UNIVERSITÉ BORDEAUX 1

Leçons de mathématiques d'aujourd'hui

Jeudi 4 novembre 1999

Nombres p-adiques, représentations Galoisiennes, et leurs applications arithmétiques[1]

Jean-Marc FONTAINE

Université Paris-sud

[1]Rédigé par Niels BORNE.

Table des matières

Le sujet que je vais aborder n'est pas facile à présenter. Je pense que je ne vais pas vraiment pouvoir entrer dans la technique, et même je vais éviter de le faire, au risque de paraître un peu flou par moments. J'ai vu que dans l'assistance il y a quelques personnes qui connaissent déjà une bonne partie des choses que je vais raconter ; je leur demande de bien vouloir m'excuser, parce que si j'ai bien compris les règles, il faut que je fasse comme s'il étaient moins savants qu'ils ne le sont.

1 Nombres p-adiques

Je vais d'abord parler de nombres p-adiques. Ma façon préférée d'expliquer ce que sont ces nombres consiste à dire qu'*à l'école primaire, on apprend ce que sont les nombres* 10-*adiques*. (10 n'est pas un nombre premier, mais ce n'est pas grave.) Vous savez tous que ce qu'on apprend à l'école primaire, c'est à faire des additions et des multiplications de nombres entiers positifs, avec des retenues qui peuvent se propager de proche en proche :

$$\begin{array}{cccccccc} & 4 & 8 & 7 & 6 & 5 & 4 & 3 \\ + & 2 & 1 & 2 & 3 & 5 & 4 & 5 \\ \hline & 7 & 0 & 0 & 0 & 0 & 8 & 8 \end{array}$$

Et vous pouvez constater que si je n'arrête pas de mettre des chiffres :

$$\begin{array}{cccccccccc} & . & . & . & 4 & 8 & 7 & 6 & 5 & 4 & 3 \\ + & . & . & . & 2 & 1 & 2 & 3 & 5 & 4 & 5 \\ \hline & . & . & . & 7 & 0 & 0 & 0 & 0 & 8 & 8 \end{array}$$

il n'y a aucun obstacle à faire une addition. Bien sûr, ce ne sont plus des nombres entiers au sens habituel, mais c'est exactement en cela que consistent les *nombres entiers* 10-*adiques*. Vous pouvez faire la même chose avec la multiplication. Par exemple, dans :

$$\begin{array}{cccccccc} & . & 4 & 8 & 7 & 6 & 5 & 4 & 3 \\ \times & . & . & . & . & . & 5 & 4 & 5 \\ \hline \end{array}$$

vous commencez par multiplier par cinq :

$$\begin{array}{cccccccc} & . & 4 & 8 & 7 & 6 & 5 & 4 & 3 \\ \times & . & . & . & . & . & 5 & 4 & 5 \\ \hline & . & . & . & . & . & 7 & 1 & 5 \end{array}$$

puis vous multipliez par quatre, en décalant d'un cran :

$$\begin{array}{cccccccc} & . & 4 & 8 & 7 & 6 & 5 & 4 & 3 \\ \times & . & . & . & . & . & 5 & 4 & 5 \\ \hline & . & . & . & . & . & 7 & 1 & 5 \\ & . & . & . & . & . & 7 & 2 & \end{array}$$

puis par cinq, en décalant encore d'un cran :

$$\begin{array}{cccccccccc} & . & 4 & 8 & 7 & 6 & 5 & 4 & 3 \\ \times & . & . & . & . & . & 5 & 4 & 5 \\ \hline & . & . & . & . & . & 7 & 1 & 5 \\ & . & . & . & . & . & 7 & 2 & \\ & . & . & . & . & . & 5 & & \end{array}$$

Etc. Vous obtenez sous la barre une infinité de nombres, mais comme ils sont tous décalés d'un cran, sur chaque colonne il n'y a qu'un nombre fini de chiffres, et vous n'avez aucun mal à les additionner :

$$\begin{array}{cccccccccc} & . & 4 & 8 & 7 & 6 & 5 & 4 & 3 \\ \times & & & & & & 5 & 4 & 5 \\ \hline & . & . & . & . & & 7 & 1 & 5 \\ & . & . & . & . & . & 7 & 2 & \\ & . & . & . & . & . & 5 & & \\ \hline & . & . & . & . & . & 9 & 3 & 5 \end{array}$$

Et vous avez ainsi défini la multiplication. Voilà, c'est ça les nombres 10-adiques ! Et c'est *plus facile* que l'addition et la multiplication des nombres décimaux, parce que pour les nombres décimaux, il n'y a pas unicité de l'écriture. En particulier vous savez que

$$1,00\cdots$$

est la même chose que

$$0,999\cdots$$

Si vous voulez expliquer ce que sont l'addition et la multiplication des nombres décimaux, d'une part, vous devez tenir compte de cette ambiguïté, et d'autre part, vous êtes obligés de parler de séries convergentes et de choses de ce genre, parce qu'il peut arriver que vous ayez à changer tous les chiffres depuis le début en raison d'un phénomène qui se passe très loin ; tandis que pour les nombres 10-adiques, ce genre de problème ne se présente pas : c'est vraiment très simple.

Maintenant, ces objets "10-adiques" sont-ils bien des *nombres*? Qu'est-ce-qu'il y a derrière? Il y a une addition et une multiplication, qui définissent une structure d'anneau : c'est l'anneau $\mathbb{Z}_{10}$; ce n'est pas $\mathbb{Z}$ modulo $10\mathbb{Z}$, c'est vraiment le $\mathbb{Z}_{10}$ des spécialistes des nombres p-adiques, bien qu'on n'en parle jamais pour $p = 10$. C'est simplement, en termes savants, la limite projective :

$$\mathbb{Z}_{10} = \lim_{\leftarrow m\in\mathbb{N}} \mathbb{Z}/10^m\mathbb{Z}$$

pour m décrivant $\mathbb{N}$; $\mathbb{Z}$ est un anneau, $10^m\mathbb{Z}$ est l'idéal de $\mathbb{Z}$ engendré par 10^m, vous faites le quotient : vous avez un anneau. La limite projective $\lim_{\leftarrow m\in\mathbb{N}} \mathbb{Z}/10^m\mathbb{Z}$ est l'ensemble des suites :

$$\alpha = (\alpha_m)_{m\in\mathbb{N}}, \quad \alpha_m \in \mathbb{Z}/10^m\mathbb{Z},$$

ayant la propriété que α_{m+1} s'envoie sur α_m :

$$\alpha_{m+1} \to \alpha_m.$$

Une autre façon de le dire est qu'il y a une bijection entre ces suites et les nombres 10-adiques que j'ai décrits tout à l'heure : l'ensemble des entiers de 0 à $10^m - 1$ est en bijection avec $\mathbb{Z}/10^m\mathbb{Z}$:

$$@R = 0pt\{0, 1, 2, \cdots 10^m - 1\}[r]\mathbb{Z}/10^m\mathbb{Z}\, A_m[r]\alpha_m$$

parce que n'importe quel entier modulo $10^m\mathbb{Z}$ est la classe d'un élément de $\{0, 1, 2, \cdots 10^m - 1\}$ et d'un seul. Et donc vous pouvez représenter cet α comme une collection

$$\alpha = (A_m)_{m\in\mathbb{N}},$$

où les A_m sont des entiers compris entre 0 et $10^m - 1$ pour tout m. Vous voyez donc que la règle est la suivante :

$$A_{m+1} = A_m + 10^m a_m$$

où a_m est un chiffre (c'est-à-dire un entier compris entre 0 et 9). Se donner un élément de $\mathbb{Z}_{10}$ c'est se donner une suite infinie de chiffres :

$$a_0,\ a_1,\ a_2,\ a_3,\ \cdots$$

Voilà l'anneau des entiers 10-adiques.

Alors pourquoi est-ce qu'on ne parle jamais de nombres 10-adiques, et toujours de nombres p-adiques où p est un nombre premier? Bien sûr, on peut définir pour n'importe quel entier $N \geqslant 2$ la limite projective

$$\mathbb{Z}_N = \lim_{\leftarrow m\in\mathbb{N}} \mathbb{Z}/N^m\mathbb{Z}$$

(vous faites le même jeu en divisant les nombres par N). Mais le "théorème chinois" sur les restes vous dit par exemple que :

$$\frac{\mathbb{Z}}{10^m\mathbb{Z}} \simeq \frac{\mathbb{Z}}{2^m\mathbb{Z}} \times \frac{\mathbb{Z}}{5^m\mathbb{Z}}\ ;$$

ce qui fait que quand vous passez à la limite, vous obtenez :

$$\mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5\ .$$

Attention ce n'est pas $\mathbb{Z}$ modulo 2, c'est *l'anneau des entiers 2-adiques*. Plus généralement, vous obtenez :

$$\mathbb{Z}_N = \lim_{\leftarrow m\in\mathbb{N}} \frac{\mathbb{Z}}{N^m\mathbb{Z}} \simeq \prod_{p\ premier\ divisant\ N} \mathbb{Z}_p\ .$$

C'est la raison pour laquelle on se ramène toujours aux nombres p-adiques avec p premier. Pour tout nombre premier p, l'anneau $\mathbb{Z}_p$ est intègre ; son corps des fractions s'appelle $\mathbb{Q}_p$, c'est le "corps de nombres p-adiques", qu'on obtient simplement : il suffit d'inverser p :

$$\mathbb{Z}_p \subset \mathrm{Frac}\ \mathbb{Z}_p = \mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}].$$

C'est, disons, le point de vue des algébristes pour $\mathbb{Z}_p$. Mais il y a aussi un point de vue plus analytique, et j'aimerais, dans cet exposé, vous montrer qu'on joue de temps en temps avec l'un de ces deux points de vue, et de temps en temps avec l'autre. Le point de vue analytique consiste à regarder les différentes valeurs absolues qu'il y a sur le corps des nombres rationnels ; il y a la valeur absolue usuelle :

$$\alpha \in \mathbb{Q} \quad |\alpha|_\infty = \text{valeur absolue usuelle.}$$

C'est α si $\alpha \geqslant 0$, c'est $-\alpha$ sinon. Par ailleurs, à chaque fois que vous avez un nombre premier p, il y a la valeur absolue p-adique $|\alpha|_p$; pour la définir, il faut écrire α comme un quotient de deux entiers :

$$\alpha = p^r \frac{a}{b},$$

où a et b sont des entiers premiers à p, du moins si α n'est pas nul ; et alors on pose :

$$|\alpha|_p = p^{-r}.$$

Vous voyez, par exemple, que si α est entier, dire que α est très petit, c'est dire qu'il est divisible par une très grosse puissance de p. C'est vraiment une valeur absolue, et vous pouvez compléter le corps $\mathbb{Q}$ pour ces différentes valeurs absolues. Vous savez que pour $|\cdot|_\infty$ on obtient le corps $\mathbb{R}$ des nombres réels :

$$\alpha \in \mathbb{Q} \quad |\alpha|_\infty = \text{valeur absolue usuelle} \quad \to \mathbb{R}$$

et pour $|\cdot|_p$ on obtient le corps $\mathbb{Q}_p$:

$$\alpha = p^r \frac{a}{b} \qquad |\alpha|_p = p^{-r} \quad \to \mathbb{Q}_p,$$

le même que celui qu'on avait défini comme corps des fractions, et pour la raison que j'ai dite : c'est que, pour deux entiers par exemple, "être très voisins" signifie que la différence est divisible par une très grande puissance de p, et c'est exactement ce qu'on avait au début de l'exposé, sauf que p était remplacé par 10.

Le *théorème d'Ostrowski* dit qu'à équivalence près, les valeurs absolues non triviales sur $\mathbb{Q}$, sont, d'une part, la valeur absolue classique, archimédienne : $|\cdot|_\infty$; et d'autre part, les valeurs absolues p-adiques $|\cdot|_p$ (p premiers). Cela explique que, quand on veut travailler avec des objets qui sont définis sur le corps des nombres rationnels, par exemple des variétés algébriques, une chose à faire, dans un premier temps, est de remplacer $\mathbb{Q}$ par ses différentes complétions ; c'est-à-dire, soit par $\mathbb{R}$ (et on est conduit aux techniques d'analyse réelle) soit par une extension finie de $\mathbb{R}$, c'est-à-dire par $\mathbb{C}$ (ce qui conduit à l'analyse complexe), soit encore par $\mathbb{Q}_p$ (et on tombe sur des notions d'*analyse p-adique*).

Si vous regardez les écrits des arithméticiens, vous verrez qu'on y on parle tantôt de $\mathbb{Z}_p$, tantôt de $\mathbb{Z}_l$: l est un nombre premier, et vous allez voir tout à l'heure qu'il y a un jeu entre p et l. Le but de cet exposé est de vous faire voir que les choses les plus intéressantes, en un sens, se passent lorsque $l = p$; mais il n'en reste pas moins que, quand on écrit $\mathbb{Z}_l$, on pense souvent aux choses algébriques, et quand on écrit $\mathbb{Z}_p$ on pense souvent aux choses analytiques. Maintenant que je vous ai expliqué ce que sont les nombres p-adiques, la suite de l'exposé va être consacrée aux représentations galoisiennes.

2 Représentations galoisiennes

En général, quand on apprend la théorie de Galois pour la première fois, on se limite aux extensions finies. Ici, ça ne sera pas le cas, donc je suis obligé de faire un peu attention. Soit

F un corps de caractéristique 0.

Souvent, ce sera $\mathbb{Q}$, ou éventuellement, une de ses complétions $\mathbb{R}$ ou $\mathbb{Q}_p$, ou des extensions finies de ces corps. Je vais noter :

$$\overline{F} \text{ une clôture algébrique de } F.$$

J'en choisis une : tout le monde sait qu'il en existe, et qu'elles sont toutes isomorphes, bien qu'il n'y en ait pas de canonique (c'est pour ça que je viens de dire *une* et pas *la* clôture algébrique).

Soit :

$$G_F = \mathrm{Gal}(\overline{F}/F)$$

le groupe de Galois de l'extension $\overline{F}/F$: c'est le groupe des automorphismes du corps $\overline{F}$ qui laissent fixes tous les éléments de F. En général, ce n'est pas un groupe fini, mais il y a une topologie naturelle sur ce groupe, qu'il faut que j'explique. Notons

$$\mathcal{F} \text{ l'ensemble des extensions finies galoisiennes } L \text{ de } F \text{ contenues dans } \overline{F}.$$

Pour tout L dans $\mathcal{F}$, je peux *restreindre* le groupe de Galois :

$$G_F \to \mathrm{Gal}(L/F),$$

en associant à tout élément g de G_F sa restriction à L (qui est stable par g) : c'est bien un élément du groupe de Galois de L sur F. Donc j'ai une flèche $G_F \to \mathrm{Gal}(L/F)$ pour chaque L dans $\mathcal{F}$, et toutes ces flèches forment même un système projectif. En passant à la limite projective, on obtient un morphisme de groupes :

$$G_F \to \lim_{\leftarrow L \in \mathcal{F}} \mathrm{Gal}(L/F),$$

qui est en fait un isomorphisme. Concrètement, ça veut dire que connaître un élément du groupe de Galois, c'est la même chose que connaître sa restriction à toutes les extensions *finies* galoisiennes L de F contenues dans $\overline{F}$; et que, inversement, si vous vous donnez pour chaque L un élément du groupe fini $\mathrm{Gal}(L/F)$, avec des propriétés de compatibilité évidentes, vous définissez un élément de G_F.

Grâce à cela, il y a une topologie naturelle sur G_F, qui est la topologie de la limite projective (avec, bien sûr, la topologie discrète sur chaque groupe fini), et la seule chose dont j'ai besoin pour la suite, c'est de savoir ce que sont les sous-groupes invariants *ouverts*, par exemple. La réponse est qu'on a une *bijection* :

$$\text{Sous-groupes invariants ouverts} @ <- > [d] \mathrm{Gal}(\overline{F}/L) \mathcal{F} L [u]$$

En fait, G_F s'envoie surjectivement sur le groupe $\mathrm{Gal}(L/F)$, et le noyau est précisément le groupe $\mathrm{Gal}(\overline{F}/L)$:

$$1 \to \mathrm{Gal}(\overline{F}/L) \to G_F \to \mathrm{Gal}(L/F) \to 1.$$

Ce sont exactement les sous-groupes invariants ouverts. Vous voyez qu'en particulier, un sous-groupe invariant ouvert est un sous-groupe d'indice fini. (La réciproque est fausse, en général.) Les sous-groupes ouverts sont simplement les sous-groupes qui contiennent un sous-groupe invariant ouvert. Un sous-groupe est fermé s'il est l'intersection des sous-groupes ouverts qui le contiennent. Voilà tout ce qu'on a besoin de savoir sur cette topologie. Vous remarquez que, comme une limite projective de compacts est compacte, ce sont des groupes compacts (un

groupe fini est tout ce qu'il y a de plus compact pour la topologie discrète); ce sont des groupes topologiques assez exotiques pour les gens qui sont habitués à regarder les nombres réels ou les nombres complexes, mais du même type que la topologie p-adique, par exemple.

Maintenant, qu'est-ce qu'une représentation galoisienne? Dans ces histoires, il y a deux corps: il y a le corps de base, F, et puis il y a un corps de coefficients, E, que je vais supposer de caractéristique 0. Les représentations galoisiennes, pour moi, seront des représentations du groupe de Galois $G_F = \mathrm{Gal}(\overline{F}/F)$ à coefficients dans E. Autrement dit, je me donne

$$V = \text{ un espace vectoriel de dimension finie sur } E,$$

et je fais agir G_F linéairement sur cet espace. Plus précisément, je me donne un homomorphisme:

$$\rho \ : G_F \to \mathrm{Aut}_E(V).$$

Si je vous ai parlé de la topologie de G_F, c'est évidemment parce que je vais demander que cette application soit *continue*.
Pour que cela ait un sens, il faut qu'il y ait une topologie sur $\mathrm{Aut}_E(V)$. La première chose qui vient à l'esprit, c'est de mettre sur E la topologie discrète. Alors, l'image d'un groupe compact sera un groupe compact, donc (ici) un groupe fini: mais dans ce cas, ce n'était pas la peine de parler d'extensions galoisiennes infinies, parce qu'une représentation galoisienne de ce genre, avec la topologie discrète, peut se factoriser à travers $\mathrm{Gal}(L/F)$:

$$G_F[rr][dr]\mathrm{Aut}_E(V)\mathrm{Gal}(L/F)[ur]$$

pour une extension finie L convenable. C'est donc simplement une représentation linéaire du groupe fini $\mathrm{Gal}(L/F)$. Ce sont des choses sur lesquelles il y a beaucoup à dire, mais ce n'est pas ce dont j'ai envie de parler.
Maintenant, bien sûr, l'étape suivante consiste à travailler avec les différentes complétions de $\mathbb{Q}$, ou leurs extensions finies. E désignera toujours un tel corps par la suite. Par exemple, je peux travailler avec $\mathbb{R}$ ou $\mathbb{C}$ comme corps de coefficients:

$$E = \mathbb{R} \textit{ ou } \mathbb{C}.$$

Il y a une topologie naturelle sur les espaces vectoriels de dimension finie sur $\mathbb{R}$ ou $\mathbb{C}$, donc je peux demander un homomorphisme ρ *continu*. Mais la topologie de $\mathbb{R}$ ou de $\mathbb{C}$ est trop différente de la topologie des groupes profinis pour qu'il se passe quelque chose d'intéressant. De nouveau, si ρ est continue, son noyau est forcément un sous-groupe ouvert d'indice fini. On n'a que des représentations finies: plus précisément, elle se factorisent à travers le groupe de Galois d'une extension finie. Donc la théorie, jusque-là, n'est pas très intéressante.

En revanche, les choses deviennent intéressantes quand

$$E = \mathbb{Q}_l \text{ (ou une extension finie de } \mathbb{Q}_l).$$

C'est-à-dire les nombres l-adiques, l étant un nombre premier. Dans un espace vectoriel de dimension finie sur $\mathbb{Q}_l$, il y a une topologie naturelle, la topologie l-adique. Et du coup, vous pouvez regarder les homomorphismes *continus*, et là, au contraire de ce qui se passait avec $\mathbb{R}$ ou $\mathbb{C}$, il y a énormément de possibilités. On peut avoir des images de Galois qui sont énormes. Ce

sont forcément des sous-groupes compacts, bien sûr, parce que le groupe de Galois au départ est compact, mais par exemple, il y a quantités d'exemples de représentations de $G_{\mathbb{Q}}$:

$$\rho \ : G_{\mathbb{Q}}[r]\mathrm{GL}_h\mathbb{Q}_l$$

et il est facile de voir que si vous avez un tel homomorphisme continu, h étant un certain entier, alors, à conjugaison près, vous pouvez toujours vous ramener dans $\mathrm{GL}_h(\mathbb{Z}_l)$, le groupe des matrices carrés inversibles à coefficients dans $\mathbb{Z}_l$, ou le groupe des matrices à coefficients dans $\mathbb{Z}_l$ dont le déterminant est une unité l-adique, c'est-à-dire un élément inversible de cet anneau :

$$\rho \ : G_{\mathbb{Q}}[rr][dr]\mathrm{GL}_h\mathbb{Q}_l\mathrm{GL}_h\mathbb{Z}_l\text{surjectivité possible}$$

et cette fois-ci, vous pouvez vraiment fabriquer des exemples où le morphisme $G_{\mathbb{Q}} \to \mathrm{GL}_h\mathbb{Z}_l$ est surjectif. Vous voyez, cela produit des groupes qui ne sont pas du tout finis.

Maintenant la question qui se pose est : *comment fabrique-t-on des représentations galoisiennes intéressantes ?* Mais, avant de répondre à cette question, je voudrais dire la chose suivante. L'un des objets de l'arithmétique (pas le seul) est d'étudier le groupe de Galois $G_{\mathbb{Q}}$. Du point de vue de l'arithmétique, c'est un problème intéressant, sur lequel il y a des quantités de questions ouvertes, vous l'avez sans doute entendu dire. Et c'est un groupe qui est trop compliqué. Quand un problème est trop compliqué, on essaye toujours de le remplacer par un problème plus simple. On peut procéder de la façon suivante : vous partez de $\mathbb{Q}$, vous choisissez votre clôture algébrique $\overline{\mathbb{Q}}$, et maintenant à chaque fois que vous choisissez un nombre premier p, $\overline{\mathbb{Q}}$ se plonge dans le corps $\mathbb{Q}_p$ des nombres p-adiques. Je peux choisir une clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$, et je peux choisir un plongement de $\overline{\mathbb{Q}}$ dans $\overline{\mathbb{Q}_p}$:

$$\overline{\mathbb{Q}_p}@-[dd]\overline{\mathbb{Q}}@-[dd]@(- >[ur]\mathbb{Q}_p\mathbb{Q}@-[ur]$$

Il y a là un choix à faire, ce n'est pas du tout unique. Et à chaque fois que j'ai fait un tel choix, si j'appelle $G_{\mathbb{Q}_p}$ le groupe de Galois, $\overline{\mathbb{Q}_p}$ étant stable par $G_{\mathbb{Q}_p}$, la restriction à $\overline{\mathbb{Q}}$ d'un élément de $G_{\mathbb{Q}_p}$ me donne un élément de $G_{\mathbb{Q}}$, donc j'ai une flèche naturelle :

$$G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$$

qui en fait est injective, et qui identifie $G_{\mathbb{Q}_p}$ à un sous-groupe fermé de $G_{\mathbb{Q}}$. Ce qui fait qu'à chaque fois que vous avez une représentation l-adique de $G_{\mathbb{Q}}$, vous avez une représentation l-adique de $G_{\mathbb{Q}_p}$ pour tout nombre premier p. Et une des choses qu'on est tenté de faire (j'espère que j'aurai le temps d'en parler un peu à la fin de l'exposé), c'est, à chaque fois qu'on a une représentation l-adique de $G_{\mathbb{Q}}$, *d'utiliser le fait que c'est une représentation l-adique de $G_{\mathbb{Q}_p}$ pour chaque nombre premier p*, les groupes $G_{\mathbb{Q}_p}$ étant beaucoup mieux compris que $G_{\mathbb{Q}}$: en particulier ce sont des limites projectives de groupes finis résolubles.
Maintenant, il faut que j'essaye d'expliquer comment on fabrique des exemples de représentations galoisiennes intéressantes.

3 Exemples de représentations galoisiennes

En fait, avant d'aborder le sujet, j'ai envie de parler un peu d'un autre problème qui intéresse les arithméticiens et, si vous me permettez d'exagérer un petit peu, c'est le seul problème

qui intéresse les arithméticiens : il s'agit du problème des équations diophantiennes. Qu'est ce que c'est qu'un système d'équations diophantiennes ? Vous vous donnez un nombre fini de polynômes, à un nombre fini de variables et à coefficients dans $\mathbb{Z}$, par exemple,

$$P_1,\ P_2,\ \cdots\ P_r \in \mathbb{Z}[x_1, x_2, \cdots, x_s]$$

et vous vous intéressez à l'ensemble des solutions dans $\mathbb{Z}$ du système d'équations :

$$P_i(x_1, x_2, \cdots, x_s) = 0\ \ (1 \leqslant i \leqslant r).$$

C'était du moins ce qu'était l'arithmétique à l'époque de Diophante, si je comprends bien. Mais en termes savants, ça veut dire qu'on s'intéresse aux points rationnels sur $\mathbb{Z}$ d'un certain schéma affine, qui est défini par ces équations. Bien sûr, on peut, dans un premier temps au moins, se débarrasser d'un certain nombre de pathologies. Ce qui conduit en fait à regarder, disons, des variétés projectives lisses, régulières si vous voulez ; on est sur un corps de caractéristique zéro, à l'origine c'était $\mathbb{Q}$, mais on peut aller sur un autre corps E : quand on a une variété sur $\mathbb{Q}$, on peut la regarder sur $\mathbb{Q}_p$, etc. Donc, il est naturel de regarder ces variétés en elles-mêmes, si on s'intéresse au problème des équations diophantiennes.

Mais ce sont aussi ces variétés qui nous fournissent des exemples de représentations galoisiennes, et je pense que ce sont les exemples non triviaux les plus intéressants. Parce qu'à chaque fois que vous avez une telle variété X, vous pouvez regarder la variété sur $\overline{E}$ qui est déduite de X par extension des scalaires de E à $\overline{E}$: ainsi vous regardez les solutions des *mêmes* équations, mais au lieu de les regarder dans E, vous les regardez dans $\overline{E}$. Et maintenant vous avez une variété projective lisse sur un corps algébriquement clos de caractéristique 0, donc il est tout à fait raisonnable de regarder un objet, que je ne vais sûrement pas définir ici, qui est la *cohomologie étale l-adique* de cette variété :

$$H^m_{et}(X_{\overline{E}}, \mathbb{Q}_l).$$

De cette façon, pour chaque entier m, pour chaque nombre premier l, vous avez un espace vectoriel de dimension finie sur $\mathbb{Q}_l$ sur lequel le groupe de Galois opère de façon naturelle : c'est cela que l'on appelle une représentation l-adique de G_E ; c'est un $\mathbb{Q}_l$-espace vectoriel de dimension finie muni d'une action linéaire et continue de G_E. L'ennui de ce genre de choses, bien sûr, c'est qu'il est très long d'expliquer ce qu'est la cohomologie étale. En fait, ce n'est pas si long que cela, mais une fois qu'on l'a définie, on ne comprend d'abord pas comment on peut démontrer que c'est de dimension finie, et ensuite comment on peut calculer quoi que ce soit avec. Je voudrais quand même donner un exemple, qui est bien suffisant pour ce que je veux raconter aujourd'hui : c'est le cas particulier où X est une variété abélienne. Ça veut dire qu'on sait définir une multiplication sur X :

$$X \times X \to X$$

une loi de groupe, algébrique bien sûr. Vous pouvez mettre dans la définition, si ça vous fait plaisir, que c'est une loi de groupe commutatif ; en fait, c'est automatique, mais peu importe. Disons que c'est une variété abélienne de dimension g.

Pour regarder un exemple très concret, on va prendre le cas où $g = 1$. X est alors une courbe elliptique, et on peut toujours la voir comme une cubique plane non singulière : vous vous donnez un polynôme

$$p = a_0 + a_1 x + a_2 x^2 + x^3 \in E[x]$$

dont les trois racines dans $\overline{E}$ sont distinctes, et vous regardez la courbe d'équation :

$$y^2 = P(x).$$

Il faut ajouter un point à l'infini, de façon à avoir vraiment une variété projective (une courbe projective lisse) ; donc vous considérez les solutions de l'équation homogène :

$$Y^2Z = a_0Z^3 + a_1XZ^2 + a_2X^2Z + X^3.$$

Cela définit une courbe elliptique comme courbe projective dans le plan. Et il y a une loi de groupe sur cette courbe, définie de la manière suivante. Dessinons la courbe :

Il faut choisir un zéro. La règle du jeu est que la somme de trois points alignés est nulle. Si on veut savoir définir une addition, il faut donc choisir l'origine. Il est souvent commode de prendre l'origine à l'infini. Vous dessinez la droite joignant P à Q, elle coupe la courbe en un troisième point, et vous prenez le symétrique par rapport à l'axe des x : c'est le point $P + Q$. Cela définit une loi de groupe abélien.
Par exemple (et cet exemple va jouer un rôle par la suite), vous pouvez choisir un nombre p, un nombre premier si vous voulez (ce n'est pas essentiel), et supposez qu'il existe trois entiers a, b et c dans $\mathbb{N}$, premiers entre eux, tels que :

$$c^p = a^p + b^p.$$

Vous pouvez alors fabriquer une courbe elliptique, définie en coordonnées non homogènes par :

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

Et comme vous le savez, quand Wiles a démontré le dernier théorème de Fermat, ce qu'il a prouvé en fait, c'est que cette courbe elliptique ne peut pas exister pour $p \geqslant 3$. J'en dirai un mot à la fin.

Maintenant, il faut que j'explique, dans le cas des variétés abéliennes, ce qu'est la cohomologie étale. Parce que là, c'est quelque chose qui se comprend, qui existait avant qu'on ait

inventé la cohomologie étale : celle-ci a été inventée pour pouvoir démontrer les conjectures de Weil, en prenant justement comme intuition ce qui se passait dans le cas des courbes et des variétés abéliennes. Soit :

$$X \text{ une variété abélienne de dimension } g \text{ sur } E.$$

Si on a $g = 1$, c'est une courbe elliptique. Vous pouvez regarder les points de X à valeur dans $\overline{E}$. C'est un vrai groupe, au sens élémentaire du terme, un vrai groupe abélien. Je vais le noter additivement. Et si maintenant je me donne un nombre premier l, et un entier n supérieur ou égal à zéro, je peux regarder la multiplication par l^n :

$$0[r]X_{l^n}(\overline{E})[r]X(\overline{E})[r]^{l^n}X(\overline{E})[r]0$$

dont on peut démontrer qu'elle est surjective. On démontre aussi que le noyau est un groupe fini : ce sont les points d'ordre l^n de X à valeurs dans $\overline{E}$. Comme groupes abstraits, on a l'isomorphisme :

$$X_{l^n}(\overline{E}) \simeq (\mathbb{Z}/l^n\mathbb{Z})^{2g} \quad .$$

C'est un groupe abélien, dont tout élément est annulé par l^n ; on obtient donc une structure de module sur l'anneau $\mathbb{Z}/l^n\mathbb{Z}$, et c'est un module libre de rang $2g$. Avec cela, vous pouvez fabriquer ce qu'on appelle le module de Tate de X, il y en a un pour chaque nombre premier l :

$$T_l(X) = \lim_{\leftarrow n\in\mathbb{N}} X_{l^n}(\overline{E}).$$

Ça veut dire que se donner un élément u du module de Tate, c'est la même chose que se donner une collection $(u_n)_{n\in\mathbb{N}}$, où u_n est un point dont l'ordre divise l^n, autrement dit u_n est dans $X_{l^n}(\overline{E})$, et $lu_{n+1} = u_n$: c'est exactement *cela*, un élément du module de Tate. Le fait que $X_{l^n}(\overline{E})$ ait cette structure entraîne que $T_l(X) \simeq \mathbb{Z}_l^{2g}$: c'est une structure de $\mathbb{Z}_l$-module libre de rang $2g$. Comme j'ai dit que je parlais de représentations l-adiques vectorielles sur $\mathbb{Q}_l$, je peux regarder ce que je vais appeler $V_l(X)$, qui est ce qu'on obtient en étendant les scalaires de $\mathbb{Z}_l$ à $\mathbb{Q}_l$:

$$V_l(X) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(X).$$

Il s'agit de rendre l inversible, et c'est tout ce qu'il faut faire. $V_l(X)$ est un $\mathbb{Q}_l$-espace vectoriel de dimension $2g$. C'est en un sens le plus simple des exemples non triviaux de représentations l-adiques. Vous voyez que le groupe de Galois opère de façon évidente sur $X(\overline{E})$, parce qu'il opère sur $\overline{E}$, et X est défini par des équations qui sont dans E. Donc, quand on applique un élément du groupe de Galois à une solution des équations, on obtient une autre solution. Bien sûr, c'est compatible avec la structure de groupe. On a une action sur $X_{l^n}(\overline{E})$, et par passage à la limite une action sur $T_l(X)$, et aussi sur $V_l(X)$, en rendant l inversible. Ce qui fait que $V_l(X)$ est vraiment une représentation l-adique de G_E.
Et maintenant, si vous voulez savoir ce qu'est la cohomologie étale de la variété abélienne, je peux vous donner la réponse. Mais encore une fois, parce qu'on s'intéresse aux variétés abéliennes, ce n'est justement pas la peine de définir la cohomologie étale. $H^m_{et}(X_{\overline{E}}, \mathbb{Q}_l)$ est simplement le $\mathbb{Q}_l$-espace vectoriel des formes m-linéaires alternées sur $V_l(X)$:

$$H^m_{et}(X_{\overline{E}}, \mathbb{Q}_l) = \wedge^m_{\mathbb{Q}_l} V_l(X)^*,$$

i.e. c'est la puissance extérieure m-ième du dual. En particulier, c'est non nul si et seulement si m est compris entre 0 et $2g$. Bien sûr, il y a une action de Galois par fonctorialité sur ces espaces. Le module de Tate donne tous les renseignements qu'on veut sur ces représentations.

Il faut quand même que je donne un dernier petit exemple de représentation l-adique. Ce que j'ai fait avec une variété abélienne, on peut aussi le faire avec le groupe multiplicatif. Bien sûr le groupe multiplicatif n'est pas une variété projective, mais ça n'a pas d'importance, on peut quand même refaire la même chose : je peux regarder :

$$\mathbb{G}_m(\overline{E}) = \overline{E}^*,$$

muni de la loi de composition qu'est la multiplication ; le noyau de la multiplication par l^n est exactement ce qu'on appelle le groupe des racines l^n-ièmes de l'unité :

$$\mu_{l^n}(\overline{E}) = \{x \in \overline{E} \mid x^{l^n} = 1\}.$$

C'est cyclique d'ordre l^n, ce qui veut dire que c'est un $\mathbb{Z}/l^n\mathbb{Z}$-module libre de rang 1. Et je peux regarder de nouveau :

$$\lim_{\leftarrow n \in \mathbb{N}} \mu_{l^n}(\overline{E}) = T_l(\mathbb{G}_m).$$

C'est cela qu'on appelle module de Tate du groupe multiplicatif, et qu'on note en général $\mathbb{Z}_l(1)$. Et si je veux, je peux regarder $V_l(\mathbb{G}_m)$; je rends l inversible pour avoir un $\mathbb{Q}_l$-espace vectoriel de dimension 1, que je peux noter $\mathbb{Q}_l(1)$. Si t est un élément non nul de $V_l(\mathbb{G}_m)$, par exemple un générateur de $\mathbb{Z}_l(1)$, il y a une action naturelle de Galois dessus, donnée par :

$$g(t) = \chi_l(g)t,$$

où χ_l est un certain caractère, c'est-à-dire un homomorphisme continu de G_E à valeurs dans $\mathbb{Z}_l^*$, qu'on appelle le caractère cyclotomique. Maintenant, si vous vous donnez un entier i supérieur ou égal à zéro, vous pouvez définir :

$$\mathbb{Q}_l(i) = \mathrm{Sym}^i_{\mathbb{Q}_l}\mathbb{Q}_l(1),$$

et puis

$$\mathbb{Q}_l(-i) = \mathbb{Q}_l(i)^*.$$

Vous voyez maintenant que, pour tout i dans $\mathbb{Z}$, on sait définir $\mathbb{Q}_l(i)$: c'est un $\mathbb{Q}_l$-espace vectoriel de dimension 1, engendré par t^i, et sur lequel il y a une action de Galois. Cette action est à travers la puissance i-ème du caractère cyclotomique. Il faut savoir que cet élément t joue dans le monde l-adique l'analogue du rôle que joue $2i\pi$ dans le monde complexe.

Voilà, j'ai donné des exemples de représentations galoisiennes. Il serait complètement faux de dire que toutes les représentations galoisiennes l-adiques proviennent de la cohomologie étale des variétés algébriques ; mais on a beaucoup de mal à les fabriquer autrement, sauf en déformant des représentations provenant de la cohomologie étale l-adique : on peut alors obtenir des représentations qui n'en proviennent plus ; mais ça, je ne vais pas en parler.
Je voudrais faire une petite parenthèse (donc je vais être très vague) : je vais parler de *cohomologie de de Rham* et de *structures de Hodge*.

4 Cohomologie de de Rham et structures de Hodge

Je dois parler de ces deux notions, parce qu'on va vouloir en faire par la suite l'analogue p-adique. Comme je n'aurai pas le temps de donner des définitions explicites dans l'univers

p-adique, je ne vais pas passer un quart d'heure à rappeler les définitions précises dans l'univers réel ou complexe. Je voudrais quand même dire deux mots de ce qui se passe. À chaque fois qu'on a :

$$X \text{ une variété projective lisse sur } E,$$

E étant un corps de caractéristique zéro, on peut définir la cohomologie de de Rham de X, c'est-à-dire, pour tout $m \in \mathbb{N}$:

$$H^m_{dR}(X).$$

C'est un objet purement algébrique, bien que, dans le cas des variétés réelles ou complexes, on ait des définitions analytiques, beaucoup plus simples en un sens. La définition algébrique est une définition plus savante, on parle de l'hypercohomologie du complexe de de Rham, le complexe des formes différentielles, qui est un complexe de faisceaux pour la topologie de Zariski. Je ne vais sûrement pas vous en rappeler la définition, mais c'est un objet purement algébrique sur lequel il y a une filtration, la *filtration de Hodge*, qui est une filtration décroissante par des sous-E-espaces vectoriels :

$$\mathrm{Fil}^i\ H^m_{dR}(X) \supset \mathrm{Fil}^{i+1}\ H^m_{dR}(X).$$

Tout ce que je peux dire, puisque je ne dis pas les choses complètement ici, c'est que :

$$\begin{cases} \mathrm{Fil}^0\ H^m_{dR}(X) & = & H^m_{dR}(X), \\ \mathrm{Fil}^{m+1}\ H^m_{dR}(X) & = & 0, \\ \mathrm{Fil}^i\ H^m_{dR}(X)/\mathrm{Fil}^{i+1}\ H^m_{dR}(X) & = & H^{m-i}(X, \Omega^i_X). \end{cases}$$

Ω^i_X est un faisceau de Zariski, le faisceau des formes différentielles de degré i, et $H^{m-i}(X, \Omega^i_X)$ est le $(m-i)$-ième groupe de cohomologie des faisceaux de Zariski. Je vais considérer cette filtration comme une boîte noire, on n'a pas besoin d'aller regarder à l'intérieur.

Prenez une variété projective lisse X, définie sur E, et donnez-vous un plongement de E dans le corps des complexes :

$$E \subset \mathbb{C} ;$$

(par exemple E peut être déjà le corps des complexes, ou le corps des rationnels) ; vous pouvez regarder la variété $X_{\mathbb{C}}$ qui est déduite de X par extension des scalaires de E à $\mathbb{C}$; c'est une variété projective lisse sur $\mathbb{C}$. On a bien sûr quantité de techniques pour étudier cette variété et pour définir la cohomologie autrement. Je vais juste en donner une, rapidement : par exemple on peut voir $X_{\mathbb{C}}$ comme une variété différentiable réelle de dimension $2 \dim X$. La cohomologie de de Rham de $X_{\mathbb{C}}$ est simplement :

$$H^m_{dR}(X_{\mathbb{C}}) = \mathbb{C} \otimes_E H^m_{dR}(X);$$

mais je peux aussi la définir de façon plus naïve comme étant l'ensemble des formes différentielles $\mathcal{C}^\infty$ fermées de degré m, modulo les différentielles exactes. J'ai aussi un complexe de chaînes $\mathcal{C}^\infty$ qui me permet de définir l'homologie simpliciale :

$$H_m(X_{\mathbb{C}}, \mathbb{Z}).$$

Ce sont des groupes, des $\mathbb{Z}$-modules de type fini. Et comme vous le savez, on peut intégrer ces formes différentielles fermées, et grâce à la formule de Stokes, ça passe à la cohomologie, donc on a une application :

$$@R = 0pt H^m_{dR}(X_{\mathbb{C}}) \times H_m(X_{\mathbb{C}}, \mathbb{Z})[r]\mathbb{C}(\tilde{\omega}, \gamma)[r] \int_\gamma \omega$$

C'est simplement l'intégration. Et c'est une application qui est non dégénérée, en un sens évident. Je peux regarder ce que je vais appeler le m-ième groupe de cohomologie de Betti : je prends le dual de $H_m(X_{\mathbb{C}}, \mathbb{Z})$ et j'étends les scalaires à $\mathbb{Q}$. La façon la plus simple de donner la définition, c'est de dire ce que sont les homomorphismes de groupes de $H_m(X_{\mathbb{C}}, \mathbb{Z})$ à valeurs dans $\mathbb{Q}$:

$$H_B^m(X_{\mathbb{C}}) = \mathcal{L}_{\mathbb{Z}}(H_m(X_{\mathbb{C}}, \mathbb{Z}), \mathbb{Q}).$$

Dit de cette façon, ça peut paraître un peu compliqué, mais pourquoi pas ? Alors, ce que me dit le fait que l'intégration est non degénérée, c'est que $H_B^m(X_{\mathbb{C}})$ est en fait un $\mathbb{Q}$-espace vectoriel, de même dimension que le $\mathbb{C}$-espace vectoriel $H_{dR}^m(X_{\mathbb{C}})$; et quand on étend les scalaires, on obtient un *isomorphisme de comparaison complexe* :

$$\mathbb{C} \otimes_E H_{dR}^m(X) \simeq \mathbb{C} \otimes_{\mathbb{Q}} H_B^m(X_{\mathbb{C}}).$$

Il y a aussi des structures supplémentaires, comme vous le savez, sur la cohomologie de de Rham, et l'isomorphisme de comparaison permet de munir la cohomologie de Betti d'une structure de Hodge pure de poids m. Maintenant, passons à l'analogue p-adique.

5 Structures de Hodge p-adiques

Pourquoi chercher un analogue p-adique? D'abord parce que c'est une maladie des matheux de vouloir faire des analogues, mais ce n'est pas une assez bonne raison. Il y en a une meilleure : c'est le fait que ces structures de Hodge sont vraiment utiles à tout un tas de choses. S'il y a un analogue p-adique, il devrait être utile ; et, de fait, c'est vrai : il y a des applications.
Qu'est-ce-que c'est qu'une structure de Hodge p-adique? D'abord il y a quelque chose qui *n'a pas* d'analogue p-adique : c'est la cohomologie de Betti. Il y a des gens à Bordeaux qui savent que ce que je dis n'est pas complètement vrai : il y a des analogues, mais ces analogues ne sont pas de bonnes théories de cohomologie. Ce qui veut dire qu'on ne sait pas définir une chose comme $H_B^m(X_{\mathbb{C}})$, qui est un $\mathbb{Q}$-espace vectoriel de dimension finie, quand on a une variété algébrique projective lisse sur $\mathbb{Q}_p$ ou sur une extension de $\mathbb{Q}_p$, quelle qu'elle soit.
En revanche, ce qu'il faut savoir, c'est que dans la situation complexe, il y a quelque chose que j'ai le droit de faire : on a $H_B^m(X_{\mathbb{C}})$, qui est un $\mathbb{Q}$-espace vectoriel ; pour chaque nombre premier l, on a la cohomologie étale l-adique de $X_{\mathbb{C}}$ à coefficients dans $\mathbb{Q}_l$: $\mathbb{C}$ est un corps parfaitement honnête, algébriquement clos de caractéristique zéro, donc je peux regarder $H_{et}^m(X_{\mathbb{C}}, \mathbb{Q}_l)$; bien sûr, il n'y a pas une grosse action de Galois là-dessus, mais ça ne fait rien, et quand on étend les scalaires de $\mathbb{Q}$ à $\mathbb{Q}_l$, on a un isomorphisme canonique :

$$H_B^m(X_{\mathbb{C}}) \otimes_{\mathbb{Q}} \mathbb{Q}_l \simeq H_{et}^m(X_{\mathbb{C}}, \mathbb{Q}_l).$$

Résumons : la cohomologie de Betti est un objet complètement transcendant, qui utilise des techniques d'analyse réelle ou complexe, et on ne sait pas faire autrement. J'exagère un peu, il y a la topologie, mais on n'a pas d'analogue p-adique. Cependant, dès qu'on tensorise par $\mathbb{Q}_l$, on a un analogue l-adique, quel que soit l, qu'il soit égal à p ou différent : c'est la cohomologie étale.

Donc maintenant, on va se donner :

$$K = \text{ une extension finie de } \mathbb{Q}_p,$$

$$X_K = \text{ une variété projective lisse sur } K.$$

Par exemple, vous partez d'une variété projective lisse sur $\mathbb{Q}$ et vous étendez les scalaires à K.

Il y a plusieurs théories de cohomologie ; d'abord celle de de Rham, pour chaque entier m :

$$H^m_{dR}(X_K) = \text{ un } K\text{-espace vectoriel de dimension finie, muni de la filtration de Hodge ;}$$

et puis, pour chaque nombre premier l, il y a la cohomologie étale l-adique. Il faut pour cela étendre les scalaires de K à une clôture algébrique $\overline{K}$ de K :

$$H^m_{et}(X_{\overline{K}}, \mathbb{Q}_l) = \text{ un } Q_l\text{-espace vectoriel de dimension finie, } \textit{plus} \text{ une action de } G_K.$$

C'est une représentation l-adique.

Une chose qui est frappante, c'est que quand $l = p$, on a l'impression d'avoir deux théories cohomologiques p-adiques : il y a la *cohomologie de de Rham*, qui est un espace vectoriel de dimension finie sur K, lequel est une extension finie de $\mathbb{Q}_p$, et la *cohomologie étale p-adique*, qui nous donne un espace vectoriel de dimension finie sur $\mathbb{Q}_p$, avec action de G_K. Il est donc naturel de se dire que l'analogue p-adique de l'isomorphisme de comparaison doit être quelque chose du même genre, et on aurait envie d'écrire :

$$? \otimes_K H^m_{dR}(X_K) \simeq ? \otimes_{\mathbb{Q}_p} H^m_{et}(X_{\overline{K}}, \mathbb{Q}_p).$$

Qu'est-ce-que doit être ce "?" ? Ça a été un problème pendant très longtemps. On aurait envie que ça soit un corps contenant K, pour que $? \otimes_K H^m_{dR}(X_K)$ ait un sens, déjà. On voudrait un isomorphisme canonique et fonctoriel, mais on voudrait aussi tenir compte des structures qu'il y a sur $H^m_{et}(X_{\overline{K}}, \mathbb{Q}_p)$, sur lequel il y a une action de Galois. Donc on aurait envie que "?" soit muni d'une action de G_K, et on voudrait que cet isomorphisme soit compatible avec l'action de Galois.
Bien sûr, il y a un objet qui a l'air d'avoir été fait pour ça, sur lequel Galois opère topologiquement : c'est $\overline{K}$. Est-ce-qu'on pourrait prendre :

$$? = \overline{K} \quad ?$$

Mais il est très facile de voir que ça ne marche pas. C'est impossible : il ne peut pas y avoir un tel isomorphisme qui soit compatible avec l'action de Galois.
On s'est posé la question au début des années soixante (c'était une correspondance entre Grothendieck et Tate). On se dit, bien sûr, que ce n'est pas $\overline{K}$ qu'il faut prendre, mais son complété pour la topologie p-adique :

$$? = \widehat{\overline{K}},$$

que les gens ont tendance à appeler $\mathbb{C}_p$, en pensant que c'est l'analogue p-adique de $\mathbb{C}$.
C'est un peu le point de départ de la théorie. Tate a introduit ce qu'on appelle les constructions de Hodge-Tate, et le point de vue qui s'est revélé utile est de définir un certain corps, le bon analogue p-adique de $\mathbb{C}$:

$$B_{dR} = \text{le corps des périodes } p\text{-adiques.}$$

Il s'appelle corps des périodes p-adiques parce que, précisement, c'est là que vivent les périodes. Je ne vais pas vous donner la définition de B_{dR}, c'est en ce sens que je ne vais pas être précis. Je pourrais le faire, ça prendrait peut-être cinq ou dix minutes, mais ce n'est pas très instructif

en soi. Ce qu'il faut savoir, c'est que B_{dR} est le corps de fractions d'un certain anneau, qu'on appelle B_{dR}^+, et que B_{dR}^+ contient $\overline{K}$ de façon canonique. Il y a une action naturelle de G_K dessus. B_{dR}^+ est muni d'une topologie un peu compliquée à décrire, et $\overline{K}$ est dense dedans, ce qui fait qu'en un sens, le bon anneau à regarder, c'est quand même le complété de $\overline{K}$, mais pour une topologie beaucoup plus difficile à définir que la topologie p-adique. Ce qu'il faut savoir, aussi, c'est que B_{dR}^+ contient également l'élément que j'ai appelé t tout à l'heure, c'est-à-dire les éléments de $\mathbb{Z}_p(1)$, et que :

$$\frac{B_{dR}^+}{tB_{dR}^+} \simeq \mathbb{C}_p.$$

Par ailleurs, B_{dR}^+ est séparé et complet pour la topologie t-adique, et t n'est pas un élément nilpotent, ce qui fait que d'un point de vue abstrait, B_{dR} est isomorphe à un corps de séries formelles à une variable à coefficients dans $\mathbb{C}_p$:

$$B_{dR} \simeq \mathbb{C}_p((t)).$$

Mais ce n'est pas du tout un bon point de vue, parce que ce n'est pas un isomorphisme canonique ; il n'y a pas de plongement canonique de $\mathbb{C}_p$ dans B_{dR}^+, il n'y en a même pas qui commute avec l'action de Galois. En revanche, B_{dR}^+ est bien un anneau de valuation discrète complet, de corps résiduel $\mathbb{C}_p$, et t est une *uniformisante*.
On a alors le théorème de comparaison suivant :

Théorème 1. *Il y a un isomorphisme canonique, naturel, qui commute à l'action de Galois :*

$$B_{dR} \otimes_K H_{dR}^m(X_K) \simeq B_{dR} \otimes_{\mathbb{Q}_p} H_{et}^m(X_{\overline{K}}, \mathbb{Q}_p).$$

Ce théorème a une longue histoire, il y a tout un tas de techniques qui ont été mises sur pied pour le démontrer. Il y a eu d'abord des résultats partiels, dus à beaucoup de gens différents. Le résultat final, avec les techniques que je viens d'évoquer, a été obtenu par Takeshi Tsuji : c'est lui qui a vraiment *démontré* le théorème. Son article [Tsu] est paru dans les *Inventiones* ; je pense que c'est le record : je n'ai jamais vu d'article aussi long qui soit paru dans cette revue. C'est l'aboutissement de tout un travail ; ça vous donne une idée de la complexité, de la technicité des démonstrations. En un sens, techniquement, toutes les idées étaient déjà là pour démontrer ce théorème ; il fallait avoir du souffle. Cela dit, c'est une démonstration que tout le monde comprend, du moins tous les experts du sujet. Il existe des démonstrations plus récentes et indépendantes, dont une, due à Faltings, utilise une méthode complètement différente, la théorie des extensions *presque étales* ; il y a un spécialiste dans la salle, je ne suis pas sûr qu'il ait tout compris ; à ma connaissance personne n'a tout compris à la démonstration. Faltings en est tout à fait conscient, c'est un véritable problème. Il y aussi une ancienne élève de Faltings, Wieslawa Niziol, qui a fait une démonstration très différente de celle de Faltings, en utilisant la K-théorie et des travaux de Thomasson, mais que personne à ma connaissance n'a comprise non plus, parce qu'il se trouve que la théorie de Thomasson n'est pas une chose très facile à comprendre, et qu'il n'y a pas vraiment de gens qui soient experts de tous les ingrédients de la démonstration. C'est pour vous dire que le sujet est compliqué, mais qu'il bouge.

En fait, Tsuji démontre un peu plus que le théorème ci-dessus. Si vous vous donnez :

$$V = \text{ une représentation } p\text{-adique de } G_K,$$

vous pouvez toujours définir quelque chose, que je vais appeler :

$$D_{dR}(V) = (B_{dR} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Vous étendez les scalaires de $\mathbb{Q}_p$ à B_{dR}, et vous prenez la partie fixe par G_K. Alors comme :

$$B_{dR}^{G_K} = K,$$

$D_{dR}(V)$ est un K-espace vectoriel, et on peut démontrer que :

$$\dim_K D_{dR}(V) \leqslant \dim_{\mathbb{Q}_p} V \ ;$$

on dit que V est de *de Rham* lorsqu'on a l'égalité. Il se trouve que, comme je l'ai dit, B_{dR} est le corps des fractions d'un anneau de valuation discrète. Ceci permet de définir une filtration décroissante naturelle sur $D_{dR}(V)$:

$$\mathrm{Fil}^i D_{dR}(V) = (B_{dR}^+ t^i \otimes_{\mathbb{Q}_p} V)^{G_K} \quad (i \in \mathbb{Z}),$$

et on a une autre façon complètement équivalente d'écrire le théorème, compatible non seulement avec l'action de Galois, mais aussi avec cette autre structure qu'est la filtration de Hodge : à savoir que $V := H^m_{et}(X_{\overline{K}}, \mathbb{Q}_p)$ *est une représentation de de Rham* (bien sûr, vous voyez pourquoi on appelle ce genre de représentations des représentations de de Rham) *et que* $D_{dR}(V) \simeq H^m_{dR}(X)$ *en tant que* K*-espaces vectoriels filtrés.*
Pour les structures de Hodge réelles ou complexes, il y avait plus que ce que j'avais dit, et ici aussi il y a plus que ce que je vous ai dit : à l'intérieur de cette théorie des représentations de de Rham, il y a une notion plus restrictive, qui est la théorie des représentations p-adiques *semi-stables*. Les représentations p-adiques semi-stables sont certaines représentations de de Rham, mais pas toutes. Il y a aussi une notion de représentations p-adiques *potentiellement semi-stables*, et on conjecture que ce sont exactement les représentations de de Rham. Mais en tout cas elles sont de de Rham, et le théorème de Tsuji est plus fort : il démontre que la cohomologie étale p-adique est une représentation potentiellement semi-stable, ce qui fait qu'il y a des structures supplémentaires sur la cohomologie de de Rham, et c'est cela qu'on a envie d'appeler les *structures de Hodge p-adiques*. Ces structures supplémentaires déterminent complètement la représentation. Il y a une équivalence de catégories entre les représentations p-adiques potentiellement semi-stables et certains objets élémentaires, purement algébriques, que je pourrais définir au tableau en cinq minutes. Ces objets sont complètement explicites, tandis qu'une vraie représentation de Galois n'est jamais explicite, parce que le groupe de Galois est une chose compliquée. Mais je ne vais pas en dire davantage ici, et je vais passer à l'avant-dernier paragraphe que je veux évoquer : la notion de représentation l-adique géométrique. Je vais avoir le temps de parler de deux applications.

6 Représentations l-adiques géométriques

Je vais me restreindre au cas de $\mathbb{Q}$, c'est beaucoup plus simple. Prenons le groupe de Galois :

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),$$

où $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$. Soient de plus l un nombre premier, et V une représentation l-adique de $G_{\mathbb{Q}}$. Je pense qu'arrivé à ce point de l'exposé, ce n'est plus la peine de faire semblant

d'avoir défini tous les termes que je vais employer. Vous voyez que, pour chaque nombre premier p, cette représentation l-adique de $G_{\mathbb{Q}}$ fournit une représentation l-adique de $G_{\mathbb{Q}_p}$. Donc je vais dire :

Définition. *V est géométrique si*

1. *pour presque tout p, V est non ramifiée comme représentation $G_{\mathbb{Q}_p}$.*
2. *pour $p = l$, V est potentiellement semi-stable.*

Que signifie la première condition? Dans un corps p-adique il y a un corps résiduel (en l'occurence c'est $\mathbb{F}_p$) ; on demande que l'action de Galois se factorise à travers le groupe de Galois de la clôture algébrique du corps résiduel : c'est la première condition. Et la deuxième condition est une condition locale en $l = p$. On pourrait mettre "de de Rham" au lieu de "potentiellement semi-stable", conjecturalement c'est la même chose, mais autant mettre une définition un peu plus restrictive : ça donne un peu plus de chances d'arriver à démontrer des choses.
Maintenant, il y a un théorème qui dit que toute représentation qui provient de la géométrie algébrique est géométrique. Et une conjecture dont je vais dire quelque chose tout à l'heure, dit que la réciproque est vraie.

Théorème 2. *Pour tout entier m, $H^m_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)$ est une représentation géométrique.*

En fait le théorème dit plus que cela. Pour $p = l$, c'est exactement le résultat de Tsuji. Pour $p \neq l$, c'est un résultat extrêmement classique. Pour en parler, il faut évoquer une notion de *bonne réduction* pour les représentations l-adiques de $G_{\mathbb{Q}_p}$: dire que la représentation a bonne réduction signifie, si $p \neq l$, que la représentation est non ramifiée ; si $p = l$, c'est une condition technique savante qui dit que V est *cristalline*. Pour une variété projective lisse, il y a toujours bonne réduction, mais je ne vais pas l'expliquer (c'est une chose naturelle, on peut trouver un modèle entier lisse). Ce qu'on démontre, et c'est tout à fait classique, c'est qu'une variété X a bonne réduction pour presque tous les nombres premiers p, et quand $p \neq l$, dès que la variété a bonne réduction, la représentation aussi. C'est aussi vrai pour $p = l$.
Vous voyez qu'on démontre plus que le fait que la représentation est géométrique : partout où la variété a bonne réduction, c'est aussi le cas de la représentation. Il y a en plus une notion de "semi-stabilité", et partout où la variété est semi-stable, la représentation l'est aussi. Il y a autre chose qu'on peut associer à une représentation géométrique : si V est une représentation géométrique, il y a un

$$D_{dR}(V) = (B_{dR} \otimes_{\mathbb{Q}_l} V)^{G_{\mathbb{Q}_l}}.$$

C'est le cas $l = p$. $D_{dR}(V)$ est un espace vectoriel sur $\mathbb{Q}_l$, muni d'une filtration. Et les poids de Hodge-Tate de V sont les entiers i tels que

$$\mathrm{Fil}^{-i} D_{dR}(V)/\mathrm{Fil}^{-i+1} D_{dR}(V) \neq 0.$$

Le signe n'est là que pour des raisons historiques. Voici la première conjecture dont je voudrais parler :

Conjecture 1. *Soit m un entier inférieur ou égal à 10, l un nombre premier, et V une représentation l-adique géométrique avec bonne réduction partout, de poids de Hodge-Tate compris entre $-m$ et 0. Alors :*

$$V \text{ semi-simple} \implies \text{il existe des entiers naturels } n_{-m}, \ldots, n_0 \text{ tels que } V \simeq \oplus_{i=0}^{-m} \mathbb{Q}_l(i)^{n_i}.$$

Ce qui veut dire que les seules représentations qu'on obtient de cette façon sont les représentations bêtes dont je vous ai parlé au début. Je n'ai pas le temps d'expliquer pourquoi cette conjecture est justifiée (quoique très loin d'être démontrée), mais il y a des résultats partiels :

1. C'est vrai pour $m = 1$ si $l \in \{2, 3, 5, 7, 11, 13, 17\}$. On le démontre en constatant que ces représentations ont de très bonnes propriétés de ramification (elles ne sont pas trop ramifiées). Pour $p \neq l$, elles ne sont pas ramifiées du tout : c'est ce que veut dire "avoir bonne réduction". Pour $p = l$, elles sont cristallines, avec des poids de Hodge-Tate qui ne sont pas trop grands. Il faut majorer la ramification et il faut utiliser les bornes d'Odlyzko, telles qu'elles ont été calculées par Diaz y Diaz. Une conséquence est qu'il n'y a pas de variété abélienne sur $\mathbb{Q}$ qui ait bonne réduction partout. Parce que pour chaque nombre premier l, le $H^1_{et}(X, \mathbb{Q}_l)$ doit être une représentation du type $\oplus_{i=0}^{-m} \mathbb{Q}_l(i)^{n_i}$. On peut prendre $l = 3$ par exemple, et $H^1_{et}(X, \mathbb{Q}_l)$ doit être nul parce que, pour des raisons de poids, ça ne peut pas être une somme directe de $\mathbb{Q}_l$ et de $\mathbb{Q}_l(-1)$. Donc la variété est triviale.

2. C'est vrai pour $m = 3$ et $l = 7$. Les techniques de démonstration sont les mêmes. Une conséquence est que si X est une variété projective lisse sur $\mathbb{Q}$ ayant bonne réduction partout, alors
$$H^j(X, \Omega^i_X) = 0 \text{ pour } i \neq j \text{ et } i + j \leqslant 3.$$

Enfin, il faut remarquer que la conjecture serait fausse avec $m = 11$ parce que dans ce cas la représentation associée à la forme modulaire Δ est un contre-exemple.
Pour terminer, je voudrais dire un mot de la réciproque ; parce que c'est la partie la plus excitante, et parce que c'est elle qui a eu le plus d'applications spectaculaires :

Conjecture 2. *Toute représentation géométrique provient de la géométrie algébrique.*

Si on veut un énoncé précis, où l'on serait capable de tenir compte de toutes les représentations géométriques, il faut parler de motifs mixtes, et ce n'est pas mon but ici. Je vais faire une conjecture précise, mais en me limitant ici aux représentations *semi-simples* ; je vais même les supposer *irréductibles*.

Conjecture A. *Si V est une représentation géométrique irréductible de $G_{\mathbb{Q}}$, il existe $m \in \mathbb{N}$, $i \in \mathbb{Z}$, X variété projective lisse sur $\mathbb{Q}$, tels que V soit isomorphe à un facteur direct de $H^m_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l) \otimes \mathbb{Q}_l(i)$.*

En fait la conjecture est plus précise, par exemple on peut dire quels sont i et m en fonction de la représentation V.

Exemple. *Si les poids de Hodge-Tate de V sont 0 et 1, il doit exister une variété abélienne X sur $\mathbb{Q}$ telle que V soit un facteur direct de $V_l(X)$.*

C'est la première forme de cette conjecture. Je vais faire une *conjecture B*, dont je vais parler très vaguement (et la *conjecture C* encore plus vaguement).
Quand il y a des variétés algébriques, il y a des fonctions L. Et en fait, à toute représentation l-adique V, géométrique, de $G_{\mathbb{Q}}$, on sait associer une certaine série de Dirichlet :
$$L(V, s) = \sum n \geqslant 1 \frac{a_n}{n^s}.$$

Pour cela il faut choisir un plongement de $\mathbb{Q}_l$ dans les complexes (c'est un peu innocent). Cette série de Dirichlet est définie comme un produit eulérien, un produit de termes en p ; il suffit

de connaître V comme représentation l-adique de $G_{\mathbb{Q}_p}$. Classiquement, on sait le faire pour $p \neq l$, mais si on parle de représentations potentiellement semi-stables, on sait le faire aussi pour $p = l$. On sait même définir un facteur eulérien à l'infini. Donc on sait définir une fonction L complétée :

$$\Lambda(V, s) = L_\infty(V, s)L(V, s).$$

On définit également un facteur ε uniquement en termes de représentations.

Conjecture B. $\Lambda(V, s)$ *admet un prolongement analytique à tout le plan complexe et satisfait à une équation fonctionnelle.*

On peut écrire cette équation fonctionnelle explicitement, mais je ne vais pas le faire. Voilà donc la *conjecture B*. Et la *conjecture C*, c'est ce que dit la *conjecture B* quand on l'applique à cette représentation et à ses tordues par le caractère cyclotomique, dans le cas de dimension 2. Je vais supposer que V est une représentation de dimension 2 sur E, une extension finie de $\mathbb{Q}_l$ (il n'y a pas de raison de se restreindre à $\mathbb{Q}_l$). Si vous regardez ce que dit la conjecture B pour V et ses tordues par le caractère cyclotomique, et que vous utilisez le théorème de Weil, vous aboutissez à ceci :

Conjecture C. *Si V est une représentation géométrique de dimension 2 sur E, irréductible, de poids de Hodge-Tate i et j avec $i \leqslant j$, alors $V \otimes_{\mathbb{Q}_l} \mathbb{Q}_l(i-j)$ est isomorphe à la représentation associée à une forme modulaire de poids $j - i + 1$.*

Ces trois conjectures ont des quantités d'implications fantastiques, et elles sont complètement inabordables en l'état actuel du sujet. Mais tous les travaux autour de la démonstration du théorème de Fermat-Wiles utilisent cette notion de représentation semi-stable, et en fait contiennent, comme résultats intermédiaires, des *démonstrations* de *petits bouts* des conjectures A, B et C ci-dessus. Par exemple, il y a maintenant un théorème :

Théorème 3. *Toute courbe elliptique E sur $\mathbb{Q}$ est modulaire.*

Comme vous le savez, cela implique Fermat, vu que la courbe elliptique que j'ai regardée au début : $y^2 = x(x - a^p)(x + b^p)$ ne peut être modulaire. Comme la courbe en question est semi-stable, il suffisait de savoir démontrer que toute courbe elliptique E sur $\mathbb{Q}$ est modulaire dans le cas semi-stable. C'est ce qu'avaient fait Wiles et Taylor. En fait, ils l'avaient fait dans des cas un peu plus précis. Après les premiers cas cruciaux traités par Wiles et Taylor, il y a des gens qui ont essayé d'améliorer, de bricoler autour de ces résultats : il y a eu Taylor, Diamond, Darmon. Et le résultat final, qui consistait à regarder le cas des courbes elliptiques dont le conducteur était divisible par 27, 81 ou 243 (on ne peut pas aller plus loin, heureusement) est dû à Breuil, Conrad, Diamond et Taylor. Et en fait, ce qu'il démontrent, c'est la chose suivante : si vous partez d'une courbe elliptique E, vous regardez $V_l(E)$, son module de Tate ; c'est une représentation géométrique, et tautologiquement elle vérifie la *conjecture A* (vous trouvez une variété abélienne : c'est la courbe elliptique elle-même) ; mais ce qu'elle ne vérifie pas tautologiquement, c'est la *conjecture C*, et c'est exactement ce qu'il s'agissait de démontrer pour prouver que la courbe est modulaire. Je n'ai pas le temps d'en dire plus, mais il faut savoir qu'il y a beaucoup d'applications de ce genre de théories, autour de ce type de problèmes.

Bibliographie

[F1], J.-M. FONTAINE, *Le corps des périodes p-adiques, avec un appendice par Pierre Colmez*, in *Périodes p-adiques*, Astérisque **223**, Soc. Math. France, 1994, p. 59-111.

[F2], J.-M. FONTAINE, *Représentations p-adiques semi-stables*, in *Périodes p-adiques*, Astérisque **223**, Soc. Math. France, 1994, p. 113-184.

[Hel], Y. HELLEGOUARCH, *Invitation aux mathématiques de Fermat-Wiles*, Masson, 1997.

[Ko], N. KOBLITZ, *p-adic Numbers, p-adic Analysis and Zeta-functions*, Grad. Texts in Math. **58**, Springer, 1977.

[TaWi], H. L. TAYLOR and A. WILES, *Ring theoretic properties of certain Hecke algebras*, Ann. Math. 141 (1995), p. 553-572.

[Tsu], T. TSUJI, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. Math. **137** (1999), No. 2, p. 233-411.

[Wi], A. WILES, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. 141 (1995), p. 443-551.