Introduction au domaine de recherche : Les représentations galoisiennes

Béranger Seguin

14 mai 2021

Résumé

Depuis le milieu des années 1950, l'étude des représentations des groupes de Galois a pris une place de plus en plus importante au sein de la théorie algébrique des nombres. La preuve par Wiles du théorème de Fermat dans les années 1990 est l'aboutissement d'un long chemin dont nous allons essayer de présenter une esquisse.

Table des matières

1 Introduction 1
2 Local et global 4
3 Représentations galoisiennes 6
4 Cohomologie galoisienne 10
5 Un exemple d'utilisation des représentations galoisiennes 11
6 Déformations 12
7 Le grand théorème de Fermat 14
8 Un point de vue moderne sur la question : les anneaux de déformation dérivés 16
9 Aller plus loin 17

1 Introduction

1.1 Des équations aux extensions

Le centre d'intérêt principal de l'arithmétique est la résolution d'équations en nombres entiers ou rationnels. Par exemple, un problème historique célèbre est le théorème de Fermat, démontré à la fin du vingtième siècle par Andrew Wiles, et sur lequel des mathématicien·ne·s (par exemple Pierre de Fermat, Sophie Germain ou Ernst Kummer) ont travaillé pendant des siècles. Ce théorème énonce que, lorsque n est un entier au moins égal à 3, l'équation :

$$a^n + b^n = c^n$$

n'a pas de triplets solutions (a, b, c), où a, b et c sont trois entiers non nuls. Les outils développés au fil des siècles pour résoudre des cas particuliers de ce problème sont à la base de l'algèbre et de

l'arithmétique modernes. Par exemple, dans la solution du cas $n = 3$, Euler a été conduit à utiliser un système de nombres un peu plus grand que celui des nombres rationnels, à savoir l'ensemble $\mathbb{Q}[\sqrt{-3}]$ des nombres de la forme $a + \sqrt{3}ib$ avec a et b rationnels. Cela motive les définitions informelles suivantes :

Définition 1 (Corps, extension de corps)**.** Un *corps* est un système de nombres dans lequel on peut additionner, soustraire, multiplier et diviser par des éléments non nuls, avec les propriétés usuelles de ces opérations (la distributivité, la commutativité, etc.). On dit qu'un corps L est une *extension* du corps K si les éléments de K sont dans L, et l'extension est dite *finie* quand il existe un nombre fini d'éléments de L à partir desquels on peut décrire tout élément de L (comme somme à coefficients dans K). On appelle le nombre minimal de tels éléments la *dimension* de l'extension $L \mid K$.

Par exemple, vous connaissez sans doute le corps $\mathbb{Q}$ des nombres rationnels, le corps $\mathbb{R}$ des nombres réels, le corps $\mathbb{C}$ des nombres complexes, le corps $\bar{\mathbb{Q}}$ des nombres algébriques (les nombres complexes qui sont racines d'un polynôme non nul à coefficients rationnels). Le corps $\mathbb{C}$ est une extension de $\mathbb{R}$ et de $\bar{\mathbb{Q}}$, qui sont tous deux des extensions de $\mathbb{Q}$.

L'exemple historique d'extension donné plus haut, à savoir $\mathbb{Q}[\sqrt{-3}] \mid \mathbb{Q}$, illustre un lien entre équations sur $\mathbb{Q}$ et extensions de $\mathbb{Q}$. On peut voir une autre manifestation de ce lien, plus connue sans doute, dans le fait qu'on doive utiliser des nombres complexes lors de la résolution de certaines équations de degré 3, même si c'est pour finalement découvrir que les solutions sont réelles.

En poursuivant l'approche suggérée par ces exemples, on a compris que le problème de la résolution d'équations polynomiales dans $\mathbb{Q}$ était en lien étroit avec la compréhension des extensions finies de $\mathbb{Q}$, qu'on appellera par la suite des *corps de nombres*. Ce sont les corps qu'on obtient en « rajoutant les racines de certains polynômes » à $\mathbb{Q}$, par exemple $\mathbb{Q}[\sqrt{2}]$ ou $\mathbb{Q} + i\mathbb{Q} = \mathbb{Q}[\sqrt{-1}]$.

1.2 Des extensions aux groupes de Galois

Depuis Galois, on sait qu'il existe une correspondance entre les extensions d'un corps et les sous-objets d'un objet algébrique, le groupe de Galois (d'une extension fixée) :

Définition 2 (groupe de Galois)**.** Lorsque L est une extension finie de K, le groupe de Galois de $L \mid K$ est défini ainsi :

$$\mathrm{Gal}(L \mid K) = \mathrm{Aut}_{K-\mathrm{Alg}}(L) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{id}_K\}.$$

Dit d'une manière plus imagée, $\mathrm{Gal}(L \mid K)$ est l'ensemble des manières d'identifier le corps L à lui-même sans toucher aux éléments de K. La conjugaison complexe, par exemple, donne une identification non-triviale entre $\mathbb{C}$ et $\mathbb{C}$, donnée par :

$$a + ib \mapsto a - ib,$$

et celle-ci n'a aucun effet sur les nombres réels. Elle définit donc un élément de $\mathrm{Gal}(\mathbb{C} \mid \mathbb{R})$.

Remarque 3. Si z est une racine dans L d'un polynôme P à coefficients dans K et que $\sigma \in \mathrm{Gal}(L \mid K)$, alors $\sigma(z)$ est aussi une racine dans L de P. Un élément du groupe de Galois $\mathrm{Gal}(L \mid K)$ permute donc les racines dans L des polynômes à coefficients dans K.

Définition 4. Soit une extension de corps $L \mid K$. On dit qu'elle est *algébrique* lorsque tout élément de L est racine d'un polynôme non nul à coefficients dans K. Dans ce cas, on peut associer à tout élément $x \in L$ son *polynôme minimal*, unitaire et de degré minimal parmi les polynômes non nuls à coefficients dans K dont x est racine.

Par exemple, une extension finie $L \mid K$ est toujours algébrique [1]. Lorsqu'une extension algébrique $L \mid K$ est séparable et normale (c'est-à-dire que les polynômes minimaux des éléments de L sont scindés sur L et n'ont que des racines simples), on dit qu'elle est *galoisienne*. Dans ce cas, on a une description explicite des sous-groupes de $\mathrm{Gal}(L \mid K)$:

Théorème 5 (correspondance de Galois)**.** *Lorsque $L \mid K$ est une extension galoisienne, les sous-groupes de $\mathrm{Gal}(L \mid K)$ sont en correspondance avec les sous-extensions de L, c'est-à-dire les corps E vérifiant $K \subset E \subset L$. Cette correspondance est très explicite : étant donné un sous-groupe H de $\mathrm{Gal}(L \mid K)$, on peut regarder :*

$$L^H = \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$$

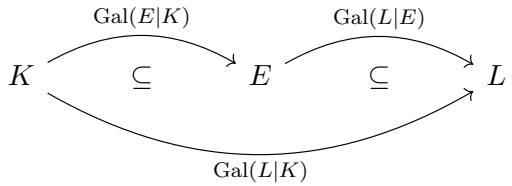
qui est une sous-extension de L. Et réciproquement, si E est une sous-extension, on peut regarder :

$$H = \{\sigma \in \mathrm{Gal}(L \mid K) \mid \forall x \in E, \sigma(x) = x\}$$

qui est un sous-groupe de $\mathrm{Gal}(L \mid K)$, isomorphe à $\mathrm{Gal}(L \mid E)$. En fait, on a une suite exacte :

$$0 \to \mathrm{Gal}(L \mid E) \overset{\subseteq}{\to} \mathrm{Gal}(L \mid K) \overset{\sigma \mapsto \sigma_{|E}}{\to} \mathrm{Gal}(E \mid K) \to 0.$$

ce qui signifie grossièrement que $\mathrm{Gal}(L \mid K)$ est fait de deux morceaux : l'un ressemble à $\mathrm{Gal}(E \mid K)$ et l'autre à $\mathrm{Gal}(L \mid E)$. On peut ainsi « découper » l'extension. On dessine parfois le diagramme suivant :



Le théorème précédent montre que comprendre les groupes de Galois a un intérêt pour comprendre les corps de nombres : si on a une description du groupe de Galois d'un corps de nombres, on a une description de toutes ses sous-extensions grâce à cette correspondance. Il est alors tentant de chercher une extension algébrique « maximale » de $\mathbb{Q}$...

1.3 La théorie de Galois infinie

Pour le moment, on a autant d'objets d'études (extensions et groupes de Galois) qu'il y a de corps de nombres. Pour transformer cette question « multiple » en une question unique, on cherche

1. Pour celleux qui ont fait un peu d'algèbre linéaire : si $x \in L$, la famille $(x^n)_{n \in \mathbb{N}}$ est infinie et donc forcément liée, puisque L est de dimension finie sur K.

des objets « universels » qui compilent l'information sur toutes ces extensions et sur leurs groupes de Galois.

Le corps des nombres algébriques, $\bar{\mathbb{Q}}$ contient *toutes* les racines des polynômes sur $\mathbb{Q}$: il est donc une extension algébrique maximale et les corps de nombres sont exactement ses sous-extensions finies. C'est donc un bon candidat si on cherche un unique objet d'étude.

On a envie de définir son groupe de Galois, avec en tête l'idée que ses sous-groupes d'indice fini seront les groupes de Galois de ses sous-extensions finies, et donc de tous les corps de nombres. La définition naïve qu'on pourrait tenter, à savoir :

$$\mathrm{Aut}_{\mathbb{Q}-\mathrm{Alg}}(\bar{\mathbb{Q}}),$$

ne permet pas d'avoir ces propriétés. Il faut donc définir ce groupe de Galois de façon un peu particulière, par un procédé de « passage à la limite » (on parle de « limite projective ») :

$$\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q}) = \varprojlim_{K \text{ extension finie de } \mathbb{Q}} \mathrm{Gal}(K \mid \mathbb{Q}).$$

De cette manière, un élément de $\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})$ peut être vu comme un automorphisme de corps de $\bar{\mathbb{Q}}$ fixant $\mathbb{Q}$, qui a de plus la particularité de pouvoir être décrit comme une collection « compatible » d'automorphismes sur chaque corps de nombres. La définition laisse effectivement penser qu'on « assemble » entre eux les groupes de Galois de tous les corps de nombres. Cette définition astucieuse permet une description simple des sous-groupes d'indice fini [2] de $\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})$ puisque le théorème vu auparavant « passe à la limite » :

Théorème 6. *Les sous-groupes d'indice fini de* $\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})$ *sont en correspondance avec les extensions finies de* $\mathbb{Q}$*, c'est-à-dire les corps de nombres.*

Autrement dit, puisqu'on était arrivé à la conclusion qu'il nous fallait comprendre les corps de nombres, on a envie d'avoir autant d'informations que possible sur le groupe $\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})$, qu'on notera $G_{\mathbb{Q}}$ par la suite (on dit que c'est le *groupe de Galois absolu* de $\mathbb{Q}$). En effet, une propriété de ce groupe se traduit (via la correspondance de Galois) en une information sur *tous* les corps de nombres : on devine donc la puissance de cette stratégie. C'est pour cette raison que le groupe de Galois absolu de $\mathbb{Q}$ peut être vu comme l'objet d'étude principal de l'arithmétique moderne.

2 Local et global

Pour de bonnes références sur le contenu de cette section, on peut consulter [Ser62] et [Neu99].

2.1 Descente vers le cas local

Hélas, il y a un prix à payer pour cette universalité : le groupe $G_{\mathbb{Q}}$ est extrêmement compliqué à comprendre. Une manière de rendre son étude moins compliquée est de compléter $\mathbb{Q}$ (ce qui permet de « tuer » tous les idéaux maximaux de $\mathbb{Z}$ sauf un, et donc de simplifier la situation) puis de

2. Ou, de manière équivalente, ouverts pour la topologie profinie.

considérer le groupe de Galois absolu du corps ainsi obtenu. Il n'y a que deux façons de faire ceci (c'est le théorème d'Ostrowski) :

— Soit on complète $\mathbb{Q}$ pour la valeur absolue usuelle. On obtient alors $\mathbb{R}$ et on connaît très bien $G_{\mathbb{R}} := \mathrm{Gal}(\mathbb{C} \mid \mathbb{R})$ puisque c'est $\mathbb{Z}/2\mathbb{Z}$ (avec pour générateur la conjugaison complexe). De ce cas, on ne peut pas déduire grand chose d'autre que l'existence d'un morphisme :

$$\mathbb{Z}/2\mathbb{Z} \to G_{\mathbb{Q}}$$

ou, dit autrement, l'existence d'éléments d'ordre deux dans $G_{\mathbb{Q}}$, qui correspondent aux différents plongements de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$. La théorie de Galois est peu utile pour faire ce constat, puisqu'on voit sans faire appel à elle qu'étant donné un plongement $\bar{\mathbb{Q}} \to \mathbb{C}$, la conjugaison complexe est l'élément d'ordre deux cherché.

— Soit on complète $\mathbb{Q}$ pour une des valeurs absolues p-adiques (avec p un nombre premier), c'est-à-dire :

$$\left|\frac{a}{b}\right|_p = p^{v_p(b)-v_p(a)}$$

où $v_p(a)$ est la puissance de p dans la décomposition en produit de nombres premiers de a.

On obtient alors un corps, noté $\mathbb{Q}_p$, dans lequel $\mathbb{Q}$ se plonge. On a alors un morphisme de (co)restriction :

$$G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}_p} \mid \mathbb{Q}_p) \to G_{\mathbb{Q}}$$

qui suggère que comprendre $G_{\mathbb{Q}_p}$ pour tous les nombres premiers p nous aidera à comprendre $G_{\mathbb{Q}}$. On dit qu'on est dans le cas local.

Le même principe peut se formuler directement à partir des extensions. Si K est un corps de nombres et p un nombre premier, on peut considérer sa complétion K_v par rapport à une valeur absolue qui « étend » la valeur absolue p-adique sur $\mathbb{Q}$ (on parle plus formellement d'une place non-archimédienne au-dessus de p). Alors K_v est une extension finie de $\mathbb{Q}_p$ (on appelle une telle extension un *corps local p-adique*). On cherche alors à comprendre les corps locaux p-adiques pour tous les nombres premiers p dans l'espoir d'obtenir des informations sur les corps de nombres.

La situation ainsi simplifiée par ce procédé de complétion, on peut montrer de nombreuses choses sur les groupes $G_{\mathbb{Q}_p}$. Par exemple, pour $p \neq 2$, on en connaît aujourd'hui une description explicite sous forme d'une liste de générateurs (topologiques) et de relations.

2.2 Remontée vers le cas global

La question naturelle suivante consiste à trouver des théorèmes de passage local-global : on aimerait combiner les informations « locales » dont on dispose aujourd'hui sur $G_{\mathbb{Q}_p}$ (ou sur les corps p-adiques) pour en déduire des informations « globales » sur $G_{\mathbb{Q}}$ (ou sur les corps de nombres). C'est un problème difficile.

La même difficulté s'observe directement en considérant des équations sur $\mathbb{Q}$. Pour les équations de degré deux, on sait qu'une équation a une solution dans $\mathbb{Q}$ si et seulement si elle en a dans $\mathbb{R}$ et dans $\mathbb{Q}_p$ pour tout nombre premier p : c'est le théorème de Hasse–Minkowski. On aimerait généraliser ce résultat... mais dans le cas général, il y a des obstructions à ce passage local-global.

Dans certains cas, on sait cependant bien effectuer ce passage local-global. Par exemple, une théorie puissante, la *théorie du corps de classe*, permet d'obtenir une description de $G_{\mathbb{Q}}^{\mathrm{ab}}$ (qui classifie les extensions abéliennes de $\mathbb{Q}$, c'est-à-dire celles dont le groupe de Galois est commutatif) en la reliant aux différents $G_{\mathbb{Q}_p}^{\mathrm{ab}}$ $\left(= \widehat{\mathbb{Q}_p^\times}\right)$ (et elle permet même de décrire G_K^{ab} pour tout corps de nombres).

3 Représentations galoisiennes

3.1 Définition

Une représentation galoisienne (de dimension n) est une action d'un groupe de Galois sur A^n, où A désigne un anneau commutatif. On peut aussi la voir comme un morphisme de groupes :

$$\rho : \mathrm{Gal}(L \mid K) \to \mathrm{GL}_n(A).$$

Ces représentations apparaissent naturellement dans de nombreux contextes. Notamment, si on a une construction naturelle de module ou d'espace vectoriel à partir d'un corps, c'est-à-dire un foncteur :

$$F : \mathrm{Corps} \to A\text{-}\,\mathrm{Mod},$$

alors tout élément $g \in \mathrm{Gal}(L \mid K)$, vu comme un morphisme $L \to L$, induit un morphisme $F(g) : F(L) \to F(L)$, et cela de manière fonctorielle ($F(gg') = F(g)F(g')$). Autrement dit, il y a une action de $\mathrm{Gal}(L \mid K)$ sur le A-module $F(L)$, et donc une représentation galoisienne.

L'idée fondamentale derrière l'étude des représentations galoisiennes est que les comprendre permet de mieux comprendre les groupes de Galois, ce qui comme on l'a vu nous renseigne sur les extensions de corps. Cette idée ne devrait pas surprendre : si on se souvient à quel point l'étude des représentations était utile dans le cas des groupes finis, on peut se douter qu'elle l'est aussi pour des groupes plus compliqués.

On donne maintenant deux situations géométriques dans lesquelles des représentations galoisiennes apparaissent naturellement.

3.2 Représentation associée à une courbe elliptique

Cet exemple est particulièrement important historiquement : c'est lui qui est en œuvre dans le grand théorème de Fermat. Soit une courbe elliptique E, c'est-à-dire l'ensemble des couples (x, y) de réels satisfaisant une équation de la forme :

$$y^2 = x^3 + ax + b$$

avec (dans notre cas) $a, b \in \mathbb{Q}$, auquel on ajoute un point à l'infini, noté ∞. Il est alors possible de munir cet ensemble d'une structure de groupe additif d'élément neutre ∞ (dans les grandes lignes : je prends deux points x, y de la courbe, je trace la droite qui les unit ; elle coupe la courbe en un troisième point ; la réflexion par rapport à l'axe $y = 0$ de ce point est notée $x + y$).

On peut ne regarder que l'ensemble $E_{\bar{\mathbb{Q}}}$ des points de E dont les coordonnées sont algébriques. Cet ensemble est clairement stable par la loi de groupe de la courbe elliptique. Le groupe $G_{\mathbb{Q}}$ agit sur $E_{\bar{\mathbb{Q}}}$ coordonnée par coordonnée, et l'ensemble des points fixes de cette action est exactement l'ensemble $E_{\mathbb{Q}}$ des points rationnels de la courbe.

Soit un nombre premier p fixé. On désignera par $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ et par $\mathbb{Z}_p$ l'anneau des entiers de $\mathbb{Q}_p$, qui est un anneau local d'idéal maximal $p\mathbb{Z}_p$; qu'on peut aussi définir comme :

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

On dit qu'un point $x \in E_{\bar{\mathbb{Q}}}$ est de p^n-torsion lorsque $\underbrace{x + x + \ldots + x}_{p^n \text{ fois}} = \infty$.

On peut montrer (voir [Dat18]) que les points de p^n-torsion de E dans $\bar{\mathbb{Q}}$ forment un sous-groupe de E isomorphe à $(\mathbb{Z}/p^n\mathbb{Z})^2$. La restriction à ce groupe de l'action de $G_{\mathbb{Q}}$ donne une famille de représentations galoisiennes compatibles entre elles :

$$\bar{\rho}_n : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}).$$

En passant à la limite sur n (c'est-à-dire en « assemblant ces représentations galoisiennes en une seule »), on obtient une représentation galoisienne dite p-adique :

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

L'étude de cette représentation galoisienne est au cœur de nombreuses théories arithmétiques. Notamment, l'analyse de ses propriétés permet d'étudier les propriétés de la courbe elliptique E (par exemple la modularité).

On peut remarquer que par construction, le diagramme suivant commute :

$$\begin{array}{ccc} & & \mathrm{GL}_2(\mathbb{Z}_p) \\ & \overset{\rho}{\nearrow} & \downarrow \\ \mathrm{Gal}(\bar{K} \mid K) & \xrightarrow{\bar{\rho}_1} & \mathrm{GL}_2(\mathbb{F}_p) \end{array}$$

On dira plus tard que ρ est une déformation (cadrée) de $\bar{\rho}_1$. Une grande idée de l'arithmétique moderne est d'essayer de « transférer » des propriétés des représentations à leurs déformations.

3.3 La cohomologie des variétés est une représentation

Voici un autre exemple, qui généralise le précédent : si X est une variété algébrique sur un corps K (la·e lecteur·rice qui n'a jamais vu cette notion ne doit pas s'inquiéter : il faut la voir comme une version plus générale de la courbe elliptique vue précédemment), on peut considérer la variété algébrique $X_{\bar{K}}$ sur $\bar{K}$ suivante :

$$X_{\bar{K}} = X \underset{\mathrm{Spec}(K)}{\times} \mathrm{Spec}(\bar{K}).$$

L'action du groupe de Galois absolu $G_K := \mathrm{Gal}(\bar{K} \mid K)$ sur $\bar{K}$ (et donc sur $\mathrm{Spec}(\bar{K})$) induit par fonctorialité une action sur $X_{\bar{K}}$.

Sur les variétés algébriques, les mathématicien·ne·s ont développé de nombreuses théories de la cohomologie, telles que la cohomologie étale, la cohomologie cristalline, la cohomologie de de Rham, la cohomologie ℓ-adique, etc. Si vous n'avez jamais rencontré la cohomologie des variétés, il vous suffit pour comprendre ce qui suit de savoir que toutes ces cohomologies sont des foncteurs à valeurs dans une catégorie de modules, et d'admettre qu'elles ont leur importance dans l'étude des variétés. Pour en apprendre plus, on peut lire [Har77] et [Mil13].

On prend l'exemple de la cohomologie étale. Puisqu'on a dit qu'elle était fonctorielle, l'action de G_K sur $X_{\bar{K}}$ induit une action sur le $\mathbb{Z}/p^n\mathbb{Z}$-module suivant :

$$H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p^n\mathbb{Z})$$

puis, par passage à la limite projective, sur la cohomologie étale p-adique, qui est un $\mathbb{Q}_p$-espace vectoriel :

$$H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_p) = \left(\varprojlim_n H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p^n\mathbb{Z}) \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Dit autrement, la cohomologie étale p-adique définit une représentation galoisienne à coefficients dans $\mathbb{Q}_p$ (on parle de représentation galoisienne p-adique). Cet exemple est fondamental car il décrit avec une grande généralité les représentations galoisiennes « d'origine géométrique ».

En fait, il existe de nombreuses représentations galoisiennes, et la plupart ne proviennent pas de ce genre de situations géométriques. Les représentations obtenues par les procédés ci-dessus vérifient des propriétés remarquables qui simplifient leur étude. Une des conjectures les plus importantes de la théorie des représentations galoisiennes (la conjecture de Fontaine–Mazur) prédit que toute représentation ayant d'assez bonnes propriétés de ce type est un sous-quotient de la cohomologie étale d'une variété. L'exemple que nous venons de voir est donc fondamental et très général.

3.4 Les représentations galoisiennes p-adiques

Dans le cas local, si p et ℓ sont deux nombres premiers, on peut regarder les représentations :

$$\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(A_\ell)$$

où A_ℓ est $\mathbb{Q}_\ell$, $\mathbb{Z}_\ell$ ou $\mathbb{F}_\ell$. Il y a alors deux cas très différents :

— Si $p \neq \ell$, il y a très peu de telles représentations (elles forment un espace « discret »). On parle de la théorie des représentations ℓ-adiques. Puisqu'il y en a peu, on est intéressé par une compréhension fine de la structure de cet espace : c'est une théorie plutôt algébrique.

— Si $p = \ell$, il y a énormément de telles représentations (elles forment un espace « continu »). On parle de la théorie des représentations p-adiques. Notamment, on s'intéresse à comprendre comment distinguer différentes classes de régularité des représentations (lesquelles sont issues de la cohomologie étale, lesquelles sont issues de la cohomologie cristalline, lesquelles sont modulaires) à partir de conditions telles que la ramification, la platitude, etc. : c'est une théorie plutôt analytique.

Une représentation particulière est la suivante : si ζ_n est une racine primitive p^n-ième de l'unité et $\sigma \in G_{\mathbb{Q}_p}$, alors $\sigma(\zeta_n)$ est une autre racine p^n-ième de l'unité, qu'on peut écrire $(\zeta_n)^{a_n}$. L'entier a_n est défini uniquement modulo p^n, ne dépend clairement pas de la racine ζ_n choisie, et par ailleurs :

$$\sigma(\zeta_{n+1}^p) = (\zeta_{n+1}^p)^{a_n} = ((\zeta_{n+1})^{a_{n+1}})^p,$$

ce qui montre que $a_n = a_{n+1}$ modulo p^n. Ainsi la suite (a_n) définit un élément de $\mathbb{Z}_p^\times$. On a ainsi défini un morphisme :

$$\chi : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times,$$

c'est-à-dire un caractère (une représentation de dimension 1) de $G_{\mathbb{Q}_p}$.

3.5 Un mot sur la théorie de Hodge p-adique

La complétion $\mathbb{C}_p$ de $\overline{\mathbb{Q}_p}$ est un corps à la fois complet et algébriquement clos. Notons $\mathbb{C}_p(i)$ (avec $i \in \mathbb{Z}$) ce corps lorsqu'il est muni de l'action suivante :

$$\forall g \in G_{\mathbb{Q}_p},\ \forall x \in \mathbb{C}_p,\ g.x = \chi(g)^i x.$$

Soit une représentation $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(\mathbb{Q}_p)$. On peut calculer son *$i$-ième poids de Hodge-Tate* :

$$d_\rho(i) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p^n \otimes_{\mathbb{Q}_p} \mathbb{C}_p(-i))^{G_{\mathbb{Q}_p}}$$

où :

— l'action de G_K sur $\mathbb{Q}_p^n$ est celle donnée par ρ : $g.x = \rho(g)(x)$;

— l'action de G_K sur le produit tensoriel est défini par la formule $g.(x \otimes y) = (g.x) \otimes (g.y)$;

— la notation $H^{G_{\mathbb{Q}_p}}$ désigne l'ensemble des points fixes d'une représentation H de $G_{\mathbb{Q}_p}$.

Moralement, $d_\rho(i)$ désigne la dimension du sous-espace de $\mathbb{C}_p^n$ sur lequel la représentation ρ se comporte comme la puissance i-ième du caractère cyclotomique. On a l'inégalité :

$$\sum_{i \in \mathbb{Z}} d_\rho(i) \leq n$$

et, lorsqu'il y a égalité, on dit que la représentation ρ est de Hodge–Tate. Cela signifie que ρ (dans $\mathbb{C}_p$) se découpe en puissances du caractère cyclotomique. En quelque sorte, cette propriété est comparable à la diagonalisabilité.

D'autres conditions plus subtiles existent. Par exemple, le caractère de de Rham, semi-stable, cristallin des représentations, ont été définis dans cet esprit, avec les implications suivantes :

$$\text{cristalline} \Rightarrow \text{semi-stable} \Rightarrow \text{de de Rham} \Rightarrow \text{de Hodge–Tate}.$$

Il se trouve que les représentations galoisiennes « naturelles », issues de contextes géométriques comme ceux vus précédemment, sont toujours de Hodge–Tate et même de de Rham voire semi-stables ou cristallines dans des contextes assez réguliers.

Pour montrer ce genre de résultat, la plupart des preuves s'appuient sur des comparaisons entre cohomologies : la cohomologie de de Rham algébrique, la cohomologie cristalline, la cohomologie p-adique, etc. Plus précisément, on utilise des résultats de la forme :

$$B \otimes H_1^i \simeq B \otimes H_2^i$$

où H_1 et H_2 sont deux cohomologies différentes, et où B est ce qu'on appelle un *anneau de périodes* (par exemple l'anneau de périodes correspondant aux représentations de Hodge–Tate est $B_{HT} = \mathbb{C}_p[t, t^{-1}]$) [3]. Pour en apprendre plus sur cette théorie, on peut consulter [FO08] et [Ber04].

On voit assez bien le lien avec la théorie de Hodge ordinaire, qui fait des liens entre différentes cohomologies ($H^i_{\text{sing}} \otimes \mathbb{C}$, $H^i_{\text{dR}} \otimes \mathbb{C}$, $H^i_{\text{Dolbeault}}$, $\bigoplus_{p,q} H^{p,q}$, ...). Une bonne introduction à ce sujet, qui parle aussi de cette analogie, se trouve dans [Car19].

Pour résumer, la théorie de Hodge p-adique permet de « mettre de l'ordre » dans le vaste espace des représentations galoisiennes p-adiques.

4 Cohomologie galoisienne

Pour cette section, les références seront principalement [Ser62] et [AW67].

4.1 Cohomologie des groupes

Une action d'un groupe G sur un groupe abélien, autrement dit un $\mathbb{Z}[G]$-module, permet de définir des groupes de cohomologie. Plus précisément, il existe une unique suite de foncteurs $H^i(G, -)$ tels que si :

$$0 \to A \to B \to C \to 0$$

est une suite exacte de $\mathbb{Z}[G]$-modules, il existe une suite exacte longue de groupes :

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \dots$$

où $H^0(G, M)$ désigne le sous-groupe M^G des points fixes de l'action de G pour tout $\mathbb{Z}[G]$-module M, et où $H^i(G, M) = 0$ lorsque M est de la forme $\text{Hom}(\mathbb{Z}[G], X)$ avec $X \in \mathbf{Ab}$ et $i > 0$.

3. La plupart des conditions sur les représentations $G_K \to \text{Aut}(V)$ demandent que $\dim(B \otimes V)^{G_K} = \dim(V)$ pour un certain anneau de périodes B. Pour définir ces classes de représentations, on choisit en fait le B des théorèmes de comparaisons cohomologiques, d'où le fait que les représentations géométriques tendent à être dans ces classes.

4.2 Cohomologie galoisienne

Le cas particulier où G est un groupe de Galois est particulièrement intéressant, entre autres parce que les groupes de Galois agissent naturellement sur divers objets. Par exemple, on a le théorème 90 de Hilbert :

$$H^1(G_K, \bar{K}^\times) = 0$$

et de nombreuses théories arithmétiques, qui précédent parfois la définition de cette cohomologie, telles que l'étude du groupe de Brauer, la théorie de Kummer ou celle d'Artin–Schreier, la dualité de Tate,... s'expriment en termes de cohomologie galoisienne.

Grâce à la cohomologie, on a un invariant algébrique associé aux actions du groupe de Galois. Cela est applicable aux représentations. Notamment, si :

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

est une représentation, on peut munir $\mathfrak{M}_n(A)$ de l'action définie par $g.M = \rho(g)M\rho(g)^{-1}$ et s'intéresser à ses groupes de cohomologie. Cela fait un lien entre représentations galoisiennes et cohomologie galoisienne. Lorsqu'il sera muni de cette action, on désignera $\mathfrak{M}_n(A)$ par $\mathrm{ad}(\rho)$.

On verra plus tard que dans certains cas, un certain espace de représentations galoisiennes (les déformations) peut être muni d'une structure géométrique. Dans ce cas, on peut déduire des informations sur les invariants géométriques associés à cette structure à partir des invariants cohomologiques associés à l'action précédente : la cohomologie galoisienne est donc un outil de plus pour étudier les représentations galoisiennes.

5 Un exemple d'utilisation des représentations galoisiennes

Durant mon stage de M1, j'ai utilisé les représentations galoisiennes pour démontrer un résultat très concret, dû à Mochizuki ([Moc97]) :

Théorème 7. *Soit K un corps local p-adique (une extension finie de $\mathbb{Q}_p$). On pose $G_K = \mathrm{Gal}(\bar{K} \mid K)$. Si L est une extension finie de K et $i \in \{-1, 0, 1, 2, 3, \ldots\}$, on définit :*

$$\mathrm{Gal}(L \mid K)_i = \{\sigma \in \mathrm{Gal}(L \mid K) \mid \forall x \in L, v_L(\sigma(x) - x) \geq i + 1\}$$

où v_L est l'unique extension de la valuation p-adique à L. Ceci définit une filtration de $\mathrm{Gal}(L \mid K)$:

$$\mathrm{Gal}(L \mid K) = \mathrm{Gal}(L \mid K)_{-1} \supset \mathrm{Gal}(L \mid K)_0 \supset \mathrm{Gal}(L \mid K)_1 \supset \ldots$$

qui induit par passage à la limite projective une filtration, dite de ramification :

$$G_K \supset (G_K)_0 \supset (G_K)_1 \supset (G_K)_2 \supset (G_K)_3 \supset \ldots$$

et on définit de même la filtration $(G_{K'})_i$ associée à un deuxième corps p-adique K'. Alors les corps K et K' sont isomorphes si et seulement s'il existe un isomorphisme entre G_K et $G_{K'}$ qui préserve de plus la filtration de ramification (c'est-à-dire qu'il envoie $(G_K)_i$ sur $(G_{K'})_i$).

Ce théorème, dans sa formulation, ne fait pas appel à la notion de représentation galoisienne : il s'agit de montrer que deux corps p-adiques de groupes de Galois absolus isomorphes (avec des conditions supplémentaires) sont isomorphes. Pourtant, on va voir que les représentations galoisiennes sont utiles à sa preuve.

Preuve. On détaille ici le squelette de la preuve. On fixe un isomorphisme $\Phi : G_K \to G_{K'}$ qui préserve la filtration de ramification. On doit montrer que K et K' sont isomorphes. La preuve se découpe en deux parties :

— On commence par montrer que Φ préserve les poids de Hodge-Tate des représentations galoisiennes, c'est-à-dire que si ρ est une représentation $G_K \to \mathrm{Aut}(V)$, la représentation

$$\rho \circ \Phi^{-1} : G_{K'} \to \mathrm{Aut}(V)$$

a les mêmes poids de Hodge-Tate que ρ (ce sont les $d_\rho(i)$ définis dans la sous-section 3.5).

— En utilisant un résultat très général de Serre, on parvient à montrer qu'un isomorphisme entre groupes de Galois absolus qui préserve les poids de Hodge-Tate est induit un isomorphisme entre les corps p-adiques (on choisit un corps E dans lequel K se plonge et tel que le fait pour un corps de se plonger dans E soit équivalent à une condition sur les poids de Hodge-Tate d'une représentation particulière, et puisque ces poids sont préservés par Φ, K' se plonge aussi dans E ; on montre alors que les images de K et K' dans E sont deux sous-corps isomorphes).

Une fois le problème ramené à des questions relatives aux représentations galoisiennes, de nombreux outils sont à notre disposition pour montrer le théorème initial : la décomposition de Hodge-Tate, la cohomologie galoisienne, la théorie du corps de classes local. La puissance de ces outils est un argument très fort pour justifier l'étude des représentations galoisiennes même dans les problèmes où elles n'apparaissent pas initialement. □

6 Déformations

6.1 Résultat principal

Si A est un anneau qui a un unique idéal maximal $\mathfrak{m}_A$, on dit que A est *local*, et dans ce cas $A/\mathfrak{m}_A$ est un corps, qu'on appelle *corps résiduel* de A.

Soit un nombre premier p fixé. On appellera *anneau de coefficients* un anneau local dont le corps résiduel est isomorphe à $\mathbb{F}_p$, et qui est de plus nœthérien (toute suite croissante d'idéaux stationne) et complet (il suffit pour qu'une suite (x_n) converge que pour tout k on ait $x_i - x_j \in \mathfrak{m}_A^k$ pour i, j assez grands).

À toute représentation ρ d'un groupe de Galois dans un anneau de coefficients A, on peut associer une représentation $\bar{\rho}$ dans $\mathbb{F}_p$, via la surjection $A \twoheadrightarrow A/\mathfrak{m}_A \simeq \mathbb{F}_p$. On a alors le diagramme suivant :

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \mathrm{GL}_n(A) \\ & \searrow^{\bar{\rho}} & \downarrow \\ & & \mathrm{GL}_n(\mathbb{F}_p) \end{array}$$

De plus, pour toute matrice de $\mathrm{GL}_n(A)$ de la forme $I_n + M$ avec M ayant ses coefficients dans $\mathfrak{m}_A$, on a toujours le diagramme précédent si on remplace ρ par $\rho' = M\rho M^{-1}$. On dira que deux représentations ρ et ρ' sont *strictement équivalentes* s'il existe une telle matrice M les reliant. Pour éviter de compter plusieurs fois les solutions à notre problème de relèvement, on s'intéresse aux représentations ρ qui s'inscrivent dans le diagramme ci-dessus, modulo l'équivalence stricte : on les appelle alors des *déformations* de $\bar{\rho}$ à A.

On s'intéresse alors à l'application $\mathrm{Def}_{\bar{\rho}}$ qui à un anneau A associe l'ensemble des déformations de $\bar{\rho}$ à A. C'est un foncteur de la catégorie des anneaux de coefficients dans la catégorie des ensembles. Un théorème très puissant, le critère de Schlessinger, permet de montrer que ce foncteur est *représentable* dès lors que G vérifie certaines propriétés que les groupes de Galois qui nous intéressent vérifient, et que toutes les matrices de $\mathfrak{M}_n(k)$ qui commutent avec $\bar{\rho}(g)$ pour tout g sont scalaires. On se place dans le cas où ces conditions techniques sont vérifiées.

La représentabilité de ce foncteur signifie qu'il existe un anneau de coefficients $\mathfrak{R}$ (l'anneau de déformation universel) et une déformation $\boldsymbol{\rho} : G \to \mathfrak{R}$ (la déformation universelle) tels que pour tout anneau de coefficients A, il y ait une correspondance entre les déformations de $\bar{\rho}$ à A et les morphismes d'anneaux $\varphi : \mathfrak{R} \to A$, donnée par l'application :

$$\varphi \mapsto \varphi \circ \boldsymbol{\rho}.$$

Autrement dit, on a comme un espace de paramètres qui permet d'explorer les déformations de manière simple. Ce résultat est très puissant car les anneaux de coefficients ont beaucoup plus de structure que l'ensemble des déformations : ils disposent par exemple d'un espace tangent, dont on peut calculer des invariants comme la dimension ; on peut aussi calculer la « différentielle » de morphismes entre anneaux de coefficients et ainsi simuler certains phénomènes de la géométrie différentielle, etc.

6.2 Une description cohomologique de l'anneau de déformation universel

On a vu que la représentation $\bar{\rho}$ définit un $\mathbb{F}_p[G]$-module $\mathrm{ad}(\bar{\rho})$. Cela permet de définir la dimension de son i-ième groupe de cohomologie galoisienne, qui est un invariant numérique intéressant :

$$d_i = \dim_k \left(H^i(G, \mathrm{ad}(\bar{\rho})) \right).$$

6.2.1 Dimension de l'espace tangent

On appelle *espace cotangent* de $\mathfrak{R}$ le $\mathbb{F}_p$-espace vectoriel $t^*_{\mathfrak{R}} := \mathfrak{m}_{\mathfrak{R}}/\mathfrak{m}^2_{\mathfrak{R}}$. Sa dimension est importante, par exemple $\mathfrak{R}$ peut être décrit sous la forme :

$$\mathfrak{R} = \mathbb{Z}_p[[X_1, X_2, \ldots, X_d]]/I$$

pour un certain idéal I, où $d = \dim_{\mathbb{F}_p} t^*_{\mathfrak{R}}$. Or il se trouve qu'on a le résultat suivant :

$$\dim_{\mathbb{F}_p} t^*_{\mathfrak{R}} = d_1.$$

Il ne reste donc « plus » qu'à décrire l'idéal des obstructions I.

6.2.2 Dimension de Krull

La dimension de Krull d'un anneau A est la taille maximale d d'une chaîne d'idéaux premiers de A de la forme $p_0 \subsetneq p_1 \subsetneq \ldots \subsetneq p_d \subsetneq A$. On peut minorer la dimension de Krull de $\mathfrak{R}/p\mathfrak{R}$ à l'aide de la cohomologie galoisienne :

$$\dim_{\text{Krull}}(\mathfrak{R}/p\mathfrak{R}) \geq d_1 - d_2$$

Il est conjecturé que sous certaines hypothèses faibles ($\bar{\rho}$ est absolument irréductible, ce qui implique notamment $d_0 = 1$), il y a toujours égalité dans cette formule. Dans le cas où K est un corps local p-adique (avec $[K : \mathbb{Q}_p] = d_K$), on peut calculer explicitement $d_1 - d_2$ (la preuve se trouve dans [Seg18]) :

$$d_1 - d_2 = d_0 + nd_K^2$$

et une formule similaire existe dans le cas global (voir [Gou91]).

6.2.3 Obstruction

Lorsque $d_2 = 0$, on sait décrire explicitement $\mathfrak{R}$ puisqu'il s'écrit :

$$\mathfrak{R} = \mathbb{Z}_p[[X_1, X_2, \ldots, X_{d_0}]]$$

et on a en particulier :

$$\dim_{\text{Krull}}(\mathfrak{R}/p\mathfrak{R}) = d_1.$$

On dit alors que le problème de déformation est *non-obstrué* : dans ce cas, on peut toujours relever une déformation $G \to \mathrm{GL}_n(B)$ de $\bar{\rho}$ par une surjection $A \twoheadrightarrow B$. Les résultats de ce paragraphe permettent de comprendre pourquoi les obstructions au relèvement des représentations peuvent être vues comme des éléments de $H^2(G, \mathfrak{M}_n(\mathbb{F}_p))$.

7 Le grand théorème de Fermat

La théorie des déformations des représentations galoisiennes a notamment permis à Wiles de démontrer le grand théorème de Fermat. On explique ici le lien entre le problème initial et la théorie présentée dans la section précédente.

Il existe un moyen d'associer à toute forme modulaire (une certaine classe de fonctions holomorphes sur le demi-plan complexe) une courbe elliptique. Avant Wiles, une conjecture ouverte

prédisait que toute courbe elliptique pouvait être obtenue par ce procédé (on dit que la courbe elliptique est modulaire). Le caractère modulaire d'une courbe elliptique peut se déduire en étudiant la représentation galoisienne associée, et on dit dans ce cas que la représentation est modulaire.

Soit un contre-exemple (hypothétique) au grand théorème de Fermat de la forme $a^p + b^p = c^p$ ($p \geq 5$ premier, $a, b, c \neq 0$). On considère alors la courbe elliptique sur $\mathbb{Q}$ d'équation suivante :

$$y^2 = x(x - a^p)(x + b^p).$$

En étudiant cette courbe elliptique, Ribet montra que, si elle existait, elle était semi-stable et ne pouvait pas correspondre à une forme modulaire. Autrement dit, l'existence d'un contre-exemple au grand théorème de Fermat impliquait qu'il existât une courbe elliptique semi-stable non modulaire. Ce que Wiles a prouvé est que toute courbe elliptique semi-stable sur $\mathbb{Q}$ est modulaire, rejetant ainsi l'hypothèse de l'existence d'un contre-exemple au grand théorème de Fermat.

Pour démontrer cela, partant d'une courbe elliptique semi-stable E quelconque, Wiles a considéré la représentation $\rho_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ associée. Il a réussi à montrer que la représentation résiduelle induite $\bar{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ était modulaire et que ρ_p avait un certain nombre de propriétés intéressantes (liées à son déterminant, et à son caractère non-ramifié/semi-stable/plat en des nombres premiers). On dira que ρ_p est une *bonne* représentation pour ne pas rentrer dans les détails.

Pour montrer que E est modulaire, Wiles a compris qu'il lui suffisait de montrer que toute *bonne* déformation de $\bar{\rho}_p$ était modulaire. Pour obtenir ce résultat, il a considéré deux anneaux :

— D'une part, l'anneau de déformation $\mathfrak{R}$ correspondant aux *bonnes* déformations de $\bar{\rho}_p$;

— D'autre part, un anneau, noté $\mathbf{T}$ (une algèbre de Hecke), qu'on peut voir comme un espace classifiant les formes modulaires associées aux bonnes déformations modulaires de $\bar{\rho}_p$.

Entre ces deux anneaux, il y a un morphisme naturel :

$$\mathfrak{R} \to \mathbf{T}$$

dont il suffisait de montrer qu'il s'agissait d'un isomorphisme pour montrer la correspondance entre les *bonnes* déformations de $\bar{\rho}_p$ et les formes modulaires, et donc à établir la modularité de ρ_p. Wiles réussit à ramener cette question à une égalité numérique (selon un principe philosophiquement comparable aux invariants cohomologiques décrits plus haut), puis à démontrer l'égalité en question.

Dans ce schéma de preuve, on voit toute la force de la théorie des représentations galoisiennes et de leurs déformations : les anneaux de déformation permettent de ramener des problèmes compliqués (par exemple le relèvement de représentations résiduelles modulaires en représentations modulaires) à des questions sur des objets munis d'une structure géométrique, et sur lesquels on a donc des invariants de type « dimension », qui sont autant d'outils additionnels pour affronter le problème.

Une approche similaire a permis de faire des progrès dans la conjecture de Fontaine–Mazur. La recherche sur ce sujet est très actuelle.

8 Un point de vue moderne sur la question : les anneaux de déformation dérivés

Soit p un nombre premier, k un corps parfait de caractéristique p (typiquement, $\mathbb{F}_p$). De même qu'on s'était intéressé à la catégorie des anneaux de coefficients, on peut définir une catégorie $\mathbf{sArt}_k$ des anneaux *simpliciaux* de coefficients. Sans rentrer dans les détails, un anneau simplicial est une sorte d'espace géométrique dont les points, les segments, les faces, etc. peuvent être additionnés et multipliés comme dans un anneau. L'ajout de cette composante géométrique rend la structure de ces objets beaucoup plus complexe. Par exemple, ils disposent de groupes d'homotopie :

$$\pi_i(\mathfrak{R})$$

qui encodent de l'information supplémentaire (pour un anneau « normal » R, on a $\pi_i(R) = 0$ pour $i > 0$). En ne considérant que les π_0 (l'anneau des composantes connexes) de ces anneaux, on retrouve la théorie des anneaux ordinaires.

Soit une représentation $\bar{\rho}$ d'un groupe profini Γ (par exemple un groupe de Galois) dans $\mathrm{GL}_n(k)$. Dans l'article fondateur de Galatius et Venkatesh ([GV16]), les auteurs expliquent qu'il est possible de considérer une généralisation du foncteur des déformations, qui est cette fois à valeur dans les ensembles *simpliciaux* :

$$\mathrm{Def}_{\bar{\rho}} : \mathbf{sArt}_k \to \mathbf{sSet}.$$

Là aussi, sous certaines hypothèses, en utilisant une version dérivée du critère de Schlessinger due à Lurie, on peut montrer que ce foncteur admet un représentant (dans la catégorie des pro-anneaux simpliciaux de coefficients, en un sens particulier) qu'on note $\mathfrak{R}_{\bar{\rho}}$. On a donc :

$$\underline{\mathrm{Hom}_{\mathrm{Pro}(\mathbf{sArt}_k)}}(\mathfrak{R}_{\bar{\rho}}, -) \simeq \mathrm{Def}_{\bar{\rho}}(-)$$

où $\simeq$ désigne la relation d'*équivalence naturelle faible entre foncteurs simplicialement enrichis*. Il s'agit alors de décrire $\mathfrak{R}_{\bar{\rho}}$. Cette approche moderne relie la théorie des déformations (en géométrie arithmétique) à des domaines assez lointains tels que la théorie de l'homotopie (en topologie algébrique) et l'étude des catégories des modèles.

Il se trouve que si on regarde $\pi_0\mathfrak{R}_{\bar{\rho}}$, on retrouve l'anneau de déformation universel classique, et que l'information supplémentaire apportée par les $\pi_i\mathfrak{R}_{\bar{\rho}}$ élargit notre compréhension de la situation arithmétique : elle donne des informations sur l'idéal des relations I qui apparaît dans la description de l'anneau de déformation universel (usuel) $W(k)[[t_1, \ldots, t_{d_1}]]/I$, et plus généralement sur les obstructions au relèvement de $\bar{\rho}$.

L'étude de ces anneaux de déformation dérivés est un sujet de recherche très actuel, et de nombreux·ses chercheur·euse·s travaillent sur des versions « dérivées » du théorème de relèvement modulaire de Wiles dans ce contexte. Comme la théorie usuelle des déformations, cette variante dérivée existe dans un cadre plus général que celui des représentations galoisiennes. Dans la thèse sur laquelle j'ai commencé à travailler avec Pierre Dèbes et Ariane Mézard, j'entreprends de décrire les anneaux de déformation dérivés associés à des représentations plus simples (entre groupes finis, ou à valeurs dans les groupes d'automorphismes de revêtements de courbes).

9 Aller plus loin

— Une présentation très différente (et élémentaire) du sujet est faite ici :
`http://images.math.cnrs.fr/Representations-galoisiennes-et.html`

— Dans mon mémoire de M2, je rentre beaucoup plus dans les détails techniques :
`http://lebarde.alwaysdata.net/maths/l3m2/memoire.pdf`
Notamment, on peut regarder les références présentes dans la bibliographie, qui sont généralement de grande qualité.

— Pour en apprendre plus sur la théorie de Hodge p-adique, le document suivant de Laurent Berger est très instructif (mais difficile !) :
`http://perso.ens-lyon.fr/laurent.berger/articles/article05.pdf`

— Le livre *Modular Forms and Fermat's Last Theorem* (Springer 1997) donne une idée assez claire de la preuve du théorème de Fermat par Wiles et présente la plupart des outils nécessaires.

Références

[AW67] M. F. Atiyah et C. T. C. Wall. "Cohomology of Groups". In : J. W. S. Cassels et A. Fröhlich. *Algebraic Number Theory*. 1967.

[Ber04] Laurent Berger. "An Introduction to the Theory of p-adic Representations". In : (2004).

[Car19] Xavier Caruso. *An introduction to p-adic period rings*. 2019. eprint : `arXiv:1908.08424`. url : `https://arxiv.org/abs/1908.08424`.

[Dat18] Jean-François Dat. *Introduction à l'arithmétique des courbes elliptiques*. 2018-2019, p. 38.

[FO08] Jean-Marc Fontaine et Yi Ouyang. *Theory of p-adic Galois Representations*. 2008.

[Gou91] Fernando Q. Gouvêa. *Deformations of Galois Representations*. American Mathematical Society, 1991.

[GV16] Soren Galatius et Akshay Venkatesh. "Derived Galois deformation rings". In : (2016). doi : `10.1016/j.aim.2017.08.016`. eprint : `arXiv:1608.07236`.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer-Verlag New York, 1977.

[Mil13] James S. Milne. *Lectures on Etale Cohomology (v2.21)*. Available at `www.jmilne.org/math/`. 2013.

[Moc97] Shinichi Mochizuki. "A Version of the Grothendieck Conjecture for p-Adic Local Fields". In : 1997.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. T. 322. Grundlehren der mathematischen Wissenschaften. Springer-Verlag Berlin Heidelberg, 1999, p. 140-141.

[Seg18] Béranger Seguin. "Les Déformations de Représentations Galoisiennes". Mém. de mast. Sorbonne Université, 2018-2019. url : `http://lebarde.alwaysdata.net/maths/l3m2/memoire.pdf`.

[Ser62] Jean-Pierre Serre. *Corps Locaux*. Hermann, Paris, 1962.