Dossier de candidature de Xavier Caruso

— Concours 41/01, année 2018 —

Résumé des travaux de recherche

Table des matières

1 Théorie de Hodge p-adique **3**
- 1.1 Les problématiques de la théorie de Hodge p-adique . . . 3
- 1.2 La théorie de Breuil en présence de ramification . . . 5
- 1.3 La théorie de Breuil–Kisin et les (φ, τ)-modules . . . 8
- 1.4 Variétés de Kisin et espaces de déformations galoisiennes . . . 10

2 Algorithmique des nombres p-adiques **12**
- 2.1 Semi-simplifiée modulo p des représentations semi-stables . . . 13
- 2.2 Une théorie de la précision p-adique . . . 15
- 2.3 La méthode de la précision adaptative . . . 16
- 2.4 Structures p-adiques aléatoires . . . 18

3 Polynômes de Ore et équations différentielles **20**
- 3.1 Factorisation des polynômes de Ore sur les corps finis . . . 20
- 3.2 Sur la p-courbure des équations différentielles . . . 21
- 3.3 Factorisation par les pentes de polynômes de Ore . . . 22
- 3.4 Article de synthèse sur les polynômes de Ore . . . 24

4 Bref résumé des autres activités **24**
- 4.1 Enseignement de la licence au doctorat . . . 24
- 4.2 Étudiants en thèse . . . 25
- 4.3 Diffusion des mathématiques . . . 26
- 4.4 Responsabilités collectives et administration de la recherche . . . 26

Liste de publications, prépublications et production logicielle **28**

Nouveautés depuis ma dernière candidature

Algorithmique des nombres p-adique

évoqué au

Article [24] sur le calcul du polynôme caractéristique d'une matrice p-adique . . . §2.2

Package SageMath [39] permettant un suivi optimal de la précision p-adique . . . §2.2

Notes de cours [29] sur le calcul numérique avec les nombres p-adiques . . . §2.3

Polynômes de Ore

Article [25] sur la multiplication rapide des polynômes tordus . . . §3.1

Notes de cours [30] sur les polynômes de Ore en une variable . . . §3.4

Responsabilités collectives

Lancement des Annales Henri Lebesgue . . . §4.4.4

Mon domaine de recherche se situe à l'interface entre la théorie des nombres et l'algorithmique. Mes centres d'intérêt sont variés, allant des théories les plus abstraites (*e.g.* la correspondance de Langlands p-adique) aux plus appliquées (*e.g.* la conception et l'implantation d'algorithmes pour la manipulation des matrices et des polynômes). Ils gardent néanmoins pour dénominateur commun l'étude des phénomènes portant sur les nombres p-adiques ou sur la caractéristique positive. Schématiquement, ils peuvent se répartir comme ceci :

☞ *la théorie de Hodge p-adique*, ce qui inclut notamment
- — les théorèmes de comparaison entre diverses cohomologies p-adiques
- — une étude des réseaux dans les représentations galoisiennes semi-stables
- — le calcul explicite de certains espaces de déformations galoisiennes

☞ *l'algorithmique des nombres p-adiques*, ce qui inclut notamment
- — une étude fine du comportement de la précision dans le cadre ultramétrique
- — la conception d'algorithmes stables et efficaces pour la manipulation des matrices, des polynômes et des séries p-adiques
- — des résultats de probabilité sur les matrices et polynômes p-adiques aléatoires

☞ *les équations différentielles en caractéristique p et p-adiques*, ce qui inclut notamment
- — l'obtention de formules pour la p-courbure propices à l'évaluation rapide
- — l'obtention d'un théorème et d'un algorithme de factorisation de certains polynômes de Ore (duquel j'ai déduit plusieurs applications)

Le découpage que je viens de présenter pourrait laisser penser que mes activités de recherche sont éparses et décousues. Ce n'est, en réalité, pas du tout le cas et il y a, au contraire, une véritable unité dans mon travail. J'espère la rendre évidente dans la suite de ce document, d'une part, en m'attardant sur les multiples connexions entre mes différents sujets d'étude et, d'autre part, en m'efforçant continuellement de retracer le cheminement de mes idées.

Par ailleurs, j'ai pu constater très concrètement à plusieurs reprises que les compétences que j'ai acquises au cours de mon parcours m'ont été utiles dans des circonstances *a priori* inattendues. Par exemple, comme je l'expliquerai plus en détails dans la suite de ce document au §3, la théorie des algèbres simples centrales et des algèbres d'Azumaya qui m'avait été enseignée lorsque j'apprenais la géométrie algébrique s'est révélée être l'ingrédient essentiel de notre algorithme de factorisation des polynômes de Ore sur les corps finis, ainsi que de nos algorithmes de calcul de p-courbure des opérateurs différentiels. Ces connexions, aux conséquences remarquables, n'avaient jusqu'alors jamais été observées par les algorithmiciens et ont ainsi fortement bénéficié du regard neuf d'un géomètre algébriste qui s'intéressait aux questions algorithmiques.

Dans la suite, la lettre p désigne toujours un nombre premier. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments, $\mathbb{Z}_p$ l'anneau des entiers p-adiques et $\mathbb{Q}_p$ son corps des fractions. On fixe également, une fois pour toutes, une clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ et on note v_p la valuation p-adique sur $\bar{\mathbb{Q}}_p$ normalisée par $v_p(p) = 1$. On note $\bar{\mathbb{F}}_p$ le corps résiduel de $\bar{\mathbb{Q}}_p$; il s'identifie à une clôture algébrique de $\mathbb{F}_p$. Enfin, pour toute puissance q de p, on désigne par $\mathbb{F}_q$ l'unique sous-corps de $\bar{\mathbb{F}}_p$ à q éléments. À partir de maintenant, toutes les extensions algébriques de $\mathbb{Q}_p$ que nous considèrerons seront implicitement supposés vivre à l'intérieur de $\bar{\mathbb{Q}}_p$.

1 Théorie de Hodge p-adique

Mes premiers pas en recherche se sont inscrits dans la thématique de la théorie de Hodge p-adique, une branche de la géométrie arithmétique qui a été développée principalement sous l'influence de Fontaine à partir des années 1970. Le présent chapitre commence par une très brève introduction aux problématiques de la théorie de Hodge p-adique (§1.1) puis entre dans le vif du sujet en présentant, de manière analytique, mes principales contributions dans le domaine.

1.1 Les problématiques de la théorie de Hodge p-adique

La théorie de Hodge classique peut se définir comme l'étude de la cohomologie des variétés algébriques (ou plus généralement kählériennes) complexes. De la même manière, la théorie de Hodge p-adique trouve son origine dans la volonté de comprendre les différentes cohomologies des variétés algébriques p-adiques. Pour l'expliquer plus en détails, considérons une extension finie K de $\mathbb{Q}_p$ d'anneaux des entiers $\mathcal{O}_K$ et de corps résiduel k. On note W l'anneau des vecteurs de Witt à coefficients dans k et on pose $K_0 = W[1/p]$. Ce dernier corps apparaît comme la sous-extension maximale de K non ramifiée sur $\mathbb{Q}_p$. À une variété propre et lisse X définie sur K, on peut associer au moins deux cohomologies naturelles : sa cohomologie de de Rham $H^r_{\text{dR}}(X)$ et sa cohomologie étale $H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p)$ (qui, en un certain sens, apparaît comme un analogue de la cohomologie singulière). Dans le cas complexe, on sait que les cohomologies de de Rham et singulière s'identifient après extension des scalaires à $\mathbb{C}$: c'est le théorème de comparaison de de Rham. Dans le cadre p-adique, l'analogue de ce théorème existe mais est nettement plus subtil. Il a été démontré dans les années 1990 à la suite de travaux conséquents de plusieurs auteurs (Faltings, Fontaine, Messing, Illusie, Kato, Tsuji...) et affirme qu'il existe un isomorphisme canonique et fonctoriel :

$$H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{dR}} \simeq H^r_{\text{dR}}(X) \otimes_K B_{\text{dR}} \tag{1}$$

où B_{dR} est une certaine extension de $\bar{\mathbb{Q}}_p$ (dont la construction est délicate) souvent appelée le corps des périodes p-adiques. Il se trouve, de plus, que les espaces de cohomologie p-adique considérés ci-dessus portent des structures supplémentaires : la cohomologie de de Rham est munie d'une filtration tandis que la cohomologie étale est munie d'une action de $\text{Gal}(\bar{\mathbb{Q}}_p/K)$. Le corps B_{dR}, quant à lui, possède ces deux structures additionnelles et il est possible de choisir l'isomorphisme (1) de manière à ce qu'il les préserve. Lorsque la variété X a réduction semi-stable [1], le théorème de comparaison (1) peut être rendu plus précis ; en effet, on a dans ce cas :

$$H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{st}} \simeq H^r_{\text{log-cris}}(X) \otimes_{K_0} B_{\text{st}} \tag{2}$$

où B_{st} est une certaine sous-K_0-algèbre de B_{dR} et $H^r_{\text{log-cris}}(X)$ désigne une troisième cohomologie : la cohomologie log-cristalline de X. Cette dernière apparaît naturellement comme une K_0-structure de $H^r_{\text{dR}}(X)$, de sorte que l'isomorphisme (2) redonne (1) après extension des scalaires à B_{dR}. En outre, $H^r_{\text{log-cris}}(X)$ est muni d'un endomorphisme de Frobenius φ ainsi que d'un opérateur de monodromie N : on dit que c'est un (φ, N)-module filtré. L'anneau B_{st} porte également un φ et un N et est, par ailleurs, stable par l'action de $\text{Gal}(\bar{\mathbb{Q}}_p/K)$. L'isomorphisme (2), quant à lui, est compatible à toutes les structures : la filtration après

1. On entend par là qu'il existe un prolongement $\mathcal{X}$ de X à l'anneau des entiers de K avec les propriétés suivantes : $\mathcal{X}$ est propre, plat et sa fibre spéciale est un diviseur à croisements normaux.

extension des scalaires à B_{dR}, l'action de φ, celle de N et celle de $\text{Gal}(\bar{\mathbb{Q}}_p/K)$. Cette version rafinée est intéressante car elle est à l'origine de recettes purement algébriques permettant de passer de $H^r_{\text{log-cris}}(X)$ à $H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p)$ et *vice versa*. En effet, elle implique :

$$\begin{aligned} H^r_{\text{log-cris}}(X) &= \big(H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{st}}\big)^{\text{Gal}(\bar{\mathbb{Q}}_p/K)} \\ H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p) &= \big(H^r_{\text{log-cris}}(X) \otimes_{K_0} B_{\text{st}}\big)^{\varphi=1, N=0} \cap \text{Fil}^0\big(H^r_{\text{log-cris}}(X) \otimes_{K_0} B_{\text{dR}}\big). \end{aligned}$$

Devant ce constat (qui était encore conjectural à l'époque), Fontaine a eu l'idée d'abstraire la situation en oubliant la variété X et sa cohomologie et en ne retenant que la recette algébrique. Précisément, il définit la notion de (φ, N)-module filtré et démontre que si D est un tel objet, la formule :

$$V(D) = \big(D \otimes_{K_0} B_{\text{st}}\big)^{\varphi=1, N=0} \cap \text{Fil}^0\big(D \otimes_{K_0} B_{\text{dR}}\big)$$

définit une $\mathbb{Q}_p$-représentation de $\text{Gal}(\bar{\mathbb{Q}}_p/K)$. Lorsque $V(D)$ a la même dimension que D, on dit que D est *admissible*. Les représentations de la forme $V(D)$ pour D admissible sont, quant à elles, qualifiées de *semi-stables*. Les représentations de la forme $H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p)$ sont donc semi-stables dès que X a réduction semi-stable ; on s'attend ainsi à ce que les représentations semi-stables présentent un intérêt particulier. L'histoire a indubitablement confirmé cette attente et, mieux encore, elle a donné à la notion de représentation semi-stable un rôle central en théorie des nombres qui déborde largement du cadre strict de l'étude des cohomologies p-adiques et s'étend désormais, parmi d'autres choses, aux conjectures de type Serre sur les formes modulaires ou encore à la correspondance de Langlands.

Après avoir mis en évidence la notion de représentation semi-stable, Fontaine démontre que l'association $D \mapsto V(D)$ définit une équivalence de catégories entre (φ, N)-modules filtrés admissibles et représentations semi-stables, de sorte que l'on dispose d'un outil efficace pour étudier ses dernières. Les poids de Hodge–Tate de V, définis initialement comme les entiers h_i pour lesquels

$$V \otimes_{\mathbb{Q}_p} \mathbb{C}_p = \bigoplus_{i=1}^{\dim V} \mathbb{C}_p(-h_i) \qquad (\text{où } \mathbb{C}_p \text{ est le complété de } \bar{\mathbb{Q}}_p)$$

se retrouvent, en particulier, sur cette description : ils correspondent aux sauts de la filtration sur le (φ, N)-module filtré associé à V. On en déduit, en particulier, que les poids de Hodge–Tate de $H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p)$ sont tous compris entre 0 et r.

Le tableau dont je viens de brosser les grandes lignes est celui de la théorie de Hodge p-adique rationnelle dans laquelle on s'intéresse à la cohomologie à coefficients dans $\mathbb{Q}_p$ ou, si l'on préfère, aux représentations galoisiennes à coefficients dans $\mathbb{Q}_p$. Toutefois, les problématiques et les méthodes actuelles de la théorie des nombres requièrent de plus en plus souvent de travailler au niveau entier, c'est-à-dire avec des représentations à coefficients dans $\mathbb{Z}_p$; ceci se produit par exemple inévitablement dès lors que l'on est amené à considérer des espaces de déformations de représentations galoisiennes (qui sont des objets qui ont acquis une importance considérable depuis que Wiles les a utilisés avec brio pour démontrer la conjecture de Taniyama–Weil et, comme corollaire, le grand théorème de Fermat).

Afin de s'attaquer à ces nouveaux défis, les mathématiciens ont dû développer une version entière (resp. de torsion) de la théorie de Hodge p-adique, c'est-à-dire une version de la théorie de Hodge p-adique qui s'intéresse à la cohomologie et aux représentations galoisiennes à coefficients dans $\mathbb{Z}_p$ (resp. dans un $\mathbb{Z}/p^n\mathbb{Z}$). Dans le cadre entier, et *a foriori*

dans le cadre de torsion, de nouvelles difficultés apparaissent. En effet, bien qu'il soit vrai que les cohomologies log-cristalline et étale possèdent toutes les deux une structure entière canonique (cela résulte de leur définition), celles-ci ne se correspondent généralement pas sous l'isomorphisme (2). Pour dépasser cette difficulté, l'idée est de travailler sur une nouvelle base, en l'occurrence Spec $W[t]$. Après le choix d'une uniformisante π de $\mathcal{O}_K$, on dispose d'un morphisme Spec $\mathcal{O}_K \to$ Spec $W[t]$ obtenu en envoyant t sur π. L'idée est alors de considérer la cohomologie log-cristalline de X relativement à Spec $W[t]$. Toutefois, cela ne fonctionne pas directement car $W[t]$ n'est pas muni de puissances divisées comme l'exige le formalisme cristallin. Au lieu de $W[t]$, on travaille donc avec l'anneau S défini comme le complété p-adique de l'enveloppe à puissances divisées de $W[t]$ relativement au noyau de $W[t] \to \mathcal{O}_K$, $t \mapsto \pi$. On considère la cohomologie log-cristalline de X relativement à S que l'on notera, dans la suite, $H^r_{\text{log-cris}}(X/S)$. Il s'agit ici du cas entier mais le cas de torsion se traite pareillement en remplaçant S par $S_n = S/p^nS$. Lorsque $K/\mathbb{Q}_p$ est non ramifiée et $r < p-1$, Breuil démontre que $H^r_{\text{log-cris}}(X/S)$ et $H^r_{\text{log-cris}}(X/S_n)$ possèdent une structure particulière — appelée aujourd'hui *module de Breuil* — et que la cohomologie étale s'en déduit par une recette purement algébrique. En outre, de même que dans le cas rationnel, Breuil donne une version abstraite, indépendante de la géométrie, de sa théorie. Sous l'unique hypothèse $r < p-1$, il définit des catégories de modules de Breuil $\text{Mod}^r_{/S}$ et $\text{Mod}^r_{/S_n}$ ainsi que des foncteurs (contravariants) T_{st} qui associent, à tout objet de l'une de ces catégories, des représentations galoisiennes. Lorsque $K/\mathbb{Q}_p$ est non ramifiée, il démontre en outre des propriétés de structure sur $\text{Mod}^r_{/S}$, $\text{Mod}^r_{/S_n}$ et T_{st}. Il en déduit notamment que le foncteur T_{st} induit une équivalence de catégories entre $\text{Mod}^r_{/S}$ et la catégorie des $\mathbb{Z}_p$-réseaux galoisiens dans les représentations semi-stables à poids de Hodge–Tate compris entre 0 et r. Au niveau des modules de torsion, Breuil démontre que le fonction T_{st} défini sur la catégorie $\text{Mod}^r_{/S_n}$ est pleinement fidèle (de sorte qu'il induit une équivalence de catégories entre $\text{Mod}^r_{/S_n}$ et son image essentielle).

1.2 La théorie de Breuil en présence de ramification

Telle que je viens de la décrire, la théorie de Breuil ne fonctionne que pour une extension $K/\mathbb{Q}_p$ qui est non ramifiée. Il s'agit, en réalité, d'une limitation ennuyeuse car les situations pratiques dans lesquelles on aurait envie de l'appliquer ne vérifient que rarement cette hypothèse. Il paraissait donc important d'étendre la théorie de Breuil en ramification arbitraire ; c'est ce à quoi je me suis attelé d'abord pendant ma thèse puis pendant mes premières années comme chargé de recherche au CNRS.

1.2.1 Les résultats de structure

Références :
[5] X. Caruso, *Représentations semi-stables de torsion dans le cas* $er < p-1$
[6] X. Caruso, *Conjecture de l'inertie modérée de Serre*
[8] X. Caruso, T. Liu, *Quasi-semi-stable representations*
[13] X. Caruso, $\mathbb{F}_p$*-représentations semi-stables*

En notant e l'indice de ramification de $K/\mathbb{Q}_p$, j'ai d'abord traité, dans ma thèse, le cas où $er < p-1$. J'ai obtenu, sous cette hypothèse, la généralisation directe des résultats de Breuil à savoir :

Théorème 1. *Supposons $er < p-1$. Pour tout entier n, la catégorie $\mathrm{Mod}^r_{/S_n}$ est abélienne. Le foncteur T_{st} defini sur icelle est pleinement fidèle tandis que son image essentielle est stable par quotient et par sous-objet.*

De plus, si X est une variété propre et lisse sur K admettant un modèle semi-stable, alors $H^r_{\text{log-cris}}(X/S_n) \in \mathrm{Mod}^r_{/S_n}$ et :

$$H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Z}/p^n\mathbb{Z}) = T_{\mathrm{st}}\big(H^r_{\text{log-cris}}(X/S_n)\big).$$

En contrepartie, lorsque l'indice de ramification e devient trop grand, le théorème 1 ne vaut pas et l'analyse devient nettement plus subtile. L'observation fondamentale qui permet de débloquer la situation est que les fibres non vides du foncteur T_{st} défini sur $\mathrm{Mod}^r_{/S_1}$ possèdent une structure naturelle de treillis [2] de hauteur finie, un module M_1 étant considéré inférieur à un module M_2 s'il existe une flèche $M_1 \to M_2$ dont l'image par T_{st} est l'identité. On déduit de cela l'existence d'un foncteur $\mathrm{Max} : \mathrm{Mod}^r_{/S_1} \to \mathrm{Mod}^r_{/S_1}$ défini en associant à un objet M le plus grand élément de la fibre (non vide) au-dessus de $T_{\mathrm{st}}(M)$. Par définition, le foncteur T_{st} se factorise par Max : on a $T_{\mathrm{st}} = T_{\mathrm{st}} \circ \mathrm{Max}$. De plus, Max est clairement une projection dans le sens où il vérifie $\mathrm{Max} \circ \mathrm{Max} = \mathrm{Max}$. En notant $\mathrm{Max}^r_{/S_1}$ l'image essentielle de Max, j'ai démontré, en partie en collaboration avec Tong Liu, le théorème suivant qui résonne comme un analogue de la première partie du théorème 1 :

Théorème 2. *La catégorie $\mathrm{Max}^r_{/S_1}$ est abélienne. La restriction du foncteur T_{st} à $\mathrm{Max}^r_{/S_1}$ est pleinement fidèle et son image essentielle est stable par quotient et par sous-objet.*

De surcroît, j'ai complété la théorie de Breuil sur un point essentiel en construisant un inverse à gauche M_{st} du foncteur T_{st}. L'existence d'un tel foncteur admet au moins deux corollaires intéressants. Premièrement, il permet de détecter les représentations qui sont dans l'image essentielle de T_{st} : ce sont exactement les représentations V pour lesquelles la dimension sur S_1 de $M_{\mathrm{st}}(V)$ est égale à la dimension sur $\mathbb{F}_p$ de V. Deuxièmement, il permet d'incorporer, à moindre frais, des données supplémentaires variées à la théorie des modules de Breuil. Typiquement, si la représentation $V \in T_{\mathrm{st}}(\mathrm{Mod}^r_{/S_1})$ est munie d'une forme symplectique, celle-ci se remonte immédiatement *via* le foncteur M_{st} au module de Breuil maximal correspondant à V. On obtient ainsi de cette manière, sans argument supplémentaire, une théorie des modules de Breuil symplectiques.

La démonstration du théorème 2 n'est pas immédiate : elle occupe deux articles et fait un usage décisif de la théorie de Breuil–Kisin qui sera détaillée dans la suite.

1.2.2 Quelques applications

Références :

[6] X. Caruso, *Conjecture de l'inertie modérée de Serre*

[7] X. Caruso, D. Savitt, *Polygones de Hodge, de Newton et de l'inertie modérée des représentations semi-stables*

[12] X. Caruso, T. Liu, *Some bounds for ramification of p^n-torsion semi-stable representations*

Comme expliqué précédemment, les théorèmes 1 et 2 fournissent un accès aux représentations galoisiennes semi-stables. Ils permettent ainsi de démontrer des résultats non triviaux (et souvent inaccessibles par d'autres voies) sur ces représentations et donc, en particulier, sur la cohomologie p-adique des variétés algébriques p-adiques.

2. Par définition, un treillis est un ordre dont toute partie finie non vide admet une borne inférieure et une borne supérieure.

Action de l'inertie modérée. Comme illustration particulièrement frappante de ce fait, signalons que le théorème 1 m'a permis de démontrer la conjecture de l'inertie modérée de Serre. Avant d'en expliquer le mécanisme, rappelons brièvement l'énoncé de cette conjecture. On part d'une variété X que l'on suppose propre et lisse sur K à réduction semi-stable et on considère la représentation galoisienne $V = H^r_{\text{ét}}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_p)$. Un théorème, dû à Brauer et Nesbitt, affirme que si $T \subset V$ est un $\mathbb{Z}_p$-réseau stable par l'action de Galois, la semi-simplifiée de T/pT ne dépend que de V (et pas du choix de T) ; on l'appelle la semi-simplifiée modulo p de V et on la notera $\bar{V}$. La conjecture de l'inertie modérée de Serre donne des bornes sur l'action du sous-groupe d'inertie sur $\bar{V}$. Rappelons que le sous-groupe d'inertie I est défini comme le noyau du morphisme naturel $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ et qu'il s'identifie à $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\text{nr}})$ où $\mathbb{Q}_p^{\text{nr}}$ désigne l'extension maximale non ramifiée de $\mathbb{Q}_p$. Pour un entier n fixé, considérons ξ_n une racine (p^n-1)-ième d'une uniformisante π de K. L'application :

$$\begin{array}{rccl} \omega_n : & I & \to & \mathbb{F}_{p^n} \\ & g & \mapsto & \text{réduction modulo } p \text{ de } \frac{g(\xi_n)}{\xi_n} \end{array}$$

définit alors un caractère de I d'ordre p^n-1 à coefficients dans $\mathbb{F}_{p^n}$ appelé *caractère fondamental de niveau* n. En oubliant l'action de $\mathbb{F}_{p^n}$, on s'aperçoit que ω_n, et plus généralement les puissances de ω_n, définissent également des $\mathbb{F}_p$-représentations de dimension n de I. Il se trouve que cette construction épuise les représentations irréductibles de I de dimension n. Ainsi, en décomposant l'exposant en base p, on trouve que chaque constituant irréductible de $\bar{V}$ est associé à un caractère de la forme

$$\omega_n^{a_0} \cdot \omega_n^{pa_1} \cdots \omega_n^{p^{n-1}a_{n-1}}$$

pour un certain n et certains entiers $a_i \in \{0, \ldots, p-1\}$. La conjecture de l'inertie modérée de Serre prédit que ces entiers sont tous compris entre 0 et er.

Remarque. La conjecture de l'inertie modérée de Serre est ainsi dénommée car elle ne donne d'information que sur l'action du groupe d'inertie modérée, défini comme le quotient de I par son unique pro-p-groupe I_p. En effet, le caractère semi-simple de la représentation $\bar{V}$ implique (par un lemme classique de théorie de groupes) que I_p agit sur $\bar{V}$ de manière triviale.

La conjecture de l'inertie modérée de Serre est vide lorsque $er \geq p-1$; on peut donc supposer $er < p-1$ et se mettre ainsi dans les conditions d'application du théorème 1. Or, d'après celui-ci, il suffit de démontrer que si M est un objet simple de $\text{Mod}^r_{/S_1}$ alors $T_{\text{st}}(M)$ est associé à un caractère $\omega_n^{a_0} \cdot \omega_n^{pa_1} \cdots \omega_n^{p^{n-1}a_{n-1}}$ avec $0 \leq a_i \leq er$. Avec un peu de travail, on peut donner une classification complète des objets simples de $\text{Mod}^r_{/S_1}$ puis calculer de façon entièrement explicite l'action de T_{st} sur ceux-ci. Pour conclure, on a plus qu'à constater que les exposants a_i calculés vérifient bien l'inégalité attendue. En outre, la démonstration dont je viens d'esquisser les grandes lignes reste valable dès lors que V est une représentation semi-stable dont les poids de Hodge–Tate sont compris entre 0 et r.

Fort de ce résultat, je suis par la suite allé encore plus loin dans cette direction. Précisément, j'ai obtenu, en collaboration avec David Savitt, un raffinement de la conjecture de Serre. Étant donnée une représentation V de $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, Savitt et moi-même définissons les *poids de l'inertie modérée* de V comme la collection de tous les entiers a_i (comptés avec multiplicité) associés aux facteurs irréductibles de $\bar{V}$. Si V est de dimension d, on définit comme ceci d poids de l'inertie modérée que je note $m_1, \ldots, m_d$ avec $m_1 \leq m_2 \leq \cdots \leq m_d$. Nous appellons *polygone de l'inertie modérée* la ligne brisée reliant les points de coordonnées $(i, \frac{m_1+\cdots+m_i}{e})$ pour i variant de 0 à d. Nous démontrons le théorème suivant :

Théorème 3. *Supposons $er < p-1$. Soit V une représentation semi-stable de* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ *dont les poids de Hodge–Tate sont tous compris entre 0 et r. Alors le polygône de l'inertie modérée de V est au-dessus de son polygone de Hodge*[3] *et ces deux polygones ont même point terminal.*

Il est à noter que le théorème précédent est un énoncé plus précis que la conjecture de l'inertie modérée de Serre. En effet, les pentes du polygône de Hodge d'une représentation V vérifiant l'hypothèse de l'énoncé sont toutes plus petites que r. Le théorème 3 implique qu'il va de même pour celles du polygone de l'inertie modérée, c'est-à-dire que $\frac{m_i}{e} \leq r$ pour tout i.

Action de l'inertie sauvage. En collaboration avec Tong Liu, je me suis également intéressé à l'action du sous-groupe d'inertie sauvage I_p (défini comme le pro-p-groupe de I) sur les représentations semi-stables. Pour énoncer notre résultat, rappelons que le groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ est filtré par une suite décroissante de sous-groupes $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)^{(\mu)}$ indexée par le paramètre $\mu \in \mathbb{Q}$. Le sous-groupe $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)^{(0)}$ (resp. $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)^{(1)}$) n'est autre que le sous-groupe d'inertie (resp. le sous-groupe d'inertie sauvage). Pour $\mu \geq 1$, on obtient une filtration de I_p dont les quotients successifs ont une réinterprétation plus simple. Une version simplifiée du théorème que nous avons obtenu avec Tong Liu s'énonce comme suit :

Théorème 4. *Soit V une représentation semi-stable de* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ *à poids de Hodge–Tate compris entre 0 et r. Soit T un $\mathbb{Z}_p$-réseau de V stable par l'action de Galois. Alors, pour tout n, le sous-groupe* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)^{(\mu)}$ *agit trivialement sur T/p^nT dès lors que*

$$\mu > 1 + e \cdot \left(n + 1 + \log_p r\right)$$

où e désigne l'indication de ramification de $K/\mathbb{Q}_p$.

Plusieurs résultats avaient déjà été obtenus dans la veine du théorème 4 par Fontaine et Abrashkyn mais ils ne s'appliquaient tous qu'avec des restrictions fortes sur e et r. De plus, ils donnaient la trivialité de l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)^{(\mu)}$ pour une borne μ de la forme $\mu = n + \frac{er}{p-1} + O(1)$. Fontaine avait d'ailleurs demandé si une telle borne était valable généralement. Notre résultat répond donc positivement à la question de Fontaine mais va bien au-delà de cela car il met en évidence, pour la première fois, la croissance *logarithmique* de μ vis-à-vis de r alors que, semble-t-il, on ne s'attendait *a priori* qu'à une croissance *linéaire*.

1.3 La théorie de Breuil–Kisin et les (φ, τ)-modules

Référence :

[14] X. Caruso, *Représentations galoisiennes p-adiques et (φ, τ)-modules*

Vers la fin des années 1990, Breuil a proposé une alternative, d'apparence bien plus simple, à la théorie des modules de Breuil en introduisant des nouvelles catégories $\mathrm{Mod}^r_{/\mathfrak{S}}$ et $\mathrm{Mod}^r_{/\mathfrak{S}_n}$. Celle-ci a été ensuite reprise et largement complétée par Kisin, de sorte que la théorie résultante s'appelle aujourd'hui la théorie de Breuil–Kisin.

L'anneau $\mathfrak{S}$ qui est apparu précédemment est $W[[u]]$. Contrairement à l'anneau S, qui servait de base aux modules de Breuil, il ne fait pas apparaître de puissances divisées et semble ainsi plus simple. En outre, un module de Breuil–Kisin, c'est-à-dire un objet de la

3. Pour rappel, il s'agit du polygone dont les pentes successives sont les poids de Hodge–Tate de V et ces derniers sont tous compris entre 0 et er

catégorie $\mathrm{Mod}^r_{/\mathfrak{S}}$, est défini comme un $\mathfrak{S}$-module libre $\mathfrak{M}$ muni d'un opérateur semi-linéaire ϕ vérifiant la condition suivante :

$$E(u)^r\mathfrak{M} \subset \langle \phi(\mathfrak{M}) \rangle_{\mathfrak{S}} \quad \text{où } E(u) \text{ est le polynôme minimal de } \pi \text{ sur } K_0. \tag{3}$$

Cependant $\mathfrak{M}$ ne porte ni filtration, ni d'opérateur de monodromie. Pour ces raisons, travailler avec les modules de Breuil–Kisin s'avère généralement plus facile. En outre, la théorie de Breuil–Kisin s'applique sous des hypothèses plus faibles puisqu'elle ne requiert plus la contrainte $r < p-1$ qui est était nécessaire à la définition des modules de Breuil. La contrepartie est que les modules de Breuil–Kisin n'encodent malheureusement pas toute l'information galoisienne. Précisément, fixons $(\pi_s)_{s\geq 0}$ un système compatible de racines p^s-ièmes de l'uniformisante π et posons $K_s = K(\pi_s)$ et $K_\infty = \bigcup_{s\geq 0} K_s$. Avec ces notations, à un module de Breuil–Kisin, on ne peut associer qu'une représentation du $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_\infty)$ qui, en général, n'a aucune raison d'admettre un prolongement à $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$. Malgré tout, soulignons qu'au moins dans le cas où $r < p-1$, il existe un lien fort entre modules de Breuil et modules de Breuil–Kisin et être capable de jongler entre les deux approches est souvent la clé permettant de débloquer de nombreuses situations ; la démonstration des théorèmes 2 et 4 qui ont été cités précédemment repose par exemple sur ces principes généraux.

Toutefois, cette approche n'est pas entièrement satisfaisante et il semblerait nettement plus commode de pouvoir enrichir les modules de Breuil–Kisin de façon à obtenir un objet qui encode de manière complète toute l'information intéressante. L'observation fondamentale qui permet d'avancer dans cette direction consiste à dire que le groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ est engendré topologiquement par le sous-groupe $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_\infty)$ auquel il faut ajouter un élément additionnel noté τ. À partir de là, en utilisant des méthodes classiques dûes à Fontaine et Wintenberger et en menant à son terme une stratégie initiée par Liu, j'ai construit une équivalence de catégories entre la catégorie des représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ et une catégorie de (φ,τ)-modules que j'ai définie à cette occasion. L'intérêt de cette construction est sa proximité avec la théorie de Breuil–Kisin ; en effet, par construction, l'action de φ sur un (φ,τ)-module correspond exactement à l'action du sous-groupe $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_\infty)$ du côté galoisien et donc à l'opérateur φ des modules de Breuil–Kisin. En injectant à présent la condition (3), je parviens à isoler une sous-catégorie de la catégorie des (φ,τ)-modules qui est la catégorie des modules de Breuil–Kisin enrichis évoquée précédemment, en ce sens qu'elle correspond exactement aux réseaux dans les représentations semi-stables à poids de Hodge–Tate compris entre 0 et r. Un avantage important de ma construction est qu'elle replace, du côté des (φ,τ)-modules, les représentations semi-stables à l'intérieur de la catégorie des toutes les représentations (ce qui n'est pas le cas, par exemple, dans la théorie de Breuil–Kisin). Je déduis de ce travail le théorème suivant qui répond par l'affirmative à une question de Kisin :

Théorème 5. *Il existe un entier s ne dépendant que de K pour lequel toute $\mathbb{Q}_p$-représentation V de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ dont la restriction de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_\infty)$ provient d'un module de Breuil–Kisin est semi-stable en restriction à $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_s)$.*

Un des intérêts de ce résultat est la justification *a posteriori* de la pertinence de se restreindre à l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K_\infty)$ et donc la pertinence de la vision de Breuil et de la théorie de Breuil–Kisin qui en a résulté.

Par ailleurs, de part leur construction, la théorie des (φ,τ)-modules présente un parallèle évident avec la théorie plus classique des (φ,Γ)-modules ; il est ainsi naturel de se demander si les théorèmes et constructions usuelles sur les (φ,Γ)-modules ont un pendant du côté des

(φ,τ)-modules. Typiquement, existe-t-il un théorème des (φ,τ)-modules ? C'est une question que je pose dans mon article et à laquelle Gao et Liu ont très récemment apporté une réponse positive. Ce dernier résultat me paraît particulièrement intéressant car il ouvre la porte, je pense, à de nombreuses applications.

1.4 Variétés de Kisin et espaces de déformations galoisiennes

Références :
[22] X. Caruso, *Dimensions de certaines variétés de Kisin*
[26] X. Caruso, A. David, A. Mézard, *Un calcul d'anneaux de déformations potentiellement Barsotti–Tate*
[19] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate*

Un autre avantage décisif des modules de Breuil–Kisin, qui a été mis en lumière par Kisin, consiste en la facilité (relative) qu'on a à les déformer, fournissant par là-même un nouvel angle d'attaque pour l'étude et le calcul des espaces de déformations galoisiennes p-adiques. Concrètement, considérons un certain espace de déformations galoisiennes que l'on écrit sous la forme $R(\mathcal{C},\bar\rho)$ où, ici, $\bar\rho$ désigne une représentation galoisienne en caractéristique p et la lettre $\mathcal{C}$ symbolise les conditions que l'on impose sur les déformations [4]. Dans les bons cas, $\mathcal{C}$ et $\bar\rho$ se relèvent au niveau des modules de Breuil–Kisin et il est possible de construire un espace de déformations de modules de Breuil-Kisin qui est un schéma formel que nous noterons $\mathscr{GR}(\mathcal{C},\bar\rho)$. On dispose en outre d'un morphisme :

$$\mathscr{GR}(\mathcal{C},\bar\rho) \to \text{Spf } R(\mathcal{C},\bar\rho)$$

qui induit un isomorphisme en fibre générique. Par ailleurs, en notant les fibres spéciales et génériques par les indices s et η respectivement, il existe un morphisme de spécialisation $\text{sp} : \mathscr{GR}(\mathcal{C},\bar\rho)_\eta \to \mathscr{GR}(\mathcal{C},\bar\rho)_s$. Le calcul de $\mathscr{GR}(\mathcal{C},\bar\rho)_\eta \simeq \text{Spm } R(\mathcal{C},\bar\rho)[\frac{1}{p}]$ peut ainsi se découper en trois étapes comme suit : (1) le calcul de $\mathscr{GR}(\mathcal{C},\bar\rho)_s$, (2) le calcul des fibres de sp et (3) le recollement de ces fibres.

Ce point de vue prend tout son intérêt lorsque l'on se rend compte que les deux premières étapes (au moins) paraissent abordables, voire automatisables. En effet, les variétés $\mathscr{GR}(\mathcal{C},\bar\rho)_s$ — nommés *variétés de Kisin* par Pappas et Rapoport — admettent une définition alternative qui s'exprime dans le langage de la théorie des groupes et peuvent ainsi être étudiées à l'aide d'outils puissants spécifiques. De même, le calcul des fibres de sp se formule de manière simple en termes matriciels et semble ainsi, lui aussi, accessible.

Un exemple en dimension 2. Avec Agnès David et Ariane Mézard, nous avons récemment étudié une famille d'exemples pour lesquels nous sommes parvenus à faire fonctionner la stratégie jusqu'à son terme et à exhiber de cette manière des candidats, encore conjecturaux, pour les espaces de déformations considérés.

La situation que nous avons étudiée est la suivante. Soient f un entier naturel strictement positif et F l'unique extension non ramifiée de $\mathbb{Q}_p$ de degré f incluse dans $\bar{\mathbb{Q}}_p$. Soit $\bar\rho : \text{Gal}(\bar{\mathbb{Q}}_p/F) \to \text{GL}_2(\bar{\mathbb{F}}_p)$ une représentation de dimension 2. À $\bar\rho$ enrichi d'une donnée supplémentaire $\mathbf{t}$ que l'on appelle le *type galoisien*, on sait associer une $\bar{\mathbb{Z}}_p$-algèbre $R(\mathbf{t},\bar\rho)$ qui paramètre les relevés $\rho : \text{Gal}(\bar{\mathbb{Q}}_p/F) \to \text{GL}_2(\bar{\mathbb{Z}}_p)$ de $\bar\rho$ dont la restriction à un sous-groupe ouvert convenable provient d'un groupe p-divisible et qui vérifient une condition supplémentaire

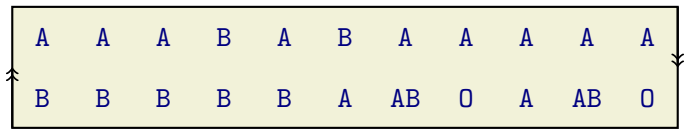
4. Typiquement, on considère des déformations semi-stables à poids de Hodge–Tate fixés, ou encore potentiellement semi-stables avec poids de Hodge–Tate et type galoisien fixés.

(qui s'exprime dans le langage de la théorie de Hodge p-adique) liée au type galoisien $\mathbf{t}$. Lorsque $\bar{\rho}$ est générique et $\mathbf{t}$ est non ramifié, les anneaux $R(\mathbf{t}, \bar{\rho})$ avaient été complètement calculés par Breuil et Mézard. Avec Agnès David et Ariane Mézard, nous souhaitions ôter l'hypothèse de généricité car, s'il est vrai qu'elle est commode pour mener à bien les calculs, elle ne permet malheureusement d'embrasser qu'une partie infime de la complexité de la situation.

Pour commencer, nous nous sommes rendus compte que la simplicité des calculs dans le cas générique était reflétée par une propriété simple de la variété de Kisin sous-jacente : le fait qu'elle soit de dimension nulle. Sans l'hypothèse de généricité, la variété de Kisin prend des formes plus variées mais sa géométrie reste néanmoins contrôlée. Le théorème ci-après, énoncé de manière volontairement vague, résume les résultats que nous avons obtenus dans cette direction :

Théorème 6. *On suppose que le type galoisien* $\mathbf{t}$ *est non ramifié. La variété de Kisin* $\mathcal{X}(\mathbf{t}, \bar{\rho})$ *associé aux données* $\mathbf{t}$ *et* $\bar{\rho}$ *apparaît comme une sous-variété fermée de* $(\mathbb{P}^1)^f$ *donnée par une famille explicite d'équations.*

Il serait trop long d'expliquer en détails dans ce texte comment les équations explicites dont il est question dans le théorème ci-dessus s'obtiennent. Mentionnons cependant qu'elles sont toutes de degré au plus 2 et que chacune d'elles ne fait intervenir que les coordonnées projectives sur deux copies successives de $\mathbb{P}^1$. En réalité, ces équations se lisent directement sur une donnée combinatoire simple associée au couple $(\mathbf{t}, \bar{\rho})$ que nous avons appelée le *gène* de $(\mathbf{t}, \bar{\rho})$ et qui, concrètement, est une suite de $2f$ symboles choisis dans l'ensemble à quatre éléments $\{\mathtt{O}, \mathtt{A}, \mathtt{B}, \mathtt{AB}\}$ que l'on représente sur un ruban de Moebius. En voici un exemple, lorsque $f = 11$:



Ce même gène a d'autres vertus. Il encode, en effet, également les fibres de l'application de spécialisation sp. Précisément, nous démontrons que chaque fibre est de la forme :

$$\mathrm{sp}^{-1}(x) = A_1(x) \times A_2(x) \times \cdots \times A_f(x)$$

où, pour chaque i et pour chaque x, le facteur $A_i(x)$ est soit une boule, soit une couronne, ce dernier choix se lisant de manière explicite sur le gène. À partir de là, nous proposons une construction géométrique permettant de trouver de manière conjecturale l'anneau $R(\mathbf{t}, \bar{\rho})[1/p]$: il s'agit concrètement d'une suite d'éclatements et de complétés formels à partir d'un produit de copies de $\mathbb{P}^1$, qui est entièrement dictée par le gène de couple $(\mathbf{t}, \bar{\rho})$.

Le point de vue que nous avons adopté dans ce travail, qui met en avant les variétés de Kisin, a depuis été repris par plusieurs auteurs et a abouti, d'une part, à de nouveaux résultats explicites comparables à ceux que nous avons obtenu et, d'autre part, à une compréhension plus raffinée de la géométrie des espaces de déformations.

Variétés de Kisin dans le cas général. L'extension du travail précédent au cadre général soulève de réelles difficultés (et, de fait, on s'attend à ce que les espaces de déformations soient nettement plus complexes). Sur les encouragements de Rapoport, je me suis toutefois attelé à

comprendre la géométrie des variétés de Kisin dans le cas particulier des déformations plates de la représentation triviale en dimension quelconque. J'ai, dans ce contexte, obtenu des résultats partiels qui *a fortioti* me paraissent particulièrement intéressants car ils m'ont permis de formuler des conjectures *générales* sur la taille des variétés de Kisin (qui dépassent donc très largement le cadre de l'exemple que j'ai étudié).

Rappelons brièvement la définition alternative des variétés de Kisin dans le langage de la théorie des groupes. Étant donnés un corps k de caractéristique p supposé algébriquement clos pour simplifier, un groupe réductif G défini sur k, un élément $b \in G(k((u)))$ et un copoids dominant μ, on définit la variété $\mathcal{X}_\mu^G(b)$ par :

$$\mathcal{X}_\mu^G(b)(k) = \left\{ \, g \in G(k((u)))/G(k[[u]]) \;\middle|\; g^{-1}bg^\sigma \in G(k[[u]])u^\mu G(k[[u]]) \, \right\}$$

où l'endomorphisme σ agit sur $k((u))$ comme une puissance du Frobenius sur k et en envoyant u sur u^b pour un certain entier $b \geq 2$. J'ai tout d'abord étudié les variétés $\mathcal{X}_\mu^G$ lorsque le groupe G est GL_d et l'élément b est l'identité ; du point de vue de la théorie de Hodge p-adique, cette situation correspond, lorsque σ agit trivialement sur k et envoie u sur u^p, aux déformations de la représentation triviale de dimension d de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ lorsque K est totalement ramifié sur $\mathbb{Q}_p$. Le copoids dominant μ s'interprète dans ce cas particulier comme un d-uplet d'entiers $(\mu_1, \ldots, \mu_d)$ vérifiant $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_d$. Le théorème que j'obtiens porte sur la dimension de $\mathcal{X}_\mu^{\mathrm{GL}_d}(I_d)$ et s'énonce comme suit :

Théorème 7. *Avec les notations précédentes, on a :*

$$\dim \mathcal{X}_\mu^{\mathrm{GL}_d}(I_d) = (b-1) \cdot \min_{w \in \mathfrak{S}_d} \sum_{i=1}^{d} \sum_{n=1}^{\infty} \mu_i \cdot \frac{d+1-i-w^n(i)}{b^n} \; + \; O(1)$$

où le $O(1)$ ne dépend que de d.

La démonstration du théorème ci-dessus se décompose en plusieurs étapes. Tout d'abord, m'inspirant de travaux de Viehmann, je définis une stratification de la variété $\mathcal{X}_\mu^{\mathrm{GL}_d}(I_d)$ dont les strates ont une géométrie relativement simple. En particulier, je parviens à estimer — voire à déterminer complètement dans les bons cas — la dimension de celles-ci. Le problème du calcul de la dimension de $\mathcal{X}_\mu^{\mathrm{GL}_d}(I_d)$ se transforme alors complètement jusqu'à devenir une question de programmation linéaire entière pure dans laquelle la géométrie a complètement disparu. La résolution de ce nouveau problème est néanmoins très subtile et repose sur une étude très fine des propriétés combinatoires des objets mis en jeu.

Il est important de noter que la formule qui apparaît dans le membre de droite de l'égalité du théorème 7 peut s'interpréter complètement dans le langage de la théorie des groupes comme un infimum, pris sur le groupe de Weyl de G, de certains produits scalaires calculés dans l'espace de cocaractères de G. Cette remarque m'a permis de proposer des formules conjecturales pour la dimension de *toutes* les variétés de Kisin $\mathcal{X}_\mu^G(b)$. En 2015, mon étudiant Charles Savel a démontré une partie de mes conjectures dans le cas du groupe $G = \left(\mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_p}\mathrm{GL}_d\right)_k$ et de l'élement b égal à l'élement neutre. Du point de vue de la théorie de Hodge p-adique, cette situation correspond aux déformations de la représentation triviale de dimension d de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ sans hypothèse sur K.

2 Algorithmique des nombres p-adiques

Au fil des recherches que je viens de présenter, j'ai pu observer à plusieurs occasions que les calculs qui apparaissent en théorie de Hodge p-adique sont souvent laborieux, voire

inextricables. C'est suite à cette constation que j'ai commencé à m'intéresser très sérieusement à l'algorithmique. Ci-dessous, je présente mes principales contributions dans le domaine en respectant l'ordre chronologique de manière à rendre le cheminement de ma recherche plus apparent.

2.1 Semi-simplifiée modulo p des représentations semi-stables

Références :
[15] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*
[17] X. Caruso, *Random matrices over a DVR and LU factorization*
[28] X. Caruso, D. Lubicz, *Semi-simplifiée modulo p des représentations semi-stables : une approche algorithmique*
[35] X. Caruso, D. Lubicz, *Algorithmics of $\mathfrak{S}_\nu$-modules*, librairie MAGMA
[36] X. Caruso, *Bounded series over ultrametric rings*, librairie SAGEMATH
[37] X. Caruso, *Lattices in semi-stable representations*, librairie SAGEMATH

Une première question de nature algorithmique sur laquelle j'ai travaillé a été celle du calcul de la semi-simplifiée modulo p des représentations semi-stables (voir aussi §1.2.2). Il s'agit d'une question importante dans le domaine qui a récemment reçu beaucoup d'attention en vertu du fait que les premiers résultats partiels dans cette direction ont été interprétés comme les premières preuves tangibles de l'existence d'une correspondance de Langlands p-adique. Néanmoins, même dans le cas le plus simple des représentations cristallines de dimension 2, les résultats actuels sont encore très partiels et c'est pour cette raison qu'il m'a semblé intéressant d'aborder le problème selon l'approche algorithmique. Avec David Lubicz, nous avons obtenu le résultat suivant :

Théorème 8. *Il existe un algorithme de complexité polynômiale qui prend en entrée un (φ, N)-module filtré admissible D (donné à une précision suffisamment grande) associée à une représentation semi-stable V et renvoie la semi-simplifiée modulo p de V (sous la forme d'une somme directe de puissances de caractères fondamentaux).*

L'algorithme dont le théorème précédent affirme l'existence fait un usage intensif de la théorie de Breuil–Kisin que nous avons présentée précédemment (voir §1.3). En plus de cela, il requiert deux ingrédients supplémentaires essentiels que nous avons développés pour l'occasion. Le premier est de nature théorique : c'est un résultat de surconvergence des modules de Breuil–Kisin qui, nous pensons, a un intérêt indépendant. Pour l'énoncer, introduisons pour tout réel $\nu > 0$, l'anneau

$$\mathfrak{S}_\nu = \left\{ \sum_{i=0}^{\infty} a_i u^i \quad \text{avec} \quad a_i \in K_0 \text{ et } v_p(a_i) + \nu i \geq 0, \forall i \geq 0 \right\}$$

Du point de vue de la géométrie, l'anneau $\mathfrak{S}_\nu$ est l'anneau des fonctions analytiques bornées par 1 sur le disque fermé de centre 0 et de rayon $p^{-\nu}$. La catégorie $\mathrm{Mod}^r_{/\mathfrak{S}_\nu}$ des modules de Breuil–Kisin de hauteur $\leq r$ sur $\mathfrak{S}_\nu$ est définie de manière évidente.

Théorème 9. *Pour tout $\nu \in [0, \frac{p-1}{per}[$, le foncteur d'extension des scalaires de $\mathfrak{S}_\nu$ à $\mathfrak{S}$ réalise une équivalence entre les catégories $\mathrm{Mod}^r_{/\mathfrak{S}_\nu}$ et $\mathrm{Mod}^r_{/\mathfrak{S}}$.*

Le second ingrédient qui intervient dans la preuve du théorème 8 est la conception d'une algorithmique efficace pour la manipulation des $\mathfrak{S}_\nu$-modules. Deux difficultés principales sont apparues à ce stade. La première d'entre elles est de nature théorique : elle est liée

au fait qu'il n'existe pas de théorème de structure pour les $\mathfrak{S}_\nu$-modules qui soit facilement exploitable au niveau algorithmique (et évite notamment l'explosion exponentielle de la taille des objets). La solution que nous avons retenue pour surmonter ce problème a été de travailler à quasi-isomorphisme près, c'est-à-dire d'identifier deux modules $M_1 \subset M_2$ lorsque le quotient M_2/M_1 est de longueur finie. En effet, il se trouve, d'une part, que (comme nous le montrons) cela n'a pas d'impact pour l'application que nous avons en vue et, d'autre part, qu'(une variante d')un théorème d'Iwasawa nous apprend que tout $\mathfrak{S}_\nu$-module de type fini est quasi-isomorphe à un $\mathfrak{S}_\nu$-module qui est aisément représentable sur machine.

La seconde difficulté que nous avons rencontrée est directement liée aux limitations des ordinateurs qui, ayant nécessairement une mémoire finie, ne peuvent travailler qu'avec des troncations d'éléments de $\mathfrak{S}_\nu$. Nous avons donc dû comprendre comment l'arithmétique de $\mathfrak{S}_\nu$ et des $\mathfrak{S}_\nu$-modules (à quasi-isomorphisme près) se transposait au niveau des approximations. Une conclusion intéressante de notre travail est que, sur ordinateur, il n'est pas possible de travailler à ν fixé : chaque calcul élémentaire sur les $\mathfrak{S}_\nu$-modules (somme, intersection, *etc.*) oblige à augmenter ν d'une valeur strictement positive. En ce sens-là, du point de vue algorithmique, le paramètre ν ne doit pas être considéré comme une donnée invariable du problème mais plutot comme une donnée de précision supplémentaire !

Ces préliminaires étant établis, nous pouvons maintenant présenter les grandes étapes de l'algorithme promis par le théorème 8 :

1. on calcule, à l'aide d'une formule explicite, le module de Breuil–Kisin « sous-convergent » $\mathfrak{M}_\nu[1/p]$ associé à V pour un paramètre ν suffisamment petit
2. on choisit un réseau L_0 dans $\mathfrak{M}_\nu[1/p]$ et on calcule la suite des (L_i) uniquement déterminée par les deux conditions suivantes :
   - pour tout i, L_i est un réseau dans $\mathfrak{M}_\nu[1/p]$ qui est libre sur $\mathfrak{S}_\nu$
   - pour tout i, L_{i+1} est quasi-isomorphe à $L_i + \phi(L_i)$

   jusqu'à ce que la suite stationne à une valeur limite notée L_∞
3. en utilisant des résultats de la thèse de Le Borgne, on calcule une décomposition isocline du ϕ-module L_∞/pL_∞ de laquelle on déduit directement $\bar{V}$.

Un point important à souligner est que la description précédente fait comme si la pente ν restait constante tout au long de l'exécution de l'algorithme alors que ce n'est pas le cas comme nous l'avons expliqué précédemment. En pratique, il faut donc en outre contrôler cet accroissement de la pente ν et faire constamment attention à ce qu'il ne dépasse pas la valeur critique $\frac{p-1}{per}$ donnée par le théorème 9. Nous montrons néanmoins que ceci est possible et que l'algorithme résultant reste de complexité polynômiale comme annoncé.

L'algorithme que je viens de décrire a été implanté en SAGEMATH par mes soins. Malheureusement, les premiers essais ont été plutôt décevants : ils n'ont, pour l'instant, pas permis d'aller beaucoup plus loin que les exemples qui avaient déjà été calculés à la main. La raison principale est liée à la précision requise qui atteint des valeurs indues — bien que, théoriquement, ne croissant que de façon polynômiale — dès les premiers exemples en dimension 2. C'est pour cette raison que j'ai commencé à m'intéresser sérieusement à l'étude fine et systématique du comportement de la précision p-adique lors de l'exécution de programmes informatiques. Je présente mes résultats dans ce domaine dans la partie §2.2 ci-dessous.

2.2 Une théorie de la précision p-adique

Références :
[16] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*
[18] X. Caruso, D. Roe, T. Vaccon, *p-adic stability in linear algebra*,
[24] X. Caruso, D. Roe, T. Vaccon, *Characteristic polynomial of p-adic matrices*,
[39] X. Caruso, D. Roe, T. Vaccon, ZpL *: lattice precision for p-adics*

Dans le §2.1, nous avons travaillé avec des séries p-adiques mais le problème de la précision se pose déjà avec les nombres p-adiques eux-mêmes. En effet, ceux-ci sont composés d'une infinité de « chiffres » et, à l'instar des séries, ils ne peuvent être stockés intégralement en machine. Ainsi, il est d'usage dans les logiciels de calcul formel de travailler avec des troncations qui prennent la forme $x + O(p^n)$ pour un certain entier n que l'on appelle la *précision absolue*. Ces troncations sont aisément manipulables. On a, par exemple :

$$\big(x_1 + O(p^{n_1})\big) + \big(x_2 + O(p^{n_2})\big) = x_1 + x_2 + O\big(p^{\min(n_1,n_2)}\big)$$

et il existe des formules analogues pour les autres opérations arithmétiques élémentaires : soustraction, multiplication, division. Cette manière de suivre la précision s'apparente à l'arithmétique d'intervalles utilisée avec les nombres réels et, malheureusement, elle surestime de la même manière les pertes de précision (bien que la norme p-adique ne soit pas archimédienne). Les mauvaises performances de l'algorithme du §2.1 s'expliquent, tout simplement, ainsi.

En collaboration avec David Roe et Tristan Vaccon, nous avons développé une alternative à cette « arithmétique d'intervalles » qui a l'avantage décisif de l'optimalité. L'idée directrice de notre travail consiste à grouper les variables et à modéliser la précision sur un groupement de d variables par un unique objet global, à savoir un $\mathbb{Z}_p$-réseau dans $\mathbb{Q}_p^d$. Concrètement, au lieu de travailler avec des expressions de la forme :

$$x_1 + O(p^{n_1}),\ x_2 + O(p^{n_2}),\ \ldots,\ x_d + O(p^{n_d}) \tag{4}$$

nous considérons des sous-ensembles de $\mathbb{Q}_p^d$ de la forme :

$$(x_1, \ldots, x_d) + H \tag{5}$$

où H est un $\mathbb{Z}_p$-réseau de $\mathbb{Q}_p^d$. Remarquons d'ores et déjà que cette nouvelle approche étend les méthodes traditionnelles ; en effet, les formules (4) et (5) encodent la même information dans le cas d'un réseau H diagonal (c'est-à-dire engendré par des multiples des vecteurs de la base canonique). Pour nous, l'intérêt de travailler avec ces structures plus générales est que celles-ci sont extrêmement stables par l'essentiel des opérations (élémentaires ou non-élémentaires) que l'on est amené à effectuer sur les nombres p-adiques. Précisément, David Roe, Tristan Vaccon et moi-même démontrons le théorème d'analyse ultramétrique suivant :

Théorème 10. *Soit $f : \mathbb{Q}_p^d \to \mathbb{Q}_p^n$ une application de classe C^1. Soit $\underline{x}$ un point de $\mathbb{Q}_p^d$ en lequel la différentielle de f, notée $f'(\underline{x})$, est surjective. Alors, pour tout réseau H de $\mathbb{Q}_p^d$ vérifiant certaines hypothèses techniques, on a :*

$$f(\underline{x} + H) = f(\underline{x}) + f'(\underline{x})(H).$$

Pour le problème qui nous occupe, il faut penser à la fonction f comme une opération d'arité d. Le théorème nous assure alors que si l'entrée $\underline{x} = (x_1, \ldots, x_d)$ n'est connue qu'à précision H, le résultat de l'opération à effectuer est connu à précision $f'(\underline{x})(H)$. L'égalité dans la conclusion du théorème assure en outre que ce résultat est optimal. Par ailleurs, on observera, à bon escient, que $f'(\underline{x})(H)$ reste un réseau dans $\mathbb{Q}_p^n$ sous l'hypothèse de surjectivité de $f'(\underline{x})$.

Les premières opérations auxquelles on peut penser sont l'addition, la soustraction, la multiplication et la division, bien entendu. Toutefois, le théorème s'applique pareillement avec des fonctions f nettement plus complexes, comme la fonction qui à une matrice associe son déterminant, ou encore celle qui à un système polynomial associe sa base de Gröbner réduite ! Toujours en collaboration avec David Roe et Tristan Vaccon, nous avons ainsi étudié la stabilité numérique de nombreuses opérations basiques en algèbre linéaire : produit de matrices, déterminant, polynôme caractéristique, intersection et somme de sous-espaces vectoriels, *etc.* Pour chacune de ces opérations, nous avons constaté que les pertes de précision théoriques (calculées par le théorème 10) étaient souvent très limitées, alors que les algorithmes classiques basés sur l'arithmétique d'intervalle usuelle conduisent souvent à des résultats beaucoup moins saillants (au moins lorsque ceux-ci sont appliqués sans une étude spécifique particulière préalable).

Ces constatations nous ont conduit à écrire une extension de SAGEMATH (actuellement proposée pour inclusion dans la distribution standard du logiciel [5]), le *package* `ZpL`, permettant d'effectuer un suivi automatique de la précision p-adique fondé sur le théorème 10. Mettant de côté les difficultés techniques qui apparaissent, l'idée que nous suivons est une traduction algorithmique directe de notre approche. À tout instant, notre *package* maintient à jour la liste $L = (x_1, \ldots, x_n)$ de toutes les variables p-adiques qui ont été affectées jusqu'alors et modélise la précision sur ce n-uplet par un réseau dans l'espace vectoriel $\bigoplus_{i=1}^n \mathbb{Q}_p dx_i$. La mise à jour du réseau de précision se fait à l'aide d'un procédé de différentiation automatique, conformément au résultat du théorème 10.

Sous des hypothèses standard de nature informatique, dites de *localité temporelle*, nous montrons que l'impact de notre suivi de précision sur la complexité est au plus quadratique, dans le sens où il transforme un algorithme de complexité c en un algorithme de complexité $O(c^2)$. En pratique, tout se passe bien tant que le nombre de variables mis en jeu reste modéré, disons en-deça de quelques centaines (ce qui couvre déjà de nombreuses applications). Au-delà de cette limite, des lenteurs commencent à se faire sentir. Nous sommes en train de travailler à l'optimisation du code dans l'espoir de repousser cette limite.

Une démonstration des possibilités et des performances du *package* est présentée sur ma page web : `http://xavier.toonywood.org/softwares/ZpL-demo.html`

2.3 La méthode de la précision adaptative

Références :
[16] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*
[23] X. Caruso, *Numerical stability of Euclidean algorithm over ultrametric fields*
[29] X. Caruso, *Computations with p-adic numbers*

Malheureusement, dans le cas d'un nombre de variables trop elévé, la méthode envisagée dans le numéro précédent ne peut être considérée comme réellement satisfaisante, ne serait-ce que parce que la taille du réseau de précision est elle-même beaucoup plus volumineuse que

5. Voir `https://trac.sagemath.org/ticket/23505`

la taille des variables elles-mêmes. Pour donner des éléments de réponse à ce problème, nous avons développé, à nouveau en collaboration avec David Roe et Tristan Vaccon, une stratégie que nous avons appelé la *méthode de la précision adaptative*.

Afin d'en esquisser les principes, imaginons que l'on soit en train d'exécuter un algorithme `F` consistant en une succession de n étapes $\mathtt{G}_1, \ldots, \mathtt{G}_n$. Si $f, g_1, \ldots, g_n$ sont les fonctions mathématiques calculées respectivement par $\mathtt{F}, \mathtt{G}_1, \ldots, \mathtt{G}_n$, on a l'égalité :

$$f = g_n \circ \cdots \circ g_2 \circ g_1.$$

Posons $f_i = g_i \circ \cdots \circ g_1$; il s'agit de la fonction mathématique qui rend compte de l'exécution des i premières étapes de l'algorithme. Remarquons que f_i prend ses valeurs dans l'espace vectoriel $\mathbb{Q}_p^{d_i}$ où d_i est le nombre de variables p-adiques restant en jeu après l'exécution de $\mathtt{G}_i$. Notons $\underline{x}_i = f_i(\underline{x})$. Par le théorème 10, nous savons (sous certaines hypothèses) que, si `F` est exécuté sur l'entrée $\underline{x} + H$, la précision optimale sur $\underline{x}_i$ est donnée par le réseau $H_i = f_i'(\underline{x})(H)$. Supposons à présent que l'on dispose, pour tout i, d'un réseau diagonal :

$$H_i' = p^{\mu_{i,1}}\mathbb{Z}_p \oplus p^{\mu_{i,2}}\mathbb{Z}_p \oplus \cdots \oplus p^{\mu_{i,d_i}}\mathbb{Z}_p$$

ayant la propriété suivante : l'exécution de l'étape $\mathtt{G}_i$ sur l'entrée $\underline{x}_i + H_i'$ (cela signifie que la j-ième coordonnée de $\underline{x}_i$ est donnée à précision $O(p^{\mu_{i,j}})$) renvoie une valeur $\underline{x}_{i+1} + H_{i+1}''$ avec $H_{i+1}'' \subset H_{i+1}$. Dans ces conditions, il suit du théorème 10 que l'algorithme 1 ci-dessous calcule $f(\underline{x} + H)$ à la précision optimale H_n.

Algorithme 1 : Version stabilisée de `F`

Entrée : $\underline{x}$ donné à précision H
Sortie : $f(\underline{x})$ correct à précision H_n

1 $\underline{x}_0 \leftarrow \underline{x}$
2 **for** $i = 0, \ldots, n-1$ **do**
3 **relever** (arbitrairement) $\underline{x}_i$ à la précision H_i'
4 $\underline{x}_{i+1} \leftarrow \mathtt{G}_i(\underline{x}_i)$ (calculé *via* l'arithmétique d'intervalles)
5 **return** $\underline{x}_n$

Pour ce qui concerne la construction des H_i', elle se fera généralement à l'aide d'arguments théoriques spécifiques au problème considéré. (Des méthodes de différentiation automatique peuvent également être envisagées mais celles-ci sont coûteuses et reviennent *in fine* à reproduire le travail de notre *package* `ZpL`.)

La terminologie « précision adaptative » est transparente au vu de l'algorithme 1 : à l'issue de chaque étape de l'exécution de `F`, on adapte la précision sur les valeurs calculées. Plus précisément, on augmente la précision sur ces valeurs de manière à compenser les pertes trop fortes provoquées par l'utilisation de l'arithmétique d'intervalles. Autrement dit, l'arithmétique d'intervalles nous garantit l'exactitude d'un certain nombre de chiffres mais... cela ne nous satisfait pas alors nous décidons que d'autres chiffres qui n'étaient *a priori* pas garantis sont également corrects. Ainsi formulé, il paraît surprenant que ce tour de passe-passe n'influence pas l'exactitude du résultat final ; c'est pourtant bel et bien le cas !

J'ai mis en pratique les idées précédentes dans deux cas concrets : l'algorithme d'élimination de Gauss pour le calcul de la décomposition LU et l'algorithme d'Euclide étendu pour le calcul du PGCD et des coefficients de Bézout. Dans le deux cas, pour une complexité qui n'en souffre

pas, on passe en moyenne d'une perte de précision qui croît linéairement avec la taille de l'entrée en une perte de précision qui grandit seulement de manière logarithmique en la taille de l'entrée ! Ces résultats me paraissent très prometteurs en vue de l'écriture d'une version stable de l'algorithme du §2.1 étant donné que les primitives de calcul constamment utilisées dans ce dernier algorithme sont justement des variantes de l'algorithme de Gauss, d'une part, et de l'algorithme d'Euclide, d'autre part.

En janvier 2017, j'ai été invité à donner un cours de 3h aux *Journées nationales de calcul formel* (JNCF) sur l'algorithmique des nombres p-adiques. Cela a été pour moi l'occasion de rédiger des notes de cours sur le sujet [29]. Bien que celles-ci soient déjà relativement fournies et documentées (plus de 80 pages), j'ai le projet de les compléter afin de les transformer en livre, qui pourrait servir de référence sur le sujet.

2.4 Structures p-adiques aléatoires

Références :
[17] X. Caruso, *Random matrices over a DVR and LU factorization*
[23] X. Caruso, *Numerical stability of Euclidean algorithm over ultrametric fields*
[27] X. Caruso, *Almost all non-archimedean Kakeya sets have measure zero*

Les derniers résultats que je viens de citer, concernant la stabilisation des algorithmes de Gauss et d'Euclide, décrivent le comportement d'un algorithme en moyenne. Afin de les établir de manière rigoureuse, j'en suis venu à m'intéresser aux matrices et aux polynômes p-adiques aléatoires. La notion d'aléatoire dans le cadre p-adique est facile à définir car $\mathbb{Z}_p$ est un groupe compact et hérite, par conséquent, d'une mesure de Haar qui est une mesure de probabilité. Concrètement, si les éléments de $\mathbb{Z}_p$ sont écrits sous la forme $\sum_{i=0}^{\infty} a_i p^i$ avec $a_i \in \{0, \dots, p-1\}$, les variables aléatoires a_i sont uniformément distribuées dans $\{0, \dots, p-1\}$ et indépendantes. Autrement dit, choisir un élément aléatoire de $\mathbb{Z}_p$ revient à choisir de manière indépendante chacun des a_i selon la mesure uniforme.

Matrices aléatoires p-adiques. Le premier exemple sur lequel je me suis attardé est celui de la factorisation LU. Étant donnée une matrice carrée aléatoire M de taille d à coefficients dans $\mathbb{Z}_p$, je me suis intéressé à la variable aléatoire V_L associant à une matrice $M \in M_d(\mathbb{Z}_p)$ l'opposé de la plus petite valuation d'un coefficient du facteur L de la décomposition LU de M. J'ai obtenu une description alternative simple de cette variable aléatoire, à partir de laquelle j'ai pu démontrer le théorème suivant :

Théorème 11. *L'espérance de V_L vaut $\log_q d + O(1)$ et son écart-type est borné par une constante universelle (qui peut être choisie égale à 7).*

Les pertes de précision logarithmiques annoncées à la fin du §2.2 découlent du théorème précédent.

Polynômes aléatoires p-adiques. Par la suite, je me suis intéressé aux polynômes p-adiques aléatoires. Plus précisément, j'ai étudié les variables aléatoires V_j donnant la valuation du j-ième sous-résultant scalaire de deux polynômes p-adiques aléatoires unitaires de degré fixé (car ce sont elles qui contrôlent les pertes de précision). J'obtiens une description de la loi de V_j en termes « combinatoires » :

Théorème 12. *Soient $X_0, \dots, X_{d-1}$ des variables aléatoires indépendantes suivant une loi géométrique de paramètre $(1 - p^{-1})$. Alors V_j suit la même loi que la variable aléatoire*

$$Y_j = \sum_{i=0}^{d} \min(X_{j-i}, X_{j-i+1}, \dots, X_{j+i})$$

où, par convention, $X_i = +\infty$ *if* $i < 0$ *et* $X_i = 0$ *if* $i \geq d$*. En particulier :*

- ☞ $\frac{1}{q-1} \leq \mathbb{E}[V_j] < \frac{q}{(q-1)^2}$
- ☞ $\frac{\sqrt{q}}{q-1} \leq \sigma[V_j] < \frac{q\sqrt{q+1}}{(q-1)^2}$
- ☞ $\mathbb{P}[V_j \geq m] \leq q^{-m+O(\sqrt{m})}$
- ☞ $\mathbb{E}[\max(V_0, \dots, V_{d-1})] \leq \log_q d + O(\sqrt{\log_q d})$

Je suis en train de rédiger un article plus complet sur le thème des polynômes p-adiques aléatoires, dans lequel j'étudie notamment le décompte et la répartition de leurs racines. Comme mise en bouche, j'y établis le résultat suivant (très simple mais surprenant au premier abord) :

Théorème 13. *Le nombre moyen de racines dans* $\mathbb{Q}_p$ *d'un polynôme* p*-adique aléatoire de degré* $d \geq 1$ *à coefficients dans* $\mathbb{Z}_p$ *est* 1 *(indépendamment de* d *et de* p*).*

J'obtiens également des extensions de ce théorème lorsque $\mathbb{Q}_p$ est remplacé par l'un de ces sous-ensembles (mesurables) ou par l'une de ses extensions finies ou infinies. Dans ce dernier cas, les racines ont tendance à se concentrer le long des sous-corps et je décris de façon explicite ces phénomènes.

Ensembles de Kakeya p*-adiques.* Dans un autre registre, et de manière plus anecdotique, je me suis récemment intéressé aux ensembles de Kakeya p-adiques aléatoires. Rappelons que, dans le cas réel, un ensemble de Kakeya est un sous-ensemble de $\mathbb{R}^d$ balayé par une aiguille de longueur 1 qui tourne de manière continue sur elle-même en passant par toutes les directions de l'espace. Besikovitch a démontré au début du 20ème siècle qu'il existe des ensembles de Kakeya de mesure arbitrairement petite. Les ensembles de Kakeya, qui sont ensuite restés un moment dans l'oubli, connaissent une seconde jeunesse depuis plusieurs décennies en raison des liens étroits qu'ils entretiennent avec certaines problèmes centraux en analyse harmonique.

En particulier, la question de Kakeya a été posée sur d'autres corps ; le cas le plus célèbre est probablement celui des corps finis [6] mais le cas des corps non archimédiens a également été évoqué par Wolff puis repris par Ellenberg, Oberlin et Tao. Dans le cas de $\mathbb{Q}_p$, la question peut se formuler ainsi : existe-t-il une fonction *continue* $f : \mathbb{S}^{d-1}(\mathbb{Q}_p) \to \mathbb{Q}_p^d$ (où $\mathbb{S}^{d-1}(\mathbb{Q}_p)$ est la sphère unité de $\mathbb{Q}_p^d$ pour la norme infinie) pour laquelle l'ensemble

$$K(f) = \big\{ta + f(a) \ : \ a \in \mathbb{S}^{d-1}(\mathbb{Q}_p),\, t \in \mathbb{Z}_p\big\}$$

soit de mesure nulle. Dummit et Hablicsek ont apporté une réponse positive en exhibant une fonction f particulière répondant à la question. De mon côté, j'ai considéré la question sous un angle probabiliste et ai obtenu le théorème suivant :

Théorème 14. *Pour presque toute fonction* 1*-lipschitzienne* $f : \mathbb{S}^{d-1}(\mathbb{Q}_p) \to \mathbb{Z}_p^d$*, l'ensemble* $K(f)$ *est de mesure nulle.*

6. Sur les corps finis, la question se formule ainsi : existe-t-il une constante c_d pour laquelle tout sous-ensemble de $\mathbb{F}_q^d$ contenant une droite affine dans chaque direction a au moins $c_d q^d$ éléments. Dans un article célèbre, Dvir a apporté une réponse affirmative à cette question (avec $c_d = \frac{1}{d!}$) grâce à ce que l'on appelle désormais la *méthode polynômiale*.

3 Polynômes de Ore et équations différentielles

Les polynômes de Ore sont une variante non commutative des polynômes usuels : si R est un anneau muni d'un endomorphisme $\theta : R \to R$ et d'une θ-dérivation [7] ∂, l'anneau de Ore $R[X, \theta, \partial]$ est identique à l'anneau des polynômes usuels sur R sauf que la multiplication (non commutative, en général) est régie par la règle $Xa = \theta(a)X + \partial(a)$ pour $a \in R$. Ces polynômes sont apparus à plusieurs reprises lors de mes recherches. En effet, lorsque $\partial = 0$, ils entretiennent un lien étroit avec l'algèbre semi-linéaire dont la théorie de Hodge p-adique est friande. Au contraire, lorsque $\theta = \mathrm{id}$, les polynômes de Ore sont liés aux équations différentielles linéaires qui entretiennent, elles aussi, des liens étroits avec la théorie de Hodge p-adique.

Les propriétés de factorisation des polynômes de Ore sont particulièrement intéressantes car elles sont le reflet de théorèmes de décomposition de φ-modules ou de modules à connexions. En particulier, du point de vue algorithmique (et parfois aussi théorique), il peut être avantageux d'attaquer ces questions de décomposition sous l'angle des polynômes de Ore qui sont généralement plus facilement manipulables.

3.1 Factorisation des polynômes de Ore sur les corps finis

Références :
[21] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields*
[25] X. Caruso, J. Le Borgne, *Fast multiplication for skew polynomials over finite fields*
[34] X. Caruso, *Skew polynomials over finite fields*, librairie SAGEMATH

Soient $\mathbb{F}_q$ un corps fini de cardinal q et θ un automorphisme de $\mathbb{F}_q$. Concrètement, θ est une puissance du Frobenius : si $q = p^n$ (où p est un nombre premier et n est un entier), on a $\theta(x) = x^{p^s}$ où s est un entier défini modulo n. Dans la suite, on appelle r l'ordre de θ. Le sous-corps de $\mathbb{F}_q$ fixé par θ est ainsi $\mathbb{F}_{p^{n/r}}$; on le notera également $\mathbb{F}_q^{\theta=1}$. Avec Jérémy Le Borgne, nous avons étudié la factorisation dans l'anneau de Ore $\mathbb{F}_q[X, \theta, 0]$, que l'on notera plus simplement $\mathbb{F}_q[X, \theta]$ dans la suite. Notre motivation première était l'étude algorithmique des $\mathbb{F}_p$-représentations galoisiennes d'un corps p-adique (*via* l'équivalence de catégories de Katz) mais les résultats que nous avons obtenus sortent largement de ce cadre et il nous a semblé nettement plus intéressant de les replacer et de les énoncer dans le langage des polynômes de Ore. Le point culminant de notre travail est le résultat suivant (pour lequel on utilise les notations de complexité usuelles : $\tilde{O}$ signifie que les termes logarithmiques ont été cachés et ω désigne l'exposant de la multiplication des matrices) :

Théorème 15. *Il existe un algorithme de complexité $\tilde{O}(dr^\omega \cdot \log q)$ (opérations binaires) qui ramène la factorisation d'un polynôme de Ore $P \in \mathbb{F}_q[X, \theta]$ de degré d à la factorisation commutative d'un polynôme de degré d dans $\mathbb{F}_q^{\theta=1}[X]$.*

Ce théorème constitue une amélioration considérable en comparaison des résultats de factorisation qui étaient connus jusqu'alors dont la complexité vis-à-vis de d était en $\tilde{O}(d^4)$. Sachant que les meilleurs algorithmes connus pour la factorisation commutative ont actuellement une complexité quasi-linéaire en $d^{3/2}$, on observe en outre que l'algorithme que nous obtenons a une complexité qui, lorsque r est petit, est théoriquement plus performant que la factorisation commutative !

7. Une θ-dérivation ∂ est une application additive vérifiant la règle de Leibniz tordue $\partial(ab) = \theta(a)\partial(b) + b\partial(a)$.

Les ingrédients que nous utilisons pour démontrer le théorème 15 sont, à la fois, de nature théorique et algorithmique. Du point de vue théorique, nous nous basons sur un vieux théorème d'Ikehata qui affirme que $\mathbb{F}_q[X,\theta]$ est une algèbre d'Azumaya sur son centre $\mathbb{F}_q^{\theta=1}[X^r]$. Par la théorie générale des algèbres d'Azumaya, on dispose ainsi d'une norme réduite $\mathcal{N} : \mathbb{F}_q[X,\theta] \to \mathbb{F}_q^{\theta=1}[X^r]$. Avec Le Borgne, nous démontrons que l'application $\mathcal{N}$ possède des propriétés décisives en lien avec la factorisation. La proposition suivante en fournit un exemple simple.

Proposition 16. *Soit $P \in \mathbb{F}_q[X,\theta]$. Soit N un diviseur irréductible (dans le centre) de $\mathcal{N}(P)$. On suppose que N^2 ne divise pas $\mathcal{N}(P)$. Alors le* PGCD *à droite de P et de N est un diviseur irréductible à droite de P.*

Dans le cas où $\mathcal{N}(P)$ est un polynôme séparable, la proposition 16 permet de déterminer une factorisation complète de P de la manière suivante : (1) on écrit $\mathcal{N}(P) = N_1 N_2 \cdots N_\ell$ où les N_i sont des polynômes centraux irréductibles deux à deux distincts, (2) on extrait un facteur irréductible à droite P_ℓ de P en calculant le PGCD de N_ℓ et de P et (3) on applique récursivement le même procédé à partir du polynôme P/P_ℓ dont la norme réduite est $\mathcal{N}(P)/N_\ell = N_1 N_2 \cdots N_{\ell-1}$. De manière intéressante, remarquons que puisque les N_i vivent dans le centre, ils peuvent être permutés entre eux, de sorte que l'on a également $\mathcal{N}(P) = N_{\sigma(1)} \cdots N_{\sigma(\ell)}$ pour toute permutation σ de $\{1,\dots,\ell\}$. On obtient ainsi non seulement une factorisation de P mais, mieux encore, $\ell!$ factorisations différentes de P correspondant aux $\ell!$ permutations de $\{1,\dots,\ell\}$. Il se trouve de surcroît que ces $\ell!$ factorisations épuisent toutes les factorisations de P.

Les véritables difficultés commencent lorsque $\mathcal{N}(P)$ n'est pas séparable. Dans ce cas, nous nous servons de toute la puissance des algèbres d'Azumaya afin de ramener la question de la factorisation qui nous préoccupe à des problèmes concrets d'algèbre linéaire, que nous parvenons à résoudre dans un second temps.

En ce qui concerne les aspects purement algorithmiques, nous développons toute une technologie pour le calcul rapide sur les polynômes de Ore. Comme souvent, la brique de base est la multiplication pour laquelle nous proposons un algorithme de complexité $\tilde{O}(dr^{\omega-1})$ (si $d \geq r$). À nouveau, les résultats théoriques qui sous-tendent cet algorithme sont liés à la structure d'algèbre d'Azumaya de $\mathbb{F}_q[X,\theta]$. À partir de là, nous adaptons les techniques usuelles valables dans le cadre commutatif et déduisons ainsi des algorithmes rapides (de complexité quasi-linéaire en le degré) pour toutes les opérations arithmétiques classiques : division euclidienne, PGCD, *etc.*

J'ai réalisé une implémentation des algorithmes présentés ci-dessus pour le logiciel de calcul formel SAGEMATH, disponible sous forme de librairie. Une partie de cette librarie (revue par Arpit Merchant et Johan Rosenkilde) a été incluse dans la distribution standard de SAGEMATH.

3.2 Sur la p-courbure des équations différentielles

Références :

[1] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the characteristic polynomial of the p-curvature*

[2] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the p-curvature*

[3] A. Bostan, X. Caruso, É. Schost, *Computation of the similarity class of the p-curvature*

Si k est un corps de caractéristique p, l'anneau de Ore $k(x)[\partial, \mathrm{id}, \frac{d}{dx}]$ — noté plus traditionnellement $k(x)\langle\partial\rangle$ — jouït de propriétés analogues à $\mathbb{F}_q[X,\theta]$; par exemple, ce sont

tous les deux des algèbres d'Azumaya et ils sont en particulier tous les deux munis d'une norme réduite. Il m'est ainsi très vite apparu tentant de voir si les méthodes que nous avions développées avec Le Borgne dans le cadre de $\mathbb{F}_q[X, \theta]$ pouvaient s'étendre aux opérateurs différentiels.

La clé m'est apparue après une discussion avec Alin Bostan qui s'intéressait au calcul rapide de la p-courbure. Rappelons que la p-courbure est un invariant de première importance associé à un polynôme différentiel $L \in k(x)\langle\partial\rangle$: il s'agit d'un endomorphisme linéaire qui, d'une part, reflète les propriétés de factorisation de L et, d'autre part, mesure la taille de l'espace des solutions de l'équation différentielle $L(f) = 0$ (c'est-à-dire, si l'on préfère, mesure le défaut au théorème de Cauchy–Lipschitz en caractéristique positive). En collaboration avec Alin Bostan et Éric Schost, nous avons mis en évidence un lien profond entre norme réduite et p-courbure, en démontrant le théorème suivant :

Théorème 17. *Pour $L \in k(x)\langle\partial\rangle$, la norme réduite $\mathcal{N}(L)$ s'identifie, à une renormalisation près, au polynôme caractéristique de la p-courbure de L.*

Forts de ce résultat, nous avons commencé à explorer les applications potentielles à l'algorithmique. En démontrant un analogue du théorème 17 dans le cas des équations aux récurrences, nous avons réussi à ramener le calcul du polynôme caractéristique de la p-courbure d'un opérateur L à celui d'une factorielle de matrices pour lequel des algorithmes efficaces étaient disponibles dans la littérature. Ceci nous a permis de concevoir un algorithme de calcul du polynôme caractéristique de la p-courbure dont la complexité vis-à-vis de p est quasi-linéaire en $\sqrt{p}$. Il s'agit d'un résultat remarquable car la taille de la p-courbure elle-même grandit généralement de manière linéaire par rapport à p (alors que celle de son polynôme caractéristique n'est qu'en $O(\log p)$) ; en particulier, notre algorithme évite le calcul de la p-courbure. Notons, en outre, qu'avant notre algorithme, la meilleure complexité connue pour le calcul du polynôme caractéristique de la p-courbure était à peine sous-quadratique en p.

Avec les mêmes auteurs, nous nous sommes par la suite intéressés au calcul « complet » de la p-courbure et avons obtenu, par des méthodes différentes, un algorithme quasi-optimal pour ce problème. Notre stratégie consiste à plonger $k(x)$ dans un anneau de séries formelles à puissances divisées sur lequel on dispose d'un analogue du théorème de Cauchy–Lipschitz. La p-courbure s'interprète alors en termes d'un système fondamental de solutions et peut-être calculée efficacement *via* une itération de Newton. Il est à noter que l'algorithme résultant est fortement parallélisable et s'étend sans diffilculté supplémentaire aux systèmes différentiels quelconques. Dans un troisième volet de ce travail, nous avons adapté la méthode esquissée ci-dessus aux invariants de similitude de la p-courbure pour lesquels nous obtenons un algorithme de calcul ayant à nouveau une complexité quasi-linéaire en $\sqrt{p}$.

3.3 Factorisation par les pentes de polynômes de Ore

Références :
[20] X. Caruso, D. Roe, T. Vaccon, *Euclidean division and factorization of p-adic polynomials*
[31] X. Caruso, *Slope factorization of Ore polynomials*

Les polygones de Newton sont un outil très classique dans le monde ultramétrique qui apparaissent dans la littérature dans des contextes très différents, par exemple pour l'étude des équations algébriques p-adiques, des φ-modules, des équations différentielles p-adiques

ou complexes, des équations aux différences, des équations de Mahler, *etc.* Malgré tout, à ma connaissance, une théorie suffisamment générale des polygones de Newton qui arriverait à englober tous les exemples précédemment cités manquait à l'appel. Pourtant une telle approche unificatrice me paraît extrêmement intéressante car elle permettrait de créer un lien très concret entre diverses questions qui ont déjà fait l'objet de nombreux travaux avec l'espoir non dissimulé de favoriser une circulation efficace, voire automatique, des méthodes développées dans ces différents contextes.

Or, le lien entre tous les exemples que j'ai cités précédemment s'établit concrètement au niveau des polynômes de Ore. Il m'a donc semblé intéressant de développer une théorie générale des polygones de Newton pour les polynômes de Ore définis sur des corps ultramétriques complets. Il se trouve que, dans le cas des corps, il est possible de découpler entièrement les deux données θ et ∂. On est ainsi ramené à considérer séparément les deux cas $K[X,\theta]$ et $K[X,\partial]$. Dans chacune de ces situations, j'ai donné une construction générale des polygones de Newton associés aux polynômes de Ore. De manière très brève, disons que, si $P=\sum_{i=0}^d a_iX^i$, le polygone de Newton $\mathrm{NP}(P)$ de P s'obtient en considérant l'enveloppe convexe dans le plan de points A_i associés à chacun de monômes a_iX^i ainsi que de certains points supplémentaires à l'infini D_j. Mentionnons toutefois que la définition précise des A_i et des D_j présente quelques subtilités. Ceci étant posé, je démontre des propriétés de multiplicativité des polygones de Newton et j'étudie leur comportement vis-à-vis de la division euclidienne. Je me penche ensuite sur la factorisation pour laquelle j'obtiens le résultat suivant :

Théorème 18. *Soit $P=\sum_{i=0}^n a_iX^i \in K[X,\bullet]$. Supposons que le point A_d (pour un certain $d\in\{0,\dots,n\}$) correspondant au monôme a_dX^d soit un point extrémal de* $\mathrm{NP}(P)$. *Alors la suite $(A_i)_{i\geq 0}$ défini par :*

$$\begin{aligned} A_0 &= \sum_{i=0}^{d} a_iX^i \\ A_{i+1} &= A_i + (\textit{reste de la division euclidienne à droite de } P \textit{ par } A_i) \end{aligned}$$

converge vers une limite A_∞ vérifiant les deux propriétés suivantes :

- ☞ *A_∞ est un diviseur à droite de P, et*
- ☞ *le polygone de Newton de A_∞ s'identifie avec la partie de* $\mathrm{NP}(P)$ *située à gauche de la droite verticale passant par A_d*

Remarque. Lorsque l'anneau de Ore $K[X,\bullet]$ admet une division euclidienne à gauche (c'est-à-dire lorsque θ est bijectif), on dispose d'un analogue du théorème précédent qui assure l'existence d'un diviseur à gauche de P dont le polygone de Newton correspond — mais n'est généralement pas égal — à la partie de $\mathrm{NP}(P)$ située à gauche de la droite verticale passant par A_d.

La démonstration du théorème 18 que je propose frappe par sa simplicité conceptuelle : elle consiste à estimer les polygônes de Newton des différences $A_{i+1}-A_i$ et de montrer que ceux-ci montent vers l'infini. La clé pour y parvenir est un lemme donnant une minoration du polygone de Newton du reste dans une division euclidienne ; à nouveau, cela se fait de manière directe et pédestre en estimant séparément la contribution de chaque monôme du dividende. Il est à noter, cependant, que la convergence de la suite (A_i) du théorème 18 est relativement lente. Dans certains cas favorables, précisément lorsque le centre de $K[X,\bullet]$ est

d'indice fini, nous démontrons toutefois qu'il est possible (au prix d'efforts supplémentaires non négligeables) d'accélérer cette convergence jusqu'à la rendre quadratique, retrouvant ainsi la vitesse d'un schéma classique de Newton. Cette amélioration est importante pour les applications algorithmiques éventuelles.

Le théorème 18 présente plusieurs atouts. Tout d'abord, celui de la généralité. En effet, en considérant les bons anneaux de polynômes de Ore, il redonne et complète par spécialisation de nombreux résultats classiques de décomposition portant sur les extensions algébriques, l'algèbre semi-linéaire p-adique, les représentations galoisiennes, les modules à connexions... Le deuxième atout décisif du théorème 18 est celui de la simplicité qui autorise son utilisation du point de vue algorithmique, là où les démonstrations connues précédemment étaient souvent difficiles à rendre effectives. C'est ainsi que, par exemple, je suis parvenu, à partir du seul énoncé du théorème 18, à obtenir des algorithmes stables et efficaces, d'une part, pour le calcul de la décomposition de Dieudonné–Manin et, d'autre part, pour le calcul des rayons de convergence d'une équation différentielle p-adique.

3.4 Article de synthèse sur les polynômes de Ore

Référence :
[30] X. Caruso, *Polynômes de Ore en une variable*

Les polynômes de Ore sont des objets relativement classiques du calcul formel qui avaient déja été étudiés par de nombreux auteurs. Le point de vue que mes coauteurs et moi-même avons adopté sur le sujet est cependant original. En effet, il fait la part belle aux constructions mathématiques raffinées (telles les algèbres d'Azumaya) alors que les optimisations précédentes étaient plus souvent de nature algorithmique. Selon moi, c'est bel et bien cette innovation conceptuelle qui nous a permis de repousser aussi loin les barrières de complexité sur lesquelles les algorithmiciens butaient jusqu'alors.

Pour cette raison, il m'a semblé utile de rédiger des notes de cours [30] sur le sujet. J'y mets en place posément les bases de la théorie des algèbres simples centrales et celles des algèbres d'Azumaya. Puis, dans un second temps, je démontre leur efficacité pour l'étude aussi bien théorique qu'algorithmique des polynômes de Ore. J'ai choisi une présentation pédagogique, illustrée par de nombreux exemples et qui évite au maximum les prérequis, en particulier la topologie étale ou la notion de séparabilité dans les algèbres non commutatives. J'espère ainsi être accessible au plus grand nombre et notamment aux informaticien(ne)s et aux mathématicien(ne)s qui n'auraient pas suivi de formation préalable en géométrie algébrique ou en algèbre non-commutative générale.

4 Bref résumé des autres activités

En plus de mon activité de recherche, je consacre une partie significative de mon temps à d'autres activités : enseignement, diffusion des mathématiques, organisation de conférences, gestion de projet, responsabilités collectives.

4.1 Enseignement de la licence au doctorat

J'aime enseigner et je choisis chaque année d'y consacrer une partie de mon temps en fonction des besoins de mon UFR. Ainsi :

- ☞ j'ai donné trois cours d'école doctorale : (1) *Aspects algébriques de la théorie de Hodge p-adique*, (2) *Analyse, probabilités et informatique avec les nombres p-adiques*, (3) *Polynômes de Ore en une variable* ;
- ☞ j'ai dispensé trois cours au niveau master : *Corps locaux*, *Algorithmique de base* et *Algèbre commutative, géométrie algébrique* ;
- ☞ je participe, en moyenne une année sur deux, à la préparation à l'agrégation (en encadrant des leçons et/ou en faisant passer des oraux blancs) ;
- ☞ il m'arrive occasionnellement de donner des cours et des TD au niveau licence ; cette année, par exemple, j'ai donné un cours d'introduction aux codes correcteur d'erreurs pour les éléves de première année de l'ENS de Rennes, parcours informatique.

En outre, de 2011 à 2016, j'ai fait partie du comité de pilotage du master de cryptographie de l'universite de Rennes. J'ai également participé à la conception de l'offre de cours de M2 en géométrie en 2014 en lien avec le semestre thématique de géométrie du Centre Henri Lebesgue (CHL) que je supervisais. J'encadre de plus chaque année le stage d'un ou de plusieurs étudiants dont la durée moyenne avoisine les deux mois et dont le niveau a varié du L2 au M2.

4.2 Étudiants en thèse

Depuis la soutenance de mon habilitation à diriger les recherches en 2011, j'ai encadré trois thèses.

La thèse de Jérémy Le Borgne (coencadrée avec David Lubicz). L'objectif de la thèse était de concevoir un algorithme de calcul de la semi-simplifiée d'une représentation du groupe de Galois absolu d'un corps p-adique à coefficients dans un corps fini $\mathbb{F}_q$. Pour cela, Jérémy a mis au point un algorithme de décomposition des φ-modules sur le corps de séries de Laurent $\mathbb{F}_q((u))$. Ceci l'a conduit, d'une part, à mener une étude fine du comportement de la la précision u-adique puis, une fois ce problème résolu, à se concentrer sur la classification (théorique et effective) des φ-modules sur le corps $\mathbb{F}_q$ lui-même. C'est ainsi que nous en sommes venus à la factorisation des polynômes de Ore sur les corps finis.

Jérémy a soutenu sa thèse en avril 2012. Il a maintenant un poste d'agrégé préparateur à l'ENS de Rennes.

La thèse de Tristan Vaccon. Le contexte de la thèse était l'étude de la précision p-adique. Sa thèse comporte deux volets. Il a, d'autre part, en collaboration avec moi-même et David Roe, élaboré la théorie de la précision p-adique que j'ai présentée dans ce document aux §§2.2–2.3. D'autre part, il s'est longuement intéressé au calcul des bases de Gröbner p-adiques (et aux questions de précision afférentes) : il a étudié la stabilité numérique des algorithme F5 et FGLM, en a proposé des améliorations dans le contexte p-adique, et a développé en parallèle une approche tropicale, nettement plus stable, dans laquelle la contribution de la valuation p-adique est prise en compte.

Tristan a soutenu sa thèse en juillet 2015. Il est maintenant maître de conférences à l'université de Limoges.

La thèse de Charles Savel. Le contexte de la thèse était l'étude des variétés de Kisin, faisant suite au travail que j'ai présenté au §1.4. Charles s'est concentré sur le cas des groupes

réductifs obtenus par restriction des scalaires à la Weil à partir du groupe GL_d. Pour ces groupes particuliers, il a établi des formules approchées pour la dimension des variétés de Kisin correspondantes, en accord avec les conjectures que j'avais énoncées.

Charles a soutenu sa thèse en octobre 2015. Il est maintenant enseignant (vacataire) en mathématiques.

4.3 Diffusion des mathématiques

La diffusion des mathématiques fait partie des missions des chargés de recherche et je m'y investis assurément notamment par le biais des actions menées par *Animath* et *Cap'Maths*. Ci-après, je liste mes principales activités dans cette direction.

Depuis plus de 15 ans, je participe (avec plus ou moins d'assiduité selon les périodes) à la préparation de la délégation française aux diverses compétitions olympiques de mathématiques. J'ai rédigé dans ce cadre de nombreuses feuilles d'exercices ainsi que plusieurs cours et ai participé, en tant qu'animateur, à de nombreux stages d'entrainement.

Avec Jos Leys, j'ai réalisé en 2009 un film d'animation d'une demi-heure intitulé *Mais où est donc le petit côté ?* dont l'objectif est de présenter puis d'expliquer le phénomène de réfraction de la lumière. Le film s'adresse à tous les publics et, en particulier, aux lycéens.

Depuis mon arrivée à Rennes, je participe régulièrement à la fête de la science et au festival des sciences. Dans ce cadre, je donne un exposé de vulgarisation pour le grand public ou j'interviens auprès des scolaires (primaire, collège ou lycée) environ une fois par an.

Entre 2011 et 2013, j'ai participé à l'élaboration et à l'animation de trois stages MathC2+ qui ont eu lieu à l'actuelle ÉNS de Rennes.

Depuis la création de la revue, je propose régulièrement des articles et des billets pour *Images des Mathématiques*. Depuis 2013, j'en suis également éditeur.

En 2017, j'ai participé à l'organisation de l'édition rennaise du *Forum des mathématiques vivantes* (événement national mis en place sous l'impulsion de la *Commission Française pour l'Enseignement des Mathématiques*).

Je fais partie du comité d'organisation d'une école mathématique d'été pour jeunes brillants mathématiciens en herbe (entre 15 et 19 ans) en provenance du monde entier. L'école aura lieu à l'ENS de Paris du 16 au 27 juillet 2018.

4.4 Responsabilités collectives et administration de la recherche

4.4.1 Coordination de projets

De 2009 à 2014, j'ai été le coordinateur principal du projet ANR *Calculs effectifs en théorie de Hodge p-adique* (CETHop). À ce titre, j'ai notamment organisé deux conférences internationales, des *Sage Days* ainsi que plusieurs rencontres de travail.

J'ai, cette année, soumis, en tant de coordinateur, un nouveau projet ANR *Correspondance de Langlands p-adique : une approche constructive et algorithmique* (CLap–CLap). Le projet fait intervenir trois nœuds (Rennes, Paris et Lyon) et regroupe une vingtaine de chercheuses et de chercheurs.

4.4.2 Organisation de séminaires

J'ai participé à l'organisation de l'exposition, de la semaine de colloque et de l'après-midi grand public qui ont eu lieu à l'IHP en 2011 à l'occasion du bicentenaire de la naissance

d'Évariste Galois. Pour l'occasion, j'ai rédigé plusieurs articles de vulgarisation sur les idées de Galois.

Depuis 2011, je suis un des principaux organisateurs du séminaire *Mathematic Park* qui réunit une fois par mois à l'IHP une centaine d'étudiants et d'enseignants de la région parisienne pour un exposé dont l'objectif est de présenter, à leur niveau, un domaine de recherche actuel des mathématiques. Depuis un an, j'organise une version rennaise de ce sémaine, destinée aux étudiants de licence et intitulée *Mathematic World*.

En 2014, j'ai été l'un des principaux organisateurs du semestre thématique de géométrie du centre Henri Lebesgue (CHL) et j'ai notamment significativement contribué à l'organisation de l'école de printemps sur les théories de Hodge classique et p-adique qui a réuni plus de 100 participants sur deux semaines à Rennes. À cette occasion, je me suis également beaucoup investi dans la programmation du site web `www.lebesgue.fr` : j'ai réalisé une interface permettant de créer automatiquement un site web pour une conférence puis de gérer les inscriptions, la facturation, *etc*.

Depuis 2015, je suis coorganisateur du séminaire filmé *Les 5 minutes Lebesgue* dont l'objectif est de réaliser des petits clips vidéo de cinq minutes qui présentent la variété des mathématiques qui intéressent les membres du CHL.

Je suis coorganisateur de la conférence internationale *Numerical methods for algebraic curves* qui aura lieu à Rennes du 19 au 23 février, dans le cadre d'un semestre thématique du CHL. Lors de cette conférence, une journée spéciale sera consacrée aux méthodes p-adiques.

Enfin, je suis coorganisateur des *Journées Louis Antoine* à Rennes et du séminaire de l'équipe *Géométrie et algèbre effectives*.

4.4.3 Responsabilités

J'ai été d'octobre 2012 à septembre 2016 membre élu du comité national de la recherche scientifique (CoNRS). À ce titre, j'ai participé à l'évaluation des chercheurs CNRS et au comité de recrutement des différents concours CNRS. J'ai également présidé le comité d'évaluation du GDS *Mathrice* et ai participé aux comités HCERES pour l'évaluation de l'*Institut mathématique de Bordeaux* (IMB), du *Laboratoire de mathématique Nicolas Oresme* (LMNO) à Caen et de l'*Institut Élie Cartan de Lorraine* (IECL) à Nancy et à Metz.

J'ai participé à plusieurs comités de sélection, j'ai une activité de *referee* régulière et j'ai été rapporteur de quatre thèses.

De 2012 à 2016, j'ai été membre nommé du conseil de laboratoire du l'*Institut de recherche en mathématiques de Rennes* (IRMAR).

Depuis 2016, je suis membre du comité de pilotage des *États de la recherche* de la SMF.

4.4.4 Les Annales Henri Lebesgue

Nous le savons, les problèmatiques de l'édition scientifique occupent une place de plus en plus importante dans les inquiétudes de la communauté mathématique. Récemment, de nombreux collègues ont signé l'appel de Jussieu pour la science ouverte et la bibliodiversité ; le conseil scientifique du CNRS a diffusé un certain nombre de recommandations à propos du droit d'auteur, de l'archivage, *etc.* ; plusieurs universités ont résilié leur abonnement Springer, ce qui a permis une évolution des négociations portées par le collectif Couperin.

Dans le périmètre du centre Henri Lebesgue, nous sommes également très sensibles à ces préoccupations et, afin d'apporter notre contribution au combat contre les éditeurs commer-

ciaux, nous avons très récemment lancé une nouvelle revue aux pratiques « vertueuses » : les Annales Henri Lebesgue. Cette revue est généraliste (mathématiques pures et appliquées) et purement électronique. Elle est entièrement gratuite pour l'auteur et le lecteur. Elle est dirigée par des collègues, qui ont pour uniques objectifs la diffusion, la valorisation et l'archivage des travaux mathématiques.

À titre personnel, je suis éditeur des Annales Henri Lebesgue et également coordinateur du pôle géométrie de la revue. Depuis le mois de septembre, je me suis énormément investi pour que cette revue puisse naître et prospérer dans les meilleures conditions ; en particulier, je suis l'un des principaux auteurs du site web `annales.lebesgue.fr`, je suis coauteur d'un article d'annonce à paraître dans la Gazette des Mathématiciens [33] et j'ai réalisé un clip publicitaire de 4 minutes pour faire la promotion de la revue [40].

Je ne peux donc que vous encourager à y soumettre vos meilleurs articles `:-)`.

Liste de publications, prépublications et production logicielle

[1] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the characteristic polynomial of the p-curvature*, proceddings de la conférence ISSAC 2014

[2] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the p-curvature*, proceddings de la conférence ISSAC 2015

[3] A. Bostan, X. Caruso, É. Schost, *Computation of the similarity class of the p-curvature*, proceddings de la conférence ISSAC 2016

[4] A. Bostan, X. Caruso, G. Christol, P. Dumas, *Fast computation of the N-th term of an algebraic series in positive characteristic*, en préparation

[5] X. Caruso, *Représentations semi-stables de torsion dans le cas $er < p-1$*, J. reine angew. Math. **594** (2006), 35–92

[6] X. Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), 629–699

[7] X. Caruso, D. Savitt, *Polygones de Hodge, de Newton et de l'inertie modérée des représentations semi-stables*, Math. Ann. **343** (2009), 777–789

[8] X. Caruso, T. Liu, *Quasi-semi-stable representations*, Bull. Soc. Math. France **137** (2009), 185–223

[9] X. Caruso, *Sur la classification de quelques φ-modules simples*, Mosc. Math. J. **9** (2009), 562–568

[10] X. Caruso, D. Savitt, *Poids de l'inertie modérée de certaines représentations cristallines*, J. Théor. Nombres Bordeaux **22** (2010), 79–96

[11] X. Caruso, *Classification of integral models of $(\mathbb{Z}/p^2\mathbb{Z})_K$ via Breuil-Kisin theory*, J. of Algebra **323** (2010), 1955–1957

[12] X. Caruso, T. Liu, *Some bounds for ramification of p^n-torsion semi-stable representations*, J. of Algebra **325** (2011), 70–96

[13] X. Caruso, *$\mathbb{F}_p$-représentations semi-stables*, Ann. Inst. Fourier **61** (2011), 1683–1747

[14] X. Caruso, *Représentations galoisiennes p-adiques et (φ,τ)-modules*, Duke Math. J. **162** (2013), 2525–2607

[15] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*, LMS J. Comput. Math. **17** (2014), 302–344

[16] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*, LMS J. Comput. Math. **17** (2014), 274–294

[17] X. Caruso, *Random matrices over a DVR and LU factorization*, J. Symbolic Comput. **71** (2015), 98–123

[18] X. Caruso, D. Roe, T. Vaccon, *p-adic stability in linear algebra*, proceddings de la conférence ISSAC 2015

[19] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate*, J. Inst. Math. Jussieu (2016), https://doi.org/10.1017/S1474748016000232

[20] X. Caruso, D. Roe, T. Vaccon, *Euclidean division and factorization of p-adic polynomials*, proceddings de la conférence ISSAC 2016

[21] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields*, J. Symbolic Comput. **79** (2017), 411–443

[22] X. Caruso, *Dimensions de certaines variétés de Kisin*, J. reine angew. Math. **723** (2017), 1–77

[23] X. Caruso, *Numerical stability of Euclidean algorithm over ultrametric fields*, J. Number Theor. Bordeaux **29** (2017), 503–534

[24] X. Caruso, D. Roe, T. Vaccon, *Characteristic polynomial of p-adic matrices*, proceddings de la conférence ISSAC 2017

[25] X. Caruso, J. Le Borgne, *Fast multiplication for skew polynomials over finite fields*, proceddings de la conférence ISSAC 2017

[26] X. Caruso, A. David, A. Mézard, *Un calcul d'anneaux de déformations potentiellement Barsotti–Tate*, à paraître à Trans. Amer. Math. Soc.

[27] X. Caruso, *Almost all non-archimedean Kakeya sets have measure zero*, à paraître à Confluentes Math.

[28] X. Caruso, D. Lubicz, *Semi-simplifiée modulo p des représentations semi-stables : une approche algorithmique*, prépublication (2013), 35 pages

[29] X. Caruso, *Computations with p-adic numbers*, prépublication (2017), 83 pages

[30] X. Caruso, *Polynômes de Ore en une variable*, prépublication (2017), 93 pages

[31] X. Caruso, *Slope factorization of Ore polynomials*, en préparation

[32] X. Caruso, D. Roe, T. Vaccon, ZpL *: a p-adic precision package*, en préparation

[33] D. Cerveau, X. Caruso, S. Gouëzel, X. Lachambre, N. Raymond, S. Vũ Ngọc, *Les annales Henri Lebesgue*, à paraître dans la Gazette des Mathématiciens

[34] X. Caruso, *Skew polynomials over finite fields*, librairie SAGEMATH (2013)

[35] X. Caruso, D. Lubicz, *Algorithmics of $\mathfrak{S}_\nu$-modules*, librairie MAGMA (2013)

[36] X. Caruso, *Bounded series over ultrametric rings*, librairie SAGEMATH (2013)

[37] X. Caruso, *Lattices in semi-stable representations*, librairie SAGEMATH (2013)

[38] X. Caruso, *Utilitaire pour la gestion des conférences et des semetres du CHL*, librairie DRUPAL (2014)

[39] X. Caruso, D. Roe, T. Vaccon, ZpL *: lattice precision for p-adics*, librairie SAGEMATH (2017), $\sim$ 2000 lignes

[40] X. Caruso, *Les annales Henri Lebesgue*, vidéo de promotion du journal, version française https://annales.lebesgue.fr/video/promoAHL-fr.mp4, version anglaise https://annales.lebesgue.fr/video/promoAHL-en.mp4

Dossier de candidature de Xavier Caruso

— Concours 41/01, année 2018 —

Projet de recherche

Table des matières

1 Algorithmique des représentations galoisiennes p-adiques **1**
- 1.1 Semi-simplifiée des représentations galoisiennes 2
- 1.2 Espaces de déformations de représentations galoisiennes 3

2 Factorisation des polynômes de Ore **4**
- 2.1 Sur la factorisation par les pentes 4
- 2.2 Sur la factorisation des opérateurs différentiels 5

3 À propos de mes vœux d'affectation **6**

Les dernières années de ma carrière de chercheur ont été marquées par une forte diversification de mes centres d'intérêts, incluant en particulier une ouverture thématique vers l'algorithmique et, plus généralement, vers l'informatique. Ce basculement a, bien entendu, nécessité un investissement personnel important dont j'ai désormais envie de (continuer à) récolter les fruits. Ceci est d'autant plus justifié qu'une lecture attentive du *résumé de mes travaux de recherche* [Travaux] montre que de nombreux points ont été laissés en suspens. En voici quelques exemples :

- ☞ la stratégie de calcul des espaces de déformations galoisiennes p-adiques basée sur les variétés de Kisin que j'ai mise au point avec Agnès David et Ariane Mézard (voir [Travaux, §1.4]) demande encore à être approfondie ;
- ☞ l'algorithme de calcul des réseaux dans les représentations galoisiennes semi-stables que j'ai mis au point avec David Lubicz (voir [Travaux, §2.1]) demande encore à être amélioré du point de vue de la stabilité numérique ;
- ☞ mon théorème de factorisation par les pentes des polynômes de Ore (voir [Travaux, §3.3]) demande à être étendu à une base plus générale que le spectre d'un corps.

Pour ces raisons, le projet de recherche que je vais présenter dans ce document se place, pour l'essentiel, dans la continuité de mes travaux précédents. Cela ne l'empêche toutefois pas, en tout cas à mon avis, d'être suffisamment conséquent et diversifié pour pouvoir stimuler mes recherches futures sur plusieurs années.

1 Algorithmique des représentations galoisiennes p-adiques

Ma priorité pour les années à venir reste la mise en place d'une base algorithmique complète et efficace pour pouvoir travailler sereinement avec les représentations galoisiennes p-adiques des corps p-adiques sur ordinateur. Bien entendu, il s'agit d'un sujet très vaste qui n'a été, pour l'instant, que très peu exploré et dans lequel il reste donc

pratiquement tout à faire. Je suis, malgré tout, convaincu qu'il s'agit d'un sujet d'avenir qui saura s'imposer dans les prochaines décennies une fois que les outils fondamentaux seront disponibles et bien rodés.

De nombreuses questions émergent autour de cette thématique et il serait certainement trop long d'en faire un recensement exhaustif dans ce document. Au contraire, je me propose ci-après de me focaliser sur deux d'entre elles qui résonnent fortement avec mes recherches passées et, pour cette raison, me tiennent particulièrement à cœur. Le lecteur intéressé trouvera d'autres problématiques connexes dans le projet CLap–CLap [1] (dont une copie est jointe à mon dossier de candidature) que j'ai soumis cette année à l'ANR, en tant que coordinateur.

1.1 Semi-simplifiée des représentations galoisiennes

La première problématique que j'aimerais présenter fait suite à mon travail avec David Lubicz sur le calcul algorithmique de la semi-simplifiée des représentations galoisiennes semi-stables [3]. Comme je l'ai expliqué dans [Travaux, §2.1], l'algorithme auquel nous avons abouti, bien qu'ayant théoriquement une complexité polynomiale, reste encore relativement inopérant en pratique. Une investigation rapide a montré que la source du problème est liée à sa forte instabilité numérique : il n'est pas rare, même pour les plus petits exemples en dimension 2, que notre algorithme ait besoin d'une précision en entrée qui dépasse les 1000 chiffres significatifs, ce qui est complètement déraisonnable !

Afin de résoudre ce problème, je me propose de mettre en application la méthode de la précision adaptative (que j'ai brièvement esquissée dans [Travaux, §2.3]) afin de stabiliser notre algorithme. Il est permis de croire que cela pourra fonctionner car il se trouve, d'une part, que la méthode de la précision adaptative a déjà porté ses fruits dans le cas des algorithmes de Gauss (pour l'échelonnement de matrices) et d'Euclide (pour le calcul de PGCD et des coefficients de Bézout) et, d'autre part, que notre algorithme fait un usage intensif de ces deux primitives de calcul.

Malgré tout, plusieurs sources de difficulté sont attendues. La première d'entre elles provient du fait que notre algorithme manipule des séries p-adiques qui sont des objets qui vivent naturellement dans des espaces de dimension infinie. Or, dans son état actuel d'avancement, la méthode de la précision adaptative n'a été étudiée qu'en dimension finie ! Bien qu'*a priori*, aucun obstacle théorique ne semble empêcher son extension à la dimension infinie, des complications théoriques et calculatoires sont susceptibles d'apparaître à ce stade ; typiquement le calcul explicite des différentielles a de fortes chances de prendre une forme nettement plus complexe.

Une autre source de difficulté est liée au fait que nous avons choisi de travailler à quasi-isomorphisme près (ceci, rappelons-le, afin d'éviter l'explosion de la taille des objets). Or ce choix fait particulièrement mauvais ménage avec la théorie de la précision p-adique car il détruit la continuité — et donc *a fortiori* la différentiabilité — de certaines opérations. Typiquement si $\mathcal{R}_{d,\nu}$ désigne l'espace des $\mathfrak{S}_\nu$-réseaux à l'intérieur de $\mathfrak{S}_\nu[1/p]^d$, autant l'application « somme » induit une fonction continue $\mathcal{R}_{d,\nu} \times \mathcal{R}_{d,\nu} \to \mathcal{R}_{d,\nu}$, autant elle induit une fonction *partout discontinue*

$$\mathcal{R}_{d,\nu}/\text{qis} \times \mathcal{R}_{d,\nu}/\text{qis} \longrightarrow \mathcal{R}_{d,\nu}/\text{qis}$$

1. Correspondance de Langlands p-adique : une approche constructive et algorithmique

où $\mathcal{R}_{d,\nu}/\mathrm{qis}$ désigne l'ensemble des réseaux à quasi-isomorphisme près. En réalité, nous avons déjà rencontré ce même problème dans notre travail initial avec David Lubicz ; c'est notamment lui qui nous avait contraint à faire varier continuellement la valeur de ν. Pourra-t-on utiliser ce même artifice pour la mise en place de la méthode de la précision adaptative ? Voici la question centrale sur laquelle, je pense, va reposer la réussite de ce projet.

1.2 Espaces de déformations de représentations galoisiennes

L'objectif à long terme que je me fixe ici est l'automatisation aussi complète que possible du calcul des espaces de déformations de représentations galoisiennes avec lesquels on travaille classiquement en théorie de Hodge p-adique. À cette fin, je me propose de suivre la stratégie que nous avons initiée avec Agnès David et Ariane Mézard dans [4] (voir aussi [Travaux, §1.4]) qui passe par les variétés de Kisin.

Bien entendu, avant toute autre chose, il s'agit de compléter le travail de [4] qui, comme je l'ai expliqué dans [Travaux, §1.4], reste encore en partie conjectural ; en effet, cet article se conclut par la construction d'un *candidat* plausible pour l'espace de déformations considéré mais nous n'avons pour l'instant ni obtenu une description explicite dudit candidat, ni démontré que celui-ci était bel et bien le bon. Nous travaillons actuellement, avec Agnès David et Ariane Mézard, sur ces questions et espérons pouvoir les résoudre dans un délai raisonnable (sachant que nous avons déjà obtenu des résultats partiels encourageants).

Une fois que cela sera fait, la question de la généralisation à d'autres contextes[2] va se poser pleinement. Une première difficulté d'ordre théorique se pose d'entrée de jeu ; elle est liée aux limitations actuelles de la théorie de Breuil–Kisin dont nous faisons un usage intensif. En effet, si celle-ci fonctionne particulièrement bien pour les petits poids de Hodge–Tate et les types galoisiens modérément ramifiés, des complications surgissent rapidement dès lors que l'on s'éloigne de ce cadre. Pourtant les espaces de déformations les plus chargés d'informations sont certainement ceux associés à de grands poids de Hodge–Tate et des types galoisiens sauvagement ramifiés. Il me semble donc nécessaire, en guise de préliminaire, d'améliorer la théorie de Breuil–Kisin sur ce point. Si je n'ai, pour l'instant, pas d'idée très précise pour ce qui concerne la ramification des types galoisiens, j'ai la nette impression que la restriction sur les poids de Hodge–Tate pourrait être levée à l'aide de la théorie des (φ,τ)-modules [2] (voir aussi [Travaux, §1.3]).

Vient ensuite le calcul de la variété de Kisin $\mathscr{GR}(\mathcal{C},\bar{\rho})_s$ (voir [Travaux, §1.4] pour les notations). À première vue, ce problème paraît abordable par l'outil algorithmique. En effet, la variété de Kisin apparaît, de par sa définition, comme un sous-espace (compact) d'une grassmannienne affine défini par des conditions qui peuvent être rendues entièrement explicites. En stratifiant la grassmannienne affine à l'aide de la décomposition d'Iwasawa, on obtient une stratification de la variété de Kisin (appelée *stratification par le genre*) ainsi que des équations explicites pour chacune des strates.

L'étape suivante est le calcul des fibres du morphisme de spécialisation

$$\mathrm{sp} : \mathscr{GR}(\mathcal{C},\bar{\rho})_\eta \to \mathscr{GR}(\mathcal{C},\bar{\rho})_s.$$

Il se trouve que ce problème se reformule complètement en termes matriciels, devenant ainsi très concret et susceptible d'être attaqué par les algorithmes classiques de calculs

2. Rappelons que la situation étudiée dans [4] était très spécifique.

d'invariants et de bases de Gröbner. Signalons que l'algorithmique des bases de Gröbner dans le contexte p-adique a été récemment développée par Vaccon [7, 8] et devrait pouvoir être utilisée telle quelle dans notre cadre.

Demeure enfin la question du recollement des fibres de sp qui me paraît, de loin, la plus délicate. L'espoir demeure cependant que la construction géométrique de [4] s'étende à des cas plus généraux, permettant ainsi de définir des candidats pour les espaces de déformations à l'aide d'éclatements et de complétés formels à partir d'un relèvement formel de la grassmannienne dans laquelle est plongée naturellement la variété de Kisin $\mathscr{GR}(\mathcal{C}, \bar{\rho})_s$. Ne resterait alors plus qu'à mettre en place les outils algorithmiques adéquats pour calculer des équations explicites de ces candidats.

Pour conclure, je concède volontiers que le parcours que je propose de suivre est long et semé d'embuches et que, de ce fait, il est peu probable que ce projet aboutisse dans les termes exacts évoqués précédemment (s'il aboutit). Je le trouve néanmoins très motivant pour au moins deux raisons : d'une part, il contient de nombreux sous-problèmes qui me paraissent à la fois abordables et intéressants en eux-mêmes (calcul explicite des variétés de Kisin, développement de la théorie des invariants dans le cadre p-adique, calcul explicite d'éclatements sur ordinateur dans le cadre de la géométrie formelle, *etc.*) et, d'autre part, il fixe un cap clairement identifié pour mes recherches futures.

2 Factorisation des polynômes de Ore

Mes travaux sur les polynômes de Ore ont également laissé plusieurs questions en suspens. Ci-après, je détaille deux d'entre elles qui me paraissent intéressantes.

2.1 Sur la factorisation par les pentes

La premier thème sur lequel j'aimerais m'attarder est la continuation de mon travail sur la factorisation par les pentes de polynômes de Ore [5]. Jusqu'à présent, je me suis limité au cas où le corps de base est valué complet (pour une valuation de rang 1). Or, les corps valués complets apparaissent comme les points de la géométrie de Berkovich. En utilisant des arguments géométriques d'extension à un voisinage et de recollement, j'ai bon espoir de pouvoir étendre mon théorème à des espaces géométriques « globaux » comme, par exemple, des courbes analytiques p-adiques (possiblement affines pour commencer). Précisément, si R est un anneau normé complet (suffisamment gentil), je m'attends à ce que l'on puisse associer à tout polynôme de Ore $P \in R[X, \bullet]$ une fonction « polygone de Newton » définie sur l'espace de Berkovich $\mathscr{M}(R)$ de façon à ce que le résultat suivant soit vrai : si d est un point de cassure des polygones de Newton associés à P pour tout point $x \in \mathscr{M}(R)$, alors la suite récurrente définie par :

$$A_0 = \sum_{i=0}^{d} a_i X^i \quad \text{(où les } a_i\text{'s sont les coefficients de } P\text{)}$$
$$A_{i+1} = A_i + \text{(reste de la division euclidienne à droite de } P \text{ par } A_i\text{)}$$

converge vers un diviseur à droite de P de degré d ayant le polygone de Newton attendu.

Un tel résultat pourrait avoir plusieurs applications intéressantes. Dans le contexte des équations différentielles, premièrement, il redonnerait un théorème de décomposition

globale des équations différentielles p-adiques (selon le polygone de Newton des rayons de convergence) et, de surcroît, le complèterait par un algorithme calculant cette décomposition. Deuxièmement, appliqué dans un contexte d'algèbre semi-linéaire, il donnerait un théorème effectif de décomposition des fibrés sur (certains ouverts de) la courbe de Fargues–Fontaine [6] qui s'inscrirait dans la continuité des travaux de Fargues, Fontaine, Kedlaya, Liu, Scholze...

Un certain nombre de difficultés sont toutefois attendues. Les deux principales que j'entrevois sont les suivantes. Tout d'abord, dans le cas de $R[X, \theta]$ où θ est un endomorphisme, il est tout à fait possible que θ agisse de manière non triviale sur les points de $\mathscr{M}(R)$. Ainsi un polynôme de Ore $P \in R[X, \theta]$ ne se spécialise *a priori* pas en chaque point de $\mathscr{M}(R)$ et il ne semble ainsi pas possible de réduire directement l'étude du cas général à celui du cas local déjà traité. Cette objection ne me semble toutefois pas très sérieuse car s'il est vrai que cela n'a pas de sens de spécialiser P en un point de $\mathscr{M}(R)$, il reste possible de définir le polygone de Newton de P en chaque point $x \in \mathscr{M}(R)$ (simplement en considérant les normes des coefficients de P selon x), ce qui pourrait être suffisant pour faire fonctionner la machine.

Une seconde objection concerne le cas différentiel, c'est-à-dire le cas de $R[X, \partial]$ où ∂ est une dérivation sur R. En effet, dans ce cas, le polygone de Newton que nous avons défini dans [5] est « incomplet » dans le sens où les pentes trop petites (par rapport au module de continuité de ∂) ont été volontairement mises à l'écart. Cette troncation n'avait que des répercussions limitées dans le cas local mais elle risque de prendre des proportions gênantes dans le cas global ; en effet, même dans le cas le plus simple où $R = \mathbb{Z}_p\{t\}$ et $\partial = \frac{d}{dt}$, le module de continuité de ∂ tend vers l'infini au voisinage des points rigides de $\mathscr{M}(R)$, vidant ainsi totalement de sa substance l'énoncé que nous envisageons. Il me semble donc absolument nécessaire de retravailler la définition des polygones de Newton dans le cadre différentiel pour s'affranchir de ces désagréments. S'inspirant du cas $R = \mathbb{Z}_p\{t\}$, $\partial = \frac{d}{dt}$, une solution à notre problème pourrait venir de l'action du Frobenius.

2.2 Sur la factorisation des opérateurs différentiels

Lors de mes travaux avec Alin Bostan et Éric Schost [1], nous avons introduit de nouvelles méthodes pour calculer efficacement la p-courbure des opérateurs différentiels de $k(x)\langle\partial\rangle$ (où k est un corps de caractéristique p). Or, aussi bien du point de vue théorique qu'algorithmique, la p-courbure est classiquement utilisée comme un ingrédient primordial à la factorisation. Il paraît donc naturel que nous nous intéressions à présent au problème de la factorisation des opérateurs différentiels en caractéristique p. En combinant les techniques que nous avons introduites avec celles que Jérémy Le Borgne et moi-même avons développées dans notre travail sur la factorisation des polynômes de Ore sur les corps finis, nous pensons pouvoir aboutir à un algorithme complet de factorisation dont la complexité serait quasi-linéaire vis-à-vis du paramètre p.

Une difficulté majeure est toutefois attendue : l'utilisation des techniques sus-mentionnées demandera certainement d'étendre le cadre d'étude à des opérateurs différentiels définis sur des revêtements quelconques de la droite projective (et non plus uniquement à la droite projective) pouvant possiblement être ramifiés, voire sauvagement ramifiés. Hormis quelques complications techniques, cela ne semble toutefois pas poser de véritable problème sur la plan théorique. Les complications algorithmiques s'annoncent toutefois plus sérieuses (sans pour autant, à première vue, paraître insurmontables) : il s'agira

de travailler dans des extensions finies de $k(x)$ en lieu et place de $k(x)$ lui-même. Les algorithmes pour ce faire existent mais sont évidemment moins performants et il faudra ainsi être particulièrement vigilent afin de conserver la complexité annoncée en $\tilde{O}(p)$.

3 À propos de mes vœux d'affectation

Afin de mener au mieux le projet de recherche détaillé ci-dessus, je souhaiterais pouvoir être affecté (en cas de recrutement) soit à l'institut mathématique de Bordeaux (UMR 5251) soit à l'unité de mathématiques pures et appliqués à l'ÉNS de Lyon (UMR 5669).

L'institut mathématique de Bordeaux

Mon intégration à l'institut mathématique de Bordeaux (IMB) me paraît être la plus naturelle tant mes thématiques de recherche complètent logiquement celles de l'équipe de théorie des nombres de l'IMB. En effet, il est clair tout d'abord que je trouverais très rapidement ma place au sein de cette équipe : j'aurais immédiatement des interlocuteurs privilégiés aussi bien dans le domaine de l'algorithmique (Jean-Marc Couveignes, Karim Belabas...) que dans celui de la théorie de Hodge p-adique (Denis Benois, Olivier Brinon, Dajano Tossici...).

Mais, de la même manière, je suis certain que je saurais, moi aussi, apporter à l'équipe de théorie des nombres de Bordeaux de nouvelles compétences qui permettront, d'une part, de renforcer sa cohésion interne et, d'autre part, de lui ouvrir de nouveaux horizons. Par exemple, j'apporte avec moi une thématique nouvelle qui est celle de la précision p-adique dont je pourrais implémenter les rouages dans le logiciel PARI/GP et faire ainsi de ce dernier un pionnier dans le domaine.

Je voudrais souligner également qu'au délà de l'équipe de théorie des nombres et de l'IMB, les possibilités d'échange et de collaboration avec les chercheurs bordelais foisonnent : il y a bien sûr l'équipe-projet LFANT qui travaille déjà en étroite collaboration avec l'IMB ; il y a aussi plusieurs membres du LaBRI avec lesquels je pourrais échanger sur la théorie algébrique des équations différentielles qui est fortement liée à l'étude combinatoire des marches telle qu'ils la pratiquent ; il y a encore les membres du projet européen *OpenDreamKit* avec lesquels j'aurai certainement beaucoup à échanger sur le logiciel SAGEMATH.

L'unité de mathématiques pures et appliquées (ÉNS de Lyon)

Une autre possibilité pour une éventuelle affectation, qui me paraît également pleine de sens, serait l'unité de mathématiques pures et appliquées (UMPA) de l'ÉNS de Lyon. En effet, de même qu'à Bordeaux, d'une part, mon intégration dans l'équipe de théorie des nombres de l'UMPA me semble tout à fait naturelle et, d'autre part, j'y apporterais des compétences nouvelles en algorithmique qui viendront la renforcer. J'espère également pouvoir être à l'origine d'une intensification des relations entre l'UMPA et le laboratoire d'informatique du parallélisme (LIP) situé un étage en dessous ; je pense d'ores et déjà avoir en main les clés pour y parvenir étant donné que je cotoie déjà plusieurs chercheurs en provenance de chacun de ces deux laboratoires.

À côté de cela, Lyon est également une ville qui est à la pointe pour toutes les activités de diffusion des mathématiques : la revue en ligne *Images des mathématiques* est née à

Lyon, le GDS *AuDiMath* est basée à Lyon, *etc.* Étant moi-même fortement sensibilisé à la question de la diffusion des mathématiques, il est certain que je saurais m'épanouïr dans cet environnement et que j'évertuerais à en faire profiter au mieux toute la communauté.

Références

[Travaux] X. Caruso, *Résumé des travaux de recherche*, joint à mon dossier de candidature

[1] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the p-curvature*, proceddings de la conférence ISSAC 2015

[2] X. Caruso, *Représentations galoisiennes p-adiques et (φ, τ)-modules*, Duke Math. J. **162** (2013), 2525–2607

[3] X. Caruso, D. Lubicz, *Semi-simplifiée modulo p des représentations semi-stables : une approche algorithmique*, prépublication (2013), 35 pages

[4] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate* J. Inst. Math. Jussieu (2016), https://doi.org/10.1017/S1474748016000232

[5] X. Caruso, *Slope factorization of Ore polynomials*, en préparation

[6] L. Fargues, J.-M. Fontaine, *Courbes et fibrés vectoriels en théorie de Hodge p-adique*, prépublication (2014)

[7] T. Vaccon, *Matrix-F5 algorithms over finite-precision complete discrete valuation fields*, proceddings de la conférence ISSAC 2014

[8] T. Vaccon, *Matrix-F5 algorithms and tropical Gröbner bases computation*, proceddings de la conférence ISSAC 2015

Dossier de candidature de Xavier Caruso

— Concours 41/01, année 2018 —

Liste complète de publications

Prépublications et articles en préparation

[1] X. Caruso, D. Lubicz, *Semi-simplifiée modulo p des représentations semi-stables : une approche algorithmique*, prépublication (2013), 35 pages

[2] X. Caruso, *Computations with p-adic numbers*, prépublication (2017), 83 pages

[3] X. Caruso, *Polynômes de Ore en une variable*, prépublication (2017), 93 pages

[4] X. Caruso, *Slope factorization of Ore polynomials*, en préparation

[5] A. Bostan, X. Caruso, G. Christol, P. Dumas, *Fast computation of the N-th term of an algebraic series in positive characteristic*, en préparation

[6] X. Caruso, D. Roe, T. Vaccon, ZpL *: a p-adic precision package*, en préparation

Articles parus ou à paraître

[7] X. Caruso, *Représentations semi-stables de torsion dans le cas $er < p-1$*, J. reine angew. Math. **594** (2006), 35–92

[8] X. Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), 629–699

[9] X. Caruso, D. Savitt, *Polygones de Hodge, de Newton et de l'inertie modérée des représentations semi-stables*, Math. Ann. **343** (2009), 777–789

[10] X. Caruso, T. Liu, *Quasi-semi-stable representations*, Bull. Soc. Math. France **137** (2009), 185–223

[11] X. Caruso, *Sur la classification de quelques φ-modules simples*, Mosc. Math. J. **9** (2009), 562–568

[12] X. Caruso, *Bounding Galois action on semi-stable representations*, Oberwolfach Report **30** (2009), 1709–1712

[13] X. Caruso, D. Savitt, *Poids de l'inertie modérée de certaines représentations cristallines*, J. Théor. Nombres Bordeaux **22** (2010), 79–96

[14] X. Caruso, *Classification of integral models of $(\mathbb{Z}/p^2\mathbb{Z})_K$ via Breuil-Kisin theory*, J. of Algebra **323** (2010), 1955–1957

[15] X. Caruso, T. Liu, *Some bounds for ramification of p^n-torsion semi-stable representations*, J. of Algebra **325** (2011), 70–96

[16] X. Caruso, *$\mathbb{F}_p$-représentations semi-stables* Ann. Inst. Fourier **61** (2011), 1683–1747

[17] X. Caruso, *Représentations galoisiennes p-adiques et (φ,τ)-modules*, Duke Math. J. **162** (2013), 2525–2607

[18] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*, LMS J. Comput. Math. **17** (2014), 302–344

[19] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*, LMS J. Comput. Math. **17** (2014), 274–294

[20] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the characteristic polynomial of the p-curvature*, proceedings de la conférence ISSAC 2014

[21] X. Caruso, *Random matrices over a DVR and LU factorization*, J. Symbolic Comput. **71** (2015), 98–123

[22] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the p-curvature*, proceedings de la conférence ISSAC 2015

[23] X. Caruso, D. Roe, T. Vaccon, *p-adic stability in linear algebra*, proceedings de la conférence ISSAC 2015

[24] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate*, J. Inst. Math. Jussieu (2016), https://doi.org/10.1017/S1474748016000232

[25] X. Caruso, D. Roe, T. Vaccon, *Euclidean division and factorization of p-adic polynomials*, proceddings de la conférence ISSAC 2016

[26] A. Bostan, X. Caruso, É. Schost, *Computation of the similarity class of the p-curvature*, proceddings de la conférence ISSAC 2016

[27] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields*, J. Symbolic Comput. **79** (2017), 411–443

[28] X. Caruso, *Estimation des dimensions de certaines variétés de Kisin*, J. reine angew. Math. **723** (2017), 1–77

[29] X. Caruso, *Numerical stability of Euclidean algorithm over ultrametric fields*, J. Number Theor. Bordeaux **29** (2017), 503–534

[30] X. Caruso, D. Roe, T. Vaccon, *Characteristic polynomial of p-adic matrices*, proceddings de la conférence ISSAC 2017

[31] X. Caruso, J. Le Borgne, *Fast multiplication for skew polynomials over finite fields*, proceddings de la conférence ISSAC 2017

[32] X. Caruso, A. David, A. Mézard, *Un calcul d'anneaux de déformations potentiellement Barsotti–Tate*, à paraître à Trans. Amer. Math. Soc.

[33] X. Caruso, *Almost all non-archimedean Kakeya sets have measure zero*, à paraître à Confluentes Math.

Logiciels

[34] X. Caruso, *Skew polynomials over finite fields*, librairie SageMath (2013), $\sim$ 8000 lignes

[35] X. Caruso, D. Lubicz, *Algorithmics of $\mathfrak{S}_\nu$-modules*, librairie Magma (2013), $\sim$ 2000 lignes

[36] X. Caruso, *Bounded series over ultrametric rings*, librairie SageMath (2013), $\sim$ 3000 lignes

[37] X. Caruso, *Lattices in semi-stable representations*, librairie SageMath (2013), $\sim$ 1500 lignes

[38] X. Caruso, *Utilitaire pour la gestion des conférences et des semetres du CHL*, librairie drupal (2014), $\sim$ 5000 lignes

[39] X. Caruso, D. Roe, T. Vaccon, ZpL *: lattice precision for p-adics*, librairie SageMath (2017), $\sim$ 2000 lignes

Articles parus dans la Revue de Mathématiques Spéciales

[40] X. Caruso, P. Bornsztein, *Des formes bilinéaires en combinatoire*, RMS 114-3 (2004), 35–44

[41] X. Caruso, P. Bornsztein, *Des formes bilinéaires en combinatoire II*, RMS 114-3 (2005), 12–14

[42] X. Caruso, *Nombre d'or et tournesol*, RMS 116-4 (2006), 7–23

[43] X. Caruso, *Quelques identités combinatoires en faveur de l'existence du corps à un élément*, RMS 117-1 (2006), 36–44

[44] X. Caruso, D. Pigeon, *Autour du théorème des nombres premiers*, RMS 118-3 (2008), 3–15

[45] X. Caruso, *Trisection de l'angle et duplication du cube*, RMS 118-4 (2008), 24–28

[46] X. Caruso, *Construction à la règle trop courte et au compas à ouverture limitée*, RMS 119-2 (2009), 7–13

[47] X. Caruso, *Une incarnation peu connue du corps des nombres réels*, RMS 119-4 (2009), 5–8

[48] X. Caruso, I. Kortchemski, *Statistiques du nombre de cycles d'une permutation*, RMS 121-4 (2011)

[49] X. Caruso, *Application des fractions continues à la construction des gammes musicales*, RMS 123-1 (2012)

Articles de diffusion des mathématiques

[50] X. Caruso, *La réforme du statut des enseignants chercheurs*, Images des Mathématiques (2008)

[51] X. Caruso, *À propos du nombre d'Erdös*, Images des Mathématiques (2008)

[52] X. Caruso, *Que se passe-t-il lorsqu'un mathématicien va à la piscine ?*, Images des Mathématiques (2009)

[53] X. Caruso, *Que doit-on attendre d'un bon séminaire*, Images des Mathématiques (2009)

[54] X. Caruso, *Lettre à une amie fidèle*, Images des Mathématiques (2009)

[55] X. Caruso, *Un problème de remplissage de verres*, Images des Mathématiques (2009)

[56] X. Caruso, *Polska Biblioteka Wirtualna Nauki*, Images des Mathématiques (2009)

[57] X. Caruso, *Rencontre du troisième type*, Images des Mathématiques (2009)

[58] X. Caruso, *Que se passe-t-il lorsqu'un mathématicien va à la piscine : les vidéos !*, Images des Mathématiques (2009)

[59] X. Caruso, *Je pars à Moscou dans un mois*, Images des Mathématiques (2009)

[60] X. Caruso, *Mais où est donc le petit côté ?*, Images des Mathématiques (2009)

[61] X. Caruso, *L'art de rendre la monnaie*, Images des Mathématiques (2009)

[62] X. Caruso, *D'une simplicité déconcertante*, Images des Mathématiques (2009)

[63] X. Caruso, P. Bornsztein, *Au cœur des Olympiades Internationales de Mathématiques*, Quadrature **71** (2009), 31–44

[64] X. Caruso, *Autour de l'hypothèse du continu : construction de* $\aleph_1$, Quadrature **73** (2009), 16–19

[65] X. Caruso, *La vie au laboratoire Poncelet*, Images des Mathématiques (2010)

[66] X. Caruso, *Fête mathématique (de Moscou)*, Images des Mathématiques (2010)

[67] X. Caruso, *Que se passe-t-il lorsqu'une mathématicienne fait du point de croix ?*, Images des Mathématiques (2010)

[68] X. Caruso, *Hausdorff Research Institute for Mathematics*, Images des Mathématiques (2010)

[69] X. Caruso, *Petite leçon sur le calcul des intérêts bancaires*, Images des Mathématiques (2010)

[70] X. Caruso, *École d'été « Mathématiques contemporaines » à Doubna*, Images des Mathématiques (2010)

[71] X. Caruso, *Rechercher, c'est...*, Images des Mathématiques (2010)

[72] X. Caruso, *Les imaginaires de l'arithmétique*, Images des Mathématiques (2011)

[73] X. Caruso, *Logiciels de topologie et de géométrie*, Images des Mathématiques (2011)

[74] X. Caruso, *Mathematic Park*, Images des Mathématiques (2011)

[75] X. Caruso, B. Teheux, *De l'ambiguité des puzzles aux idées de Galois*, Images des Mathématiques (2011)

[76] X. Caruso, B. Teheux, *Quel est ce nombre ?*, Images des Mathématiques (2011)

[77] X. Caruso, L. Fourquaux, *Au feu les pompiers — L'algorithme de Ford-Fulkerson*, Images des Mathématiques (2013)

[78] X. Caruso, *Qui est-ce ? — Le codage de Hamming*, Images des Mathématiques (2013)

[79] X. Caruso, *Brainpop français*, Images des Mathématiques (2013)

[80] X. Caruso, *Des mathématiques à la photographie numérique : bruit, dynamique*, Images des Mathématiques (2014)

[81] X. Caruso, *À la conquête du nord-est*, Images des Mathématiques (2014)

[82] X. Caruso, *L'IHP fait son ciné-club*, Images des Mathématiques (2014)

[83] X. Caruso, *Les nombres p-adiques*, exposé pour les 5 minutes Lebesgue

[84] X. Caruso, V. Duchêne, *Deux jeux mathématiques*, exposé pour les 5 minutes Lebesgue

Articles publicitaires

[85] X. Caruso, *Mathematic Park*, Gazette des Mathématiciens **148** (2016)

[86] X. Caruso, B. Grébert, X. Lachambre, S. Vũ Ngọc, *Les 5 minutes Lebesgue*, Gazette des Mathématiciens **151** (2017)

[87] D. Cerveau, X. Caruso, S. Gouëzel, X. Lachambre, N. Raymond, S. Vũ Ngọc, *Les annales Henri Lebesgue*, à paraître dans la Gazette des Mathématiciens

[88] X. Caruso, *Les annales Henri Lebesgue*, vidéo de promotion du journal, version française https://annales.lebesgue.fr/video/promoAHL-fr.mp4, version anglaise https://annales.lebesgue.fr/video/promoAHL-en.mp4