Mémoire de magistère

Arithmétique et p-adique

par

Xavier Caruso

Table des matières

L'arithmétique est principalement l'étude de l'anneau des entiers relatifs $\mathbb{Z}$, de son corps des fractions $\mathbb{Q}$ formé de ce que l'on appelle les nombres rationnels et des extensions finies ou algébriques de ce dernier. Ce texte se propose de décrire un des multiples aspects de cette étude, et d'énoncer un résultat encore conjectural permettant de voir quelle genre de choses on attend et en quoi elles sont intéressantes.

Ce texte commence donc par faire de très brefs rappels sur la géométrie algébrique et la localisation qui débouchent naturellement sur la présentation de $\mathbb{Q}_p$ et de ses extensions. Il nous faudra aussi consacrer quelques pages à l'étude des groupes de Galois de ces extensions car il s'agit vraiment de l'objet simple à manipuler qui détient énormément d'informations. On sera alors en mesure de conclure en énonçant le résultat dont on a déjà parlé et de donner quelque vague idée de la façon dont on peut l'attaquer.

1 Un peu de géométrie algébrique

1.1 Les idées de base de la géométrie algébrique

Comme son nom l'indique, la géométrique algébrique essaie de donner un sens géométrique à un objet purement algébrique, précisément aux anneaux. L'idée consiste plus ou moins, étant donné un anneau A, de voir A comme l'anneau des polynômes sur un certain « objet géométrique ». Bien entendu, pour l'instant cela n'a pas grand sens : il reste encore à définir « objet géométrique » et même « anneau des polynômes » parce que si l'on sait ce que sont les polynômes à coefficients dans $\mathbb{R}$, $\mathbb{C}$ ou même n'importe quel anneau, on ne sait pas *a priori* ce qu'est l'anneau des polynômes à coefficients dans un « objet géométrique », typiquement un espace topologique.

Nous n'allons pas ici détailler toutes les constructions permettant de concrétiser la chose précédente car elles ne rentrent pas dans le cadre de cet exposé. Nous allons plutôt présenter un exemple qui permet de se faire une idée intuitive de la situation, puis appliquer cet exemple à l'arithmétique, c'est-à-dire à l'anneau $\mathbb{Z}$.

Donc, pour commencer, on remplace $\mathbb{Z}$ par $\mathbb{C}[u]$, l'anneau des polynômes à une variable à coefficients complexes. D'après ce qui a été dit précédemment, il n'est pas surprenant d'apprendre que l'« objet géométrique » associé à cet anneau est la droite complexe, $\mathbb{C}$ donc. De la même façon, si on avait choisi de considérer $\mathbb{C}[u,v]$, l'anneau des polynômes en deux variables à coefficients complexes, l'« objet géométrique » associé aurait été le plan complexe, c'est-à-dire $\mathbb{C}^2$.

Mais restons avec la droite complexe et donc avec l'anneau $\mathbb{C}[u]$. Ce qu'il est important de remarquer, c'est que ce dictionnaire que nous n'avons que peu détaillé est compatible avec les extensions. Mais, déjà, extension de quoi ? On n'a toujours pas de corps pour l'instant. En fait, le corps que l'on va considérer est le corps des fractions de $\mathbb{C}[u]$, c'est-à-dire $\mathbb{C}(u)$, le corps des fractions rationnelles à coefficients complexes, et ce un peu de la même façon qu'en arithmétique $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. Bien évidemment, cela ne se généralise pas directement à toutes les situations : il faut au moins supposer que l'anneau considéré est intègre, et même un peu plus pour que les choses se passent correctement, mais nous n'allons pas non plus entrer dans ces détails.

Considérons maintenant K une extension disons finie de $\mathbb{C}(u)$. À partir de cela, on peut en fait construire un nouvel anneau, qui sera inclus dans K, dont le corps des fractions sera K et qui correspondra moralement à l'extension $K/\mathbb{C}(u)$ mais vue simplement sur $\mathbb{C}[u]$. Plus précisément, on a la définition suivante :

Définition 1.1.1. *On reprend les notations de la situation précédente. Un élément $x \in K$ est dit* entier *sur $\mathbb{C}[u]$ s'il existe un polynôme P* unitaire *à coefficients dans $\mathbb{C}[u]$ vérifiant $P(x) = 0$. Cela revient en fait simplement à demander que le polynôme minimal de x sur $\mathbb{C}(u)$ soit à coefficient dans $\mathbb{C}[u]$.*

*On définit finalement l'*anneau des entiers *de l'extension $K/C(u)$ comme l'ensemble des éléments $x \in K$ entiers sur $\mathbb{C}[u]$ (dont il faut vérifier par ailleurs qu'il forme bien un anneau). On le note souvent $\mathcal{O}_K$.*

On peut résumer la situation par le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & K \\ {\scriptstyle n}\downarrow & & \downarrow{\scriptstyle n} \\ \mathbb{C}[u] & \longrightarrow & \mathbb{C}(u) \end{array}$$

On a alors plusieurs propriétés intéressantes sur cet anneau des entiers $\mathcal{O}_K$, notamment le fait que si n désigne le dégré de l'extension $K/\mathbb{C}(u)$, $\mathcal{O}_K$ est en fait un $\mathbb{C}[u]$-module libre de dimension n également.

Mais prenons encore un exemple. Prenons tout d'abord $K = \mathbb{C}(u, v)$ qui certes n'est pas une extension finie de $\mathbb{C}(u)$ mais cela n'a pas pour l'instant d'importance. On ne peut pas dans ce cas définir l'anneau des entiers, mais il est ici tout à fait légitime de considérer qu'il s'identifie à $\mathbb{C}[u, v]$.

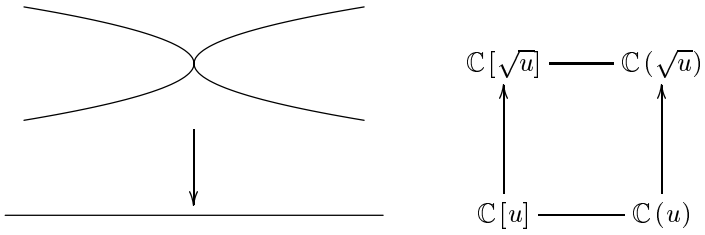
Essayons maintenant de comprendre la vision géométrique. L'« objet géométrique » associé à $\mathbb{C}[u]$ est, comme on l'a déjà dit, la droite complexe $\mathbb{C}$. Également, l'« objet géométrique » associé à $\mathbb{C}[u, v]$ est le plan complexe $\mathbb{C}^2$. L'extension, elle, est en outre donnée par une application $C(u) \to C(u, v)$. Bien entendu, il était sous-entendu précédemment que celle-ci était l'inclusion canonique. Ce qu'il est important de constater, c'est qu'à cette inclusion correspond une application entre les objets géométriques : ici, c'est précisément la première projection $\varphi : \mathbb{C}^2 \to \mathbb{C}$. Pourquoi cela ? Parce que si l'on prend $P \in \mathbb{C}[u]$ et qu'on le compose par φ, c'est-à-dire qu'on lui associe le polynôme $\tilde{P}(u, v) = P \circ \varphi(u, v) = P(u)$, on retrouve précisément l'inclusion canonique qui définissait l'extension dont on était parti.

Essayons maintenant de faire la même chose sur un exemple qui est une extension finie. Prenons par exemple $\mathbb{C}(\sqrt{u})$ qui est bien une extension de $\mathbb{C}(u)$, là encore en utilisant l'inclusion canonique. On peut encore déterminer l'anneau des entiers dans ce cas et voir qu'il s'identifie à $\mathbb{C}[\sqrt{u}]$. Pour comprendre quel « objet géométrique » on va associer à cet anneau, il est nécessaire de modifier un peu son écriture. Ajouter $\sqrt{u}$, c'est ajouter une nouvelle variable v et imposer que celle-ci vérifie $v^2 = u$. Autrement dit, $\mathbb{C}[\sqrt{u}]$ n'est autre que le quotient $\mathbb{C}[u, v] / (v^2 - u)$. Il s'agit donc de trouver une partie de $\mathbb{C}^2$ sur laquelle les polynômes sont définies à $(v^2 - u)$ près, c'est-à-dire sur laquelle ajouter ou enlever $(v^2 - u)$ ne modifie rien, c'est-à-dire sur laquelle $(v^2 - u)$ est nul. On prend donc la partie :

$$A = \left\{ (u, v) \in \mathbb{C}^2 \;\middle|\; v^2 = u \right\}$$

Il s'agit d'une parabole et de la même façon que tout à l'heure l'application de A dans $\mathbb{C}$ qui correspond à notre extension est encore la première projection.

Récapitulons avec le dessin suivant :



1.2 De l'intérêt de la localisation et de la complétion

On aimerait dire au vu du dessin précédent que l'extension $\mathbb{C}(\sqrt{u})/\mathbb{C}(u)$ ne se comporte pas de la même façon en 0 qu'ailleurs. Mais dit comme ça, cette phrase n'a pas de sens. C'est ce que nous allons plus ou moins préciser dans ce paragraphe.

Notons que l'on aimerait une description locale certes, mais aussi purement algébrique puisque l'on aimerait l'appliquer ensuite à l'arithmétique, c'est-à-dire à $\mathbb{Z}$ et $\mathbb{Q}$. On n'a donc plus le choix maintenant, il va nous falloir préciser quelque peu comment on construit l'« objet géométrique » associé à un anneau donné. Citons pour cela le théorème suivant :

Théorème 1.2.1. *Les idéaux maximaux de $\mathbb{C}[u]$ sont exactement ceux engendrés par les éléments $(u - x)$ où x parcourt $\mathbb{C}$.*

Ce théorème dit si l'on peut regarder la droite complexe non pas comme un ensemble de complexes justement, mais plutôt comme un ensemble d'idéaux maximaux de l'anneau $\mathbb{C}(u)$. Plus précisément au lieu de parler du complexe x, il s'agit de parler de l'idéal engendré par $(u - x)$ (qui est maximal), mais cela ne modifie guère les choses finalement. Cette définition se généralise en fait plus ou moins, et dans de bonnes conditions, on peut

considérer que l'« objet géométrique » associé à un anneau est en fait l'ensemble de ces idéaux maximaux[1]. Bien évidemment, il faut encore définir la géométrie sur cet objet mais nous n'allons pas le faire.

On aimerait maintenant faire la chose suivante. On considère un complexe x ou si l'on préfère un idéal maximal de $\mathbb{C}(u)$ et on aimerait construire à partir de cela, on nouvel anneau dont l'« objet géométrique » associé serait le seul point x. On aimerait en outre que si l'on part d'une extension de $\mathbb{C}(t)$, celle-ci fournisse une « extension » de ce nouveau anneau, dont l'« objet géométrique » associé soit exactement l'ensemble des points qui se projettent sur x.

Une solution pour arriver à ça est d'éliminer tous les idéaux maximaux de $\mathbb{C}[u]$ différents de $(u-x)$. Cela se fait en inversant formellement tous les éléments qui n'appartiennent pas à l'idéal engendré par $(u-x)$. On pose donc :

$$\mathbb{C}[u]_x = \left\{ \frac{P}{Q} \;\middle|\; (u-x) \text{ ne divise pas } Q \right\}$$

Ce nouvel anneau s'appelle naturellement le *localisé* de $\mathbb{C}[u]$ en l'idéal maximal engendré par $(u-x)$ et répond bien à la question que l'on se posait.

Mais cela ne nous suffit pas, principalement car l'étude des « extensions » de cet anneau repose en général principalement sur l'étude de l'extension correspondante du corps des fractions et on peut vérifier facilement que le corps des fractions n'a pas changé. Donc, après avoir *localisé*, il va falloir *compléter*. L'idée qui se cache derrière le procédé de complétion est en fait assez simple. Comme tout à l'heure on a rajouté formellement des inversibles, il s'agit maintenant de rajouter l'élément $\sqrt{u}$, mais seulement au « voisinage » de $x \in \mathbb{C}^\star$, de sorte qu'il n'apparaisse plus lorsque l'on regarde l'extension de notre nouveau corps, et ce pour la bonne raison qu'il y était déjà avant. Cela pour l'instant n'a pas grand sens mais voyons comment on procède.

Un bon moyen de s'en sortir dans ce cas est de considérer non plus l'anneau des polynômes à une variable à coefficients dans $\mathbb{C}$, mais celui des séries formelles. On remarquera qu'ainsi on a en outre rajouter les inverses qui nous manquaient tout à l'heure. On constatera d'ailleurs que cela revient exactement à rajouter la fonction $\frac{1}{u}$ au « voisinage » de $x \neq 0$.

La situation est donc maintenant devenue la suivante. On part de $\mathbb{C}[\![u]\!]$, l'anneau des séries formelles à coefficients dans $\mathbb{C}$, on considère son corps des fractions $\mathbb{C}((u))$. L'extension qui correspond à $\mathbb{C}(\sqrt{u})$ est $\mathbb{C}((\sqrt{u}))$ ou encore $\mathbb{C}((u,v)) \,/\, \left(v^2-u\right)$. On ne voit peut-être pas encore très bien l'intérêt de considérer ces objets plus gros, ni pourquoi d'ailleurs ce corps ne contient vraiment qu'une information locale mais cela va devenir clair avec le théorème suivant :

Théorème 1.2.2 (Puiseux). *Toute extension finie de $\mathbb{C}((u))$ est de la forme $\mathbb{C}((\sqrt[n]{u}))$ où n est tout simplement de l'extension considérée.*

Sur notre exemple, si l'on regarde au-dessus de 0, l'extension est comme on vient de le voir $\mathbb{C}((\sqrt{u}))$, ce qui signifie qu'au dessus de 0 deux courbes se croisent. Ailleurs, l'extension n'aurait pas été un corps, elle aurait été $\mathbb{C}((u)) \times \mathbb{C}((u))$, ce qui signifie bien qu'il y a deux courbes mais qu'elles ne se croisent pas. Plus généralement, si au-dessus d'un point l'extension est $\mathbb{C}((\sqrt[n_1]{u})) \times \ldots \times \mathbb{C}((\sqrt[n_k]{u}))$, cela voudra dire qu'on aura un paquet de n_1 courbes qui se croisent en un point, puis un paquet de n_2 courbes qui se croisent en un autre point et ainsi de suite.

Noter finalement que ceci n'aurait pas marché aussi bien si l'on avait remplacé $\mathbb{C}$ par $\mathbb{R}$ par exemple. En effet, $\mathbb{C}((t))$ est aussi une extension finie de $\mathbb{R}((t))$ et pourtant n'entre pas dans le cadre précédent. Là, l'erreur n'est pas difficile à corriger puisqu'il suffit d'autoriser $\mathbb{R}$ et $\mathbb{C}$. Plus généralement si on remplace $\mathbb{C}$ par un corps k de caractéristique nulle, l'erreur se corrige encore de la même façon en disant que les extensions finies de $k((u))$ sont de la forme $K((\sqrt[n]{u}))$ où n est un entier et K une extension finie de k. Cette extension finie toutefois ne va pas se voir directement sur le dessin.

2 Un peu d'arithmétique

À partir de maintenant, on remplace l'anneau $\mathbb{C}[u]$ par $\mathbb{Z}$, l'anneau des nombres entiers relatifs. On remplace donc évidemment $\mathbb{C}(u)$ par $\mathbb{Q}$, le corps des nombres rationnels et on va essayer de généraliser la vision géométrique donnée précédemment à cet exemple.

[1] La définition générale consiste non pas à prendre l'ensemble des idéaux maximaux, mais plutôt l'ensemble des idéaux premiers pour former ce que l'on appelle le *spectre* de l'anneau.

2.1 L'identité géométrique des entiers

L'« objet géométrique » associé à l'anneau $\mathbb{Z}$ va être comme on l'a déjà plus ou moins expliqué l'ensemble des nombres premiers, que l'on va noter $\mathcal{P}$.

Prenons maintenant K ce que l'on appelle un *corps de nombres*, c'est-à-dire une extension finie de $\mathbb{Q}$. Comme tout à l'heure, on peut considérer l'anneau des entiers et l'une des questions que l'on peut se poser est de décrire $\mathcal{O}_K$ et en particulier de décrire l'« objet géométrique » qui lui est associé.

De fait, les méthodes précédentes s'adaptent pour la description de cet objet géométrique. On commence par choisir un nombre premier p, on localise, on complète, on obtient ainsi un corps appelé $\mathbb{Q}_p$ dont la construction sera expliquée au paragraphe suivant. L'extension K va fournir une algèbre au-dessus de $\mathbb{Q}_p$, précisément l'algèbre $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ et celle-ci va se décomposer en produits d'extensions finies de $\mathbb{Q}_p$ et comme précédemment il y a un moyen relativement simple étant donné une extension finie de $\mathbb{Q}_p$ de déterminer à combien d'intersections elle correspond.

2.2 Présentation de $\mathbb{Q}_p$

Tout à l'heure, on a un peu sorti magiquement l'anneau $\mathbb{C}[\![u]\!]$, mais en fait ceci n'a rien d'anecdotique et peut même se généraliser relativement simplement. Pour cela, il faut avoir le bon point de vue sur les séries formelles : une série formelle est en fait la donnée pour tout entier n d'un polynôme de degré n et ce de façon compatible, cela voulant dire que les coefficients de bas degré coïncident quand ils le peuvent. Dans un langage que certains trouvent châtié, cela s'écrit :

$$\mathbb{C}[\![u]\!] = \varprojlim_{n\in\mathbb{N}} \mathbb{C}[u]/u^n$$

Bien entendu si l'on avait voulu regarder au voisinage de 1, il aurait fallu considérer :

$$\varprojlim_{n\in\mathbb{N}} \mathbb{C}[u]/(u-1)^n$$

Pour $\mathbb{Z}$, on fait la même chose en posant :

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

Un élément de $\mathbb{Z}_p$ est ainsi une sorte de série formelle en p, mais il faut faire attention qu'il ne faut ni les additionner, ni les multiplier comme on le fait avec des séries formelles classiques. Cela est dû au fait que $\mathbb{Z}/p^n\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$ ni en tant qu'anneau, ni même en temps que groupe. Il est même possible de dire *via* ces analogies où on devrait prendre les coefficients pour former une telle série formelle : il s'agit simplement du premier quotient de la limite projective, c'est-à-dire ici $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

On a en fait un énoncé précis qui dit tout ça :

Théorème 2.2.1 (Développement de Hensel). *Soit S un système de représentants dans $\mathbb{Z}$ des classes de $\mathbb{Z}/p\mathbb{Z}$ (par exemple on peut prendre $S = \{0, 1, \ldots, p-1\}$). Alors tout élément $x \in \mathbb{Z}_p$ s'écrit de façon unique sous la forme :*

$$x = \sum_{n=0}^{\infty} a_n p^n$$

où tous les a_n sont des éléments de S.

On remarque tout d'abord que l'addition ce coup-ci est vraiment celle de $\mathbb{Z}_p$ mais qu'il n'y a pas de formules simples pour exprimer les coefficients qui apparaissent dans la décomposition de $x + y$ en fonction de ceux qui apparaissent dans celle de x et celle de y. Il n'y a pas non plus de formule simple pour le produit.

On remarque en outre qu'il aurait été possible de choisir les éléments de S non pas dans $\mathbb{Z}$ mais dans $\mathbb{Z}_p$, ceci principalement car pour tout entier n, les anneaux $\mathbb{Z}/p^n\mathbb{Z}$ et $\mathbb{Z}_p/p^n\mathbb{Z}_p$ sont isomorphes et donc $\mathbb{Z}_p$ s'écrit également comme la limite projective suivante :

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p$$

Il s'agit finalement de définir $\mathbb{Q}_p$ qui est bien entendu le corps des fractions de $\mathbb{Z}_p$. De la même façon que pour les séries formelles, il suffisait d'inverser u pour passer de $\mathbb{C}[\![u]\!]$ à $\mathbb{C}((u))$, ici, il suffit d'inverser p pour passer de $\mathbb{Z}_p$ à $\mathbb{Q}_p$. De plus, le développement de Hensel s'adapte aussi pour décrire les éléments de $\mathbb{Q}_p$:

Théorème 2.2.2 (Développement de Hensel). *Soit S un système de représentants dans $\mathbb{Z}$ des classes de $\mathbb{Z}/p\mathbb{Z}$ (par exemple on peut prendre $S = \{0, 1, \ldots, p-1\}$). Alors tout élément $x \in \mathbb{Q}_p$ s'écrit de façon unique sous la forme :*

$$x = \sum_{n=-\infty}^{\infty} a_n p^n$$

où tous les a_n sont des éléments de S et les a_n sont nuls pour n suffisamment petit.

2.3 Description de $\mathbb{Q}_p$

Il est possible d'améliorer quelque peu le développement de Hensel. En fait, il existe une unique application $T : \mathbb{F}_p \to \mathbb{Z}_p$ qui soit multiplicative et une section de la projection canonique.

Si $a \in \mathbb{F}_p$, on note traditionnellement $[a]$ l'image de a par l'application T définie précédemment, c'est ce que l'on appelle le *représentant de Teichmüller* de a. Il n'est pas forcément difficile de la construire mais nous n'allons pas le faire ici.

On peut maintenant utiliser ces représentants particuliers dans le développement de Hensel, les opérations pouvant alors s'exprimer par des formules certes compliquées mais qui existent. Elles sont de la forme, si a_n et b_n sont des éléments de $\mathbb{F}_p$:

$$\begin{aligned}
\left(\sum_{n\in\mathbb{N}} [a_n]\, p^n\right) + \left(\sum_{n\in\mathbb{N}} [b_n]\, p^n\right) &= \sum_{n\in\mathbb{N}} [S_n]\, p^n \\
\left(\sum_{n\in\mathbb{N}} [a_n]\, p^n\right) \times \left(\sum_{n\in\mathbb{N}} [b_n]\, p^n\right) &= \sum_{n\in\mathbb{N}} [P_n]\, p^n
\end{aligned}$$

où S_n et P_n s'expriment comme des polynômes à coefficients entiers en $a_0, \ldots, a_n, b_0, \ldots, b_n$, polynômes très laborieux à écrire au demeurant.

On remarquera que cette description aurait aussi permis de définir directement $\mathbb{Z}_p$ par un autre procédé. Il aurait fallu considérer les suites d'éléments de $\mathbb{F}_p$ et mettre sur cet ensemble les lois définies par les polynômes mentionnés précédemment. Cela n'est en fait pas sans intérêt car l'on peut remplacer $\mathbb{F}_p$ par n'importe quel anneau et l'on construit ainsi à chaque fois un anneau. L'anneau construit à partir de A s'appelle l'*anneau des vecteurs de Witt* de A et se note traditionnellement $W(A)$.

On peut de façon analogue construire le développement « décimal » d'un élément de $\mathbb{Q}_p$, c'est-à-dire un élément du quotient de $\mathbb{Q}_p/\mathbb{Z}_p$ en invoquant les *covecteurs de Witt*. Finalement, on peut aussi construire les éléments de $\mathbb{Q}_p$ ce coup-ci avec les *bi-vecteurs de Witt*.

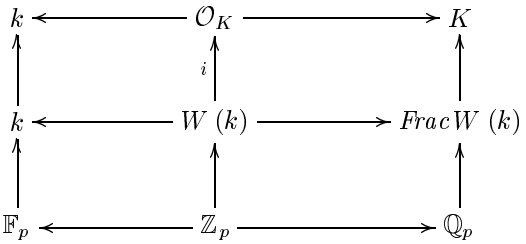
2.4 Les extensions finies de $\mathbb{Q}_p$

On aimerait avoir un théorème analogue à l'énoncé 1.2.2, mais ceci ne se passe aussi bien dans ce contexte et ce parce que $\mathbb{F}_p$ n'est ni algébriquement clos, ni de caractéristique nulle.

Commençons par voir ce que l'on peut faire pour le premier écueil. On avait vu dans les remarques suivant ledit théorème que si $\mathbb{C}[u]$ était remplacé par $k[u]$, il fallait faire attention à ne pas oublier les extensions de la forme $K[u]$ où K était une extension finie de k. Ici, c'est pareil à quelques transpositions près : si k est une extension finie de $\mathbb{Q}_p$, il ne faut pas oublier les extensions du type $\operatorname{Frac} W(k)$, où W désigne toujours l'anneau des vecteurs de Witt.

Un résultat précis est le théorème suivant :

Théorème 2.4.1. *Soit K une extension finie de $\mathbb{Q}_p$. On note $\mathcal{O}_K$ l'anneau des entiers de K et k le quotient $K/\mathcal{O}_K$ appelé généralement le corps résiduel. Dans ces conditions, il existe une unique application $i : W(k) \to \mathcal{O}_K$ faisant commuter le diagramme suivant :*



l'application $W(k) \to k$ étant celle qui à la suite $(a_0, \ldots, a_n, \ldots)$ associe a_0.

Ce théorème dit donc que l'on peut intercaler au milieu d'une extension finie K de $\mathbb{Q}_p$ une extension ayant le même corps résiduel que K et qui plus est peut se construire à partir des vecteurs de Witt. Ce que l'on aimerait désormais, c'est que K s'obtienne à partir de $W(k)$ simplement en ajoutant une racine n-ième de $p = (0, 1, 0, \ldots, 0, \ldots)$ pour un certain n. Mais cela n'est pas vrai et c'est là qu'intervient le deuxième écueil.

Toutefois la situation n'est pas aussi désespérée qu'on pourrait le croire car cela est vrai si le degré de l'extension n'est pas un multiple du nombre premier p. Récipatulons tout cela en énonçant un nouveau théorème :

Théorème 2.4.2. *Soit k une extension finie de $\mathbb{F}_p$ et K une extension finie du corps $FracW(k)$ dont le degré n est premier à p. Alors l'extension $K/FracW(k)$ est isomorphe à l'extension $FracW(k)\left[\sqrt[n]{p}\right]/FracW(k)$.*

Attention, cela n'est plus vrai si p divise e.

2.5 La clôture algébrique de $\mathbb{Q}_p$

Ce que l'on a dit précédemment s'applique plus ou moins également à la clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$. Donnons tout de suite le diagramme qui résume les résultats que l'on va commenter par la suite.

$$\begin{array}{ccc}
\bar{\mathbb{F}}_p & & \bar{\mathbb{Q}}_p \\
| & & | \, I_s \\
\bar{\mathbb{F}}_p & & \mathbb{Q}_p^{\mathrm{mr}} \\
| & & | \, I_m = \varprojlim_{p \nmid n} \mathbb{Z}/n\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_\ell \\
\bar{\mathbb{F}}_p & & \mathbb{Q}_p^{\mathrm{nr}} \\
| & & | \, \mathrm{Gal}\left(\bar{\mathbb{F}}_p/\mathbb{F}_p\right) = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} \\
\mathbb{F}_p & & \mathbb{Q}_p
\end{array}$$

Tout d'abord, on regarde l'extension que l'on obtient en rajoutant des éléments dans le corps résiduels : c'est $\mathbb{Q}_p^{\mathrm{nr}}$, l'*extension maximale non ramifiée* comme on l'appelle généralement[2]. $\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p$ est une extension galoisienne et le groupe de Galois s'identifie au groupe de Galois absolu de $\mathbb{F}_p$.

Vient ensuite l'extension maximale modérément ramifiée. Elle s'obtient précisément en rajoutant à $\mathbb{Q}_p^{\mathrm{nr}}$ toutes les racines n-ième de p où n parcourt l'ensemble des entiers qui ne divisent pas p. Le théorème 2.4.2 s'applique également à cette situation et dit donc que si K est une extension finie de $\mathbb{Q}_p^{\mathrm{nr}}$ de degré premier à p, alors elle est incluse dans $\mathbb{Q}_p^{\mathrm{mr}}$.

Déterminer le groupe de Galois est quelque chose de relativement simple. Il suffit pour cela de choisir un entier n qui ne divise pas p et de se convaincre que l'extension $\mathbb{Q}_p^{\mathrm{nr}}\left[\sqrt[n]{p}\right]/\mathbb{Q}_p$ est galoisienne de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$.

[2]Le terme *non ramifié* vient du fait que si l'on regarde l'« objet géométrique » associé à cette extension, il n'y a qu'un trait, pas plusieurs qui se croisent.

Ce groupe de Galois est noté I_m et s'appelle le *groupe d'inertie modérée*. C'est lui qui va nous intéresser par la suite.

La dernière extension, elle, est plus compliquée à étudier. Elle est galoisienne évidemment et son groupe de Galois, noté I_s, est le *groupe d'inertie sauvage*. Décrire ce groupe n'est pas quelque chose d'immédiat, il est encore nécessaire pour cela d'introduire des extensions intermédiaires et même *a priori* en nombre infini. Nous n'allons pas plus détailler les choses vu que par la suite on ne s'intéressera systématiquement pas à ce groupe.

Finalement disons que le groupe de Galois de l'extension $\bar{\mathbb{Q}_p}/\mathbb{Q}_p^{\mathrm{nr}}$ est appelé le *groupe d'inertie*.

3 Énoncé du résultat conjectural principal

Ce résultat commence par construire par des moyens géométriques des représentations dans un $\mathbb{F}_p$-espace vectoriel du groupe de Galois absolu de $\mathbb{Q}_p$, plus ou moins décrit précédemment donc. L'objet du théorème est de décrire ces représentations. Mais ces descriptions sont difficiles à faire principalement parce que la structure complète du groupe de Galois est difficile à décrire ; on va donc se débrouiller par la suite pour n'obtenir des représentations que du groupe d'inertie modérée que lui, on connaît quand même mieux.

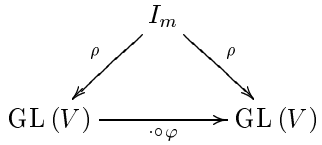
On commence cette partie en expliquant comment l'on peut classifier quelques unes des représentations de ce groupe d'inertie modérée.

3.1 Représentations simples du groupe d'inertie modérée

On se donne ρ une représentation *continue* de groupe d'inertie modérée de dimension finie, disons r, dans un $\mathbb{F}_p$-espace vectoriel. On rappelle que cela signifie que ρ est un morphisme de groupes de I_m dans $\mathrm{GL}(V)$ où V est un $\mathbb{F}_p$-espace vectoriel de dimension r. On peut aussi également voir ρ comme une action du groupe I_m sur l'espace vectoriel V, action respectant la linéarité.

La continuité de la représentation est simplement la continuité de ρ lorsque I_m est munie de la topologie profinie d'un groupe de Galois et lorsque V est muni de la topologie discrète. Si vous ne savez pas ce qu'est la topologie profinie d'un groupe de Galois, la continuité revient simplement à supposer que le noyau de ρ est d'indice finie dans I_m.

On va supposer pour l'instant que la représentation ρ est simple, c'est-à-dire qu'il n'existe pas de sous-espace vectoriel strict et non nul de V stable par tous les endomorphimes de l'image de ρ. On peut alors considérer l'ensemble des endomorphismes de ρ, souvent noté $\mathrm{End}(\rho)$. Il s'agit de l'ensemble des applications linéaires $\varphi : V \to V$ faisant commuter le diagramme suivant :



Il est remarquable de voir que muni de l'addition et de la composition des applications, l'ensemble $\mathrm{End}(\rho)$ hérite d'une structure de corps. Pour cela, il suffit de voir que toute application linéaire $\varphi \in \mathrm{End}(\rho)$, $\varphi \neq 0$, est une bijection. Mais si φ est non nulle, son noyau ne peut être V tout entier, mais il s'agit d'un espace stable pour tous les éléments de l'image de φ comme on peut le constater facilement, et donc comme on a supposé que ρ était simple, φ est injective. De même, en considérant l'image on montre que φ est surjective.

Une autre chose de remarquable est que l'ensemble $\mathrm{End}(\rho)$ est fini, puisque par exemple inclus dans $\mathrm{M}_r(\mathbb{F}_p)$, et donc il s'agit d'un corps fini. Celui-ci est donc en particulier commutatif. En outre, il est facile de voir que ce corps est de caractéristique p. Il est donc finalement isomorphe (non canoniquement) à $\mathbb{F}_q$ où $q = p^{r'}$ est une certaine puissance de p. Introduire $\mathbb{F}_q$ de cette façon n'est sans doute pas très adroit ; il est probablement mieux de fixer au préalable une clôture algébrique de $\mathbb{F}_p$, disons $\bar{\mathbb{F}_p}$, et de définir $\mathbb{F}_q$ par :

$$\mathbb{F}_q = \left\{ x \in \bar{\mathbb{F}_p} \mid x^q = x \right\}$$

Maintenant, V hérite d'une structure de $\mathrm{End}(\rho)$-espace vectoriel simplement en faisant naturellement agir les applications de $\mathrm{End}(\rho)$ sur les éléments de V. Mais tout $\mathrm{End}(\rho)$-sous-espace vectoriel de V va être directement

stable par tous les éléments de l'image de ρ. Comme on rappelle que l'on a supposé que ρ était simple, cela implique que V est en fait de dimension 1 sur End (ρ). En comptant les éléments maintenant, on obtient en outre $r = r'$.

Fixons maintenant un isomorphisme de corps $\varphi : \text{End}\,(\rho) \to \mathbb{F}_q$ où $q = p^r$. Une chose à remarquer alors est que l'image de ρ est consitité d'applications End (ρ)-linéaires et pas simplement $\mathbb{F}_p$-linéaires. D'autre part, comme V est de dimension 1 sur End (ρ), les applications End (ρ)-linéaires de V sont simplement les multiplications par des scalaires, et donc on peut dire :

$$\rho : I_m \to (\text{End}\,(\rho))^\star$$

ou encore si on utilise l'identification *via* φ :

$$\rho : I_m \to \mathbb{F}_q^\star$$

En outre, comme ρ est supposée continue, rappelons-le, la description de I_m nous dit que ρ va se factoriser en une application :

$$\rho : \text{Gal}\left(\mathbb{Q}_p^{\text{nr}}\left[\sqrt[n]{p}\right]/\mathbb{Q}_p^{\text{nr}}\right) \to \mathbb{F}_q^\star$$

où n est un entier non divisible par p, et on peut même choisir $n = q - 1$.

Mais le groupe de Galois $\text{Gal}\left(\mathbb{Q}_p^{\text{nr}}\left[\sqrt[q-1]{p}\right]/\mathbb{Q}_p^{\text{nr}}\right)$ s'identifie à l'ensemble des racines $(q-1)$-ième de l'unité dans $\bar{\mathbb{Q}}_p$, tout simplement en regardant par quoi est multiplié π, une racine $(q-1)$-ième de p ajoutée et fixée à l'avance. Et on peut montrer que l'ensemble de ces racines s'identifie également après réduction modulo p à l'ensemble $\left\{x \in \bar{\mathbb{F}_p} \;\middle|\; x^{q-1} = 1\right\}$ qui est précisément $\mathbb{F}_q^\star$.

Finalement ρ peut être vue comme un endomorphisme de groupes de $\mathbb{F}_q^\star$. Le groupe $\mathbb{F}_q^\star$ est cyclique de cardinal $q-1$, cet endomorphisme est donc simplement la multiplication d'un élément de $\mathbb{Z}/(q-1)\,\mathbb{Z}$. Mais ce nombre n'est pas canonique, il dépend de l'isomorphisme φ choisi au début. En fait, il n'est pas dur de voir que si l'on change φ en un φ', ce nombre va être multiplié par une puissance de p. L'idée consiste donc à écrire ce nombre en base p et à regarder la suite des chiffres écrits qui elle ne dépend pas de φ (plus précisément, seul l'endroit où l'on commence à lire la suite en dépend).

Récapitulons brièvement ce que l'on vient de faire. On vient d'associer à toute représentation continue simple de I_m dans un $\mathbb{F}_p$-espace vectoriel de dimension r, une suite de r entiers compris entre 0 et $p-1$. Cette association dépend en fait du choix d'un isomorphisme entre End (V) et $\mathbb{F}_q^\star$ mais une fois ce choix fait, on obtient presque une bijection, le seul écueil étant que les deux suites $(0,\ldots,0)$ et $(p-1,\ldots,p-1)$ correspondent toutes deux à la représentation triviale qui d'ailleurs n'est pas simple si $r \geqslant 2$. En outre, lorsque l'on modifie le choix de l'isomorphisme φ, la suite se modifie simplement par translation des termes ; en particulier les valeurs prises sont exactement les mêmes.

3.2 Un cas particulier

On considère ici une variété abélienne sur $\mathbb{Q}_p$. Nous n'allons pas définir précisément ce qu'est une *variété abélienne*, il est en gros nécessaire de savoir qu'il s'agit d'une variété, c'est-à-dire quelque chose défini localement comme le domaine d'annulation dans $\mathbb{Q}_p^n$ de polynômes à n variables à coefficients dans $\mathbb{Q}_p$. Le terme supplémentaire « abélienne » dit que l'on suppose quelques conditions de régularité sur la variété correspondant moralement à la connexité, à la compacité et à la lissité et que l'on met en outre sur cette variété une structure de groupe commutatif dont les lois de multiplication et de passage à l'inverse sont données par des formules polynômiales à coefficients dans $\mathbb{Q}_p$.

On suppose maintenant que cette variété abélienne à un modèle sur $\mathbb{Z}_p$, c'est-à-dire en fait que les polynômes qui servent à la définir ainsi que ceux servant à définir les lois peuvent être choisis à coefficients dans $\mathbb{Z}_p$. On suppose en outre des conditions de régularité sur le modèle, c'est-à-dire sur la variété définie sur $\mathbb{Z}_p$ par les polynômes précédents. Ces conditions de régularité sont encore moralement la compacité et la lissité.

On étend dans un premier temps les scalaires à $\bar{\mathbb{Q}}_p$, cela revient à dire que l'on regarde la variété définie sur $\bar{\mathbb{Q}}_p$ par les mêmes polynômes que précédemment. On regarde ensuite dans cette nouvelle variété les points de p-torsion, c'est-à-dire l'ensemble des points qui sont tués par p pour la structure de groupe donnée sur la variété. On peut montrer qu'il s'agit d'un groupe fini, dont bien évidemment tous les éléments sont tués par p, c'est-à-dire en fait d'un $\mathbb{F}_p$-espace vectoriel, disons V.

Sur cet espace vectoriel agit naturellement le groupe de Galois de $\bar{\mathbb{Q}_p}$ sur $\mathbb{Q}_p$, mais on a dit que celui-ci était trop compliqué et qu'on préférait se restreindre au groupe d'inertie modérée, il s'agit donc de récupérer une action du groupe d'inertie modérée.

Dans un premier temps, le groupe d'inertie est un sous-groupe du groupe de Galois absolu de $\mathbb{Q}_p$. On peut donc commencer par restreindre la réprésentation d'inertie. Maintenant, on aimerait pouvoir factoriser par le groupe d'inertie sauvage, mais pour cela il faudrait qu'il agisse trivialement ce qui n'est en général pas le cas.

Ce que l'on fait, c'est que l'on considère une suite de Jordan-Hölder de notre représentation. Le résultat est qu'il existe toujours une suite :

$$0 = V_0 \subset V_1 \subset \ldots \subset V_k = V$$

qui soit telle que tous les V_i sont stables par la représentation et que celle-ci déduite sur le quotient V_{i+1}/V_i est simple. On peut en même montrer que ces quotients sont uniquement déterminés à réordonnement près.

Cela permet donc de récupérer $\rho : I_m \to W$ une représentation en choisissant l'un des quotients précédents.

Un petit lemme prouve que cette nouvelle représentation, du fait de sa simplicité, est triviale sur le groupe d'inertie sauvage I_s. Démontrons-le. Le groupe I_s est un pro-p-groupe qui agit sur V. Si $x \in W$, l'orbite de x est naturellement en bijection avec un sous-groupe de I_s et donc est de cardinal une puissance de p. Ainsi si x n'est pas fixé par I_s, son orbite va être de cardinal un multiple de p et finalement l'ensemble des $x \in W$ fixés par I_s va aussi être de cardinal un multiple de p. Cet ensemble sera donc non trivial, mais il forme un sous-espace stable de V. Comme la représentation est supposée simple, il est égal à W, ce qui démontre la propriété.

On récupère ainsi une représentation encore simple $\rho : I_m \to W$ qui d'après le paragraphe précédent peut-être décrite pour une suite de r entiers compris entre 0 et $p-1$. Le résultat, dû à Raynaud dit que dans ce cas, tous les entiers qui apparaissent sont soit 0, soit 1.

3.3 L'énoncé général

L'énoncé précédent peut en fait se généraliser amplement. Nous allons juste donner l'énoncé et pas essayer d'expliquer rigoureusement tous les termes qui apparaissent parce que ce serait désespéremment trop long.

On commence donc par prendre K une extension finie de $\mathbb{Q}_p$. Si k est le corps résiduel de K, on a vu que K pouvait être vu comme une extension du corps $\operatorname{Frac} W(k)$. Le degré de cette extension est noté e et est appelé l'*indice de ramification absolu* de K. Par exemple, si $K = \mathbb{Q}_p$, ce nombre vaut 1.

On considère maintenant une variété X propre et lisse sur K et on suppose que X admet un modèle propre, à réduction semi-stable sur l'anneau des entiers $\mathcal{O}_K$. Il faut juste savoir ici que « propre » est moralement un équivalent de « compact », que « à réduction semi-stable » signifie que l'on autorise certains types de singularités mais relativement gentilles.

On remarquera que l'on ne prend pas, dans ce cas général, une structure de groupe sur la variété. Ce qui va remplacer les points de p-torsion va être le dual d'un groupe de cohomologie étale. Plus précisément pour tout entier i, on peut regarder le groupe :

$$H^{i\,\star}_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p\mathbb{Z})$$

où $\bar{K}$ est une clôture algébrique de K et donc $X_{\bar{K}}$ l'extension de X à $\bar{K}$. Si vous ne savez pas ce qu'est la cohomologie étale, il est sans doute bien de voir ça comme une boîte noire, comme une façon de construire un groupe qui décrit en gros la forme de la variété.

On fait ensuite la même chose que précédemment. Sur ce groupe de cohomologie, agit naturellement le groupe de Galois absolu de K. On restreint son action au groupe d'inertie (que l'on définit de la même façon que dans le cas de $\mathbb{Q}_p$), on considère un quotient de Jordan-Hölder, la représentation obtenu est alors simple et se factorise par le groupe d'inertie modérée. Il apparaît comme précédemment des nombres *a priori* compris entre 0 et $p-1$. La conjecture générale dit que ces nombres sont toujours inférieurs ou égaux à *ie*.

Références

[Ber77] P. Berthelot. Systèmes de honda des schémas en $\mathbb{F}_q$-vectoriels. *Bull. Soc. math. France*, 105 :225–239, 1977.

[Bre] C. Breuil. Cohomologie étale de p-torsion et cohomologie cristalline en réduction semi-stable. *Duke Mathematical Journal*, 95 :523–620.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Number 52 in GTM. Springer, 1977.

[Ray74] M. Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. math. France*, 102 :241–280, 1974.

[Ser68] Jean Pierre Serre. *Corps locaux*. Hermann, 1968.

[Ser72] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones math.*, 15 :259–331, 1972.