Rapport d'activités de Xavier Caruso

Période : décembre 2010 — juin 2013

1 Curriculum vitæ

Xavier Caruso
(né le 24 avril 1980 à Cannes)
IRMAR – Université Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
Tél : 02 23 23 58 92
E-Mail : xavier.caruso@normalesup.org
Page web : http://perso.univ-rennes1.fr/xavier.caruso/
Marié, un enfant

Parcours scolaire et professionnel

2011 Habilitation à diriger les recherches soutenue le 3 juin à l'université de Rennes 1 durant le jury composé de Laurent Berger, Christophe Breuil, Pierre Colmez, Jean-Marc Fontaine et Michael Rapoport.

2009–2010 Mobilité d'une année au laboratoire Poncelet à l'Université Indépendante de Moscou

2006– Chargé de recherche au CNRS affecté à l'Université de Rennes 1.

2005 Thèse sous la direction de Christophe Breuil intitulée *Conjecture de l'inertie modérée de Serre* et soutenue le 7 décembre devant le jury composé de Ahmed Abbes, Pierre Berthelot (rapporteur), Lawrence Breen, Christophe Breuil (directeur de thèse), Michel Raynaud. Autre rapporteur : Mark Kisin.

2003–2006 Moniteur à l'université Paris 13.

1999–2003 Élève de de l'École normale supérieure de Paris

Responsabilités

2013– Rédacteur du journal en ligne *Images des mathématiques*

2012–2016 Membre élu du CoNRS (Comité National de la Recherche Scientifique)

2012–2016 Membre nommé du conseil de l'IRMAR (Institut de Recherche en Mathématiques de Rennes)

2009–2013 Coordinateur du projet ANR CETHop (Calculs effectifs en théorie de Hodge p-adique)

Divers

1997 Premier accessit au concours général de mathématiques.
Quatrième accessit au concours général de physique.
Participation aux olympiades internationales de mathématiques à Mar del Plata (Argentine). Obtention d'une *honourable mention*.

Langues : français (langue maternelle), anglais (parlé et écrit), russe (assez bonne connaissance)

2 Recherche scientifique

Je rappelle que mon domaine de recherche traditionnel est l'étude des représentations galoisiennes p-adiques *via* les techniques de la théorie de Hodge (p-adique). J'avais déjà expliqué dans mes précédents rapports d'évaluation mon envie de développer des outils algorithmiques — et, à terme, des logiciels informatiques — pour venir en aide au théoricien s'engageant dans la voie de la théorie de Hodge p-adique, tant les calculs qu'elles impliquent s'avèrent souvent longs et fastidieux. J'ai consacré l'essentiel de mon activité de ces cinq dernières semestres à ce virage vers l'algorithmique.

La suite de ce rapport est découpé en trois grandes parties :
- dans la première, je reviens rapidement sur mes contributions « traditionnelles » ;
- dans la deuxième, j'explique mes résultats principaux à propos de l'algorithmique de la théorie de Hodge p-adique ;
- dans la troisième, je détaille quelques travaux en cours.

Première partie : Reminiscences

Habilitation à diriger les recherches

Référence : [1] X. Caruso, *Une contribution à la théorie de Hodge p-adique entière et de torsion*

J'ai soutenu mon habilitation à diriger les recherches le 3 juin 2011 à l'université de Rennes 1 durant le jury composé de Laurent Berger, Christophe Breuil, Pierre Colmez, Jean-Marc Fontaine et Michael Rapoport.

Cela a été pour moi l'occasion d'écrire une synthèse (voir [1]) d'une soixantaine de pages sur mes recherches « traditionnelles ».

La théorie des (φ,τ)-modules

Référence : [2] X. Caruso, *Représentations galoisiennes p-adiques et (φ,τ)-modules*, à paraître à Duke Math. Journal

La théorie des (φ,τ)-modules est une variante de la théorie « classique » des (φ,Γ)-modules de Fontaine qui permet de décrire les représentations p-adiques du groupe de Galois absolu d'une extension finie K de $\mathbb{Q}_p$ (p désignant ici un nombre premier fixé, que l'on suppose impair).

Rappelons que, dans cette dernière théorie, on considère l'extension cyclotomique $K(\zeta_{p^\infty})$ engendrée par toutes les racines p^s-ième de l'unité (prises dans une clôture algébrique $\bar{K}$ de K) avec s parcourant $\mathbb{N}$. Le groupe de Galois de l'extension $K(\zeta_{p^\infty})/K$ — noté traditionnellement Γ — apparaît naturellement comme un sous-groupe de $\mathbb{Z}_p^\times$ *via* le caractère cyclotomique ; en particulier, il est commutatif et même procyclique dès que $p>2$. D'un autre côté, la théorie du corps des normes de Fontaine et Wintenberger entraîne que le groupe de Galois $\mathrm{Gal}(\bar{K}/K(\zeta^{p^\infty}))$ est canoniquement isomorphe au groupe de Galois absolu d'un corps de séries formelles à coefficients dans le corps résiduel de K ce qui permet, en supposant l'extension $K/\mathbb{Q}_p$ non ramifiée pour simplifier la présentation, de décrire les $\mathbb{Q}_p$-représentations de $\mathrm{Gal}(\bar{K}/K(\zeta^{p^\infty}))$ à l'aide de φ-modules étales sur le corps de séries

$$\mathcal{E}=\left\{\sum_{i=-\infty}^{+\infty} a_iX^i,\quad a_i\in K,\ (a_i)\text{ bornés},\ \lim_{i\to-\infty}a_i=0\right\}$$

muni du Frobenius φ envoyant $a_i\in K$ sur son image par le Frobenius arithmétique usuel et X sur $(1+X)^p-1$. Rappelons qu'un *φ-module* sur $\mathcal{E}$ est un $\mathcal{E}$-espace vectoriel D de dimension finie d muni d'un endomorphisme $\varphi:D\to D$ semi-linéaire par rapport à φ. Il est dit *étale* s'il existe une base de D dans laquelle la matrice de φ appartient à $\mathrm{GL}_d(\mathcal{O}_\mathcal{E})$ où $\mathcal{O}_\mathcal{E}$ désigne le sous-anneau de $\mathcal{E}$ formé des séries $\sum_{i=-\infty}^{+\infty}a_iX^i$ pour lesquelles tous les a_i sont dans $\mathcal{O}_K$. Il résulte de ceci une description des $\mathbb{Q}_p$-représentations de $G_K=\mathrm{Gal}(\bar{K}/K)$ *via* des objets appelés (φ,Γ)-modules étales, qui sont des φ-modules étales sur $\mathcal{E}$ munis d'une action supplémentaire de Γ vérifiant certaines relations de commutation.

La théorie des (φ,τ)-modules reprend les idées précédentes sauf que l'extension cyclotomique $K(\zeta_{p^\infty})$ est remplacée par l'extension K_∞, parfois appelée extension de Breuil-Kisin, obtenue à partir de K en ajoutant un système compatible $(\pi_s)_{s\geqslant 0}$ de racines p^s-ième d'une uniformisante π fixée[1].

1. On note que K_∞ dépend du choix de π et des π_s.

L'avantage — pressenti par Breuil puis concrétisé par Kisin — d'utiliser l'extension K_∞ plutôt que $K(\zeta_{p^\infty})$ est que la théorie qui est résulte s'articule de façon plus harmonieuse et plus complète avec d'autres aspects de la théorie de Hodge p-adique fournissant une description des représentations semi-stables à l'aide de (φ, N)-modules filtrés. Quoi qu'il en soit, le théorème de Fontaine et Wintenberger s'applique encore dans ce nouveau contexte et entraîne que les $\mathbb{Q}_p$-représentations de $G_\infty = \mathrm{Gal}(\bar{K}/K_\infty)$ sont décrites par des φ-modules étales sur

$$\mathcal{E}_u = \left\{ \sum_{i=-\infty}^{+\infty} a_i u^i, \quad a_i \in W[1/p],\ (a_i) \text{ bornés},\ \lim_{i\to-\infty} a_i = 0 \right\}$$

où W désigne l'anneau des entiers de la sous-extension maximale non ramifiée de $K/\mathbb{Q}_p$ et où $\mathcal{E}_u$ est muni du Frobenius envoyant u sur u^p et agissant comme le Frobenius usuel sur W. Il paraît toutefois nettement plus difficile de comprendre ce qu'il faut ajouter pour passer de G_∞ à G_K, le problème étant que l'extension K_∞/K n'est pas galoisienne ! Une solution possible est de remarquer que G_K est topologiquement engendré par le sous-groupe G_∞ et un élément τ agissant sur π_s par $\tau(\pi_s) = \zeta_{p^s} \cdot \pi_s$. Si T est une $\mathbb{Q}_p$-représentation de G_K, cet élément τ n'induit malheureusement pas un endormorphisme du φ-module D associée à $T_{|G_\infty}$ mais il induit néanmoins un endormorphisme de $L \otimes_{\mathcal{E}_u} D$ où L est une certaine extension de $\mathcal{E}_u$. De surcroît, réciproquement, la donnée de cette action permet de reconstruire intégralement la représentation T.

Malheureusement, le corps L qui est apparu ci-dessus est compliqué, ce qui rend la théorie difficilement praticable en l'état. On remarque toutefois que le logarithme de τ, pour peu qu'on arrive à le définir rigoureusement, devrait jouïr de propriétés plus agréables. En effet, de la relation de commutation $g\tau \equiv \tau^{\chi(g)} g \pmod{G_\infty \cap \ker \chi_{\mathrm{cycl}}}$ valable pour $g \in G_\infty$ montre que, si on sait définir un opérateur $\log \tau$ vérifiant les propriétés usuelles du logarithme, alors la formule $\frac{\log \tau}{p\mathbf{t}}$ (où $\mathbf{t}$ est un certain élément explicite de L) envoie D dans lui-même — ou peut-être dans un espace très légèrement plus grand.

Une bonne partie de [2] est consacrée à l'étude du cas où D de $E(u)$-hauteur finie — qui est particulièrement intéressant car, comme nous allons l'expliquer ensuite, il correspond, peu ou prou, au cas des représentations semi-stables. Un φ-module D sur $\mathcal{E}_u$ est dit de *$E(u)$-hauteur finie* s'il admet une base dans laquelle la matrice de φ est à coefficients dans $W[[u]]$ et si son déterminant s'écrit comme le produit d'un élément inversible de $W[[u]]$ et d'une puissance du polynôme minimal $E(u)$ de π sur $W[1/p]$. Je montre, dans ce cas, que $\log \tau$ est bien défini. Dans l'état actuel, l'argument est assez compliqué ; il se développe en plusieurs étapes comme suit :

(1) en étudiant attentivement la ramification sauvage des représentations qui entrent en jeu, on établit des bornes sur l'action de $\tau^{p^s} - \mathrm{id}$ pour tout entier s ; de là, on déduit que la suite des $\frac{(\mathrm{id}-\tau)^i}{i}$ est bornée (dans un certain sens précisé dans l'article) ;

(2) on introduit les logarithmes tronqués :

$$\log_m \tau = \sum_{i=1}^{p^m-1} \frac{(\mathrm{id}-\tau)^i}{i}$$

et on montre, à l'aide de la relation $g\tau \equiv \tau^{\chi(g)} g \pmod{G_\infty \cap \ker \chi_{\mathrm{cycl}}}$, que $\frac{\log_m \tau}{p\mathbf{t}}$ envoie D sur $D + O_m$ où (O_m) est une suite décroissante d'espaces que l'on contrôle précisément ;

(3) de la compacité de D (pour une bonne topologie) et de certaines propriétés des opérateurs $\log_m \tau$, on déduit que la suite des $(\log_m \tau)$ admet une valeur d'adhérence que l'on appelle $\log \tau$;

(4) en utilisant la théorie de Kisin, on associe une représentation semi-stable à l'opérateur $N_\nabla = \frac{\log \tau}{p\mathbf{t}}$ et on démontre que celle-ci s'identifie à la représentation associée à D à une partie finie près que l'on contrôle explicitement.

Comme conséquence, on déduit le théorème suivant :

Théorème 1. *Supposons (pour simplifier) que l'extension $K/\mathbb{Q}_p$ soit non ramifiée*[2]*. Soit V une $\mathbb{Q}_p$-représentation de G_K et soit D son (φ,τ)-module associé. Alors V est semi-stable à poids de Hodge-Tate positifs ou nuls si, et seulement si D est de $E(u)$-hauteur finie.*

Remarque 2. Le fait que toute représentation semi-stable soit de $E(u)$-hauteur finie est un résultat de Kisin. La réciproque, par contre, est nouvelle.

2. Ceci assure que la « partie finie » dont il a été question précédemment est en fait triviale.

Dans le cas général (où l'on ne suppose plus que D est $E(u)$-hauteur finie), la même stratégie devrait fonctionner sous réserve d'avoir un théorème de surconvergence des (φ,τ)-modules à l'instar du théorème de Cherbonnier-Colmez dans le cadre des (φ,Γ)-modules. Je bute cependant sur des problèmes techniques pour établir un tel résultat ; j'ai soumis le problème à Floric Tavares Ribeiro et nous travaillons (plus ou moins activement) à sa résolution. Si ce travail aboutit, il devrait permettre d'établir le résultat suivant que j'énonce — de façon volontairement vague pour ce rapport — pour l'instant sous la forme d'une conjecture.

Conjecture 3. *Il existe une équivalence de catégories entre :*
- *la catégorie des $\mathbb{Q}_p$-représentations d'un sous-groupe $G_s = \mathrm{Gal}(\bar{K}/K(\pi_s))$ pour un s variable (un morphisme entre deux telles représentations étant un morphism G_s-équivariant pour un entier s suffisamment grand), et*
- *la catégorie des (φ, N_∇)-modules étales*[3] *sur l'anneau de Robba*[4].

Deuxième partie : Le projet CETHop

L'acronyme CETHop signifie « Calculs Effectifs en Théorie de Hodge p-adique » et le projet CETHop est un projet ANR dont je suis le coordinateur depuis septembre 2009. Comme son nom l'indique, son objectif est de mettre au point des méthodes pour effectuer sur ordinateur les calculs souvent ardus et fastidieux de la théorie de Hodge p-adique.

De façon plus précise, la question principale qui a guidé mes recherches durant ces cinq derniers semestres est celle du calcul de la semi-simplifiée modulo p de certaines représentations galoisiennes p-adiques. Rappelons que, si V est une $\mathbb{Q}_p$-représentation de G_K, un théorème de Brauer et Nesbitt affirme que, si $T \subset V$ est un $\mathbb{Z}_p$-réseau stable par l'action de G_K, la somme des composants irréductibles de T/pT ne dépend que de V. C'est elle que l'on appelle la *semi-simplifiée modulo p* de V et que l'on note souvent $\bar{V}^{\mathrm{ss}}$. Une remarque importante est la suivante : la restriction à G_∞ définit une bijection entre les $\mathbb{F}_p$-représentations irréductibles de G_K et celles de G_∞. Ainsi, pour calculer $\bar{V}^{\mathrm{ss}}$, on peut *dès le départ* restreindre la représentation V à G_∞. Je me suis, en fait, particulièrement intéressé au cas où V est une représentation semi-stable à poids de Hodge-Tate positifs ou nuls. En effet, comme cela a déjà été entrevu au numéro précédent, la théorie de Kisin permet de décrire $V_{|G_\infty}$ à l'aide d'un φ-module $\mathfrak{D}$ défini sur $\mathfrak{S}[1/p]$ où, par définition, $\mathfrak{S} = W[[u]]$. Les deux résultats suivants de Kisin :
- il y a une bijection canonique entre l'ensemble des réseaux $T \subset V$ stables par G_∞ et l'ensemble des $\mathfrak{S}$-réseaux $\mathfrak{M} \subset \mathfrak{D}$ qui sont stables par φ et de $E(u)$-hauteur finie[5] (le φ-module $\mathfrak{M}$ associé à T est souvent appellé le *module de Kisin* de T) ;
- avec les notations précédentes, le quotient T/pT est déterminé (par une recette simple) à partir de $\mathfrak{M}/p\mathfrak{M}$

ramènent le calcul de $\bar{V}^{\mathrm{ss}}$ à une suite de calculs sur des φ-modules définis sur $\mathfrak{S}[1/p]$, $\mathfrak{S}$ et enfin $k[[u]]$.

Algorithmique des $\mathfrak{S}$-modules

Références :
[5] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*, prepublication (2012)
[10] X. Caruso, D. Lubicz, *Algorithmics of $\mathfrak{S}_\nu$-module*, librairie MAGMA (2013)
[11] X. Caruso, *Bounded series over ultrametric rings*, librairie SAGE (2013), version non documentée

Au vu de ce qui précède, on comprend aisément qu'en guise de préliminaire, il a été nécessaire de développer des méthodes algorithmiques pour travailler sur ordinateur avec des $\mathfrak{S}$-modules et des $\mathfrak{S}[1/p]$-modules. J'ai accompli cette partie du travail en commun avec David Lubicz.

Au moins d'un point de vue théorique, les anneaux $\mathfrak{S}$ et $\mathfrak{S}[1/p]$ sont bien compris depuis longtemps. On sait, par exemple, que $\mathfrak{S}[1/p]$ est un anneau euclidien, ce qui se trouve être la situation idéale pour les applications algorithmiques : tout $\mathfrak{S}[1/p]$-module de type fini sans torsion est libre, et on peut généralement facilement en calculer une base par de l'« élimination à la Gauss ». L'anneau

3. Informellement, et sans surprise, un (φ, N_∇)-module étale et un φ-module étale muni d'un opérateur supplémentaire N_∇ vérifiant certains axiomes de commutation.

4. L'anneau de Robba est l'anneau des séries $\sum_{i=-\infty}^{+\infty} a_i u^i$ (avec $a_i \in W$) convergent sur un couronne de la forme $r < |x| < 1$ pour un certain réel $r \in]0,1[$ dépendant de la série.

5. Cette seconde condition est en réalité automatique. Mieux encore, on peut démontrer que tout réseau $\mathfrak{M} \subset \mathfrak{D}$ stable par φ est de $E(u)$-hauteur $\leqslant r$ où r est le plus grand poids de Hodge-Tate de la représentation semi-stable.

$\mathfrak{S}$, quant à lui, est local noethérien régulier de dimension 2. En particulier, il résulte d'un théorème d'Iwasawa que si M est un sous-$\mathfrak{S}$-module de $\mathfrak{S}[1/p]^d$, alors le sous-module $\mathrm{Max}(M) \subset \mathfrak{S}[1/p]^d$ défini par

$$\mathrm{Max}(M) = \left\{ x \in \mathfrak{S}[1/p]^d \quad \middle| \quad \exists n \in \mathbb{N},\, u^n x \in M \text{ et } p^n x \in M \right\}$$

est un module libre. Mieux encore, il s'agit du plus petit sous-$\mathfrak{S}$-module de $\mathfrak{S}[1/p]^d$ qui est libre et qui contient M. La philosophie que nous suivons dans [5] est de remplacer systématiquement le résultat d'un calcul sur les $\mathfrak{S}$-modules, disons M, par $\mathrm{Max}(M)$, ceci afin d'avoir la garantie de manipuler uniquement des modules libres (ce qui a de multiples avantages, comme celui de limiter la taille nécessaire pour représenter ces modules en machine). Ainsi, par exemple, si M_1 et M_2 sont deux sous-modules (libres) de $\mathfrak{S}[1/p]^d$, on ne travaillera pas avec la somme usuelle $M_1 + M_2$ qui peut ne pas être un module libre mais avec la « somme libre » :

$$M_1 +_{\mathrm{free}} M_2 = \mathrm{Max}(M_1 + M_2)$$

qui, elle, est toujours libre. En contrepartie, il est vrai que l'on ne calcule pas ce que l'on voudrait mais c'est, semble-t-il, le prix à payer pour avoir une algorithmique efficace. Par ailleurs, gardons quand même à l'esprit que M et $\mathrm{Max}(M)$ ne sont pas si éloignés, dans le sens où le conoyau de l'inclusion canonique $M \to \mathrm{Max}(M)$ est un module de longueur finie.

Dans [5], reprenant une démonstration du théorème d'Iwasawa dûe à Cohen, nous décrivons une méthode qui calcule une base de $\mathrm{Max}(M)$ connaissant une famille de générateurs de M. En particulier, elle s'applique directement pour le calcul des « sommes libres ». Cette méthode n'est toutefois pas, à proprement dit, un algorithme car elle suppose que la machine sait manipuler les élements de $\mathfrak{S}[1/p]$ dans leur intégralité. Or, un élément de $\mathfrak{S}[1/p]$ est une série qui fait intervenir un nombre infini de coefficients qui ne peuvent pas tous tenir dans la mémoire d'un ordinateur. Lorsque l'on manipule des éléments de $\mathfrak{S}[1/p]$ sur machine, on est donc obligé de tronquer les séries qui les représentent, c'est-à-dire concrètement de replacer $\sum_{i=0}^{\infty} a_i u^i$ par :

$$\sum_{i=0}^{N-1} \big(\tilde{a}_i + O(p^{N_i})\big) u^i + O\big(u^N\big) \tag{1}$$

où $\tilde{a}_i$ est une approximation de a_i qui vit dans un anneau exact. (Par exemple si les a_i sont dans $\mathbb{Q}_p$, on considèrera généralement des éléments $\tilde{a}_i$ dans $\mathbb{Z}[1/p]$.) On se rend très vite compte que cette contrainte basique d'origine informatique a des conséquences terrifiantes pour l'algorithme des $\mathfrak{S}$-modules que l'on souhaite développer. Supposons par exemple que l'on souhaite calculer la « somme libre » de $M_1 = p\mathfrak{S} \subset \mathfrak{S}[1/p]$ et $M_2 = (p + u^n)\mathfrak{S} \subset \mathfrak{S}[1/p]$ où n est un entier. Revenant aux définitions, on obtient sans difficulté $M_1 +_{\mathrm{free}} M_2 = \mathfrak{S}$. Par contre, si n est supérieur ou égal à l'entier N de l'équation 1, l'ordinateur ne « verra » pas le terme u^n dans la définition de M_2 et calculera $M_1 +_{\mathrm{free}} M_2 = p\mathfrak{S}$. En d'autres termes, on vient simplement d'illustrer le fait que l'opération « somme libre » n'est pas continue... ce qui est certainement gênant lorsque l'on ne peut travailler qu'avec des approximations.

Dans [5], nous proposons une solution à ce problème (qui n'est sans doute pas satisfaisante sur tous les plans mais qui s'avère néanmoins particulièrement bien adaptée pour les applications qui nous intéressent). Notre première idée consiste à compléter la représentation des objets sur machine en ajoutant ce que nous avons appelé des *garanties*. On choisit de représenter (une approximation d')un élément de $\mathfrak{S}[1/p]$ par :

1. la *précision* : un entier N et des nombres rationnels $N_0, \ldots, N_{N-1}$;
2. l'*approximation* : des éléments $\tilde{a}_0, \ldots, \tilde{a}_{N-1}$ qui vivent dans un anneau exact approximant W et qui vérifient :
$$a_i = \tilde{a}_i + O(p^{N_i})$$
pour tout $i \in \{0, \ldots, N-1\}$;
3. la *garantie* : un entier v vérifiant $v_p(a_i) \geqslant v$ pour tout $i \geqslant N$.

Pour alléger la suite du texte, on appelle *représentation PAG* (pour Précision-Approximation-Garantie) la représentation ci-dessus. Additionner et multiplier des éléments de $\mathfrak{S}[1/p]$ dont on ne connaît que la représentation PAG et donner le résultat de l'opération selon cette même représentation ne pose pas de difficulté particulière. Nous expliquons en outre dans [5] comment réaliser des divisions euclidiennes (toujours selon la représentation PAG) et obtenons pour ce faire un algorithme de complexité logarithmique en la précision (alors que l'algorithme naïf serait plutôt linéaire).

L'introduction de la garantie v n'est cependant pas suffisante pour résoudre notre problème et, de fait, l'exemple que l'on a mentionné précédemment continue de pêcher exactement de la même manière. La seconde idée — qui, bien que fortement inspirée d'« une philosophie de la surconvergence » très classique en théorie de Hodge p-adique et plus généralement en géométrie rigide, nous paraît véritablement nouvelle dans le contexte algorithmique — que nous avons introduite dans [5] est celle de *changement de pente*. Précisément, au lieu de travailler uniquement avec l'anneau $\mathfrak{S}$, on travaille avec toute une famille d'anneaux $\mathfrak{S}_\nu$ dépendant d'un paramètre $\nu \in \mathbb{Q}^+$ que l'on appelle la *pente*. Par définition,

$$\mathfrak{S}_\nu = \left\{ \sum_{i=0}^{\infty} a_i u^i, \quad a_i \in W[1/p],\ v_p(a_i) + \nu i \geqslant 0 \text{ pour tout } i \right\}.$$

On a bien sûr $\mathfrak{S}_0 = \mathfrak{S}$. D'un point de vue analytique, l'anneau $\mathfrak{S}_\nu$ est un classique : il s'agit de l'anneau des fonctions analytiques convergentes et bornées par 1 sur le disque $D_\nu = \{|x| > \nu\}$. Ainsi, $\mathfrak{S}_\nu[1/p]$ est l'anneau des fonctions analytiques convergentes et bornées sur D_ν. D'un point de vue algébrique, $\mathfrak{S}_\nu$ est un anneau local de dimension 2 mais il n'est malheureusement pas régulier (sauf si ν est entier) de sorte que le théorème d'Iwasawa ne s'applique pas. Cependant, la construction Max, elle, s'étend comme suit : si M est un sous-$\mathfrak{S}_\nu$-module de $\mathfrak{S}_\nu[1/p]^d$, on pose

$$\mathrm{Max}(M) = \left\{ x \in \mathfrak{S}_\nu[1/p]^d \quad \middle| \quad \exists n \in \mathbb{N},\ (\tfrac{u^b}{p^a})^n\, x \in M \text{ et } p^n x \in M \right\} \qquad (\nu = \tfrac{a}{b}).$$

Dans [5], nous étendons la méthode de calcul du Max « à la Cohen » au calcul des Max_ν (quelques difficultés supplémentaires apparaissent) et donnons une borne uniforme sur le nombre de générateurs de $\mathrm{Max}_\nu(M)$ qui s'exprime à partir du développement en fractions continues de ν. Enfin, l'intérêt d'introduire les anneaux $\mathfrak{S}_\nu$ pour notre problème est concrétisé par le théorème suivant :

Théorème 4. *On se donne la représentation PAG d'un élément $x \in \mathfrak{S}_\nu[1/p]^d$. Alors, on peut calculer un nombre rationnel $\nu' > \nu$ ainsi que la représentation PAG de vecteurs $b_1, \dots, b_d$ qui forment une base de $\mathrm{Max}_{\nu'}(\mathfrak{S}_{\nu'}^d + x\mathfrak{S}_{\nu'})$.*

Remarque 5. Le théorème admet plusieurs variantes. Notamment, il existe une version qui stipule que l'on peut calculer $\mathrm{Max}_{\nu'}(M_1 + x\mathfrak{S}_{\nu'})$ où M_1 est un certain sous-$\mathfrak{S}_\nu$-module libre de rang maximal de $\mathfrak{S}_\nu[1/p]^d$ dont on connaît la représentation PAG des vecteurs d'une base.

En termes plus explicites, le théorème affirme que *si l'on s'autorise à changer continuellement la pente ν*, alors on peut faire effectivement faire la plupart des calculs que l'on souhaite sur les $\mathfrak{S}_\nu$-modules. D'un point de vue algorithmique, cela semble signifier que la pente ν doit être pensée comme faisant partie de la précision. Attention toutefois : l'opération Max_ν ne commute généralement pas avec les autres opérations (addition, intersection, *etc.*), ce qui veut dire que des applications répétées du théorème 4 conduisent souvent à un résultat dont la signification n'est pas absolument claire.

David Lubicz et moi-même avons implémenté ces algorithmes en MAGMA [10]. J'ai, par ailleurs, implémenté en SAGE (avec un plus grand souci de complétude) l'algorithmique des anneaux $\mathfrak{S}_\nu$ [11], mais je n'ai pas encore eu le temps de m'attaquer aux modules sur ceux-ci.

Calcul de réseaux dans les représentations semi-stables

Références :

[6] X. Caruso, D. Lubicz, *Un algorithme de calcul de réseaux dans les représentations semi-stables*, prepublication (2013)

[12] X. Caruso, *Effective Computations in p-adic Hodge Theory*, librairie SAGE (2013), version préliminaire

Forts des résultats du paragraphe précédent, nous pouvons maintenant nous attaquer au problème du calcul des réseaux dans les représentations semi-stables *via* la théorie de Kisin. C'est l'objet de l'article [6] que j'ai écrit à nouveau en collaboration avec David Lubicz. Précisément, le but de cet article est de décrire un algorithme :

- qui prend en entrée une représentation semi-stable à poids de Hodge-Tate positifs ou nuls, donnée par l'intermédiaire de son (φ, N)-module filtré de Fontaine, et
- renvoie le module de Kisin d'un réseau $T \subset V$ stable par le sous-groupe G_∞ (voir l'introduction de la deuxième partie pour le rappel des définitions).

La difficulté dans ce travail réside dans les détails : les idées sous-jacentes à l'algorithme sont fort naturelles et simples — au moins pour qui est familier avec les modules de Kisin — mais leur mise en œuvre nous a fait plutôt suer.

Première étape : le calcul de $\mathfrak{D}$

On commence par calculer le φ-module $\mathfrak{D}$ (sur $\mathfrak{S}[1/p]$) associé au (φ, N)-module filtré D reçu en entrée. Pour cela, on dispose de formules « presque » explicites qui remontent essentiellement à l'article originel de Kisin : pour tout idéal maximal $\mathfrak{m}$ de $\mathfrak{S}[1/p]$, il existe un morphisme injectif $\iota_{\mathfrak{m}} : \mathfrak{D}/\mathfrak{m}\mathfrak{D} \to \mathfrak{S}[1/p]/\mathfrak{m} \otimes_W D$ dont on connaît explicitement le conoyau et, de plus, ce conoyau est non nul seulement si $\mathfrak{m} = (\varphi^n(E(u)))$ pour un certain entier n.

On voit déjà ici apparaître une première difficulté : il y a une infinité d'idéaux maximaux $\mathfrak{m}$ pour lesquels le conoyau $\iota_{\mathfrak{m}}$ est susceptible d'être non trivial et donc, *a priori*, une infinité de conditions à prendre en compte. Difficile pour un ordinateur ! La solution, qui m'est apparue évidente après la lecture de l'article [23] de Génestier et de Lafforgue, est à nouveau de remplacer l'anneau $\mathfrak{S}$ par $\mathfrak{S}_\nu$ pour un certain rationnel $\nu > 0$. En effet, dans $\mathfrak{S}_\nu[1/p]$, l'élement $\varphi^n(E(u)))$ est inversible si $n > n_0(\nu)$ où $n_0(\nu) = -\log_p(e\nu)$ avec $e = \deg E$. Ceci a pour effet de supprimer la contrainte correspondante et de ramener ainsi à une quantité finie le nombre de conditions à satisfaire. Nous reformulons alors le problème en termes purement matriciels et le résolvons à l'aide d'outils classiques (essentiellement le lemme chinois et la décomposition LU).

En contrepartie, si nous choisissons de travailler avec $\mathfrak{S}_\nu$ en lieu et place de $\mathfrak{S}$, nous ne calculons pas $\mathfrak{D}$ mais bel et bien $\mathfrak{D}_\nu = \mathfrak{S}_\nu \otimes_{\mathfrak{S}} \mathfrak{D}$. Toutefois, cela ne prête pas à conséquence grâce à un théorème de surconvergence des modules de Kisin que nous démontrons également dans notre article. Précisément, pour tout nombre rationnel $\nu \geqslant 0$, nous définissons un *module de Kisin* sur $\mathfrak{S}_\nu$ de $E(u)$-*hauteur* $\leqslant r$ comme la donnée d'un $\mathfrak{S}_\nu$-module libre $\mathfrak{M}_\nu$ muni d'un endomorphisme semi-linéaire $\varphi : \mathfrak{M}_\nu \to \mathfrak{M}_\nu$ dont l'image engendre un $\mathfrak{S}_\nu$-module qui contient $E(u)^r\mathfrak{M}_\nu$. (On remarquera que, lorsque $\nu = 0$, on retrouve la notion classique de module de Kisin.)

Théorème 6 (Surconvergence des modules de Kisin)**.** *Soient r un entier strictement positif et ν un nombre rationnel dans l'intervalle $[0, \frac{p-1}{per}[$. Le foncteur*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{modules de Kisin sur } \mathfrak{S} \\ \text{de } E(u)\text{-hauteur } \leqslant r \end{array} \right\} & \longrightarrow & \left\{ \begin{array}{c} \text{modules de Kisin sur } \mathfrak{S}_\nu \\ \text{de } E(u)\text{-hauteur } \leqslant r \end{array} \right\} \\ \mathfrak{M} & \mapsto & \mathfrak{M}_\nu = \mathfrak{S}_\nu \otimes_{\mathfrak{S}} \mathfrak{M} \end{array}$$

est une équivalence de catégories.

Deuxième étape : calcul d'un réseau

À présent que nous avons déterminé $\mathfrak{D}_\nu$, il reste à trouver un $\mathfrak{S}_\nu$-réseau $\mathfrak{M}_\nu \subset \mathfrak{D}_\nu$ qui soit stable par φ et de $E(u)$-hauteur $\leqslant r$ où r désigne le plus grand poids de Hodge-Tate de la représentation semi-stable qui correspond à $\mathfrak{D}$. On notera que l'entier r est très facile à déterminer car il est égal au plus grand saut de la filtration sur le (φ, N)-module filtré D.

À nouveau, l'idée est ce qu'il y a de plus naturel : en quelques mots, on part d'un réseau quelconque que l'on sature jusqu'à ce le rendre stable par φ. Toutefois, comme je l'ai expliqué à la fin de la section sur l'algorithmique des $\mathfrak{S}$-modules, faire ces calculs en pratique sur ordinateur demande de modifier continuellement la pente ν. De nombreux problèmes techniques se posent alors ; voici les deux principaux :

- il faut contrôler le plus précisément possible la croissance de la pente ν afin de s'assurer qu'elle ne dépasse jamais la valeur limite $\frac{p-1}{per}$;
- il faut s'assurer qu'à la fin, le module que l'on calcule est libre sur un anneau $\mathfrak{S}_\nu$ (en effet on rappelle que, lorsque ν n'est pas entier, un module de la forme $\mathrm{Max}_\nu(M)$ n'a pas de raison d'être libre).

Dans [6], nous apportons des solutions à chacun de ces problèmes et obtenons *in fine* un algorithme de complexité polynomiale en tous les paramètres pertinents.

J'ai déjà écrit un premier brouillon d'une implémentation en SAGE de cet algorithme [12] ; il fonctionne, pour l'instant, uniquement sur des petits exemples, ce qui semble suggérer qu'un important travail d'optimisation doit encore être fourni.

Interlude : Décomposition LU des matrices p-adiques

Référence : [4] X. Caruso, *Random matrices over a DVR and LU factorization*, prepublication (2012)

Dans la première étape de l'algorithme précédent, nous avons utilisé, en tant qu'outil, la décomposition LU des matrices p-adiques. J'en suis venu, de cette façon, à me poser la question de la stabilité — au sens de l'analyse numérique — des méthodes classiques. Sans véritable grande surprise, je me suis rendu compte que la méthode usuelle du pivot de Gauss était très instable. Pour illustrer ceci, considérons une matrice carrée aléatoire [6] M de taille $n \times n$ à coefficients dans $\mathbb{Z}_p$ connus à précision $O(p^N)$. Si $M = LU$ est la décomposition LU de M (qui existe presque sûrement), calculer la matrice L à l'aide d'une décomposition de Gauss demande de diviser successivement n fois par un pivot. Or, sachant que (1) on peut montrer que ces pivots sont distribués uniformément dans $\mathbb{Z}_p$, (2) l'espérance de la valuation d'un élément de $\mathbb{Z}_p$ est $\frac{1}{p-1}$ et (3) diviser par un élément de valuation v fait chuter la précision d'un facteur p^{2v} environ [7], on obtient une perte de précision moyenne de l'ordre de $\frac{2n}{p-1}$. (Cela signifie, qu'après calcul, la précision la plus faible sur un coefficient de L sera en moyenne approximativement $O(p^{N-2n/(p-1)})$.)

À côté de cela, il existe des formules de type Cramer qui permettent d'exprimer chaque coefficient de la matrice L comme un quotient de deux déterminants, le dénominateur étant toujours un mineur principal de M (c'est-à-dire le déterminant d'une sous-matrice de M obtenue en supprimant les k dernières lignes et les k dernières colonnes de M). Dans [4], je démontre le résultat suivant :

Théorème 7. *Soit $V : M_n(\mathbb{Z}_p) \to \mathbb{N}$ la variable aléatoire qui à une matrice M associe la plus grande valuation d'un mineur principal de M. Alors $\mathcal{E}[V] = \log_p n + O(1)$ et $\sigma(V) = O(1)$ où les $O(1)$ sont absolus (*i.e. *majorés par des constantes qui ne dépendent d'aucun paramètre).*

Il résulte de ce théorème que l'utilisation des formules de type Cramer fournit une seconde méthode, qui s'avère beaucoup plus stable, pour calculer la matrice L de la décomposition LU de M. En effet, on obtient comme ceci une perte de précision de l'ordre de $2 \cdot \log_p n$, à comparer avec $\frac{2n}{p-1}$ que l'on a trouvé précédemment. Malheureusement, on le sait bien, les formules de Cramer ne sont pas adaptées à l'algorithmique car elles sont très longues à évaluer. Dans [4], je propose un algorithme (qui, par certains aspects, ressemble à l'algorithme de Bareiss) qui combine les avantages de la stabilité des formules de Cramer et de la rapidité de la réduction à la Gauss. En réalité, j'obtiens même une version rapide de cet algorithme — en $O(n^\omega)$ au lieu de $O(n^3)$ où ω est l'exposant de la multiplication des matrices — en adaptant les méthodes usuelles de Hafner et McCauley [25].

L'algorithmique des φ-modules en torsion

Référence : [27] J. Le Borgne, *Représentations galoisiennes et φ-modules : aspects algorithmiques*, thèse (2012)

Revenons à présent à nos moutons, c'est-à-dire au calcul de la semi-simplifiée $\bar{V}^{\mathrm{ss}}$ de notre représentation semi-stable V. Rappelons que l'on a déjà calculé le module de Kisin $\mathfrak{M}_\nu$ (pour une certaine pente $\nu < \frac{p-1}{per}$) ; il ne nous reste donc plus qu'à calculer la semi-simplifiée de la représentation de G_∞ associée à $\mathfrak{M}_\nu/p\mathfrak{M}_\nu$. Bien que cette dernière étape ne soit pas mon travail à proprement parler mais celui de mon étudiant Jérémy Le Borgne, j'aimerais quand même la mentionner rapidement pour donner un aperçu plus complet de l'unité de mon activité — et, en particulier, rendre limpide le lien avec la partie suivante.

À vrai dire, les résultats de Le Borgne ne concernent pas les φ-modules sur $\mathfrak{S}_\nu/p\mathfrak{S}_\nu$ mais ceux sur $k[[u]]$. Toutefois, cela n'est pas gênant car il suit d'un résultat classique que tout φ-module $\tilde{\mathfrak{M}}$ sur $k[[u]]$ vérifiant

$$k[[u]]/u^a \otimes_{k[[u]]} \tilde{\mathfrak{M}} \simeq k[[u]]/u^a \otimes_{\mathfrak{S}_\nu} \mathfrak{M}_\nu \qquad \text{avec } a = \left\lceil \frac{1+per}{p-1} \right\rceil$$

définit la même représentation galoisienne que $\mathfrak{M}_\nu/p\mathfrak{M}_\nu$. Autrement dit, on peut remplacer $\mathfrak{M}_\nu/p\mathfrak{M}_\nu$ par $\tilde{\mathfrak{M}}$ et supposer ainsi que le φ-module avec lequel on travaille est défini sur $k[[u]]$.

6. Chaque coefficient de la matrice est tirée selon la mesure de Haar sur $\mathbb{Z}_p$.

7. Précisément, si $x \in \mathbb{Z}_p$ et $y \in \mathbb{Z}_p^\times$, on a

$$\frac{x + O(p^N)}{p^v y + O(p^N)} = \frac{p^{-v}x + O(p^{N-v})}{y + O(p^{N-v})} = (p^{-v}x + O(p^{N-v}) \cdot (y^{-1} + O(p^{N-v}) = \frac{x}{y} + O(p^{N-2v+v_p(x)}).$$

Classification des représentations irréductibles de G_∞

Si la classification des représentations irréductibles de G_∞ à coefficients dans un corps *algébriquement clos* de caractéristique p (penser à $\bar{\mathbb{F}}_p$, bien sûr) fait partie des résultats classiques, il semble que personne ne s'était encore vraiment penché sur la classification des représentations irréductibles de G_∞ à coefficients dans $\mathbb{F}_p$ (ou, plus généralement, dans un corps fini de caractéristique p). Un premier résultat de Le Borgne a été de combler cette lacune de la littérature. À une $\mathbb{F}_p$-représentation comme ci-dessus, Le Borgne associe une pente μ (qui est un nombre rationnel modulo une certaine relation d'équivalence) ainsi qu'(une classe de similarité d')un polynôme tordu [8] $P(X)$ irréductible à coefficients dans une certaine extension finie de $\mathbb{F}_p$ et démontre que ces deux paramètres classifient les $\mathbb{F}_p$-représentations irréductibles de G_∞.

Réduction des φ-modules sur $k((u))$

On sait que la catégorie des $\mathbb{F}_p$-représentations de G_∞ est équivalente à la catégorie des φ-modules étales sur $k((u))$. Les objets simples de ces deux catégories doivent donc se correspondre bijectivement ; ainsi, les φ-modules simples étales sur $k((u))$ devraient être paramétrés par un couple $(\mu, P(X))$ où μ est une pente et $P(X)$ un polynôme tordu.

Et, de fait, Le Borgne démontre ce résultat de classification des φ-modules simples sans passer par les représentations mais en travaillant uniquement du côté des φ-modules. Hormis le fait qu'il obtient ainsi un résultat un peu plus général, cette approche a l'énorme avantage pour nous d'aboutir à un algorithme qui

- prend en entrée la matrice d'un opérateur φ agissant sur un φ-module étale M, et
- calcule une suite de Jordan-Hölder de M et, pour chaque quotient successif, renvoie le couple $(\mu, P(X))$ qui lui correspond.

Je ne détaille pas davantage cette partie ; pour de nombreux compléments, je vous renvoie à la thèse de Le Borgne.

Factorisation des polynômes tordus sur les corps finis

Références :

[7] X. Caruso, J. Le Borgne, *Some algorithms for skew polynomials over finite fields*, prépublication (2013)
[8] X. Caruso, *Skew polynomials over finite fields*, librairie SAGE (2013)
[28] J. Le Borgne, *Skew polynomials over finite fields*, librairie MAGMA (2013)

Dans la section précédente, nous avons vu apparaître l'anneau $k[X, \sigma]$ (où k est un corps fini et σ est un automorphisme de k) des polynômes tordus. Étant donné, en outre, que les φ-modules simples correspondent aux polynômes irréductibles, on imagine sans mal qu'à un moment donné dans l'algorithme de Le Borgne, on est amené à factoriser un polynôme de $k[X, \sigma]$. C'est ainsi que Le Borgne et moi-même nous sommes intéressés à la factorisation des polynômes tordus et, en particulier, à l'article de Giesbrecht [24] faisant autorité en la matière. Notre objectif initial était simplement d'implémenter l'algorithme (il semblerait que cela n'ait jamais vraiment été fait) mais, en lisant l'article de Giesbrecht, nous nous sommes rapidement rendus compte que nous savions l'améliorer de façon substentielle en plusieurs endroits. Nous avons donc entrepris un travail de plus grande envergure.

Rappelons rapidement que $k[X, \sigma]$ est un anneau euclidien à gauche et à droite et donc, en particulier, principal à gauche et à droite. Un théorème de Öre affirme que tout $P \in k[X, \sigma]$ se décompose comme produits d'irréductibles $P = P_1 \cdots P_n$ et que, dans deux telles décompositions, le nombre de facteurs est toujours le même et, mieux encore, les facteurs se correspondent [9] deux à deux. Le centre de $k[X, \sigma]$ est également facile à déterminer : c'est l'anneau des polynômes sur k^σ en la variable X^r où, par définition, k^σ désigne le sous-corps des points fixes de σ et r est l'ordre de σ. Une autre propriété très intéressante que nous avons mis en évidence [10] dans [7] est donnée par la proposition suivante :

8. Si $\mathbb{F}_q$ est un corps fini de caractéristique p muni d'un automorphisme σ, l'anneau (non commutatif) des polynômes tordus — aussi appelé parfois anneau de Öre — $\mathbb{F}_q[X, \sigma]$ est l'ensemble $\mathbb{F}_q[X]$ muni de l'addition usuelle et de la multiplication qui résulte la loi $X \cdot a = \sigma(a) \cdot X$.

9. Ils ne sont pas égaux comme dans le cas commutatif, mais similaires, ce qui est une relation d'équivalence un peu plus compliquée.

10. Nous n'avons pas réussi à trouver une trace antérieure de cette propriété dans la littérature, bien que l'on trouve de nombreux énoncés très proches (notamment des versions moins fortes) dont la difficulté est comparable.

Proposition 8. *Le localisé $k[X,\sigma][\frac{1}{X}]$ est une algèbre d'Azumaya*[11] *sur son centre $k^\sigma[X^r][\frac{1}{X^r}]$.*

Cette proposition a plusieurs conséquences très intéressantes pour le problème de la factorisation. La première d'entre elles est l'existence d'une application *norme réduite* $\mathcal{N} : k[X,\sigma] \to k^\sigma[X^r]$ que l'on peut définir, par exemple, en recollant l'application déterminant sur un recouvrement étale qui trivialise $k[X,\sigma][\frac{1}{X}]$. Cette application jouït des propriétés suivantes héritées des propriétés classiques du déterminant :

(i) elle est multiplicative

(ii) si P est central, alors $\mathcal{N}(P) = P^r$

(iii) P divise $\mathcal{N}(P)$.

La seconde conséquence de la proposition 8 est l'existence, pour tout polynôme irréductible $N \in k^\sigma[X^r]$, $N \neq X^r$, d'un isomorphisme (non canonique) :

$$k[X,\sigma]/N \simeq M_r(k^\sigma[X^r]/N). \tag{2}$$

En effet, $k[X,\sigma]/N$ est une algèbre simple centrale sur le corps fini $k^\sigma[X^r]/N$; elle est donc isomorphe à une algèbre de matrice sur ce corps puisque les groupes de Brauer des corps finis sont triviaux (par le théorème de Wedderburn). On déduit de l'isomorphisme (2) que les algèbres $k[X,\sigma]/N$ et $k^\sigma[X^r]/N$ sont Morita-équivalentes, c'est-à-dire qu'il existe une équivalence de catégories entre la catégorie des modules à gauche sur $k[X,\sigma]/N$ et la catégorie des modules sur $k^\sigma[X^r]/N$. Ces observations ont, à nouveau, d'importantes conséquences sur l'application $\mathcal{N}$; en effet, nous montrons qu'elles entraînent les deux énoncés suivants :

(iv) un polynôme P est irréductible dans $k[X,\sigma]$ si, et seulement si $\mathcal{N}(P)$ est irréductible dans $k^\sigma[X^r]$; en particulier, si $P = P_1 \cdots P_n$ est la décomposition de P en facteurs irréductibles, alors $\mathcal{N}(P) = \mathcal{N}(P_1) \cdots \mathcal{N}(P_n)$ est la décomposition de $\mathcal{N}(P)$ en facteurs irréductibles (dans $k^\sigma[X^r]$)

(v) réciproquement, si N est un facteur irréductible de $\mathcal{N}(P)$, alors il existe $Q \in k[X,\sigma]$ qui divise P à droite et vérifie $\mathcal{N}(Q) = N$.

Nous en venons ensuite aux applications algorithmiques. Nous obtenons des algorithmes pour le calcul de la norme réduite et en déduisons une première réduction pour le problème de la factorisation. En effet, partant de $P \in k[X,\sigma]$, on peut calculer $\mathcal{N}(P)$ et trouver un facteur irréductible N de ce dernier polynôme dans l'anneau de polynômes commutatifs $k^\sigma[X^r]$. Le polynôme $\text{RGCD}(N,P)$ (où RGCD signifie « plus petit commun diviseur à droite ») est alors un diviseur (à droite) de P qui a la propriété supplémentaire de diviser un polynôme irréductible du centre.

Pour le problème de factorisation, on peut donc supposer sans perte de généralité que le polynôme $P \in k[X,\sigma]$ à factoriser divise un polynôme irréductible $N \in k^\sigma[X^r]$. Cette hypothèse additionnelle nous met en bonne position pour utiliser l'isomorphisme (2) ainsi que l'équivalence de Morita qui en résulte. Précisément, en utilisant ces ingrédients, nous démontrons dans [7], d'une part, que $\mathcal{N}(P) = N^e$ pour un certain entier $e \leqslant r$ et, d'autre part, qu'il existe une bijection (abstraite) entre l'ensemble des diviseurs à droite de D et l'espace projectif standard de dimension $e-1$ sur le corps fini $k^\sigma[X^r]/N$. Ceci nous permet de reformuler la question de la factorisation en une question d'algèbre linéaire pure qui est celle de la construction d'une droite dans un certain espace vectoriel de dimension e, que l'on appelera V. Malheureusement, en pratique, nous n'avons que peu de prise sur V ; notamment, on ne connaît pas ses éléments et on sait donc encore moins les manipuler. Nous arrivons, par contre, à obtenir une description sympathique de son anneau des endomorphisme $\text{End}(V)$ et à interpréter à l'aide de RGCD les diviseurs qui correspondent au noyau et à l'image d'un élément de $\text{End}(V)$. Ceci nous permet de déterminer un diviseur irréductible de P en procédant comme suit : (1) on tire un élément aléatoire de $\text{End}(V)$, (2) on calcule son polynôme minimal χ, (3) on calcule une racine simple $\alpha \in k^\sigma[X^r]/N$ de χ — une telle racine avec probabilité $\geqslant 0,3$ — et (4) on calcule et on renvoie le diviseur correspondant à l'espace propre de α (qui est une droite).

Les idées expliquées ci-dessus conduisent à un algorithme complet de factorisation de complexité

$$\tilde{O}(dr^3 + d\log^2 q + d^{1+\varepsilon}(\log q)^{1+O(1)}) + F(d,q) \qquad \text{opérations binaires} \tag{3}$$

11. On rappelle qu'une algèbre d'Azumaya est une algèbre qui est localement une algèbre de matrices pour la topologie étale.

où d désigne le degré du polynôme à factoriser, q est le cardinal du corps fini k^σ, ε est n'importe quel nombre réel strictement positif et, enfin, $F(d,q)$ est la complexité de la factorisation d'un polynôme *commutatif* sur un corps de cardinal q. Actuellement, la meilleure valeur asymptotique connue pour $F(d,q)$ est dûe à Kedlaya et Umans [26] et vaut :

$$F(d,q) = \left(d^{3/2+o(1)} + d^{1+o(1)} \log q\right) \cdot (\log q)^{1+o(1)}.$$

On remarque que si $r^3 \ll d$, le terme dominant de (3) est $F(d,q)$; autrement dit, toujours sous l'hypothèse $r^3 \ll d$, notre algorithme de factorisation des polynômes tordus est d'une complexité équivalente aux meilleurs algorithmes de factorisation des polynômes commutatifs.

À titre de comparaison, l'algorithme de Giesbrecht a pour complexité

$$\tilde{O}(d^4 r^2 \log q + d^3 r^3 \log q + d^{\omega+1} r^\omega \log q + d^2 r \log^2 q) \qquad \text{opérations binaires.}$$

Nous sommes donc meilleurs sur tous les plans.

Au niveau de l'implémentation, Le Borgne a écrit une librairie MAGMA [28] incluant l'algorithme de factorisation des polynômes tordus et j'ai moi-même écrit une librairie SAGE sur le sujet [8] qui est encore plus complète.

Entracte : Une étude théorique des gammes musicales

Référence : [3] X. Caruso, *Application des fractions continues à la construction des gammes musicales*, RMS 123-1

Suite à un exposé auquel j'ai assisté au séminaire des doctorants en géométrie de Rennes sur les gammes musicales, je me suis un temps intéressé à la question et ai écrit un petit article — dont je ne peux que trop mal juger de l'originalité — dans lequel je définis une axiomatique des gammes musicales (avec et sans tempérament) ainsi que la notion de *gamme optimale*. Je démontre que la gamme usuelle (à 12 notes, bien tempérée), ainsi que d'autres gammes courantes (comme la gamme pentatonique ou la gamme des solfèges) sont des gammes optimales. J'ai proposé cet article à la Revue de Mathématiques Spéciales (RMS) qui l'a publié dans son numéro 123-1.

Troisième partie : Quelques travaux en cours

Une réflexion générale sur la précision p-adique

Référence : [9] X. Caruso, *p-adic precision*, librairie SAGE (2013), version *très* préliminaire

Lors de mes pérégrinations algorithmiques, j'ai été plusieurs fois confronté au problème de la précision p-adique sous différentes formes. On en a, en fait, déjà vu apparaître une instance dans la partie « *Décomposition LU des matrices p-adique* » où je me posais la question de la stabilité de la réduction de Gauss dans le monde p-adique. En réalité, ma première rencontre sérieuse avec ce problème est antérieure à cela et remonte à une discussion que j'ai eue avec David Roe à l'automne 2010. La motivation de Roe était de développer une « nouvelle philosophie » du calcul sur les p-adiques dont l'idée directrice était celle de la séparation de l'approximation et de la précision. Par exemple, pour le calcul du déterminant d'une matrice p-adique M connue avec une certaine précision H — où H est un certain sous-espace de $M_n(\mathbb{Z}_p)$, typiquement un sous-$\mathbb{Z}_p$-module — Roe proposait de procéder en deux étapes indépendantes comme suit :

1. on relève M en $\tilde{M} \in M_n(\mathbb{Z})$ et on calcule le déterminant de $\tilde{M}$ (éventuellement modulo une grande puissance de p)
2. on calcule, à partir de M et H, la précision du résultat, c'est-à-dire le plus grand entier N — ou, peut-être, une bonne approximation inférieure de celui-ci — tel que :

$$\det(M+H) \subset \det \tilde{M} + O(p^N) \tag{4}$$

Un des intérêts de cette approche est de garantir une gestion optimale des pertes de précision — ou, au moins, une bonne gestion de celles-ci dans le cas où l'on ne saurait pas déterminer l'entier N optimal — qui, de surcroît, *ne dépend pas* de l'algorithme utilisé par le calcul du déterminant. Celui-ci peut donc être très instable, cela n'est *a priori* pas génant. Toutefois, à l'époque, Roe ne

savait pas comment déterminer de façon efficace cet entier N. Nous avons donc réfléchi à ce problème ensemble et l'avons finalement rapidement résolu. Mais, mieux encore, ce faisant, nous avons dégagé la proposition suivante (très facile) qui fournit un cadre général pour résoudre toutes les questions du même type.

Proposition 9. *Soient X et Y deux $\mathbb{Q}_p$-espaces vectoriels de dimension finie et $f : X \to Y$ une application de classe C^1. Soit $x \in X$. On suppose que df_x est surjective. Alors, pour tout $\mathbb{Z}_p$-réseau H inclus dans X, on a :*

$$f(x + p^n H) = f(x) + p^n df_x(H) \tag{5}$$

pour n suffisamment grand.

Analysons un instant le contenu de l'équation (5). Elle dit que si l'entrée x est connue avec précision $p^n H$, alors la sortie $f(x)$ est connue *exactement* avec précision $p^n df_x(H)$. Il en résulte que l'on peut espérer une gestion optimale de la précision en considérant uniquement des précisions H qui sont des $\mathbb{Z}_p$-modules et en calculant des différentielles ! Comme, en outre, les différentielles se composent, on peut également imaginer une implémentation des p-adiques où, lors de l'exécution d'une certaine procédure, l'ordinateur calcule, en même temps que les valeurs des différentes variables, les « différentielles » qui conduisent à ces valeurs et, de ce fait, soit en mesure à tout moment de connaître la précision optimale de n'importe quelle variable (au moins, dans le cas, où la proposition 9 s'applique).

Telle qu'elle est énoncée, la proposition 9 souffre de deux problèmes majeurs. Le premier est que l'on ne dispose *a priori* d'aucun contrôle sur l'entier n qui apparaît. On peut néanmoins espérer en obtenir en supposant la fonction f plusieurs fois différentielles, voire analytique. Je n'ai pas encore entièrement étudié la question mais je pense que, sous cette hypothèse supplémentaire, on peut obtenir des bornes explicites et facilement calculables sur n en fonction d'un « polygône de Newton » des différentielles successives de f défini comme l'enveloppe convexe des points de coordonnées (i, v_i) où v_i désigne l'infimum des valuations de $\frac{\partial^{\underline{i}} f}{\partial x^{\underline{i}}}$ où $\underline{i}$ parcourt l'ensemble des multi-indices de somme i.

Le second problème avec la proposition 9 est qu'elle suppose que X et Y sont des $\mathbb{Q}_p$-espaces vectoriels de dimension finie. Or, il arrive que l'on ait à travailler avec des éléments qui vivent dans des espaces de dimension infinie, voire dans des structures plus exotiques. Je pense notamment à des séries p-adiques (qui vivent dans des espaces de dimension finie) ou encore à des points sur une courbe elliptique p-adique ou des sous-espaces vectoriels d'un espace donnée (qui sont naturellement des éléments d'une grassmanienne). Cependant, tout cela n'est pas vraiment gênant (au moins d'un point de vue théorique) car la proposition 9 s'étend assez facilement au cas où X et Y sont des variétés localement modelées sur des espaces de Banach p-adiques, la précision H étant alors un $\mathbb{Z}_p$-réseau fermé qui vit dans l'espace tangent.

David Roe et moi-même sommes en train [12] d'écrire un article reprenant et détaillant les idées précédentes. Je suis également en train d'écrire une nouvelle implémentation des p-adiques en SAGE qui propose une gestion très fine de la précision p-adique (ce qui inclut notamment le fait de laisser de laisser l'ordinateur tout gérer automatiquement à partir du résultat de la proposition 9). Une première version très incomplète de cette libraire est déjà disponible [9].

Calcul explicite de certains anneaux de déformation

Il s'agit d'un travail que j'ai débuté il y a déjà plusieurs années avec Agnès David et Ariane Mézard après avoir entendu un exposé de David sur la question et m'être immédiatement rendu compte que les méthodes algorithmiques que j'étais en train de développer pouvaient apporter une aide substantielle.

Le but de ce travail est de calculer explicitement, dans la veine de [18], certains anneaux de déformation dits *non génériques* (voir plus bas pour une définition) qui appraissent dans la version raffinée de la conjecture de Breuil-Mézard énoncée dans *loc. cit.* Précisément, soient F une extension finie non ramifiée de $\mathbb{Q}_p$ et E une extension de $\mathbb{Q}_p$ suffisamment grande que l'on supposera contenir au moins F. On appelle $\mathcal{O}_E$ (resp. ϖ_E, resp. k_E) l'anneau des entiers (resp. une uniformisante, resp. le corps résiduel) de E et on note G_F le groupe de Galois absolu de F. On se donne en outre une représentation $\bar{\rho} : G_F \to \bar{\mathbb{F}}_p$ de dimension 2 et un caractère $\psi : G_F \to \bar{\mathbb{Z}}_p^\times$. Pour simplifier, on suppose que $\bar{\rho}$ est irréductible. À partir de ces données, on sait construire une $\mathcal{O}_E$-algèbre noethérienne locale complète $R^\psi(\bar{\rho})$ vérifiant la propriété suivante : pour toute $\mathcal{O}_E$-algèbre locale artinienne A de corps résiduel k_E, l'ensemble $\mathrm{Hom}(R(\bar{\rho}), A)$ s'identifie canoniquement à l'ensemble des A-représentations

12. Avec, il faut l'avouer, très peu d'avancement depuis longtemps.

libres de rang 2 de G_F (modulo isomorphisme) dont le déterminant est ψ et la réduction modulo l'idéal maximal de A est isomorphe à $\bar{\rho}$. L'anneau $R^{\psi}(\bar{\rho})$ s'appelle l'*anneau de déformation universel* de $\bar{\rho}$. Il vient naturellement avec une $R^{\psi}(\bar{\rho})$-représentation libre de rang 2 — qui correspond essentiellement [13] au morphisme identité de $R^{\psi}(\bar{\rho})$ dans lui-même — que l'on appelle la *déformation universelle* de $\bar{\rho}$.

Depuis Kisin [29], on sait construire des quotients de $R^{\psi}(\bar{\rho})$ qui paramètrent (dans un certain sens que nous ne préciserons pas davantage dans ce texte) les déformations de $\bar{\rho}$ qui sont potentiellement semi-stables et dont les poids de Hodge-Tate et le type [14] sont fixés. Si v désigne un vecteur de poids de Hodge-Tate et t un type, on note généralement $R^{\psi}(\bar{\rho}, v, t)$ le quotient $R^{\psi}(\bar{\rho})$ correspondant. Les $R^{\psi}(\bar{\rho}, v, t)$ sont généralement difficiles à calculer mais une conjecture — souvent appelée *conjecture de Breuil-Mézard* bien qu'elle prenne de multiples formes qui ne sont pas toujours dues à ces auteurs — donne des renseignements précis sur la fibre générique $k_E \otimes_{\mathcal{O}_E} R^{\psi}(\bar{\rho}, v, t)$. La version numérique de la conjecture de Breuil-Mézard prédit la multiplicité d'Hilbert-Samuel de cette fibre générique ; d'après elle, on devrait avoir

$$\mathrm{mult}_{\mathrm{HS}}(k_E \otimes_{\mathcal{O}_E} R^{\psi}(\bar{\rho}, v, t)) = \sum_{\sigma \in D} m(\sigma, \bar{\rho}) \cdot m(\sigma, v, t).$$

De nombreuses notations sont apparues ci-dessus. Tout d'abord, l'ensemble D est l'ensemble des *poids de Serre*, c'est-à-dire des $\bar{\mathbb{F}}_p$-représentations irréductibles de $\mathrm{GL}_2(k_E)$. Le nombre $m(\sigma, v, t)$ est un entier positif ou nul qui a une définition *explicite* en termes de représentations de $\mathrm{GL}_2(k_E)$ — que nous omettons pour ce document. En contrepartie, le terme $m(\sigma, \bar{\rho})$ est bien plus mystérieux dans le sens où la conjecture ne prédit pas la valeur de ces nombres, mais uniquement leur existence et le fait qu'ils soient des entiers strictement positifs.

L'objectif de notre travail avec David et Mézard est de calculer quelques [15] nombres $m(\sigma, \bar{\rho})$ dans le cas où t est non ramifié et $v = (0, 1)$ pour chaque plongement de F dans $\bar{\mathbb{Q}}_p$, cas pour lequel la conjecture est Breuil-Mézard a été démontrée par Gee et Kisin [22]. Sous ces hypothèses supplémentaires, quelques simplifications apparaissent. Par exemple, les nombres $m(\sigma, v, t)$ ont le bon goût de prendre uniquement les valeurs 0 et 1. On note $D(t)$ l'ensemble des poids de Serre σ tels que $m(\sigma, v, t) = 1$; ce sont les poids du type t et on peut les décrire entièrement à l'aide de formules combinatoires relativement simples. Des résultats partiels sont également connus sur les mystérieux nombres $m(\sigma, \bar{\rho})$: d'après [18], on sait qu'ils valent 1 dès que la représentation $\bar{\rho}$ est générique dans le sens suivant.

Définition 10. On pose $f = [F : \mathbb{Q}_p]$, on note I_F le sous-groupe d'inertie de G_F et, pour tout entier h, on appelle $\omega_h : I_F \to \bar{F}_p$ le caractère fondamental de Serre de niveau h.

La représentation $\bar{\rho}$ est dite *générique* si

$$\bar{\rho}_{|I_F} \simeq \omega_f^n \otimes (\omega_{2f}^m \oplus \omega_{2f}^{p^f m}) \tag{6}$$

où m et n sont des entiers tels que l'écriture en base p de m ne comporte aucun des chiffres 0, 1, $p-2$, $p-1$.

Remarque 11. Toute représentation irréductible $\bar{\rho}$ satisfait à la condition (6) pour certains n et m. Seulement, il n'est pas toujours possible de choisir m satisfaisant la condition de la définition ci-dessus.

En fait, Kisin conjecture que les $m(\sigma, \bar{\rho})$ valent toujours 1, et c'est ce que nous souhaitions vérifier ou infirmer. Pour calculer les $m(\sigma, \bar{\rho})$, nous avions pour projet de suivre la méthode de [18] qui passe par la détermination explicite de l'anneau $R^{\psi}(\bar{\rho}, v, t)$. La stratégie est la suivante :

(1) on classifie, grâce à la théorie de Kisin [16] tous les réseaux dans les représentations potentiellement semi-stables à poids de Hodge-Tate $(0, 1)$ pour tout plongement $F \hookrightarrow \bar{\mathbb{Q}}_p$;

(2) pour chaque réseau T comme ci-dessus, on calcule la représentation $T/\varpi_E T$ et on fait la liste des réseaux T pour lesquels $T/\varpi_E T$ est isomorphe à $\bar{\rho}$;

(3) à partir de la liste précédente, on construit un anneau R et une R-représentation libre de rang 2 de G_F, candidats à être respectivement l'anneau de déformation $R^{\psi}(\bar{\rho}, v, t)$ que l'on cherche et la déformation universelle de $\bar{\rho}$ vue comme cet anneau ;

13. Il faut prendre quelques précautions car $R^{\psi}(\bar{\rho})$ n'est pas une algèbre artinienne.
14. Le type est la représentation de Weil-Deligne associée ; voir [21] pour une définition.
15. Voire tous...
16. Dans [18], les auteurs n'utilisent pas la théorie de Kisin mais la théorie de Breuil. Cela dit, la traduction entre les deux est presque transparente et, selon nous, les calculs avec la théorie de Kisin sont plus faciles à mener.

(4) on démontre que les candidats ci-dessus sont bel et bien ce que l'on attend.

Dans notre situation, l'étape (1) est identique au cas de Breuil et Mézard, à la reformulation près entre théorie de Breuil et théorie de Kisin. Toutefois, pour expliquer au mieux les difficultés que nous avons rencontrées par la suite, j'aimerais dire quelques mots sur la classification en question. Cette dernière fait intervenir la notion de genre : un *genre* est la donnée d'un f-uplet de symbôles, chacun étant pris dans l'ensemble à trois éléments $\{\mathrm{I}_\eta, \mathrm{I}'_\eta, \mathrm{II}\}$. À tout réseau T comme il convient, on associe un genre $g = (g_1, \dots, g_f)$ ainsi qu'un f-uplet $(b_1, \dots, b_f)$ d'élements de $\mathcal{O}_E$ tels que $v_p(p) < v_p(b_i) < +\infty$ pour tout i tel que $g_i = \mathrm{II}$, et on obtient ce faisant un $(2f)$-uplet $(g_1, \dots, g_f, b_1, \dots, b_f)$ qui classifie les réseaux qui nous intéressent.

En ce qui concerne l'étape (2), le fait de travailler avec la théorie de Kisin plutôt qu'avec celle de Breuil nous a permis de simplifier, et surtout de rendre entièrement automatique, la méthode pour le calcul de $T/\varpi_E T$. Nous avons entièrement implémenté cette étape en SAGE : nous avons écrit une fonction qui prend en entrée une représentation $\bar\rho$ et renvoie la liste dont il est question dans l'étape (2) ; d'après la classification de l'étape (1), les éléments de cette liste sont des $(2f)$-uplets $(g_1, \dots, g_f, b_1, \dots, b_f)$. Des exemples de résultats sont disponibles en ligne à

`https://cethop.math.cnrs.fr:8443/home/pub/8/`

Ces listes sont très différentes de celles qui appairaissent dans le cas des représentations génériques traité par Breuil et Mézard. En effet, dans le cas générique, tous les éléments de la liste partageaient les mêmes g_i, ainsi que les mêmes $\bar b_i = b_i \bmod \pi_E$. Dans nos exemples non génériques, plusieurs genres peuvent apparaître et les $\bar b_i$ parcourent l'ensemble des E-points d'une variété algébrique définie sur $\mathbb{F}_p$ qui peut être de dimension $\geqslant 1$; en particulier, leur nombre peut dépendre du corps des coefficients E.

Ces « anomalies » font qu'il est nettement plus difficile de trouver le bon candidat R de l'étape (3). En effet, si l'on a l'habitude de travailler avec des anneaux de déformation, on aimerait croire que chaque valeur possible pour le $(2f)$-uplet $(g_1, \dots, g_f, \bar b_1, \dots, \bar b_f)$ détermine une composante irréductible de R. Or, cela n'est pas possible dans notre cas car il est bien connu que le nombre de composantes irréductibles de R ne dépend aucunément du E. Nous avons étudié en détails un exemple numérique [17] pour lequel il apparaît que les différentes valeurs de $(g_1, \dots, g_f, \bar b_1, \dots, \bar b_f)$ déterminent non pas des composantes irréductibles mais des ouverts rigides qui s'entremêlent de manière non triviale. Nous espérons que ce phénomène se répète dans la situation générale, mais ne savons pour le moment pas le démontrer.

Quoi qu'il en soit, à partir de chaque $(2f)$-uplet $(g_1, \dots, g_f, \bar b_1, \dots, \bar b_f)$ qui apparaît dans la liste, on peut définir un anneau *explicite* R muni d'un morphisme $f : R^\psi(\bar\rho, v, t) \to R$ qui donne, après réduction modulo π_E, un morphisme $\bar f : k_E \otimes_{\mathcal{O}_E} R^\psi(\bar\rho, v, t) \to \bar R = k_E \otimes_{\mathcal{O}_E} R$. De la forme (connue) de $\bar R$, on déduit que l'image de $\operatorname{Spec} \bar f$ est une composante irréductible de $\operatorname{Spec}(k_E \otimes_{\mathcal{O}_E} R^\psi(\bar\rho, v, t))$. On aurait pu espérer, comme c'est souvent le cas, que $\operatorname{Spec} \bar f$ soit une immersion fermée — ce qui revient à dire que $\bar f$ est surjectif — mais malheureusement, ce n'est pas le cas en général dans les exemples non génériques que nous considérons. Nous avons cependant mis au point une méthode, basée sur des calculs de certains Ext^1, pour calculer l'image de $\bar f$ et, par suite, $\operatorname{Spec}(\operatorname{im}\bar f)$ qui est isomorphe à l'image de $\operatorname{Spec} \bar f$ dans $\operatorname{Spec}(k_E \otimes_{\mathcal{O}_E} R^\psi(\bar\rho, v, t))$. On obtient comme ceci une description de certaines composantes irréductibles de $\operatorname{Spec}(k_E \otimes_{\mathcal{O}_E} R^\psi(\bar\rho, v, t))$ et, de ce fait, une estimation de la multiplité d'Hilbert-Samuel de ce dernier schéma. Toutefois, ce travail est encore en cours et nous n'avons pas encore bien compris les résultats obtenus. À suivre.

D'autres développements autour des polynômes tordus

Après notre travail avec Le Borgne [7], j'ai continué à m'intéresser à la factorisation des polynômes tordus définis sur des corps plus généraux que les corps finis. Je présente ci-après quelques unes des réflexions que je me suis faite à ce sujet qui n'ont pour l'instant pas donner lieu à publication mais devraient le faire prochainement.

Factorisation des polynômes tordus sur les corps p-adiques

Le premier exemple que j'ai régardé est celui des corps p-adiques, c'est-à-dire des corps K qui sont des extensions finis de $\mathbb{Q}_p$. Si σ est un automorphisme continu de K — c'est-à-dire un élément

17. À savoir $f = 2$, $p = 7$, $\bar\rho = \omega_4^3$.

de $\mathrm{Gal}(K/\mathbb{Q}_p)$ — on rappelle que l'anneau des polynômes tordus $K[X,\sigma]$ est l'anneau des polynômes usuels $K[X]$ avec la multiplication modifiée résultant de la règle $X \cdot a = \sigma(a) \cdot X$ (pour tout $a \in K$).

La factorisation dans $K[X,\sigma]$ est directement réliée à la décomposition des φ-modules sur K ; précisément si $P \in K[X,\sigma]$, l'espace quotient $D_P = K[X,\sigma]/K[X,\sigma]P$ est naturellement un φ-module (l'action de φ étant donnée par la multiplication par X) et une factorisation de P correspond à une suite de Jordan-Hölder de D_P. Or, il existe un résultat classique sur la décomposition des φ-modules sur les corps p-adiques non absolument ramifiés : c'est le théorème de Dieudonné-Manin qui affirme que, lorsque $K/\mathbb{Q}_p$ est non ramifiée, tout φ-module sur K s'écrit, de façon unique, comme une somme directe de sous-modules isoclines.

Je me suis rapidement rendu compte que ce résultat admettait un analogue simple dans le contexte de la factorisation dans $K[X,\sigma]$, sans hypothèse additionnelle sur K. Pour l'énoncer, je commence par définir le polygone de Newton d'un élément P de $K[X,\sigma]$ comme le polygone de Newton du polynôme P sous-jacent considéré comme élément de $K[X]$. On a alors :

Proposition 12. *Soit $P \in K[X,\sigma]$. Soient $\alpha_1, \dots, \alpha_n$ les pentes (deux à deux distinctes) du polygone de Newton de P et, pour tout $i \in \{1,\dots,n\}$, soit d_i la multiplicité (c'est-à-dire la longueur sur l'axe des abscisses) de la pente α_i. Alors P se factorise sous la forme*

$$P = P_1 \cdot P_2 \cdots P_n \tag{7}$$

où $P_i \in K[X,\sigma]$ est un polynôme de degré d_i et dont le polygone de Newton a une unique pente qui est α_i.

Bien entendu, la proposition précédente étend le résultat classique de « factorisation par pentes » des polynômes p-adiques usuels. Remarquons que l'énoncé de la proposition ne suppose pas que les pentes α_i sont triées par ordre croissant ou décroissant. Ainsi on en déduit qu'il y a une factorisation (7) pour chaque ordre possible des α_i ; bien sûr, comme l'anneau $K[X,\sigma]$ n'est pas commutatif, il n'est pas clair — et pas vrai d'ailleurs — que les polynômes P_i eux-mêmes restent inchangés lorsque l'on passe d'un ordre à un autre. Par ailleurs, notons que la démonstration de la proposition 12 est très effective : elle fournit en fait un algorithme qui calcule la factorisation (7). Celui-ci est linéaire en la précision que l'on souhaite atteindre, ce qui n'est sans doute pas optimal. Je continue à travailler à l'amélioration de cette complexité. Une dernière remarque importante est que l'on peut déduire le théorème de Dieudonné-Manin de la proposition 12. On obtient, de cette façon, une nouvelle démonstration du théorème de Dieudonné-Manin qui est entièrement effective et aussi plus simple dans le sens où elle ne demande pas de travailler avec une clôture algébrique de K et d'utiliser des théorèmes de descente.

En complément de cela, signalons que l'approche que nous avions suivie avec Le Borgne dans notre article [7] s'étend, au moins en partie, à cette nouvelle situation. En particulier, la proposition 8 vaut encore si l'on remplace le corps fini k par le corps p-adique K. L'isomorphisme (2), par contre, n'est plus valide, le problème étant que les corps p-adiques ont un groupe de Brauer non trivial. Pour un polynôme irréductible $N \in K^\sigma[X^r]$, $N \neq 0$, on a en fait uniquement

$$K[X,\sigma]/N \simeq M_s(F)$$

où F est une algèbre à divisions sur $K^\sigma[X^r]/N$ et $s = \frac{r}{\sqrt{\dim F}}$. Toutefois, il s'avère que cela n'est pas vraiment gênant ; en effet, je me suis aperçu qu'en utilisant la classification des algèbres à divisions sur les corps p-adiques, on pouvait *a priori* déterminer F par des méthodes simples de nature combinatoire. En outre, une fois que F est connue, les arguments de [7] semblent s'adapter *verbatim*. Un travail de vérification et de rédaction reste à faire mais celui-ci devrait être routinier et aboutir rapidement à un algorithme complet et efficace de factorisation des polynômes tordus p-adiques.

Sur le calcul de la p-courbure d'un polynôme différentiel

Récemment, j'ai été invité au séminaire de calcul formel du LIX pour présenter les résultats que nous avions obtenus avec Le Borgne. À l'issue de mon exposé, Alin Bostan m'a demandé s'il pensait que nos méthodes pourraient également s'appliquer à l'anneau des opérateurs différentiels $k\langle x,\delta\rangle$ où k est un corps fini. Je m'étais de fait déjà posé la question tant il est vrai que $k\langle x,\delta\rangle$ ressemble par bien des aspects à un anneau de polynômes tordus, mais Bostan avait une question plus précise à

laquelle je n'avais pas pensé : il se demandait avec quelle complexité vis à vis de p, on pouvait calculer la p-courbure [18] d'un opérateur différentiel $P \in k\langle x, \delta\rangle$ si k est de un corps fini de caractéristique p.

Très rapidement (le temps de rentrer en train à Rennes), je me suis rendu compte que les méthodes de mon exposé, si elles ne permettaient, semble-t-il, pas de calculer la p-courbure elle-même, permettaient néanmoins d'envisager un nouvel angle d'attaque pour calculer son polynôme caractéristique. En effet, on peut démontrer la proposition suivante :

Proposition 13.

(i) L'algèbre $k\langle x, \delta\rangle$ est une algèbre d'Azumaya sur son centre $k[x^p, \delta^p]$.

(ii) Pour tout polynôme $P \in k\langle x, \delta\rangle$ unitaire, le polynôme caractéristique de la p-courbure de P s'identifie à sa norme réduite.

Remarque 14. Contrairement au cas des polynômes tordus, il est clair ici que l'alinéa (i) de la proposition 13 était déjà bien connue. Par contre, je n'ai pas trouvé, pour l'instant, de référence dans la littérature pour l'alinéa (ii).

À partir de la proposition 13, il y a plusieurs possibilités pour calculer efficacement la polynôme caractéristique de la p-courbure. Je présente rapidement ci-après celle qui a ma préférence. On introduit l'opérateur d'Euler $\theta = x\delta \in k\langle x, \delta\rangle$; il satisfait à la relation

$$\delta \cdot \theta = (\theta + 1) \cdot \delta \tag{8}$$

de sorte que l'anneau $k\langle \theta, \delta\rangle$ est un anneau de polynômes tordus à coefficients dans l'anneau $k[\theta]$ muni de l'automorphisme $\theta \mapsto \theta + 1$. De plus, on a une inclusion (stricte) $k\langle \theta, \delta\rangle \hookrightarrow k\langle x, \delta\rangle$ qui a la propriété algorithmique intéressante suivante : étant donné un polynôme $P \in k\langle x, \delta\rangle$, on peut rapidement décider si $P \in k\langle \theta, \delta\rangle$ et le cas échéant l'écrire comme élément de cet anneau. Par ailleurs, l'algèbre $k\langle \theta, \delta\rangle$ est, elle-même, une algèbre d'Azumaya sur son centre $k[\theta^p - \theta, \delta^p]$ et on a le diagramme commutatif :

$$\begin{array}{ccc} k\langle \theta, \delta\rangle & \longrightarrow & k\langle x, \delta\rangle \\ \mathcal{N}\downarrow & & \downarrow\mathcal{N} \\ k[\theta^p - \theta, \delta^p] & \xrightarrow{\theta^p - \theta \mapsto x^p\delta^p} & k[x^p, \delta^p] \end{array}$$

où $\mathcal{N}$ désigne les normes réduites. Avec un peu de travail supplémentaire, on se ramène, de cette façon, au calcul de la norme réduite dans $k\langle \theta, \delta\rangle$ et, par suite, au calcul du polynôme caractéristique de la matrice δ^p agissant sur un quotient de la forme $k\langle \theta, \delta\rangle / k\langle \theta, \delta\rangle P$. De la relation de commutation (8), on ramène le calcul de l'action de δ^p à une « exponentielle de matrices » pour laquelle on connait des algorithmes en $O(\sqrt{p})$. Mettant tout ensemble, on obtient un algorithme de calcul du polynôme caractéristique de la p-courbure ayant cette même complexité, améliorant ainsi nettement les précédentes méthodes connues.

Avec Alin Bostan et Éric Schost, nous sommes en train de rédiger ce travail qui pourrait être soumis au prochain congrès ISSAC.

Rayon de convergence des équations différentielles p-adiques

À la suite d'une des réunions du projet CETHop, j'ai commencé à m'intéresser avec Gilles Christol et Andrea Pulita au calcul effectif sur machine du rayon de convergence d'une équation différentielle linéaire p-adique. Initialement, nous nous intéressions au cas des équations différentielles de rang 1 suivant les travaux de Christol [20], mais récemment, Pulita a proposé une nouvelle méthode pour aborder le problème en rang quelconque [30]. La méthode de Pulita utilise de façon essentielle de nombreux *pull-back* par Frobenius, ce qui a l'inconvénient de faire croître, possiblement de façon très importante, le rang de l'équation différentielle que l'on considère. Il en résulte que l'algorithme que l'on obtient ainsi a une complexité exponentielle et n'est donc pas vraiment utilisable dans la pratique.

Je me suis rendu compte que l'on pouvait éviter cette explosion en éliminant au fur et à mesure du processus les éléments parasites, ce qui revient concrètement à factoriser (selon les pentes) un polynôme différentiel à coefficients dans $\mathcal{R}\langle x, \delta\rangle$ et à ne conserver que certains facteurs. L'anneau $\mathcal{R}$ qui vient d'apparaître est l'anneau de Robba borné, c'est-à-dire l'anneau des séries convergentes

18. Je rappelle que, dans ce contexte, la p-courbure de P est simplement la matrice de l'action de δ^p — qui s'avère être un opérateur linéaire — sur le quotient $k\langle x, \delta\rangle / k\langle x, \delta\rangle P$.

bornées sur une couronne d'équation $r < |x| < 1$ pour un certain nombre réel $r < 1$ non précisé (qui dépend de la série). Je n'ai pas encore vérifié tous les détails, mais j'ai bel et bien l'impression que la proposition 12 — ainsi que sa démonstration — s'étend sans difficulté à ce nouveau contexte. Ceci devrait permettre d'améliorer notablement la complexité de l'algorithme de Pulita.

3 Enseignement, formation et diffusion de la culture scientifique

Durant ces cinq derniers semestres, je me suis beaucoup — peut-être trop ? — investi dans la formation et la diffusion de la culture. Ci-dessous, je détaille les points principaux de mon activité.

Enseignement et formation

Cours de M1

En 2011-2012 et 2012-2013, j'ai donné le cours d'*Algorithmique de base* du M1 du master cryptographie de Rennes. Cela a été pour moi l'occasion de compléter ma formation en algorithmique qui était restée, malgré tout, relativement superficielle.

Stages de M2

En 2010-2011, j'ai encadré les stages de M2
- de Tristan Vaccon : le sujet, très classique, consistait à comprendre et à exposer la théorie du corps de classes
- de Cao Tung Pham : le sujet, également très classique, consistait à comprendre et à exposer, la théorie de vecteurs de Witt et son application à la théorie de Artin-Schreier-Witt

Direction de thèse

La thèse de Jérémy Le Borgne

Avec David Lubicz, nous avons codirigé la thèse de Jérémy Le Borgne de septembre 2009 à avril 2012. Sa thèse portait sur l'étude algorithmique des φ-modules ou des (φ, Γ)-modules sur les anneaux de séries formelles et sur les applications aux représentations galoisiennes de corps p-adiques. Pour plus de détails, je vous renvoie à la section « *L'algorithmique des φ-modules en torsion* ».

La thèse de Tristan Vaccon

Tristan Vaccon a commencé sa thèse sous ma direction en septembre 2011. Je lui ai proposé comme sujet la recherche d'algorithmes de calcul d'espaces de déformations galoisiennes (dans la veine de mon travail actuel avec David et Mézard, mais dans des contextes différents). En guise de préliminaire, j'ai suggéré à Tristan de travailler sur les bases de Gröbner p-adiques, sachant qu'il avait déjà précédemment fait un stage sur les bases de Gröbner. Ce second sujet lui a manifestement particulièrement plu car cela fait maintenant deux ans qu'il travaille dessus et obtient constamment de nouveaux résultats intéressants (avec, finalement, très peu d'aide de ma part). Récemment, j'ai quand même réorienté sa recherche vers son sujet initial afin que sa thèse puisse contenir une application originale de ses travaux purement algorithmiques.

La thèse de Charles Savel

Charles Savel a commencé sa thèse sous ma direction en septembre 2011, en même temps que Tristan. Comme sujet, je lui ai proposé d'étudier les conjectures que j'avais émises sur la dimension des variétés de Kisin dans [19]. À l'instar des variétés affines de Deligne-Lusztig auxquelles elles ressemblent beaucoup, ces variétés sont paramétrées par un groupe réductif ; Charles est en train d'étudier le cas du groupe symplectique et de la restriction à la Weil du groupe GL_n (ce qui devrait constituer l'essentiel de sa thèse). Il a d'ores et déjà trouvé une petite erreur dans la formulation de mes conjectures et a su la corriger.

Le séminaire Mathematic Park

En janvier 2010, j'ai été l'instigateur du séminaire *Mathematic Park* et en suis depuis le principal organisateur. Le séminaire, qui se réunit en moyenne une fois par mois (hors vacances scolaires) à l'IHP, est destiné aux étudiants en mathématiques de la première année à la thèse. Les exposés sont donnés par des chercheurs en mathématiques reconnus et portent sur des thèmes variés. Le séminaire connaît un succès appréciable : entre 50 et 150 participants à chaque séance, sachant que certains périodes de l'année sont plus propices que d'autres. Le programme du séminaire est disponible sur le site :

`http://www.ihp.fr/fr/seminaire/mathematic-park`

dont je suis le webmaster.

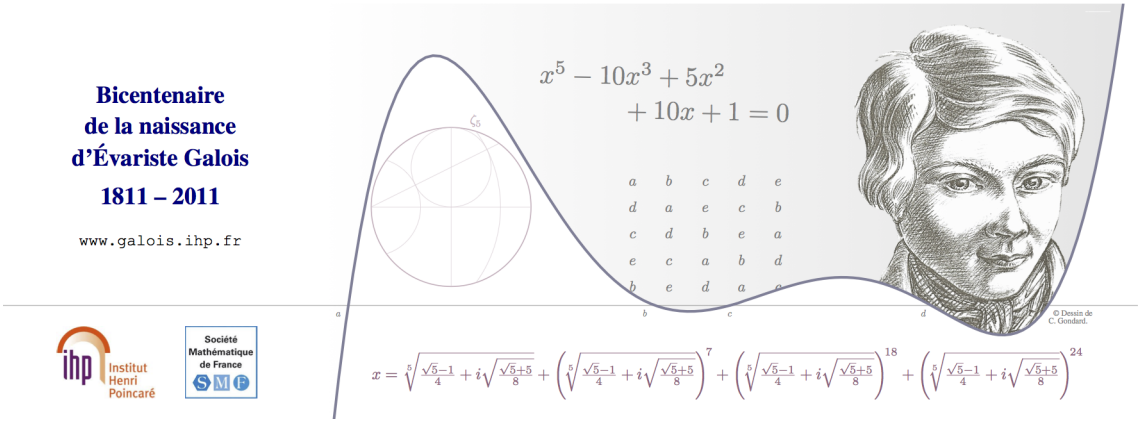
Depuis 2011, j'organise également avec un professeur du lycée Chateaubriand de Rennes une instance du séminaire *Mathematic Park* dans ce lycée. Le séminaire se déroule selon le même principe à l'exception qu'il s'adresse uniquement aux élèves de Chateaubriand.

Bicentenaire de la naissance de Galois

En 2011, nous avons célébré le bicentenaire de la naissance d'Évariste Galois et, à cette occasion, l'IHP, sous l'impulsion de Cédric Villani, a organisé un ensemble de commémorations, à savoir une conférence internationale d'une semaine une après-midi grand public et une exposition.

Villani m'a contacté pour être membre du comité d'organisation de ces diverses commémorations, ce que j'ai accepté avec joie. J'ai participé à ce comité avec enthousiasme :

- j'ai été webmaster du site `http://galois.ihp.fr/`
- j'ai conçu l'« image du mug » que voici :



- j'ai rédigé trois article de vulgarisation pour le site ci-dessus dont voici les titres :
  (1) [13] *Les imaginaires de l'arithmétique* : cet article expose la théorie des corps finis telle que Galois l'a imaginée ;
  (2) [14] *De l'ambiguité des puzzles aux idées de Galois* (avec B. Teheux) : cet article commence par présenter et analyser deux énigmes logiques et en vient de fil en aiguille aux idées de Galois sur l'étude des équations algériques *via* les permutations des racines ; il s'agit d'une présentation qui me paraît tout à fait originale ;
  (3) [15] *À propos de l'image du mug* : j'explique les mathématiques cachées derrière l'image ci-dessus ;

  et en ai sollicité trois autres dont voici les titres :
  (4) *Galois et le jeu de taquin* (par M. Coste) : cet article explique ce qu'est la signature d'une permutation et montre comment celle-ci peut être utilisée pour une application concrète (la résolution du jeu de taquin) ;
  (5) *Résolution des équations de degré* 3 *et* 4 (par A. Marrakchi) : cet article, qui reprend un exposé de Mathematic Park, expose l'analyse de Legendre (*via* la théorie de la permutation des racines) de la résolutation des équations algébriques de degré 3 et 4 ;

(6) *Représentations galoisiennes et théorème de Fermat-Wiles* (par B. Edixhoven) : cet article présente les courbes elliptiques, les représentations galoisiennes qui leur sont associées et explique très rapidement comment celles-ci ont été utilisées par Wiles pour démontrer le grand théorème de Fermat.

– j'ai donné plusieurs interviews.

Participation au rayonnement de l'IHP

Suite à mon implication dans le séminaire *Mathematic Park* d'une part et dans les festivités Galois d'autre part, Cédric Villani me propose désormais régulièrement de participer à des opérations de vulgarisation .

Rédacteur à Images des Mathématiques

C'est ainsi qu'en janvier 2013, je suis entré dans le comité de rédaction de la revue en ligne *Images des Mathématiques* (IdM) en tant que responsable de la rubrique *L'IHP, une maison de sciences pour tous*. Le but de cette rubrique est de donner un écho dans IdM à diverses activités organisées à l'IHP qui sont destinées à un public de non-spécialistes.

Le premier événement que j'ai couvert dans ce cadre est le festival *Futur en Seine* (voir ci-dessous) ; quatre articles sont parus ou à paraître.

Le festival Futur en Seine

Le festival *Futur en Seine* est un rendez-vous annuel où de nombreuses entreprises travaillant dans les sciences du numérique ont l'occasion de présenter leurs dernières innovations. Le festival accueille également des stands d'enseignement ou de diffusion de la connaissance scientifique et/ou technologie et c'est, à ce titre, que depuis plusieurs années l'INRIA y participe

En 2013, pour la première fois, l'IHP s'est joint à l'INRIA pour présenter un stand commun dont l'objectif affiché était de faire de la publicité pour les revues en ligne *Images des Mathématiques* d'une part et *Interstices* (revue d'informatique) d'autre part. J'étais responsable de la partie IHP/IdM et en plus d'avoir fait acte de présence sur le festival pendant trois jours, j'ai imaginé deux petites animations à présenter sur le stand :

(1) une sur l'algorithme de Ford-Fulkerson

(2) une sur le codage de Hamming

L'INRIA, de son côté, a proposé deux autres animations :

(3) une sur les diagrammes de Voronoï

(4) une sur un programme de contrôle optimal

Pour chacune de deux animations de mon ressort, j'ai devéloppé — avec Lionel Fourquaux pour celle sur l'algorithme de Ford-Fulkerson — un petit jeu en javascript et ai écrit un article pour IdM [16, 17].

Semestre de géométrie du Labex Lebesgue

Récemment, l'université de Rennes 1, l'université de Nantes et l'antenne de Bretagne de l'ÉNS de Cachan ont décroché un Labex : le Labex *Lebesgue*. Ce Labex organise un semestre thématique par an. La saison 2013-2014 est dédiée à la géométrie et plus particulièrement aux espaces de modules.

J'ai été propulsé — sans bien comprendre pourquoi — coordinateur de ce semestre. Le travail n'a, à vrai dire, pas encore vraiment commencé mais j'ai déjà rédigé la plupart des pages accessibles depuis

`http://www.lebesgue.fr/content/sem2014-espaces-de-modules`

Je suis également organisateur, avec Christophe Mourougane, de l'école de printemps sur les théories de Hodge classique et p-adique.

Autres

Voici quelques autres activités auxquelles je participe mais pour lesquelles je suis, de fait, relativement peu impliquées :

- les journées Louis-Antoine à Rennes : mon rôle se limite essentiellement à réserver les pauses café ;
- le stage MathC2+ qui a lieu tous les ans à Ker-Lann : j'ai proposé plusieurs sujets et ai participé une fois au café des métiers ;
- le festival des sciences à Rennes où j'ai encadré plusieurs animations.

4 Transfert technologique, relations industrielles et valorisation

5 Encadrement, animation et management de la recherche

Dans le cadre du projet CETHop

Depuis septembre 2009, je suis coordinateur du projet ANR CETHop. À ce titre, j'ai écrit le site web `http://cethop.cnrs.math.fr/` et en suis actuellement webmaster. Outre le contenu standard — liste des membres de l'ANR, liste des publications réalisées dans le cadre de l'ANR, *etc.* — il est à noter que ce site héberge un « SAGE Notebook ». Ce « Notebook » est un serveur sur lequel n'importe qui peut demander un compte ; une fois cela fait, il peut utiliser en ligne les logiciels MAGMA et SAGE et a, en particulier, accès aux librairies qui ont été développés pour ces logiciels dans le cadre du projet CETHop.

Toujours dans ce cadre, j'ai également organisé deux conférences internationales d'une semaine chacune :

- une à l'ENS de Lyon en juin 2011 qui s'intitulait « Théorie de Hodge p-adique, équations différentielles p-adiques et leurs applications »et qui a réuni environ 60 participants ;
- une à Luminy en avril 2013 qui s'intitulait « Représentations galoisiennes et théorie de Hodge p-adique : aspects théoriques et effectifs » et qui a réuni une cinquantaine de participants.

Toujours dans le cadre du projet CETHop, je suis en train d'organiser des SAGE *Days* (il s'agit d'un groupe de travail pour le développement de SAGE) qui devrait réunir entre 15 et 20 personnes à Rennes la première semaine de septembre 2013.

Membres de conseils/comités

Je suis membre de plusieurs comités ou conseils, à savoir :

- le conseil de l'IRMAR (Institut de Recherche en Mathématiques à Rennes),
- le comité scientifique du séminaire de cryptographie de Rennes,
- le comité de pilotage du master cryptographie de Rennes,
- le comité de culture scientifique de l'IHP.

Concrètement, pour chacun de ces items, il s'agit de quelques réunions par an (entre 2 et 4). Cela ne me prend donc que peu de temps.

Comité National de la Recherche Scientifique (CoNRS)

Depuis septembre 2012, comme vous le savez, je suis membre élu du CoNRS.

Bibliographie

Mémoire écrit pendant les 5 derniers semestres

[1] X. Caruso, *Une contribution à la théorie de Hodge p-adique entière et de torsion*, mémoire d'habilitation (2011), 62 pages

Articles de recherche écrits pendant les 5 derniers semestres

[2] X. Caruso, *Représentations galoisiennes p-adiques et (φ,τ)-modules*, à paraître à Duke Math. Journal, 83 pages

[3] X. Caruso, *Application des fractions continues à la construction des gammes musicales*, RMS 123-1 (2012), 11 pages

[4] X. Caruso, *Random matrices over a DVR and LU factorization*, prépublication (2012), 23 pages

[5] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*, prépublication (2012), 38 pages

[6] X. Caruso, D. Lubicz, *Un algorithme de calcul de réseaux dans les représentations semi-stables*, prépublication (2013), 35 pages

[7] X. Caruso, J. Le Borgne, *Some algorithms for skew polynomials over finite fields*, prépublication (2013), 32 pages

Logiciels écrits pendant les 5 derniers semestres

[8] X. Caruso, *Skew polynomials over finite fields*, librairie SAGE (2013), $\sim$ 8000 lignes [19]

[9] X. Caruso, *p-adic precision*, librairie SAGE (2013), version *très* préliminaire, $\sim$ 5000 lignes

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

[11] X. Caruso, *Bounded series over ultrametric rings*, librairie SAGE (2013), version non documentée, $\sim$ 3000 lignes

[12] X. Caruso, *Effective Computations in p-adic Hodge Theory*, librairie SAGE (2013), version préliminaire, $\sim$ 1500 lignes

Articles de vulgarisation écrits pendant les 5 derniers semestres

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

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

[15] X. Caruso, *À propos de l'image du mug*, disponible à `http://www.galois.ihp.fr/ressources/vie-et-oeuvre-de-galois/les-mathematiques-de-galois/a-propos-de-limage-du-mug/`

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

[17] X. Caruso, *Qui est-ce ? — Le codage de Hamming*, à paraître dans Images des Mathématiques

Autres références utilisées dans le document

[18] C. Breuil, A. Mézard, *Multiplicités modulaires raffinées*, à paraître dans Bull. Soc. Math. France

[19] X. Caruso, *Dimension de certaines variétés de Kisin*, prépublication (2010), 55 pages

[20] G. Christol, *The radius of convergence function for first order differential equations*, Contemp. Math. **551** (2011), 71–89

[21] J.-M. Fontaine, *Représentations ℓ-adiques potentiellement semi-stables*, Astérisque **223** (1994), 321–347

[22] T. Gee, M. Kisin, *The Breuil-Mézard conjecture for potentially Barsotti-Tate representations*, prépublication (2013), 36 pages

[23] A. Genestier, V. Lafforgue, *Structures de Hodge-Pink pour les $(\varphi/\mathfrak{S})$-modules de Breuil et Kisin*, Compos. Math. 148 (2012), 751–789

[24] M. Giesbrecht, *Factoring in skew polynomial rings over finite finite fields*, J. Symb. Comp. **26** (1998), 463–486

[25] J. L. Hafner, K. S. McCauley, *Asymptotically fast triangularization of matrices over rings*, SIAM Journal of Comp. **20** (1991), 1068–1083

[26] K. Kedlaya, C. Umans, *Fast modular composition in any characteristic*, Foundations of Computer Science, IEEE Annual Symposium on **0** (2008), 146–155.

[27] J. Le Borgne, *Représentations galoisiennes et φ-modules : aspects algorithmiques* thèse de doctorat (2012), 140 pages

[28] J. Le Borgne, *Skew polynomials over finite fields*, librairie MAGMA (2013), $\sim$ 800 lignes

[29] M. Kisin, *Potentially semi-stable deformation rings*, J. Amer. Math. Soc. **21** (2008), 513–546

[30] A. Pulita, *An algorithm computing non solvable spectral radii of p-adic differential equations*, disponible à `http://arxiv.org/pdf/1301.1124.pdf`, 5 pages

19. Pour une comparaison avec un article, on peut compter 100 lignes pour une page.