Introduction au domaine de recherche : Les représentations galoisiennes

Béranger Seguin (2019)

Table des matières

1 Introduction

1.1 Des équations aux extensions

Le problème central 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 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, et on note $L|K$, si les éléments de K sont dans L. L'extension $L|K$ est *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) ; le nombre minimal de tels éléments est alors la *dimension* de l'extension $L|K$, qu'on note $[L : K]$.

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 $\mathbb{Q}[\sqrt{-3}]|\mathbb{Q}$, illustre le 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, il est apparu 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 $L|K$ est défini ainsi :

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

De façon plus imagée, $\mathrm{Gal}(L|K)$ 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 $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$.

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

Définition 4. Soit une extension de corps $L|K$. 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 $L|K$ est toujours algébrique[1]. Lorsqu'une extension algébrique $L|K$ est séparable et normale (c'est-à-dire que les polynômes minimaux des éléments de L

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.

sont scindés sur L et n'ont que des racines simples), on dit qu'elle est *galoisienne*. Dans ce cas, on a la correspondance suivante, au cœur de la théorie :

Théorème 5 (correspondance de Galois)**.** *Lorsque $L|K$ est une extension galoisienne, les sous-groupes de* $\mathrm{Gal}(L|K)$ *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* $\mathrm{Gal}(L|K)$*, on peut définit la sous-extension suivante de L :*

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

Réciproquement, si E est une sous-extension, on définit le sous-groupe suivant de $\mathrm{Gal}(L|K)$ *:*

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

On a alors la suite exacte suivante :

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

En première approximation, cela s'interprète de la façon suivante : $\mathrm{Gal}(L|K)$ *est fait de deux morceaux, l'un ressemblant à* $\mathrm{Gal}(E|K)$ *et l'autre à* $\mathrm{Gal}(L|E)$*.*

La correspondance 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 peut lister toutes ses sous-extensions grâce à cette correspondance.

1.3 La théorie de Galois infinie

Pour le moment, on a autant d'objets d'études (extensions, groupes de Galois) qu'il y a de corps de nombres. Pour transformer cette question « multiple » en une question unique, on construit des objets « universels » qui compilent l'information sur toutes ces extensions.

Le corps des nombres algébriques, $\bar{\mathbb{Q}}$ contient *toutes* les racines des polynômes sur $\mathbb{Q}$: il est donc une extension algébrique maximale de $\mathbb{Q}$, 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 souhaite alors définir son groupe de Galois, avec en tête l'idée que ses quotients finis seront les groupes de Galois de ses sous-extensions finies, et donc de tous les corps de nombres. La définition naïve, à savoir $\mathrm{Aut}(\bar{\mathbb{Q}})$, ne permet pas d'avoir ces propriétés. Il faut en fait définir ce groupe de Galois de façon un peu particulière, par un procédé de « passage à la limite » (on parle de « limite projective ») :

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

Ainsi, un élément de $\mathrm{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$ est un automorphisme de corps de $\bar{\mathbb{Q}}$ particulier, qui peut 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 $\mathrm{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$ puisque le correspondance de Galois « passe à la limite » :

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

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

Puisqu'on était arrivé à la conclusion qu'il nous fallait comprendre les corps de nombres, on a désormais envie d'avoir autant d'informations que possible sur le groupe $\mathrm{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$, qu'on note $G_{\mathbb{Q}}$ par la suite (on dit que c'est le *groupe de Galois absolu* de $\mathbb{Q}$). En effet, chaque information au sujet de ce groupe se traduit (via la correspondance de Galois) en une information sur *tous* les corps de nombres : on devine ainsi la puissance de cette stratégie. Pour cette raison, le groupe de Galois absolu de $\mathbb{Q}$ est peut-être l'objet central 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. Une manière de rendre son étude moins ardue est de *compléter* $\mathbb{Q}$: cela qui permet de « tuer » tous les idéaux maximaux de $\mathbb{Z}$ sauf un, et donc de simplifier la situation. 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 habituelle (« archimédienne »). On obtient alors $\mathbb{R}$ et on connaît très bien $G_{\mathbb{R}} := \mathrm{Gal}(\mathbb{C}|\mathbb{R})$ 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 de morphismes de groupes $\mathbb{Z}/2\mathbb{Z} \to G_{\mathbb{Q}}$ ou, dit autrement, l'existence d'éléments d'ordre deux dans $G_{\mathbb{Q}}$, qui correspondent aux différents plongements de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$. En effet, étant donné un plongement $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, on retrouve un élément d'ordre deux en considérant la conjugaison complexe.

— Soit on complète $\mathbb{Q}$ pour une valeur absolue p-adique (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 note $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$, et on a alors un morphisme de groupes $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$. Vient alors l'idée que la description de $G_{\mathbb{Q}_p}$ pour tous les nombres premiers p nous aidera à comprendre $G_{\mathbb{Q}}$. Lorsqu'on étudie $\mathbb{Q}_p$ pour un nombre premier p fixé, on dit qu'on est dans le cas *local*.

Cette philosophie s'observe directement en termes d'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 p-adique*). On cherche alors à comprendre les corps p-adiques pour tous les nombres premiers p dans l'espoir d'obtenir des informations sur les corps de nombres.

Une fois la situation 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 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 qui suit naturellement consiste à trouver des théorèmes de passage local-global : on voudrait 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'interprète concrètement 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, qui est un résultat très percutant de « passage local-global ». Hélas, ce résultat ne s'étend pas aux équations de degré supérieur. Dans le cas général, il y a des obstructions au passage local-global.

Il y a cependant d'autres cas dans lesquels on sait effectuer ce passage local-global. Par exemple, la *théorie du corps de classes* permet d'obtenir pour tout corps de nombres K une description de G_K^{ab} (qui classifie les extensions abéliennes de K, c'est-à-dire celles dont le groupe de Galois est commutatif) en reliant ce groupe aux groupes $G_{K_v}^{\mathrm{ab}}$ obtenus pour les différentes complétions K_v de K. De plus, ces derniers sont eux-aussi décrits très explicitement.

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 topologique commutatif. On peut aussi la voir comme un morphisme de groupes continu :

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

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 de la catégorie des corps dans la catégorie des A-modules, alors tout élément $g \in \mathrm{Gal}(L|K)$ induit un morphisme $F(g) : F(L) \to F(L)$, et cela de manière fonctorielle ($F(gg') = F(g) \circ F(g')$). Autrement dit, il y a une action continue de $\mathrm{Gal}(L|K)$ sur le A-module $F(L)$, et donc (lorsque le module $F(L)$ est libre) une représentation galoisienne.

L'étude des représentations galoisiennes est motivée par l'idée que leur description permet de mieux comprendre les groupes de Galois et donc, comme on l'a vu nous, les extensions de corps et les équations polynomiales. Pour un point de vue très élémentaire et différent sur ces représentations, on peut aussi consulter cet article de Bas Edixhoven : `https://images-archive.math.cnrs.fr/Representations-galoisiennes-et-theoreme-de-Fermat-Wiles.html`.

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

3.2 Représentation associée à une courbe elliptique

Cet exemple est historiquement important : 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 : étant donnés deux points x, y de la courbe, je trace la droite qui les unit ; elle coupe la courbe en un troisième point ; la réflexion de ce point par rapport à l'axe des abscisses est notée $x + y$).

On peut ne regarder que l'ensemble $E_{\bar{\mathbb{Q}}}$ des points de E dont les coordonnées sont algébriques. 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. Les ensembles $E_{\bar{\mathbb{Q}}}$ et $E_{\mathbb{Q}}$ sont tous deux stables par la loi de groupe de la courbe elliptique.

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 montre (voir [Dat18]) que le groupe formé par les points de p^n-torsion de $E_{\bar{\mathbb{Q}}}$ est 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 des propriétés de cette représentation galoisienne permet d'étudier les propriétés de la courbe elliptique E.

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

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

On dira plus tard que ρ est une déformation (cadrée) de $\bar{\rho}_1$. Une idée centrale, au cœur de la preuve de Wiles, est d'essayer de « transférer » des propriétés des représentations à leurs déformations. Dans le cas présent, cela nous informe alors sur les propriétés de la courbe elliptique E dont on est parti.

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 $G_K := \mathrm{Gal}(\bar{K}|K)$ 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 « cohomologiques », 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, il vous suffit pour comprendre ce qui suit de savoir que toutes ces théories cohomologiques donnent lieu à 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].

Prenons 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 $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p^n\mathbb{Z})$ puis, par passage à la limite projective, sur la cohomologie étale p-adique, qui est un $\mathbb{Q}_p$-espace vectoriel :

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

Ainsi, 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 sont trop pathologiques pour provenir de ce genre de situations géométriques. Une des principales conjectures de la théorie des représentations galoisiennes (la conjecture de Fontaine–Mazur) prédit que toute représentation ayant d'assez bonnes propriétés 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 représentations : elles forment en quelque sorte un espace « discret ». On parle de la théorie des *représentations ℓ-adiques*.

— Si $p = \ell$, il y a énormément de représentations : elles forment un espace « continu ». On parle de la théorie des *représentations p-adiques*. Puisqu'il y en a beaucoup, on souhaite distinguer

différentes classes de régularité pour classer les représentations : cela donne à cette théorie un côté « 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, et s'écrit donc $(\zeta_n)^{a_n}$. L'entier a_n est défini uniquement modulo p^n, ne dépend pas de la racine ζ_n choisie, et par ailleurs $a_n = a_{n+1}$ modulo p^n puisque $\sigma(\zeta_{n+1}^p)$ est égal à la fois à $(\zeta_{n+1}^p)^{a_n}$ et $\sigma(\zeta_{n+1})^p = ((\zeta_{n+1})^{a_{n+1}})^p$. Ainsi la suite $(a_n)_{n\geq 1}$ définit un élément de $\mathbb{Z}_p^\times$. On définit de cette façon un morphisme de groupes (le *caractère cyclotomique*) :

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

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. Si $i \in \mathbb{Z}$, on utilise la notation $\mathbb{C}_p(i)$ pour désigner ce corps lorsqu'il est muni de l'action de $G_{\mathbb{Q}_p}$ suivante :

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

Soit une représentation $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(\mathbb{Q}_p)$. Son *$i$-ième poids de Hodge-Tate* est défini de la façon suivante :

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

où :

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

— l'action de $G_{\mathbb{Q}_p}$ 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, $d_\rho(i)$ est 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 χ. On a l'inégalité :

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

Lorsqu'il y a égalité, on dit que la représentation ρ est *de Hodge–Tate*. Cela signifie que ρ (vue sur $\mathbb{C}_p$) se découpe en puissances du caractère cyclotomique. En quelque sorte, cette propriété est analogue à la diagonalisabilité (les puissances du caractère cyclotomique remplaçant les homothéties).

D'autres conditions plus subtiles existent. Par exemple, on peut dire d'une représentation qu'elle est « de de Rham », « semi-stable », « cristalline », etc. Les représentations galoisiennes « naturelles », issues de contextes géométriques comme ceux vus précédemment, sont toujours de Hodge–Tate, et tombent même généralement dans ces catégories plus finies lorsque les objets géométriques dont elles proviennent sont suffisamment 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 proviennent de deux théories cohomologiques 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, on peut consulter [FO08] et [Ber04].

Cette théorie possède une ressemblance formelle avec la théorie de Hodge de la géométrie complexe, 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, qui détaille aussi cette analogie, se trouve dans [Car19].

En somme, la théorie de Hodge p-adique permet de « mettre de l'ordre » dans le vaste espace des représentations galoisiennes p-adiques, et notamment de reconnaître celles qui sont de nature « géométrique ».

4 Cohomologie galoisienne

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

4.1 Cohomologie des groupes

Soit G un groupe. Un $\mathbb{Z}[G]$-*module* est un groupe abélien sur lequel G agit. Il existe une unique suite de foncteurs $H^i(G, -)$, de la catégorie des $\mathbb{Z}[G]$-modules dans celle des groupes, satisfaisant les propriétés suivantes :

1. pour tout $\mathbb{Z}[G]$-module M, $H^0(G, M)$ est le sous-groupe M^G des points fixes de l'action de G sur M ;
2. toute suite exacte de $\mathbb{Z}[G]$-modules :

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

   induit une suite exacte longue :

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

3. $H^i(G, M)$ est nul (pour tout $i \geq 1$) chaque fois qu'il existe un groupe abélien A tel que $M \simeq \text{Hom}(\mathbb{Z}[G], A)$

On dit que $H^i(G, M)$ est le *i-ème groupe de cohomologie* du $\mathbb{Z}[G]$-module M.

4.2 Cohomologie galoisienne

Le cas particulier où G est un groupe de Galois est particulièrement intéressant, notamment parce que les groupes de Galois agissent naturellement sur divers objets. De nombreuses théories, parfois antérieures à la définition de la cohomologie des groupes, admettent des reformulations élégantes et compactes en termes de cohomologie galoisienne : cela inclut les théories de Kummer et d'Artin–Schreier, l'étude du groupe de Brauer, ou encore la dualité de Tate. Par exemple, on a le théorème 90 de Hilbert :

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

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.

La cohomologie associe un invariant algébrique aux actions du groupe de Galois. On peut alors relier représentations galoisiennes et cohomologie galoisienne. En effet, si :

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

est une représentation, on s'intéresse aux groupes de cohomologie du $\mathbb{Z}[G]$-module $\mathrm{ad}(\rho)$ obtenu en munissant $\mathfrak{M}_n(A)$ de l'action définie par $g.M = \rho(g)M\rho(g)^{-1}$.

On verra plus tard que l'espace de représentations galoisiennes (plus précisément des déformations d'une représentation fixée) admet parfois une structure « géométrique ». Les invariants géométriques de cet espace sont alors directement reliés aux invariants cohomologiques de $\mathrm{ad}(\rho)$. La cohomologie galoisienne est donc un outil important 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 comprendre la preuve de Mochizuki d'un résultat très concret ([Moc97]) :

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

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

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

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

puis, par passage à la limite projective, une filtration de G_K :

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

C'est la filtration de ramification. *On définit de même la filtration $(G_{K'})_i$ associée à un autre 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 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. Pourtant, on va voir que les représentations galoisiennes sont utiles à sa preuve.

On détaille à présent le squelette de la démonstration. Pour cela, on fixe un isomorphisme $\Phi : G_K \to G_{K'}$ qui préserve la filtration de ramification. On souhaite montrer que les corps K et K' sont isomorphes. La preuve se découpe en deux parties :

— On montre d'abord 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 montre qu'un isomorphisme entre groupes de Galois absolus qui préserve les poids de Hodge-Tate induit un isomorphisme entre les corps p-adiques. Pour cela, on construit 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. Puisque les poids sont préservés par Φ, K' se plonge aussi dans E. On conclut alors en montrant 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 disponibles : la décomposition de Hodge-Tate, la cohomologie galoisienne, la théorie du corps de classes local, etc. La puissance de ces outils justifie l'intervention des représentations galoisiennes dans des 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. Un *anneau de coefficients* est un anneau local dont le corps résiduel est $\mathbb{F}_p$, qui est 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).

Si ρ est une représentation d'un groupe de Galois G dans un anneau de coefficients A, on obtient une représentation $\bar{\rho}$ dans $\mathbb{F}_p$ via la surjection $A \twoheadrightarrow A/\mathfrak{m}_A \simeq \mathbb{F}_p$.

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

Pour toute matrice de $\mathrm{GL}_n(A)$ de la forme $I_n + M$ où M a ses coefficients dans $\mathfrak{m}_A$, le diagramme ci-dessus est toujours commutatif si on remplace ρ par $\rho' = M\rho M^{-1}$. On dira que deux représentations ρ et ρ' sont *strictement équivalentes* si elles sont ainsi conjuguées par une matrice M. 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 appelle alors les classes d'équivalence des *déformations de $\bar{\rho}$ à A*.

On s'intéresse alors au foncteur $\mathrm{Def}_{\bar{\rho}}$ qui associe à un anneau de coefficients A l'ensemble des déformations de $\bar{\rho}$ à A. En utilisant le « critère de Schlessinger », on montre que ce foncteur est *représentable*[4]. Cela 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 bijective entre les déformations de $\bar{\rho}$ à A et les morphismes

4. Il faut pour cela que G vérifie certaines propriétés, que les groupes de Galois qui nous intéressent vérifient, et que toutes les matrices de $\mathfrak{M}_n(k)$ commutant avec l'image de $\bar{\rho}$ soient scalaires. On se place dans le cas où ces conditions sont vérifiées.

d'anneaux $\varphi : \mathfrak{R} \to A$, donnée par l'application :

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

Autrement dit, on a une sorte d'« espace de paramètres » qui permet d'explorer les déformations. L'intérêt est que cet anneau de déformation, en tant qu'anneau de coefficients, a une structure riche : par exemple, il dispose d'un espace tangent, dont on peut calculer la dimension, etc.

6.2 Description cohomologique de l'anneau de déformation universel

On a vu que la représentation $\bar{\rho}$ définit un $\mathbb{F}_p[G]$-module $\mathrm{ad}(\bar{\rho})$. On définit alors l'invariant numérique $d_i := \dim_k H^i(G, \mathrm{ad}(\bar{\rho}))$, la dimension de son i-ième groupe de cohomologie.

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 $d = \dim_{\mathbb{F}_p} t^*_{\mathfrak{R}}$ donne beaucoup d'informations sur $\mathfrak{R}$; 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. Or, on peut montrer que $d = d_1$. Pour décrire $\mathfrak{R}$, il ne reste alors « plus qu'à » décrire l'idéal 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 :

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

Il est conjecturé que cette inégalité est une égalité sous des hypothèses faibles ($\bar{\rho}$ est absolument irréductible, ce qui implique notamment $d_0 = 1$). Lorsque K est un corps p-adique, on peut calculer explicitement $d_1 - d_2$ (cf. [Seg18, sous-section 4.3.3]) :

$$d_1 - d_2 = d_0 + n \cdot [K : \mathbb{Q}_p]^2$$

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

6.2.3 Obstruction

On sait décrire explicitement $\mathfrak{R}$ lorsque $d_2 = 0$. En effet, dans ce cas, on a :

$$\mathfrak{R} \simeq \mathbb{Z}_p[[X_1, X_2, \ldots, X_{d_1}]],$$

et en particulier $\dim_{\mathrm{Krull}}(\mathfrak{R}/p\mathfrak{R}) = d_1$. On dit alors que le problème de déformation est *non-obstrué* : étant donné une déformation une déformation $G \to \mathrm{GL}_n(B)$ et une surjection $A \twoheadrightarrow B$, on peut toujours trouver une déformation $G \to \mathrm{GL}_n(A)$ qui fasse « commuter le diagramme ». Cela permet de comprendre pourquoi les obstructions à la déformation se trouvent dans le groupe $H^2(G, \mathrm{ad}(\bar{\rho}))$.

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.

Avant Wiles, une conjecture ouverte prédisait que toute courbe elliptique était *modulaire*, c'est-à-dire liée à une certaine « forme modulaire » (une certaine classe de fonctions holomorphes sur le demi-plan complexe). Le fait qu'une courbe elliptique soit modulaire ou non s'observe en fait au niveau de 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 (semi-stable) d'équation suivante :

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

Ribet a montré que cette courbe elliptique, si elle existait, ne pouvait pas être « 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 démontré est que toute courbe elliptique semi-stable sur $\mathbb{Q}$ est modulaire, rejetant donc 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 (notamment liées à sa ramification). On dira simplement que ρ_p est une *bonne* représentation, sans définir ce que l'on veut dire par là.

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

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

— D'autre part, l'« algèbre de Hecke » $\mathbf{T}$, qu'on peut voir comme un espace paramétrant les formes modulaires associées aux bonnes déformations modulaires de $\bar{\rho}_p$.

Pour établir la correspondance entre *bonnes* déformations de $\bar{\rho}_p$ et formes modulaires, et donc pour établir la modularité de ρ_p, il suffit alors de montrer que les anneaux $\mathfrak{R}$ et $\mathbf{T}$ sont isomorphes. Wiles réussit à ramener cette question à une égalité numérique (dans l'esprit des 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 transforment des problèmes, comme la question du relèvement de représentations résiduelles modulaires en représentations modulaires, en des questions géométriques sur des espaces classifiants. En utilisant des invariants tels que la « dimension », on a alors des outils additionnels pour affronter le problème. Une approche similaire a permis de faire des progrès dans la conjecture de Fontaine–Mazur.

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

Soit p un nombre premier et k un corps parfait de caractéristique p (typiquement, $\mathbb{F}_p$). 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, ..., peuvent être additionnés et multipliés comme dans un anneau. Cet aspect géométrique rend la structure de ces objets beaucoup plus riche. Par exemple, ils disposent de groupes d'homotopie π^i, 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 définissent 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 encore, sous certaines hypothèses, une version dérivée du critère de Schlessinger due à Lurie entraîne que ce foncteur admet un représentant $\mathfrak{R}_{\bar{\rho}}$, dans la catégorie des pro-anneaux simpliciaux de coefficients (en un sens particulier). 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 $\pi_i\mathfrak{R}_{\bar{\rho}}$ raffine 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 $\bar{\rho}$.

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 (version révisée en 2024)". Mém. de mast. Sorbonne Université, 2018-2019. url : https://beranger-seguin.fr/assets/pdf/memoire.pdf.

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