_1 - d_2$ équivaut à dire que le couple (K, p) vérifie la conjecture de Leopoldt ; ici $d_1 - d_2 = 1 + r_2$ puisque $\mathrm{Ad}(\bar{\rho}) = \mathbb{F}$.

Revenons à la situation générale en dimension n. Le cas le plus simple pour lequel l'égalité a lieu est donné par $d_2 = 0$, c'est le cas sans obstruction. Citons un exemple tiré de [Maz 1]. On note $K/\mathbb{Q}$ le corps de décomposition de $X^3 - X + 1$. Le groupe de Galois associé à ce polynôme est le groupe symétrique S_3, $K/\mathbb{Q}$ est p-ramifiée avec $p = 23$. Comme S_3 s'injecte dans $\mathrm{GL}_2(\mathbb{F}_{23})$, il existe une représentation $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_{23})$ absolument irréductible (avec $S = \{23\}$). Mazur montre alors que ce problème est sans obstruction et donc $R(\bar{\rho}) \simeq \mathbb{Z}_{23}[[X_1, X_2, X_3]]$.

1.3.3.5. Cas Local. — Soit $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathbb{F})$ une représentation continue. Lorsque $\mathrm{C}(\bar{\rho}) = \mathbb{F}$, la formule d'Euler-Poincaré pour le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ donne :

$$d_1 - d_2 = 5.$$

Comme dans le cas global, donnons un exemple d'anneau sans obstruction. Dans [Ra 3], il figure une condition suffisante pour que d_2 soit nul. Les représentations absolument irréductibles $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathbb{F}_p)$ sont connues, on trouve leur table dans [FM], §.9 par exemple. On peut énoncer le théorème suivant, légèrement différent de celui de [Ra 3] (cf. [FM]).

Théorème 1.3.32 **([Ra 3], Th.4.1).** — *Soit $p \geq 3$ et soit $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue et absolument irréductible. Alors on est dans le cas sans obstruction $d_2 = 0$ et donc*

$$R(\bar{\rho}) \simeq \mathbb{Z}_p[[X_1, \ldots, X_5]].$$

1.4. Condition de déformation, foncteur relativement représentable

Soit $F : \mathcal{C} \to \mathrm{Ens}$ un foncteur tel que $F(\mathbb{F})$ soit réduit à un élément. Soit G un sous-foncteur de F, i.e. $G(A) \subseteq F(A)$ pour tout $A \in \mathcal{C}$. On suppose que $G(\mathbb{F}) = F(\mathbb{F})$. Il s'agit de mettre en évidence une condition (être relativement représentable) pour que le foncteur G soit pro-représentable dès que F l'est. Une condition de déformation définit un foncteur relativement représentable ; dans la pratique, l'arithmétique motive l'introduction des conditions de déformation. De cette façon, le problème de déformation est différent de celui posé au départ mais dans cette nouvelle configuration il y a encore un anneau de déformation (uni)versel, c'est un quotient de $R(\bar{\rho})$. Nous y reviendrons dans le **chapitre 2** (en rappelant certains éléments de cette section).

Soit $\bar{\rho} : \Pi \to \mathrm{GL}_n(\mathbb{F})$ une représentation résiduelle fixée. Soit D une propriété satisfaite par $\bar{\rho}$. La définition suivante présente une classe de propriété D, appelée condition de déformation.

Définition 1.4.1. — On dit que D est une condition de déformation lorsque les deux points suivants sont vérifiés :
1) Soit $\alpha : A \to B$ un morphisme d'algèbres de coefficients. Si ρ_A vérifie D alors $\alpha \circ \rho_A$ vérifie aussi D.
2) Soit $\rho : \Pi \to \mathrm{GL}_n(A \times_C B)$ une déformation de $\bar{\rho}$ avec A, B, C trois anneaux locaux Artiniens. Soit $p_A : A \times_C B \to A$ et $p_B : A \times_C B \to B$ les deux projections naturelles. Alors :
$$\rho \text{ satisfait } D \Leftrightarrow [p_A \circ \rho \text{ et } p_B \circ \rho \text{ satisfont } D].$$

Le premier point permet d'utiliser le langage fonctoriel, on confond ainsi la condition de déformation D et le foncteur $\mathbf{Def}_D(\bar{\rho})$ associé à D défini de la manière suivante :

$$\begin{array}{ccc} \mathcal{C} & \to & \mathrm{Ens} \\ A & \mapsto & \{\rho_A \in \mathbf{Def}(\bar{\rho})(A) \text{ vérifiant } D\}. \end{array}$$

On étend ce foncteur à la catégorie $\widehat{\mathcal{C}}$ par continuité

$$\mathbf{Def}_D(\bar{\rho})(R) = \varprojlim_j \mathbf{Def}_D(\bar{\rho})(R)(R/{m_R}^j) \text{ avec } R \in \widehat{\mathcal{C}}.$$

Pour montrer que $\mathbf{Def}_D(\bar{\rho})(R)$ est pro-représentable, on peut le voir comme un foncteur relativement représentable par rapport à $\mathbf{Def}(\bar{\rho})$.

Définition 1.4.2. — On dit que G est relativement représentable par rapport à F si pour chaque diagramme dans $\mathcal{C}$

$$\begin{array}{ccc} A & & B \\ & {\scriptstyle\alpha}\searrow \quad \swarrow{\scriptstyle\beta} & \\ & C & \end{array}$$

le diagramme naturel

$$\begin{array}{ccc} G(A \times_C B) & \longrightarrow & G(A) \times_{G(C)} G(B) \\ \downarrow & & \downarrow \\ F(A \times_C B) & \longrightarrow & F(A) \times_{F(C)} F(B) \end{array}$$

identifie $G(A \times_C B)$ avec le produit fibré $F(A \times_C B) \underset{F(A)\times_{F(C)}F(B)}{\times} \left(G(A) \times_{G(C)} G(B)\right)$.

Un foncteur relativement représentable par rapport à F possède les mêmes propriétés que le foncteur F comme l'indique la proposition suivante.

Proposition 1.4.3 ([Maz 2], §.19). — *Soit G un foncteur relativement représentable par rapport à F.*
1) Pour $i = 1, \ldots, 4$, si F vérifie la propriété Hi alors G la vérifie aussi.
2) Si F est pro-représentable par un anneau $R \in \widehat{\mathcal{C}}$, alors G est pro-représentable par un quotient de R.

Proposition 1.4.4 **([Maz 2], §.23)**. — *Si D est une condition de déformation pour $\bar{\rho}$, alors le foncteur $\boldsymbol{Def}_D(\bar{\rho})$ est relativement représentable par rapport à $\boldsymbol{Def}(\bar{\rho})$.*

Comme conséquence directe, il vient :

Théorème 1.4.5. — *On suppose que $\mathrm{C}(\bar{\rho}) = \mathbb{F}$. Si D est une condition de déformation, alors le foncteur $\boldsymbol{Def}_D(\bar{\rho})$ satisfait les propriétés H1, H2, H3 et H4 de [Sc]. Autrement dit, $\boldsymbol{Def}_D(\bar{\rho})$ est un foncteur représentable par un quotient de $R(\bar{\rho})$.*

Donnons deux exemples de condition de déformation, le premier est le plus simple et concerne la ramification des déformations de $\bar{\rho}$ de dimension n ; quant au second il nous est donné par la théorie des formes modulaires dites ordinaires en p, i.e. les formes modulaires classiques $f = \sum_n a_n q^n$ pour lesquelles a_n est une unité p-adique, cela concerne les représentations en dimension 2.

Exemple 1.4.6 **(Ramification)**. — 1) Soit K un corps de nombres. On dit qu'une représentation

$$\rho_R : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_n(R)$$

est non-ramifiée en une place v de K lorsque pour chaque $w|v$:

$$\rho_R(I_w) = (1),$$

où I_w est le sous-groupe d'inertie associé à la place $w|v$. Comme les groupes d'inertie sont conjugués, il suffit en réalité de vérifier que $I_w \subseteq \ker \rho_R$ pour une place $w|v$. Dire que ρ_R est non-ramifiée en v revient à dire que v est non-ramifiée dans l'extension $\overline{\mathbb{Q}}^{\ker \rho_R}/K$. "Etre non-ramifiée en v" est une condition de déformation. On se donne une représentation résiduelle $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_n(\mathbb{F})$ non-ramifiée en dehors de l'ensemble fini de places S. Or, $\bar{\rho}$ est non-ramifiée en dehors de l'ensemble fini T dès que T contient S. On note $G_{K,S}$ le groupe de Galois de l'extension maximale de K non-ramifiée hors de S. On souhaite déformer $\bar{\rho} : G_{K,S} \to \mathrm{GL}_n(\mathbb{F})$ et $\bar{\rho} : G_{K,T} \to \mathrm{GL}_n(\mathbb{F})$, dont les anneaux de déformation (uni)versels sont notés $R_S(\bar{\rho})$ et $\bar{\rho}_T(\bar{\rho})$. Avec ce qui précède, on sait que l'anneau R_T est un quotient de R_S. Il est naturel de vouloir en savoir plus sur cette surjection, sur son noyau en particulier. Certains cas sont traités dans [Bo 2].

2) En revanche, "être ramifiée en v" n'est pas une condition de déformation.

Exemple 1.4.7 **(Déformation presque ordinaire, déformation presque extraordinaire)**

Soit L/K une extension galoisienne du corps de nombres K. Considérons deux sous-groupes de $\mathrm{Gal}(L/K)$: G_v et I_v les groupes de décomposition et d'inertie associés à une place de L au-dessus d'une place v de K.

Soit $R \in \mathcal{C}$ et soit $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_2(R)$ une représentation. Enfin V_ρ désigne l'espace associé à ρ.

On dit que ρ est :

1) *presque ordinaire* en v lorsque V_ρ admet un sous-R-module libre V_1 qui est G_v-stable et facteur direct de rang 1 de V_ρ.
2) *presque extraordinaire* en v lorsque V_ρ admet une décomposition en facteurs directs de R-modules libres de rang 1 et G_v-stables : $V_\rho = V_1 \oplus V_2$.
3) *ordinaire* en v lorsque ρ est presque ordinaire en v et $V_1 = V_\rho^{I_v}$.
4) *extraordinaire* en v lorsque ρ est presque extraordinaire en v et $V_1 = V_\rho^{I_v}$.

Proposition 1.4.8. — *Chacune des propriétés ci-dessus est une condition de déformation. Les algèbres de coefficients qui leur sont associées sont respectivement notées :*

$$R^{no}, R^{neo}, R^{o} \text{ et } R^{eo}.$$

D'après le théorème 1.4.5, on dispose des flèches naturelles :

$$R^{no} \twoheadrightarrow R^{o},\ R^{neo} \twoheadrightarrow R^{eo} \text{ et } R^{o} \twoheadrightarrow R^{eo}.$$

Démonstration. — On se limite au foncteur associé à la propriété *presque extraordinaire en v*. Soit $\bar{\rho} : \mathrm{Gal}(L/K) \to \mathrm{GL}_2(\mathbb{F})$ une représentation presque extraordinaire en v. Avec les notations de la définition 1.4.1, supposons que $p_A \circ \rho$ et $p_B \circ \rho$ soient presque extraordinaires en v. $V_{p_A \circ \rho}$ (respectivement $V_{p_B \circ \rho}$) admet un sous-A-module libre V_A (resp. un sous-B-module libre M_B) G_v-stable et facteur direct de rang 1 de $V_{p_A \circ \rho}$ (resp. de $V_{p_B \circ \rho}$). Le C-module $V_C = V_A \otimes_A C$ est libre de rang 1. V_C est isomorphe au C-module $V_B \otimes_B C$. Ainsi, le $A \times_C B$-module $V_A \times_{V_C} V_B$ est libre de rang 1. Par construction, c'est un facteur direct de V_ρ. □

1.5. Représentations galoisiennes

On présente ici des résultats classiques sur les représentations galoisiennes en dimension deux. Tout au long de cette section, la lettre K désigne un corps de nombres et S un ensemble fini de places de K. On note K_S l'extension maximale de K (dans une clôture $\overline{\mathbb{Q}}$) non-ramifiée en dehors de S, le groupe $G_{K,S}$ désigne le groupe de Galois $\mathrm{Gal}(K_S/K)$. Pour chaque place $v \in S$, on note Frob_v un Frobenius associé à v dans $G_{K,S}$ et $[\mathrm{Frob}_v]$ sa classe de conjugaison. Enfin, le traditionnel caractère χ_p désigne le caractère cyclotomique modulo p ou à valeurs dans $\mathbb{Z}_p^\times$ selon le contexte.
On considère ici les morphismes de groupes $\rho : \Pi \to \mathrm{GL}_2(X)$ continus où :
(1) Π désigne un sous-groupe d'un quotient de $G_{K,S}$,
(2) X désigne un sous-corps de $\overline{\mathbb{F}}_p$ muni de la topologie discrète ou de $\overline{\mathbb{Q}}_p$ muni de la topologie p-adique.

1.5.1. Cebotarev et semi-simplicité. — On rappelle le théorème de densité de Cebotarev et la classification -qui en découle grâce au théorème de Brauer-Nesbitt- des représentations galoisiennes semi-simples.

Les classes de conjugaison des Frob_v engendrent topologiquement le groupe de Galois sous-jacent, c'est l'objet du théorème de densité de Cebotarev (cf. [Se 4], par exemple).

Théorème 1.5.1 **(Cebotarev)**. — *Soit K un corps de nombres et soit L/K une extension galoisienne non-ramifiée en dehors d'un ensemble fini de places S.*
Alors la famille formée des $[\mathrm{Frob}_v]$ pour $v \notin S$ est dense dans le groupe $\mathrm{Gal}(L/K)$.

On rappelle une version du théoèrme de Brauer-Nesbitt (cf. [Ch], par exemple) qui caractérise les modules isomorphes grâce à leurs polynômes caractéristiques.

Théorème 1.5.2 **(Brauer-Nesbitt)**. — *Soit k un corps et soit A une k-algèbre. On note M et N deux A-modules semi-simples de dimension finie. Alors M et N sont isomorphes si et seulement si les polynômes caractéristiques de M et de N sont égaux.*

Avec le théorème de Brauer-Nesbitt et le théorème de densité de Cebotarev, on obtient :

Théorème 1.5.3. — *Soit k un corps topologique.*
Soient $\rho_1 : G_{K,S} \to \mathrm{GL}_2(k)$ et $\rho_2 : G_{K,S} \to \mathrm{GL}_2(k)$ deux représentations continues. On suppose que ρ_1 et ρ_2 sont semi-simples. Si l'égalité entre les polynômes en X suivants se produit pour tout $v \notin S$

$$\det(X - \rho_1(\mathrm{Frob}_v)) = \det(X - \rho_2(\mathrm{Frob}_v)),$$

alors

$$\rho_1 \simeq \rho_2.$$

Remarque 1.5.4. — Lorsque $2 \in k^\times$, il suffit de vérifier que $\mathrm{tr}\ (\rho_1(\mathrm{Frob}_v)) = \mathrm{tr}\ (\rho_2(\mathrm{Frob}_v))$ pour tout $v \in S$ pour dire que $\rho_1 \simeq \rho_2$.

1.5.2. Représentation associée à une courbe elliptique. — Soit E une courbe elliptique définie sur $\mathbb{Q}$, i.e. une variété projective lisse de genre 1 définie sur le corps $\mathbb{Q}$ et munie d'un point rationnel. En plongeant E dans l'espace projectif de dimension 2, la partie affine de E possède une équation de la forme

$$y^2 = x^3 + Ax + B, \text{ avec } A, B \in \mathbb{Q}.$$

La multiplication par un entier $m \in \mathbb{Z}$ définit un morphisme de groupe :

$$\begin{array}{rccc} [m] : & E(\overline{\mathbb{Q}}) & \to & E(\overline{\mathbb{Q}}) \\ & P & \mapsto & mP. \end{array}$$

On note $E[m]$ le noyau de ce morphisme, il est formé des points de m-torsion de $E(\overline{\mathbb{Q}})$. Lorsque p désigne un nombre premier et n un entier naturel non-nul, on sait que

$$E[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}.$$

En choisissant des bases compatibles pour les applications naturelles $E[p^n] \leftarrow E[p^{n+1}]$, on obtient l'isomorphisme :

$$\varprojlim_n E[p^n] \simeq \mathbb{Z}_p^2.$$

On appelle module de Tate p-adique de E le $\mathbb{Z}_p$-module $\mathrm{Ta}_p(E)$ libre de rang 2 :

$$\mathrm{Ta}_p(E) = \varprojlim_n E[p^n].$$

Comme la courbe E est donnée par une équation algébrique à coefficients rationnels, le groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur E. De la même façon, ce groupe agit sur les points de torsion $E[p^n]$ et par compatibilité, on récupère une action sur le module de Tate $\mathrm{Ta}_p(E)$. Après avoir fixé une base, on dispose des deux représentations

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p),$$

et

$$\bar{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p),$$

associées respectivement à l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur le module de Tate de E et sur $E[p]$. De plus, la réduction de $\rho_{E,p}$ modulo p coïncide avec $\bar{\rho}_{E,p} : \rho_{E,p} \mod p = \bar{\rho}_{E,p}$.
Soit l un premier ne divisant pas le conducteur N de la courbe elliptique E. Alors E a bonne réduction modulo l, on note $\bar{E}_l$ cette réduction. Le résultat suivant figure dans [DDT] (cf. §.2.2) par exemple.

Proposition 1.5.5. — *Soit E une courbe elliptique définie sur $\mathbb{Q}$, de conducteur N.*

1) Soit p un nombre premier. Alors la représentation $\rho_{E,p}$ est non-ramifiée en dehors des premiers qui divisent pN. Pour chaque premier $l \nmid pN$, on a :

$$\text{tr } \rho_{E,p}(\text{Frob}_l) = l + 1 - |\bar{E}_l(\mathbb{F}_l)|.$$

La représentation $\rho_{E,p}$ est absolument irréductible et $\det \rho_{E,p} = \chi_p$.
2) La représentation $\bar{\rho}_{E,p}$ est absolument irréductible pour presque tout p.

On peut remarquer que la trace de $\rho_{E,p}(\text{Frob}_l)$ est indépendante du premier p, avec $p \neq l$. Par ailleurs, le déterminant de l'image d'une conjugaison complexe par $\rho_{E,p}$ ou $\bar{\rho}_{E,p}$ vaut -1, ces représentations sont impaires.

1.5.3. Théorème de Deligne, Eichler-Shimura. — Dans cette section, on aborde les représentations associées aux formes paraboliques classiques et modulo p. Le cadre choisi pour la notion de forme parabolique modulo p est celui de [Se 2]. Une forme modulaire appartenant à $\text{S}_k(\Gamma_1(N), \mathbb{C})(\varepsilon)$ est par définition parabolique, de poids k et de caractère $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ pour $\Gamma_1(N)$. La définition est analogue pour $\text{S}_k(\Gamma_1(N), \overline{\mathbb{F}}_p)(\bar{\varepsilon})$.

Théorème 1.5.6 **([DS], Th.6.1)**. — *Soit $k \geq 2$, $N \geq 1$ et p un nombre premier qui ne divise pas N. Soit $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un caractère.*
Soit $f = \sum_{n\geq 1} a_n(f)q^n \in \text{S}_k(\Gamma_1(N), \mathbb{C})(\varepsilon)$ une forme parabolique propre pour les opérateurs de Hecke et normalisée. Alors il existe une représentation irréductible et non-ramifiée en dehors de pN

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{Q}}_p)$$

telle que pour tout $l \nmid pN$:

$$\text{tr } \rho_f(\text{Frob}_l) = a_l(f) \text{ et } \det \rho_f(\text{Frob}_l) = \varepsilon(l)l^{k-1}.$$

On dit que ρ_f est associée à f.

D'après le théorème 1.5.3, une telle représentation est unique et son déterminant est donné par :

$$\det \rho_f = \varepsilon \cdot \chi_p^{k-1}.$$

En particulier, ρ_f est impaire : $\det \rho_f(c_\infty) = -1$, où c_∞ désigne une conjugaison complexe.
Le théorème ci-dessus peut s'énoncer de façon plus précise à l'aide du corps de nombres $\mathbb{Q}(f) := \mathbb{Q}(\{a_n(f)\}_n)$ associée à f ; en particulier la représentation prend ses valeurs dans un complété $\mathbb{Q}(f)_v$ de $\mathbb{Q}(f)$ (où $v|p$). On sait qu'il existe un réseau dans $\mathbb{Q}(f)_v^2$ stable sous l'action du groupe de Galois absolu. Cela nous autorise à réduire la représentation ρ_f. On prend ensuite sa semi-simplifiée, i.e. la somme directe de ses facteurs de Jordan-Hölder. La représentation obtenue est bien entendu semi-simple et ne dépend pas du réseau choisi au départ.
La conséquence de cette observation s'énonce de la façon suivante :

Théorème 1.5.7 **([DS], Th.6.7)**. — *Soit $k \geq 2$, $N \geq 1$ et p un nombre premier qui ne divise pas N. Soit $\bar{\varepsilon} : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ un caractère.*
Soit $f = \sum_{n\geq 1} a_n(f)q^n \in \text{S}_k(\Gamma_1(N), \overline{\mathbb{F}}_p)(\bar{\varepsilon})$ une forme parabolique propre pour les opérateurs de Hecke et normalisée. Alors il existe une représentation semi-simple et non-ramifiée en dehors de pN

$$\bar{\rho}_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{F}}_p)$$

telle que pour tout $l \nmid pN$ *:*

$$\text{tr } \bar{\rho}_f(\text{Frob}_l) = a_l(f) \text{ et } \det \bar{\rho}_f(\text{Frob}_l) = \bar{\varepsilon}(l)l^{k-1}.$$

On dit que $\bar{\rho}_f$ *est associée à* f*.*

Comme le groupe $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ est muni de la topologie discrète, l'image de $\bar{\rho}_f$ est un groupe fini. Il existe donc un corps fini $\mathbb{F}$ de caractéristique p tel que $\bar{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$. Par ailleurs, avec ce que l'on a vu auparavant, on sait que la représentation $\bar{\rho}_f$ est impaire.

1.5.4. Formes compagnons. — On se penche ici sur certaines formes modulaires mod p appelées formes compagnons ("companion forms"). On laisse tomber la notation $\bar{\varepsilon}$ au profit de ε, jusqu'à la fin il s'agit de formes modulaires modulo p.
Soit $f = \sum_n a_n q^n \in \mathrm{S}_k(\Gamma_1(N), \overline{\mathbb{F}}_p)(\varepsilon)$ une forme propre et normalisée telle que les a_n appartiennent à un corps fini $\mathbb{F}$ de caractéristique p. Par la suite, on dit qu'une telle forme f est propre et normalisée de type (k, ε) pour $\Gamma_1(N)$.
La définition d'une forme compagnon nécessite de parler du poids k' donné par :

$$k' = \begin{cases} p+1-k & \text{si } k \neq p, \\ p & \text{si } k = p. \end{cases}$$

Définition 1.5.8. — On suppose que $2 \leq k \leq p$ et que $a_p \neq 0$. On suppose aussi que $a_p^2 \neq \varepsilon(p)$ lorsque $k = p$. On dit que f admet une forme compagnon lorsqu'il existe une forme $g = \sum_n b_n q^n$ propre et normalisée de type (k', ε) pour $\Gamma_1(N)$ telle que :
1) $b_n = a_n n^{k'-1}$ pour tout entier n premier avec p,
2) $a_p b_p = \varepsilon(p)$.
Un tel couple (f, g) est appelé couple de formes compagnons, la notion de forme compagnon est symétrique.

Une reformulation de cette définition, grâce aux théorèmes 1.5.3 et 1.5.7, s'énonce de la façon suivante :

Lemme 1.5.9. — *Les points suivants sont équivalents :*
1) Le couple (f, g) *est composé de formes compagnons,*
2) $\bar{\rho}_f \simeq \bar{\rho}_g \otimes \chi_p^{k-1}$,
3) $\bar{\rho}_g \simeq \bar{\rho}_f \otimes \chi_p^{k'-1}$.

L'étude de ces formes modulaires a été motivée par la recherche du poids optimal de la forme modulaire f associée, d'après la conjecture de Serre, à une représentation impaire et absolument irréductible $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$.

On distingue les formes modulaires modulo p selon que a_p est nul ou non-nul. Il s'agit respectivement du cas supersingulier ou ordinaire. Les formes compagnons sont ordinaires par définition. La théorème suivant, prouvé par Deligne et qui figure par exemple dans [Gro] (cf. Prop.12.1), décrit l'image de la restriction $\bar{\rho}_{f,p}$ au groupe de décomposition $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ dans le cas où f est ordinaire. On a besoin du caractère non-ramifié

$$\lambda(a) : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathbb{F}^\times$$

qui envoie le Frobenius Frob_p sur l'élément $a \in \mathbb{F}^\times$.

Théorème 1.5.10. — *Soit $f = \sum_n a_n q^n$ une forme propre et normalisée de type (k, ε) pour $\Gamma_1(N)$. On suppose que $2 \leq k \leq p+1$ et que $a_p \neq 0$. Alors*

$$\bar{\rho}_{f,p} \simeq \begin{pmatrix} \chi_p^{k-1}\lambda\left(\frac{\varepsilon(p)}{a_p}\right) & * \\ 0 & \lambda(a_p) \end{pmatrix}.$$

Il s'agit de décrire des situations pour lesquelles la représentation $\bar{\rho}_{f,p}$ est diagonalisable, i.e. de caractériser les cas où $* = 0$.
La réciproque du lemme suivant, conjecturée par Serre, a été démontrée par Gross dans [Gro].

Lemme 1.5.11 **([Gro], Prop.13.8)**. — *On suppose que f admet une forme compagnon. Alors $\bar{\rho}_{f,p}$ est diagonalisable :*

$$\bar{\rho}_{f,p} \simeq \chi_p^{k-1}\lambda\left(\frac{\varepsilon(p)}{a_p}\right) \oplus \lambda(a_p).$$

Démonstration. — Notons g la forme compagnon de f. Dans le lemme 1.5.9, on a vu que $\bar{\rho}_f \simeq \bar{\rho}_g \otimes \chi_p^{k-1}$. Avec le théorème 1.5.10, on voit ainsi que l'espace sous-jacent à la représentation $\bar{\rho}_{f,p}$ possède une droite stable sur laquelle le groupe agit via le caractère $\chi_p^{k-1}\lambda\left(\frac{\varepsilon(p)}{a_p}\right)$ et une droite stable sur laquelle le groupe agit via le caractère $\lambda\left(\frac{\varepsilon(p)}{b_p}\right)$. Or, on sait que $\frac{\varepsilon(p)}{b_p} = a_p$ (et que $a_p^2 \neq \varepsilon(p)$ lorsque $k = p$). Ainsi, les deux droites stables sont distinctes et on a bien $\bar{\rho}_{f,p} \simeq \chi_p^{k-1}\lambda\left(\frac{\varepsilon(p)}{a_p}\right) \oplus \lambda(a_p)$. □

Le sous-corps fixé par le noyau d'une représentation $\bar{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ associée à une forme compagnon f est modérément ramifié en p. Les déformations de cette représentation admettant un comportement local analogue doivent pouvoir fournir des extensions peu ramifiées. C'est pour cette raison que nous nous sommes intéressés aux formes compagnons.

Définition 1.5.12. — On dit que $\bar{\rho}_f$ est modérée en p lorsque l'image de l'inertie en p par $\bar{\rho}_f$ est d'ordre premier à p.

Voici une caractérisation des représentations $\bar{\rho}_f$ modérées en p.

Lemme 1.5.13 **([Gro], Prop.13.7)**. — *Soit $f = \sum_n a_n q^n$ une forme propre et normalisée de type (k, ε) pour $\Gamma_1(N)$. On suppose que $a_p \neq 0$. Lorsque $k = p$, on suppose de plus que $a_p^2 \neq \varepsilon(p)$. Alors on a l'équivalence suivante :*

$$\bar{\rho}_{f,p} \simeq \chi_p^{k-1}\lambda\left(\frac{\varepsilon(p)}{a_p}\right) \oplus \lambda(a_p) \Longleftrightarrow \bar{\rho}_f \text{ est modérée en } p.$$

Le théorème suivant est dû à Gross. On a déjà vu l'implication 2) ⇒ 1) (cf. les lemmes 1.5.11 et 1.5.13). La difficulté se concentre sur l'implication 1) ⇒ 2).

Théorème 1.5.14 **([Gro], Th.13.10)**. — *On se donne f une forme propre et normalisée de type (k, ε) pour $\Gamma_1(N)$. Supposons que $2 \leq k \leq p$, $a_p \neq 0$, $a_p^2 \neq \varepsilon(p)$ lorsque $k = p$ et enfin que la représentation $\bar{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ associée à f est absolument irréductible.*
Alors les assertions suivantes sont équivalentes :
1) La représentation $\bar{\rho}_f$ est modérément ramifiée en p lorsque $k \neq p$ et non-ramifiée en p lorsque $k = p$.
2) La forme f possède une forme compagnon.

Exemple 1.5.15 **([Gro], §.17)**. — Des calculs menés par Elkies et Atkin lorsque $N = 1$ décrivent les formes compagnons modulo p, avec $p < 3500$. Seules les formes f pour lesquelles l'image de $\bar{\rho}_f$ contient le groupe $\mathrm{SL}_2(\mathbb{F}_p)$ ont été retenues. Par exemple, la forme modulaire de poids 12 pour $\mathrm{SL}_2(\mathbb{Z})$:

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$$

est sa propre forme compagnon modulo 23, mais l'image de $\bar{\rho}_\Delta$ dans $\mathrm{GL}_2(\mathbb{F}_{23})$ est isomorphe au groupe symétrique S_3.
Les nombres premiers exceptionnels, i.e. ceux pour lesquels l'image de $\bar{\rho}_f$ ne contient pas $\mathrm{SL}_2(\mathbb{F}_p)$, ne nous intéressent pas puisque notre objectif est de construire des extensions galoisiennes avec des groupes de Galois du type SL_2.
Soit

$$E_4 = 1 + 240 \sum_n \sigma_3(n) q^n$$

et

$$E_6 = 1 - 504 \sum_n \sigma_5(n) q^n.$$

A partir de ces deux séries d'Eisenstein, posons :

$$\Delta_{16} = E_4 \Delta,\ \Delta_{18} = E_6 \Delta,\ \Delta_{20} = E_4^2 \Delta,\ \text{et}\ \Delta_{26} = E_4^2 E_6 \Delta.$$

Alors chacun des couples (f, p) suivants désigne une forme compagnon f modulo p :

$$(\Delta_{16}, 397),\ (\Delta_{18}, 271),\ (\Delta_{20}, 139),\ (\Delta_{20}, 379),\ \text{et}\ (\Delta_{26}, 107).$$

CHAPITRE 2

RELÈVEMENT DE REPRÉSENTATIONS PRESQUE EXTRAORDINAIRES EN p

Introduction

Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ be a continuous, absolutely irreducible, 2-dimensional representation, with $\mathbb{F}$ a finite field of characteristic $p \geq 5$. Serre has conjectured (see [Se 1]) that $\bar{\rho}$ is modular when it is odd, i.e. when the image of a complex conjuation by $\bar{\rho}$ is of determinant -1. A refined form of this conjecture predicts the minimal weight and level of the newform associated to $\bar{\rho}$. It is now a theorem proved by Khare and Wintenberger (see [Kh 2] for the level one case, [KW 1], [KW 2] and [KW 3]). Potential modularity lifting theory and global deformation theory in the sense of Mazur ([Maz 1]) are involved in [Kh 2]. The results in the first theory mentionned are linked to the conjecture of Fontaine-Mazur [FM](see, e.g., [Ta 2] and [Ki 1]).
In our work, we focus on the global deformation theory with local conditions. To be more precise, assuming that $\bar{\rho}$ is locally abelian (all the restrictions of $\bar{\rho}$ to the decomposition groups have an abelian image), we study the deformations of $\bar{\rho}$ which are also locally abelian. The main example arises from $\bar{\rho}$ attached to a companion modular form (in p) ; in this case the restriction of $\bar{\rho}$ to the inertia group I_p is isomorphic to the sum $1 \oplus \chi$ of two characters. In some sense, it is the only example available on $\mathbb{Q}$ (see [Gro]).

The main result is the following.

Theorem A. — *Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous, odd and unramified outside p representation of the Galois group $G_{\mathbb{Q}}$, with $p \geq 5$. Assume that $\bar{\rho}_{|G_{\mathbb{Q}_p}}$ is nearly extraordinary, i.e. that it is isomorphic to the sum of two characters. Moreover assume that the image* $\mathrm{im}(\bar{\rho})$ *contains* $\mathrm{SL}_2(\mathbb{F}_p)$.
Then there exists a lift $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ of $\bar{\rho}$ and a finite set of primes T containing p such that

$$\rho \text{ is } T\text{-ramified and } \rho_{|G_{\mathbb{Q}_p}} \text{ is isomorphic to the sum of two characters.}$$

In fact, we will prove the more general theorem which deals with an arbitrary number field K (for the notations and terminologies, see below).

Theorem B. — *Let $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ be a continuous representation, unramified outside $S = S_p$, with $p \geq 5$. Assume that $\bar{\rho}$ is totally odd, nearly extraordinary in v for each $v \in S$ and that the image of $\bar{\rho}$ is full.*
Suppose that K is totally real and that $\mu_p \nsubseteq K_v$, for each $v \in S$.
Then there exists a deformation $(\mathrm{W}(\mathbb{F}), \rho)$ of $\bar{\rho}$ and a finite set of primes $T \supseteq S$ such that

$$\rho \text{ is } T\text{-ramified and } (\mathrm{W}(\mathbb{F}), \rho_{|G_v}) \in C_v^{neo}(\mathrm{W}(\mathbb{F})),$$

for all $v \in S_p$.

When $K = \mathbb{Q}$, note that we know that $\bar{\rho}$ is odd if and only if it is modular ; that is a theorem of Khare and Wintenberger (see, e.g., [KW 1]).

Our proof of Theorem B builds on the ideas of Ramakrishna [Ra 2] and Taylor [Ta 1]. Before explaining the outlines of the proof, we give the following corollary which uses some computations of Elkies and Atkin on companion forms in [Gro]. In [Oh], Ohtani has got an unramified Galois extension of $\mathbb{Q}(\mu_{p^\infty})$ with Galois group isomorphic to $\mathrm{SL}_2(\mathbb{Z}_p[[X]]/(b'))$ ([Oh, Corollary 0.2.]), without information on b'. Here, one has :

Theorem C. — *Let $p \in \{107, 139, 271, 379\}$.*
Then there exists a Galois extension $M/\mathbb{Q}(\mu_{p^\infty})$ unramified at S_p such that

$$\mathrm{Gal}(M/\mathbb{Q}(\mu_{p^\infty})) \simeq \mathrm{SL}_2(\mathbb{Z}_p).$$

Moreover, there is a finite set of primes T' such that $M/\mathbb{Q}(\mu_{p^\infty})$ is T'-ramified and tamely ramified at w, for each $w \in T'$.

We explain the main ideas of the proof of Theorem B. We use the formalism of the deformation theory introduced by Mazur [Maz 1]. Thus we attach a local deformation functor to the property "nearly extraordinary in v" (for $v|p$), denoted by C_v^{neo}. We show (Lemmas 2.3.7 and 2.3.8) that, for each $v|p$, this functor is a deformation condition, continuous and smooth. In other words, if L_v^{neo} denotes the tangent space of C_v^{neo}, then (C_v^{neo}, L_v^{neo}) is admissible, which means that it satisfies the properties $P1, \ldots, P7$ formalized by [Ta 1] and recalled in Definition 2.2.4. Hence, we know that C_v^{neo} is unobstructed.

Afterwards, we use the following inequality ([Bö 1]), based on the Poitou-Tate duality,

$$\mathrm{gen}(J_{\{C_v\}}) \leq \sum_{v \in S} \mathrm{gen}(J_v) + \dim_{\mathbb{F}} H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1)),$$

which is recalled in Proposition 2.2.9. It is a weak local-global principle.

The ideal of relations J_v of the versal ring of C_v^{neo} is trivial since this functor is unobstructed. If the Selmer group in the right-hand side in the above inequality is trivial, then the ideal of relations $J_{\{C_v\}}$ is also trivial and our global deformation problem admits a universal ring of characteristic zero (see Propostion 2.2.10). Otherwise, we need to make the Selmer group trivial. That is the object of the subsection 2.4.1 and of Lemma 2.4.3. In this subsection, we describe an algorithm which decreases the dimension of the Selmer group by adding a finite number of primes of K to the set S. The tangent spaces L_v^{neo} need to be big enough in order to initialize the algorithm (see Proposition 2.4.4).
We call this algorithm the Taylor-Ramakrishna method. Moreover, we give a bound for the primes added, based on an effective version of Cebotarev density theorem, when $K = \mathbb{Q}$.

We itemise the contents of the article. In **Section 2.1** we recall the basic preliminaries in deformation theory. The proof of Theorem B needs some local-global principle for admissible deformation functors, this is the object of **Section 2.2**. We show that (C_v^{neo}, L_v^{neo}) is admissible and we give the dimension of the tangent space L_v^{neo} in **Section 2.3**. In **Section 2.4**, Theorem B is finally proved. Some applications and the proof of Theorem C are given in **Section 2.5**.

Notation. —

- $p \geq 5$ is a fixed prime number.
- Let $K/\mathbb{Q}$ be a number field (we fix an algebraic closure of K). We will denote by G_K its absolute Galois group and by $G_{K,S}$ the group $\mathrm{Gal}(K_S/K)$ where S is a finite set of places of K and where K_S denotes the maximal extension of K which is unramified outside S. We denote by S_p the set of all places of K above p and denote by $Pl_\infty(K)$ the set of infinite places of K.
- Let χ_p denote both the p-adic and mod p cyclotomic characters, this should cause no confusion depending on the context.
- Let G_v denote an absolute decomposition group above a finite place v of K, let I_v denote the inertia subgroup of G_v and Frob_v denote an arithmetic Frobenius in G_v/I_v.
- Let $\mathbb{F}$ denote a finite extension of $\mathbb{F}_p$ and $\mathrm{W}(\mathbb{F})$ for its ring of Witt vectors.
- If M represents a $\mathbb{F}[G_v]$-module, we will denote by $M(i)$ the module M with the action twisted by χ_p^i (for $i \in \mathbb{Z}$) and by M' the module $\mathrm{Hom}(M, \mu_p)$.
- Let $\mathrm{Ad}^0(\rho_R)$ be the trace zero submodule of the adjoint $\mathrm{Ad}(\rho_R)$ which is the set $M_2(R)$ with the conjugation action by ρ_R, where ρ_R denotes a representation (with values in $\mathrm{GL}_2(R)$) specified in the context.
- Let γ be a representation of G_K. We denote by $K(\gamma)$ the splitting field of γ, that is the subfield fixed by $\ker\gamma$.
- Let $\mathbb{F}[\epsilon]$ represent the quotient ring of dual numbers $\mathbb{F}[x]/(x^2)$, where $\epsilon = x$.

All representations are supposed to be continuous.

2.1. Deformation theory

2.1.1. Deformation functor. — We denote by $\widehat{\mathcal{C}}$ the category of complete Noetherian local rings with residue field $\mathbb{F}$, with the natural morphisms of such local rings which are the identity by restriction to the residue field $\mathbb{F}$. Let $\mathcal{C}$ be the subcategory of Artinian rings of $\widehat{\mathcal{C}}$. Let $A \in \widehat{\mathcal{C}}$. The object A has a natural structure of a $\mathrm{W}(\mathbb{F})$-algebra and there exists an integer m such that A is a quotient $\mathrm{W}(\mathbb{F})[[X_1, ..., X_m]]/I$, where I is called the ideal of relations of A (see [Bou]). In fact, $m = \dim_{\mathbb{F}} m_A/({m_A}^2, p)$, where m_A denotes the maximal ideal of A.

Let Π be a profinite group which satisfies the *p-finiteness* hypothesis :

$$\forall\ U \text{ open subgroup of } \Pi : \mathrm{Hom}_c(U, \mathbb{F}_p) \text{ is finite.}$$

Let $\bar{\rho} : \Pi \to \mathrm{GL}_2(\mathbb{F})$ be a continuous representation.

Two representations $\rho_A, \rho'_A : \Pi \to \mathrm{GL}_2(A)$ are strictly equivalent if they are conjugated by an element $M \in \ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{F}))$. We will write $[\rho_A]$ for the strict equivalence class of ρ_A and we will identify ρ_A and the class $[\rho_A]$ when the properties studied are stable by conjugation by $\ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{F}))$.

The *deformation functor* $\mathbf{Def}(\bar{\rho}) : \widehat{\mathcal{C}} \longrightarrow \mathrm{Set}$, with values in the category of sets, is defined by

$$\mathbf{Def}(\bar{\rho})(A) = \{[\rho_A] | (\rho_A \ mod \ m_A) = \bar{\rho}\}.$$

Its *tangent space* is the $\mathbb{F}$-vector space $\mathbf{Def}(\bar{\rho})(\mathbb{F}[\epsilon])$. This space is isomorphic to $H^1(\Pi, \mathrm{Ad}\bar{\rho})$.

We recall that $\mathrm{C}(\bar{\rho}) := \{M \in \mathrm{M}_2(\mathbb{F}) \mid \forall g \in \Pi : \ M\bar{\rho}(g) = \bar{\rho}(g)M\}$. The following theorem, based on the deformation theory developed in [Sc], is due to Mazur ([Maz 1])

***Theorem 2.1.1* (Mazur, [Maz 1]).** — *Let Π be a profinite group as above and $\bar{\rho} : \Pi \to \mathrm{GL}_2(\mathbb{F})$ be a continuous representation.*
(1) Then $\boldsymbol{Def}(\bar{\rho})$ admits a pro-hull $(R(\bar{\rho}), \rho)$ in the sense of [Sc].
(2) Assume that $\mathrm{C}(\bar{\rho}) = \mathbb{F}$; put $\mathrm{d}_i = \dim_{\mathbb{F}} H^i(\Pi, \mathrm{Ad}(\bar{\rho}))$, for $i = 1, 2$. Then the functor $\boldsymbol{Def}(\bar{\rho})$ is representable by a ring

$$R(\bar{\rho}) \simeq \mathrm{W}(\mathbb{F})[[X_1, ..., X_{\mathrm{d}_1}]]/I, \ \textit{where } \mathrm{gen}(I) := \dim_{\mathbb{F}}(I/m_R \cdot I) \leq \mathrm{d}_2,$$

i.e.

$$\boldsymbol{Def}(\bar{\rho})(-) \simeq \mathrm{Hom}_{\mathrm{W}(\mathbb{F})}(R(\bar{\rho}), -).$$

In (1), the ring $R(\bar{\rho})$ is called the *versal* deformation ring for $\bar{\rho}$.
In (2), the ring $R(\bar{\rho})$ is called the *universal* deformation ring for $\bar{\rho}$.
By local and global class field theory, the absolute Galois group of a local field and the group $G_{K,S}$ satisfy the p-finiteness hypothesis. We will apply Theorem 2.1.1 for such profinite groups.

2.1.2. Deformation conditions. — (See **Section** 1.4)

2.1.2.1. Fixed determinant. — For $R \in \widehat{\mathcal{C}}$, we denote by $\eta_R : \mathrm{W}(\mathbb{F}) \to R$ the natural morphism deduced from the $\mathrm{W}(\mathbb{F})$-algebra structure of R.
Let $\bar{\rho}$ be a residual representation of Π and let $\delta : \Pi \to \mathrm{W}(\mathbb{F})^\times$ be a fixed morphism such that $\det(\bar{\rho}) = \eta_{\mathbb{F}} \circ \delta$.
We consider the deformations ρ_R of $\bar{\rho}$ with fixed determinant, i.e. such that

$$\det \rho_R = \eta_R \circ \delta.$$

This defines a subfunctor $\mathrm{Def}_\delta(\bar{\rho})$ which is a deformation condition; its tangent space is $H^1(\Pi, \mathrm{Ad}^0\bar{\rho})$.

2.1.2.2. Examples. — We recall Example 1.4.7. More details can be found in, e.g., [Maz 2] and [Oh].
Let $\rho : G_K \to \mathrm{GL}_2(R)$ be an absolutely irreducible representation, where $R \in \widehat{\mathcal{C}}$. Let M_ρ represent the free R-module of rank 2 defined by ρ.

Definition 2.1.2. — *Let v be a place of K. The representation ρ is :*
1) nearly ordinary in v if M_ρ has a free sub-R-module M_1 which is is stable by G_v and a direct summand of rank 1 of M_ρ.
2) nearly extraordinary in v if $M_\rho = M_1 \oplus M_2$ where M_1 and M_2 are free R-modules of rank 1 and are stable by G_v.
3) ordinary in v if ρ is nearly ordinary in v and $M_1 = M_\rho^{I_v}$.
4) extraordinary in v if ρ is nearly extraordinary in v and $M_1 = M_\rho^{I_v}$.
When it is clear from the context, we shall omit the reference to v.

Proposition 2.1.3 **(Mazur, [Maz 2]).** — *The above properties are deformation conditions.*
Denote by R^{no}, R^{neo}, R^o and R^{eo} the versal rings associated respectively to nearly ordinary, nearly extraordinary, ordinary, extraordinary properties in v. Then there are natural surjections :

$$R^{no} \twoheadrightarrow R^o, R^{neo} \twoheadrightarrow R^{eo} \text{ and } R^o \twoheadrightarrow R^{eo}.$$

2.2. Local-Global

We recall that K is a number field with absolute Galois group G_K. For a place v of K, there is a natural restriction $res_v : G_v \to G_K$.

Let $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ denote an absolutely irreducible representation. Then $\bar{\rho}$ is unramified outside a finite set S of primes of K. We make the assumption that S contains all the places of K above p. For each $v \in S$, denote by $\bar{\rho}_v : G_v \to \mathrm{GL}_2(\mathbb{F})$ the natural restriction $\bar{\rho}_{|G_v}$ of $\bar{\rho}$ to G_v.

Until the end of this article, we will work with **deformations with fixed determinant**. So by deformation, we will mean deformation with fixed determinant. The module associated to this condition is $\mathrm{Ad}^0\bar{\rho}$, i.e. we will deal with tangent space $H^1(G_K, \mathrm{Ad}^0\bar{\rho})$ and its subspaces.

2.2.1. Selmer groups. — We will study local deformation conditions and associated tangent spaces, i.e. some subspaces of $H^1(G_v, \mathrm{Ad}^0\bar{\rho})$. Afterwards, the obtained results will be applied to the module $\mathrm{Ad}^0\bar{\rho}$.
From now on we fix M a finite discrete $\mathbb{F}[G_{K,S}]$-module and denote by $M^* = \mathrm{Hom}(M, \mathbb{F})$ its dual representation.
First, let us recall the following classical result about Tate local duality ; it could be found in [Se 3] for example.

Proposition 2.2.1. — *Suppose that $i \in \{0, 1, 2\}$. Then by local duality, the perfect pairing*

$$M \times M^* \to \mathbb{F}$$

induces a perfect pairing

$$H^i(G_v, M) \times H^{2-i}(G_v, M^*(1))) \to H^2(G_v, \mathbb{F}(1)).$$

Definition 2.2.2. — *We fix a sub-$\mathbb{F}$-vector space L_v of $H^1(G_v, M)$, for every $v \in S$. Denote by $L_v^\perp \subseteq H^1(G_v, M^*(1))$ the annihilator of L_v under the perfect pairing of Proposition 2.2.1.*
The preimage of $L(S) := \bigoplus_{v\in S} L_v$ under the natural restriction map

$$H^1(G_{K,S}, M) \to \bigoplus_{v\in S} H^1(G_v, M)$$

is called the Selmer group associated to $(K, L(S))$ and it is denoted by

$$H^1_{\{L(S)\}}(G_{K,S}, M).$$

In the same way, the preimage of $L(S)^\perp = \bigoplus_{v\in S} L_v^\perp$ *under the natural restriction map*

$$H^1(G_{K,S}, M^*(1)) \to \bigoplus_{v\in S} H^1(G_v, M^*(1))$$

is called the Selmer group associated to $(K, L(S)^\perp)$ *and it is denoted by*

$$H^1_{\{L(S)^\perp\}}(G_{K,S}, M^*(1)).$$

It is a hard task to determine such Selmer groups. For example, in the case where $L_v = (0)$ for all $v \in S$, these are the classical Shafarevitch groups. Nevertheless, the following Euler-Poincaré formula provides the value of the quotient of the orders of these groups. It is based on the Poitou-Tate exact sequence.

Theorem 2.2.3. — [DDT, Theorem 2.19]
1) The Selmer group $H^1_{\{L(S)\}}(G_{K,S}, M)$ *is finite.*
2) The following exact sequence holds :

$$\begin{array}{ccccc} H^1(G_{K,S}, M) & \to & \bigoplus_{v\in S} H^1(G_v, M)/L_v & \to & H^1_{\{L(S)^\perp\}}(G_{K,S}, M^*(1))^\vee \\ & \to & H^2(G_{K,S}, M) & \to & \bigoplus_{v\in S} H^2(G_v, M). \end{array}$$

3) The finite orders of the Selmer groups satisfy the equality

$$\frac{|H^1_{\{L(S)\}}(G_{K,S}, M)|}{|H^1_{\{L(S)^\perp\}}(G_{K,S}, M^*(1))|} = \frac{|H^0(G_K, M)|}{|H^0(G_K, M^*(1))|} \prod_{v\in S} \frac{|L_v|}{|H^0(G_v, M)|}.$$

2.2.2. Admissible local conditions. — The main result of this article gives a lift ρ of $\bar\rho$ to $\mathrm{W}(\mathbb{F})$ such that each restriction ρ_v satisfies some property C_v. If the C_v's are subject to some sufficient functorial properties of deformation and smoothness and if a certain Selmer group is trivial, it is known (see Proposition 2.2.10) that the universal deformation ring that is associated to $\mathbf{Def}(\bar\rho)_{\{C_v\}}$ (see Definition 2.2.8 for notations) exists and is smooth over $\mathrm{W}(\mathbb{F})$. We recall the definition given by Taylor in [Ta 1] where the properties of the C_v are listed ; this definition formalizes the work of Ramakrishna [Ra 2].

2.2.2.1. Definition. —

Definition 2.2.4. — *(Taylor, [Ta 1]) Let* $C_v : \widehat{\mathcal{C}} \to Set$ *be a collection of couples* (R, ρ) *such that* $R \in \widehat{\mathcal{C}}$ *and* $\rho_R : G_v \to \mathrm{GL}_2(R)$ *is a representation with determinant* δ_v *and* $(\rho_R \bmod m_R) = \bar\rho$ *; and let* L_v *be a subspace of* $H^1(G_v, \mathrm{Ad}^0\bar\rho)$.
A pair (C_v, L_v) *is admissible if it satisfies the following properties :*
P1. $(\mathbb{F}, \bar\rho_v) \in C_v$.
P2. The set of lifts in C_v *to a fixed ring* R *is closed under conjugation by the subgroup* $\ker(\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbb{F}))$.
P3. If $(R, \rho) \in C_v$ *and if* $f : R \to S$ *is a morphism of elements of* $\widehat{\mathcal{C}}$, *then* $(S, f \circ \rho) \in C_v$.
P4. Let R_1 *and* R_2 *be in* $\mathcal{C}$. *Suppose that* $(R_1, \rho_1) \in C_v$ *and* $(R_2, \rho_2) \in C_v$. *Suppose also that* I_1 *is an ideal of* R_1 *and* I_2 *an ideal of* R_2 *such that there is an isomorphism* $\alpha : R_1/I_1 \to R_2/I_2$ *satisfying :* $\alpha(\rho_1 \bmod I_1) = (\rho_2 \bmod I_2)$. *Then* $(R_3, \rho_1 \oplus \rho_2) \in C_v$, *where* R_3 *is the fibred product* $R_1 \oplus_\alpha R_2$ *over the natural projections* $R_1 \to R_1/I_1 \xrightarrow{\alpha} R_2/I_2$ *and* $R_2 \to R_2/I_2$.
P5. Let (R, ρ) *be a deformation of* $\bar\rho_{|G_v}$. *If* $(R/(m_R)^n, \rho) \in C_v$ *for every* $n > 0$, *then* $(R, \rho) \in C_v$.

P6. Let $R \in \widehat{\mathcal{C}}$ and I be an ideal of R such that $m_R \cdot I = (0)$. If $(R/I, \rho) \in C_v$, then there exists a deformation ρ' of $\bar{\rho}_v$ to R such that $(R, \rho') \in C_v$ and $(\rho' \mod I) = \rho$.
P7. Let (R, ρ_1) and (R, ρ_2) be deformations of $\bar{\rho}_v$ with $(R, \rho_1) \in C_v$. Suppose that I is an ideal of R such that $m_R \cdot I = (0)$ and $(\rho_1 \ mod\ I) = (\rho_2 \ mod\ I)$. We will let $[\rho_2 - \rho_1]$ denote the element $g \mapsto \rho_2(g)\rho_1(g)^{-1} - 1$ of $H^1(G_v, \mathrm{Ad}^0\bar{\rho}) \otimes_{\mathbb{F}} I$. Then : $[\rho_2 - \rho_1] \in L_v \otimes_{\mathbb{F}} I$ if and only if $(R, \rho_2) \in C_v$.
Moreover, we say that C_v is admissible if it satisfies P1, $\cdots$, P6.

Remark 2.2.5. — *1) Properties P1, P2, P3 and P4 show that C_v can be seen as a functor which is a deformation condition for $\bar{\rho}_v$. For example, if P4 is satisfied by C_v, then so is the third item of Definition 1.4.1 with $R_1 = p_A(A \times_C B), R_2 = p_B(A \times_C B)$ and $I_i = \ker(R_i \to C)$, for $i = 1, 2$. We will identify C_v with the associated functor from $\widehat{\mathcal{C}}$ to Set; so C_v admits a versal ring.*
2) Property P5 means that $C_v : \widehat{\mathcal{C}} \to Set$ is a continuous functor.
3) Property P6 means that the versal ring of C_v is smooth over $\mathrm{W}(\mathbb{F})$. See [Sc, Remark 2.10] *for example.*

2.2.2.2. L_v and tangent spaces. — Every space L_v can be obtained in a systematic way as the tangent space of C_v. It is the object of Proposition 2.2.7, the proof of which is based on the following lemma.
Let us first explain the abuse of notations in the following lemma. Denote by $\mathbb{F}[I]$ the $\mathbb{F}$-vector space $\mathbb{F} \oplus I$. We identify φ with $\varphi(\epsilon)$ thanks to the isomorphism of $\mathbb{F}$-spaces :

$$\begin{array}{ccc} \mathrm{Hom}(\mathbb{F}[\epsilon], \mathbb{F}[I]) & \simeq & I \\ \varphi & \mapsto & \varphi(\epsilon). \end{array}$$

It holds for all $\rho_R \in \mathbf{Def}(\bar{\rho})(R)$: $\varphi(\epsilon)\rho_R = \varphi(\epsilon)\bar{\rho}$ (because $m_R \cdot I = (0)$).

Lemma 2.2.6. — *Let D be a deformation condition for the representation $\bar{\rho}_v = \bar{\rho}_{|G_v}$ and $F : \widehat{\mathcal{C}} \to Set$ be the functor*

$$F(R) = \boldsymbol{Def}_D(\bar{\rho})(R).$$

Then for all rings $R \in \widehat{\mathcal{C}}$ and all ideals I of R such that $m_R \cdot I = (0)$, the following map is surjective :

$$\begin{array}{ccc} F(R) \times (F(\mathbb{F}[\epsilon]) \otimes_{\mathbb{F}} I) & \longrightarrow & F(R) \times_{F(R/I)} F(R) \\ (\rho_1, (1 + \epsilon[c])\bar{\rho} \otimes \varphi) & \longmapsto & (\rho_1, (1 + \varphi(\epsilon)[c])\rho_1). \end{array}$$

Proof. — The map of the lemma is the composition $a_4 \circ a_3 \circ a_2 \circ a_1$ where the a_i's are defined below. So we need to show surjectivity of the following maps.
$$a_1 : \begin{cases} F(R) \times (F(\mathbb{F}[\epsilon]) \otimes_{\mathbb{F}} I) \to F(R) \times F(\mathbb{F}[I]) \\ (\rho_1, (1 + \epsilon[c])\bar{\rho} \otimes \varphi) \mapsto (\rho_1, (1 + \varphi(\epsilon)[c])\bar{\rho}) \end{cases}$$
The map a_1 is a bijection from Lemma 2.10 of [Sc].
$$a_2 : \begin{cases} F(R) \times F(\mathbb{F}[I]) \to F(R \times_{\mathbb{F}} \mathbb{F}[I]) \\ (\rho_1, \rho) \mapsto \rho_1 \oplus \rho \end{cases}$$
The map a_2 is a surjection from Theorem 2.11 and Remark (2.13) of [Sc]. Note that we can apply Theorem 2.11 since D is a deformation condition, so F admits a hull.

$a_3 : F(R \times_{\mathbb{F}} \mathbb{F}[I]) \to F(R \times_{R/I} R)$ is the bijection induces by the isomorphism (2.16) of [Sc] : $\begin{cases} R \times_{\mathbb{F}} \mathbb{F}[I] \to R \times_{R/I} R \\ r \oplus (x_0 + x) \mapsto r \oplus (x + r) \end{cases}$, where $x_0 + x$ means $x_0 \in \mathbb{F}$ and $x \in I$ according to $\mathbb{F}[I] = \mathbb{F} \oplus I$.
$a_4 : \begin{cases} F(R \times_{R/I} R) \to F(R) \times_{F(R/I)} F(R) \\ \rho_1 \oplus \rho_2 \mapsto (\rho_1, \rho_2) \end{cases}$
At last, the map a_4 is a surjection from Theorem 2.11 of [Sc]. □

Proposition 2.2.7. — *The tangent space of C_v satisfies property P7. From now on we will write L_v for*

$$\{[c] \in H^1(G_v, \mathrm{Ad}^0\bar{\rho}) \mid (1 + \epsilon[c])\bar{\rho} \in C_v(\mathbb{F}[\epsilon])\}.$$

Proof. — It is a direct consequence of Lemma 2.2.6. □

2.2.2.3. Selmer group and global tangent space. — We fix some useful notations for the next proposition.
The deformation functor of $\bar{\rho} : G_{K,S} \to \mathrm{GL}_2(\mathbb{F})$ is denoted by $\mathbf{Def}(\bar{\rho})$. The deformation functor of $\bar{\rho}_{|G_v} : G_v \to \mathrm{GL}_2(\mathbb{F})$ is denoted by $\mathbf{Def}(\bar{\rho})_v$. We fix a set of places S and pairs (C_v, L_v) such that C_v is a functor satisfying $P1, ..., P5$ and L_v is its tangent space, for each $v \in S$. Following the terminology recalled in [Bö 1, Definition 3.1], we see that C_v is a continuous functor which is relatively representable as a subfunctor of $\mathbf{Def}(\bar{\rho})_v$.
We study the deformations (R, ρ_R) of $\bar{\rho}$ whose restrictions at $v \in S$ are of type C_v, i.e. such that $(R, \rho_R) \in C_v$.

Definition 2.2.8. — *The functor associated to the local requirements C_v, denoted by $\boldsymbol{Def}(\bar{\rho})_{\{C_v\}}$, is the pullback in the following diagram*

$$\begin{array}{ccc} \boldsymbol{Def}(\bar{\rho})_{\{C_v\}} & \longrightarrow & \prod_{v \in S} C_v \\ \downarrow & & \downarrow \\ \boldsymbol{Def}(\bar{\rho}) & \longrightarrow & \prod_{v \in S} \boldsymbol{Def}(\bar{\rho})_v. \end{array}$$

Recall that $\mathrm{gen}(I) := \dim_{\mathbb{F}}(I/m_R \cdot I)$ for an ideal I in the ring R. We can state the following proposition.

Proposition 2.2.9. — [Bö 1, Prop 3.4, Theo 4.2]
1) The functor C_v admits a versal ring of deformation R_v.
2) $\boldsymbol{Def}(\bar{\rho})_{\{C_v\}}$ is representable by a ring denoted by $R_{\{C_v\}}$.
3) $H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho})$ is the tangent space of $\boldsymbol{Def}(\bar{\rho})_{\{C_v\}}$, where $L(S) = \bigoplus_{v \in S} L_v$.
4) Let J_v denote the ideal of relations of R_v for each $v \in S$, and $J_{\{C_v\}}$ denote the same for $R_{\{C_v\}}$. So, it holds

$$\mathrm{gen}(J_{\{C_v\}}) \leq \sum_{v \in S} \mathrm{gen}(J_v) + \dim_{\mathbb{F}} H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})^*(1)).$$

Proof. — Proof of 1) is well-known and originates from Theorem 1.4.5 ; 2) corresponds to [Bö 1, Prop 3.4] and 4) to [Bö 1, Theo 4.2]. Point 3) is a consequence of the definition of tangent spaces of functors in the diagram which defines $\mathbf{Def}(\bar{\rho})_{\{C_v\}}$. Note that, of course, the proof of [Bö 1, Theo 4.2] uses the Poitou-Tate exact sequence. □

2.2.3. Smoothness and lift. — Recall that $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ is unramified outside S. The following proposition represents a key result proved in [Ta 1], it is based on an interpretation of the Poitou-Tate exact sequence (recalled in Theorem 2.2.3) with *P5* and *P6*. That is the proof of [Ta 1, Lemma 1.1]. We propose an alternative proof thanks to the inequality in Proposition 2.2.9.

Proposition 2.2.10. — *For each $v \in S$, let (C_v, L_v) be an admissible pair such that $\bar{\rho}_{|G_v} \in C_v(\mathbb{F})$. If $H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1)) = (0)$, then there exists a deformation $(\mathrm{W}(\mathbb{F}), \rho)$ of $\bar{\rho}$ which is S-ramified and such that $\rho_{|G_v} \in C_v(\mathrm{W}(\mathbb{F}))$, for all places $v \in S$.*

Proof. — The functors C_v are smooth by *P6*, thus their ideals of relations J_v are trivial. We conclude, with item 4 of Proposition 2.2.9, that the ideal of relations $J_{\{C_v\}}$ is also trivial and so $R_{\{C_v\}}$ is a power series ring over $\mathrm{W}(\mathbb{F})$ in $\dim_{\mathbb{F}} H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho})$ variables. □

2.2.4. Example : tamely ramified lift. — In this subsection, we fix a finite place w of K which is not above p.

Lemma 2.2.11. — *Let $\bar{\rho}_w : G_w \to \mathrm{GL}_2(\mathbb{F})$ be an unramified representation with $w \nmid p$. Then the lifts of $\bar{\rho}_w$ are tamely ramified.*

Proof. — Let (R, ρ_R) be a lift of $(\mathbb{F}, \bar{\rho}_w)$. Note that, since $\bar{\rho}_w$ is unramified, one gets $\rho_R(I_w) \subseteq \ker(\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbb{F}))$. But the kernel $\ker(\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbb{F}))$ is the projective limit of the p-groups $\ker(\mathrm{GL}_2(R/{m_R}^n) \to \mathrm{GL}_2(\mathbb{F}))$ for $n \geq 1$, so it is a pro-p-group. □

We recall Example E3 given in [Ta 1]. The lifts involved will be used for the prime in $T - S$ from Theorem B.
Suppose that $w \nmid p$, that either $Nw \not\equiv 1 \mod p$ (where Nw is the cardinal of the residue field of K_w) or $p \mid |\bar{\rho}(G_w)|$.
Assume that

$$\bar{\rho}_{|G_w} \simeq \begin{pmatrix} \chi_p\bar{\chi} & * \\ 0 & \bar{\chi} \end{pmatrix}, \text{ with respect to some basis } e_1, e_2 \text{ of } \mathbb{F}^2.$$

Take C_w^t to be the class of deformations of $\bar{\rho}_{|G_w}$ of the form

$$\begin{pmatrix} \chi_p\chi & * \\ 0 & \chi \end{pmatrix}, \text{ where } \chi \text{ lifts } \bar{\chi}.$$

Take L_w^t to be the tangent space of C_w^t, and denote by $\mathrm{Hom}(\mathbb{F}e_2, \mathbb{F}e_1)$ the submodule of $\mathrm{Ad}^0\bar{\rho}$ formed by the matrices $\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$.

Lemma 2.2.12. — [Ta 1, Section 1 (E3)] *Under the above assumptions, the following properties hold.*
1) The pair (C_w^t, L_w^t) *is admissible.*
2) The space L_w^t *is equal to*

$$\mathrm{im}\left(H^1(G_w, \mathrm{Hom}(\mathbb{F}e_2, \mathbb{F}e_1)) \to H^1(G_w, \mathrm{Ad}^0\bar{\rho})\right)$$

and

$$\dim_{\mathbb{F}} L_w^t = \dim_{\mathbb{F}} H^1(G_w/I_w, \mathrm{Ad}^0\bar{\rho}).$$

2.3. The admissible pair (C_v^{neo}, L_v^{neo})

Let S be equal to S_p, the set of all places of K above p. For each $v \in S$, let $\bar{\rho}_v : G_v \to \mathrm{GL}_2(\mathbb{F})$ be a continuous representation. Assume that

$$\bar{\rho}_v \text{ is nearly extraordinary, for every } v \in S.$$

This means that, for each $v \in S$, there exists a basis in which $\bar{\rho}_v = \chi_{v,1} \oplus \chi_{v,2}$, where $\chi_{v,i}$ are two characters (see Definition 2.1.2). We fix such basis.
By abuse of notation, we omit the reference to v and denote by χ_i the characters instead of $\chi_{v,i}$.
Assume also that

$$\chi_1\chi_2^{-1} \notin \{1, \chi_p, \chi_p^{-1}\}.$$

Definition 2.3.1. — *For each* $v \in S$, *let* (C_v^{neo}, L_v^{neo}) *be the following pair*

$$C_v^{neo}(A) = \boldsymbol{Def}(\bar{\rho})_{neo}(\bar{\rho}_v, A), \text{ with } A \in \widehat{\mathcal{C}}.$$

i.e.

$$C_v^{neo}(A) = \{[\rho_A] | (\rho_A \bmod m_A = \bar{\rho}_v), \rho_A \simeq \phi_1 \oplus \phi_2, \text{ where } \phi_i \text{ are characters}\}.$$

and

$$L_v^{neo} = \{[c] \in H^1(G_v, \mathrm{Ad}^0\bar{\rho}) | (1 + \epsilon[c])\bar{\rho} \in C_v^{neo}(\mathbb{F}[\epsilon])\}.$$

Let $\mathrm{Diag}(\mathrm{Ad}^0\bar{\rho})$ denote the sub-$\mathbb{F}[G_v]$-module of $\mathrm{Ad}^0\bar{\rho}$ of diagonal matrices. The aim of this section is to prove the next two results.

Proposition 2.3.2. — *The following properties hold.*
1) The functor C_v^{neo} *satisfies* $P1, \ldots, P5$, *for each* $v \in S$.
2) Assume that $\mu_p \nsubseteq K_v$, *for* $v \in S$. *Then the pair* (C_v^{neo}, L_v^{neo}) *is admissible.*
3) One has

$$L_v^{neo} = H^1(G_v, \mathrm{Diag}(\mathrm{Ad}^0\bar{\rho})).$$

Thus

$$\dim_{\mathbb{F}} L_v^{neo} = [K_v : \mathbb{Q}_p] + 1 + \delta(\mu_p(K_v)),$$

where $\delta(\mu_p(K_v)) = 1$ *if* $\mu_p \subseteq K_v$ *and* 0 *otherwise.*

Remark 2.3.3. — *In* [Oh, Lemma 1.6.], *it is proved that* C_v^{neo} *satisfies P4 in a different way.*

The proof is performed in two steps. In section 2.3.1, parts 1) and 2) of Proposition 2.3.2 are proved. Afterwards, we will study the structure of the module $\mathrm{Ad}^0\bar{\rho}$ for the action of G_v and we will give the dimensions of the spaces L_v^{neo} in section 2.3.2.2. Before this, we give a direct consequence of Proposition 2.3.2 needing the following definition.

Definition 2.3.4. — *$\delta_1(\bar{\rho})$ is the number of places in $Pl_\infty(K)$ which are even for $\bar{\rho}$, and $\delta_{-1}(\bar{\rho})$ is the analogous number for odd places in $Pl_\infty(K)$.*
When K is totally real, $\bar{\rho}$ is totally odd when $[K:\mathbb{Q}] = \delta_{-1}(\bar{\rho})$.

Corollary 2.3.5. — *We fix $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ which is unramified outside $S = S_p$.*
Then

$$\sum_{v\in S} \dim_{\mathbb{F}} L_v^{neo} \geq \sum_{v\in S\cup Pl_\infty(K)} \dim_{\mathbb{F}} H^0(G_v, \mathrm{Ad}^0\bar{\rho})$$

is equivalent to

$$[K:\mathbb{Q}] + \sum_{v\in S} \delta(\mu_p(K_v)) \geq 3\delta_1(\bar{\rho}) + \delta_{-1}(\bar{\rho}).$$

Proof. — One has $\dim_{\mathbb{F}} H^0(G_v, \mathrm{Ad}^0\bar{\rho}) = 1$ for each $v \in S$, and

$$\dim_{\mathbb{F}} H^0(G_v, \mathrm{Ad}^0\bar{\rho}) = 1, \text{ for every odd place } v \in Pl_\infty(K),$$
$$\dim_{\mathbb{F}} H^0(G_v, \mathrm{Ad}^0\bar{\rho}) = 3, \text{ for every even place } v \in Pl_\infty(K).$$

This implies the desired equivalence. □

2.3.1. About C_v^{neo}. — The following key lemma, whose proof is quite computational, gives us a nice matrix representation of elements in C_v^{neo}. This representation is unique in the following sense :

Lemma 2.3.6. — *1) Assume that $\rho \in C_v^{neo}(A)$, where $A \in \widehat{\mathcal{C}}$.*
Then there exists a representative of ρ of the form

$$M^{-1}\begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix} M, \text{ with } M = \begin{pmatrix} 1 & y \\ z & 1 \end{pmatrix} \text{ and } y, z \in m_A.$$

2) Let $\rho_1 = M_1^{-1}\begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix} M_1$ and $\rho_2 = M_2^{-1}\begin{pmatrix} \psi_1' & 0 \\ 0 & \psi_2' \end{pmatrix} M_2$ two lifts of $\bar{\rho}_v$ to $A \in \widehat{\mathcal{C}}$,
where $M_i = \begin{pmatrix} 1 & y_i \\ z_i & 1 \end{pmatrix}$ and $y_i, z_i \in m_A$, for $i \in \{1,2\}$.
Let $g \in G_v$ and assume that :
(i) $\rho_1(g) = \rho_2(g)$,
(ii) $\bar{\rho}_v(g)$ is not scalar matrix.
Then

$$M_1 = M_2 \text{ and } \psi_i(g) = \psi_i'(g) \text{ for } i \in \{1,2\}.$$

Proof. — 1) Since $\rho \in C_v^{neo}(A)$, there exists two characters ψ_1, ψ_2 such that $\rho \simeq \psi_1 \oplus \psi_2$. We define the following sets :

$$\mathrm{Com}(\rho) = \{M \in \mathrm{GL}_2(A) \mid M\begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix} M^{-1} = \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix}\},$$

$$\mathrm{B}(\rho) = \{M \in \mathrm{GL}_2(A) \mid M\rho M^{-1} = \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix}\}.$$

Since $\psi_1 \neq \psi_2$, the subgroup $\mathrm{Com}(\rho)$ is equal to the subgroup of diagonal matrices of $\mathrm{GL}_2(A)$. Next, note that $\mathrm{Com}(\rho)$ acts on the left on $\mathrm{B}(\rho)$ by multiplication. Describing the orbit of a matrix $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathrm{B}(\rho)$ under this action, we deduce part 1).

2)Let $a = \psi_1(g), b = \psi_2(g), c = \psi_1'(g)$ and $d = \psi_2'(g)$.
Part (i) implies that $a + b = c + d$ and $ab = cd$. Hence, $ab = a(c + d - a)$ and then $(a - c)(a - d) = 0$. But $(a - d) \in A^\times$ from hypotheses (i) and (ii). This shows that $a = c$ and it follows that $b = d$. Now, we prove the equality $M_1 = M_2$. We get $y_1(a-b)(1-y_2z_2) = y_2(a-b)(1-y_1z_1)$ comparing the antidiagonal of the matrices $M_1^{-1}N_1M_1$ and $M_2^{-1}N_2M_2$, and we get $(a-b)y_1z_1 = (a-b)y_2z_2$ comparing the diagonal of the same matrices. Thanks to (ii), $(a-b) \in A^\times$. It follows that $y_1(1 - y_2z_2) = y_2(1 - y_1z_1)$, $y_1z_1 = y_2z_2$ and $y_1 = y_2$. The same way, we obtain $z_1 = z_2$. □

Lemma 2.3.7. — *C_v^{neo} satisfies P1, P2, P3 and P5.*

Proof. — It is easy to see that C_v^{neo} satisfies *P1*, *P2* and *P3*.
For *P5*, we work with the expression given in Lemma 2.3.6 for each $\rho_n = (\rho \, mod \, R/(m_R)^n)$:

$$\rho_n = M_n^{-1} \begin{pmatrix} \psi_n & 0 \\ 0 & \varphi_n \end{pmatrix} M_n$$

where $M_n = \begin{pmatrix} 1 & y_n \\ z_n & 1 \end{pmatrix}$. The projective limit of the ρ_n exists thanks to item 2) of Lemma 2.3.6 and is equal to ρ. Thus, C_v^{neo} satisfies property *P5*.

□

Lemma 2.3.8. — *Property of fibred products P4 stands for C_v^{neo}.*

Proof. — We will use Lemma 2.3.6. Let (R_1, ρ_1) and (R_2, ρ_2) be as in *P4*, and show that $(R_3, \rho_1 \oplus \rho_2) \in C_v^{neo}(R_3)$, in keeping notations of Definition 2.2.4.
As $(R_i, \rho_i) \in C_v^{neo}(R_i)$, we know from 2.3.6 there exists $y_i, z_i \in m_{R_i}$ such that

$$\rho_i = M_i \begin{pmatrix} \psi_{i,1} & 0 \\ 0 & \psi_{i,2} \end{pmatrix} M_i^{-1}$$

where

$$M_i = \begin{pmatrix} 1 & y_i \\ z_i & 1 \end{pmatrix} \text{ and } (\psi_{i,j} \, mod \, m_{R_i}) = \chi_j.$$

We have to find $X \in \mathrm{GL}_2(R_1)$ and two characters $(\phi_1 \oplus \phi_2), (\varphi_1 \oplus \varphi_2)$ with values in $R_3^\times$ satisfying :

$$(M_1X \oplus M_2) \in \mathrm{GL}_2(R_3)$$
$$\text{and } \rho_1 \oplus \rho_2 = (M_1X \oplus M_2) \begin{pmatrix} \phi_1 \oplus \phi_2 & 0 \\ 0 & \varphi_1 \oplus \varphi_2 \end{pmatrix} (M_1X \oplus M_2)^{-1}.$$

We search for an $X \in \mathrm{GL}_2(R_1)$ which commutes with $\begin{pmatrix} \psi_{1,1} & 0 \\ 0 & \psi_{1,2} \end{pmatrix} \, mod \, I_1$ and such that $\alpha(M_1X \, mod \, I_1) = (M_2 \, mod \, I_2)$. Up to conjugate $(\rho_1 \, mod \, I_1)$ by $\alpha^{-1}(M_2 \, mod \, I_2)$, we can assume that $(M_2 \, mod \, I_2) = Id$, i.e.

$$(\rho_2 \, mod \, I_2) = \begin{pmatrix} \psi_{2,1} & 0 \\ 0 & \psi_{2,2} \end{pmatrix} \, mod \, I_2.$$

From now on, we omit the reference to α. Since $(\rho_1 \ mod\ I_1) = (\rho_2 \ mod\ I_2)$, we get :

$$(1-y_1z_1)^{-1}\begin{pmatrix} \psi_{1,1}-y_1z_1\psi_{1,2} & y_1(\psi_{1,1}-\psi_{1,2}) \\ z_1(\psi_{1,2}-\psi_{1,1}) & \psi_{1,2}-y_1z_1\psi_{1,1} \end{pmatrix} \ mod\ I_1$$

$$= \begin{pmatrix} \psi_{2,1} & 0 \\ 0 & \psi_{2,2} \end{pmatrix} \ mod\ I_2.$$

Since $\psi_{1,1} \neq \psi_{1,2}\ (mod\ m_{R_1})$, it holds

$$y_1, z_1 \in I_1 \text{ and } (\psi_{1,j} \ mod\ I_1) = (\psi_{2,j} \ mod\ I_2).$$

We can conclude with the following suitable choice

$$X = Id, \phi_1 \oplus \phi_2 = \psi_{1,1} \oplus \psi_{2,1} \text{ and } \varphi_1 \oplus \varphi_2 = \psi_{1,2} \oplus \psi_{2,2}.$$

□

Remark 2.3.9. — *Note that the choice of X is quite immediate here thanks to Lemma 2.3.6 ; we give the details of the proof to illustrate the usual approach for P4.*

Lemma 2.3.10. — *If $\mu_p \nsubseteq K_v$, then C_v^{neo} satisfies P6.*

Proof. — If $\mu_p \nsubseteq K_v$, then the versal ring of C_v^{neo} is smooth over $\mathrm{W}(\mathbb{F})$ (see Example 1.3.21). Property *P6* is established for C_v^{neo} thanks to Remark 2.2.5. □

2.3.2. The tangent space L_v^{neo}. —

2.3.2.1. The Galois modules $\mathrm{Ad}^0\bar{\rho}$ *and* $(\mathrm{Ad}^0\bar{\rho})(1)$. — The G_K-equivariant and perfect pairing

$$\begin{array}{ccc} \mathrm{Ad}^0\bar{\rho} \times \mathrm{Ad}^0\bar{\rho} & \to & \mathbb{F} \\ (A,B) & \mapsto & \mathrm{Tr}(AB) \end{array}$$

shows that the representation $\mathrm{Ad}^0\bar{\rho}$ is self-dual : $\mathrm{Ad}^0\bar{\rho} \simeq (\mathrm{Ad}^0\bar{\rho})^*$, where $(\mathrm{Ad}^0\bar{\rho})^* = \mathrm{Hom}(\mathrm{Ad}^0\bar{\rho}, \mathbb{F})$. For $i \in \{0,1,2\}$, Proposition 2.2.1 states that

$$H^i(G_v, \mathrm{Ad}^0\bar{\rho}) \times H^{2-i}(G_v, (\mathrm{Ad}^0\bar{\rho})(1)) \to H^2(G_v, \mathbb{F}(1)) \simeq \mathbb{F}.$$

We will describe the cohomology of the module $\mathrm{Ad}^0\bar{\rho}$.

Proposition 2.3.11. — *1) As $\mathbb{F}[G_v]$-modules :*

$$\mathrm{Ad}^0\bar{\rho} \simeq \mathbb{F} \oplus \mathbb{F}(\chi_1^{-1}\chi_2) \oplus \mathbb{F}(\chi_1\chi_2^{-1}).$$

2) The following holds :

$$H^0(G_v, \mathrm{Ad}^0\bar{\rho}) = \mathrm{Diag}(\mathrm{Ad}^0\bar{\rho}) \simeq \mathbb{F},$$

$$\dim_{\mathbb{F}} H^2(G_v, \mathrm{Ad}^0\bar{\rho}) = \delta(\mu_p(K_v)),$$

and

$$\dim_{\mathbb{F}} H^1(G_v, \mathrm{Ad}^0\bar{\rho}) = 1 + \delta(\mu_p(K_v)) + 3\ [K_v : \mathbb{Q}_p].$$

Proof. — The proof of 1) is immediate. We recall that $\chi_1\chi_2^{-1} \notin \{1, \chi_p, \chi_p^{-1}\}$. Thus, with 1), it holds $H^0(G_v, \mathrm{Ad}^0\bar{\rho}) = \mathrm{Diag}(\mathrm{Ad}^0\bar{\rho}) \simeq \mathbb{F}$. By local duality, the group $H^2(G_v, \mathrm{Ad}^0\bar{\rho})$ is the Pontryagin dual of $H^0(G_v, (\mathrm{Ad}^0\bar{\rho})')$, with $(\mathrm{Ad}^0\bar{\rho})' = \mathrm{Hom}((\mathrm{Ad}^0\bar{\rho}), \mu_p)$.
Thanks to 1), one has $(\mathrm{Ad}^0\bar{\rho})' \simeq \mathbb{F}(\chi_p) \oplus \mathbb{F}(\chi_1^{-1}\chi_2\chi_p) \oplus \mathbb{F}(\chi_1\chi_2^{-1}\chi_p)$; the group G_v acts on $(\mathrm{Ad}^0\bar{\rho})'$ in the following way, with $\sigma \in G_v$ and $f \in (\mathrm{Ad}^0\bar{\rho})'$:

$$(\sigma \cdot f)(m_1) = f(m_1)^{\chi_p(\sigma)},$$

$$(\sigma \cdot f)(m_2) = f(m_2)^{(\chi_1^{-1}\chi_2\chi_p)(\sigma)} \text{ and } (\sigma \cdot f)(m_3) = f(m_3)^{(\chi_2^{-1}\chi_1\chi_p)(\sigma)},$$

where $m_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $m_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $m_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. If the action of G_v on μ_p is trivial, then $\dim_{\mathbb{F}} H^0(G_v, (\mathrm{Ad}^0\bar{\rho})') = 1$, otherwise the space H^0 is trivial. We deduce the dimension of H^1 with the local Euler-Poincaré characteristic. □

2.3.2.2. Proof of item 3) in Proposition 2.3.2. — Thanks to Lemma 2.3.6 and to Proposition 2.3.11, it follows that

$$L_v^{neo} = H^1(G_v, \mathrm{Diag}(\mathrm{Ad}^0\bar{\rho})),$$

$$\text{i.e. } L_v^{neo} = \mathrm{Hom}(G_v/([G_v, G_v]G_v^p), \mathbb{F}).$$

By local class field theory, one gets

$$\dim_{\mathbb{F}} L_v^{neo} = [K_v : \mathbb{Q}_p] + 1 + \delta(\mu_p(K_v)),$$

where $\delta(\mu_p(K_v)) = 1$ if $\mu_p \subseteq K_v^\times$ and 0 otherwise. □

2.3.3. About C_v^{eo}. — In this subsection, we speak about the links between our work and the article [Oh]. Let $S = S_p$. We fix $\bar{\rho}_{eo} : G_{K,S} \to \mathrm{GL}_2(\mathbb{F})$ which is extraordinary in v, for all $v \in S$. In [Oh], Ohtani studied the functor which parametrizes the S-ramified and extraordinary in v deformations of $\bar{\rho}_{eo}$. Here, we impose an additional and minor condition by fixing derminant of such deformations. The functor associated to all these requirements is denoted by $\mathrm{Def}_{\{C_v^{eo}\}}$. By definition, it is the pullback in the following diagram

$$\begin{array}{ccc} \mathrm{Def}_{\{C_v^{eo}\}} & \longrightarrow & \prod_{v\in S} C_v^{eo} \\ \downarrow & & \downarrow \\ \mathrm{Def}(\bar{\rho}_{eo}) & \longrightarrow & \prod_{v\in S} \mathrm{Def}_v(\bar{\rho}_{eo|G_v}), \end{array}$$

where $\mathrm{Def}(\bar{\rho}_{eo})$ is the deformation functor of $\bar{\rho}_{eo}$, $\mathrm{Def}_v(\bar{\rho}_{eo|G_v})$ the same for $\bar{\rho}_{eo|G_v}$ and C_v^{eo} its subfunctor which parametrizes the extraordinary deformations of $\bar{\rho}_{eo|G_v}$.
Let $L_v^{eo} = \{[c] \in H^1(G_v, \mathrm{Ad}^0\bar{\rho}) | (1 + \epsilon[c])\bar{\rho}_{eo} \in C_v^{eo}(\mathbb{F}[\epsilon])\}$.

Proposition 2.3.12. — *The following properties hold.*
1) If $\mu_p \nsubseteq K_v$, for $v \in S$, then the pair (C_v^{eo}, L_v^{eo}) is admissible.
2) One has $L_v^{eo} = H^1(G_v/I_v, \mathrm{Diag}(\mathrm{Ad}^0\bar{\rho}))$ and $\dim_{\mathbb{F}} L_v^{eo} = 1$ for all $v \in S$.
3) We have the following equality

$$\sum_{v\in S} \dim_{\mathbb{F}} L_v^{eo} - \sum_{v\in S\cup Pl_\infty(K)} \dim_{\mathbb{F}} H^0(G_v, \mathrm{Ad}^0) = -(3\delta_1 + \delta_{-1}).$$

Proof. — For item 1), we just use Lemma 2.3.6 and Proposition 2.3.11 as for the proof of Proposition 2.3.2. Note that ψ_1 is unramified character in the extraordinary case. Items 2) and 3) are direct consequences thanks to Lemma 2.3.6. □

Proposition 2.3.12 implies the following inequality

$$\sum_{v\in S}\dim_{\mathbb{F}} L_v^{eo} < \sum_{v\in S\cup Pl_\infty(K)}\dim_{\mathbb{F}} H^0(G_v,\mathrm{Ad}^0).$$

Hence the initial hypothesis about the dimensions of tangent spaces in Propostion 2.4.4 fails, these tangent spaces are too small. It is due to the fact that ψ_1 is unramified character, which is too restrictive to use Taylor-Ramakrishna's method with the data (C_v^{eo}, L_v^{eo}). That is why we relax the assumption about the ramification of ψ_1 and work with (C_v^{neo}, L_v^{neo}) in Theorem B (see Corollary 2.3.5 for inequality about $\dim_{\mathbb{F}} L_v^{neo}$).

2.4. Main Theorem

In this section, thanks to Propositon 2.2.10 and 2.4.4, we prove Theorem B :

Theorem B. — *Let $\bar\rho : G_K \to \mathrm{GL}_2(\mathbb{F})$ be a continuous representation, unramified outside $S = S_p$, with $p \geq 5$. Assume that $\bar\rho$ is totally odd, nearly extraordinary in v for each $v \in S$ and that the image of $\bar\rho$ is full.*
Suppose that K is totally real and that $\mu_p \nsubseteq K_v$, for each $v \in S$.
Then there exists a deformation $(\mathrm{W}(\mathbb{F}), \rho)$ of $\bar\rho$ and a finite set of primes $T \supseteq S$ such that

$$\rho \text{ is } T\text{-ramified and } (\mathrm{W}(\mathbb{F}), \rho_{|G_v}) \in C_v^{neo}(\mathrm{W}(\mathbb{F})),$$

for all $v \in S_p$.

2.4.1. Strategy. — Let $\bar\rho : G_K \to \mathrm{GL}_2(\mathbb{F})$ be a continuous representation, unramified outside S.
The following strategy is due to Ramakrishna [Ra 2]. The mean idea is the following. We want to find a finite set T of places and $\{(C_v, L_v)\}_{v\in T}$ admissible pairs such that $H^1_{\{L(T)^\perp\}}(G_{K,T}, (\mathrm{Ad}^0\bar\rho)(1)) = (0)$, where $L(T) = \bigoplus_{v\in T} L_v$; in that case, we know (thanks to Proposition 2.2.10) that there exists a deformation $(\mathrm{W}(\mathbb{F}), \rho)$ of $\bar\rho$ such that $\rho_{|G_v} \in C_v(\mathrm{W}(\mathbb{F}))$, for all $v \in T$. So we want to make trivial a Selmer group by adding some primes to S in order to apply Proposition 2.2.10. We will be more specific.
Subsections 2.4.4 and 2.4.3 describe some estimations of the places w (when $K = \mathbb{Q}$) introduced in the following description.

1) a) If $H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar\rho)(1))$ is already trivial, we use Proposition 2.2.10 and then there exists a deformation $(\mathrm{W}(\mathbb{F}), \rho)$ of $\bar\rho$ such that $\rho_{|G_v} \in C_v(\mathrm{W}(\mathbb{F}))$, for all $v \in S$. We take $T = S$ and $(\mathrm{W}(\mathbb{F}), \rho)$ in Theorem B where C_v stands for C_v^{neo}.
b) Otherwise, assume that $H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar\rho)(1)) \neq (0)$. Write ϕ a non-trivial element in $H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar\rho)(1))$. Let w be a place not in S and $L_w^\perp$ be a subspace of $H^1(G_w, (\mathrm{Ad}^0\bar\rho)(1))$. The following natural sequence is exact

$$\begin{aligned}0 \to\ & H^1_{\{L(S)^\perp\oplus L_w^\perp\}}(G_{K,S\cup\{w\}}, (\mathrm{Ad}^0\bar\rho)(1)) \\ & \to H^1_{\{L(S)^\perp\oplus H^1(G_w,(\mathrm{Ad}^0\bar\rho)(1))\}}(G_{K,S\cup\{w\}}, (\mathrm{Ad}^0\bar\rho)(1)) \to\ H^1(G_w, \mathrm{Ad}^0\bar\rho(1))/L_w^\perp\ .\end{aligned}$$

We want to find a place w depending on the pair $(L(S)^{\perp}, G_{K,S})$ such that :
(i) $H^1_{\{L(S)^{\perp}\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1)) = H^1_{\{L(S)^{\perp}\oplus H^1(G_w,(\mathrm{Ad}^0\bar{\rho})(1)\}}(G_{K,S\cup\{w\}}, (\mathrm{Ad}^0\bar{\rho})(1))$,
(ii) the image of ϕ in $H^1(G_w, \mathrm{Ad}^0\bar{\rho}(1))/L_w^{\perp}$ is nonzero.

2) Now we discuss the the above equality in (i). Note that

$$\ker(H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho}) \to H^1(G_w/I_w, \mathrm{Ad}^0\bar{\rho})) = H^1_{\{L(S)\}}(G_{K,S\cup\{w\}}, \mathrm{Ad}^0\bar{\rho}),$$

where the map considered in the kernel is the natural restriction.
Point 3) in Theorem 2.2.3 implies that

$$\frac{|H^1_{\{L(S)^{\perp}\oplus H^1(G_w,(\mathrm{Ad}^0\bar{\rho})(1)\}}(G_{K,S\cup\{w\}}, (\mathrm{Ad}^0\bar{\rho})(1))|}{|H^1_{\{L(S)^{\perp}\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1))|}$$

$$= \frac{|H^1_{\{L(S)\}}(G_{K,S\cup\{w\}}, \mathrm{Ad}^0\bar{\rho})|}{|H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho})|}|H^1(G_w/I_w, \mathrm{Ad}^0\bar{\rho})|.$$

So the above equality in (i) holds if and only if
(i)' the natural restriction $H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho}) \to H^1(G_w/I_w, \mathrm{Ad}^0\bar{\rho})$ is surjective.

We see that we search for a place w such that (i)' and (ii) hold. Note that for simplicity we focus on place w such that $H^1(G_w/I_w, \mathrm{Ad}^0\bar{\rho})$ is a one dimensional space over $\mathbb{F}$. We prove such a w exists in Lemma 2.4.3.

3) We continue in this fashion obtaining, after a finite number of iterations, a finite set of places $T = S \cup \{w_1, ..., w_t\}$ such that

$$H^1_{\{L(T)^{\perp}\}}(G_{K,T}, \mathrm{Ad}^0\bar{\rho}(1)) = (0)$$

where $t \leq \dim_{\mathbb{F}} H^1_{\{L(S)^{\perp}\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1))$ and $L(T)^{\perp} = (\bigoplus_{v\in S} L_v^{\perp}) \oplus L_{w_1}^{\perp} \oplus ... \oplus L_{w_t}^{\perp}$.

2.4.2. Proofs : cohomology and Cebotarev. — We need the following lemmas to prove Proposition 2.4.4. The method is in the spirit of [Ta 1]. We give the details of the proofs of two lemmas for the convenience of the reader.
Let $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ denote a representation unramified outside $S = S_p$. Assume also that $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{im}(\bar{\rho})$.
The image of $\mathrm{PGL}(\bar{\rho})$ is not solvable, since it contains $\mathrm{PGL}_2(\mathbb{F})$, with $p \geq 5$. It implies that $\mathrm{Ad}^0\bar{\rho}$ and $(\mathrm{Ad}^0\bar{\rho})(1)$ are absolutely irreducible $\mathbb{F}[G_{K,S}]$-modules (see, e.g., [Ra 1, Lemma 17]).

Lemma 2.4.1. — [DDT, lemma 2.48] *Denote by $K(\mathrm{Ad}^0\bar{\rho})$ the extension of K cuts out by $\ker \mathrm{PGL}(\bar{\rho})$ and by E the Galois extension $K(\mathrm{Ad}^0\bar{\rho})K(\mu_p)$ over K. Assume that $p \geq 5$. Then*

$$H^1(\mathrm{Gal}(E/K), \mathrm{Ad}^0\bar{\rho}) = (0) \text{ and } H^1(\mathrm{Gal}(E/K), (\mathrm{Ad}^0\bar{\rho})(1)) = (0).$$

Lemma 2.4.2. — *Assume that $p \geq 5$. Let L and L' represent two affine proper subspaces inside $(\mathrm{Ad}^0\bar{\rho})(1)$ and $\mathrm{Ad}^0\bar{\rho}$ respectively. Assume that $\phi \in H^1_{\{L(S)^{\perp}\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1))$ and $\psi \in H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho})$ are nonzero elements. By abuse, we denote also by ϕ and ψ their associated cocycles.*

Then there exists $g \in \mathrm{Gal}(E(\phi)E(\psi)/E)$ *such that*

$$\phi(g) \notin L \text{ and } \psi(g) \notin L'.$$

Proof. — Lemma 2.4.1 states the restrictions to $\mathrm{Gal}(K_S/E)$ of the 1-cocycles ϕ and ψ are morphisms, also denoted by $\phi : \mathrm{Gal}(K_S/E) \to (\mathrm{Ad}^0\bar{\rho})(1)$ and $\psi : \mathrm{Gal}(K_S/E) \to \mathrm{Ad}^0\bar{\rho}$. The subfields fixed by these morphisms are denoted by $E(\phi)$ and $E(\psi)$ respectively. Note that the abelian extensions $E(\phi)/E$ and $E(\psi)/E$ are non-trivial since the cocyles are nonzero and so are the morphims. The $\mathbb{F}[G_{K,S}]$-modules $\mathrm{Ad}^0\bar{\rho}$ and $(\mathrm{Ad}^0\bar{\rho})(1)$ are irreducible since $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{im}(\bar{\rho})$. Hence, the following $\mathrm{Gal}(E/K)$-equivariant injections

$$\mathrm{Gal}(E(\phi)/E) \to (\mathrm{Ad}^0\bar{\rho})(1) \text{ and } \mathrm{Gal}(E(\psi)/E) \to \mathrm{Ad}^0\bar{\rho}$$

are isomorphisms. We now need to distinguish two cases.

(i) Assume that the $\mathbb{F}[G_{K,S}]$-modules $\mathrm{Ad}^0\bar{\rho}$ and $(\mathrm{Ad}^0\bar{\rho})(1)$ are not isomorphic.
Hence, the extensions $E(\phi)$ and $E(\psi)$ are disjoint over E ; the group

$$\mathrm{Gal}(E(\phi)E(\psi)/E) = \mathrm{Gal}(E(\phi)/E) \times \mathrm{Gal}(E(\psi)/E)$$

admits a $\mathbb{F}[\mathrm{Gal}(E/K)]$-module structure, and it surjects on $(\mathrm{Ad}^0\bar{\rho})(1) \times \mathrm{Ad}^0\bar{\rho}$.

(ii) Assume that the $\mathbb{F}[G_{K,S}]$-modules $\mathrm{Ad}^0\bar{\rho}$ and $(\mathrm{Ad}^0\bar{\rho})(1)$ are isomorphic.
As $\mathrm{Ad}^0\bar{\rho}$ is irreducible, it holds $E(\phi) = E(\psi)$. Since $|\mathbb{F}| > 2$, one has $|\phi^{-1}(L) \cup \psi^{-1}(L')| \leq 2|\mathbb{F}|^2 < |\mathrm{Gal}(E(\phi)/E)|$ and so we are done.

□

Thanks to Lemma 2.4.1, to Lemma 2.4.2 and to Cebotarev density theorem, we obtain the following classical result. We recall that the pair (C_w^t, L_w^t) is defined in Subsection 2.2.4.

Lemma 2.4.3. — *Let* $p \geq 5$. *Let* (C_v, L_v) *be admissible for each* $v \in S$.
If $\phi \in H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1))$ *and* $\psi \in H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho})$ *are nonzero, then there exists* $w \notin S$ *such that* (C_w^t, L_w^t) *is admissible for* $\bar{\rho}_{|G_w}$, *such that* $\chi_p(\mathrm{Frob}_w) = 1$ *and such that :*
1) ϕ *does not map to zero in* $H^1(G_w, (\mathrm{Ad}^0\bar{\rho})(1))/{L_w^t}^\perp$,
2) ψ *does not map to zero in* $H^1(G_w/I_w, \mathrm{Ad}^0\bar{\rho})$,
3) $\dim_{\mathbb{F}} L_w^t = \dim_{\mathbb{F}} H^1(G_w/I_w, \mathrm{Ad}^0\bar{\rho}) = 1$.

Proof. — The image of the map

$$\mathrm{PGL}(\bar{\rho}) \times \chi_p : G_{K,S} \to \mathrm{PGL}_2(\mathbb{F}) \times \mathbb{F}^\times$$

contains the product $\mathrm{PSL}_2(\mathbb{F}) \times \chi_p(G_{K,S})$. Indeed $|\mathbb{F}| \geq 5$, and so, the derivative subgroup $[\mathrm{PSL}_2(\mathbb{F}), \mathrm{PSL}_2(\mathbb{F})]$ is equal to the whole group $\mathrm{PSL}_2(\mathbb{F})$. This implies that $\mathrm{PGL}(\bar{\rho})(\ker \chi_p) \supseteq \mathrm{PGL}(\bar{\rho})([G_{K,S}, G_{K,S}]) \supseteq \mathrm{PSL}_2(\mathbb{F})$.
We fix some basis e_1, e_2 of $\mathbb{F}^2$. We now take $\alpha \in G_{K,S}$ such that

$$\mathrm{PGL}(\bar{\rho})(\alpha) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \chi_p(\alpha) = 1.$$

We work in the Galois extension $E(\psi)E(\phi)/K$ and identify α and its projection in $\mathrm{Gal}(E(\psi)E(\phi)/K)$. Take L to be

$$((\mathrm{Hom}(\mathbb{F}e_1, \mathbb{F}e_1) \oplus \mathrm{Hom}(\mathbb{F}e_2, \mathbb{F}e_2)) \cap \mathrm{Ad}^0\bar{\rho})(1) \oplus \mathrm{Hom}(\mathbb{F}e_2, \mathbb{F}e_1)(1),$$

and take L' to be

$$\mathrm{Hom}(\mathbb{F}e_1, \mathbb{F}e_2) \oplus \mathrm{Hom}(\mathbb{F}e_2, \mathbb{F}e_1).$$

By Lemma 2.4.2, there exists $g \in \mathrm{Gal}(E(\phi)E(\psi)/E)$ such that

$$\phi(g) + \phi(\alpha) \notin L \text{ and } \psi(g) + \psi(\alpha) \notin L'.$$

From Cebotarev density theorem, we know that there exists a place $w \notin S$ unramified in the extension $E(\psi)E(\phi)/K$ and such that $\mathrm{Frob}_w = g\alpha$. We see that $\bar{\rho}_{|G_w} = \begin{pmatrix} \chi_p\bar{\chi} & * \\ 0 & \bar{\chi} \end{pmatrix}$. Moreover, if $b : G_w/I_w \to \mathrm{Ad}^0\bar{\rho}$ denotes a 1-cobord and if $[c] \in (L_w^t)^\perp$, then one gets $b(\mathrm{Frob}_w) \in L'$ and that $[c](G_w) \subseteq L$. Since $p \mid |\bar{\rho}(G_w)|$, we conclude thanks to Lemma 2.2.12. □

We can state the result below and give the proof of Theorem B.

Proposition 2.4.4. — *Let $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ denote a representation unramified outside $S = S_p$. Assume that $\bar{\rho}$ is nearly extraordinary in v, for each $v \in S$. Suppose that $\mu_p \nsubseteq K_v$, for each $v \in S$. Assume also that*

$$(i)\ \mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{im}(\bar{\rho})$$

and

$$(ii)\ \sum_{v\in S} \dim_{\mathbb{F}} L_v^{neo} \geq \sum_{v\in S\cup Pl_\infty(K)} \dim_{\mathbb{F}} H^0(G_v, \mathrm{Ad}^0\bar{\rho}).$$

Then there exists a finite set of places T containing S such that :

$$H^1_{\{L(T)^\perp\}}(G_{K,T}, \mathrm{Ad}^0\bar{\rho}(1)) = (0),$$

where $L(T)^\perp = L(S)^\perp \oplus (\bigoplus_{w\in T-S} L_w^{t\,\perp})$ and where L_w^t is the tangent space of C_w^t (defined in Subsection 2.2.4).

Proof. — Thanks to Proposition 2.3.2, we know that the pair (C_v^{neo}, L_v^{neo}) is admissible, for each $v \in S$. Suppose that there is $\phi \in H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1))$ nonzero. It follows, from Assumption (ii) in Proposition 2.4.4 and from Item 3) in Theorem 2.2.3, that there exists $\psi \in H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho})$ nonzero. Then we take a place w given in Lemma 2.4.3. We conclude thanks to Subsection 2.4.1 : the place w is such that the following strict injection holds

$$H^1_{\{L(S)^\perp\oplus(L_w^t)^\perp\}}(G_{K,S\cup\{w\}}, (\mathrm{Ad}^0\bar{\rho})(1)) \hookrightarrow H^1_{\{L(S)^\perp\}}(G_{K,S}, (\mathrm{Ad}^0\bar{\rho})(1)).$$

□

Proof of Theorem B. — Thanks to Proposition 2.3.2, we know that the pair (C_v^{neo}, L_v^{neo}) is admissible, for each $v \in S$. Since $\mu_p \nsubseteq K_v$, Corollary 2.3.5 and Proposition 2.4.4 imply that there exists a finite set of places T containing S such that $H^1_{\{L(T)^\perp\}}(G_{K,T}, \mathrm{Ad}^0\bar{\rho}(1)) = (0)$, with $L(T)$ as in Proposition 2.4.4. Proposition 2.2.10, applied to the admissible pairs C_v^{neo} (for $v \in S$) and C_w^t (for $w \in T - S$), give a T-ramified deformation ρ of $\bar{\rho}$ such that

$$\rho_{|G_w} \in C_w^t(\mathrm{W}(\mathbb{F})),\ \text{for } w \in T - S,$$

and

$$\rho_{|G_v} \in C_v^{neo}(\mathrm{W}(\mathbb{F})),\ \text{for } v \in S.$$

□

2.4.3. About $\dim_{\mathbb{F}} H^1_{\{L(S)\}}(G_{K,S}, \mathrm{Ad}^0\bar{\rho})$**.** — We fix $K = \mathbb{Q}$, $\mathbb{F} = \mathbb{F}_p$ and $S = S_p$; we assume that $\bar{\rho}$ is odd, nearly extraordinary and unramified outside S.
In this subsection, we will give a bound for $\dim_{\mathbb{F}} H^1_{\{L(S)\}}(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho})$ which depends on $\dim_{\mathbb{F}}(\mathrm{Cl}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))[p])$, where $\mathrm{Cl}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))$ denotes the class group of $\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})$, and $\mathrm{Cl}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))[p]$ its subroup killed by p. It gives a bound for the number of places added to make trivial (we recall that this method is decribed in Section 2.4.1) the Selmer group associated to $(\mathbb{Q}, \oplus_{v\in S} L_v^{neo\perp})$. Indeed, we know that

$$\dim_{\mathbb{F}} H^1_{\{L(S)\}}(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho}) = \dim_{\mathbb{F}} H^1_{\{L(S)^\perp\}}(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho}(1)),$$

when $L(S) = \oplus_{v\in S} L_v^{neo}$.
Since $H^1_{\{L(S)\}}(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho})$ is a subspace of $H^1(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho})$, the following proposition gives a desired bound.

Proposition 2.4.5. — *Let* $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ *denote a nearly extraordinary, odd and* S*-ramified representation. Assume that* $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{im}(\bar{\rho})$.
Then

$$\begin{aligned}\dim_{\mathbb{F}} H^1(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho}) \quad &\leq 3\ [\ (p+1)(p^2-p) + \textstyle\sum_{v\in S} \delta(\mu_p(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})_v)) \\ &\qquad + \dim_{\mathbb{F}}(\mathrm{Cl}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))[p])].\end{aligned}$$

Proof. — [DDT, Lemma 2.48] tells that $H^1(\mathrm{SL}_2(\mathbb{F}), \mathrm{Ad}^0\bar{\rho}) = \{0\}$.
Hence $H^1(\mathrm{imPGL}(\bar{\rho}), \mathrm{Ad}^0\bar{\rho}) = \{0\}$ because $\mathrm{SL}_2(\mathbb{F}) \subseteq \mathrm{im}(\bar{\rho})$. Then one has

$$H^1(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho}) \hookrightarrow H^1(\ker \mathrm{PGL}(\bar{\rho}), \mathrm{Ad}^0\bar{\rho})^{\mathrm{imPGL}(\bar{\rho})}.$$

Since the action of $\ker \mathrm{PGL}(\bar{\rho})$ on $\mathrm{Ad}^0\bar{\rho}$ is trivial, it comes

$$\dim_{\mathbb{F}} H^1(G_{\mathbb{Q},S}, \mathrm{Ad}^0\bar{\rho}) \leq 3 \dim_{\mathbb{F}} \mathrm{Hom}(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})), \mathbb{F}).$$

We need [Ko, Theorem 11.8] and we can state that

$$\begin{aligned}\dim_{\mathbb{F}} \mathrm{Hom}(G_{\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}),S}, \mathbb{F}) \quad &\leq \textstyle\sum_{v\in S} [\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})_v : \mathbb{Q}_p] + \sum_{v\in S} \delta(\mu_p(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho})_v)) \\ &\qquad + \dim_{\mathbb{F}}(\mathrm{Cl}(\mathbb{Q}(\mathrm{Ad}^0\bar{\rho}))[p]).\end{aligned}$$

□

2.4.4. Effective version of the Cebotarev density theorem. — (We thank P.Lebacque for conversations around this subject) Let S' be a finite set of primes containing $S = S_p$.
We fix nonzero elements

$$\psi \in H^1_{\{L(S')\}}(G_{\mathbb{Q},S'}, \mathrm{Ad}^0\bar{\rho}) \text{ and } \phi \in H^1_{\{L(S')^\perp\}}(G_{\mathbb{Q},S'}, \mathrm{Ad}^0\bar{\rho}(1)),$$

where $L(S') = \bigoplus_{v\in S} L_v^{neo} \ \oplus \bigoplus_{v\in S'-S} L_v^t$ (see Subsection 2.2.4 for the definition of L_v^t).
We recall that $E = \mathbb{Q}(\mathrm{Ad}^0\bar{\rho})\mathbb{Q}(\mu_p)$. We used Cebotarev density theorem to prove Lemma 2.4.3, where $E(\phi)E(\psi)/\mathbb{Q}$ is the Galois extension involved.
In this subsection, following [Se 5], we propose a classical estimation of the primes which make trivial the Selmer group associated to $(\mathbb{Q}, L(S)^\perp)$.
The finite Galois extension $E(\phi)E(\psi)/\mathbb{Q}$ is unramified outside S'. In this situation, [Se 5, Théorème 6] gives the next proposition.

Proposition 2.4.6. — *Let n denote $[E(\phi)E(\psi):\mathbb{Q}]$.*
We fix $g \in \mathrm{Gal}(E(\phi)E(\psi)/\mathbb{Q})$.
1) Then there exists a prime $l \notin S'$ such that $\mathrm{Frob}_l = g$ and

$$\log(l) \leq \log(2) + 2n\ c_{11}(\log(n) + \sum_{q \in S'} \log(q)),$$

where c_{11} is an absolute constant (it means that c_{11} does not depend on n and on g).
2) Assume that the Generalized Riemann Hypothesis (GRH) is true. Then the prime l can be chosen such that :

$$l \leq c_{12}\ n^2(\log(n) + \sum_{q \in S'} \log(q))^2, \text{ with } c_{12} = 280.$$

2.5. Applications, companion forms

We prove Theorem C in this section.

2.5.1. Locally abelian and unramified extensions. — Recall that $p \geq 5$.
In this subsection we keep the assumptions and the notations of Theorem B, with $\mathbb{F} = \mathbb{F}_p$. Hence, $\bar{\rho}$ is totally odd ; and the field K is totally real and such that

$$\mu_p \nsubseteq K_v, \text{ for each } v \in S.$$

Moreover, $\rho : G_K \to \mathrm{GL}_2(\mathbb{Z}_p)$ is the nearly extraordinary lift of $\bar{\rho}$ obtained in Theorem B. We begin with the next result which gives us an unramified extension above $K(\mu_{p^\infty})$. Afterwards, we give the Galois group of $K(\rho)/K(\det\rho)$ thanks to a lifting property in group theory (see, e.g., [Se 4]). Thus, under the "cyclotomic assumption" $\ker(\det\rho) = \ker\chi_p$, we obtain the Galois group of the unramified extension $K(\rho)/K(\mu_{p^\infty})$.

Proposition 2.5.1. — *Assume that p splits completely in $K/\mathbb{Q}$. Then the Galois extension $K(\mu_{p^\infty})K(\rho)/K(\mu_{p^\infty})$ is unramified at p.*

Proof. — As we assume that p splits in K, it follows that $G_v^{ab} = \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ for each $v \in S$. The lift ρ is nearly extraordinary in v, for all $v \in S$. Denote by ρ_v the restriction of ρ to G_v. So, $\mathbb{Q}_p(\rho_v)/\mathbb{Q}_p$ is abelian, for $v|p$. Since the extension $\mathbb{Q}_p^{ab}/\mathbb{Q}_p(\mu_{p^\infty})$ is unramified, we see that $\mathbb{Q}_p(\rho_v)\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p(\mu_{p^\infty})$ is also unramified and we can conclude. □

The following proposition is a direct consequence of Lemma 5 in [Se 4, Ch. IV,§3].

Proposition 2.5.2. — *Recall that $K(\det\rho)$ denotes the splitting field of $\det\rho$.*
Then $\mathrm{Gal}(K(\rho)/K(\det\rho))$ is isomorphic to $\mathrm{SL}_2(\mathbb{Z}_p)$.

Proof. — Thanks to Lemma 5 in [Se 4, Ch. IV,§3], we know that $\mathrm{SL}_2(\mathbb{Z}_p) \subseteq \mathrm{im}(\rho)$. We recall some details of the proof of Lemma 5 for the convenience of the reader. Let $H = \mathrm{im}(\rho) \cap \mathrm{SL}_2(\mathbb{Z}_p)$. We will show that $\mathrm{SL}_2(\mathbb{Z}_p) \subseteq H$. By assumption, one has $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \mathrm{im}(\bar{\rho})$ and thus $\mathrm{PSL}_2(\mathbb{F}_p) \in \mathrm{Occ}(\mathrm{im}(\rho))$ (see [Se 4] for the notation $\mathrm{Occ}(\cdot)$). Since $\mathrm{Occ}(\mathrm{im}(\rho)) = \mathrm{Occ}(H) \cup \mathrm{Occ}(\mathrm{im}(\rho)/H)$ and since $\mathrm{PSL}_2(\mathbb{F}_p) \notin \mathrm{Occ}(\mathrm{im}(\rho)/H)$ (indeed, $\mathrm{im}(\rho)/H$ is isomorphic to a closed subgroup of $\mathbb{Z}_p^\times$ and $p \geq 5$), we deduce that $\mathrm{PSL}_2(\mathbb{F}_p) \in \mathrm{Occ}(H)$. We denote by $\widetilde{H}$ the image of H mod p. The kernel $\ker(H \to \widetilde{H})$ is a pro-p-group and thus $\mathrm{Occ}(H) = \mathrm{Occ}(\widetilde{H})$. It implies that $\widetilde{H} = \mathrm{SL}_2(\mathbb{F}_p)$ as no proper subroup of $\mathrm{SL}_2(\mathbb{F}_p)$

maps onto $\mathrm{PSL}_2(\mathbb{F}_p)$ and as $\mathrm{PSL}_2(\mathbb{F}_p) \in \mathrm{Occ}(\widetilde{H})$. Thanks to Lemma 3 [Se 4, Ch. IV,§3], it comes that $\mathrm{SL}_2(\mathbb{Z}_p) = H$.
Hence, the restriction of ρ to $\mathrm{Gal}(\bar{\mathbb{Q}}/K(\det\rho))$ maps onto $\mathrm{SL}_2(\mathbb{Z}_p)$ and we conclude. □

2.5.2. Companion forms. — If $f = \sum_{n\geq 1} a_n q^n \in \mathrm{S}_k(\Gamma_1(1);\overline{\mathbb{F}})(\varepsilon)$ is a mod p cuspidal eigenform, then there is a continuous, odd, semisimple Galois representation $\bar{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ attached to f. This representation is p-ramified and characterized by

$$\det(X - \bar{\rho}_f(\mathrm{Frob}_l)) = X^2 - a_l X + \varepsilon(l) l^{k-1}, \text{ for all prime } l \neq p.$$

Thanks to [Gro], we know that $\bar{\rho}_f$ is p-extraordinary if and only if f admits a companion form (with the additional hypothesis $a_p^2 \neq \varepsilon(p)$ if $k = p$). We recall the definition of a companion form.

Definition 2.5.3. — *Let $g = \sum_{n\geq 1} b_n q^n$, where $b_n = n^{1-k} a_n$ for all n such that $\gcd(n,p) = 1$ and where $b_p = a_p$.*
The eigenform f, with weight $2 \leq k \leq p$, admits a companion form if

$$a_p \neq 0 \quad \textit{and if} \quad g \in \mathrm{S}_{k'}(\Gamma_1(1);\overline{\mathbb{F}})(\varepsilon),$$

where $k' = p + 1 - k$.

In [Gro, §17], a table lists the primes $p < 3500$ for which there are f with companion forms such that the image of $\bar{\rho}_f$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. These computations are due to Elkies and Atkin. The following pairs satisfy these requirements :

$$(p,k) \in \{(107,26),(139,20),(271,18),(379,20),(397,16)\}.$$

The pairs

$$(p,k) \in \{(107,26),(139,20),(271,18),(379,20)\}$$

satisfy the additional assumption $\gcd(k-1,p-1) = 1$.

Theorem C is a reformulation of the following corollary.

Corollary 2.5.4. — *Let f be a companion form mod p of weight k and level $N = 1$. Assume that the image of the Galois representation associated to f*

$$\bar{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

contains $\mathrm{SL}_2(\mathbb{F}_p)$. Suppose that $\gcd(k-1,p-1) = 1$.
Then there exists a finite set of primes $T \supseteq \{p\}$ such that $\bar{\rho}_f$ admits a lift

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

which is T-ramified and nearly extraordinary in p.
Hence, the Galois extension $\mathbb{Q}(\rho_f)/\mathbb{Q}(\mu_{p^\infty})$ is unramified at p and

$$\mathrm{Gal}(\mathbb{Q}(\rho_f)/\mathbb{Q}(\mu_{p^\infty})) \simeq \mathrm{SL}_2(\mathbb{Z}_p).$$

Proof. — We can use Theorem B since $\bar{\rho}_f$ is odd. Recall that we work with fixed determinant. Here, one has

$$\det\rho_f = \chi_p^{k-1}.$$

One gets $\mathbb{Q}(\det\rho_f) = \mathbb{Q}(\mu_{p^\infty})$, as $(k-1)$ is prime to $p-1$. The conclusion comes from Proposition 2.5.1 and Proposition 2.5.2. □

Remarque 2.5.1. — Let f be the unique normalized cusp form of level $N = 1$, weight $k = 18, 20$ or 26. Consider the representations $\bar{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ for the pairs $(p, k) \in \{(107, 26), (139, 20), (271, 18), (379, 20)\}$ as above. Thanks to [We 1, Th.5.6], we know that T contains at most two finite places different from p.

CHAPITRE 3

ARITHMÉTIQUE DES EXTENSIONS PEU RAMIFIÉES EN p

Introduction

Soit p un nombre premier. Dans ce chapitre, en vue d'applications à la théorie des déformations de représentations galoisiennes, nous étudions certains quotients de la pro-p-extension maximale d'un corps de nombres K. Toutes les extensions de $\mathbb{Q}$ considérées seront dans une clôture algébrique $\overline{\mathbb{Q}}$ fixée. Soit S et T deux ensembles finis et disjoints de places de K avec T formé de places de K au-dessus de p. Le corps $\widetilde{K}_S^T$, est le compositum des pro-p-extensions L de K qui contiennent la $\mathbb{Z}_p$-extension cyclotomique K^{cyc} de K et telles que L/K^{cyc} soit non-ramifiée en dehors de S et totalement décomposée en T. On note $\widetilde{G}_S^T$ le groupe de Galois de $\widetilde{K}_S^T/K$.

Dans la Partie I, nous déterminons le nombre minimal de générateurs et de relations du pro-p-groupe $\widetilde{G}_S^T$. Lorsque $S \cup T$ contient les places au-dessus de p, on donne des situations inconnues jusqu'à présent pour lesquelles le groupe $\widetilde{G}_S^T$ est libre.

Dans la Partie II, nous appliquons à la théorie des déformations les résultats de la Partie I. On obtient une minoration de la dimension de Krull de l'anneau de déformation d'une représentation $\bar{\rho} : \mathrm{Gal}(\widetilde{K}_S^T/K) \to \mathrm{GL}_2(\mathbb{F}_p)$. Notre étude est motivée par les déformations de représentations $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_{\{p\}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ dites extraordinaires en p, où $\overline{\mathbb{Q}}_{\{p\}}$ désigne l'extension maximale de $\mathbb{Q}$ non-ramifiée en dehors des places au-dessus de p. Les représentations extraordinaires proviennent de formes modulaires mod p dites compagnons (cf. sous-section 1.5.4). Le comportement local de ces représentations fournit des extensions $L/\mathbb{Q}$ non-ramifiées hors de p et localement abéliennes, i.e. telles que $L_v/\mathbb{Q}_p$ soient abéliennes pour chaque $w|p$. Cet aspect des déformations extraordinaires est à l'origine de l'étude de $\widetilde{G}_S^T$.

On détaille les deux parties de ce chapitre.

PARTIE I : A propos de $\widetilde{G}_S^T$

Dans la **section 3.1**, nous commençons par rappeler la théorie p-adique du corps de classes selon [Ja].

Dans la **section 3.2**, nous présentons les objets arithmétiques que nous allons étudier : la pro-p-extension $\widetilde{K}_S^T$ du corps de nombres K et les corps locaux associés qui proviennent

des propriétés locales de $\widetilde{K}_S^T$ fixées par les ensembles finis de places S, T de K. Nous déterminons le groupe de normes de $(\widetilde{K}_S^T)^{ab}/K$ et introduisons le module de Kummer $\widetilde{V}_S^T$ figurant dans l'approximation du groupe $H^2(\widetilde{G}_S^T, \mathbb{F}_p)$.

Dans la **section 3.3**, après avoir fixé un sous-corps k de K tel que K/k soit galoisienne, de groupe de Galois H, on regarde les objets arithmétiques en question comme des modules sur lesquels H agit de manière naturelle. Dans un cadre semi-simple (l'ordre de H est supposé premier à p) on décrit les caractères associés aux modules $H^i(\widetilde{G}_S^T, \mathbb{F}_p)$, avec $i = 1, 2$.

On présente nos résultats dans la **section 3.4**. Il s'agit d'une généralisation de ceux établis dans [Sa]. Nous déterminons le nombre minimal de générateurs et de relations du groupe $\widetilde{G}_S^T$. Comme conséquence, dans la sous-section 3.4.3, nous produisons des exemples de groupes $\widetilde{G}_S^T$ libres avec S et T non-vides tels que $S \cup T$ soit formé des places au-dessus de p. Ces exemples sont nouveaux.

PARTIE II : Applications aux déformations

Dans la **section 3.5**, on fixe le cadre des déformations galoisiennes et on propose un bref bilan des questions naturelles associées.

La **section 3.6** est consacrée aux techniques introduites par Boston ([Bo 1]) pour expliciter des anneaux de déformation de représentations galoisiennes (dont l'image est modérée, i.e. d'ordre premier à p), elles reposent sur des observations en théorie des pro-p-groupes et sur un dévissage du groupe de Galois à déformer selon un de ses pro-p-groupes. Le principe dit "prime-to-ajoint" donne des conditions suffisantes pour que l'anneau de déformation (uni)versel soit sans obstruction, i.e. lisse sur $\mathbb{Z}_p$.

Enfin dans la **section 3.7**, on applique ces raisonnements lorsque le groupe de Galois à déformer se dévisse grâce à $\widetilde{G}_S^T$. Le théorème 3.4.1 permet de minorer la dimension de Krull (d'un quotient) de l'anneau de déformation universel et de donner des situations sans obstructions.

PARTIE I : A propos de $\widetilde{G}_S^T$

3.1. Théorie p-adique du corps de classes

L'objet de la théorie (locale ou globale) du corps de classes est de décrire les extensions abéliennes d'un corps (de nombres ou d'un corps local) à l'aide d'éléments de ce corps et de proposer une correspondance locale-globale. Différentes formulations existent. Ici, la théorie p-adique du corps de classes introduite par Jaulent ([Ja]) sera celle que nous utiliserons. Nous proposons d'en rappeler les grandes lignes dans cette section. En un mot, tout revient à travailler initialement avec des $\mathbb{Z}_p$-modules définis à partir des groupes multiplicatifs $K^\times$ et $K_v^\times$. Les résultats obtenus concernent ainsi des (pro-)p-extensions abéliennes décrites en termes semi-locaux. Nous renvoyons le lecteur à l'article [Ja] pour les démonstrations, que nous omettons.

3.1.1. Le p-groupe des idèles. — Soit K un corps de nombres et soit p un nombre premier. On note $Pl_p(K)$ l'ensemble des places de K au-dessus de p. Nous proposons des rappels généraux sur les objets p-adifiés. On note E_K^S le groupe des S-unités de K lorsque S est un ensemble fini de places de K.

Définition 3.1.1. — 1) Soit $\mathcal{R}_K := \mathbb{Z}_p \otimes_{\mathbb{Z}} K^\times$ le p-groupe des idèles principaux de K. Ce groupe $\mathcal{R}_K$ est la réunion des $\mathcal{E}_K^S := \mathbb{Z}_p \otimes_{\mathbb{Z}} E_K^S$, avec S parcourant les ensembles finis de places de K.

2) Pour chaque place v de K, on pose $\mathcal{R}_v = \varprojlim K_v^\times / K_v^{\times p^n}$ et $\mathcal{U}_v = \varprojlim U_v / U_v^{p^n}$, U_v désignant ici les unités du complété K_v.

Proposition 3.1.2 **([Ja], Prop.1.2)**. — *1) Le p-groupe des idèles principaux $\mathcal{R}_K$ est un $\mathbb{Z}_p$-module topologique pour la limite inductive des modules nœtheriens $\mathcal{E}_K^S$.*

2) Le groupe $\mathcal{R}_v$ est un $\mathbb{Z}_p$-module nœtherien topologique pour la topologie définie par ses sous-modules d'indice fini.

3) Soit v une place archimédienne de K.

a) Si v est réelle et si $p = 2$, alors on a $\mathcal{R}_v \simeq \mathbb{Z}/2\mathbb{Z}$.

b) Sinon, $\mathcal{R}_v$ est nul.

4) Soit v une place non-archimédienne. On note π_v une uniformisante de K_v.

Alors $\mathcal{R}_v = \pi_v^{\mathbb{Z}_p} \mathcal{U}_v$.

De plus, $\mathcal{U}_v$ s'identifie :

– au p-Sylow du groupe des racines de l'unité de K_v, lorsque $v \nmid p$,

– au groupe des unités principales de K_v, lorsque $v|p$.

Définition 3.1.3. — Le p-groupe des idèles $\mathcal{J}_K$ du corps K est défini comme la réunion des $\prod_{v\in S} \mathcal{R}_v \prod_{v\notin S} \mathcal{U}_v$, où S parcourt les ensembles finis de places de K.
Le sous-groupe des idèles unités $\mathcal{U}_K$ est le produit des $\mathcal{U}_v$ pour v parcourant les places de K.

La topologie de $\mathcal{J}_K$ est celle de la limite inductive, chaque $\prod_{v\in S} \mathcal{R}_v \prod_{v\notin S} \mathcal{U}_v$ étant compact.

Remarque 3.1.4. — L'injection canonique $K^\times \hookrightarrow K_v^\times$ induit l'injection diagonale

$$\mathcal{R}_K \hookrightarrow \mathcal{J}_K.$$

Considérons les valeurs absolues p-adiques associées au corps K (cf. [Ja], Déf.1.7)

$$|\ |_v : \mathcal{R}_v \to 1 + p\mathbb{Z}_p.$$

En composant ces valeurs absolues avec l'application naturelle $\mathcal{R}_K \to \mathcal{R}_v$, on dispose d'applications

$$|\ |_{K,v} : \mathcal{R}_K \to 1 + p\mathbb{Z}_p,$$

appelées valeurs absolues principales.
Posons ensuite (cf. [Ja], Prop.1.10)

$$\widetilde{\mathcal{U}}_v := \ker |\ |_v.$$

En prenant le produit des valeurs absolues p-adiques, produit indexé par l'ensemble des places de K, on définit une application produit

$$|\ |_K : \mathcal{J}_K \longrightarrow 1 + p\mathbb{Z}_p.$$

Cela est bien défini car tous les termes du produit, sauf un nombre fini d'entre eux, sont égaux à 1.
On note

$$\widetilde{\mathcal{J}}_K \text{ le noyau du morphisme de groupes } |\ |_K.$$

C'est un sous-groupe fermé de $\mathcal{J}_K$ contenant $\mathcal{R}_K$ (cf. [Ja], Prop.1.8).
Un sous-groupe naturel de $\widetilde{\mathcal{J}}_K$ est celui formé par le produit des noyaux des valeurs absolues :

$$\widetilde{\mathcal{U}}_K := \prod_v \widetilde{\mathcal{U}}_v.$$

Proposition 3.1.5. — *Le groupe abélien $\widetilde{\mathcal{U}}_v$ est décrit de la manière suivante.*
1) Si $v \notin Pl_p(K)$, alors $\widetilde{\mathcal{U}}_v = \mathcal{U}_v$.
2) Si $v \in Pl_p(K)$, alors $\widetilde{\mathcal{U}}_v \simeq \mu_{\mathcal{P}}(K_v) \times \mathbb{Z}_p^{[K_v:\mathbb{Q}_p]}$, où $\mu_{\mathcal{P}}(K_v)$ désigne le groupe des racines de l'unité p-primaires de K_v.

Remarque 3.1.6. — En tant que $\mathbb{Z}_p$-modules, le noyau $\widetilde{\mathcal{U}}_v$ et les unités $\mathcal{U}_v$ ont le même rang ; cela provient du fait que l'image de $\mathcal{R}_v$ par $|\ |_v$ est d'indice fini dans $1 + p\mathbb{Z}_p$.

3.1.2. Symbole d'Artin et correspondance. — On rappelle des résultats de la théorie du corps de classes locale et globale ; les références sont nombreuses ([Gra],[Ja], [AT]). Les symboles locaux ou d'Artin jouent un rôle qui n'est pas détaillé ici. On rappelle que $\widehat{K}$ (respectivement $\widehat{K}_v$) désigne la plus grande pro-p-extension de K (resp. de K_v), dans un clôture algébrique fixée au départ.

Corps de classes local

Définition 3.1.7. — Le corps $\widehat{K}_v^{ab}$ est la plus grande pro-p-extension abélienne de K_v. Le corps K_v^{nr} est la plus grande pro-p-extension non-ramifiée de K_v. Le corps $K_v^{cyc} = \mathbb{Q}_v^{cyc} K_v$ est la $\mathbb{Z}_p$-extension cyclotomique de K_v.

Le théorème suivant rappelle la correspondance pour les pro-p-extensions $\widehat{K}_v^{ab}$, K_v^{nr} et K_v^{cyc} de K_v.

Théorème 3.1.8 **([Ja], Th.2.7)**. — *L'application de réciprocité induit les isomorphismes de $\mathbb{Z}_p$-modules topologiques suivants :*

$$\mathcal{R}_v \simeq \mathrm{Gal}(\widehat{K}_v^{ab}/K_v),$$

$$\mathcal{U}_v \simeq \mathrm{Gal}(\widehat{K}_v^{ab}/K_v^{nr})$$

$$et \quad \widetilde{\mathcal{U}_v} \simeq \mathrm{Gal}(\widehat{K}_v^{ab}/K_v^{cyc}).$$

De plus, si $v \nmid p$, alors la ramification est modérée et $\mathrm{Gal}(\widehat{K}_v^{ab}/K_v^{nr})$ est isomorphe au p-Sylow des racines de l'unité de K_v.
En revanche, si $v|p$, alors la ramification est sauvage, le sous-groupe d'inertie possède une filtration canonique provenant de la filtration canonique des unités principales de K_v.

Corps de classes global
Le p-corps de Hilbert d'un corps de nombres K est défini comme la plus grande p-extension abélienne non-ramifiée de K. La proposition suivante décrit le groupe de Galois du p-corps de Hilbert d'un corps de nombres.

Proposition 3.1.9 **([Ja], Ex.2.8)**. — *Le groupe quotient $\mathcal{J}_K/\mathcal{R}_K\mathcal{U}_K$ s'identifie naturellement au p-groupe des classes de K.*

Le résultat central de la théorie du corps de classes admet la formulation suivante.

Théorème 3.1.10 **([Ja], Th.2.3)**. — *Soit K un corps de nombres et $\widehat{K}^{ab}$ la pro-p-extension abélienne maximale de K. L'application de réciprocité induit un isomorphisme continu*

$$\mathcal{J}_K/\mathcal{R}_K \simeq \mathrm{Gal}(\widehat{K}^{ab}/K).$$

On parlera de correspondance (globale) en référence à l'isomorphisme de réciprocité du théorème ci-dessus. Le lemme suivant tisse le lien entre la théorie du corps de classes locale et globale en mettant en lumière la compatibilité "local-global" de la correspondance.

Proposition 3.1.11 **([Ja], Th.2.3, Lem.2.4)**. — *Soit S un ensemble fini de places du corps de nombres K.*
Alors la surjection naturelle

$$\oplus_{v\in S}\mathcal{R}_v \to \oplus_{v\in S}\mathcal{R}_v\mathcal{R}_K/\mathcal{R}_K$$

est un isomorphisme de $\mathbb{Z}_p$-modules compacts.
En particulier, la correspondance globale respecte la compatibilité locale suivante :
- *le sous-groupe de décomposition d'une place v de K est l'image dans $\mathrm{Gal}(\widehat{K}^{ab}/K)$ du sous-groupe $\mathcal{R}_v$ de $\mathcal{J}_K$.*
- *le sous-groupe d'inertie d'une place v de K est l'image dans $\mathrm{Gal}(\widehat{K}^{ab}/K)$ du sous-groupe $\mathcal{U}_v$ de $\mathcal{J}_K$.*

On résume à présent, dans le tableau qui suit, la correspondance pour des extensions abéliennes de base qui interviendront par la suite. Dans la colonne "Groupe de Galois", on donne un représentant à isomorphisme (continu) près du groupe de Galois de l'extension associée.

Définition 3.1.12. — Le corps $\widehat{K}^{ab}$ est la plus grande pro-p-extension abélienne de K. Le corps K^{nr} est la plus grande pro-p-extension abélienne non-ramifiée de K et K^{cyc} est la $\mathbb{Z}_p$-extension cyclotomique de K.
Par ailleurs, désignons par $K^{loc.cyc}$ la pro-p-extension maximale abélienne de K contenant K^{cyc} et complètement décomposée sur K^{cyc} en chacune de ses places.

Cette définition justifie la notation *loc.cyc*, puisque cette extension est localement cyclotomique. Le module

$$\widetilde{\mathcal{U}}_K := \prod_{v \in Pl(K)} \widetilde{\mathcal{U}}_v$$

intervient pour décrire le groupe de Galois $\mathrm{Gal}(\widehat{K}^{ab}/K^{loc.cyc})$.

Extension	Groupe de Galois
$\widehat{K}^{ab}/K$	$\mathcal{J}_K/\mathcal{R}_K$
$\widehat{K}^{ab}/K^{nr}$	$\mathcal{U}_K\mathcal{R}_K/\mathcal{R}_K$
$\widehat{K}^{ab}/K^{cyc}$	$\widetilde{\mathcal{J}}_K/\mathcal{R}_K$
$\widehat{K}^{ab}/K^{loc.cyc}$	$\widetilde{\mathcal{U}}_K\mathcal{R}_K/\mathcal{R}_K$

3.2. Présentation des objets arithmétiques

On fixe un nombre premier p. Soit $K/\mathbb{Q}$ un corps de nombres de clôture algébrique $\overline{K}$. On s'intéresse au pro-p-quotient maximal de $\mathrm{Gal}(\overline{K}/K)$ et on note $\widehat{K}$ la plus grande pro-p-extension de K dans $\overline{K}$.
Pour chaque place v de K, on rappelle que K_v désigne le complété de K en v et $\widehat{K}_v$ sa plus grande pro-p-extension.
Les deux courtes sous-sections suivantes présentent les objets arithmétiques que nous souhaitons étudier dans ce chapitre.

3.2.1. Objets locaux. —

On commence avec la définition suivante.

Définition 3.2.1. — L'extension $K_v^{cr} := K_v^{nr}K_v^{cyc}$ est la pro-p-extension de K_v appelée extension cyclotomiquement ramifiée.

Remarque 3.2.2. — Si $v \nmid p$, les trois extensions suivantes de K_v coïncident : $K_v^{cyc} = K_v^{nr} = K_v^{cr}$.

On recense dans le tableau ci-dessous les sous-extensions de $\widehat{K}_v/K_v$ que nous aurons à manipuler, on en profite pour fixer les notations des groupes de Galois associés :

Extension	Groupe de Galois
$\widehat{K}_v/K_v$	$\widehat{G}_v$
$\widehat{K}_v/K_v^{nr}K_v^{cyc}$	$\widetilde{I}_v$
$\widehat{K}_v/K_v^{cyc}$	$\widetilde{D}_v$
K_v^{cr}/K_v	G_v^{cr}
K_v^{cyc}/K_v	G_v^{cyc}

3.2.2. Objets Globaux. — On note S et T deux ensembles finis de places finies de K vérifiant :

$$S \cap T = \emptyset \text{ et } T \subseteq Pl_p(K).$$

On partitionne S de la façon suivante : $S = S_p \sqcup S_0$, avec $S_p = S \cap Pl_p(K)$ et $S_0 = S - S_p$. Dans la suite, nous allons nous intéresser au corps $\widetilde{K}_S^T$ défini de la façon suivante.

Définition 3.2.3. — Le corps $\widetilde{K}_S^T$ est la plus grande pro-p-extension de K contenant K^{cyc} et telle que :

$$\widetilde{K}_S^T/K^{cyc} \text{ soit } S\text{-ramifiée et } T\text{-décomposée.}$$

Autrement dit, $\widetilde{K}_S^T/K$ est la pro-p-extension maximale vérifiant :
a) $\widetilde{K}_S^T/K$ est non-ramifiée en dehors de $Pl_p(K) \cup S_0$,
b) $(\widetilde{K}_S^T)_v \subseteq K_v^{cyc}K_v^{nr}$, pour toute place $v \notin S$,
c) $(\widetilde{K}_S^T)_v \subseteq K_v\mathbb{Q}_p^{cyc}$, pour toute place $v \in T$.

On note

$$\widetilde{G}_S^T = \mathrm{Gal}(\widetilde{K}_S^T/K).$$

Il s'agit d'un pro-p-groupe, quotient du groupe de Galois de la plus grande extension $(Pl_p \cup S_0)$-ramifiée de K. Comme $\widetilde{K}_S^T$ contient l'extension cyclotomique de K, le groupe $\widetilde{G}_S^T$ possède un quotient isomorphe au groupe $\mathbb{Z}_p$.

3.2.3. Groupe des normes et module de Kummer de $\widetilde{G}_S^T$. — L'extension galoisienne $\widetilde{K}_S^T/K$ est définie par des propriétés locales ; par compatibilité, il est ainsi facile de voir que :

$$\mathrm{Gal}(\widehat{K}^{ab}/(\widetilde{K}_S^T)^{ab}) \simeq \left(\prod_{v \notin S_0 \cup Pl_p} \mathcal{U}_v\right)\left(\prod_{v \in Pl_p - (S \cup T)} \mathcal{U}_v \cap \widetilde{\mathcal{U}}_v\right)\left(\prod_{v \in T} \widetilde{\mathcal{U}}_v\right)/\mathcal{R}_K.$$

Donnons une écriture plus synthétique pour ce groupe de normes en posant

$$\widetilde{\mathcal{U}}_S^T = \left(\prod_{v \notin S_0 \cup Pl_p} \mathcal{U}_v\right)\left(\prod_{v \in Pl_p - (S \cup T)} \mathcal{U}_v \cap \widetilde{\mathcal{U}}_v\right)\left(\prod_{v \in T} \widetilde{\mathcal{U}}_v\right),$$

i.e.

$$\mathrm{Gal}(\widehat{K}^{ab}/(\widetilde{K}_S^T)^{ab}) \simeq \widetilde{\mathcal{U}}_S^T/\mathcal{R}_K.$$

Définition 3.2.4. — On dit que

$$\widetilde{V}_S^T = \widetilde{\mathcal{U}}_S^T \mathcal{J}_K^p \cap \mathcal{R}_K$$

est le module de Kummer associé à $\widetilde{K}_S^T$.

Une manière naturelle de voir ce module de Kummer provient du dévissage de $(\widetilde{K}_S^T)^{ab}/K$ selon la p-extension abélienne non-ramifiée et T-décomposée maximale de K ; cette extension de K fait également apparaître le module de Kummer suivant :

$$V^T = \mathcal{U}_K \left(\prod_{v \in T} \mathcal{R}_v \right) \mathcal{J}_K^p \cap \mathcal{R}_K.$$

Remarque 3.2.5. — Lorsque A, B et C désignent trois groupes abéliens, on utilisera l'isomorphisme élémentaire $AB \cap CB/B \simeq AB \cap C/(C \cap B)$.

Le principe de Hasse concernant les puissances donne $\mathcal{R}_K^p = \mathcal{J}_K^p \cap \mathcal{R}_K$; ce principe de Hasse repose sur le théorème de densité de Chebotarev appliqué dans une extension de Kummer de K ([Gra]). En combinant ces deux observations, on dispose des isomorphismes suivants :

$$V^T/\mathcal{R}_K^p \simeq \mathcal{U}_K \left(\prod_{v \in T} R_v \right) \mathcal{J}_K^p \cap \mathcal{R}_K \mathcal{J}_K^p / \mathcal{J}_K^p$$

et

$$\widetilde{V}_S^T/\mathcal{R}_K^p \simeq \widetilde{\mathcal{U}}_S^T \mathcal{J}_K^p \cap \mathcal{R}_K \mathcal{J}_K^p / \mathcal{J}_K^p.$$

Lemme 3.2.6. — *On rappelle que S et T sont deux ensembles (disjoints) de places de K. On a :*

$$\widetilde{V}_{S \cup \{v\}}^T \subseteq \widetilde{V}_S^T, \text{ avec } v \notin S \cup T,$$

et

$$\widetilde{V}_S^{\emptyset} \subseteq \widetilde{V}_S^T \subseteq \widetilde{V}_{\emptyset}^T \text{ et } \widetilde{V}_S^T \subseteq V^T.$$

On présente des résultats à propos de $\widetilde{V}_S^T$ utilisés dans la section 3.4.
Soit $\mathrm{Cl}^T(K)$ le quotient du groupe des classes $\mathrm{Cl}(K)$ de K correspondant à l'extension abélienne non-ramifiée et T-décomposée (i.e. dans laquelle les places au-dessus de T sont complètement décomposées) maximale de K. Le groupe $\mathrm{Cl}^T(K)$ est fini.
Posons $\mathcal{E}_K^T := E_K^T \otimes \mathbb{Z}_p$, où E_K^T désigne le $\mathbb{Z}$-module des T-unités de K.

Lemme 3.2.7. — *Les suites de groupes abéliens suivantes sont exactes*

$$1 \to \mathrm{Cl}^T(K)[p] \to \mathrm{Cl}^T(K) \xrightarrow{p} \mathrm{Cl}^T(K) \to \mathrm{Cl}^T(K)/p \to 1,$$
$$1 \to \mathcal{E}_K^T/\mathcal{E}_K^{Tp} \to V^T/\mathcal{R}_K^p \to \mathrm{Cl}(K)^T[p] \to 1.$$

Démonstration. — De manière immédiate, on voit que la première suite est exacte. Justifions à présent que la seconde l'est aussi. Il suffit d'expliciter l'application δ partant du radical $V^T/\mathcal{R}_K^p$. Chaque $a \in V^T$ s'écrit (de manière non-nécessairement unique) sous la forme urj^p, où $u \in \mathcal{U}_K$, $r \in \prod_{v \in T} \mathcal{R}_v$, $j \in \mathcal{J}_K$. On pose

$$\delta(a) = j,$$

ceci définit une application et la suite exacte provient de cette construction. □

D'après le lemme 3.2.6, et comme $\mathrm{Cl}^T(K)[p]$ et $\mathcal{E}_K^T/\mathcal{E}_K^{Tp}$ sont finis, on obtient :

Corollaire 3.2.8. — *Les groupes abéliens V^T et $\widetilde{V}_S^T$ sont finis.*

Enfin, présentons un algorithme qui trivialise le module quotient $\widetilde{V}_S^T/\mathcal{R}_K^p$. Les modules $\widetilde{V}_S^T$ sont décroissants en S, l'idée de l'algorithme est donc de faire grossir S à l'aide du théorème de densité de Chebotarev.

Proposition 3.2.9. — *Il existe un ensemble fini S' formé de places de K étrangères à p tel que $\widetilde{V}_{S'}^T/\mathcal{R}_K^p$ soit trivial.*

Démonstration. — Supposons que $\mu_p \subseteq K$. On considère L/K la p-extension abélienne élémentaire non-ramifiée en dehors de p de K. Le théorème de densité de Chebotarev appliqué à l'extension L/K assure l'existence d'un ensemble fini de places S' de K qui ne rencontre pas $Pl_p(K)$ tel que les Frobenius associés aux places de S' engendrent $\mathrm{Gal}(L/K)$.
Soit $x \in \widetilde{V}_{S'}^T$. Par la théorie de Kummer, on sait que l'extension cyclique $K(\sqrt[p]{x})/K$ est non-ramifiée hors de p et totalement décomposée en S'. De cette façon, l'extension $K(\sqrt[p]{x})/K$ est triviale et donc x est une puissance p-ème.
Supposons que $\mu_p \nsubseteq K$ et notons ζ_p un générateur de μ_p. Notons S' un ensemble fini de permiers obtenu en appliquant la méthode précédente à l'extension $K(\zeta_p)$.
Soit $x \in \widetilde{V}_{S'}^T$. L'élément x est une puissance p-ème dans $K(\zeta_p)$. Or, l'extension $K(\zeta_p)/K$ est de degré premier à p. On conclut en considérant la norme $\mathrm{N}_{K(\zeta_p)/K}(x)$. □

3.3. Structures de $\mathbb{F}_p[H]$-modules semi-simples

Soit k un sous-corps de K. Supposons que K/k soit une extension galoisienne de groupe de Galois noté H. On souhaite faire ressortir les différentes actions du groupe H sur les objets arithmétiques étudiés. En particulier, pour chaque $\mathbb{Z}$-module M muni d'une action de H, on s'intéresse à

$$M \otimes \mathbb{F}_p \text{ vu comme } \mathbb{F}_p[H]\text{-module.}$$

Notons que cette tensorisation ne tue pas la p-torsion de M, contrairement au module obtenu en tensorisant par $\mathbb{Q}_p$ par exemple.
Pour la suite, nous ferons l'hypothèse de **semi-simplicité** classique dans ce cadre en supposant

$$\mathrm{pgcd}(|H|, p) = 1,$$

de sorte que chaque $\mathbb{F}_p[H]$-module se décompose comme somme directe de modules irréductibles. L'hypothèse de semi-simplicité revient à travailler avec une extension K/k modérément ramifiée en p.
On note $\varphi(M)$ le caractère du module M ; il arrive que l'on confonde, par abus de notation, un module et son caractère. On note $<\varphi, \psi>$ le produit scalaire de deux caractères φ et ψ :

$$<\varphi, \psi> = \frac{1}{|H|} \sum_{h \in H} \varphi(h)\psi(h^{-1}).$$

Lorsque M et N désignent deux modules, l'inégalité

$$\varphi(M) \leq \varphi(N)$$

signifie que chaque module irréductible qui figure dans la décomposition de M figure dans celle de N avec une multiplicité supérieure.
Le module trivial $\mathbb{F}_p$ est noté $\mathbf{1}$.
Par ailleurs, on suppose S et T stables sous l'action de H et on note $S(k), T(k), ...$ les places de k qui sont sous les places de $S, T, ...$
Rappelons brièvement quelques faits classiques en théorie des représentations.

Maximalité : Par maximalité, le groupe H agit sur $\widehat{G}^{ab}$ et sur $(\widetilde{G}_S^T)^{ab}$.

Induite : Soit v une place de k. Pour chaque place w de K au-dessus de v, notons H_w le groupe de décomposition associé, i.e. $H_w = \mathrm{Gal}(K_w/k_v)$. Si pour chaque $w|v$, M_w désigne un H_w-module, alors la somme directe

$$\bigoplus_{w|v} M_w$$

possède une structure naturelle de H-module puisque H permute de façon transitive les $w|v$; on note ce module

$$\mathrm{ind}_{H_v}^H M_v.$$

En particulier, comme le caractère de M_w (muni de l'action de H_w) ne dépend que de v, on notera H_v un groupe de décomposition pour une place w au-dessus de v.
Le module régulier $\mathrm{ind}_1^H(\mathbf{1})$ est noté Reg.

Dualité : Le module $M^* = \mathrm{Hom}(M, \mathbb{F}_p)$ désigne le dual du H-module M.

Compatibilité et corps de classes : Les isomorphismes de la théorie du corps de classes peuvent se lire comme des isomorphismes de $\mathbb{F}_p[H]$-modules, les objets semi-locaux étant munis de leurs structures naturelles d'induites.

Cohomologie : Partons d'une suite exacte de groupes $1 \to A \to B \to C \to 1$. On sait alors que le quotient C agit de façon naturelle sur les groupes de cohomologies $H^i(A, \mathbb{F}_p)$.

Par maximalité les extensions $\widetilde{K}_S^T/k$ sont galoisiennes, on récupère ainsi une action de H sur les $H^i(\widetilde{G}_S^T)$. De façon analogue, les mêmes observations ont lieu au niveau local, i.e. pour les groupes de décomposition.

Remarque 3.3.1. — Le groupe H agit de façon triviale sur le groupe de Galois $\mathrm{Gal}(K^{cyc}/K)$ puisque $K^{cyc} = k^{cyc}K$.

Remarque 3.3.2. — Dans notre application à la déformation d'une représentation résiduelle continue $\bar{\rho} : G_k \to \mathrm{GL}_2(\mathbb{F}_p)$, le groupe H sera l'image de $\bar{\rho}$ et K l'extension de k fixée par le noyau de $\bar{\rho}$:

$$H = \mathrm{Gal}(K/k) = \mathrm{im}(\bar{\rho}).$$

Dans la suite, les modules en jeu proviennent par dualité et induction des trois modules :

$$\mathbf{1}, \mu_p(K), \mu_p(K_v).$$

Lorsque les racines p-èmes de l'unité n'appartiennent pas au corps K (ou K_v), le module $\mu_p(K)$ (ou $\mu_p(K_v)$) n'est rien d'autre que le module nul. On insiste quelques fois en notant le caractère $\varphi(\mu_p(K))$ de la façon suivante

$$\delta(\mu_p(K))\omega,$$

ω étant le caractère de Teichmüller, $\delta(\mu_p(K))$ valant 1 si $\mu_p \subset K$, et 0 sinon.

La sous-section 3.3.1 propose des rappels concernant la structure des modules de Kummer V^T et celle des unités avec le théorème de Dirichlet.
Dans la sous-section 3.3.2, la structure de $H^1(\widetilde{G}_S^T)$ est complètement explicitée en faisant appel à $\widetilde{V}_S^T$. Les méthodes sont classiques, notre travail porte donc essentiellement sur une description soigneuse dans ce contexte arithmétique nouveau.
Enfin, dans la sous-section 3.3.3, deux espaces cohomologiques locaux H^2 sont décrits, notamment grâce à la dualité de Tate. Lors du dévissage de $H^2(\widetilde{G}_S^T)$, ces H^2 sont présents.

3.3.1. Groupe des classes, unités et module de Kummer. — Dans la suite, on rappelle que $\mathrm{Cl}^T(K)$ est le quotient du groupe des classes $\mathrm{Cl}(K)$ de K correspondant à l'extension abélienne non-ramifiée et T-décomposée maximale de K. On rappelle aussi que $\mathcal{E}_K^T = E_K^T \otimes \mathbb{Z}_p$, où E_K^T désigne le $\mathbb{Z}$-module des T-unités de K.

Lemme 3.3.3. — *Par la théorie du corps de classes, on dispose de l'isomorphisme de $\mathbb{F}_p[H]$-modules*

$$\mathcal{J}_K/\mathcal{R}_K\mathcal{U}_K(\prod_{v\in T} R_v)\mathcal{J}_K^p \simeq \mathrm{Cl}^T(K)[p].$$

Proposition 3.3.4 **(voir par exemple** [Gra]**)**. — *(théorème de Dirichlet-Herbrand) Soit $H = \mathrm{Gal}(K/k)$ d'ordre premier à p.*
Le $\mathbb{F}_p[H]$-module $\mathcal{E}_K^T/\mathcal{E}_K^{Tp}$ est décrit de la manière suivante :

$$\varphi(\mathcal{E}_K^T/\mathcal{E}_K^{Tp}) = \sum_{v\in Pl_\infty(k)} \mathrm{ind}_{H_v}^H(\mathbf{1}) + \sum_{v\in T(k)} \mathrm{ind}_{H_v}^H(\mathbf{1}) + \delta(\mu_p(K))\omega - \mathbf{1},$$

où ω est le caractère de Teichmüller, $\delta(\mu_p(K)) = 1$ si K contient les racines p-ième de l'unité et $\delta(\mu_p(K)) = 0$ sinon.

En faisant ressortir l'action galoisienne dans le lemme 3.2.7 , on peut énoncer le résultat suivant.

Lemme 3.3.5. — *Les suites de $\mathbb{F}_p[H]$-modules suivantes sont exactes*

$$1 \to \mathrm{Cl}^T(K)[p] \to \mathrm{Cl}^T(K) \xrightarrow{p} \mathrm{Cl}^T(K) \to \mathrm{Cl}^T(K)/p \to 1,$$

$$1 \to \mathcal{E}_K^T/\mathcal{E}_K^{Tp} \to V^T/\mathcal{R}_K^p \to \mathrm{Cl}(K)^T[p] \to 1.$$

3.3.2. Structure du $H^1(\widetilde{G}_S^T)$. — De façon à alléger les écritures, notons

$$\mathcal{R}_T = \prod_{v\in T} \mathcal{R}_v \text{ et } \mathcal{R}_T^p = \prod_{v\in T} \mathcal{R}_v^p.$$

Regarder le module $H^1(\widetilde{G}_S^T)$ équivaut par dualité à regarder $\widetilde{G}_S^T/(\widetilde{G}_S^T)^p[\widetilde{G}_S^T, \widetilde{G}_S^T]$. La proposition qui suit en donne la structure, la preuve reposant sur le corps de classes et sur la proposition 3.3.7.

Proposition 3.3.6. — *La suite suivante de $\mathbb{F}_p[H]-$modules est exacte :*

$$1 \to \widetilde{V}_S^T/\mathcal{R}_K^p \to V^T/\mathcal{R}_K^p \to \mathcal{U}_K\mathcal{R}_T/\mathcal{U}_K^p\mathcal{R}_T^p\widetilde{\mathcal{U}}_S^T \to \mathcal{J}_K/\mathcal{R}_K\mathcal{J}_K^p\widetilde{\mathcal{U}}_S^T \to \mathcal{J}_K/\mathcal{R}_K\mathcal{U}_K\mathcal{R}_T\mathcal{J}_K^p \to 1.$$

Par conséquent, le caractère du module $\widetilde{G}_S^T/(\widetilde{G}_S^T)^p[\widetilde{G}_S^T,\widetilde{G}_S^T]$ est égal à :

$$\varphi(\widetilde{V}_S^T/\mathcal{R}_K^p) - \sum_{v\in \mathrm{Pl}_\infty(k)} \mathrm{ind}_{H_v}^H(\mathbf{1}) - \varphi(\mu_p(K)) + \mathbf{1} + \sum_{v\in S_p(k)} [k_v:\mathbb{Q}_p]\varphi(\mathrm{Reg})$$
$$+ \sum_{v\in S(k)} \mathrm{ind}_{H_v}^H \varphi(\mu_p(K_v)) + \sum_{v\in \mathrm{Pl}_p(k)-(S_p(k)\cup T(k))} \mathrm{ind}_{H_v}^H(\mathbf{1}).$$

Démonstration. — Commençons par la conséquence concernant les caractères en supposant déjà prouvée la proposition 3.3.7. La théorie du corps de classes assure que le groupe de Galois $\widetilde{G}_S^T/(\widetilde{G}_S^T)^p[\widetilde{G}_S^T,\widetilde{G}_S^T]$ (qui correspond au quotient abélien p-élémentaire maximal de $\widetilde{G}_S^T$) et le quotient $\mathcal{J}_K/\mathcal{R}_K\mathcal{J}_K^p\widetilde{\mathcal{U}}_S^T$ sont des modules isomorphes. Grâce aux lemmes 3.3.5 et 3.3.3, la suite exacte proposée implique l'égalité

$$\varphi(\widetilde{G}_S^T/(\widetilde{G}_S^T)^p[\widetilde{G}_S^T,\widetilde{G}_S^T]) = \varphi(\widetilde{V}_S^T/\mathcal{R}_K^p) - \varphi(\mathcal{E}_K^T/\mathcal{E}_K^{Tp}) + \varphi(\mathcal{U}_K\mathcal{R}_T/\mathcal{U}_K^p\mathcal{R}_T^p\widetilde{\mathcal{U}}_S^T).$$

Il suffit ensuite, pour conclure, d'utiliser les propositions 3.3.4 et 3.3.7.
A présent, intéressons-nous à la suite proposée. On part de la suite exacte suivante :

$$1 \to \mathrm{Gal}(\widehat{K}^{ab}/H^T(K)) \to \mathrm{Gal}(\widehat{K}^{ab}/\widetilde{K}_S^T) \to \mathrm{Gal}(H^T(K)/K) \to 1,$$

où $H^T(K)$ désigne la p-extension abélienne, non-ramifiée, T-décomposée et maximale de K. Par la théorie du corps de classes, on peut exprimer cette suite en termes d'idèles sous la forme suivante :

$$1 \to \mathcal{U}_K\mathcal{R}_T/\mathcal{U}_K\mathcal{R}_T \cap \mathcal{R}_K\widetilde{\mathcal{U}}_S^T \to \mathcal{J}_K/\mathcal{R}_K\widetilde{\mathcal{U}}_S^T \to \mathcal{J}_K/\mathcal{R}_K\mathcal{U}_K\mathcal{R}_T \to 1$$

En tuant les puissances de p (ce qui, du point de vue galoisien, correspond à travailler avec les extensions p-élémentaires associées), on obtient la suite suivante :

$$1 \to \widetilde{V}_S^T/\mathcal{R}_K^p \xrightarrow{\alpha_4} V^T/\mathcal{R}_K^p \xrightarrow{\alpha_3} \mathcal{U}_K\mathcal{R}_T/\mathcal{U}_K^p\mathcal{R}_T^p\widetilde{\mathcal{U}}_S^T \xrightarrow{\alpha_2}$$

$$\xrightarrow{\alpha_2} \mathcal{J}_K/\mathcal{R}_K\mathcal{J}_K^p\widetilde{\mathcal{U}}_S^T \xrightarrow{\alpha_1} \mathcal{J}_K/\mathcal{R}_K\mathcal{U}_K\mathcal{R}_T\mathcal{J}_K^p \to 1$$

où
– α_1, α_2 et α_4 sont les applications naturelles,
– α_3 est définie de façon naturelle (i.e. $\alpha_4(urj^p) = ur$ avec des notations évidentes) en utilisant l'isomorphisme de la remarque 3.2.5 :

$$V^T/\mathcal{R}_K^p \simeq \mathcal{U}_K\mathcal{R}_T\mathcal{J}_K^p \cap \mathcal{R}_K\mathcal{J}_K^p/\mathcal{J}_K^p \quad .$$

Il est alors facile de voir que :

$$\ker\alpha_1 \simeq \mathcal{U}_K\mathcal{R}_T/\mathcal{U}_K\mathcal{R}_T \cap \mathcal{R}_K\mathcal{J}_K^p\widetilde{\mathcal{U}}_S^T,$$
$$\ker\alpha_2 \simeq \mathcal{U}_K\mathcal{R}_T \cap \mathcal{R}_K\mathcal{J}_K^p/\mathcal{U}_K^p\mathcal{R}_T^p\widetilde{\mathcal{U}}_S^T \cap \mathcal{R}_K\mathcal{J}_K^p$$
$$\text{et } \ker\alpha_3 \simeq \widetilde{V}_S^T/\mathcal{R}_K^p \ .$$

On peut ensuite conclure, la suite de $\mathbb{F}_p[H]$-modules de l'énoncé de la proposition est bien exacte.

□

Il nous faut donc prouver la proposition :

Proposition 3.3.7. — *La structure du $\mathbb{F}_p[H]$-module $\mathcal{U}_K\mathcal{R}_T/\mathcal{U}_K^p\mathcal{R}_T^p\widetilde{\mathcal{U}}_S^T$ est décrite de la façon suivante :*

$$\varphi(\mathcal{U}_K\mathcal{R}_T/\mathcal{U}_K^p\mathcal{R}_T^p\widetilde{\mathcal{U}}_S^T) = \sum_{v\in S_p(k)}[k_v:\mathbb{Q}_p]\varphi(\mathrm{Reg}) + \sum_{v\in S(k)}\mathrm{ind}_{H_v}^H\ \varphi(\mu_p(K_v)) + \sum_{v\in(\mathrm{Pl}_p-S_p)(k)}\mathrm{ind}_{H_v}^H\mathbf{1}.$$

Démonstration. — Commençons par écrire sous une autre forme le module en question. Le quotient $\mathcal{U}_K(\prod_{v\in T}\mathcal{R}_v)/\mathcal{U}_K^p(\prod_{v\in T}\mathcal{R}_v^p)\ \widetilde{\mathcal{U}}_S^T$ est égal au produit suivant

$$(\prod_{v\in S_p}\mathcal{U}_v/\mathcal{U}_v^p)(\prod_{v\in S_0}\mathcal{U}_v/\mathcal{U}_v^p)(\prod_{v\in Pl_p-(S\cup T)}\mathcal{U}_v/\mathcal{U}_v^p(\mathcal{U}_v\cap\widetilde{\mathcal{U}}_v))(\prod_{v\in T}\mathcal{R}_v/\mathcal{R}_v^p\ \widetilde{\mathcal{U}}_v).$$

Nous allons détailler le calcul classique des modules qui figurent dans la décomposition précédente.

Fait : $\varphi(\bigoplus_{v\in S_p}\mathcal{U}_v/\mathcal{U}_v^p) = \sum_{v\in S_p(k)}[k_v:\mathbb{Q}_p]\ \varphi(\mathrm{Reg}) + \mathrm{ind}_{H_v}^H\varphi(\mu_p(K_v))$.

Lorsque w désigne une place de K au-dessus de $v\in Pl_p(k)$, le $\mathbb{Q}_p[H_v]$-module $\mathcal{U}_w$ s'identifie au module $U_{K_w}^1$ des unités principales de K_w. On sait que le logarithme induit un isomorphisme entre le groupe des unités $U_{K_w}^m := \{u\in U_{K_w}\mid u\equiv 1 \mod w^m\}$ et $(wO_{K_w})^m$ pour m assez grand ; on tensorise par $\mathbb{Q}_p$ et sachant que $U_{K_w}^m$ est d'indice fini dans U_K^1, le théorème de la base normale (i.e. $K_w\simeq\mathbb{Z}[H_v]\otimes_{\mathbb{Z}}k_v$) permet d'affirmer que $\mathbb{Q}_p\otimes\mathcal{U}_w\simeq\mathbb{Q}_p[H_v]^{[k_v:\mathbb{Q}_p]}$. En prenant en compte la torsion et le fait que $\mathbb{Z}_p[H_v]^{[k_v:\mathbb{Q}_p]}$ est un $\mathbb{Z}_p[H_v]$-module projectif de type fini, on obtient finalement :

$$\mathcal{U}_w/\mathcal{U}_w^p\simeq\mu_p(K_w)\oplus\mathbb{F}_p[H_v]^{[k_v:\mathbb{Q}_p]},$$

en tant que $\mathbb{F}_p[H_v]$-modules.
Ensuite, à l'aide de l'égalité

$$\bigoplus_{v\in S_p}\mathcal{U}_v/\mathcal{U}_v^p = \bigoplus_{v\in S_p(k)}\left(\bigoplus_{w\in Pl_v(K)}\mathcal{U}_w/\mathcal{U}_w^p\right),$$

on obtient

$$\varphi(\bigoplus_{v\in S_p}\mathcal{U}_v/\mathcal{U}_v^p) = \sum_{v\in S_p(k)}\mathrm{ind}_{H_v}^H\varphi(\mu_p(K_v)) + [k_v:\mathbb{Q}_p]\ \mathrm{ind}_1^H(\mathbf{1}).$$

Fait : $\varphi(\prod_{v\in S_0}\mathcal{U}_v/\mathcal{U}_v^p) = \sum_{v\in S_0(k)}\mathrm{ind}_{G_v}^G\varphi(\mu_p(K_v))$.

Lorsque w est une place de K au-dessus de $v\in S_0(k)$, on sait que $\mathcal{U}_w\simeq\mu_p(K_w)$ en tant que $\mathbb{F}_p[H_v]$-modules. Ainsi, on a

$$\bigoplus_{v\in S_0}\mathcal{U}_v/\mathcal{U}_v^p = \bigoplus_{v\in S_0(k)}\ \bigoplus_{w\in Pl_v(K)}\mathcal{U}_w/\mathcal{U}_w^p = \bigoplus_{v\in S_0(k)}\mathrm{ind}_{H_v}^H\ \varphi(\mu_p(K_v)).$$

Fait : $\varphi(\prod_{v\in Pl_p-(S\cup T)}\mathcal{U}_v/(\mathcal{U}_v\cap\widetilde{\mathcal{U}}_v)\,\mathcal{U}_v^p)=\sum_{v\in(Pl_p-(S\cup T))(k)}\mathrm{ind}_{H_v}^H(\mathbf{1})$.

Il suffit de remarquer que $\mathcal{U}_w/\mathcal{U}_w^p(\mathcal{U}_w\cap\widetilde{\mathcal{U}}_w)\simeq\mathbb{F}_p$ en tant que $\mathbb{F}_p[H_v]$-modules, lorsque w est une place de K au-dessus de $v\in Pl_p(k)$. En effet, on dispose de la suite exacte :

$$1\to\mathcal{U}_w\cap\widetilde{\mathcal{U}}_w\to\mathcal{U}_w\to\mathrm{Gal}(K_w^{cyc}/K_w)\to 1,$$

l'action de H_v sur $\mathrm{Gal}(K_w^{cyc}/K_w)$ étant triviale puisque l'action de H sur $\mathrm{Gal}(K^{cyc}/K)$ est triviale.

Fait : $\varphi(\oplus_{v\in T}\mathcal{R}_v/\mathcal{R}_v^p\,\widetilde{\mathcal{U}}_v)=\sum_{v\in T(k)}\mathrm{ind}_{H_v}^H(\mathbf{1})$.

Il suffit de remarquer, grâce à la théorie du corps de classes locale, que le module $\mathcal{R}_w/\mathcal{R}_w^p\,\widetilde{U}_w$ est isomorphe à $\mathbb{F}_p$, pour chaque place w au-dessus de $v\in Pl_p(k)$. □

Remarquons que cette preuve est indépendante de la démonstration de la proposition 3.3.6.

Remarque 3.3.8. — La structure du module $\widetilde{\mathcal{U}}_v/\widetilde{\mathcal{U}}_v^p$, qui n'intervient pas en tant que tel dans les calculs de la preuve précédente, est décrite de la façon suivante :
- si $v\nmid p$, on sait que $\widetilde{\mathcal{U}}_v=\mathcal{U}_v$.
- si $v|p$, on a $\widetilde{\mathcal{U}}_v/\widetilde{\mathcal{U}}_v^p\simeq\mathcal{U}_v/\mathcal{U}_v^p$. En effet, l'extension cyclotomique ainsi que la pro-p-extension non-ramifiée de K_v proviennent des extensions analogues de k_v, donc H_v agit trivialement sur $\mathrm{Gal}(K_v^{cyc}/K_v)$ et sur $\mathrm{Gal}(K_v^{nr}/K_v)$. Autrement dit, le groupe H_v agit trivialement sur les derniers termes des deux suites exactes suivantes :

$$1\to\mathcal{U}_v/\mathcal{U}_v^p\to\mathcal{R}_v/\mathcal{R}_v^p\to\mathcal{R}_v/\mathcal{R}_v^p\mathcal{U}_v\to 1,$$
$$1\to\widetilde{\mathcal{U}}_v/\widetilde{\mathcal{U}}_v^p\to\mathcal{R}_v/\mathcal{R}_v^p\to\mathcal{R}_v/\mathcal{R}_v^p\widetilde{\mathcal{U}}_v\to 1.$$

3.3.3. Cohomologie et action galoisienne. —

Lemme 3.3.9. — *Soit $v\in Pl_p(k)$. Pour sa structure du $\mathbb{F}_p[H]$-module, on a :*

$$\bigoplus_{w|v}H^2(G_w^{cr})\simeq\mathrm{ind}_{H_v}^H\mathbf{1}.$$

Démonstration. — On rappelle que k_v^{nr} représente la pro-p-extension maximale non-ramifiée de k_v. Fixons $w|v$. Dans ce cas, on voit que

$$G_w^{cr}=\mathrm{Gal}(K_wk_v^{cyc}k_v^{\mathrm{nr}}/K_w).$$

Comme $\mathrm{Gal}(K_wk_v^{cyc}k_v^{\mathrm{nr}}/k_v^{cyc}k_v^{\mathrm{nr}})\simeq\mathrm{Gal}(K_w/K_w\cap k_v^{cyc}k_v^{\mathrm{nr}})$, le groupe H_w agit de manière triviale sur G_w^{cr}. Et donc $H^2(G_w^{cr})\simeq H^2(\mathbb{Z}_p^2)\simeq\mathbb{F}_p$ en tant que $\mathbb{F}_p[H_w]$-modules, ce qui permet de conclure. □

Lemme 3.3.10. — *La structure du $\mathbb{F}_p[H]$-module $\bigoplus_{w|v}H^2(\widehat{G}_w)$ est donnée par l'induite suivante :*

$$\bigoplus_{w|v}H^2(\widehat{G}_v)\simeq\mathrm{ind}_{H_v}^H\ \mu_p(K_v)^*.$$

Démonstration. — Par la dualité de Tate, on a l'isomorphisme de $\mathbb{F}_p[H_v]$-modules :

$$H^2(\widehat{G}_v)^* \simeq \mathrm{Hom}_{H_v}(\mathbb{F}_p, \mu(\overline{K_v})) = \mathrm{Hom}(\mathbb{F}_p, \mu_p(K_v)),$$

où $\mu(\overline{K_v})$ désigne le module des racines de l'unité de $\overline{K}_v$; par conséquent, on a

$$H^2(\widehat{G}_v) \simeq \mu_p(K_v)^*.$$

En tant que $\mathbb{F}_p[H]$-module $\bigoplus_{w|v} H^2(\widehat{G}_v)$ est donc isomorphe à l'induite $\mathrm{ind}_{H_v}^H \mu_p(K_v)^*$. □

3.4. Générateurs et relations de $\widetilde{G}_S^T$

Soit p un nombre premier différent de 2.
On s'intéresse dans cette section aux nombres minimaux de générateurs et de relations du pro-p-groupe $\widetilde{G}_S^T$, i.e. respectivement à

$$d_1(\widetilde{G}_S^T) = \dim_{\mathbb{F}_p} H^1(\widetilde{G}_S^T, \mathbb{F}_p) \text{ et } d_2(\widetilde{G}_S^T) = \dim_{\mathbb{F}_p} H^2(\widetilde{G}_S^T, \mathbb{F}_p).$$

On énonce le résultat principal de cette section. Rappelons que $\delta(\mu_p(K))$ vaut 1 si K contient les racines p-èmes de l'unité μ_p et vaut 0 sinon ; la convention est analogue pour $\delta(\mu_p(K_v))$.

Théorème 3.4.1. — *On dispose de l'égalité suivante concernant les caractères de $\mathbb{F}_p[H]$-modules :*

$$\begin{aligned}\varphi(H^1(\widetilde{G}_S^T)) = \quad & \varphi((\widetilde{V}_S^T)^*) + \mathbf{1} + \sum_{v\in \mathrm{Pl}_p(k)-(S_p(k)\cup T(k))} \mathrm{ind}_{H_v}^H(\mathbf{1}) - \sum_{v\in \mathrm{Pl}_\infty(k)} \mathrm{ind}_{H_v}^H(\mathbf{1}) \\ & + \sum_{v\in S_p(k)} [k_v : \mathbb{Q}_p]\varphi(\mathrm{Reg}) + \sum_{v\in S(k)} \mathrm{ind}_{H_v}^H \varphi(\mu_p(K_v))^* - \varphi(\mu_p(K))^*.\end{aligned}$$

Le caractère du $\mathbb{F}_p[H]$-module $H^2(\widetilde{G}_S^T)$ est inférieur ou égal à :

$$\varphi((\widetilde{V}_S^T)^*) + \sum_{v\in Pl_p(k)-(S_p(k)\cup T(k))} \mathrm{ind}_{H_v}^H(\mathbf{1}) + \sum_{v\in S(k)} \mathrm{ind}_{H_v}^H \varphi(\mu_p(K_v))^* - \delta(S)\varphi(\mu_p(K))^*,$$

où $\delta(S)$ vaut 0 si $S = \emptyset$ et 1 sinon.
En particulier le nombre minimal de générateurs et le nombre minimal de relations de $\widetilde{G}_S^T$ satisfont :

$$d_1(\widetilde{G}_S^T) = \dim_{\mathbb{F}_p}(\widetilde{V}_S^T/\mathcal{R}_K^p) + 1 + |Pl_p - (S_p \cup T)| - r_1(K) - r_2(K) + \sum_{v\in S_p} [K_v : \mathbb{Q}_p]$$

$$+ \sum_{v\in S} \delta(\mu_p(K_v)) - \delta(\mu_p(K)).$$

et

$$d_2(\widetilde{G}_S^T) \leq \dim_{\mathbb{F}_p}(\widetilde{V}_S^T/\mathcal{R}_K^p) + |Pl_p - (S_p \cup T)| + \sum_{v\in S} \delta(\mu_p(K_v)) - \delta(S)\delta(\mu_p(K)),$$

où $\delta(S)$ vaut 0 si $S = \emptyset$ et 1 sinon.

Comme conséquences immédiates, il vient :

Corollaire 3.4.2. — *Le groupe $\widetilde{G}_S^T$ possède un nombre fini de générateurs et de relations.*

Corollaire 3.4.3. — *On note $\varphi(\chi_2(\widetilde{G}_S^T)) := \mathbf{1} - \varphi(H^1(\widetilde{G}_S^T)) + \varphi(H^2(\widetilde{G}_S^T))$.*
On suppose $S \neq \emptyset$. Alors la combinaison de caractères vérifie l'inégalité :

$$\varphi(\chi_2(\widetilde{G}_S^T)) \leq \sum_{v \in Pl_\infty(k)} \mathrm{ind}_{H_v}^H(1) - \sum_{v \in S_p(k)} [k_v : \mathbb{Q}_p]\varphi(\mathrm{Reg}).$$

En particulier, on a :

$$\chi_2(\widetilde{G}_S^T) \leq r_1(K) + r_2(K) - \sum_{v \in S_p} [K_v : \mathbb{Q}_p],$$

où $(r_1(K), r_2(K))$ désigne la signature de K.

La sous-section 3.4.1 est consacrée à la démonstration du théorème 3.4.1.
La partie du théorème 3.4.1 concernant $H^2(\widetilde{G}_S^T)$ possède une interprétation à l'aide du noyau de Shafarevich, on la présente dans la sous-section 3.4.2.
Dans la sous-section 3.4.3, les propositions 3.4.22 et 3.4.24, obtenues comme conséquences du théorème 3.4.1, donnent des conditions arithmétiques pour que $\widetilde{G}_S^T$ soit libre. L'inégalité portant sur $d_2(\widetilde{G}_S^T)$ donne une condition suffisante naturelle pour que le groupe $\widetilde{G}_S^T$ soit libre. Dans ce cas, le nombre minimal de générateurs du groupe est égal à $1 - r_1(K) - r_2(K) + \sum_{v \in S_p}[K_v : \mathbb{Q}_p]$.

3.4.1. Preuve du théorème 3.4.1. — Le dual de $H^1(\widetilde{G}_S^T)$ est décrit dans la proposition 3.3.6. On démontre ici la partie du théorème qui concerne $H^2(\widetilde{G}_S^T)$. Commençons par rappeler le lemme suivant :

Lemme 3.4.4 ([Ko]). — *La flèche de restriction est injective :*

$$H^2(\widehat{G}) \hookrightarrow \bigoplus_v H^2(\widehat{G}_v).$$

L'idée de départ de la démonstration du théorème 3.4.1, résumée dans la proposition suivante, repose sur un principe local-global ; introduisons les notations utilisées avant de l'énoncer. Les groupes $\widehat{G}_v$ et $\widetilde{G}_v$ désignent respectivement les sous-groupes de décomposition de $\widehat{G}$ et $\widetilde{G}_S^T$ en v. En particulier,

$$H^2(\widetilde{G}_v) = (0) \text{ dès que } v \in T.$$

Enfin, rappelons que $G_v^{cr} = \mathrm{Gal}(K_v^{cr}/K_v)$.
De cette façon, on dispose :
– des trois inflations locales :

$$inf_v : H^2(G_v^{cr}) \longrightarrow H^2(\widehat{G}_v),$$
$$inf_v : H^2(\widetilde{G}_v) \longrightarrow H^2(\widehat{G}_v),$$
$$\text{et} \quad inf_v : H^2(G_v^{cr}) \longrightarrow H^2(\widetilde{G}_v), \text{ lorsque } v \notin S \cup T.$$

– de l'inflation globale :

$$inf : H^2(\widetilde{G}_S^T) \longrightarrow H^2(\widehat{G}).$$

– et des applications naturelles de localisation, notamment :

$$H^2(\widetilde{G}_S^T) \longrightarrow H^2(G_v^{cr}), \text{ lorsque } v \notin S \cup T.$$

Combiné avec le lemme 3.4.4, le bilan de ces observations donne :

Proposition 3.4.5. — *Le diagramme suivant, dont les flèches sont des applications naturelles, est commutatif*

$$\begin{array}{ccc} H^2(\widetilde{G}_S^T) & \xrightarrow{\quad inf \quad} & H^2(\widehat{G}) \\ \downarrow & \searrow^{\phi} & \downarrow \\ \bigoplus_{v\notin S\cup T} H^2(G_v^{cr}) \oplus \bigoplus_{v\in S} H^2(\widetilde{G}_v) & \longrightarrow & \bigoplus_v H^2(\widehat{G}_v) \end{array}$$

En particulier, on a

$$\ker\Big(\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G})\Big) = \ker\phi.$$

On convient de noter $\delta(S) = 0$ si $S = \emptyset$ et 1 sinon. Avec la suite exacte de Poitou-Tate ([NSW], Th. 8.6.10), on obtient comme corollaire :

Corollaire 3.4.6. — *L'inégalité suivante entre les caractères a lieu :*

$$\varphi(H^2(\widetilde{G}_S^T)) \leq \varphi(\ker\inf) + \sum_{v\notin T} \varphi(\text{im } \inf_v) - \delta(S)\varphi(\mu_p(K))^*,$$

avec $\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G})$, $\inf_v : H^2(G_v^{cr}) \to H^2(\widehat{G}_v)$ *lorsque* $v \notin S \cup T$ *et* $\inf_v : H^2(\widetilde{G}_v) \to H^2(\widehat{G}_v)$ *lorsque* $v \in S$.

La fin de cette sous-section est consacrée aux caractères $\varphi(\text{im } \inf_v)$ et puis à $\varphi(\ker\inf)$.

3.4.1.1. Sur les modules $\text{im}\,(\inf_v)$. — Les applications $\inf_v$ prennent leurs valeurs dans $H^2(\widehat{G}_v)$ dont la structure de module est rappelée dans le lemme 3.3.10.
Notons que l'hypothèse faite sur p, à savoir $p > 2$, intervient dans la preuve du lemme suivant.

Lemme 3.4.7. — *Soit* $v \in Pl(K)$.
Alors l'inflation naturelle $H^2(G_v^{cr}) \longrightarrow H^2(\widehat{G}_v)$ *est d'image nulle.*

Démonstration. — Soit $v \in Pl(K)$.
Lorsque $v \notin Pl_p(K)$, l'extension K_v^{cr} coïncide avec K_v^{cyc}, et ainsi le groupe G_v^{cr} est isomorphe au groupe libre $\mathbb{Z}_p$. Dans ce cas, $H^2(G_v^{cr}) = (0)$.
Lorsque $v \in Pl_p(K)$, l'extension K_v^{cr} est obtenue comme compositum de K_v et de $\mathbb{Q}_p^{cr}$; de cette façon, on dispose des deux surjections naturelles suivantes :

$$\widehat{G}_v \twoheadrightarrow \text{Gal}(\widehat{\mathbb{Q}}_p K_v/K_v) \twoheadrightarrow G_v^{cr}.$$

Comme $\text{Gal}(\widehat{\mathbb{Q}}_p K_v/K_v) \simeq \text{Gal}(\widehat{\mathbb{Q}}_p/K_v \cap \widehat{\mathbb{Q}}_p)$ est libre en tant que sous-groupe du groupe libre $\text{Gal}(\widehat{\mathbb{Q}}_p/\mathbb{Q}_p)$ (ici $p > 2$), le lemme est prouvé. □

Ainsi, seules les images des $\inf_v$ associées aux places $v \in S$ contribuent à la somme $\sum_v \varphi(\text{im } \inf_v)$.
Les lemmes 3.4.7 et 3.3.10 impliquent :

Proposition 3.4.8. — *On dispose des inégalités de caractères suivantes :*

$$\varphi(\text{im } \phi) \leq \sum_{v\in S} \varphi(\text{im } \inf_v) - \delta(S)\varphi(\mu_p(K))^* \leq \sum_{v\in S} \text{ind}_{H_v}^H \varphi(\mu_p(K_v))^* - \delta(S)\varphi(\mu_p(K))^*,$$

avec $\delta(S) = 0$ *si* $S = \emptyset$ *et* 1 *sinon.*

3.4.1.2. Sur le module $\ker\Big(\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G})\Big)$. — Commençons par rappeler que : $\widehat{G} = \text{Gal}(\widehat{K}/K)$, $\widetilde{G}_S^T = \text{Gal}(\widetilde{K}_S^T/K)$ et $\widetilde{V}_S^T = \widetilde{\mathcal{U}}_S^T \mathcal{J}_K^p \cap \mathcal{R}_K$; de plus, $G_v^{cr} = \text{Gal}(K_v^{cyc}\widehat{K}_v^{nr}/K)$. On démontre le résultat suivant.

Proposition 3.4.9. — *On dispose de l'inégalité suivante entre les caractères :*

$$\varphi(\ker\Big(\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G})\Big)) \leq \varphi((\widetilde{V}_S^T/\mathcal{R}_K^p)^*) + \sum_{v\notin S\cup T} \varphi(H^2(G_v^{cr})).$$

La démonstration de la proposition ci-dessus utilise la suite spectrale de Hoschild-Serre dans laquelle le groupe D_S^T intervient.

Définition 3.4.10. — Le groupe D_S^T est le groupe de Galois donné par la suite exacte

$$1 \to D_S^T \to \widehat{G} \to \widetilde{G}_S^T \to 1,$$

i.e.

$$D_S^T = \text{Gal}(\widehat{K}/\widetilde{K}_S^T).$$

Après cette définition globale, le lemme suivant propose un point de vue local sur le groupe D_S^T.

Lemme 3.4.11. — *1) D_S^T est le plus petit sous-groupe normal et fermé de $\widehat{G}$ contenant les groupes suivants :*

$$\widetilde{I}_v := \textit{ le sous-groupe d'inertie de } \text{Gal}(\widehat{K}/K^{cyc}) \textit{ pour tout } v \notin S \cup T$$

et

$$\widetilde{D}_v := \textit{ le sous-groupe de décomposition de } \text{Gal}(\widehat{K}/K^{cyc}) \textit{ pour tout } v \in T.$$

2) L'application naturelle (partant d'un produit libre) $(*_{v\notin S\cup T}\widetilde{I}_v) * (*_T \widetilde{D}_v) \to D_S^T$ induit, par dualité, l'injection suivante :

$$H^1(D_S^T)^{\widetilde{G}_S^T} \longrightarrow \bigoplus_{\substack{v\notin S\cup T \\ Nv\equiv 0 \text{ ou } 1 \text{ mod } p}} H^1(\widetilde{I}_v)^{G_v^{cr}} \oplus \bigoplus_{v\in T} H^1(\widetilde{D}_v)^{G_v^{cyc}},$$

où Nv désigne le cardinal du corps résiduel du localisé K_v.

Démonstration. — Le premier point est immédiat et permet de voir que le groupe D_S^T est topologiquement et normalement engendré par les groupes :

$$\widetilde{I}_v, \text{ avec } v \notin S \cup T \quad \text{et} \quad \widetilde{D}_v, \text{ avec } v \in T.$$

Autrement dit, il existe une flèche naturelle partant du produit libre $(*_{v\notin S\cup T}\widetilde{I}_v) * (*_T \widetilde{D}_v)$ et à valeurs dans D_S^T dont la clôture normale de l'image est le groupe D_S^T lui-même. En composant cette flèche avec le passage au quotient $D_S^T \to D_S^T/(D_S^T)^p[D_S^T, \widetilde{G}_S^T]$, on dispose du diagramme commutatif suivant :

$$\begin{array}{ccc} (*_{v\notin S\cup T}\widetilde{I}_v) * (*_T \widetilde{D}_v) & \hookrightarrow & D_S^T \\ \downarrow & \nearrow & \downarrow \\ \left(\prod_{v\notin S\cup T} \widetilde{I}_v/\widetilde{I}_v^p[\widetilde{I}_v, \widehat{G}_v]\right)\left(\prod_{v\in T} \widetilde{D}_v/\widetilde{D}_v^p[\widetilde{D}_v, \widehat{G}_v]\right) & \longrightarrow & D_S^T/(D_S^T)^p[D_S^T, \widetilde{G}_S^T] \end{array}$$

la flèche diagonale étant surjective. Par conséquent, l'application naturelle

$$\left(\prod_{\substack{v\notin S\cup T \\ Nv\equiv 0 \text{ ou } 1 \ mod\ p}} \widetilde{I}_v/\widetilde{I}_v^p[\widetilde{I}_v, \widehat{G}_v]\right)\left(\prod_{v\in T} \widetilde{D}_v/\widetilde{D}_v^p[\widetilde{D}_v, \widehat{G}_v]\right) \longrightarrow D_S^T/(D_S^T)^p[D_S^T, \widehat{G}]$$

est surjective, les groupes $\widetilde{I}_v$ étant triviaux lorsque $Nv \not\equiv 0, 1 \mod p$. Il suffit alors de dualiser pour conclure □

Avec le souci de rendre les diagrammes plus simples à lire, posons

$$\bigoplus_{v\notin S} N_v = \bigoplus_{v\notin S\cup T} H^1(G_v^{cr}) \oplus \bigoplus_{v\in T} H^1(G_v^{cyc})$$

et

$$\bigoplus_{v\notin S} M_v = \bigoplus_{v\notin S\cup T} H^1(\widetilde{I}_v)^{G_v^{cr}} \oplus \bigoplus_{v\in T} H^1(\widetilde{D}_v)^{G_v^{cyc}}.$$

Dans la proposition suivante, les lignes du diagramme proviennent de la suite spectrale de Hoschild-Serre, tandis que les colonnes proviennent des applications de localisations naturelles. On note a, b, c les trois applications naturelles de localisations dans ce diagramme ; on sait que b est injective d'après le lemme 3.4.11. On peut ainsi énoncer :

Proposition 3.4.12. — *On dispose du diagramme commutatif suivant, les lignes formant des suites exactes :*

$$\begin{array}{ccccccc} H^1(\widetilde{G}_S^T) & \hookrightarrow & H^1(\widehat{G}) & \xrightarrow{res} & H^1(D_S^T)^{\widetilde{G}_S^T} & \twoheadrightarrow & \ker\left(\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G})\right) \\ \downarrow & & \downarrow a & & \downarrow b & & \downarrow c \\ \bigoplus_{v\notin S} N_v & \hookrightarrow & \bigoplus_{v\notin S} H^1(\widehat{G}_v) & \longrightarrow & \bigoplus_{v\notin S} M_v & \longrightarrow & \bigoplus_{v\notin S\cup T} H^2(G_v^{cr}) \end{array}$$

Notons $\bar{a}$ l'application induite

$$\bar{a} : H^1(\widehat{G})/H^1(\widetilde{G}_S^T) \to \bigoplus_{v\notin S} H^1(\widehat{G}_v)/\bigoplus_{v\notin S} N_v,$$

qui permet de contrôler le noyau de c grâce au lemme du serpent :

Corollaire 3.4.13. — *On a :*

$$\ker c \hookrightarrow \operatorname{coker} \bar{a}\ .$$

A présent, nous déterminons le noyau de l'application $\bar{a}^*$ duale de $\bar{a}$:

$$\bar{a}^* : \left(\bigoplus_{v \notin S} H^1(\widehat{G}_v) / \bigoplus_{v \notin S} N_v \right)^* \longrightarrow \left(H^1(\widehat{G}) / H^1(\widetilde{G}_S^T) \right)^*.$$

Avant de décrire les espaces duaux, on énonce le lemme de théorie des pro-p-groupes :

Lemme 3.4.14. — *Soit B un pro-p-groupe de type fini. Soit A un sous-groupe fermé et distingué de B tel que B/A soit abélien et sans torsion.*
Alors

$$(A \cap B^p)[B,B] = A^p[B,B].$$

Démonstration. — Il s'agit de montrer que $(A \cap B^p)[B,B] \subseteq A^p[B,B]$. On fixe un élément $x \in (A \cap B^p)[B,B]$. On peut raisonner modulo l'ouvert $[B,B]$ et supposer ainsi qu'il existe $y \in B$ et $b \in [B,B]$ tels que $x = y^p b$. Or $[B,B] \subseteq A$, donc $y^p \in A$. Comme B/A est sans torsion, nécessairement $y \in A$, i.e. $x \in A^p[B,B]$. □

Lemme 3.4.15. — *On dispose des isomorphismes de $\mathbb{F}_p[H]$-modules suivants.*
1) $\left(H^1(\widehat{G}) / H^1(\widetilde{G}_S^T) \right)^* \simeq \mathcal{R}_K \mathcal{J}_K^p \widetilde{\mathcal{U}}_S^T / \mathcal{R}_K \mathcal{J}_K^p$.
2) $\left(\bigoplus_{v \notin S} H^1(\widehat{G}_v) / \bigoplus_{v \notin S} N_v \right)^* \simeq \widetilde{\mathcal{U}}_S^T / (\widetilde{\mathcal{U}}_S^T)^p$.

Démonstration. — 1) La théorie du corps de classes fournit cet isomorphisme (cf. sous-section 3.2.3), sachant que

$$\left(H^1(\widehat{G}) / H^1(\widetilde{G}_S^T) \right)^* = \ker \left(\widehat{G}^{ab,p} \to (\widetilde{G}_S^T)^{ab,p} \right).$$

2) Le quotient $\widehat{G}_v / \widetilde{I}_v$ est isomorphe à $\mathbb{Z}_p$ si $v \nmid p$, et à $\mathbb{Z}_p^2$ si $v|p$. Grâce au lemme 3.4.14, on voit que $\left(H^1(\widehat{G}_v) / H^1(G_v^{cr}) \right)^* \simeq \widetilde{I}_v / (\widetilde{I}_v \cap \widehat{G}_v^p)[\widehat{G}_v, \widehat{G}_v] = \widetilde{I}_v / \widetilde{I}_v^p[\widehat{G}_v, \widehat{G}_v]$. D'autre part, le quotient $\widehat{G}_v / \widetilde{D}_v$ est isomorphe à $\mathbb{Z}_p$ et donc, toujours d'après le lemme 3.4.14, on a $\left(H^1(\widehat{G}_v) / H^1(G_v^{cyc}) \right)^* \simeq \widetilde{D}_v / (\widetilde{D}_v \cap \widehat{G}_v^p)[\widehat{G}_v, \widehat{G}_v] = \widetilde{D}_v / \widetilde{D}_v^p[\widehat{G}_v, \widehat{G}_v]$. Par conséquent, on a $\left(\bigoplus_{v \notin S} H^1(\widehat{G}_v) / \bigoplus_{v \notin S} N_v \right)^* \simeq \left(\prod_{v \notin S \cup T} \widetilde{I}_v / \widetilde{I}_v^p[\widehat{G}_v, \widehat{G}_v] \right) \left(\prod_{v \in T} \widetilde{D}_v / \widetilde{D}_v^p[\widehat{G}_v, \widehat{G}_v] \right) \simeq \widetilde{\mathcal{U}}_S^T / (\widetilde{\mathcal{U}}_S^T)^p$.

□

L'application naturelle a^* peut se lire, grâce au lemme précédent, à l'aide de la théorie du corps de classes : elle est surjective et son noyau vérifie

$$\ker(a^*) = \widetilde{\mathcal{U}}_S^T \cap \mathcal{R}_K \mathcal{J}_K^p / \ (\widetilde{\mathcal{U}}_S^T)^p.$$

Lemme 3.4.16. — *La composée naturelle*

$$\widetilde{\mathcal{U}}_S^T \cap \mathcal{R}_K \mathcal{J}_K^p \to \widetilde{\mathcal{U}}_S^T \mathcal{J}_K^p \cap \mathcal{R}_K \mathcal{J}_K^p \simeq \widetilde{V}_S^T / \mathcal{R}_K^p$$

induit l'isomorphisme de $\mathbb{F}_p[H]$-modules suivant :

$$\ker(a^*) \simeq \widetilde{V}_S^T / \mathcal{R}_K^p.$$

Démonstration. — D'après la remarque 3.2.5, on sait que $\widetilde{\mathcal{U}}_S^T \mathcal{J}_K^p \cap \mathcal{R}_K \mathcal{J}_K^p \simeq \widetilde{V}_S^T / \mathcal{R}_K^p$. L'application proposée a donc bien du sens ; de plus, cette composée est surjective et son noyau est égal à l'intersection $\widetilde{\mathcal{U}}_S^T \cap \mathcal{J}_K^p$. Il reste ainsi à voir que $\widetilde{\mathcal{U}}_S^T \cap \mathcal{J}_K^p = (\widetilde{\mathcal{U}}_S^T)^p$; grâce au lemme 3.4.14 il suffit de montrer que chacun des facteurs du quotient $(\prod_{v \notin S} \mathcal{R}_v)/\widetilde{\mathcal{U}}_S^T$ est sans torsion. Or, seuls les $\mathcal{R}_v$ pour lesquels v est ultramétrique sont non-nuls et

$$\mathcal{R}_v/\mathcal{U}_v \simeq \mathbb{Z}_p \text{ lorsque } v \nmid p,$$
$$\mathcal{R}_v/(\mathcal{U}_v \cap \widetilde{\mathcal{U}}_v) \simeq \mathbb{Z}_p^2 \text{ lorsque } v|p$$

et

$$\mathcal{R}_v/\widetilde{\mathcal{U}}_v \simeq \mathbb{Z}_p \text{ lorsque } v|p.$$

□

Tous les ingrédients sont rassemblés pour démontrer la proposition 3.4.9 et le théorème 3.4.1.

Démonstration de la proposition 3.4.9. — Il suffit de dresser le bilan de nos observations en partant de la suite exacte :

$$1 \to \ker c \to \ker(\text{inf}) \to \text{im} c \to 1.$$

On sait bien sûr que $\text{im}\, c \hookrightarrow \bigoplus_{v \notin S \cup T} H^2(G_v^{cr})$. De plus, avec le lemme 3.4.16, on a

$$\ker\ c \hookrightarrow \text{coker} a \simeq (\widetilde{V}_S^T / \mathcal{R}_K^p)^*.$$

□

Démonstration du théorème 3.4.1. — C'est une conséquence directe des propositions 3.4.9 et 3.4.8, ainsi que du lemme 3.3.9. □

3.4.2. Groupe de Shafarevich. — La majoration de $d_2(\widetilde{G}_S^T)$ repose sur le principe local-global. Nous donnons ici une interprétation de la majoration du théorème 3.4.1 à l'aide du noyau de Shafarevich défini de la façon suivante.

Définition 3.4.17. — On conserve les notations utilisées jusqu'ici. On appelle groupe de Shafarevich le sous-espace vectoriel de $H^2(\widetilde{G}_S^T)$ défini par :

$$Ш(\widetilde{G}_S^T) := \ker \left[H^2(\widetilde{G}_S^T) \longrightarrow \bigoplus_{v \in S} H^2(\widehat{G}_v) \oplus \bigoplus_{v \notin S \cup T} H^2(G_v^{cr}) \right].$$

On a l'implication :

$$Ш(\widetilde{G}_S^T) = (0) \Rightarrow \begin{cases} \text{Les relations du groupe } \widetilde{G}_S^T \text{ sont entièrement} \\ \text{déterminées par des relations locales.} \end{cases}$$

Remarque 3.4.18. — Dans la définition précédente, la partie semi-locale tient compte des conditions qui définissent $\widetilde{G}_S^T$. En particulier, les $H^2(G_v^{cyc})$, avec $v \in T$, devraient figurer dans cette somme ; ces espaces sont bien sûr nuls.

On peut alors énoncer le résultat suivant de comparaison avec le module $\widetilde{V}_S^T$.

Proposition 3.4.19. — *Le groupe de Shafarevich vérifie l'inclusion :*

$$Ш(\widetilde{G}_S^T) \hookrightarrow (\widetilde{V}_S^T/\mathcal{R}_K^p)^*.$$

Démonstration. — On part du diagramme commutatif donné dans la proposition 3.4.5. Par définition, le groupe de Shafarevich vérifie $Ш(\widetilde{G}_S^T) \subseteq \ker\phi$.
Or, $\ker\phi = \ker(\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G}))$. Ainsi, on dispose de l'égalité $Ш(\widetilde{G}_S^T) = \ker c$, où c est donnée dans le diagramme commutatif :

$$\begin{array}{ccccc} H^1(\widehat{G})/H^1(\widetilde{G}_S^T) & \xrightarrow{res} & H^1(D_S^T)^{\widetilde{G}_S^T} & \twoheadrightarrow & \ker\left(\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G})\right) \\ \downarrow \bar{a} & & \downarrow b & & \downarrow c \\ \bigoplus_{v\notin S} H^1(\widehat{G}_v)/\bigoplus_{v\notin S} N_v & \longrightarrow & \bigoplus_{v\notin S} M_v & \longrightarrow & \bigoplus_{v\notin S\cup T} H^2(G_v^{cr}) \end{array}$$

On conclut grâce au lemme du serpent et au lemme 3.4.16. □

Remarque 3.4.20. — Dans la preuve précédente, on a vu que $\ker c = Ш(\widetilde{G}_S^T)$, de sorte que $\dim_{\mathbb{F}_p}\ker\left(\inf : H^2(\widetilde{G}_S^T) \to H^2(\widehat{G})\right) = \dim_{\mathbb{F}_p} Ш(\widetilde{G}_S^T) + \dim_{\mathbb{F}_p}\mathrm{im}\, c$. Cela donne un nouveau majorant de $d_2(\widetilde{G}_S^T)$:

$$d_2(\widetilde{G}_S^T) \leq \dim_{\mathbb{F}_p} Ш(\widetilde{G}_S^T) + |Pl_p - (S_p \cup T)| + \sum_{v\in S}\delta(\mu_p(K_v)) - \delta(S)\delta(\mu_p(K)),$$

où $\delta(S) = 0$ si S est vide et 1 sinon.

3.4.3. Exemples de groupes libres. — On fixe p. On note ζ_p une racine primitive p-ème de l'unité.
Commençons par rappeler deux cas classiques connus de groupes $\widetilde{G}_S^T$. D'abord lorsque $S = Pl_p$ et $T = \emptyset$, le groupe $\widetilde{G}_S^T$ correspond au groupe de Galois de la pro-p-extension maximale S-ramifiée dont on a vu qu'il est de dimension cohomologique au plus 2 (cf. théorème 0.0.5). Ensuite, le cas $S = T = \emptyset$ et $K = \mathbb{Q}(\zeta_p)$ produit $\widetilde{G}_S^T \simeq \mathbb{Z}_p$, lorsque p est un nombre premier régulier. Nous présentons des exemples nouveaux de groupes $\widetilde{G}_S^T$ libres, notamment avec deux générateurs.

On cherche des situations pour lesquelles le majorant (qui figure dans le théorème 3.4.1) de la dimension du second groupe de cohomologie $H^2(\widetilde{G}_S^T)$ est nul. Il s'agit donc d'avoir :
(i) un quotient $\widetilde{V}_S^T/\mathcal{R}^p$ trivial,
(ii) $S_p \cup T = Pl_p$,
(iii) $\sum_{v\in S}\delta(\mu_p(K_v)) = \delta(\mu_p(K))$.

Le lemme suivant provient directement de la définition du module de Kummer $\widetilde{V}_S^T$ (cf. sous-section 3.2.3).

Lemme 3.4.21. — *Supposons que toute p-extension de $K(\zeta_p)$ non-ramifiée hors de p et totalement décomposée en S soit triviale. Alors le quotient $\widetilde{V}_S^T/\mathcal{R}^p$ est trivial.*

On peut énoncer deux conséquences directes du théorème 3.4.1, la première concernant le cas "$\mu_p \subseteq K$" et la seconde le cas "$\mu_p \nsubseteq K$".

Proposition 3.4.22. — *Soit K un corps de nombres contenant les racines p-èmes de l'unité. Supposons que :*
1) S ne contienne qu'une seule place au-dessus de p, notée v,
2) $S \cup T = Pl_p(K)$,
3) toute p-extension de K non-ramifiée hors de T et totalement décomposée en S soit triviale.
Alors le groupe $\widetilde{G}_S^T$ est libre et possède $1 - r_1(K) - r_2(K) + [K_{\{v\}} : \mathbb{Q}_p]$ générateurs.

Donnons un exemple simple pour illustrer cette proposition.

Exemple 3.4.23. — Ici $p = 3$. On note x une racine du polynôme X^3+X+1. Considérons le corps de nombres $K = \mathbb{Q}(x, \zeta_3)$, où ζ_3 est une racine primitive 3-ème de l'unité. Le corps K possède une place qui divise 3 dont le degré local est égal à 4, on la note v et on note w l'autre place de K au-dessus de 3. On pose $S = \{v\}$ et $T = \{w\}$. Toute 3-extension de K non-ramifiée hors de $T = \{w\}$ est triviale. De cette façon, le groupe $\widetilde{G}_S^T$ est libre engendré par 2 générateurs. Les polynômes de la forme $X^3 + aX + 1$ permettent d'illustrer notre proposition pour des valeurs de a bien choisies.

Enfin le cas où K ne contient pas les racines p-èmes de l'unité :

Proposition 3.4.24. — *Soit K un corps de nombres ne contenant pas les racines p-èmes de l'unité. Supposons que :*
1) pour toute place $v \in S$: $\zeta_p \notin K_v$
2) $S \cup T = Pl_p(K)$,
3) toute p-extension de $K(\zeta_p)$ non-ramifiée hors de T et totalement décomposée en S soit triviale.
Alors le groupe $\widetilde{G}_S^T$ est libre et possède $1 - r_1(K) - r_2(K) + \sum_{v\in S}[K_v : \mathbb{Q}_p]$ générateurs.

3.4.4. Perspectives, travaux de Schmidt. — Nous souhaitons dans un prochain travail exploiter nos résultats sur les groupes de cohomologie de $\widetilde{G}_S^T$ pour étudier la dimension cohomologique de $\widetilde{G}_S^T$ sur le modèle de Schmidt ([Sch]). La sous-section précédente suggère que l'étude se décline en deux parties selon que $\zeta_p \in K$ ou $\zeta_p \notin K$.
Terminons avec un diagramme commutatif. On note $\cup : H^1(\widetilde{G}_S^T) \otimes H^1(\widetilde{G}_S^T) \to H^2(\widetilde{G}_S^T)$ le cup-produit. D'après les propositions 3.2.9 et 3.4.19, on peut choisir l'ensemble S tel que $Ш(\widetilde{G}_S^T)$ soit trivial ; dans cette configuration on dispose du diagramme commutatif suivant :

$$\begin{array}{ccc} H^2(\widetilde{G}_S^T) & \xrightarrow{\text{loc}} & \bigoplus_{v\in S} H^2(\widehat{G}_v) \oplus \bigoplus_{v\notin S\cup T} H^2(G_v^{cr}) \\ \cup\uparrow & \nearrow_{\varphi} & \\ H^1(\widetilde{G}_S^T) \otimes H^1(\widetilde{G}_S^T) & & \end{array}$$

Imaginons que l'on ait S tel que le morphisme naturel φ soit surjectif, alors le morphisme de localisation loc est un isomorphisme et l'inégalité sur la dimension du $H^2(\widetilde{G}_S^T)$ dans le théorème 3.4.1 est en fait une égalité. Ce commentaire s'inspire du théorème 0.0.7 de Schmidt.

PARTIE II : Applications aux déformations

3.5. Déformation explicite, cadre

Soit $\bar{\rho} : \mathrm{Gal}(\bar{k}/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue du groupe de Galois absolu du corps de nombres k, non-ramifiée en dehors d'un ensemble fini de places Σ. Le corps de nombres fixé par le noyau de $\bar{\rho}$ est noté K. L'extension maximale Σ-ramifiée de k est notée k_Σ.

On s'intéresse à deux types de déformations de $\bar{\rho}$:
- celles qui se factorisent à travers $\mathrm{Gal}(k_\Sigma/k)$; la section 3.6 (où $k = \mathbb{Q}$) présente des rappels pour ce cas ;
- celles qui se factorisent à travers $\mathrm{Gal}(M_k/k)$, où M_k désigne l'extension maximale S-ramifiée et T-décomposée de la $\mathbb{Z}_p$-extension cyclotomique k^{cyc} de k (S et T sont deux ensembles finis de places de k), c'est l'objet de la section 3.7.

Avant de dresser un panorama des résultats obtenus dans ce contexte ([Maz 1], [Bo 1], [Bo-Ma], [BöMé]), voici quelques rappels de théorie des déformations. On fixe un groupe profini Π tel que pour chaque sous-groupe ouvert U de Π, l'ensemble des morphismes continus de U dans $\mathbb{F}_p$ soit fini ; il s'agit de la propriété dite de p-finitude. On appelle déformation de $\bar{\rho} : \Pi \to \mathrm{GL}_2(\mathbb{F}_p)$ à un anneau R (local d'idéal maximal m_R, complet Noetherien de corps résiduel $\mathbb{F}_p$) une classe d'équivalence formée de $M\rho_R M^{-1}$, où $\rho_R : \Pi \to \mathrm{GL}_2(R)$ est un relèvement de $\bar{\rho}$ et où $M \in 1 + m_R \mathrm{M}_2(R)$. Mazur montre (dans [Maz 1]) l'existence d'un anneau de déformation universel lorsque le commutant de $\bar{\rho}$ est réduit aux homothéties (et versel dans le cas général). On note $R(\bar{\rho})$ cet anneau.
Il s'agit de décrire le plus précisément cet anneau de déformation. On rappelle que $\mathrm{Ad}(\bar{\rho})$ désigne $\mathrm{M}_2(\mathbb{F}_p)$ muni de l'action par conjugaison de $\bar{\rho}$. On sait que $R(\bar{\rho})$ est de la forme

$$\mathbb{Z}_p[[X_1, \ldots, X_d]]/I,$$

avec $d = \dim_{\mathbb{F}_p} H^1(\Pi, \mathrm{Ad}(\bar{\rho}))$, et I un idéal dont le nombre minimal de générateurs est inférieur ou égal à $r := \dim_{\mathbb{F}_p} H^2(\Pi, \mathrm{Ad}(\bar{\rho}))$. Il y a deux chemins possibles à partir de là. Soit on détermine explicitement l'anneau de déformation $R(\bar{\rho})$, soit on se limite à la connaissance d'un minorant de la dimension de Krull du quotient $R(\bar{\rho})/pR(\bar{\rho})$, en sachant que

$$\mathrm{dimKrull} R(\bar{\rho})/pR(\bar{\rho}) \geq d - r, \text{ avec égalité lorsque } r = 0.$$

Le cas de $\bar{\rho} : \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ est initialement traité dans [Maz 1] lorsque Σ est formé des places au-dessus de p. On dispose de la formule d'Euler-Poincaré pour donner un majorant de $\mathrm{dimKrull} R(\bar{\rho})/pR(\bar{\rho})$. On distingue les représentations $\bar{\rho}$ paires de celles qui sont impaires. Le cas où $\bar{\rho}$ est impaire a été étudié notamment par Boston, en lien avec les formes modulaires [Bo 3] : de façon générale, on s'attend à ce que l'anneau $R(\bar{\rho})$ soit isomorphe à $\mathbb{Z}_p[[X_1, X_2, X_3]]$. Le cas où $\bar{\rho}$ est paire est traité par Böckle dans [Bö 4]. A chaque fois, les méthodes s'adaptent à l'image de $\bar{\rho}$; on peut consulter [Bo 1] pour les cas où $\bar{\rho}$ est impaire d'image modérée, ou contenant $\mathrm{SL}_2(\mathbb{F}_p)$ ou bien résoluble. Il est intéressant de produire des exemples pour lesquels l'anneau $R(\bar{\rho})$ est sans obstruction, i.e. de la forme $\mathbb{Z}_p[[X_1, \ldots, X_d]]$. On s'intéresse aux déformations sans obstruction pour deux raisons : il s'agit du cas le plus simple à traiter, mais surtout parce qu'elles sont les plus répandues dans la nature au moins lorsque $\bar{\rho}$ est impaire et absolument irréductible (on peut consulter [We 1]). Le principe dit "prime-to-adjoint" donne un cadre qui produit des déformations

sans obstruction ; le cas le plus simple est bien-sûr celui où le groupe $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ est libre (ou de manière générale lorsque l'on travaille avec des extensions p-rationnelles présentées dans [JN]).
Terminons en notant l'aspect arithmétique du principe prime-to-adjoint. On peut en effet le voir comme un dérivé du principe local-global : on cherche des situations où un noyau de Shafarevich est prime-to-adjoint. Par dualité, on peut se représenter ce problème en termes de groupe des classes, de sorte que des hypothèses du type "la p-partie du groupe des classes est triviale" débouchent sur une situation prime-to-adjoint. C'est dans cette perspective que la conjecture de Vandiver (ou plus généralement la théorie d'Iwasawa) intervient dans [BöMé] et [Mé 2].

Nous allons employer ces méthodes afin d'estimer la dimension de Krull d'un anneau de déformation provenant d'une représentation galoisienne associée à l'extension $\widetilde{K}_S^T/K$ définie précédemment.

3.6. Méthode de Boston

Soit $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue. On note K le sous-corps fixe par $\ker \bar{\rho}$. Le corps K est de degré fini sur $\mathbb{Q}$, notons S un ensemble fini de places de K contenant les places qui se ramifient dans K/k. Dans la suite, on note encore $\bar{\rho} : \mathrm{Gal}(k_S/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ la représentation que l'on souhaite déformer, avec k_S l'extension maximale de k non-ramifiée hors de places au-dessus de celles de S. Le groupe $\mathrm{Gal}(k_S/k)$ vérifie la propriété dite de p-finitude de Mazur, c'est cela qui assure l'existence d'une déformation dite verselle (cf. proposition 1.3.17).
Boston a mis au point une technique basée sur la théorie des groupes pour de expliciter les déformations de $\bar{\rho}$. Nous proposons un panorama de ces méthodes. Guidé par le désir de montrer au lecteur les techniques qui explicitent l'anneau de déformation et l'image de générateurs privilégiés (dans un sens plus général lorsque l'image de $\bar{\rho}$ n'est pas modérée), la preuve du théorème 3.6.5 de Boston est reproduite. Le plan d'étude est classique ([Bo 1], [Bo-Ma], [Bö 4] et [BöMé]) au moins dans un cadre semi-simple, i.e. lorsque p ne divise pas $|\mathrm{im}(\bar{\rho})|$.

On rappelle (cf. la sous-section 1.3.1) que $\Gamma(R) = ker\,(\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbb{F}_p))$ est un pro-p-groupe. En notant $K_S(p)$ la pro-p-extension maximale S-ramifiée de K dans $\overline{\mathbb{Q}}$, on voit que tout rélèvement de $\bar{\rho}$ se factorise par $\mathrm{Gal}(K_S(p)/k)$. Nous allons nous employer à dévisser ce groupe à l'aide du sous-groupe privilégié $\mathrm{Gal}(K_S(p)/K)$.

3.6.1. Théorie des groupes profinis. — Les trois résultats de théorie des groupes présentés dans cette sous-section sont à la base des observations faites par Boston pour expliciter les déformations d'une représentation $\bar{\rho}$. Ils figurent dans [Bo 1], le lemme de Schur-Zassenhaus est montré dans [Ro]. Soit P un pro-p-groupe et soit $P^p[P,P]$ le sous-groupe fermé de P engendré topologiquement par les puissances p-èmes et les commutateurs. Le quotient $P/P^p[P,P]$ est un p-groupe dès que P est topologiquement de type fini en tant que pro-p-groupe. Dans la suite, les propriétés des groupes profinis sont à prendre au sens topologique.

***Lemme 3.6.1* (théorème de la base de Burnside).** — *Si la famille $(x_1, \dots, x_n)$ forme une base du $\mathbb{F}_p$-espace vectoriel $P/P^p[P,P]$, alors $(x_1, \dots, x_n)$ engendre le pro-p-groupe P.*

Le lemme suivant dit de Schur-Zassenhaus (cf. [Ro], par exemple) donne une condition suffisante pour que la suite exacte $1 \to P \to G \to G/P \to 1$ soit scindée.

Lemme 3.6.2. — *Soit G un groupe profini et P un pro-p-sous-groupe de Sylow normal de G. On suppose P de type fini et d'indice fini dans G. Alors le groupe G possède un sous-groupe A isomorphe à G/P. Deux sous-groupes isomorphes à G/P sont conjugués par un élément de P.*

On conserve les hypothèses du lemme précédent et on note A un sous-groupe de G isomorphe à G/P. En regardant la structure de $\mathbb{F}_p[A]$-module, Boston montre :

***Proposition 3.6.3* ([Bo 1], Lem.2.4).** — *Soit V un $\mathbb{F}_p[A]$-sous-module de $P/P^p[P,P]$, alors il existe un sous-groupe A-invariant Q de P avec $\dim_{\mathbb{F}_p} V$ générateurs et tel que son image dans $P/P^p[P,P]$ engendre V. Les générateurs de Q sont appelés générateurs privilégiés.*

3.6.2. Cas modéré. — On rappelle que $\bar{\rho} : \mathrm{Gal}(k_S/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ est la représentation que l'on souhaite déformer.
Dans cette sous-section, l'image de $\bar{\rho}$ est supposée d'ordre premier à p. En notant $H = \mathrm{im}\bar{\rho}$, l'hypothèse faite sur $|H|$ assure que les $\mathbb{F}_p[H]$-modules sont semi-simples.
Par le théorème de la base de Burnside (cf. lemme 3.6.1), on peut écrire $\mathrm{Gal}(K_S(p)/k)$ comme le produit semi-direct suivant :

$$\mathrm{Gal}(K_S(p)/k) \simeq P \rtimes A,$$

où $P = \mathrm{Gal}(K_S(p)/K)$ est un pro-p-Sylow normal de $\mathrm{Gal}(K_S(p)/k)$ et A est l'image de H dans $\mathrm{Gal}(K_S(p)/k)$.
S'intéresser aux déformations de $\bar{\rho}$ revient ainsi à regarder les relèvements de $\bar{\rho}_{|P}$ et ceux de $\bar{\rho}_{|A}$ en tenant compte de l'action par conjugaison de A sur P. Cette observation est formulée en termes fonctorielles dans cette sous-section en comparant le foncteur de déformation $\mathrm{Hom}(R(\bar{\rho}), -)$ ($R(\bar{\rho})$ désigne l'anneau de déformation (uni)versel ici) avec un foncteur dit modéré obtenu en regardant des morphismes A-invariants définis sur P.

Comme $|A|$ est premier avec p, les espaces de cohomologie $H^i(A, \mathrm{Ad}(\bar{\rho}))$ sont triviaux pour $i = 1, 2$. Cela indique que l'anneau de déformation de $\bar{\rho} : A \to \mathrm{GL}_2(\mathbb{F}_p)$ est $\mathbb{Z}_p$. Le lemme de Schur-Zassenhaus appliqué à la suite exacte

$$1 \to \ker(\mathrm{GL}_2(\mathbb{Z}_p) \to H) \to \mathrm{GL}_2(\mathbb{Z}_p) \to H \to 1$$

permet de voir $H = \mathrm{im}\bar{\rho}$ comme un sous-groupe de $\mathrm{GL}_2(\mathbb{Z}_p)$. On note $[h]$ l'image d'un élément $h \in H$ dans $\mathrm{GL}_2(\mathbb{Z}_p)$.

Lemme 3.6.4. — *La déformation verselle de $\bar{\rho} : A \to \mathrm{GL}_2(\mathbb{F}_p)$ est donnée à isomorphisme près par le couple $(\mathbb{Z}_p, \rho_A)$ dont un représentant vérifie :*

$$\rho_A : A \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_p) \text{ et } \rho_A(x) = [\bar{\rho}(x)].$$

Démonstration. — Comme $\dim_{\mathbb{F}_p} H^1(A, \mathbb{F}_p) = 0$ et comme deux relèvements de $\bar{\rho}$ sont conjugués par un élément de $\Gamma(\mathbb{Z}_p) = \ker(\mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{F}_p))$, la représentation proposée dans le lemme est bien un représentant de la déformation verselle de $\bar{\rho}$. □

Chaque anneau $R \in \widehat{\mathcal{C}}$ admet un structure naturelle de $\mathbb{Z}_p$-algèbre donnée par un morphisme canonique

$$\mathbb{Z}_p \to R.$$

De cette façon, on récupère une action naturelle par conjugaison de A sur le noyau $\ker[\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbb{F}_p)]$, via $A \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(R)$, où la dernière flèche est induite par l'application naturelle $\mathbb{Z}_p \to R$.
On définit

$$\mathbf{T}(\bar{\rho})(R) := \mathrm{Hom}_A(P, \Gamma(R)), \text{ pour } R \in \widehat{\mathcal{C}}.$$

C'est le foncteur qui associe à chaque anneau $R \in \widehat{\mathcal{C}}$ l'ensemble des morphismes continus et A-invariants de P dans $\Gamma(R)$, pour l'action de A sur P et sur $\Gamma(R)$ décrite précédemment.
Le foncteur de déformation de $\bar{\rho}$ est désigné par $\mathbf{Def}(\bar{\rho})$, il associe à chaque anneau $R \in \widehat{\mathcal{C}}$ les déformations de $\bar{\rho}$ à valeurs dans $\mathrm{GL}_2(R)$:

$$\mathbf{Def}(\bar{\rho}) : \begin{cases} \widehat{\mathcal{C}} \to \mathrm{Ens} \\ R \mapsto \{ \text{ déformations de } \bar{\rho} \text{ de la forme } \rho_R : \mathrm{Gal}(K_S(p)/k) \to \mathrm{GL}_2(R) \} \end{cases}$$

où Ens est la catégorie des ensembles.
D'après le lemme 3.6.4 et comme $\mathrm{Gal}(K_S(p)/k) \simeq P \rtimes A$, il y a un morphisme naturel :

$$\mathbf{T}(\bar{\rho}) \to \mathbf{Def}(\bar{\rho}).$$

Théorème 3.6.5 (**[Bo 1], Prop. 6.1**). — *Le foncteur $\boldsymbol{T}(\bar{\rho})$ est représentable.*
Le morphisme naturel $\boldsymbol{T}(\bar{\rho}) \to \boldsymbol{Def}(\bar{\rho})$ est :
a) un isomorphisme lorsque le commutant de $\bar{\rho}$ vérifie $\mathrm{C}(\bar{\rho}) = \mathbb{F}_p$.
b) lisse (i.e. chaque surjection $R \twoheadrightarrow S$ induit une surjection $\boldsymbol{T}(\bar{\rho})(R) \to \boldsymbol{T}(\bar{\rho})(S) \times_{\boldsymbol{Def}(\bar{\rho})(S)} \boldsymbol{Def}(\bar{\rho})(R)$) et induit un isomorphisme des espaces tangents

$$\boldsymbol{T}(\bar{\rho})(\mathbb{F}_p[\varepsilon]) \to \boldsymbol{Def}(\bar{\rho})(\mathbb{F}_p[\varepsilon]).$$

Remarque 3.6.6. — D'après ce théorème, le foncteur $\mathbf{T}(\bar{\rho})$ est représentable par un anneau isomorphe à l'anneau de déformation universel lorsque $\mathrm{C}(\bar{\rho}) = \mathbb{F}_p$ ou versel dans le cas général (cf. proposition 1.2.7).

Démonstration. — Soit $(x_1, \ldots, x_d)$ un système de générateurs topologiques de P. Se donner un morphisme $P \to \Gamma(R)$ revient à se donner l'image de chaque x_j, i.e. une famille de matrices $\begin{pmatrix} 1+m_{1,j} & m_{2,j} \\ m_{3,j} & 1+m_{4,j} \end{pmatrix}$, avec $m_{i,j} \in m_R$. Les relations entre les x_j dans P et l'action de A sur un tel morphisme $P \to \Gamma(R)$ fournissent des équations sur les $m_{i,j}$. Le foncteur $\mathbf{T}(\bar{\rho})$ est ainsi représenté par l'anneau quotient $\mathbb{Z}_p[[X_{i,j} | \ 1 \leq i \leq 4, 1 \leq j \leq d]]/I$, où l'idéal I provient des équations associées aux relations entre les x_j dans P et à l'action de A[(1)].

[(1)] Un tel raisonnement se généralise en dimension n, l'anneau qui représente le foncteur est un quotient de l'anneau des séries formelles sur $\mathbb{Z}_p$ en dn^2 indéterminées.

On fixe $R \in \widehat{\mathcal{C}}$. Pour montrer le point a), il s'agit de montrer que $\mathbf{T}(\bar{\rho})(R) \to \mathbf{Def}(\bar{\rho})(R)$ est bijective. Une déformation (R, ρ) de $\bar{\rho}$ induit un relèvement $\rho_A : A \to \mathrm{GL}_2(R)$ de $\bar{\rho}_{|A}$, n'importe quel relèvement à R de $\bar{\rho}_{|A}$ lui est $\Gamma(R)$-conjugué. Autrement dit, à conjugaison près, on n'a pas le choix pour le relèvement ρ_A. C'est exactement le sens du lemme 3.6.4. La surjectivité est démontrée, sans avoir eu à utiliser l'hypothèse $\mathrm{C}(\bar{\rho}) = \mathbb{F}_p$.

Supposons à présent que $\mathrm{C}(\bar{\rho}) = \mathbb{F}_p$. On note h_1 et h_2 deux éléments de $\mathbf{T}(\bar{\rho})(R)$ qui induisent la même déformation $[\rho_R] \in \mathbf{Def}(\bar{\rho})(R)$. Deux représentants différents ρ_1 et ρ_2 de $[\rho_R]$ sont conjugués par une matrice de $\Gamma(R)$, disons M. En particulier $\rho_1(x) = M\rho_2(x)M^{-1}$, pour tout $x \in A$. Nécessairement, M est une homothétie d'après l'hypothèse $\mathrm{C}(\bar{\rho}) = \mathbb{F}_p$ et donc $\rho_1 = \rho_2$, i.e. $h_1 = h_2$. L'injectivité est démontrée.

Enfin, pour montrer la lissité on s'y prend de la même façon que pour la surjectivité dans le point a). D'autre part, il suffit de remarquer, pour prouver l'isomorphisme des espaces tangents, que le groupe $\Gamma(\mathbb{F}_p[\varepsilon])$ est abélien et agit donc trivialement sur l'espace tangent $\mathbf{T}(\bar{\rho})(\mathbb{F}_p[\varepsilon])$ de $\mathbf{T}(\bar{\rho})$. □

L'application $M \mapsto 1+\varepsilon M$ montre que l'adjoint $\mathrm{Ad}(\bar{\rho})$ est isomorphe au A-module $\Gamma(\mathbb{F}_p[\varepsilon])$. On note $< P/P^p[P,P], \mathrm{Ad}(\bar{\rho}) >_{|A}$ le produit scalaire des caractères associés aux A-modules $P/P^p[P,P]$ et $\mathrm{Ad}(\bar{\rho})$. Le résultat suivant est une conséquence du théorème précédent puisque la dimension de l'espace tangent d'un foncteur est égal au nombre de variables de l'anneau de déformation (uni)versel associé à ce foncteur.

Corollaire 3.6.7 **([Bo 1], Cor. 6.2)**. — *Soit $\bar{\rho}$ continue.*
L'anneau de déformation (uni)versel de $\bar{\rho}$ est un quotient de $\mathbb{Z}_p[[X_1, \ldots, X_d]]$, où le nombre de variables $d =< P/P^p[P,P], \mathrm{Ad}(\bar{\rho}) >_{|A}$.

Remarque 3.6.8. — Ce corollaire peut se montrer directement. La théorie des déformations nous dit que le nombre d est égal à $\dim_{\mathbb{F}_p} H^1(\mathrm{Gal}(K_S(p)/k), \mathrm{Ad}(\bar{\rho}))$. La suite exacte de Hoschild-Serre nous assure, puisque $|A|$ est premier avec p et que $\mathrm{Gal}(K_S(p)/k) \simeq P \rtimes A$, que

$$H^1(\mathrm{Gal}(K_S(p)/k), \mathrm{Ad}(\bar{\rho})) \simeq \mathrm{Hom}_A(P, \mathrm{Ad}(\bar{\rho})) = \mathrm{Hom}_A(P/P^p[P,P], \mathrm{Ad}(\bar{\rho})).$$

3.6.3. Le principe "prime-to-adjoint". — Ce principe donne une condition suffisante de non-obstruction pour l'anneau de déformation (uni)versel de $\bar{\rho}$ ([Bo 1]), autrement dit assure que cet anneau est de la forme

$$\mathbb{Z}_p[[X_1, \ldots, X_d]],$$

avec $d = \dim_{\mathbb{F}_p} H^1(\mathrm{Gal}(K_S(p)/k), \mathrm{Ad}(\bar{\rho}))$.
On sait que l'obstruction provient du second groupe de cohomologie

$$H^2(\mathrm{Gal}(K_S(p)/k), \mathrm{Ad}(\bar{\rho})),$$

c'est donc cet espace qu'il nous faut contrôler. On peut voir le principe "prime-to-ajoint" comme l'analogue en théorie des déformations du principe local-global concernant les relations du groupe G_S (dès que $Ш(G_S, \mathbb{F}_p)$ est trivial).

Définition 3.6.9. — On dit d'un $\mathbb{F}_p[H]$-module M qu'il est premier avec $\mathrm{Ad}(\bar{\rho})$ lorsque ces deux modules ne possèdent pas de caractère irréductible commun : $< M, \mathrm{Ad}(\bar{\rho}) >_H = 0$.

Lorsque S contient les places archimédiennes et les places au-dessus de p, la fin de la suite exacte de Poitou-Tate ([NSW], Th. 8.6.10) s'écrit :

$$0 \to Ш(G_S, \mathrm{Ad}(\bar{\rho})) \to H^2(G_S, \mathrm{Ad}(\bar{\rho})) \to \bigoplus_{v \in S} H^2(G_v, \mathrm{Ad}(\bar{\rho})) \to H^0(G_S, \mathrm{Ad}(\bar{\rho})')^* \to 0,$$

où $G_S = \mathrm{Gal}(k_S/k)$, $Ш(G_S, \mathrm{Ad}(\bar{\rho}))$ est défini par la suite exacte, G_v est le groupe de décomposition de G_S en v, $\mathrm{Ad}(\bar{\rho})' = \mathrm{Hom}(\mathrm{Ad}(\bar{\rho}), \mu_p)$ et * désigne le dual de Pontryagin.
On suppose encore que $\bar{\rho}$ admet une image modérée H. On dispose ainsi de l'isomorphisme

$$H^2(P, \mathrm{Ad}(\bar{\rho}))^H \simeq H^2(G_S, \mathrm{Ad}(\bar{\rho})),$$

avec les notations des sous-sections précédentes. Or, le groupe $P = \ker \bar{\rho}$ agit trivialement sur l'adjoint, donc $H^2(P, \mathrm{Ad}(\bar{\rho})) = H^2(P, \mathbb{F}_p) \otimes \mathrm{Ad}(\bar{\rho})$.

Lemme 3.6.10. — *On a l'équivalence suivante : $H^2(P, \mathbb{F}_p)$ est premier avec $\mathrm{Ad}(\bar{\rho})$ si et seulement si $Ш(P, \mathbb{F}_p)$ et $\mathrm{coker}(\mu_p(K) \to \bigoplus_{v \in S} \mu_p(K_v))$ le sont.*

Démonstration. — Cela provient de la suite de Poitou-Tate rappelée ci-dessus. □

La description de la structure du H-module $P/P^p[P,P]$ ([Ko] et [Bo-Ma]) permet d'expliciter la déformation universelle dans le cas prime-to-adjoint. C'est ce que nous présentons ici.
On rappelle que K_v désigne le complété de K en v. On définit le module de Kummer

$$V_S = \{a \in K^\times |\ (a) \text{ soit une puissance } p\text{-ème et } a \in K_v^p \text{ pour tout } v \in S\},$$

et

$$W_S = \mathrm{coker}(\mu_p(K) \to \bigoplus_{v \in S} \mu_p(K_v)).$$

Lemme 3.6.11. — *On suppose que l'ensemble fini de places S contient les places au-dessus de p et les places archimédiennes. Supposons les ordres de H et du groupe des classes du corps K premiers avec p. On note H_∞ le sous-groupe de H image d'une conjugaison complexe, il est donc trivial ou d'ordre 2. Alors le $\mathbb{F}_p[H]$-module $P/P^p[P,P]$ est isomorphe à*

$$V_S/K^{\times p} \oplus W_S \oplus \mathbb{F}_p \oplus \mathrm{ind}_{H_\infty}^H(\mathrm{ind}_1^{H_\infty}(\mathbf{1}) - \mathbf{1}).$$

Les générateurs privilégiés de P associés à $\mathbb{F}_p$ et $\mathrm{ind}_{H_\infty}^H(\mathrm{ind}_1^{H_\infty}(\mathbf{1}) - \mathbf{1})$ sont respectivement notés x et y, ceux associés à $V_S/K^{\times p}$ et W_S sont notés de façon générique z (cf. proposition 3.6.3).

Démonstration. — C'est une conséquence de [Bo 1, Prop. 3.2] et de la suite exacte

$$0 \to V_S/K^{\times p} \to U/U^p \to \bigoplus_{v \in S} U_v/U_v^p \to P/P^p[P,P] \to 0,$$

où U, U_v désignent respectivement les unités globales et locales de K et K_v. Par la théorie du corps de classes ([Bo 1] §.3), l'exactitude provient du fait que l'ordre du groupe de classes de K est premier avec p. □

Remarque 3.6.12. — Lorsque H_∞ est non-trivial, l'induite $\mathrm{ind}_1^{H_\infty}(\mathbf{1})$ est la somme de la représentation triviale et de la représentation de dimension 1 sur laquelle H_∞ agit (non-trivialement) de manière involutive. Dans le théorème qui suit, on suppose la représentation $\bar{\rho}$ impaire, cela signifie que H_∞ est non-trivial.

Théorème 3.6.13 **([Bo 1], Prop. 6.3)**. — *Supposons $\bar{\rho} : \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ impaire et notons H son image. On suppose que l'ensemble fini de places S contient les places au-dessus de p et les places archimédiennes. Supposons les ordres de H et du groupe des classes du corps K premiers avec p.*
Enfin, supposons que les deux $\mathbb{F}_p[H]$-modules $V_S/K^{\times p}$ et W_S sont premiers avec l'adjoint. Alors l'anneau $R(\bar{\rho})$ est isomorphe à $\mathbb{Z}_p[[X_1, X_2, X_3]]$ et la déformation (uni)verselle ρ vérifie

$$\rho(x) = \begin{pmatrix} 1+X_1 & 0 \\ 0 & 1+X_1 \end{pmatrix},$$

$$\rho(y) = \begin{pmatrix} \sqrt{1+X_2X_3} & X_2 \\ X_3 & \sqrt{1+X_2X_3} \end{pmatrix},$$

et

$$\rho(z) = 1,$$

pour x, y et z les générateurs privilégiés de P mis en évidence dans le lemme 3.6.11.

Démonstration. — D'après le lemme 3.6.11, le produit $< P/P^p[P,P], \mathrm{Ad}(\bar{\rho}) >$ est égal à 3, ce qui implique de l'anneau de déformation est un quotient de $\mathbb{Z}_p[[X_1, X_2, X_3]]$ (cf. corollaire 3.6.7). On précise de nouveau les rôles joués par x, y, z. Selon la terminologie de la propositon 3.6.3, notons x, y des générateurs privilégiés de P tels que x soit fixe sous l'action de H et tels que la conjugaison complexe transforme y en y^{-1}. Autrement dit x est associé, grâce à la proposition 3.6.3, à la représentation triviale dans le lemme 3.6.11 et y à l'induite. Les autres générateurs privilégiés (notés z de façon générique) sont ceux associés aux modules $V_S/K^{\times p}$ et W_S premiers à l'adjoint, et leurs images par $\bar{\rho}$ sont triviales donc $\rho(z) = 1$.
On se donne un représentant de la déformation à A de $\bar{\rho}$ pour fixer les idées. Les conjugués de x, y, z sous l'action de A engendrent P d'après la proposition 3.6.3 et le lemme 3.6.1. Or on sait que les images de x et y par ρ vivent dans $\Gamma(R(\bar{\rho}))$ et on connait l'action (par conjugaison) de A sur $\rho(x)$ et $\rho(y)$ qui vient juste d'être décrite : $\rho(x)$ est fixe sous l'action de A, c'est donc une homothétie (car $\mathrm{C}(\bar{\rho}) = \mathbb{F}_p$) et la conjugaison complexe transforme $\rho(y)$ en $\rho(y)^{-1}$. En supposant que $\rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, où c désigne une conjugaison complexe, il est facile de voir que l'image la plus générale pour y est proposée par le théorème. Au passage, cela montre que $R(\bar{\rho}) \simeq \mathbb{Z}_p[[X_1, X_2, X_3]]$. □

Remarque 3.6.14. — Le lemme 3.6.10 indique directement que l'anneau $R(\bar{\rho})$ est sans obstruction. En effet, l'inclusion $Ш(P, \mathbb{F}_p) \hookrightarrow V_S/K^{\times p}$ ([Ko]) permet de dire que $Ш(P, \mathbb{F}_p)$ est premier avec l'adjoint lorsque $V_S/K^{\times p}$ l'est.

3.6.3.1. Exemple 1. — On a toujours S un ensemble fini de places de K contenant les places archimédiennes et les places au-dessus de p.
Remarquons que la preuve du lemme 3.6.10 montre que P est libre dès que $V_S/K^{\times p}$ et W_S sont nuls, puisque $Ш(P,\mathbb{F}_p) \subseteq V_S/K^{\times p}$.
La plupart des exemples classiques reposent sur cette observation, il s'agit de trouver une situation arithmétique favorable pour avoir un groupe P libre. On mentionne brièvement l'exemple générique des extensions cubiques spéciales ([Maz 1], [Bo-Ma]).

Soit $a \in \mathbb{Z}$ tel que $p = 27 + 4a^3$ soit premier. On note K la clôture galoisienne du corps cubique (dit spéciale) $\mathbb{Q}(x)$ où x est une racine (réelle) du polynôme $X^3 + aX + 1$; notons que le discriminant de $\mathbb{Q}(x)$ est égal à $-p$. Ici, $k = \mathbb{Q}$.
On fixe un plongement $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{S}_3 \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$, ce qui est possible car 3 divise l'ordre de $\mathrm{GL}_2(\mathbb{F}_p)$. Ce plongement définit une représentation résiduelle

$$\bar{\rho}_{\text{cubique}} : \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Mazur montre ([Maz 1], §1.13, Prop.8) que pour de tels premiers p, les modules $V_S/K^{\times p}$ et W_S sont nuls. La représentation $\bar{\rho}_{\text{cubique}}$ vérifie les hypothèses du théorème 3.6.13. Voici des exemples de tels nombres p : $23, 31, 59, 283, 1399, 4027, 5351$. On peut consulter [Maz 1] pour une liste complète de tels $p < 10^6$.

3.6.3.2. Exemple 2. — Dans le même contexte, Maire ([Mai]) étudie le cas où S ne contient pas toutes les places au-dessus de p. En particulier, la suite exacte de Poitou-Tate ne peut pas être évoquée. Les extensions cubiques dites spéciales fournissent là-aussi une famille d'exemples. Le point de vue est toutefois différent, des conditions supplémentaires sur p ressortent.
On note $a \in \mathbb{N}$ et $d = 27 + 4a^3$. Ici $k = \mathbb{Q}(\sqrt{-d})$ et K désigne la clôture galoisienne de $\mathbb{Q}(x)$, avec x racine (réelle) de $X^3 + aX + 1$. L'extension K/k est non-ramifiée, notons H son groupe de Galois. On choisit alors un nombre premier p totalement décomposé dans K/k, ne divisant ni d ni l'ordre du groupe des classes de K et pour lequel il existe une injection $H \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$. Supposons H différent du groupe des matrices scalaires.
Il y a deux places v et w au-dessus de p dans K, notons $S = \{v\}$. Il s'agit alors de déformer

$$\bar{\rho}_{\{v\}} : \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \twoheadrightarrow H \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Une condition suffisante pour que $\mathrm{Gal}(K_S(p)/K)$ soit libre est mise en évidence ([Mai], Prop.2.5). On est bien sûr dans le cas prime-to-adjoint. Voici des couples (d,p) qui vérifient de telles conditions (et pour lesquels l'anneau de déformation (uni)versel de $\bar{\rho}_{\{v\}}$ est $\mathbb{Z}_p[[X,Y]]$) : $(59,17), (59,71), (283,71), (283,73), (283,83)$.

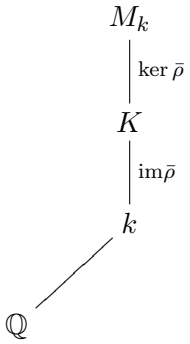
3.7. Dimension de Krull de $\widetilde{R}_S^T/p$

Le contexte arithmétique suivant est dicté par la théorie des formes modulaires mod p qui sont compagnons. Les sous-corps fixés par des déformations de représentations mod p (de dimension 2) associées à de telles formes modulaires possèdent des propriétés locales analogues aux extensions présentées ci-dessous (cf. chapitre 2).
Soit k un corps de nombres. On note S et T deux ensembles finis et disjoints de places de k avec $T \subseteq Pl_p(k)$. On suppose que S est *non-vide*, cette hypothèse va nous permettre d'utiliser les estimations les plus fines dont nous disposons concernant les espaces de cohomologie H^2.

Dans la suite, M_k désigne l'extension maximale de k contentant la $\mathbb{Z}_p$-extension cyclotomique k^{cyc} de k telle que M_k/k^{cyc} soit S-ramifiée et T-décomposée [(2)].
Soit

$$\bar{\rho} : \mathrm{Gal}(M_k/k) \to \mathrm{GL}_2(\mathbb{F}_p)$$

une représentation continue. Notons K le sous-corps fixé par le noyau de $\bar{\rho}$; cela définit la tour d'extensions suivante :



Comme le groupe $\mathrm{Gal}(M_k/k)$ vérifie donc l'hypothèse de p-finitude de Mazur, on peut énoncer le lemme qui suit.

Lemme 3.7.1. — *La déformation (uni)verselle de* $\bar{\rho} : \mathrm{Gal}(M_k/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ *existe, notons la* $(\widetilde{R}_S^T, \widetilde{\rho})$. *L'anneau* $\widetilde{R}_S^T$ *vérifie*

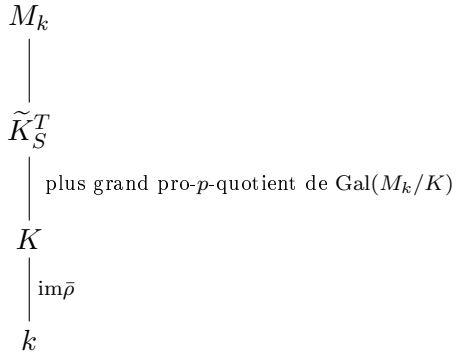
$$\mathrm{dimKrull}(\widetilde{R}_S^T/p\widetilde{R}_S^T) \geq \dim_{\mathbb{F}_p} H^1(\mathrm{Gal}(M_k/k), \mathrm{Ad}(\bar{\rho})) - \dim_{\mathbb{F}_p} H^2(\mathrm{Gal}(M_k/k), \mathrm{Ad}(\bar{\rho})),$$

avec égalité dès que $\dim_{\mathbb{F}_p} H^2(\mathrm{Gal}(M_k/k), \mathrm{Ad}(\bar{\rho})) = 0$.

Puisque la restriction suivante

$$\widetilde{\rho} : \mathrm{Gal}(M_k/K) \to \mathrm{GL}_2(\widetilde{R}_S^T)$$

prend ses valeurs dans le pro-p-groupe $\Gamma(R)$, elle se factorise à travers le plus grand pro-p-quotient de $\mathrm{Gal}(M_k/K)$. Par maximalité, ce pro-p-quotient est aussi $\mathrm{Gal}(\widetilde{K}_S^T/K)$. Autrement dit, lorsque l'on étudie la restriction à $\ker\bar{\rho}$ des relèvements de $\bar{\rho}$, on peut se ramener à la tour d'extensions suivante :



Regroupons alors les parties d'ordre une puissance de p. Plus précisément, supposons qu'une des deux situations suivantes se produise :

[(2)]On devrait noter $(k^{cyc})_S^T$ cette extension M_k, ce qui n'est pas du goût de tout le monde.

– *Cas semi-simple :* l'image $\mathrm{im}\bar{\rho}$ est d'ordre premier à p.
– *Cas p-Sylow :* l'image $\mathrm{im}\bar{\rho}$ possède un unique p-Sylow, noté P.

Quitte à considérer l'extension K^P au lieu de K lorsque l'on étudie les restrictions à $\ker\bar{\rho}$ de relèvements de $\bar{\rho}$, on peut supposer (toujours par maximalité de propriétés arithmétiques en jeu ici) que nous sommes dans la cas semi-simple. Désignons alors

$$H = \mathrm{im}\bar{\rho}.$$

On note $Pl_\infty(k)^+$ l'ensemble des places v pour lesquelles $\bar{\rho}_{|H_v}$ est paire et $Pl_\infty(k)^-$ l'ensemble des places v pour lesquelles $\bar{\rho}_{|H_v}$ est impaire[(3)] avec H_v un groupe de décomposition de v ; de cette façon, on a

$$|Pl_\infty(k)^+| + |Pl_\infty(k)^-| = r_1(k) + r_2(k),$$

avec

$$r_2(k) \leq |Pl_\infty(k)^+| \text{ et } |Pl_\infty(k)^-| \leq r_1(k).$$

On énonce le résultat principal de cette section.

Théorème 3.7.2. — *Soit $\bar{\rho} : \mathrm{Gal}(M_k/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue. Notons K le sous-corps fixé par le noyau de $\bar{\rho}$. Soit $\mathrm{Ad}(\bar{\rho})$ la représentation adjointe de $\bar{\rho}$. Notons $\widetilde{R}_S^T$ l'anneau de déformation de $\bar{\rho}$. Alors*

$$\mathrm{dimKrull}(\widetilde{R}_S^T/p\widetilde{R}_S^T) \geq \dim_{\mathbb{F}_p}\mathrm{Ad}(\bar{\rho})^H + 4\sum_{v\in S_p}[k_v:\mathbb{Q}_p] - 4|Pl_\infty(k)^+| - 2|Pl_\infty(k)^-|,$$

où S_p est formé des places de S qui sont au-dessus de p.

Démonstration. — Comme l'ordre de l'image H est premier avec p, la suite de Hoschild-Serre assure que

$$H^i(\ker\bar{\rho}, \mathrm{Ad}(\bar{\rho}))^H \simeq H^i(\mathrm{Gal}(M_k/k), \mathrm{Ad}(\bar{\rho})), \text{ pour } i = 1, 2.$$

Puisque l'action du noyau sur l'adjoint est triviale, il vient

$$H^i(\ker\bar{\rho}, \mathrm{Ad}(\bar{\rho}))^H \simeq (H^i(\ker\bar{\rho}, \mathbb{F}_p) \otimes \mathrm{Ad}(\bar{\rho}))^H.$$

Par ailleurs, la dimension de l'espace des points fixes peut être vue à travers l'égalité

$$\dim_{\mathbb{F}_p}(H^i(\ker\bar{\rho}, \mathbb{F}_p) \otimes \mathrm{Ad}(\bar{\rho}))^H = < \varphi(H^i(\ker\bar{\rho}, \mathbb{F}_p))^*, \mathrm{Ad}(\bar{\rho}) >_H .$$

Pour exprimer

$$\dim_{\mathbb{F}_p}H^1(\mathrm{Gal}(M_k/k), \mathrm{Ad}(\bar{\rho})) - \dim_{\mathbb{F}_p}H^2(\mathrm{Gal}(M_k/k), \mathrm{Ad}(\bar{\rho})),$$

il suffit donc de calculer

$$< \varphi(H^1(\ker\bar{\rho}, \mathbb{F}_p))^* - \varphi(H^2(\ker\bar{\rho}, \mathbb{F}_p))^*, \mathrm{Ad}(\bar{\rho}) > .$$

A l'aide du théorème 3.4.1, on sait que

$$\varphi(H^1(\ker\bar{\rho}, \mathbb{F}_p)) - \varphi(H^2(\ker\bar{\rho}, \mathbb{F}_p)) \geq \mathbf{1} + \sum_{v\in S_p}[k_v:\mathbb{Q}_p]\varphi(\mathrm{Reg}) - \sum_{v\in Pl_{\infty(k)}} \mathrm{ind}_{H_v}^H \mathbf{1},$$

et ainsi, grâce à la réciprocité de Frobenius :

$$< (\varphi(H^1(\ker\bar{\rho}, \mathbb{F}_p)) - \varphi(H^2(\ker\bar{\rho}, \mathbb{F}_p)))^*, \mathrm{Ad}(\bar{\rho}) > \geq$$

(3) On rappelle que $\bar{\rho}_{|H_v}$ est dite paire lorsque son image dans $\mathrm{PGL}_2(\mathbb{F}_p)$ est triviale et impaire dans le cas contraire.

$$< \mathbf{1}, \mathrm{Ad}(\bar{\rho}) > +4 \sum_{v \in S_p} [k_v : \mathbb{Q}_p] - \sum_{v \in Pl_\infty(k)} < \mathbf{1}, \mathrm{Ad}(\bar{\rho}) >_{|H_v} .$$

Pour conclure, il reste à décrire le comportement des places réelles et complexes du corps de nombres k. Si v est complexe, le groupe de décomposition H_v est triviale et dans ce cas, le produit $< \mathbf{1}, \mathrm{Ad}(\bar{\rho}) >_{|H_v}$ est égal à la dimension de l'adjoint. Lorsque v est réelle, il y a trois cas possibles :
– H_v est trivial et on vient de voir que $< \mathbf{1}, \mathrm{Ad}(\bar{\rho}) >_{|H_v} = 4$.
– H_v est d'ordre 2 et son action sur l'adjoint est triviale, on a encore $< \mathbf{1}, \mathrm{Ad}(\bar{\rho}) >_{|H_v} = 4$.
– H_v est d'ordre 2 et son action sur l'adjoint transforme la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ en la matrice $\begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$. On a alors $< \mathbf{1}, \mathrm{Ad}(\bar{\rho}) >_{|H_v} = 2$.

□

Remarque 3.7.3. — Dès que le groupe $\mathrm{Gal}(\widetilde{K}_S^T/K)$ est libre, on est dans la situation dite prime-to-adjoint, autrement dit l'anneau $R(\bar{\rho})$ est sans obstruction. Ainsi, les propositions 3.4.22 et 3.4.24 (en particulier l'exemple 3.4.23) fournissent des illustrations simples du théorème ci-dessus.

Intéressons-nous au minorant proposé. Celui-ci fait intervenir des espaces de points fixes dont les dimensions sont décrites dans le lemme suivant : elles peuvent prendre les valeurs $4, 2$ ou 1.

Lemme 3.7.4. — *Soit M un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_p)$ dont l'ordre est premier avec p. On dispose des égalités suivantes selon M :*

$$\dim_{\mathbb{F}_p} \mathrm{Ad}(\bar{\rho})^M = \begin{cases} 4 & \text{si } M \text{ est formé d'homothéties,} \\ 2 & \text{si } M \text{ est un groupe de Cartan déployé ou non-déployé,} \\ 1 & \text{si } M \text{ est projectivement diédral,} \\ 1 & \text{sinon.} \end{cases}$$

La preuve repose sur le lemme suivant de théorie des groupes, qui provient de considérations géométriques dans le cas $\mathrm{PGL}_2(\mathbb{C})$ et s'en déduit par le principe de Lefschetz.

Lemme 3.7.5 ([Se 2], **§.2.6**). — *Soit M un sous-groupe fini de $\mathrm{GL}_2(\mathbb{F}_p)$ d'ordre premier à p. On note $\overline{M}$ son image dans $\mathrm{PGL}_2(\mathbb{F}_p)$.*
Alors M satisfait un des cas suivants :
1) $\overline{M}$ est cyclique, donc M est contenu dans un sous-groupe de Cartan (unique lorsque $\overline{M} \neq \{1\}$).
2) $\overline{M}$ est isomorphe à un groupe diédral D_{2r} pour un certain r premier avec p.
3) $\overline{M}$ est isomorphe à A_4, S_4, A_5.

Démonstration du lemme 3.7.4. — Lorsque $\chi : \mathbb{F}_p \to \mathbb{F}_p^\times$ est un caractère, on désigne par $\mathbb{F}_p(\chi)$ le module $\mathbb{F}_p$ muni de l'action $m \cdot x = \chi(m)x$. La première chose à voir est la décomposition

$$\mathrm{Ad}(\bar{\rho}) \simeq \mathbb{F}_p \oplus \mathrm{Ad}^0(\bar{\rho}),$$

en tant que M-modules.

1) Le cas où M est constitué uniquement d'homothéties est trivial, car alors $\mathrm{Ad}(\bar{\rho}) \simeq \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p$.
2) Dans le cas d'un Cartan déployé, on peut supposer que l'action sur l'adjoint se fait grâce à une matrice diagonale $\begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$ avec χ_1, χ_2 deux caractères distincts et donc

$$\mathrm{Ad}(\bar{\rho}) \simeq \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p(\chi_1\chi_2^{-1}) \oplus \mathbb{F}_p(\chi_1^{-1}\chi_2).$$

Dans le cas d'un Cartan non-déployé, le groupe M est cyclique d'ordre p^2-1. En choisissant une bonne base, on trouve finalement

$$\mathrm{Ad}(\bar{\rho}) \simeq \mathbb{F}_p \oplus \mathbb{F}_p \oplus V_2,$$

où V_2 est irréductible. On peut par exemple voir le module des points fixes comme celui formé des homothéties et des matrices de la forme $\begin{pmatrix} -\frac{a}{2}x & -bx \\ x & \frac{a}{2}x \end{pmatrix}$, avec a et b fixés tels que $a^2 - 4b \notin \mathbb{F}_p^2$, cela provient de la description d'un Cartan non-déployé.
3) On suppose que projectivement, M est de la forme $\mathbb{Z}/r\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, on note s un générateur de $\mathbb{Z}/2\mathbb{Z}$ qui agit par $x \mapsto -x$ sur $\mathrm{Ad}(\bar{\rho})$; en particulier s agit sur les matrices diagonales de $\mathrm{Ad}^0(\bar{\rho})$. On trouve finalement

$$\mathrm{Ad}(\bar{\rho}) \simeq \mathbb{F}_p \oplus \mathbb{F}_p(s) \oplus V_2,$$

où V_2 est irréductible.
4) Pour terminer lorsque projectivement M est de la forme A_4, S_4, A_5, en décrivant les actions des transpositions, on voit que le module $\mathrm{Ad}^0(\bar{\rho})$ est irréductible. □

Remarque 3.7.6. — Le groupe H n'est pas formé d'homothéties puisque $\mathrm{C}(\bar{\rho}) = \mathbb{F}_p$ et ainsi la dimension de l'espace des points fixes $\mathrm{Ad}(\bar{\rho})^H$ ne dépasse pas 2. Le minorant donné dans le théorème 3.7.2 appartient donc à l'intervalle suivant :

$$\left[1 - 4(r_1(k) + r_2(k)) + 2|Pl_\infty(k)^-| \ , \ 2 + 4r_2(k) + 2|Pl_\infty(k)^-|\right].$$

La question naturelle est alors de savoir quand la minoration de la dimension de Krull que l'on a montrée s'avère pertinente, autrement dit de connaître une condition suffisante pour que le terme de droite dans l'inégalité du théorème 3.7.2 soit positif. On cherche une condition ne portant que sur l'arithmétique du corps k.

Proposition 3.7.7. — *On conserve les hypothèse du théorème 3.7.2.*
Supposons que $\sum_{v\in S_p}[k_v : \mathbb{Q}_p] \geq r_1(k) + r_2(k)$. *Alors l'inégalité du théorème 3.7.2 n'est pas triviale, autrement dit le minorant est supérieur ou égal à* 0.

Démonstration. — Il suffit d'écrire sous une autre forme la combinaison suivante :

$$4\sum_{v\in S_p}[k_v : \mathbb{Q}_p] - \sum_{v\in Pl_\infty(k)} < 1, \mathrm{Ad}(\bar{\rho}) >_{|H_v} =$$

$$4\left(\sum_{v\in S_p}[k_v : \mathbb{Q}_p] - (r_1(k) + r_2(k))\right) + \sum_{v\in Pl_\infty(k)} < \mathrm{ind}_{H_v}^H \mathrm{ind}_1^{H_v} 1 - \mathrm{ind}_{H_v}^H 1, \mathrm{Ad}(\bar{\rho}) > .$$

On peut conclure car la représentation triviale figure dans $\mathrm{ind}_1^{H_v} 1$. □

Dans le corollaire suivant, retrouvons un cas pour lequel la minoration est bonne. Ce résultat est prouvé dans ([Maz 1], § 1.10, Prop. 5) dans le cas particulier où T est vide.

Corollaire 3.7.8. — *Supposons que* $S_p = Pl_p(k)$. *Alors*

$$\mathrm{dimKrull}(\widetilde{R}_S^T/p\widetilde{R}_S^T) \geq 1 + 4r_2(k) + 2|Pl_\infty(k)^-|.$$

Remarque 3.7.9. — Lorsque la représentation à déformer est $\bar{\rho} : \mathrm{Gal}(k_S/k) \to \mathrm{GL}_2(\mathbb{F}_p)$, avec k_S l'extension maximale de k non-ramifiée hors de $S = Pl_p(k)$, alors l'anneau de déformation $R(\bar{\rho})$ de cette représentation vérifie également

$$\mathrm{dimKrull}(R(\bar{\rho})/pR(\bar{\rho})) \geq 1 + 4r_2(k) + 2|Pl_\infty(k)^-|.$$

Cette inégalité provient de la dualité de Poitou-Tate appliquée au groupe $\mathrm{Gal}(k_S/k)$, avec $S = Pl_p$ ([Maz 1]).

Remarque 3.7.10. — Si $S_p = \emptyset$, alors le minorant du théorème 3.7.2 est strictement négatif dès que k est différent de $\mathbb{Q}$. En fait, le minorant est inférieur ou égal à $2 - 2r_1(k) - 4r_2(k)$.

BIBLIOGRAPHIE

[AT] E. Artin, J. Tate, *Class field theory*, Reprinted with corrections from the 1967 original, AMS Chelsea Publishing, Providence, RI, 2009.

[BM] J. Bertin, A. Mézard, *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques*, Invent. Math. **141** (2000), no. 1, 195–238.

[Bö 1] G. Böckle, *Presentations of universal deformation rings*, L-functions and Galois representations, 24–58, London Math. Soc. Lecture Note Ser., **320**, Cambridge Univ. Press, Cambridge, 2007.

[Bö 2] G. Böckle, *The generic fiber of the universal deformation space associated to a tame Galois representation*, Manuscripta Math. **96** (1998), no. 2, 231–246.

[Bö 3] G. Böckle, *A local-to-global principle for deformations of Galois representations*, J. Reine Angew. Math. **509** (1999), 199–236.

[Bö 4] G. Böckle, *Explicit universal deformations of even Galois representations*, Math. Nachr. **206** (1999), 85–110.

[Bö 5] G. Böckle, *Demuškin groups with group actions and applications to deformations of Galois representations*, Compositio Math. **121** (2000), no. 2, 109–154.

[Bö 6] G. Böckle, *On the density of modular points in universal deformation spaces*, Amer. J. Math. **123** (2001), no. 5, 985–1007.

[Bö 7] G. Böckle, *Lifting mod p representations to characteristics p^2*, J. Number Theory **101** (2003), no. 2, 310–337.

[Bö 8] G. Böckle, *Deformations and the rigidity method*, J. Algebra **320** (2008), no. 10, 3613–3658.

[Bö 9] G. Böckle, *Deformation rings for some mod 3 Galois representations of the absolute Galois group of $\mathbb{Q}_3$*, Astérisque No. **330** (2010), 529–542.

[BöMé] G. Böckle, A. Mézard, *The prime-to-adjoint principle and unobstructed Galois deformations in the Borel case*, J. Number Theory **78** (1999), no. 2, 167–203.

[BK I] G. Böckle, C. Khare, *Mod l representations of arithmetic fundamental groups. I. An analog of Serre's conjecture for function fields*, Duke Math. J. **129** (2005), no. 2, 337–369.

[BK II] G. Böckle, C. Khare, *Mod l representations of arithmetic fundamental groups. II. A conjecture of A. J. de Jong* Compos. Math. **142** (2006), no. 2, 271–294.

[Bo 1] N. Boston, *Explicit deformation of Galois representations*, Invent. Math. **103** (1991), no. 1, 181–196.

[Bo 2] N. Boston, *Families of Galois representations—increasing the ramification*, Duke Math. J. **66** (1992), no. 3, 357–367.

[Bo 3] N. Boston, *Deformations of Galois representations associated to the cusp form* Δ, Séminaire de Théorie des Nombres, Paris 1987–88, 51–62, Progr. Math., **81**, Birkhäuser Boston, Boston, MA, 1990.

[Bo 4] N. Boston, S.V. Ullom, *Representations related to CM elliptic curves*, Math. Proc. Cambridge Philos. Soc. **113** (1993), no. 1, 71–85.

[Bo 5] N. Boston, *p-adic Galois representations and pro-p Galois groups*, New horizons in pro-p groups, 329–348, Progr. Math., **184**, Birkhäuser Boston, Boston, MA, 2000.

[Bo-Ma] N. Boston,B. Mazur, *Explicit universal deformations of Galois representations*, Algebraic number theory, 1–21, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989.

[Bou] Bourbaki, *Éléments de mathématique. Algèbre commutative*, Chapitres 8 et 9, Masson (1983).

[Ch] G. Chenevier, *The infinite fern and families of quaternionic modular forms*, cours du trimestre galoisien (Janvier-Mars 2010), http ://www.math.polytechnique.fr/ chenevier/coursihp.html.

[DDT] H. Darmon, F. Diamond, R. Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), 2–140, Int. Press, Cambridge, MA, 1997.

[DS] P. Deligne, J-P. Serre, *Formes modulaires de poids* 1, Annales scientifiques de l'École Normale Supérieure, Sér. 4, **7** no. 4 (1974), p. 507-53.

[deSL] B. De Smit, H.W. Lenstra *Explicit construction of universal deformation rings*, Modular forms and Fermat's last theorem (Boston, MA, 1995), 313-326, Springer, New York, 1997.

[FM] J-M. Fontaine, B. Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[Ge] T. Gee, *Companion forms over totally real fields. II.* Duke Math. J. **136** (2007), no. 2, 275–284.

[GV] E. Ghate, V. Vatsal, *Ordinary* Λ*-adic representations*, Ann. Inst. Fourier, **54** (2004), no.7, 2143-2162.

[Go 1] F.Q. Gouvêa, *Arithmetic of p-adic modular forms*, Lecture Notes in Mathematics, **1304** Springer-Verlag, Berlin, 1988.

[Go 2] F.Q. Gouvêa, *Deforming Galois representations : controlling the conductor*, J. Number Theory **34** (1990), no. 1, 95–113.

[Go 3] F.Q. Gouvêa, *On the ordinary Hecke algebra*, J. Number Theory **41** (1992), no. 2, 178–198.

[GM] F.Q. Gouvêa, B. Mazur *Families of modular eigenforms*, Math. Comp. **58** (1992), no. 198, 793–805.

[Gra] G. Gras, *Class field theory - from theory to practice*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003.

[Gro] B. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), no. 2, 445–517.

[Hi 1] H. Hida, *Galois representations into* $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ *attached to ordinary cusp forms*, Invent. Math. **85** (1986), no. 3, 545–613.

[Hi 2] H. Hida, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 2, 231–273.

[Ja] J-F. Jaulent, *Théorie l-adique globale du corps de classes*, J. Théor. Nombres Bordeaux **10** (1998), no. 2, 355–397.

[JM] J.-F. Jaulent, C. Maire, *Radical hilbertien et tour localement cyclotomique*, Japan. J. Math. **28** (2002), no. 2, 203–213.

[JN] J.-F. Jaulent, T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers et ramification restreinte*, J. Théor. Nombres Bordeaux **5** (1993), no. 2, 343–363.

[JS] J-F. Jaulent, J.W. Sands, *Sur quelques modules d'Iwasawa semi-simples*, Compositio Math. **99** (1995), no. 3, 325–341.

[Kh 1] C. Khare, *Base change, lifting, and Serre's conjecture*, J. Number Theory **63** (1997), no. 2, 387–395.

[Kh 2] C. Khare, *Serre's modularity conjecture : the level one case*, Duke Math. J. **134** (2006), no. 3, 557–589.

[KLR] C. Khare, M. Larsen, R. Ramakrishna, *Constructing semisimple p-adic Galois representations with prescribed properties*, Amer. J. Math. **127** (2005), no. 4, 709–734.

[KR] C. Khare, R. Ramakrishna, *Finiteness of Selmer groups and deformation rings*, Invent. Math. **154** (2003), no. 1, 179–198.

[KW 1] C. Khare, J-P. Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Ann. of Math. (2) **169** (2009), no. 1, 229–253.

[KW 2] C. Khare, J-P. Wintenberger, *Serre's modularity conjecture. I.* Invent. Math. **178** (2009), no. 3, 485–504.

[KW 3] C. Khare, J-P. Wintenberger, *Serre's modularity conjecture. II.* Invent. Math. **178** (2009), no. 3, 505–586.

[Ki 1] M. Kisin, *The Fontaine-Mazur conjecture for* GL_2. J. Amer. Math. Soc. **22** (2009), no. 3, 641–690.

[Ki 2] M. Kisin, *Modularity of some geometric Galois representations* (with an appendix by O.Gabber), London Math. Soc. Lecture Note Ser., **320**, *L*-functions and Galois representations, 438–470, Cambridge Univ. Press, Cambridge, 2007.

[Ko] H. Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Berlin, 2002.

[La] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, J. Reine Angew. Math. **596** (2006), 155–182.

[Mai] C. Maire, *Une estimation de la dimension de Krull des anneaux de déformations en ramification incomplète*, Publ. Math. Univ. Franche-Comté Besançon (2003–2006), 129–141.

[Mat] H. Matsumura, *Commutative ring theory*, second edition, Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

[Maz 1] B. Mazur, *Deforming Galois representations*, Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 385–437, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.

[Maz 2] B. Mazur, *An introduction to the deformation theory of Galois representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), 243–311, Springer, New York, 1997.

[Maz 3] B. Mazur, *Two-dimensional p-adic Galois representations unramified away from p*, Compositio Mathematica, **74** no. 2 (1990), 115-133.

[MT] B. Mazur, J. Tilouine, *Représentations galoisiennes, différentielles de Kähler et «conjectures principales»*, Publications Mathématiques de l'IHÉS, **71** (1990), 65-103.

[MW] B. Mazur, A. Wiles, *On p-adic analytic families of Galois representations*, Compositio Mathematica, **59** (1986), no. 2, 231-264.

[Mé 1] A. Mézard, *Computation of a universal deformation ring in the Borel case*, Math. Proc. Cambridge Philos. Soc. **126** (1999), no. 3, 417–442.

[Mé 2] A. Mézard, *Obstructions aux déformations de représentations galoisiennes réductibles et groupes de classes*, J. Théor. Nombres Bordeaux **17** (2005), no. 2, 607–618.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Second edition, Springer-Verlag, Berlin, 2008.

[Oh] S.Ohtani, *Deformations of locally abelian Galois representations and unramified extensions*, J. Number Theory **120** (2006), no. 2, 272–286.

[Ra 1] R. Ramakrishna, *Lifting Galois representations*, Invent. Math. **138** (1999), no. 3, 537–562.

[Ra 2] R.Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, Ann. of Math. (2) **156** (2002), no. 1, 115–154.

[Ra 3] R. Ramakrishna,*On a variation of Mazur's deformation functor*, Compositio Math. **87** (1993), no. 3, 269–286.

[Ri] K.A. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), no. 3, 151–162.

[Ro] D. Robinson, *A course in the theory of groups*, Springer-Verlag, 1982.

[Sa] L. Salle, *Sur les pro-p-extensions à ramification restreinte au-dessus de la* $\mathbb{Z}_p$*-extension cyclotomique d'un corps de nombres* J. Théor. Nombres Bordeaux **20** (2008), no. 2, 485–523.

[Sc] M. Schlessinger, *Functors of Artin rings*, Trans. Amer. Math. Soc. **130** (1968), 208–222.

[Sch] A. Schmidt, *Über pro-p-fundamentalgruppen markierter arithmetischer kurven*, (German) [On pro-p fundamental groups of marked arithmetic curves], J. Reine Angew. Math. **640** (2010), 203–235.

[Se 1] J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[Se 2] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, (French) Invent. Math. **15** (1972), no. 4, 259–331.

[Se 3] J-P. Serre, *Cohomologie galoisienne*, (French) [Galois cohomology] Fifth edition. Lecture Notes in Mathematics, **5**, Springer-Verlag, Berlin, 1994.

[Se 4] J-P. Serre, *Abelian l-adic representations and elliptic curves.* McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute W. A. Benjamin, Inc., New York-Amsterdam 1968.

[Se 5] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications Mathématiques de l'IHÉS, **54** (1981), p. 123-201.

[Se 6] J-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, 319–338. Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973.

[SW] C.M. Skinner, A. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse Math. (6) **10** (2001), no. 1, 185–215.

[Ta 1] R. Taylor, *On icosahedral Artin representations. II.*, Amer. J. Math. **125** (2003), no.3, 549–566.

[Ta 2] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur.* J. Inst. Math. Jussieu **1** (2002), no. 1, 125–143.

[Wa] L.C. Washington, *Introduction to cyclotomic fields*, Second edition, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1997.

[We 1] T. Weston, *Unobstructed modular deformation problems*, Amer. J. Math. **126** (2004), no. 6, 1237–1252.

[We 2] T. Weston, *Explicit unobstructed primes for modular deformation problems of squarefree level*, J. Number Theory **110** (2005), no. 1, 199–218, 11F80

[Wi] A. Wiles, *Modular curves and Fermat's last theorem*, Ann. of Math. **141** (1995), no.3, 443-551.