Représentations galoisiennes et phi-modules : aspects algorithmiques

Jérémy Le Borgne

N° d'ordre : 4347 ANNÉE 2012

THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Européenne de Bretagne

pour le grade de

DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : Mathématiques et applications

École doctorale Matisse

présentée par

Jérémy Le Borgne

préparée à l'unité de recherche 6625 du CNRS : IRMAR
Institut de Recherche Mathématique de Rennes
UFR de Mathématiques

Représentations galoisiennes et φ-modules : aspects algorithmiques

Thèse soutenue à Rennes le 3 avril 2012

devant le jury composé de :

Kiran S. KEDLAYA
Professor University of California, San Diego/ rapporteur

Jean-François MESTRE
Professeur Université Paris Diderot / rapporteur

Laurent BERGER
Professeur ENS Lyon / examinateur

Pierre BERTHELOT
Professeur Université Rennes 1 / examinateur

Ariane MÉZARD
Professeur UVSQ / examinateur

Xavier CARUSO
CR CNRS Université Rennes 1 / directeur de thèse

David LUBICZ
Chercheur DGA/Université Rennes 1 / directeur de thèse

Jérémy Le Borgne

REPRÉSENTATIONS GALOISIENNES ET φ-MODULES : ASPECTS ALGORITHMIQUES

Jérémy Le Borgne

REPRÉSENTATIONS GALOISIENNES ET φ-MODULES : ASPECTS ALGORITHMIQUES

Jérémy Le Borgne

Résumé. — Nous nous intéressons aux aspects algorithmiques de la théorie des représentations modulo p de groupes de Galois p-adiques. À cet effet, l'un des outils introduits par Fontaine est la théorie de φ-modules : un φ-module sur un corps K de caractéristique p est la donnée d'un espace vectoriel de dimension finie sur K muni d'un endomorphisme φ, semi-linéaire par rapport au morphisme de Frobenius sur K. Les représentations à coefficients dans un corps fini du groupe de Galois absolu de K forment une catégorie équivalente à la catégorie des φ-modules dits « étales » sur K.
Le but des travaux rassemblés ici est donner des algorithmes pour décrire le plus complètement possible la représentation associée à un φ-module donné. Nous étudions en préambule les φ-modules sur les corps finis, ce qui nous permet d'obtenir de nouveaux résultats décrivant les polynômes tordus sur un corps fini, qui sont des objets utilisés notamment en théorie des codes correcteurs. Cela nous permet d'améliorer en partie l'algorithme dû à Giesbrecht pour la factorisation de ces polynômes. Nous nous intéressons ensuite à la catégorie des φ-modules sur un corps de séries formelles de caractéristique p. Nous donnons une classification des objets simples de cette catégorie lorsque le corps résiduel est algébriquement clos, et décrivons un algorithme efficace pour décomposer un φ-module en φ-modules « isoclines ». Nous donnons des applications à l'étude algorithmique des représentations de p-torsion de groupes de Galois p-adiques.

Abstract. — We study algorithmic aspects of the theory of modular representations of p-adic Galois groups. For this purpose, one of the tools introduced by Fontaine is the theory of φ-modules. A φ-modles over a field K of positive characteristic is the data of a finite-dimensional vector space over K, endowed with an endomorphism φ that is semilinear with respect to the Frobenius morphism on K. The category of representations of the absolute galois group of K with coefficients in a finite field is equivalent to that of *étale* φ-modules over K.
The aim of the works collected here is to give algorithms to decribe the representation associated to a given φ-module as completely as possible. First, we study the φ-modules over finite fields, which allows us new results describing the so-called skew polynomials over a finite field. These are objets used for example in the theory of error-correcting codes. We improve a part of the algorithm of Giesbrecht for the factorizations of these polynomials. We the consider the category of φ-modules over a field of formal power series of characteristic p. We give a classification of the simple objects of this category when the residue field is algebraically closed. We decribe an efficient algorithm to decompose a φ-module with *isocline* φ-modules. We give applications to the algorithmic study of p-torsion representations of p-adic Galois groups.

TABLE DES MATIÈRES

REMERCIEMENTS

Je remercie d'abord mes directeurs de thèse, Xavier Caruso et David Lubicz. Cela a été un réel plaisir au cours de ces années de travailler avec eux. Ils m'ont tous deux beaucoup appris sur les mathématiques et sur les exigences du métier de chercheur, sans jamais me rendre la vie trop difficile. Ils ont toujours été d'une grande disponibilité, et très attentifs à mon travail, et je leur suis très reconnaissant pour leur aide et leurs encouragements.

Je remercie aussi Kiran Kedlaya et Jean-François Mestre pour avoir accepté de rapporter ce manuscrit, et pour l'attention qu'ils ont porté à sa lecture. Leurs commentaires m'ont été très précieux. Special thanks to Kiran for reading the material in French and correcting a few mistakes in my English.

C'est un honneur pour moi que Laurent Berger, Pierre Berthelot et Ariane Mézard aient accepté de faire partie de mon jury. Au-delà de leurs qualités de mathématiciens, Ariane et Laurent ont beaucoup compté pour moi en étant parmi les premiers à s'intéresser à mes travaux. Quant à Pierre, cela a toujours été un plaisir de le fréquenter au sein des divers séminaires et groupes de travail de l'IRMAR. Je regrette seulement d'être arrivé trop tard à l'Université de Rennes 1 pour pouvoir suivre ses cours que l'on m'a tant vantés.

L'enseignement a naturellement représenté une part importante de mon travail de doctorant. Je remercie Arnaud Debussche et Michel Pierre de m'avoir offert l'opportunité d'enseigner dans le cadre exceptionnel de l'ENS Cachan Bretagne. C'est un vrai plaisir de faire cours aux élèves et étudiants de cette École ; qu'ils soient eux aussi remerciés pour avoir été (la plupart du temps !) si sérieux, sages, attentifs et motivés. Cela a également toujours été un plaisir de venir à Ker Lann et de participer à la vie du Département. Merci à tous ses membres pour leur accueil chaleureux, particulièrement aux thésards du plateau de maths dont j'ai trop souvent encombré le tableau (et qui me l'ont pardonné).

Au cours de la préparation de ma thèse, j'ai rencontré des mathématiciens qui m'ont aidé, par quelques discussions ou simplement par l'intérêt qu'ils m'ont accordé. Hormis

ceux que j'ai déjà cités, je voudrais remercier David Roe, Agnès David, Lara Thomas, Eugen Hellman, Michael Rapoport, Mark Watkins.

Avant de commencer ma thèse, j'étais aussi un élève de Ker Lann (sérieux, sage, attentif et motivé). Les professeurs de l'École et ceux de l'Université dont j'ai suivi les cours durant ma scolarité m'ont beaucoup apporté et ont certainement contribué à m'attirer vers le monde de la recherche. Je les en remercie tous. J'adresse des remerciements plus particuliers à Grégory Vial, Florent Malrieu, Michel Pierre, Mark Baker, Dominique Cerveau, Michel Coste, Lionel Chaussade et Pascal Autissier ; ceux qui ont suivi leurs cours savent pourquoi. J'adresse également mes remerciements à ceux qui ont encadré mes stages et autres projets par le passé et qui m'ont aussi donné le goût de la recherche : Laurent Gaubert, Pascal Redou, Bruno Chiarellotto et Bernard Le Stum.

Je remercie sincèrement tous les membres de l'IRMAR pour leur accueil, et plus particulièrement l'équipe de géométrie algébrique. C'est un laboratoire où on se sent bien, et où l'ambiance est toujours agréable (même pendant les grèves). Ce serait trop long de tous les citer, mais merci à tous ceux que j'ai cotoyés pendant ces années, et en particulier à Delphine Boucher pour son aide précieuse sur certains points de cette thèse, aux participants aux groupes de travail que j'ai fréquentés pour m'avoir appris tant de choses, ainsi qu'aux organisateurs des Journées Louis Antoine pour m'avoir proposé d'y intervenir. Je pense aussi particulièrement à tous les doctorants avec qui j'ai souvent partagé de bons moments : Damian, Arnaud, Jean-Louis, Basile, Gweltaz, Gaël, Mathilde, Marie, Jean-Romain, Viktoria, Aurélien, François, Élise, Romain, Sandrine, Sébastien, Charles, Mathieu, Mathieu, Nirmal, ... J'ai une pensée particulière pour ceux qui ont partagé mon bureau et le bureau mitoyen : Cécile, Tristan, Lionel, Viviana, Julien, Colas. Je décerne une mention spéciale à Clément, qui est de loin celui qui m'a supporté pendant le plus longtemps, et qui est parvenu malgré tout à rester un excellent cobureau ; rendez-vous à l'Atelier ! Merci aussi à nos presque-voisins Richard et Fanny, notamment pour les parties de Dominion et la Coupe du Monde. Enfin, je suis reconnaissant à tout le personnel administratif de l'IRMAR et de l'UFR, ainsi que les bibliothécaires pour leur compétence et leur sympathie. Je mesure la chance que nous avons que vous soyez si efficaces et motivés.

J'ai rencontré avant la thèse de nombreux amis. J'ai eu l'occasion d'en revoir certains à Ker Lann, au cours de mes déplacements, ou à des conférences, et ils sont toujours d'agréable compagnie. Je remercie particulièrement Alain, Pierre, Camille, Camille, Thibaut et Guillaume. Je remercie aussi Cyril, Delphine, Pierre et Rémi pour les bons moments passés ensemble. Il m'est impossible de parler de mes amis kerlannais sans faire une digression sur mes amis visanais. Sans eux, ma vie n'aurait pas été la même durant ma thèse. Les Visans (de 1 à 3.5, série en cours) sont une vraie bouffée d'air frais à chaque fois (façon de

parler). Merci infiniment à vous tous : Alex, Maël, Raton, Fanny, Elio, François, Guillaume, Coko, Yvain, Guigui, Simon, Pierre, LLD, Nico, Oli, Cécile, Lolo, Pépette, Nounou, Alice, Clémence, Viko, Tom, Thibault, Tibo, Marie, Julien... (sauf deux). Merci aussi aux amis de longue date mais toujours aussi proches, pour le plaisir que j'ai à vous revoir à chaque fois, même si ce n'est pas assez souvent : Élise, Pof, Marien, Cédric, Alan, Marion, Amélie, et toute la troupe du Bout du Monde.

C'est maintenant à ma famille que je voudrais m'adresser. Je remercie mes parents, Marie-Thérèse et Henri. Ils m'ont toujours aidé ; ils m'ont aussi donné le goût d'apprendre, depuis toujours, et encouragé ma curiosité. Ces quelques lignes ne suffisent pas à exprimer toute ma gratitude et mon amour. Je remercie aussi mon frère Brice et ma sœur Floriane. Le temps que je peux passer avec eux m'est très précieux, et pas seulement parce que ce sont deux des personnes les plus drôles du monde. Merci également à ceux qui ont fait le déplacement depuis le Finistère, je suis très touché par votre présence. J'espère que les radars ne vous ont pas vu passer. Enfin, merci à Louisette et Michel pour être venus m'encourager depuis leur lointaine Bourgogne !

Coralie, merci d'être auprès de moi chaque jour. L'existence de cette thèse te doit bien plus que tu ne l'imagines. Avec toi, tout est facile, naturel, drôle, tendre, beau. Ta présence et ton sourire illuminent mes journées et ma vie.

INTRODUCTION

Le but de cette thèse est de développer un point de vue effectif en théorie de Hodge p-adique. La théorie de Hodge p-adique est un outil pour l'étude des représentations galoisiennes p-adiques, développé sous l'impulsion de Jean-Marc Fontaine à partir des années 1970. Nous allons présenter les objets usuels intervenant dans ce contexte : les représentations galoisiennes, ainsi que les objets de la théorie de Hodge p-adique, qui sont des modules sur certains anneaux munis de structures supplémentaires. Nous motiverons l'intérêt de disposer de moyens efficaces pour faire des calculs dans ce domaine, et nous décrirons certains problèmes spécifiques à cette approche. Nous donnerons ensuite plus de détails sur les résultats principaux de la thèse, avant de présenter diverses perspectives de développements futurs.

1. Représentations galoisiennes

1.1. Arithmétique et théorie de Galois. — À l'origine, l'arithmétique s'intéresse aux équations polynomiales à coefficients dans l'anneau des entiers $\mathbb{Z}$. Ces équations sont appelées *équations diophantiennes*, en hommage au savant grec Diophante d'Alexandrie. L'un des problèmes principaux de l'arithmétique est de déterminer les solutions dans $\mathbb{Z}$ d'une équation diophantienne. Parmi les exemples historiques les plus frappants, on peut citer l'équation de Fermat : $x^n + y^n = z^n$, où n est un entier supérieur ou égal à 3 : la conjecture de Fermat, formulée au XVIIe siècle, prédisait que cette équation n'avait pas de solution dans $\mathbb{N}^3$ (telle que $xyz \neq 0$). Il fallut attendre la fin du XXe siècle et les travaux de Wiles et Taylor pour obtenir une démonstration de cette conjecture. Les représentations galoisiennes figurent au nombre des outils utilisés par cette démonstration. Pour comprendre pour quelles raisons elles peuvent intervenir dans ce type de problèmes, commençons par donner quelques éléments de théorie de Galois.

La théorie de Galois s'intéresse à l'origine à l'étude des solutions d'équations algébriques, et ramène certaines questions sur la nature de ces solutions à des questions sur la structure d'un groupe associé à l'équation, appelé *groupe de Galois*. Soient K un corps, et L une extension galoisienne de K, le groupe de Galois $\mathrm{Gal}(L/K)$ est le groupe des automorphismes de L qui fixent K : si P est un polynôme à coefficients dans K, le groupe $\mathrm{Gal}(L/K)$ agit naturellement sur les racines de P dans L. Les racines de P qui sont dans K sont exactement les racines de P dans une clôture algébrique $\overline{K}$ de K et qui sont stables par le groupe de Galois $G_K = \mathrm{Gal}(\overline{K}/K)$, appelé groupe de Galois absolu de K. Ainsi, lorsque l'on cherche des solutions d'une équation diophantienne dans $\mathbb{Z}$, on peut déjà identifier celles qui sont dans $\mathbb{Q}$ comme celles qui sont stables par l'action de $G_{\mathbb{Q}}$. L'étude du groupe $G_{\mathbb{Q}}$ est l'une des questions fondamentales de l'arithmétique moderne.

Pour ne pas manipuler le groupe $G_{\mathbb{Q}}$, dont la structure est très compliquée, on peut se restreindre à certains sous-groupes particulièrement intéressants : on fixe un entier premier p, on considère le corps $\mathbb{Q}_p$ des nombres p-adiques (le complété de $\mathbb{Q}$ pour la valeur absolue p-adique) et on fixe une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ contenant $\overline{\mathbb{Q}}$. Le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) = G_{\mathbb{Q}_p}$, naturellement isomorphe à un groupe de décomposition en une place au-dessus de p. C'est un sous-groupe de $G_{\mathbb{Q}}$ dont la structure est un peu plus simple. On a notamment une suite exacte :

$$1 \to I \to G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p} \to 1,$$

où $\mathbb{F}_p$ est le corps fini de cardinal p, $G_{\mathbb{F}_p}$ est son groupe de Galois absolu, et I s'appelle le *sous-groupe d'inertie* de $G_{\mathbb{Q}_p}$. Le groupe I est par définition celui qui agit trivialement sur l'anneau des entiers de $\overline{\mathbb{Q}}_p$ modulo son idéal maximal $\mathfrak{m}$, et donc le noyau du morphisme naturel $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$. Il admet lui-même le sous-groupe distingué formé par les éléments agissant trivialement sur les extensions modérément ramifiées de $\mathbb{Q}_p$ [1], appelé *groupe d'inertie sauvage*, et noté I_p : il s'agit d'un pro-p-groupe, et le quotient $I/I_p = I_t$, appelé *groupe d'inertie modérée*, est isomorphe au produit $\prod \mathbb{Z}_\ell$, le produit portant sur tous les nombres premiers ℓ différents de p. Ce groupe va jouer un rôle important dans la suite. On peut construire une filtration de $G_{\mathbb{Q}_p}$ par les groupes de ramification d'ordre supérieur, qui stabilisent des extensions de plus en plus ramifiées de $\mathbb{Q}_p$. Cela donne une idée de la structure de $G_{\mathbb{Q}_p}$, mais la structure de I_p n'est en tout cas pas du tout immédiate à décrire.

Ce groupe de Galois est plus simple que $G_{\mathbb{Q}}$, et c'est lui que nous souhaitons maintenant étudier. On peut justifier cette restriction en soulignant qu'un élément de $\overline{\mathbb{Q}}$ stable par tous

1. Une extension modérément ramifiée est une extension dont l'indice de ramification n'est pas divisible par p.

les $G_{\mathbb{Q}_p}$ pour p premier est fixé par $G_{\mathbb{Q}}$ et donc est dans $\mathbb{Q}$. Pour étudier $G_{\mathbb{Q}_p}$, nous allons nous intéresser aux représentations linéaires de ce groupe, c'est-à-dire la façon dont il peut agir sur des espaces vectoriels de dimension finie. Il y a une topologie naturelle sur $G_{\mathbb{Q}_p}$, et nous voulons nous restreindre aux représentations qui sont continues pour cette topologie. Il s'agit de la topologie de la limite projective : le groupe $G_{\mathbb{Q}_p}$ est la limite projective de tous les $\mathrm{Gal}(L/\mathbb{Q}_p)$, où $L/\mathbb{Q}_p$ est galoisienne finie. En particulier, c'est un groupe compact, et les sous-groupes ouverts sont exactement les sous-groupes fermés d'indice fini. Pour qu'il y ait suffisamment de façons de faire agir $G_{\mathbb{Q}_p}$ continûment sur un E-espace vectoriel, où E est un corps topologique, il faut que la topologie de E soit assez proche de celle de $G_{\mathbb{Q}_p}$: cela se produit plus facilement si E est lui-même un corps p-adique. L'objet de la théorie de Hodge p-adique est justement l'étude de représentations de ce type.

1.2. Représentations linéaires de groupes. — L'un des outils puissants pour l'étude des groupes, est d'examiner la façon dont ils agissent linéairement sur un espace vectoriel. Cela tient notamment au fait que pour étudier ces actions, on dispose de toute la machinerie de l'algèbre linéaire. Soient G un groupe et E un corps. Par définition, une représentation de G à coefficients dans E est la donnée d'un E-espace vectoriel V (que nous supposerons de dimension finie ici) et d'un morphisme

$$\rho \ : \ G \to GL(V).$$

Cela revient à demander que G agisse sur V d'une manière compatible à la structure linéaire de V ; d'ailleurs, si $g \in G$ et $v \in V$, on notera souvent gv à la place de $\rho(g)(v)$.
En ce qui concerne les représentations de groupes de Galois p-adiques, on a déjà évoqué le fait que les représentations continues à coefficients dans $\mathbb{C}$ sont assez peu nombreuses. En effet, une représentation continue à coefficients dans $\mathbb{C}$ de $G_{\mathbb{Q}_p}$ se factorise à travers un quotient fini car son noyau est un sous-groupe ouvert de $G_{\mathbb{Q}_p}$ (voir [**Lau02**], §2.1). À l'opposé, si E est un corps p-adique, les représentations à coefficients dans E de $G_{\mathbb{Q}_p}$ sont très nombreuses, et il faut commencer par isoler les plus intéressantes. Pour généraliser un peu, on note K une extension finie de $\mathbb{Q}_p$, et G_K le groupe de Galois absolu de K. On dispose sur G_K du caractère cyclotomique, défini de la manière suivante : on fixe $(\varepsilon_n)_{n\in\mathbb{N}}$ une suite compatible de racines primitives p^n-èmes de l'unité dans $\overline{K}$ (cela signifie que $\varepsilon_0 = 1$, $\varepsilon_1^p = 1$ avec $\varepsilon_1 \neq 1$, et que pour $n \geq 1$, $\varepsilon_{n+1}^p = \varepsilon_n$). Alors, $g \in G_K$ agit sur ε_n par élévation à la puissance $\chi(g)$, où $\chi(g)$ est un entier déterminé modulo p^n. De plus, si g agit par élévation à la puissance $\chi(g)$ sur ε_n, il agit de la même manière sur les ε_i pour $i \leq n$. Cela montre que l'on peut voir l'application $\chi(g)$ comme étant à valeurs dans $\mathbb{Z}_p$:

$$\chi \ : \ G_K \to \mathbb{Z}_p,$$

et le noyau de χ, noté H_K, est le sous-groupe de G_K qui fixe le corps K_∞ engendré par toutes les racines de l'unité d'ordre une puissance de p. Ce corps est appelé la $\mathbb{Z}_p$-*extension cyclotomique* de K, et il jouera un rôle important par la suite, notamment dans la théorie des (ϕ, Γ)-modules. Pour $i \in \mathbb{Z}$, on note $\mathbb{Q}_p(i)$ la représentation de dimension 1 sur laquelle $g \in G_{\mathbb{Q}_p}$ agit par multiplication par $\chi^i(g)$.
Les représentations de la forme précédente font partie des « briques élémentaires » de la théorie. Comme on le voit, elles sont définies sur $\mathbb{Z}_p$. L'un des axes de développement de la théorie est justement l'étude des représentations à coefficients entiers, ou l'étude des réseaux dans les représentations galoisiennes. Soit V une $\mathbb{Q}_p$-représentation de G_K, un $\mathbb{Z}_p$-réseau de V est un sous-$\mathbb{Z}_p$-module libre T stable par G_K tel que $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. La compacité de G_K implique qu'il existe toujours un réseau stable. Si on identifie un tel réseau T, on peut former la représentation $\overline{V} = T/pT$, qui est naturellement une $\mathbb{F}_p$-représentation de G_K. Le théorème de Brauer-Nesbitt assure alors que la semi-simplifée $\overline{V}^{\mathrm{ss}}$ de $\overline{V}$ (qui est par définition la somme directe des constituants de Jordan-Hölder de $\overline{V}$) ne dépend pas du choix d'un réseau stable T. On peut alors se demander quels liens unissent la représentation V à sa « réduction modulo p » , $\overline{V}^{\mathrm{ss}}$.

Dans la suite, nous allons justement nous intéresser également aux représentations de G_K à coefficients dans un corps de caractéristique p. Une classification des représentations irréductibles de G_K à coefficients dans une extension algébrique de $\mathbb{F}_p$ sera donnée plus loin dans cette introduction et démontrée dans le chapitre IV de cette thèse. Mais, pour l'instant, limitons-nous au cas des $\overline{\mathbb{F}}_p$-représentations irréductibles de $G_{\mathbb{Q}_p}$ qui suffira à étayer notre propos. Les caractères fondamentaux de Serre (voir par exemple **[Ser72]**, §1), sont définis sur $G_{\mathbb{Q}_p}$ de la manière suivante : pour tout $n \geq 0$, soit ϖ_n une racine $(p^n - 1)$-ème de p. On note $\mathbb{Q}_{p^n} \subset \overline{\mathbb{Q}}_p$ l'extension non ramifiée de $\mathbb{Q}_p$ dont le corps résiduel est le corps fini à p^n éléments $\mathbb{F}_{p^n}$. Le caractère fondamental de niveau n est alors l'application $\omega_n : G_{\mathbb{Q}_{p^n}} \to \mathbb{F}_{p^n}^\times$ qui associe à $g \in G_{\mathbb{Q}_{p^n}}$ la classe résiduelle de l'élément $\frac{g\varpi_n}{\varpi_n}$. Remarquons que tous ces caractères sont en particulier définis sur le groupe d'inertie I. Par ailleurs, lorsque h est un entier qui n'est divisible par aucun nombre de la forme $\frac{p^n-1}{p^{n'}-1}$ pour n' divisant n, on dit que h est *primitif* par rapport à n. Si V est une $\overline{\mathbb{F}}_p$-représentation irréductible de $G_{\mathbb{Q}_p}$, alors il existe un entier $n \geq 1$, un entier h primitif par rapport à n, et un caractère non ramifié χ_λ envoyant un relevé dans $G_{\mathbb{Q}_p}$ du Frobenius sur $\overline{\mathbb{F}}_p$ sur $\lambda \in \overline{\mathbb{F}}_p$, tels que

$$V \simeq \left(\mathrm{ind}_{G_{\mathbb{Q}_{p^n}}}^{G_{\mathbb{Q}_p}} \omega_n^h\right) \otimes \chi_\lambda.$$

Pour décrire la semi-simplifiée d'une $\overline{\mathbb{F}}_p$-représentation quelconque V, il faut donc donner les triplets (n, h, λ) correspondant à tous les constituants de Jordan-Hölder de V. Par la suite, lorsque nous chercherons à calculer la semi-simplifiée d'une représentation, nous exprimerons le résultat de cette manière. Notons au passage que les représentations irréductibles de l'inertie, qui se factorisent toutes par l'inertie modérée, sont de la forme ω_n^h avec h primitif par rapport à n. La classe d'isomorphisme de ω_n^h ne dépend que des chiffres de h en base p, dans l'ordre et à permutation circulaire près. En particulier, ces chiffres sont déterminés par la classe d'isomorphisme de la représentation irréductible de I_t considérée, on les appelle les *poids de l'inertie modérée* de la représentation. Plus généralement, les poids de l'inertie modérée d'une représentation quelconque V de G_K sont formés de la collection de tous les poids de l'inertie modérée de la restriction à I_t des consituants de Jordan-Hölder de V.

1.3. Motivations géométriques. — En plus des motivations précédentes pour l'étude des représentations galoisiennes p-adiques, nous voulons mentionner une motivation de nature plus géométrique à l'origine de ce problème. En effet, la géométrie algébrique fournit naturellement de nombreuses représentations galoisiennes p-adiques : si X est une variété propre et lisse sur une extension finie K de $\mathbb{Q}_p$, la cohomologie étale de Grothendieck $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ est une représentation p-adique de G_K. À partir de la donnée de la cohomologie étale d'une variété, on retrouve certaines propriétés de l'objet de départ. Un exemple fondamental de cette construction est celui du module de Tate d'une courbe elliptique (voir [**Ser89**]). Soit $\mathcal{E}$ une courbe elliptique sur $\mathbb{Q}_p$, on note $\mathcal{E}_{\overline{\mathbb{Q}}_p}$ l'ensemble des points de $\mathcal{E}$ sur $\overline{\mathbb{Q}}_p$. Le module de Tate de $\mathcal{E}$ est $T_p(\mathcal{E}) = \lim_{\leftarrow n} \mathcal{E}_{\overline{\mathbb{Q}}_p}[p^n]$, où $\mathcal{E}_{\overline{\mathbb{Q}}_p}[p^n]$ désigne le noyau de la multiplication par p^n dans $\mathcal{E}_{\overline{\mathbb{Q}}_p}$. C'est un $\mathbb{Z}_p$-module qui est naturellement muni d'une action de $G_{\mathbb{Q}_p}$. Ainsi, $V_p(\mathcal{E}) = T_p(\mathcal{E}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ est une $\mathbb{Q}_p$-représentation de $G_{\mathbb{Q}_p}$. Dans ce cas, $H^i_{\text{ét}}(\mathcal{E}_{\overline{K}}, \mathbb{Q}_p) = \bigwedge^i V_p(\mathcal{E})^*$, sur lequel G_K agit par fonctorialité. On peut montrer qu'en particulier, $\det V_p(\mathcal{E}) \simeq \mathbb{Q}_p(1)$.

Un exemple de question d'ordre géométrique est le suivant : quelles sont les représentations p-adiques de $G_{\mathbb{Q}}$ qui se réalisent comme $H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ pour une variété X sur $\mathbb{Q}$? On dit qu'une représentation p-adique de $G_{\mathbb{Q}}$ *provient de la géométrie* si c'est un sous-quotient d'un $H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$. La conjecture de Fontaine-Mazur (voir [**FM95**], [**Kis07**]) prédit que les représentations provenant de la géométrie sont (à torsion par une puissance du caractère cyclotomique près) celles qui sont non ramifiées en tous les premiers sauf un nombre fini, et dont la restriction à $G_{\mathbb{Q}_p}$ est potentiellement semi-stable. Cette dernière notion, liée aux anneaux de périodes, est évoquée plus loin. La conjecture de Fontaine-Mazur est toujours

une question ouverte, bien qu'elle soit prouvée dans certains cas. Plus précisément, on sait qu'une représentation provenant de la géométrie vérifie les propriétés annoncées grâce à des résultats successifs de Fontaine-Messing ([**FM87**]), Faltings ([**Fal88**]) et Tsuji ([**Tsu99**]) entre autres. Parmi les avancées récentes pour la réciproque, on peut citer les travaux de Kisin (voir [**Kis09**]), qui a démontré de nombreux cas de la conjecture pour les représentations de dimension 2 en s'appuyant notamment sur la correspondance de Langlands p-adique établie par Colmez, avec l'aide de Berger-Breuil (voir [**Col10**], [**BB10**]), ainsi que les résultats d'Emerton ([**Eme11**]) s'appuyant aussi sur la correspondance de Langlands p-adique ainsi que des propriétés de compatibilité local-global.

Un autre exemple illustrant le rôle joué par les représentations galoisiennes p-adiques en géométrie est le suivant. Lorsque X est une variété propre et lisse sur $\mathbb{Q}_p$, on a une autre théorie cohomologique que la cohomologie étale p-adique : la cohomologie de de Rham, $H^i_{\mathrm{dR}}(X_K)$, qui est un K-espace vectoriel de dimension finie muni d'une filtration $\mathrm{Fil}^r H^i_{\mathrm{dR}}(X_K)$. À la différence de la cohomologie étale, elle n'est pas munie d'une action de Galois ; par ailleurs, elle peut souvent être calculée explicitement. Le problème du foncteur mystérieux de Grothendieck consiste à trouver un foncteur reliant ces deux théories. Comme nous le verrons plus tard, la stratégie de Fontaine s'inspire de ce qui se passe sur $\mathbb{C}$, et repose sur la construction d'un anneau B, muni d'une action de G_K et d'une filtration, tel que $B \otimes_K H^i_{\mathrm{dR}}(X_K) \simeq B \otimes_{\mathbb{Q}_p} H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. Nous verrons plus loin quelques exemples d'anneaux de ce type, qui sont appelés anneaux de périodes.

2. Théorie de Hodge p-adique

Le lecteur devine le rôle central joué par les travaux de Fontaine, notamment sur les anneaux de périodes, entrevus au paragraphe précédent. Nous allons maintenant donner quelques éléments de compréhension de la théorie de Hodge p-adique, en particulier le rôle de certains anneaux de périodes. L'idée est donc de ramener l'étude de représentations galoisiennes p-adiques à l'étude de modules sur certains anneaux munis de structures additionnelles en lien avec les correspondances visées : action de Galois, filtration, monodromie...

2.1. Les ϕ-modules et les (ϕ, Γ)-modules. — La première équivalence de catégories notable dans la direction évoquée a lieu purement en caractéristique p. Soit K un corps de caractéristique p, et soit K^{sep} une clôture séparable de K. Le groupe de Galois absolu de K est $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Le corps K^{sep} est évidemment muni d'une action de G_K, mais

aussi de l'action $\mathbb{F}_p$-linéaire du Frobenius $\phi : x \mapsto x^p$. On appelle *ϕ-module* sur K la donnée d'un K-espace vectoriel D muni d'un endomorphisme ϕ_D, semi-linéaire par rapport à ϕ, c'est-à-dire tel que pour $\lambda \in K$ et $x \in D$, $\phi_D(\lambda x) = \phi(\lambda)\phi_D(x)$. On dit de plus qu'un ϕ-module est *étale* si $\phi_D(D)$ contient une base de D. On a alors l'anti-équivalence de catégories suivante ([**Fon90**], proposition A.1.2.6) :

$$\left\{ \begin{array}{c} \phi\text{-modules étales} \\ \text{sur K} \end{array} \right\} \to \left\{ \begin{array}{c} \mathbb{F}_p\text{-représentations} \\ \text{de } G_K \end{array} \right\}.$$

Le foncteur réalisant cette anti-équivalence de catégories est $D \mapsto \mathrm{Hom}_\phi(D, K^{sep})$, un quasi-inverse est donné par $V \mapsto \mathrm{Hom}_{G_K}(V, K^{sep})$, et ces foncteurs préservent les dimensions des objets considérés. Les ϕ-modules en caractéristique p seront des objets centraux dans les travaux de ce mémoire.

2.2. Les (ϕ, Γ)-modules. — Soit maintenant $\mathcal{K}$ une extension finie de $\mathbb{Q}_p$ de corps résiduel k, et $H_\mathcal{K}$ le groupe de Galois absolu de la $\mathbb{Z}_p$-extension cyclotomique de $\mathcal{K}$. Si $K = k((u))$ désigne le corps des séries formelles à coefficients dans k, la théorie du corps des normes de Fontaine et Wintenberger établit un isomorphisme entre $H_\mathcal{K}$ et G_K, d'où on déduit une deuxième équivalence de catégories :

$$\left\{ \begin{array}{c} \phi\text{-modules étales} \\ \text{sur K} \end{array} \right\} \to \left\{ \begin{array}{c} \mathbb{F}_p\text{-représentations} \\ \text{de } H_\mathcal{K} \end{array} \right\}.$$

Précisons un peu les résultats sur le corps des normes. On note $\mathcal{O}_{\overline{\mathcal{K}}}$ l'anneau des entiers de $\overline{\mathcal{K}}$. Soit $R = \lim_{\leftarrow n} \mathcal{O}_{\overline{\mathcal{K}}}/p$ où les applications de transition sont $x \mapsto x^p$: c'est le « perfectisé » de $\mathcal{O}_{\overline{\mathcal{K}}}/p$. Il s'agit d'un anneau intègre, qui est même muni d'une valuation (non discrète) v_R. Si $x = (x_n)_{n\in\mathbb{N}}$, et si $\mathbb{C}_p$ est le complété de $\overline{\mathcal{K}}$, on peut définir une application $\theta : R \to \mathcal{O}_{\mathbb{C}_p}$ par la formule $\theta(x) = \lim_{n\to+\infty} \hat{x}_n^{p^n}$, où $\hat{x}_n$ est un relevé quelconque de x_n dans $\mathcal{O}_{\overline{\mathcal{K}}}$. Le résultat ne dépend pas des relevés choisis, et par définition, $v_R(x) = v_K(\theta(x))$. Le corps des fractions $\mathrm{Frac}R$ de R est bien défini, et on peut montrer qu'il est algébriquement clos. Remarquons que si $\underline{\varepsilon} = (\varepsilon_n)_{n\in\mathbb{N}}$ est une suite compatible de racines primitives p^n-èmes de l'unité, alors $\underline{\varepsilon} - 1$ définit un élément de R de valuation strictement positive. Soit $\iota : k \to R$ l'injection canonique $\lambda \mapsto (\lambda^{p^{-n}})_{n\in\mathbb{N}}$. On peut prolonger ι en un morphisme d'anneaux $\iota : k((u)) \to \mathrm{Frac}R$ en envoyant u sur $\underline{\varepsilon} - 1$. Le groupe $H_\mathcal{K}$ agit naturellement sur R et fixe tous les éléments de $K = k((u))$. Ainsi, il stabilise K^{sep}, et fournit donc un morphisme de groupes $H_\mathcal{K} \to G_K$. L'un des résulats de Fontaine-Wintenberger (voir [**Win83**], théorème 3.2.2) est que ce morphisme est un isomorphisme. En fait, le même résultat reste vrai si l'on remplace $H_\mathcal{K}$ par le groupe de

Galois absolu d'une extension infinie arithmétiquement profinie de $\mathcal{K}$ (voir [**Win83**] pour la définition), ce qui sera utile pour la théorie de Kisin.

Soit maintenant V une $\mathbb{F}_p$-représentation de $G_{\mathcal{K}}$, la restriction de V à $H_{\mathcal{K}}$ fournit *via* l'équivalence de catégories de Fontaine un ϕ-module étale sur K, naturellement muni d'une action résiduelle de $\Gamma = G_{\mathcal{K}}/H_{\mathcal{K}}$ commutant à celle de ϕ. Plus précisément, en reprenant les calculs du paragraphe précédent, on voit que l'action de $\gamma \in \Gamma$ sur les coefficients est donnée par la formule $\gamma u = (1+u)^{\chi(\gamma)} - 1$. Le groupe Γ agit sur le ϕ-module associé à V de manière semi-linéaire par rapport à cette action sur les coefficients. C'est la donnée d'un ϕ-module étale sur K muni d'une action de Γ vérifiant les propriétés précedentes qu'on appelle un (ϕ, Γ)-*module étale* sur K. On a alors une nouvelle équivalence, qui découle de [**Fon90**], A.3.4.3 :

$$\left\{ \begin{array}{c} (\phi,\Gamma)\text{-modules étales} \\ \text{sur K} \end{array} \right\} \to \left\{ \begin{array}{c} \mathbb{F}_p\text{-représentations} \\ \text{de } G_{\mathcal{K}} \end{array} \right\}.$$

Comme on s'intéresse aux représentations p-adiques plutôt qu'aux $\mathbb{F}_p$-représentations, on essaie de relever ces résultats en caractéristique nulle. C'est encore une construction de Fontaine qui permet de le faire. Soit $\mathcal{O}_{\mathcal{E}}$ le complété p-adique de $W(k)((u))$, et $\mathcal{E}$ son corps des fractions. Les anneaux $\mathcal{O}_{\mathcal{E}}$ et $\mathcal{E}$ sont munis d'un relevé du Frobenius sur K, toujours noté ϕ, ainsi que d'une action de Γ. Pour obtenir une action de $G_{\mathcal{K}}$, on va plonger naturellement $\mathcal{E}$ dans un anneau qui en est muni. Soit $W(\mathrm{Frac}R)$ l'anneau des vecteurs de Witt à coefficients dans $\mathrm{Frac}R$, alors $\mathcal{E}$ se plonge naturellement dans $W(\mathrm{Frac}R)\left[\frac{1}{p}\right]$. Soit $\mathcal{E}^{\mathrm{nr}}$ l'unique extension non ramifiée de $\mathcal{E}$ contenue dans $W(\mathrm{Frac}R)\left[\frac{1}{p}\right]$ dont le corps résiduel est K^{sep} : c'est notre candidat. On donne alors une définition analogue à la précédente pour les (ϕ, Γ)-modules étales sur $\mathcal{E}$, et on a une anti-équivalence de catégories ([**Fon90**], Théorème A.3.4.3) :

$$\left\{ \begin{array}{c} (\phi,\Gamma)\text{-modules étales} \\ \text{sur } \mathcal{E} \end{array} \right\} \to \left\{ \begin{array}{c} \mathbb{Q}_p\text{-représentations} \\ \text{de } G_{\mathcal{K}} \end{array} \right\}.$$

Le foncteur réalisant cette anti-équivalence est $D \mapsto \mathrm{Hom}_{\phi}(D, \mathcal{E}^{\mathrm{nr}})$, un quasi-inverse étant donné par $V \mapsto \mathrm{Hom}_{H_{\mathcal{K}}}(V, \mathcal{E}^{\mathrm{nr}})$.

2.3. Représentations semi-stables, représentations cristallines. — Il y a beaucoup de représentations galoisiennes p-adiques, et seul un nombre restreint d'entre elles provient de la géométrie. L'un des buts de la théorie de Hodge p-adique est justement de comprendre lesquelles, et de les décrire aussi précisément que possible. C'est dans ce but que Fontaine a introduit dans [**Fon94**] un certain nombre d'anneaux, appelés anneaux de

périodes. Nous ne décrirons pas précisément ces anneaux, qui n'interviendront pas directement dans la suite, mais il nous semble intéressant de présenter les idées de Fontaine, pour mieux comprendre les représentations cristallines ou semi-stables, qui apparaîtront au chapitre IV par l'intermédiaire des modules de Kisin et des modules de Wach. Les anneaux de périodes $B_{\mathrm{cris}} \subset B_{\mathrm{st}} \subset B_{dR}$ (pour cristalline, semi-stable, de Rham) sont des $\mathbb{Q}_p$-algèbres topologiques munies d'une action de $G_{\mathbb{Q}_p}$. De plus, B_{dR} est muni d'une filtration dont héritent B_{st} et B_{cris}. Par ailleurs, B_{st} est muni d'un Frobenius ϕ et d'un opérateur de monodromie N vérifiant $N\phi = p\phi N$, et $B_{\mathrm{cris}} = B_{\mathrm{st}}^{N=0}$, ce qui fait que B_{cris} est aussi muni de l'action de ϕ. Si V est une E-représentation de $G_{\mathbb{Q}_p}$, et si B est l'un des anneau précédents, on pose $D_B(V) = \mathrm{Hom}_{G_{\mathbb{Q}_p}}(V, B)$. On peut montrer que $D_B(V)$ un E-espace vectoriel de dimension $\leq \dim_E(V)$, et on dit que V est *cristalline*, *semi-stable* ou *de de Rham* si on a égalité lorsque B est l'anneau correspondant. Par ailleurs, $D_{\mathrm{st}}(V) = D_{B_{\mathrm{st}}}(V)$ hérite d'une filtration, d'un Frobenius et d'un opérateur de monodromie : c'est un (ϕ, N)-*module filtré*. Fontaine a défini dans [**Fon94**] les (ϕ, N)-modules filtrés *admissibles*, et des résultats de Fontaine et Colmez-Fontaine ([**CF00**]) établissent une équivalence entre la catégorie des représentations semi-stables et celle des (ϕ, N)-modules filtrés admissibles. Il y a un résultat analogue pour les représentations cristallines et les ϕ-modules filtrés admissibles. L'un des intérêt de ces constructions est que pour se donner une représentation semi-stable (qui sont en quelque sorte plus intéressantes que les représentations générales, en raison de leur lien avec la géométrie), il suffit de se donner un (ϕ, N)-module filtré admissible, que l'on considère comme plus facile à manipuler.

2.4. Théorie entière et de torsion : modules de Wach, modules de Kisin. — Nous avons déjà mentionné l'intérêt de considérer les réseaux dans une représentation galoisienne, par exemple pour calculer sa réduction modulo p. On peut se demander si les réseaux dans les représentations ont un pendant du côté théorie de Hodge p-adique, c'est-à-dire s'il y a des anneaux de périodes définis sur $\mathbb{Z}_p$ qui permettent de reconstruire les réseaux dans les représentations, d'identifier ceux qui correspondent à des représentations semi-stables ou cristallines. Les développements de la théorie dans cette direction sont plus récents : hormis une première approche due à Fontaine et Laffaille au début des années 1980 (voir [**FL82**]), ce sont les résultats de Breuil vers la fin des années 1990 ([**Bre99a**]) qui ont permis des avancées plus importantes. D'autres développements importants sont dus à Kisin, puis Caruso et Liu, et permettent de mieux comprendre les réseaux dans les représentations semi-stables (voir [**Kis06**], [**CL09**]). De manière analogue, la théorie des (ϕ, Γ)-modules (qui se comporte bien en général avec les réseaux) a un pendant important permettant de comprendre les réseaux dans les représentations qui sont cristallines :

la théorie des modules de Wach. Cette théorie, initiée par Wach dans [**Wac96**] a été reprise avec succès notamment par Berger et Berger-Breuil (voir par exemple [**BB10**]) sur le chemin de l'établissement de la correspondance de Langlands p-adique pour $GL_2(\mathbb{Q}_p)$.

2.4.1. Modules de Wach. — Soit $\mathcal{K}$ une extension finie de $\mathbb{Q}_p$, on fixe $\underline{\varepsilon} = (\varepsilon_n)_{n\in\mathbb{N}}$ une suite compatible de racines primitives p^n-èmes de l'unité, et on note $\mathcal{K}_\infty$ le sous-corps de $\overline{\mathcal{K}}$ engendré par tous les ε_n : c'est le sous-corps fixé par le noyau $H_\mathcal{K}$ du caractère cyclotomique. Comme on l'a déjà vu, $H_\mathcal{K} \simeq G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$, où $K = k((u))$ et k désigne le corps résiduel de $\mathcal{K}$. On note $W = W(k)$ l'anneau des vecteurs de Witt sur k. Soit $r \geq 0$ un entier. On note $\mathcal{O}_\mathcal{E}^+ = W[[u]]$ et $\mathcal{E}^+ = \mathcal{O}_\mathcal{E}^+[1/p]$. On appelle *module de Wach* à poids dans $[-r, 0]$ un $\mathcal{O}_\mathcal{E}^+$-module libre de type fini $\mathcal{N}$, muni d'une action de Γ et d'un endomorphisme semi-linéaire ϕ, tels que :

- l'action de Γ est semi-linéaire par rapport à l'action donnée sur $\mathcal{O}_\mathcal{E}^+$ par $\gamma u = (1 + u)^{\chi(\gamma)} - 1$, et induit l'action triviale sur $\mathcal{N}/u\mathcal{N}$;
- l'action de ϕ et celle de Γ commutent ;
- le sous-$\mathcal{O}_\mathcal{E}^+$-module engendré par $\phi(\mathcal{N})$ contient $\left(\frac{\phi(u)}{u}\right)^r \mathcal{N}$.

On note $B^+ = W(R) \cap \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$. Le résultat suivant est dû à Berger (voir [**Ber04**]), à la suite de travaux de Wach ([**Wac96**]) :

Proposition 2.4.1. — *Si T est un réseau d'une représentation cristalline V de $G_\mathcal{K}$ à poids de Hodge-Tate positifs, alors $D^+(T) = Hom_{\mathbb{Z}_p[G_\infty]}(V, B^+)$ contient un unique sous-$\mathcal{O}_\mathcal{E}^+$-module $\mathcal{N}(T)$ qui soit un module de Wach. De plus, pour une représentation cristalline donnée V, $\mathcal{N}(V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{N}(T)$ ne dépend pas du choix de T, et l'application $T \mapsto \mathcal{N}(T)$ induit une bijection respectant l'inclusion entre les réseaux de V et les modules de Wach contenus dans $\mathcal{N}(V)$ qui en sont un $\mathcal{O}_\mathcal{E}^+$-réseau.*

La donnée d'un module de Wach en torsion est plus simple, et on peut s'efforcer de comprendre algorithmiquement les propriétés de la réduction modulo p d'un réseau dans une représentation cristalline à partir de la donnée de son module de Wach. En effet, si T est un réseau dans une représentation cristalline, et $\mathcal{N}(T)$ est son module de Wach, alors $\mathcal{N}(T)/p\mathcal{N}(T)\left[\frac{1}{u}\right]$ est le (ϕ, Γ)-module sur $k(\!(u)\!)$ qui correspond à la représentation T/pT. Comme I_p agit trivialement sur la semi-simplifiée de cette représentation, l'action de Γ se résume à une action de $\mathrm{Gal}(\mathcal{K}_1/\mathcal{K})$, qui est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$. Nous verrons comment retrouver les poids de l'inertie modérée de la représentation de départ à l'aide de son module de Wach.

2.4.2. Modules de Kisin. — L'approche suivante, initiée par Breuil et perfectionnée par Kisin [(2)], permet de comprendre les analogues entiers des (ϕ, N)-modules filtrés de Fontaine. Nous ne décrirons pas complètement la catégorie des modules de Kisin ici, mais la définition apparaît dans le chapitre IV. Soit $\mathcal{K}$ une extension finie de $\mathbb{Q}_p$, de corps résiduel k. L'anneau $\mathfrak{S} = W(k)[[u]]$ est muni d'un Frobenius ϕ agissant comme le Frobenius habituel sur $W(k)$, et par $u \mapsto u^p$ sur u. Soit $\mathcal{O}$ l'anneau des séries en la variable u convergentes sur le disque ouvert de centre 0 et de rayon 1, il est muni d'une dérivation N_∇ et du Frobenius ϕ. Les (ϕ, N_∇) sont des modules sur cet anneau muni d'opérateurs ϕ et N_∇ vérifiant des conditions de compatibilité, et Kisin a construit dans **[Kis06]** une équivalence entre la catégorie des (ϕ, N_∇)-modules et celle des (ϕ, N)-modules filtrés de Fontaine.

Si on oublie l'action de N_∇, on obtient des ϕ-modules sur $\mathcal{O}$. Soit $\mathcal{K}'_\infty = \bigcup_{n\geq 0} \mathcal{K}(\pi_n)$ où π_n est une suite compatible de racines p^n-èmes de l'uniformisante de $\mathcal{K}$, et $G_\infty = \mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K}'_\infty)$. La théorie du corps des normes montre que $G_\infty \simeq G_K$, et Kisin démontre que si on se donne un ϕ-module $\mathcal{M}$ sur $\mathcal{O}$, le ϕ-module $\mathcal{E} \otimes_{\mathcal{O}} \mathcal{M}$ correspond à la restriction à G_∞ de la représentation semi-stable associée par l'intermédiaire de la théorie de Fontaine. Il montre de plus que les réseaux stables par G_∞ dans cette représentation correspondent aux $\mathfrak{S}$-réseaux stables par ϕ dans $\mathcal{O}_{\mathcal{E}} \otimes_{\mathcal{O}} \mathcal{M}$.

Les objets de p-torsion correspondants sont plus faciles à décrire, ce que nous faisons brièvement maintenant. Soit e l'indice de ramification de $\mathcal{K}/\mathbb{Q}_p$, et $r \geq 1$ un entier. On appelle *module de Kisin* (de p-torsion) de hauteur $\leq r$ un $k[[u]]$-module de type fini $\mathfrak{M}$, sans u-torsion, muni d'un Frobenius $\phi : \mathfrak{M} \to \mathfrak{M}$ (semi-linéaire par rapport au Frobenius sur $k[[u]]$), tel que le sous-$k[[u]]$-module de $\mathfrak{M}$ engendré par $\phi(\mathfrak{M})$ contienne $u^{er}\mathfrak{M}$. On note pour plus de commodité (et suivant les notations habituelles) $\mathfrak{S}_1 = k[[u]]$. Étant donné un module de Kisin de p-torsion $\mathfrak{M}$, on lui associe la représentation de G_∞, $\mathrm{Hom}_{\mathfrak{S}_1,\phi}(\mathfrak{M}, K^{\mathrm{sep}})$ (l'action de G_∞ sur K^{sep} provenant de l'isomorphisme $G_\infty \simeq G_K$). Étant donnée une $\mathbb{F}_p$-représentation de $G_{\mathcal{K}}$, on peut lui associer ses poids de l'inertie modérée (qui ont été définis à la fin de la partie 1.2). Par ailleurs, la restriction de cette représentation à G_∞ fournit une $\mathbb{F}_p$-représentation de G_K, qui a elle aussi des poids de l'inertie modérée. Du fait que $G_\infty/(G_\infty \cap I_p) \simeq G_{\mathcal{K}}/I_p$, ces deux poids coïncident. Ainsi, on peut s'intéresser à la détermination des poids de l'inertie modérée d'une représentation de $G_{\mathcal{K}}$ par l'intermédiaire des modules de Kisin sur $\mathfrak{S}_1$.

2. Nous avons ici choisi d'appeler modules de Kisin les objets considérés. Il serait peut-être plus juste de parler de modules de Breuil-Kisin, mais cette terminologie nous semble plus simple.

3. Problèmes algorithmiques

Dans les développements récents de la théorie des représentations galoisiennes p-adiques, les calculs occupent une place importante. Tout d'abord, il s'agit d'une théorie où certaines démonstrations sont constructives et donc naturellement proches d'algorithmes, en particulier dans les problèmes concernant la recherche de réseaux dans les représentations. Ensuite parce que des calculs difficiles menés par Breuil sur les représentations de dimension 2 ont permis d'établir la première correspondance de Langlands p-adique, qui n'était alors que numérique et s'est avérée par la suite être effectivement la bonne.
Par ailleurs, la réponse à plusieurs questions demeure très incertaine, notamment en ce qui concerne les liens entre une $\mathbb{Q}_p$-représentation et sa réduction modulo p. L'équivalent des calculs de Breuil semble hors de portée en calculant « à la main » dans le cas des représentations de dimension 3, et d'autres domaines proches ressentent eux aussi le besoin de pouvoir mener efficacement des calculs par ordinateur, notamment la théorie des équations différentielles p-adiques. L'objectif principal de nos travaux est donc de rendre plus effective la théorie des représentations galoisiennes. À cet effet, on se concentre sur les représentations modulo p, qui sont par nature plus faciles à manipuler par ordinateur, puisque ce sont des objets finis. L'un des outils principaux est la théorie des ϕ-modules sur un corps de caractéristique p que nous appliquons à l'étude des modules de Wach et des modules de Kisin en caractéristique p.
Les contraintes de « finitude » des objets avec lesquels on veut calculer, ainsi que d'efficacité algorithmique, au sens où l'on cherche à obtenir des algorithmes dont le temps d'exécution est polynomial en les paramètres du problème, apportent des problèmes jusque là étrangers à la théorie. Essentiellement, ce sont des problèmes concernant la taille des données que l'on s'autorise à manipuler. Notamment, puisque l'on travaille avec des ϕ-modules sur le corps de séries formelles $k((u))$, il est nécessaire de tronquer les séries que l'on considère à une certaine précision tout en s'assurant que l'on conserve toute l'information nécessaire au calcul que l'on a en vue. Ce problème est assez commun pour les spécialistes des calculs effectifs avec les nombres p-adiques, qui travaillent toujours à précision finie. De manière plus subtile, d'autres difficultés apparaissent à cause des extensions du corps résiduel. En effet, la théorie a souvent recours à l'extension des scalaires pour simplifier les calculs ou les raisonnements. À l'inverse, en pratique, il faut prendre beaucoup de précautions pour limiter les extensions de scalaires : au mieux, elles font augmenter la complexité de manière polynomiale, et au pire elles deviennent rédhibitoires pour peu que le degré de l'extension à faire soit exponentiel en les paramètres du problème. C'est - entre autres - à ces questions assez nouvelles dans le domaine que nous avons été confrontés.

Nous avons programmé en Magma les algorithmes décrits dans cette thèse, car l'objectif visé est bien l'utilisation pratique de ceux-ci pour permettre une meilleure compréhension de certains problèmes en théorie de Hodge p-adique évoqués plus haut. Le code correspondant à ces programmes n'est pas inclus dans la présente thèse, mais il est disponible en ligne [3]. Il est temps de présenter plus en détail les résultats contenus dans ce mémoire.

4. Résultats principaux

Les résultats de cette thèse concernent le calcul effectif de certains invariants associés aux ϕ-modules sur les corps finis et aux représentations modulo p de groupes de Galois p-adiques. Nous développons l'étude des ϕ-modules sur le corps $K = k((u))$ où k est un corps fini. Le résultat central est un algorithme de calcul d'une filtration d'un ϕ-module sur K par des ϕ-modules *isoclines*, permettant de trouver les poids de l'inertie modérée de la représentation associée.

4.1. Polynôme semi-caractéristique. — Soit K un corps de caractéristique p, et soit q une puissance de p. Le corps K est muni du morphisme $\sigma : K \to K$ d'élévation à la puissance q. On définit l'anneau des *polynômes tordus* $K[X, \sigma]$ comme l'anneau (non-commutatif) des polynômes à coefficients dans K muni de l'addition usuelle et de la multiplication définie par la relation $Xa = \sigma(a)X$ pour $a \in K$. La première étude approfondie de cette notion est due à Ore, voir **[Ore33]**. Si $P \in K[X, \sigma]$, on peut lui associer naturellement le ϕ-module $K[X, \sigma]/K[X, \sigma]P$, sur lequel ϕ agit par multiplication par X à gauche (c'est essentiellement le point de vue de Jacobson dans **[Jac96]**, bien qu'il n'utilise pas le formalisme des ϕ-modules). Réciproquement, étant donnés un ϕ-module (D, ϕ) sur K, et $x \in K$, on définit la notion de *polynôme semi-caractéristique* de ϕ au point x, noté $\chi_{\phi,x}$, grâce au théorème suivant :

Théorème 4.1.1. — *Soit D un ϕ-module sur K, de dimension d. On fixe une base $\mathcal{B}$ de D, et on note G la matrice de ϕ dans cette base. On fixe aussi $x \in D$, et X_0 le vecteur colonne représentant x dans la base $\mathcal{B}$. Alors il existe des applications $P_0, \ldots, P_{d-1}$ polynomiales en les coefficients de G et de X_0, telles que*

$$\phi^d(X_0) = \sum_{i=0}^{d-1} P_i \phi^i(X_0).$$

Le point important ici est que les P_i sont des polynômes, alors qu'on ne peut *a priori* que dire que ce sont des fractions rationnelles. Le polynôme semi-caractéristique est alors défini comme le polynôme $\chi_{\phi,x} = X^d - \sum_{i=0}^{d-1} P_i(G, X_0)X^i$, où $P_i(G, X_0)$ correspond à

3. http ://blogperso.univ-rennes1.fr/jeremy.le-borgne/

l'évaluation du polynôme P_i du théorème en les coefficients de G et X_0. Même s'il joue un rôle comparable à celui du polynôme caractéristique en algèbre linéaire, il dépend du choix du vecteur x. Cependant, on montre que lorsque x engendre le ϕ-module D, le polynôme semi-caractéristique ne dépend pas du choix de x à *similarité* près (la similarité est une notion généralisant aux polynômes tordus la notion de « égaux à constante multiplicative près » pour les polynômes au sens classique). On montre que lorsque x est un générateur du ϕ-module, les factorisations de $\chi_{\phi,x}$ sont en correspondance bijective avec les suites de Jordan-Hölder pour D. Cela ramène le problème de la décomposition d'un ϕ-module à celui de la factorisation d'un polynôme tordu.
La notion de polynôme semi-caractéristique réapparaîtra plusieurs fois directement ou indirectement dans la suite de la thèse. Elle se révèle utile pour comprendre la structure des ϕ-modules que l'on étudie, et la correspondance entre le problème de la factorisation de ce polynôme et celui de la décomposition d'un ϕ-module fournit une partie des idées sous-jacentes aux algorithmes que nous développons.

4.2. Théorie des ϕ-modules sur les corps finis. — Après cette partie assez générale sur les liens entre ϕ-modules et polynômes tordus, nous étudions également la catégorie des ϕ-modules sur le corps fini $k = \mathbb{F}_{q^r}$, d'un point de vue orienté sur l'algorithmique. Cette étude permet de répondre à certaines questions ouvertes concernant les polynômes tordus sur k, qui sont des objets utilisés notamment en théorie des codes correcteurs (voir par exemple [**BU09**]). On s'intéresse aussi au problème de la factorisation des polynômes tordus sur les corps finis, qui a été résolu par Giesbrecht qui a donné un algorithme efficace pour trouver une factorisation d'un polynôme tordu donné (voir [**Gie98**]).
De façon plus précise, on montre que si (D, ϕ) est un ϕ-module étale sur $\mathbb{F}_{q^r}$ et si V est la représentation de $\mathrm{Gal}(\overline{\mathbb{F}}_{q^r}/\mathbb{F}_{q^r})$ associée, alors l'action du Frobenius $x \mapsto x^{q^r}$ sur V a une matrice semblable à celle de ϕ^r. On utilise alors cette manière simple de déterminer la représentation associée à un ϕ-module pour comprendre la structure du ϕ-module naturellement associé à un polynôme tordu sur $\mathbb{F}_{q^r}$, et ainsi étudier ce polynôme. Par exemple, si $P \in \mathbb{F}_{q^r}[X, \sigma]$, il est habituel de s'intéresser aux *bornes* pour P, c'est à dire aux multiples de P qui se trouvent dans le centre $\mathbb{F}_q[X^r]$ de $\mathbb{F}_{q^r}[X, \sigma]$. Une *borne optimale* est une borne de degré minimal. Nous obtenons le théorème suivant :

Théorème 4.2.1. — *Soit (D_P, ϕ) le ϕ-module associé au polynôme $P \in \mathbb{F}_{q^r}[X, \sigma]$. Alors la borne optimale de P est $\pi_{\phi^r}(X^r) \in \mathbb{F}_q[X^r]$, où π_{ϕ^r} désigne le polynôme minimal de ϕ^r.*

Au vu de ce théorème, et comme le polynôme caractéristique est plus facile à manipuler que le polynôme minimal, on introduit la notion suivante : si $P \in \mathbb{F}_{q^r}[X, \sigma]$, et (D_P, ϕ) est le ϕ-module associé, on note $\Psi(P)$ le polynôme caractéristique de ϕ^r. Le polynôme $\Psi(P)$

a le même degré que P, en on montre qu'il est à coefficients dans $\mathbb{F}_q$. On prouve alors que polynôme $\Psi(P)(X^r)$ est une borne pour P, dont le degré est $r \deg P$ (cela améliore d'un facteur r les meilleures estimations connues sur le degré d'une borne pour P). Nous montrons en outre comment $\Psi(P)$ encode un certain nombre d'informations sur les factorisations de P. Par exemple, nous remarquons que les classes de similarité de polynômes irréductibles sont exactement les fibres de ϕ au-dessus des polynômes irréductibles sur $\mathbb{F}_q$. Lorsque $\Psi(P)$ est sans facteur carré, et a s facteurs irréductibles distincts, nous donnons un algorithme (plus efficace que celui de Giesbrecht) pour factoriser P. De plus, nous montrons que P a $s!$ factorisations qui correspondent aux diverses façons d'ordonner les facteurs irréductibles de $\Psi(P)$. Nous donnons finalement un algorithme pour déterminer le nombre de factorisations de P, basé sur le comptage du nombre de suites de Jordan-Hölder pour le ϕ-module associé, que l'on obtient en comptant le nombre de décompositions de Jordan du Frobenius agissant sur la représentation associée.

4.3. Algorithme de réduction des ϕ-modules sur $k((u))$. — Nous étudions ensuite la catégorie des ϕ-modules sur $k((u))$, où k est dans un premier temps un corps quelconque de caractéristique p. Ici, les objets considérés sont un peu plus généraux que précédemment, car l'action de ϕ sur l'uniformisante u est seulement supposée être de la forme $\phi(u) = u^b$ où b est un entier quelconque ≥ 2.
Soit k un corps de caractéristique p, et $K = k((u))$. On fixe $\sigma : k \to k$ une puissance du Frobenius $x \mapsto x^p$, et $b \geq 2$ un entier. On munit K de l'endomorphisme $\phi_K : K \to K$, défini par $\phi_K(\sum a_i u^i) = \sum \sigma(a_i) u^{bi}$. On considère la catégorie des ϕ-modules sur K, dont les objets sont des K-espaces vectoriels de dimension finie munis d'un endomorphisme $\phi : D \to D$, semi-linéaire par rapport à ϕ_K. Le premier résultat à signaler est le théorème de classification des objets simples de cette catégorie lorsque k est algébriquement clos (le cas $k = \overline{\mathbb{F}}_p$ est dû à Caruso, voir [**Car09b**]).

Théorème 4.3.1. — *On suppose que k est algébriquement clos. Alors tout ϕ-module étale simple sur K a une matrice de la forme*

$$\begin{pmatrix} 0 & & & \lambda u^s \\ 1 & 0 & & 0 \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix},$$

et on peut même choisir $\lambda = 1$ si $\sigma \neq id$.

Si la dimension d'un tel objet simple est d, alors le nombre $\frac{s}{b^d-1}$ est uniquement déterminé modulo la relation d'équivalence $x \sim y \Leftrightarrow \exists m, m' \in \mathbb{Z}$ tels que $b^m x - b^{m'} y \in \mathbb{Z}$. La

classe d'équivalence de $\frac{s}{b^d-1}$ s'appelle la *pente* de D. Maintenant, si D est un ϕ-module quelconque sur K (toujours avec k algébriquement clos), les facteurs de composition de D déterminent une famille de pentes associées à D. Dans le cas où K n'est plus nécessairement algébriquement clos, on définit les pentes d'un ϕ-module D sur K comme les pentes du ϕ-module $D \otimes_K \overline{k}((u))$.

On définit un polygone de Newton naturellement associé à un ϕ-module (D, ϕ) de dimension d de la manière suivante : on se fixe $x \in D$, et on suppose que la famille $(x, \phi(x), \ldots, \phi^{d-1}(x))$ est libre. On détermine alors une relation de dépendance linéaire $\phi^d(x) = \sum_{i=0}^{d-1} a_i \phi^i(x)$. Le polygone de Newton associé à D est alors défini à partir du polynôme $P = X^d - \sum_{i=0}^{d-1} a_i X^i$ [4]. On montre que les pentes du polygone de Newton sont en fait les pentes du ϕ-module. Bien qu'elle permette de « lire » les pentes du ϕ-module d'une manière assez simple à partir de la matrice de ce dernier, cette approche n'est pas raisonnable pour le calcul algorithmique des pentes du ϕ-module, car les valuations des coefficients du polynôme semi-caractéristique sont de l'ordre de $b^{\dim D}$ et donc manifestement pas polynomiales en $\dim D$.

Nous donnons alors un algorithme efficace (c'est-à-dire de complexité polynomiale en la taille de l'entrée) pour le calcul des pentes d'un ϕ-module sur K, lorsque le ϕ-module est donné par la matrice de ϕ dans une base de D (telle que la matrice de ϕ soit à coefficients dans $k[[u]]$). Les difficultés techniques proviennent principalement du fait que lorsque l'action de ϕ sur k est non triviale, les calculs nous conduisent naturellement à travailler dans des extensions de $k(\!(u)\!)$ qui ont un degré de l'ordre de $b^{\dim D}$. Or, pour conserver une complexité polynomiale, on ne peut pas se le permettre, et on doit ainsi développer un certain nombre d'« astuces » pour faire uniquement des calculs dans le corps de base. On montre alors que l'algorithme obtenu pour le calcul des pentes a une complexité polynomiale en les paramètres décrivant le problème (la dimension et les diviseurs élémentaires de la matrice de ϕ). Dans le cas où l'action sur k est triviale, on peut s'autoriser à faire des extensions finies de k sans faire exploser la complexité.

4.4. Calculs effectifs pour les représentations galoisiennes. — Dans le chapitre IV, on décrit les représentations irréductibles du groupe de Galois G_K d'un corps K muni d'une valuation discrète complet dont le corps résiduel fini, dont le cardinal est une puissance q de p, et à coefficients dans une extension finie $\mathbb{F}_{p^r}$ de $\mathbb{F}_p$. On note σ l'élément de G_K agissant comme le Frobenius sur le corps résiduel $\mathbb{F}_q$ et agissant trivialement sur les racines de l'uniformisante. On définit certaines représentations de G_K de la manière suivante :

4. Si ϕ agit sur K comme une puissance du Frobenius, $P = \chi_{\phi,x}$

Définition 4.4.1. — Soit τ l'ordre de q modulo p^r. Soient $\delta \in \mathbb{N}^*$, $t \in \mathbb{N}^*$ multiple de τ, s_1 un entier primitif pour $r\delta$. Soit $E = \mathrm{End}_{I_t}(\omega_{r\delta}^{s_1})$, et soit $P \in E[X, \sigma^\tau]$. On note $V_{\delta,t,s_1,P}$ la représentation décrite de la manière suivante : $V_1 = \omega_{r\delta}^{s_1}$, $V = V_1 \oplus \sigma V_1 \oplus \cdots \oplus \sigma^t V_1$, et il existe $x_1 \in V_1$ tel que $\sigma^t(V_1) = P(\sigma^\tau)(x_1)$.

On obtient alors la classification :

Proposition 4.4.2. — *Toute représentation irréductible de G_K à coefficients dans $\mathbb{F}_{p^r}$ est isomorphe à une représentation de la forme $V_{\delta,t,s,P}$. De plus, si $P \in \mathbb{F}_{p^r}[X, \sigma^\tau]$ et $i \in \mathbb{N}$, on note $P^{(q^i)}$ le polynôme où on a élevé les coefficients de P à la puissance q^i. Alors les isomorphismes entre représentations de la forme $V_{\delta,t,s,P}$ sont donnés par $V_{\delta,t,s_1,P} \simeq V_{\delta,t,q^i s_1,\tilde{P}^{(q^i)}}$ avec $0 \leq i \leq \tau - 1$ et $\tilde{P}$ similaire à P.*

On décrit ensuite la représentation associée à un ϕ-module simple sur K par la première équivalence de catégories de la théorie de Fontaine, dans le cas où $\sigma = \mathrm{id}$ (qui donne les $\overline{\mathbb{F}}_p$-représentations) et dans le cas où $\sigma \neq \mathrm{id}$ (qui donne plutôt des $\mathbb{F}_{p^r}$-représentations). On montre comment l'algorithme développé au chapitre III permet de décrire, selon les cas, les poids de l'inertie modérée ou toute la semi-simplifiée de la représentation associée à un ϕ-module donné.
On s'intéresse enfin plus spécifiquement aux représentations modulo p de groupes de Galois p-adiques, données par l'intermédiaire des théories de Wach et de Kisin. Si le cas des modules de Kisin se déduit directement de l'étude précédente, il faut inclure l'action de Γ pour comprendre la représentation associée à un module de Wach. Nous montrons comment exploiter l'algorithme de réduction des ϕ-modules pour donner un algorithme de réduction des modules de Wach en caractéristique p, et nous expliquons comment retrouver la semi-simplifiée de la réduction modulo p de la représentation cristalline correspondante. Plus généralement, on donne un algorithme pour calculer la semi-simplifiée d'un (ϕ, Γ)-module sur $\overline{\mathbb{F}}_p((u))$, et en déduire la semi-simplifiée de la réduction modulo p de la représentation correspondante par la théorie de Fontaine.

4.5. Optimisation du théorème d'Ax-Sen-Tate. — Cet appendice, largement indépendant du reste de la thèse, concerne une autre illustration de l'importance de l'extension de Breuil-Kisin du corps p-adique $\mathcal{K}$ par les racines p^n-èmes de l'uniformisante. Soit $\mathcal{K}$ une extension finie de $\mathbb{Q}_p$, soit π une uniformisante de $\mathcal{K}$, et soit v la valuation sur $\mathcal{K}$ normalisée par $v(p) = 1$. On a une action naturelle de $G_{\mathcal{K}} = \mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})$ sur l'anneau des entiers $\mathcal{O}_{\overline{\mathcal{K}}}$ de $\overline{\mathcal{K}}$. Si on se fixe une constante (réelle) quelconque C, on se demande quels sont les $x \in \overline{\mathcal{K}}$ tels que pour tout $g \in G_{\mathcal{K}}$, $v(gx - x) \geq C$. Dans [**Ax70**], Ax montre que si $x \in \mathcal{K}$ vérifie cette propriété, alors il existe $y \in \mathcal{K}$ tel que $v(x - y) \geq C - \frac{p}{(p-1)^2}$ et en déduit que

$\mathbb{C}_p^{G_\mathcal{K}} = \mathcal{K}$. Ax pose également la question de l'optimalité de la constante $\frac{p}{(p-1)^2}$.
Dans le chapitre V de cette thèse, nous répondons à cette question et allons même plus loin en donnant une description complète des $x \in \mathcal{O}_{\overline{\mathcal{K}}}$ tels que pour tout $g \in G_\mathcal{K}$, $v(gx-x) \geq C$. Pour présenter cette description, considérons la suite (π_n) définie par $\pi_0 = \pi$, et $\pi_{n+1}^p = \pi_n$, on pose alors $\mathcal{K}_n = \mathcal{K}(\pi_n)$.

Théorème 4.5.1. — *Soit $x \in \mathcal{O}_{\overline{\mathcal{K}}}$. Alors x vérifie $v(gx - x) \geq A$ pour tout $g \in G_\mathcal{K}$ si et seulement si pour tout $n \in \mathbb{N}$, il existe $x_n \in \mathcal{K}_n$ tel que $v(x - x_n) \geq C - \frac{1}{p^n(p-1)}$.*

Le cas particulier $n = 1$ fournit la réponse à la question d'Ax. En outre, cette description relativement explicite nous permet de montrer que le groupe de cohomologie $H^1(G_\mathcal{K}, \mathcal{O}_{\overline{\mathcal{K}}})$ se décrit à l'aide de suite *twist-récurrentes* (notion introduite par Kedlaya dans [**Ked01a**]). Plus précisément, soit k le corps résiduel de $\mathcal{K}$. Une suite twist-récurrente de k est une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de k vérifiant une relation du type

$$\forall n \in \mathbb{N},\ d_0 x_n + \cdots + d_r x_{n+r}^{p^r} = 0,$$

pour un certain entier r et des éléments $d_0, \ldots, d_r$ de k non tous nuls. Dans le cas où $\mathcal{K}/\mathbb{Q}_p$ est non ramifiée, on montre que $H^1(G_\mathcal{K}, \mathcal{O}_{\overline{\mathcal{K}}})$ s'identifie à l'espace des suites twist-récurrentes de k. Dans le cas général, on donne une idée pour décrire ce groupe de manière analogue, sans donner tous les détails de la construction dont la combinatoire est assez complexe.

5. Perspectives

5.1. Action de l'inertie sauvage. — L'algorithme présenté dans le chapitre III de cette thèse est efficace pour déterminer la semi-simplifiée (respectivement les pentes, selon l'action de ϕ sur k) d'un ϕ-module, et donc la semi-simplifiée (respectivement les poids de l'inertie modérée) de la représentation associée. Il ne donne par contre pas d'information sur l'action de l'inertie sauvage sur cette représentation. Il fournit néanmoins un moyen de calculer cette action, avec une complexité exponentielle. En effet, on peut adapter l'algorithme (moyennant le calcul dans des extensions de degré grand du corps de base) pour se ramener sans trop de difficulté au cas où la matrice du ϕ-module considéré, après un changement de base à coefficients dans une extension modérément ramifiée L de K, est de la forme

$$\begin{pmatrix} 1 & \alpha & (\star) & (\star) \\ 0 & 1 & \ddots & (\star) \\ \vdots & \ddots & \ddots & (\star) \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Pour comprendre le noyau de la représentation associée, il faut comprendre sur quelle extension de L ce ϕ-module est trivial. Pour cela, on est amené à résoudre des équations du type $X^p - X = \alpha$, c'est-à-dire des équations d'Artin-Schreier. Ces équations ne sont pas mutuellement indépendantes, ce qui impose de construire explicitement la tour d'extensions associée à ces équations pour toutes les connaître ! En particulier, cette construction a une complexité exponentielle en la dimension du ϕ-module en général. Il n'existe pas encore de résultats permettant d'exprimer directement la nature de l'extension en fonction des coefficients (contrairement au cas d'une seule extension d'Artin-Schreier). L'un des objectifs pour le futur est de réussir à rendre ces calculs efficaces.

5.2. Théorie de Dieudonné-Manin. — La théorie de la réduction des ϕ-modules étudiée dans cette thèse présente de nombreuses analogies avec le théorème de Dieudonné-Manin. En effet, si $\mathcal{K}$ est une extension finie de $\mathbb{Q}_p$, un F-module sur $\mathcal{K}$ est un $\mathcal{K}$-espace vectoriel de dimension finie muni d'une application F semi-linéaire par rapport au Frobenius sur $\mathcal{K}$. La théorie de Dieudonné-Manin montre que la catégorie des F-modules sur $\mathcal{K}$ est semi-simple, ces objets devraient donc être un peu plus faciles à étudier algorithmiquement. Néanmoins, l'algorithme du chapitre III s'adapte mal à la nouvelle situation, la raison étant que dans le cas de Dieudonné-Manin, l'action sur l'uniformisante est triviale, et il n'est pas facile de savoir à quelle précision il suffit de tronquer les coefficients de la matrice donnant un F-module pour obtenir un objet isomorphe. Comprendre à quelle précision il est suffisant de connaître un F-module pour déterminer sa classe d'isomorphisme fournirait certainement un moyen d'implémenter efficacement la décomposition de Dieudonné-Manin, en calquant l'approche de notre algorithme. En outre, cela serait un pas en direction de la caractéristique nulle, qui est un contexte à la fois plus naturel et plus riche pour la théorie de Hodge p-adique.

CHAPITRE I

POLYNÔMES SEMI-CARACTÉRISTIQUES, φ-MODULES ET POLYNÔMES TORDUS

Ce chapitre et le suivant font l'objet de l'article intitulé Semi-characteristic polynomials, φ-modules and skew polynomials ([**LB11a**])

The aim of this paper is to relate the theory of φ-modules over a finite field, which is semi-linear algebra, with the theory of skew polynomials, and give some applications to understand better the factorization of skew polynomials over finite fields. Let K be a field of characteristic $p > 0$ endowed with a Frobenius morphism σ, and let D be a finite-dimensional vector space over K endowed with a map φ that is semi-linear with respect to σ: this structure is called a φ-module. If one wants to evaluate a polynomial with coefficients in K at such a semi-linear map, the ring of polynomials considered should have a natural structure of skew polynomial ring (or twisted-polynomial ring, as discussed by Kedlaya in [**Ked08**]), in order for the relation $PQ(\varphi) = P(\varphi)Q(\varphi)$ to be valid. The theory of φ-modules has been widely investigated in p-adic Hodge theory, often as a tool in the theory of (φ, Γ)-modules that Fontaine introduced in [**Fon90**] for the study of p-adic representations of local fields. On the other hand, the theory of skew polynomials was founded by Ore, who gave the fundamental theorems about such polynomials. In the context of finite fields, this theory has been recently used (for example by Boucher and Ulmer in [**BU09**]) to build error-correcting codes. One of Ore's main theorems concerns factorizations of skew polynomials, and it says that in two given factorizations of a polynomial, the irreducible factors that appear do not depend on the factorization up to similarity (similarity is an equivalence relation on skew polynomials, that generalize the notion of being equal up to multiplicative constant in the case of commutative polynomials, see section 1.1 for more detail). One very important result concerning skew polynomial rings over finite fields is a polynomial-time (in the degree of the polynomial) factorization algorithm due to Giesbrecht in [**Gie98**].

In order to relate these theories, we introduce in the first part of the article the notion of semi-characteristic polynomial for a semi-linear map over a vector space over a field K of characteristic $p > 0$. Indeed, to a skew polynomial is naturally associated a φ-module (whose matrix is the companion matrix of the polynomial). Conversely, to a φ-module over K we associate a skew polynomial with coefficients in K, the semi-characteristic polynomial. This polynomial should somehow behave like the characteristic polynomial of a linear map (in particular, its degree is the same as the dimension of the underlying vector space), except that it depends on the choice of some element in the φ-module D. For the purpose of this article, our definition of the semi-characteristic polynomial is mostly interesting in the case that the φ-module has a basis of the form $(x, \varphi(x), \ldots, \varphi^{d-1}(x))$ for some $x \in D$. We give several properties of the semi-characteristic polynomial in this context, yielding the fact that the semi-characteristic polynomials given by two such x are equivalent under the similarity relation, which is a crucial equivalence relation in the theory of skew polynomials. This polynomial is denoted by $\chi_{\varphi,x}$. We give an interpretation of a study of Jacobson about skew-polynomials in our context (see [**Jac96**], Chapter 1) to understand the factorizations of the semi-characteristic polynomial of a φ-module. Our Theorem 4.4 gives a natural bijection between the Jordan-Hölder sequences of a φ-module and the factorizations of its semi-characteristic polynomial, the irreducible factors being given by the semi-characteristic polynomials of the composition factors. Conversely, our Proposition 4.5 shows any factorization of the semi-characteristic polynomial $\chi_{\varphi,x}$ yields a Jordan-Hölder sequence for the φ-module.

In the second part of the article, we use the preceding tools to study skew polynomials over finite fields. To a skew polynomial is naturally associated a so-called linearized polynomial, which is a polynomial of the form $\sum a_i X^{q^i}$, where the cardinal of the base field is a power of q. Linearized polynomials have long been related to skew polynomials (see for example [**LN94**]), and it is easy to see that the set of the roots of a linearized polynomial is a $\mathbb{F}_q$-vector space. On the other hand, to a φ-module is associated a linear representation of a Galois group by Fontaine's theory of φ-modules in characteristic p, which is recalled briefly in section 2.1. It appears that the considered representation is naturally the vector space of the roots of the associated linearized polynomial. As an application, we explain how to find the splitting field of a linearized polynomial together with the action of the Galois group on its roots:

Théorème I.1 **(Theorem 2.3)**. — *Let $P \in \mathbb{F}_{q^r}[X, \sigma]$ with nonzero constant coefficient, and let L_P be the associate linearized polynomial. Let Γ be the companion matrix of P, and $\Gamma_0 = \Gamma\sigma(\Gamma)\cdots\sigma^{r-1}(\Gamma)$. Then the characteristic polynomial Q of Γ_0 has coefficients in $\mathbb{F}_q$,*

and the splitting field of L_P has dimension m over $\mathbb{F}_{q^r}$, where m is the maximal order of a root of Q in $\overline{\mathbb{F}}_q$. Moreover, the action of a generator g of the Galois group $G_{\mathbb{F}_{q^r}}$ is given in some basis of the $\mathbb{F}_q$-vector space of the roots of L_P by the Frobenius normal form of Γ_0.

We give a fast algorithm to compute a multiple of a skew polynomial that lies in the center of the ring, which has been a natural question about skew polynomials. In particular, since Giesbrecht's algorithm for factoring uses the computation of such a multiple, we improve the complexity of this part of his algorithm. We also explain how to test the similarity of skew polynomials effectively. Then, we investigate further the relations between the factorizations of a skew polynomial P and the structure of the φ-module associated to P as suggested by our Proposition 4.2. We define a map Ψ that is shown to be multiplicative and to send a skew polynomial P to a commutative polynomial of the same degree. This map allows to compute some invariants for P such as the number and degrees of factors of P in a given class of similarity, and tests irreducibility effectively. We explain how the factorization of the associated commutative polynomial $\Psi(P)$ yields one factorization of P (and in fact, all of them) when $\Psi(P)$ is squarefree. At the level of φ-modules, this map classifies the φ-modules up to semi-simplification. We also show

***Théorème I.2* (Corollary 4.4).** — *Let $P \in \mathbb{F}_{q^r}[X, \sigma]$. Then the similarity classes of irreducible factors of P appear in all possible orders in the factorizations of P.*

We also use the map Ψ to give a new way to compute the number of monic irreducible skew polynomials of given degree over a finite field. We then give a polynomial-time algorithm in the degree to count the number of factorizations of a skew polynomial as a product of monic irreducible polynomials, and explain a method to find them all (naturally, an algorithm for this would be exponential in general because so is the number of factorizations, however our method is linear in this number).

Note that φ-modules are often used as a tool for the study of Galois representations over local fields (and usually with characteristic zero). A φ-module over a local field has a sequence of *slopes*, which are rational numbers that characterise the composition factors of the φ-module. It should be possible to recover the slopes of a φ-module over a field of positive characteristic from a factorization of its semi-characteristic polynomial, and even probably without factoring it using Newton polygons. This is not the approach of this paper, where the focus is on finite fields, but this topic will be discussed in the forthcoming paper [**LB11b**].

Let K be a field of characteristic p, let $a \geq 1$ be an integer, and $\sigma : K \to K$ be the a-th power of the absolute Frobenius. Set $q = p^a$. The fixed field of σ is the intersection of K with the finite field with q elements $\mathbb{F}_q$. From now on, we assume that $\mathbb{F}_q \subset K$. If $P, Q \in K[X]$ and φ is a semi-linear map on K^d, then it is not true in general that $PQ(\varphi) = P(\varphi)Q(\varphi)$, since φ does not act trivially on K. The right point of view for the polynomials of semi-linear maps is that of *skew polynomials*. Before investigating the properties of the semi-characteristic polynomials, we will recall some definitions and basic properties of the skew polynomial ring with coefficients in K.

I.1. Skew polynomials

Definition 1.1. — The ring of skew polynomials with coefficients in K, denoted $K[X, \sigma]$, is the set of polynomials with coefficients in K endowed with the usual addition, and the non-commutative multiplication $\cdot$ verifying $X \cdot a = \sigma(a) \cdot X$.

Definition 1.2. — Let $P, Q \in K[X, \sigma]$, we say that P is a right-divisor of Q (or that P divides Q on the right) if there exists $U \in K[X, \sigma]$ such that $Q = UP$. If this is the case, we say that Q is a left-multiple of P.

The ring of skew polynomials was first studied by Ore in **[Ore33]**. In this paper, he proves that the ring $K[X, \sigma]$ is a right-euclidean domain, and therefore a left-principal ideal domain. The notions of *right greatest common divisor* (rgcd) and *left lowest common multiple* (llcm) are well defined: we say that D is a rgcd (resp. a llcm) of P and Q if D is a left-multiple of any polynomial that divides both P and Q on the right (resp. if it is a right-divisor of any polynomial that is a left-multiple of both P and Q). The same notions exist on the other side if K is perfect. A factorization of a skew polynomial is in general not unique up to permutation of the factors and multiplication by a constant. Two different factorizations are related by the notion of similar polynomials, which we define now.

Definition 1.3. — Two skew polynomials P and Q are said to be *similar* if there exists $U \in K[X, \sigma]$, such that the right-greatest common divisor of U and P is 1, and such that QU is the left-lowest common multiple of U and P.

Theorem 1.4 **(Ore, [Ore33])**. — *Let $P_1 \cdots P_r = Q_1 \cdots Q_s \in K[X, \sigma]$ be two factorizations of a given polynomial as a product of irreducible polynomials. Then $r = s$ and there exists a permutation $\sigma \in \mathfrak{S}_r$ such that $Q_{\sigma(i)}$ and P_i are similar for all $1 \leq i \leq r$.*

We will use the notions of skew polynomials in a context of semilinear algebra, because these polynomials are naturally the polynomials of semilinear endomorphisms.

I.2. Definition of the semi-characteristic polynomial

As before, let K be a field of characteristic p and $\sigma : K \to K$ be the a-th power of the absolute Frobenius. We still assume that $\mathbb{F}_q \subset K$. A φ-module over K is a finite dimensional vector space D endowed with a map $\varphi : D \to D$ that is semi-linear with respect to σ. Such a φ-module is said to be *étale* if the image of φ contains a basis of D. The aim of this section is to associate to a φ-module a polynomial (or, more precisely, a family of polynomials) that is an analog of the characteristic polynomial for linear maps. In general, for $x \in D$, the set $I_{\varphi,x} = \{Q \in K[X,\sigma] \mid Q(\varphi)(x) = 0\}$ is a left-ideal. Indeed, $I_{\varphi,x}$ is an additive subgroup of $K[X,\sigma]$, and if $P \in I_{\varphi,x}$ and $Q \in K[X,\sigma]$, then $QP(\varphi)(x) = Q(\varphi)(P(\varphi)(x)) = 0$. Hence this ideal has a generator $m_{\varphi,x}$ that we may call the minimal polynomial of x under the action of φ. We are mostly interested in the case where the degree of this polynomial is the dimension of the φ-module. In this case, we want to give an algebraic construction of $m_{\varphi,x}$ that will be called the semi-characteristic polynomial of φ in x. The idea is that by Cramer's formulas, the coefficients of $m_{\varphi,x}$ are rational functions in the coefficients of the matrix of the map φ: indeed, if $(x, \varphi(x), \dots, \varphi^{d-1}(x))$ is a basis of the φ-module D of dimension d, then $\varphi^d(x)$ can be written as a linear combination of $x, \varphi(x), \dots, \varphi^{d-1}(x)$, the coefficients being of the form

$$\frac{\det(x, \varphi(x), \dots, \varphi^{i-1}(x), \varphi^d(x), \varphi^{i+1}, \dots, \varphi^{d-1}(x))}{\det(x, \varphi(x), \dots, \varphi^{d-1}(x))}.$$

We show that these coefficients are actually polynomials.

Let $d \in \mathbb{N}$ and let $A = K[(a_{ij})_{1 \le i,j \le d}]$. Let

$$G = \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & & \vdots \\ a_{d1} & \cdots & a_{dd} \end{pmatrix}$$

be the so-called generic matrix with coefficients in A.

Theorem 2.1. — *Let $x \in K^d \backslash \{0\}$, and let φ be the σ-semi-linear map on A^d whose matrix in the canonical basis is G. Then there exists a unique family of polynomials $P_0, \dots, P_{d-1} \in A$, depending only on x, such that*

$$\varphi^d(x) = P_{d-1}\varphi^{d-1}(x) + \cdots + P_1\varphi(x) + P_0 x.$$

Moreover, each P_i is an homogeneous polynomial in the coefficients of G.

Before proving the theorem, let us mention the following corollary :

Corollary 2.2. — *Let $L = K(x_1, \dots x_d)$, and $x = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \in L^d$. Let P_i be the polynomials defined as in Theorem 2.1. Then the P_i lie in $K[x_1, \dots, x_d][a_{ij}]$. In particular, we can define the P_i for $x = 0$.*

The proof of the corollary will be given after that of the theorem. Let $x_0 \in K^d$, and let (x_i) be the sequence of elements of A^d defined by induction by $x_{i+1} = G\sigma(x_i)$. Here, σ acts on a vector in A^d by raising each coordinate to the same power p^a as σ on K. We call this sequence the sequence of iterates of x_0 under G. We will need the following lemma:

Lemma 2.3. — *For all $x \in K^d \setminus \{0\}$, the determinant $\Delta = \det(x_0, \dots, x_{d-1})$ is an homogeneous element of A that is squarefree.*

The fact that this determinant is homogeneous is clear since for all $i \geq 0$, the coefficients of x_i are all homogeneous polynomials of degree $\sum_{j=0}^{i-1} p^j$. We first show another lemma that will simplify the proof of Lemma 2.3.

Lemma 2.4. — *With the above notations, it is enough to prove Lemma 2.3 for only one $x_0 \in K^d \setminus \{0\}$.*

Proof. — It is harmless to assume that K is algebraically closed (and hence infinite), which we will do in the proof. Let $x_0, x_0' \in K^d \setminus \{0\}$. Let (x_i) (respectively (x_i')) the sequence of iterates of x_0 (respectively x_0') under G. We assume that $\det(x_0, \dots, x_{d-1})$ is a squarefree polynomial. Let $P \in GL_d(K)$ such that $x_0' = Px_0$. Let $y_0 = x_0$ and let (y_i) be the sequence of iterates of y_0 under $P^{-1}G\sigma(P)$. We have $x_1' = G\sigma(x_0') = G\sigma(P)\sigma(x_0) = Py_1$. An easy induction shows that for all $i \geq 0$, $x_i' = Py_i$. Hence, $\det(x_0', \dots, x_{d-1}') = \det P \det(y_0, \dots, y_{d-1})$. Since $\det P \in K^\times$, it is enough to show that $\det(y_0, \dots, y_{d-1})$ is squarefree. Define a morphism of K-algebras $\theta : A \to A$ by $G \mapsto P^{-1}G\sigma(P)$ (this gives the image of all the indeterminates by θ, and hence defines a unique morphism of K-algebras). In fact, this morphism is an isomorphism, with inverse given by $G \mapsto PG\sigma(P)^{-1}$. The map θ extends naturally to A^d and $A^{d\times d}$ and commutes with σ. By definition, $\theta(x_0') = x_0 = y_0$, and $\theta(x_{i+1}) = \theta(G)\sigma(\theta(x_i)) = P^{-1}G\sigma(P)\sigma(\theta(x_i))$, which shows by induction that for all $i \geq 0$, $\theta(x_i) = y_i$. Next, we remark that $\theta(\det(x_0, \dots, x_{d-1})) = \det(y_0, \dots, y_{d-1})$. Since θ is an isomorphism, is maps a squarefree polynomial to a squarefree polynomial (the quotient of A by the ideal generated by a polynomial Q is reduced if and only if Q is squarefree). This proves the lemma. □

We can now prove Lemma 2.3.

Proof. — Let us prove the proposition by induction on the dimension d. Our induction hypothesis is that for any field K, the determinant Δ is a squarefree polynomial. If $d = 1$, then the result is obvious. Assume the proposition is proved for $d \in \mathbb{N}$, and prove it for $d + 1$. Recall that any factorization of Δ has homogeneous irreducible factors. Therefore, we note that if evaluating some of the variables to zero sends Δ to a nonzero squarefree polynomial (in the unevaluated variables), then Δ is squarefree. Indeed, if Δ has a square factor, then such an evaluation maps this square factor to either a nonconstant polynomial or to 0, and hence the evaluation also has a square factor.
We will evaluate some of the variables to zero, namely we look at

$$G = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ X_0 & & G' & \end{pmatrix},$$

where X_0 is of size $(d-1) \times 1$ and G' is of size $(d-1) \times (d-1)$.

We define by induction $X_{i+1} = G'\sigma(X_i)$ for $i \geq 0$. Now let $x_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, and (x_i) the sequence of iterates of x_0 under this evaluation of G. Let us compute (x_i). First, $x_1 = G\sigma(x_0) = \begin{pmatrix} 0 \\ X_0 \end{pmatrix}$ and $x_2 = \begin{pmatrix} 0 \\ X_1 \end{pmatrix}$. An easy induction shows that for all $i \geq 1$, $x_i = \begin{pmatrix} 0 \\ X_{i-1} \end{pmatrix}$. Therefore, the evaluation Δ' of Δ that we are computing is

$$\Delta' = \det(x_0, \ldots, x_{d-1}) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & X_0 & X_1 & \cdots & X_{d-2} \end{vmatrix}.$$

This determinant is equal to its lower right $(d-1) \times (d-1)$ minor, which is equal to $\det(X_0, \ldots, X_{d-2})$. Denote by S the set of variables appearing in X_0 (i.e., $a_{21}, \ldots, a_{d1}$), and S' the set of all the other variables appearing in G'. By induction hypothesis, applied with the field $K(S)$, the polynomial $\Delta' \in K(S)[S']$ is squarefree. This shows that if Δ' has a square factor, then the only variables appearing in this square factor lie in S. Hence it is enough to find an evaluation in S' of Δ' that is squarefree to show that Δ' is squarefree, which implies that Δ is squarefree as well. We use the previous computation that we evaluate in $G = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ X_0 & & I_{d-1} & \end{pmatrix}$, where I_{d-1} is the $d-1$ identity matrix. Then $X_i = \sigma^i(X_0)$, and the evaluation of Δ' that we are computing is $\Delta'' = \det(X_0, \sigma(X_0), \ldots, \sigma^{d-2}(X_0))$.

What we need to prove now is that, in $K[b_1, \dots, b_d]$, the determinant

$$V_q(b_1, \dots, b_d) = \begin{vmatrix} b_1 & b_1^q & \cdots & b_1^{q^{d-1}} \\ b_2 & b_2^q & \cdots & b_2^{q^{d-1}} \\ \vdots & \cdots & \cdots & \vdots \\ b_d & b_d^q & \cdots & b_d^{q^{d-1}} \end{vmatrix}$$

(which is known as the Moore determinant) is squarefree. It is a well-known fact that we have the following factorization:

$$V_q(b_1, \dots, b_d) = c \prod_{\varepsilon \in \mathbb{P}^{d-1}(\mathbb{F}_q)} \sum_{i=1}^{d} \varepsilon_i b_i,$$

with $c \in \mathbb{F}_q^\times$. By $\varepsilon \in \mathbb{P}^{d-1}(\mathbb{F}_q)$, we mean that the considered d-uples ε have their first nonzero coordinate equal to one. Note that if $\varepsilon = (\varepsilon_1, \cdots, \varepsilon_d) \in \mathbb{P}^{d-1}(\mathbb{F}_q)$, then $F_\varepsilon = \sum_{i=1}^d \varepsilon_i b_i$ is an irreducible polynomial (it is homogeneous with global degree 1). Two such distinct polynomials are not colinear since the coefficients are defined up to homothety, and hence are coprime. Moreover, if $F_\varepsilon(\beta_1, \cdots, \beta_d) = 0$, then σ being linear on $\mathbb{F}_q$ implies that the evaluation of the q-Vandermonde determinant at $(\beta_1, \cdots, \beta_d)$ is the determinant of a matrix whose rows are linearly dependant over $\mathbb{F}_q$, so this evaluation is zero. Hilbert's zeros theorem shows that F_ε divides V_q, and given the coprimality of the F_ε's, their product divides V_q. It is now enough to check that they have the same degree, that is easily seen to be $q^{d-1} + \cdots + q + 1 = \frac{q^d-1}{q-1}$. □

Proof of Theorem 2.1. — Since there exist simple φ-modules of dimension d with coefficients in A (that is, simple objects in the category of φ-modules over A, meaning that they have no nontrivial subspaces stable under the action of φ), the φ-module defined by G is simple as a φ-module over the field of fractions B of A. In particular, for all $x \in K^d \setminus \{0\}$, there exists a unique family $F_0, \dots, F_{d-1} \in B$ such that $\varphi^d(x) = F_{d-1}\varphi^{d-1}(x) + \cdots + F_1\varphi(x) + F_0 x$. We want to show that the F_i's are actually in A.

Let $x_0 = x$ and $(x_i)_{i \geq 0}$ be the sequence of iterates of x under G: for $i \geq 0$, x_i is the vector representing $\phi^i(x)$ in the canonical basis. According to Cramer's theorem, the F_i's are given by the following formula, for $i \geq 0$:

$$F_i = \frac{\det(x_0, \dots, x_{i-1}, x_d, x_{i+1}, \dots, x_{d-1})}{\det(x_0, \dots, x_{d-1})}.$$

The denominator of F_i is nothing but the determinant Δ from Lemma 2.3. Since it is squarefree according to that lemma, Hilbert's zeros theorem (assuming K is algebraically

closed) shows that it is enough to prove that the numerator vanishes whenever the denominator vanishes. If Δ is mapped to zero by the evaluation of G at $\underline{a}$, then the family $(x_0(\underline{a}), \dots, x_{d-1}(\underline{a}))$ is linearly dependent over K, so it spans a vector space of dimension at most $d-1$. But the span of this family is also stable under φ since the smallest subspace stable by φ containing $x_0(\underline{a})$ (that we denote $D_{x_0(\underline{a})}$) is spanned by the $x_i(\underline{a})$'s, and for all $r \in \mathbb{N}$, $x_{d+r}(\underline{a})$ lies in the span of $x_r(\underline{a}), \dots, x_{r+d-1}(\underline{a})$. Therefore, any family of d elements of $D_{x_0(\underline{a})}$ is linearly dependent over K, so that the numerator of F_i vanishes at $\underline{a}$ for all $0 \leq i \leq d-1$, which proves the theorem. □

Proof of Corollary 2.2. — The case $d = 1$ is obvious, so we will prove the corollary for $d \geq 2$. Recall that we want to show that, applying Theorem 2.1 with the field $L = K(x_1, \dots, x_d)$, we get the fact that the P_i's lie in $K(x_1, \dots, x_d)[a_{ij}]$. Now let $y = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$,

$P = \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 1 & \ddots & \vdots \\ \vdots & 0 & \ddots & 0 \\ x_d & \cdots & 0 & 1 \end{pmatrix}$, and $H = P^{-1}G\sigma(P)$, so that $x = Py$, and the P_i associated to x (with respect to the matrix G) and y (with respect to the matrix H) are the same (by the computation of Lemma 2.4). Since the coefficients of H lie in $K[x_1, \dots, x_d][a_{ij}][x_1^{-1}]$, so do the P_i's. Now taking another P whose determinant is, say, x_2 (which is possible since $d \geq 2$), we see that the P_i's also lie in $K[x_1, \dots, x_d][a_{ij}][x_2^{-1}]$, so they actually lie in $K[x_1, \dots, x_d][a_{ij}]$. □

Definition 2.5. — With the previous notations, the polynomial $\chi^0_{\varphi,x} = X^d - \sum_{i=0}^{d-1} P_i X^i \in A[x_1, \dots, x_d][X, \sigma]$ obtained from the vector x of Corollary 2.2 is called the *universal semi-characteristic polynomial* over K.

Given a φ-module D of dimension d over K, whose matrix in a basis $\mathcal{B}$ of K^d is $G(\underline{a})$, and $x \in D$ whose coordinates in the basis $\mathcal{B}$ are given by $\underline{\xi} = (\xi_1, \dots, \xi_d)$, the *semi-characteristic polynomial* of φ in x in the basis $\mathcal{B}$ is the evaluation of $\chi^0_{\varphi,x}$ at $\underline{a}, \underline{\xi}$, that will be denoted $\chi_{\varphi,x,\mathcal{B}}$ or just $\chi_{\varphi,x}$ when no confusion is possible.

Remark 2.6. — We will see later (see Corollary 6.1) that if the φ-module D has dimension d, then $\chi_{\varphi,0,\mathcal{B}} = X^d$.

Of course, $\chi_{\varphi,x,\mathcal{B}}$ lies in $K[X, \sigma]$. The main properties of this polynomial are that $\chi_{\varphi,x,\mathcal{B}}(\varphi)(x) = 0$ and that $\chi_{\varphi,x,\mathcal{B}}$ is constructed algebraically from $G(\underline{a})$ and the coefficients

of x. Let us give an example with $\sigma(x) = x^q$, $d = 2$, $G = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then $\chi_{\varphi,x} = X^2 + P_1(a,b,c,d)X + P_0(a,b,c,d)$, with $P_0(a,b,c,d) = adc^{q-1} - bc^q$, $P_1(a,b,c,d) = -a^q - c^{q-1}d$. Note that, when formally putting $q = 1$, we recover the expression of the characteristic polynomial. When $d = 3$, with $x = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, we can write $\chi_{\varphi,x} = X^3 + P_2X^2 + P_1X + P_0$. The polynomial P_0 has 336 terms, P_1 has 232 terms, and P_2 has 107 terms.

Lemma 2.7. — *Let (D, φ) be a φ-module of dimension d over K, endowed with a basis $\mathcal{B}$. Let $x \in D$ and let $\chi_{\varphi,x}$ be the associated semi-characteristic polynomial. Then the left-ideal $I_{\varphi,x} = \{Q \in K[X,\sigma] \mid Q(\varphi)(x) = 0\}$ contains $\chi_{\varphi,x}$, and if the φ-module D is generated by x, then $I_{\varphi,x} = K[X,\sigma]\chi_{\varphi,x}$.*

Proof. — We have already seen that $\chi_{\varphi,x}(\varphi)(x) = 0$. Assume x generates D, then $x, \varphi(x), \ldots, \varphi^{d-1}(x)$ is a linearly independent family in D, so all the nonzero elements of $I_{\varphi,x}$ have degree at least d. Then the monic generator of $I_{\varphi,x}$, which is the minimal polynomial $m_{\varphi,x}$ of x by definition, has degree d. Since $I_{\varphi,x}$ contains a unique monic element of minimal degree, $m_{\varphi,x} = \chi_{\varphi,x}$. Hence $I_{\varphi,x} = K[X,\sigma]\chi_{\varphi,x}$. □

The hypothesis that the φ-module admits a generator might not sound very satisfactory, but the following proposition shows that, at least when K is infinite, such a generator always exists.

Proposition 2.8. — *Assume the field K is infinite, and let (D, φ) be an étale φ-module over K. Then there exists $x \in D$ which generates D under the action of φ.*

Proof. — Let $d = \dim D$. What we want to prove is that there exists $x \in D$ such that the determinant $\det(x, \varphi(x), \ldots, \varphi^{d-1}(x)) \neq 0$. We work with the field $K(X_1, \ldots, X_d)$ over which the map σ extends naturally, and we denote by G the matrix of the map φ in a basis of D. Let $x_0 = (X_1, \ldots, X_d)$ and for $0 \leq i \leq d-1$, $x_{i+1} = G\sigma(x_i)$, we consider the polynomial $R = \det(x_0, \ldots, x_{d-1})$. Since K is infinite, it is enough to show that R is not the zero polynomial. Hence, it is enough to check that there is a specialization of $X_1, \ldots, X_d$ in an algebraic closure K^{alg} of K such that R is not sent to zero. Since D is isomorphic over K^{alg} to the φ-module whose matrix is identity, $R = \alpha V_q(X_1, \ldots, X_d)$ where $\alpha \in K$ is nonzero and V_q is the q-Vandermonde determinant that already appeared above, which is nonzero. This shows that $R \neq 0$. □

Remark 2.9. — We shall see later what happens when K is finite. The matter of when a φ-module over K has a generator is discussed in the section 6.1. We will also see in the

next section a more precise description of $\chi_{\varphi,x}$ when x is not a generator (see Corollary 4.3).

I.3. Basic properties

We look at some of the first properties of the semi-characteristic polynomials that are directly related to Ore's theory of skew polynomials. In particular, we explain how the notion of similarity appears naturally in our context. Note that the results of this section and the next one are mostly a reinterpretation of Chapter I of [**Jac96**].

Proposition 3.1. — *Let D be a φ-module over K and $x, y \in D$ two nonzero elements. Assume that both x and y generate D as a φ-module. Then $\chi_{\varphi,x}$ and $\chi_{\varphi,y}$ are similar.*

Proof. — Since x generates D, there exists $U \in K[X,\sigma]$ such that $y = U(\varphi)(x)$. Now, let $\mathcal{B}$ be a basis of D, and let $\chi_{\varphi,x}, \chi_{\varphi,y}$ be the semi-characteristic polynomials corresponding to x and y in this basis. Then $\chi_{\varphi,y}U(\varphi)(x) = 0$, so $\chi_{\varphi,x}$ is a right-divisor of $\chi_{\varphi,y}U$.
Since y generates D, there exists a polynomial V such that $x = V(\varphi)(y)$, so that $VU(\varphi)(x) = x$. Hence, $\chi_{\varphi,x}$ divides $VU - 1$ on the right: this exactly means that the right greatest common divisor of U and $\chi_{\varphi,x}$ is 1. Hence, $\chi_{\varphi,y}U$, that has degree $\deg U + \deg \chi_{\varphi,x}$, is the left lowest common multiple of U and $\chi_{\varphi,x}$. Conversely, let P be a monic polynomial similar to $\chi_{\varphi,x}$. Then there exists $U \in K[X,\sigma]$ and $V \in K[X,\sigma]$ two polynomials, such that U and $\chi_{\varphi,x}$ are right-coprime, and $V\chi_{\varphi,x} = PU$. Since U and $\chi_{\varphi,x}$ are right-coprime, there exist $P_1, P_2 \in K[X,\sigma]$ such that $P_1U + P_2\chi_{\varphi,x} = 1$, so $P_1(\varphi)U(\varphi)(x) = x$. In particular, $y = U(\varphi)(x)$ is a generator of D. Moreover, $P(\varphi)(y) = 0$, so $\chi_{\varphi,y}$ is a right-divisor of P. Since they have the same degree and P is monic, they are equal. □

Corollary 3.2. — *Let (D_1, φ_1) and (D_2, φ_2) be two isomorphic φ-modules. Assume that $x_1 \in D_1$ generates D_1, and $x_2 \in D_2$ generates D_2. Then the semi-characteristic polynomials χ_{φ_1,x_1} and χ_{φ_2,x_2} are similar.*

Proof. — Choosing an isomorphism mapping x_1 to some $x_2' \in D_2$, we are reduced to prove that χ_{φ_2,x_2} and $\chi_{\varphi_2,x_2'}$ are similar. This follows from Proposition 3.1. □

This shows that if x generates the φ-module D, and $\mathcal{B}$ is a basis of D, then the semi-characteristic polynomial $\chi_{\varphi,x,\mathcal{B}}$ does not depend on the choice of the basis up to similarity. Frow now on, we shall sometimes talk about *the* semi-characteristic polynomial of a φ-module, which will stand for the set of its characteristic polynomials with first vector generating the φ-module. It is contained in a similarity class that depends neither upon the class of isomorphism of the φ-module, nor upon the choice of the generator x.

More precisely, it is the set of all monic polynomials contained in this similarity class. This set will be denoted by χ_φ.

I.4. Semi-characteristic polynomials and sub-φ-modules

We now want to understand how the notion of semi-characteristic polynomial behaves with respect to sub-φ-modules.

Proposition 4.1. — *Let (D, φ) be a φ-module of dimension d over K. Then $\chi_{\varphi,x}$ is irreducible in $K[X, \sigma]$ for all $x \in D \setminus \{0\}$ if and only if D is a simple φ-module.*

Proof. — Assume that $\chi_{\varphi,x}$ is irreducible for all $x \in D \setminus \{0\}$. Using the above notations, for all x, $I_{\varphi,x} = K[X, \sigma]\chi_{\varphi,x}$. This means that for all nonzero polynomial $Q \in K[X, \sigma]$ with $\deg Q < d$, and for all x, $Q(\varphi)(x) \neq 0$. In particular, all the families $x, \ldots, \varphi^{d-1}(x)$ are linearly independent over K, so D is simple.
Conversely, assume that D is simple. Let $x \in D$, nonzero. If $\chi_{\varphi,x} = PQ$ with P, Q monic and $\deg P < d$, then $P(\varphi)Q(\varphi(x)) = 0$. The φ-module generated by $Q(\varphi(x))$ is then of dimension $< d$, so it is zero, and $Q(\varphi(x)) = 0$, which means that $\chi_{\varphi,x}$ divides Q on the right, so $Q = \chi_{\varphi,x}$. □

Proposition 4.2. — *Let $0 \to D_1 \to D \to D_2 \to 0$ be an exact sequence of φ-modules, and denote by $\varphi_1, \varphi, \varphi_2$ the respective maps on D_1, D, D_2. Let $x \in D$. Let $\bar{x} = x$ mod D_1, and $x_1 = \chi_{\varphi_2,\bar{x}}(\varphi)(x)$. Then*

$$\chi_{\varphi,x} = \chi_{\varphi_1,x_1}\chi_{\varphi_2,\bar{x}}.$$

Moreover, if x is a generator of D, then x_1 (resp. $\bar{x}$) is a generator of D_1 (resp. of D_2).

Proof. — We can assume that K is algebraically closed. The set $\{x \in D \ / \ x \text{ generates } D\}$ is the Zariski-open subset of D $\{\det(x, \varphi(x), \ldots, \varphi^{d-1}(x)) \neq 0\}$. Since it is not empty, and the identity is polynomial in the coefficients of the vector x, it is enough to prove the proposition when x is a generator of D. The result is clear if $D_1 = D$, so we assume that $D_1 \neq D$. In this case, $x \notin D_1$, otherwise x would not generate the whole of D. Therefore, $\bar{x} \neq 0$. Let $x_1 = \chi_{\varphi_2,\bar{x}}(\varphi)(x)$. Since $\chi_{\varphi_2,\bar{x}}(\varphi)(\bar{x}) = 0$, $x_1 \in D_1$. It is a generator of D_1, otherwise there would be a polynomial P with degree $< \dim D_1$ such that $P(\varphi)(x_1) = 0$, so $P\chi_{\varphi_2,\bar{x}}(\varphi)(x) = 0$, with $\deg P\chi_{\varphi_2,\bar{x}} < \dim D$, which is in contradiction with the fact that x generates D. On the other hand, it is obvious that $\bar{x}$ generates D_2. Hence, $\chi_{\varphi_1,x_1}\chi_{\varphi_2,\bar{x}}(\varphi)(x) = 0$, so $\chi_{\varphi_1,x_1}\chi_{\varphi_2,\bar{x}}$ is right-divisible by P, and the equality of the degrees proves that $\chi_{\varphi,x} = \chi_{\varphi_1,x_1}\chi_{\varphi_2,\bar{x}}$. □

Corollary 4.3. — *Let D be an étale φ-module over K of dimension d and $x \in D$. Assume that the sub-φ-module D_x generated by x has dimension $r \leq d$. Denote by φ_x the map induced by φ on D_x. Then $\chi_{\varphi,x} = \chi_{\varphi_x,x} X^{d-r}$.*

Proof. — Apply Corollary 4.3 with D_1 the sub-φ-module generated by x. Since x is 0 in D_2 and D_2 has dimension $d-r$, it remains to show that $\chi_{\varphi_2,0} = X^{d-r}$. We will show by induction on d that if D is a φ-module of dimension d, then $\chi_{\varphi,0} = X^d$. Assume K is algebraically closed. If $d = 1$, a direct computation shows that $\chi_{\varphi,0} = X$. For $d \geq 2$, D is isomorphic to the φ-module whose matrix is identity since K is algebraically closed, so we can pick a sub-φ-module D_1 of D of dimension 1. By induction hypothesis and Proposition 4.2, we get the fact that $\chi_{\varphi,0} = X \cdot X^{d-1} = X^d$. □

Theorem 4.4. — *Let $0 \subset D_m \subset \cdots \subset D_0 = D$ be a Jordan-Hölder sequence for the φ-module D. Denote by φ_i the map induced by φ on D_i, and by $\overline{\varphi_i}$ the map induced by φ on D_i/D_{i+1} for $0 \leq i \leq m-1$. Let $x \in D$. Then*

$$\chi_{\varphi,x} = \pi_{m-1} \cdots \pi_0,$$

with $\pi_i = \chi_{\overline{\varphi_i},y_i}$ for some $y_i \in D_i/D_{i+1}$, for all $0 \leq i \leq m-1$ (in particular each polynomial π_i is irreducible in $K[X,\sigma]$).

Proof. — Let us prove the theorem by induction on m. If $m = 0$ the result is clear. Assume $m \geq 1$, then Proposition 4.2 shows that $\chi_{\varphi,x} = \chi_{\varphi_1,x_1}\chi_{\overline{\varphi_0},\bar{x}}$ with $\bar{x} = x \bmod D_1$ and $x_1 = \chi_{\overline{\varphi_0},\bar{x}}(x) \in D_1$. The induction hypothesis shows that χ_{φ_1,y_1} factors as $\prod_{i=m-1}^{2} \chi_{\varphi_i,x_i}$ with $x_i \in D_i/D_{i+1}$. □

Let D be an étale φ-module that has a generator x, and let $\chi_{\varphi,x}$ be its semi-characteristic polynomial with respect to x. If $D \to D_2$ is a quotient of D (on which the induced map is denoted by φ_2), then we can associate to D_2 the semi-characteristic polynomial $\chi_{\varphi_2,\overline{x}}$ where $\overline{x}$ is the image of x in the quotient. The following proposition shows that this map is in fact a bijection.

Proposition 4.5. — *Let D be an étale φ-module that has a generator x, and let $\chi_{\varphi,x}$ be its semi-characteristic polynomial with respect to x in some basis. Then the above map is a natural bijection between the following sets:*

(i) The monic right-divisors of $\chi_{\varphi,x}$;

(ii) The quotients of the φ-module D.

Moreover, this bijection maps exactly the irreducible divisors to the simple quotients.

Proof. — First note that by Proposition 4.2, $\chi_{\varphi_2,\bar{x}}$ is an irreducible right-divisor of P. The considered map is surjective. Indeed, let $\chi_{\varphi,x} = P_1P_2$ with P_2 irreducible, and let $y = P_2(\varphi)(x)$. Let D_y be the sub-φ-module generated by y and let $D \to D/D_y$ be the canonical projection. Then $\bar{x} = x \bmod D_y$ generates D/D_y and $P_2(\varphi)(\bar{x}) = 0$, so $\chi_{\varphi,\bar{x}} = P_2$. Now, we show that the considered map is also injective. Let D', D'' be two simple quotients endowed with the induced maps φ', φ''. Denote by $\bar{x}'$ (resp. $\bar{x}''$) the image of x by the canonical projection to D' (resp. D''). Assume that $\chi_{\varphi',\bar{x}'} = \chi_{\varphi'',\bar{x}''}$. Then there exists a unique map $D' \to D''$ sending $\bar{x}'$ to $\bar{x}''$, and this map is an isomorphism. Moreover, the kernel of the composite map $D \to D''$ is the set of $y \in D$ such that $y = Q(\varphi)(x)$ for some polynomial Q that is right-divisible by $\chi_{\varphi'',\bar{x}''}$. This is exactly the kernel of the canonical map $D \to D''$, so $D' = D''$. The fact that irreducible polynomials correspond to simple φ-modules follows from Proposition 4.1. □

We have the following corollary, that will be useful to count the factorizations of a skew polynomial over a finite field.

Corollary 4.6. — *Let $P \in K[X, \sigma]$ be a monic polynomial with nonzero constant coefficient. Then there is a natural bijection between the factorizations of P as a product of monic irreducible polynomials, and the Jordan-Hölder sequences of V_P.*

Proof. — The proof is an easy induction on the number of irreducible factors of P. □

CHAPITRE II

POLYNÔMES TORDUS ET φ-MODULES SUR LES CORPS FINIS

We now want to focus on φ-modules over finite fields. We investigate some other links with skew polynomials and the so-called linearized polynomials. The reference used for basics on linearized polynomials over finite fields is **[LN94]**, Chap 4, §4.

II.1. Galois representations and φ-modules

Let K be a field of characteristic p, and K^{sep} be a separable closure of K. There is an anti-equivalence of categories between the $\mathbb{F}_q$-representations of $G_K = \text{Gal}(K^{\text{sep}}/K)$ and the étale φ-modules over K, when φ acts as $x \mapsto x^q$ on K. The functor from representations to φ-modules is $\text{Hom}_{G_K}(\cdot, K^{\text{sep}})$, and its quasi-inverse is $\text{Hom}_{\varphi}(\cdot, K^{\text{sep}})$, where G_K acts naturally on K^{sep} and φ acts as $x \mapsto x^q$ on K^{sep}. This theory was introduced by Fontaine to study the Galois representations of local fields of characteristic p and then gave birth to the theory of (φ, Γ)-modules to study the p-adic representations of p-adic fields. We want to use this tool in the context of finite fields. Here, we use the equivalence of categories to skew polynomials rather than representations. Indeed, the data of a representation of $G_{\mathbb{F}_{q^r}}$ is very simple: it is just given by the action of the Frobenius $x \mapsto x^{q^r}$ on the representation. Let p be a prime number, $q = p^a$ a power of p, and $r \geq 1$ be an integer.

Definition 1.1. — A q-linearized polynomial over $\mathbb{F}_{q^r}$ is a polynomial $L \in \mathbb{F}_{q^r}[X]$ of the form $L = \sum_{i=0}^{d} a_i X^{q^i}$ where for all $0 \leq i \leq d$, $a_i \in \mathbb{F}_{q^r}$.

Remark 1.2. — Such polynomials define $\mathbb{F}_q$-linear maps on any extension of $\mathbb{F}_{q^r}$, hence the terminology. Furthermore, the roots of a q-linearized polynomial have a natural structure of $\mathbb{F}_q$-vector space.

The vector space of q-linearized polynomials is endowed with a structure of noncommutative $\mathbb{F}_{q^r}$-algebra, with the usual sum and product given by the composition: $L_1 \times L_2(X) =$

$L_1(L_2(X))$. It is easily checked that there is a natural isomorphism between the $\mathbb{F}_{q^r}$-algebras of q-linearized polynomials over $\mathbb{F}_{q^r}$, and of skew polynomials $\mathbb{F}_{q^r}[X,\sigma]$ where $\sigma(x) = x^q$. The correspondance between linearized and skew polynomials is the following:

Definition 1.3. — Let $P \in \mathbb{F}_{q^r}[X,\sigma]$ be a skew polynomial, $P = \sum_{i=0}^{d} a_i X^i$. By definition, the associated linearized polynomial is $L_P = \sum_{i=0}^{d} a_i X^{q^i}$. Conversely, if L is a linearized polynomial over $\mathbb{F}_{q^r}$, its associated skew polynomial is denoted by P_L.

Let $P \in \mathbb{F}_{q^r}[X,\sigma]$ be a monic polynomial, say $P = X^d - \sum_{i=0}^{d-1} a_i X^i$. To P we associate the linearized polynomial L_P as before, and the φ-module D_P given by the following data:

- $D_P = \bigoplus_{i=0}^{d-1} \mathbb{F}_{q^r} e_i$,
- for $i \in \{0,\dots,d-2\}$, $\varphi(e_i) = e_{i+1}$,
- $\varphi(e_{d-1}) = \sum_{i=0}^{d-1} a_i e_i$.

We can note that in the canonical basis $(e_0,\dots,e_{d-1})$, $\chi_{\varphi,e_0} = P$.

Lemma 1.4. — *Let (D,φ) be a φ-module over $\mathbb{F}_{q^r}$. Then (D,φ^r) is a φ^r-module over $\mathbb{F}_{q^r}$. Let V be the $\mathbb{F}_q$-representation of $G_{\mathbb{F}_{q^r}}$ associated to φ and V_r be the $\mathbb{F}_{q^r}$-representation of $G_{\mathbb{F}_{q^r}}$ associated to φ^r. Then $V_r \simeq V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$.*

Proof. — It is clear that φ^r is σ^r-semi-linear (which means just linear!). Then, there is a natural injective map $V = \mathrm{Hom}_\varphi(D,\overline{\mathbb{F}}_q) \hookrightarrow \mathrm{Hom}_{\varphi^r}(D,\overline{\mathbb{F}}_q) = V_r$. A classical argument (appearing for example in the proof of Proposition 1.2.6 in **[Fon90]**) shows that a family of elements of V that is linearly independant over $\mathbb{F}_q$ remains linearly independant over $\mathbb{F}_{q^r}$. Hence $V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$ injects into V_r, and since $\dim_{\mathbb{F}_q} V = \dim_{\mathbb{F}_{q^r}} V_r$, we get $V_r \simeq V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$. □

Lemma 1.5. — *The representation V_P associated to the φ-module D_P is naturally isomorphic to the vector space of the roots of L_P endowed with the natural action of $G_{\mathbb{F}_{q^r}}$.*

Proof. — By definition, $V_P = \mathrm{Hom}_\varphi(D_P,\overline{\mathbb{F}}_q)$. Let $f \in V_P$. Let $\xi_i = f(e_i)$, the relations between the e_i's and the fact that f is φ-equivariant imply that for all $0 \le i \le d-2$, $\xi_i = \xi_0^{q^i}$. Subsequently, $\xi_0^{q^d} = \sum_{i=0}^{d-1} a_i \xi_0^{q^i}$, so that ξ_0 is a root of L_P. Conversely, the same computation shows that given any root ξ of L_P, the map $D \to \overline{\mathbb{F}}_q$ sending e_i to ξ^{q^i} is a φ-equivariant morphism. Hence, the map $\begin{pmatrix} V_P & \to & \{\text{Roots of } L_P\} \\ f & \mapsto & f(e_0) \end{pmatrix}$ is an isomorphism. Moreover, the action of $G_{\mathbb{F}_{q^r}}$ on V_P comes from that on $\overline{\mathbb{F}}_{q^r}$, so that it is just the raising to the q^r-th power, and it is compatible with the previous map, making it an isomorphism of representations. □

Theorem 1.6. — *Let (D_P,φ) be the φ-module associated to the polynomial P. Then the Frobenius map $g \in G_{\mathbb{F}_{q^r}}$ acting on V_P (by $x \mapsto x^{q^r}$) and the map φ^r on D_P have matrices that are conjugate.*

Proof. — Since the matrix of the Frobenius acting on V_P is conjugate to the matrix of the Frobenius acting on the $\mathbb{F}_{q^r}$-representation associated to (D_P, φ^r) by Lemma 1.4, we will show that the matrix of the latter is conjugate to the matrix of φ^r. By the Chinese remainders theorem, it is enough to show the result when the characteristic polynomial of φ^r is a power of an irreducible polynomial Q. By the elementary divisors theory, it is also enough to show the result when φ^r is a cyclic endomorphism. Assume that the matrix of φ^r in the basis $(e_0, \dots e_{d-1})$ is the companion matrix of a polynomial Q^e, with Q irreducible. Then the map $\mathrm{Hom}_{\varphi^r}(D_{Q^e}, \overline{\mathbb{F}}_{q^r}) \to \{\text{Roots of } L_{Q^e(X^r)}\} = V_{Q^e(X^r)}$, mapping f to $f(e_0)$ is an isomorphism of $\mathbb{F}_{q^r}$-representations by Lemma 1.5. Let ξ be a nonzero root of $L_{Q^e(X^r)}$, and let $f \in \mathrm{Hom}_{\varphi^r}(D_{Q^e}, \overline{\mathbb{F}}_{q^r})$ mapping e_0 to ξ. Let g be the Frobenius map on $V_{Q^e(X^r)}$, and χ_g be its characteristic polynomial. Then $f(\chi_g(\varphi^r)(e_0)) = \chi_g(g)(\xi) = 0$ because f is φ^r-equivariant. Hence for all $f \in \mathrm{Hom}_{\varphi^r}(D_{Q^e}, \overline{\mathbb{F}}_{q^r})$, $f(\chi_g(\varphi^r)(e_0)) = 0$. The injectivity of the map $\mathrm{Hom}_{\varphi^r}(D_{Q^e}, \overline{\mathbb{F}}_{q^r}) \to V_{Q^e(X^r)}$ implies that $\chi_g(\varphi^r) = 0$, so the minimal polynomial of φ^r divides χ_g. If $Q^\varepsilon(g) = 0$ for some $\varepsilon \leq e$, then $Q^\varepsilon(\varphi^r)(f)(x) = Q^\varepsilon(g)(f(x))$ for all $x \in D$, $f \in \mathrm{Hom}_{\varphi^r}(D_{Q^e}, \overline{\mathbb{F}}_{q^r})$, and so $Q^\varepsilon(\varphi^r) = 0$, which shows that $\varepsilon = e$. Therefore, the minimal polynomial of g is Q^e, and the matrices of g and φ^r are conjugate. □

From now on and throughout the article, we will perform complexity computations using the usual notations O and $\tilde{O}$ (we say that a complexity is $\tilde{O}(g(n))$ if it is $O(g(n)\log^k(n))$ for some integer k). For computations over finite fields, we will usually express the complexity as the number of operations needed in the base field $\mathbb{F}_q$. We will make the common assumption that the multiplication in $\mathbb{F}_{q^r}$ is quasilinear. We will denote by $MM(d)$ the complexity of the multiplication of two matrices of size $d \times d$ over $\mathbb{F}_q$, so that the multiplication of two matrices of size $d \times d$ over $\mathbb{F}_{q^r}$ is $MM(dr)$.

Remark 1.7. — The matrix of g can be computed in $O(MM(dr)\log r + d^2r^2 \log q \log r)$ multiplications in $\mathbb{F}_q$ if P has degree d and multiplication of matrices of size $d \times d$ over $\mathbb{F}_{q^r}$ has complexity $MM(dr)$. Indeed, if G is the companion matrix of φ, then the matrix of φ^r is $G\sigma(G)\cdots\sigma^{r-1}(G)$. Since applying σ^t to an element of $\mathbb{F}_{q^r}$ costs $t \log q$ operations in $\mathbb{F}_{q^r}$ (by a fast exponentiation algorithm), a divide-and-conquer algorithm allows us to compute the matrix of φ^r with $O(MM(d)\log r + d^2 r)$ operations in $\mathbb{F}_{q^r}$.

The following proposition gives another application of considering φ^r, namely testing similarity of polynomials.

Proposition 1.8. — *Let $P, Q \in \mathbb{F}_{q^r}[X, \sigma]$ be two monic polynomials. Let Γ_P (resp. Γ_Q) be the companion matrix of P (resp. Q). Then P and Q are similar if and only if the matrices $\Gamma_P \cdots \sigma^{r-1}(\Gamma_P)$ and $\Gamma_Q \cdots \sigma^{r-1}(\Gamma_Q)$ are conjugate.*

Algorithm 1 Returns $E(G,r) = G\sigma(G)\cdots\sigma^{r-1}(G)$

Input: G the matrix of φ, $r \geq 1$ an integer
Output: $E(G,r)$ the matrix of φ^r

```
if r = 1 then
  return G
else
  if r is even then
    return E(G, r/2) · σ^{r/2}(E(G, r/2))
  else
    return G · σ(E(G, (r − 1)/2) · σ^{(r−1)/2}(E(G, (r − 1)/2)))
  end if
end if
```

Proof. — Assume P and Q are similar, and let $d = \deg P = \deg Q$. Then $P = \chi_{\varphi,x}$ for some $x \in D_Q$. Therefore, there exists $U \in GL_d(\mathbb{F}_{q^r})$ such that $\Gamma_P = U^{-1}\Gamma_Q\sigma(U)$, so $\Gamma_P\cdots\sigma^{r-1}(\Gamma_P) = U^{-1}\Gamma_Q\cdots\sigma^{r-1}(\Gamma_Q)U$. Hence, these two matrices are conjugate.
Conversely, assume that these matrices are conjugate. Then the representations V_Q and V_P are isomorphic (because these matrices are conjugate to the matrices of the action of the Frobenius on the respective representations, which are therefore $\mathbb{F}_q$-conjugate), so the φ-modules D_P and D_Q are isomorphic. Hence, P and Q are similar. □

This proposition shows how similarity can be tested only by computing the Frobenius normal form of φ^r, which can be done in $\tilde{O}(MM(dr))$ operations in $\mathbb{F}_q$.

II.2. The splitting field of a linearized polynomial

In this section, we use the previous results to explain how to compute the splitting field of a q-linearized polynomial with coefficients in $\mathbb{F}_{q^r}$ and the action of $G_{\mathbb{F}_{q^r}}$ on its roots. We start with a lemma from [**LN94**].

Lemma 2.1. — *Let $Q \in \mathbb{F}_q[Y]$ with nonzero constant coefficient and let L_Q be the q-linearized associated polynomial. Then the splitting field of L_Q is $\mathbb{F}_{q^m}$, where m is the maximal order of a root of Q in $\overline{\mathbb{F}}_q^\times$.*

Remark 2.2. — If $Q = Q_1^{t_1}\cdots Q_s^{t_s}$ with the polynomials Q_i distinct monic irreducible, then setting $t = \max\{t_i\} - 1$ and $e = \max\{\text{Order of the roots of } Q_i\}$, we have $m = ep^t$.

We are ready to prove the following:

Theorem 2.3. — *Let $P \in \mathbb{F}_{q^r}[X,\sigma]$ with nonzero constant coefficient, and let L_P be the associated linearized polynomial. Let Γ be the companion matrix of P, and $\Gamma_0 = \Gamma\sigma(\Gamma)\cdots\sigma^{r-1}(\Gamma)$. Then the characteristic polynomial Q of Γ_0 has coefficients in $\mathbb{F}_q$, and the splitting field of L_P has degree m over $\mathbb{F}_{q^r}$, where m is the maximal order of a root of*

Q in $\overline{\mathbb{F}}_q$.

Moreover, the Frobenius normal form G_0 of Γ_0 has coefficients in $\mathbb{F}_q$, and the action of a generator g of the Galois group $G_{\mathbb{F}_{q^r}}$ is given (in some basis of the $\mathbb{F}_q$-vector space of the roots of L_P) by G_0.

Proof. — By Theorem 1.6, Γ_0, being the matrix of (D_P, φ^r), is conjugate to the matrix of the action of g on the roots of L_P. The latter has coefficients in $\mathbb{F}_q$ since it is the matrix of an $\mathbb{F}_q$-representation V_P of $G_{\mathbb{F}_{q^r}}$, as does the Frobenius normal form of Γ_0. It only remains to determine the splitting field of L_P. But this field is the same as the subfield of $\overline{\mathbb{F}}_{q^r}$ fixed by the kernel of the representation V_P. This again is the same as the subfield fixed by the kernel of the representation $V_P \otimes \mathbb{F}_{q^r}$, which is the same as the splitting field of L_Q. The result then follows from Lemma 2.1. □

Example 2.4. — Let $q = 7$ and $r = 5$. The field $\mathbb{F}_{7^5}$ is built as $\mathbb{F}_7[Y]/(Y^5 + Y + 4)$, and ω denotes the class of Y in $\mathbb{F}_{7^5}$. Let $L = Z^{7^3} + \omega Z^{7^2} - \omega^2 Z \in \mathbb{F}_{7^5}[Z]$. The associated skew polynomial $P \in \mathbb{F}_{7^5}[X, \sigma]$ is $X^3 + \omega X^2 - \omega^2$, so the matrix of φ on D_P is $\Gamma = \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & 1 & -\omega \end{pmatrix}$.
The characteristic polynomial of the matrix Γ_0 of φ^r is $Y^3 + Y^2 + Y + 5$, which is irreducible. The order of any root of this polynomial in $\overline{\mathbb{F}}_7$ is 171, so the splitting field of L is $\mathbb{F}_{7^{5\times 171}}$.
This also shows that the Jordan form of the matrix of φ^r is $\begin{pmatrix} 0 & 0 & -5 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$, that is the matrix of the action of $x \mapsto x^{7^5}$ on a basis of the roots of L over $\mathbb{F}_{7^5}$.

II.3. Optimal bound of a skew polynomial

The previous section has shown that, given a φ-module (D, φ) over $\mathbb{F}_{q^r}$, the φ^r-module (D, φ^r) should have interesting properties for the study of (D, φ). In this subsection, we will show how this idea can also help us solve the problem of finding a multiple of a polynomial lying in the center of $\mathbb{F}_{q^r}[X, \sigma]$. We recall the notations from the above section, that we shall use in this one: if $P \in \mathbb{F}_{q^r}[X, \sigma]$, then D_P is the associated φ-module, L_P is the associated linearized polynomial, and V_P is the associated linear representation of $G_{\mathbb{F}_{q^r}}$ (either by Fontaine's theory, or as the roots of L_P, since both are the same object by Lemma 1.5).

The following lemma is a slightly generalized version of a lemma from [**LN94**], where only the case $r = 1$ is treated.

Lemma 3.1. — *Let L_1, L be two linearized polynomials. Then L_1 is a right-divisor of L in the algebra of linearized polynomials if and only if it is a divisor of L in the classical sense.*

Proof. — First assume that L_1 divides L on the right in the sense of linearized polynomials, meaning that there exists a linearized polynomial L_2 such that $L(X) = L_2(L_1(X))$. Since the constant coefficient of L_2 is zero, this implies that L_1 divides L in the classical sense. Conversely, if L_1 divides L in the classical sense, write the right-euclidean division of L by L_1 as linearized polynomials, we have $L = L_2 \circ L_1 + R$ with $\deg R < \deg L_1$. From the first part of the proof, L_1 divides $L_2 \circ L_1$ in the classical sense, so it also divides R. Since $\deg R < \deg L_1$, $R = 0$. □

This already allows us to give an explicit description of the *optimal bound* of a skew polynomial. A bound of a skew polynomial P is a nonzero multiple of P that lies in the center of $\mathbb{F}_{q^r}[X, \sigma]$ (which is easily shown to be $\mathbb{F}_q[X^r]$), and an optimal bound is a bound with lowest degree.

Theorem 3.2. — *Let $P \in \mathbb{F}_{q^r}[X, \sigma]$ be a monic polynomial with nonzero constant term. Let π_{φ^r} be the minimal polynomial of the $\mathbb{F}_q$-linear map $\varphi^r : D_P \to D_P$. Then the optimal bound for P is $\pi_{\varphi^r}(X^r)$. It has degree at most $r \deg P$ and can be computed in $\tilde{O}(d^2 r^2 \log q + MM(rd))$ operations in $\mathbb{F}_q$.*

Proof. — Since $\pi_{\varphi^r}(\varphi^r) = 0$, $\pi_{\varphi^r}(X^r)(\varphi)(e_0) = 0$. Since $P = \chi_{\varphi, e_0}$, P is a right divisor of $\pi_{\varphi^r}(X^r)$. Conversely, if $Q \in \mathbb{F}_q[Y]$ is a monic polynomial such that $Q(X^r)$ is right-divisible by P, then $Q(\varphi^r)(e_0) = 0$. Moreover, since $Q(X^r)$ is central, $XQ(\varphi^r)(e_0) = Q(\varphi^r)(\varphi(e_0))$. An immediate induction shows that, since e_0 generates D_P under the action of φ, $Q(\varphi^r) = 0$. Hence, π_{φ^r} divides Q.
By Remark 1.7, the matrix of φ^r can be computed in $\tilde{O}(d^2 r^2 \log q + MM(rd))$ operations in $\mathbb{F}_q$. Its minimal polynomial can be computed in $\tilde{O}(MM(rd))$ operations by **[Gie95]**, hence the complexity of the computation of the optimal bound. □

Remark 3.3. — This complexity can be compared with Giesbrecht's computation of an optimal bound in $\tilde{O}(d^3 r^2 + MM(rd))$ operations in $\mathbb{F}_{q^r}$ (**[Gie98]**, Lemma 4.2). Since this part is used in his factorization algorithm, computing the optimal bound using Theorem 3.2 improves the complexity of this part of Giesbrecht's algorithm.

Theorem 2.3 has shown that the characteristic polynomial of φ^r already gives interesting information. Since the characteristic polynomial is also slightly easier to compute than the minimal polynomial, we introduce the following definition:

Definition 3.4. — Let $P \in \mathbb{F}_{q^r}[X, \sigma]$ a monic skew polynomial, and let (D_P, φ) be the associated φ-module. The polynomial $\Psi(P) \in \mathbb{F}_q[Y]$ is defined as the characteristic polynomial of φ^r, that is $\det(Y id - \varphi^r)$.

Remark 3.5. — The polynomial $\Psi(P)$ can be thought of as lying in the center $\mathbb{F}_q[X^r]$ of $\mathbb{F}_{q^r}[X, \sigma]$. This is a reason why we use the variable Y. The other reason is that $\Psi(P)$ is a commutative polynomial, and a different notation for the variable can help avoid confusions.

Remark 3.6. — By a result of Keller-Gehrig, the characteristic polynomial of an endomorphism of $\mathbb{F}_{q^r}^d$ can be computed in $O(MM(dr))$ operations in $\mathbb{F}_q$ (see **[KG85]**). Hence, if P has degree d, $\Psi(P)$ can be computed in $O(MM(dr)\log r + d^2r^2 \log r \log q)$ operations in $\mathbb{F}_q$.

Corollary 3.7. — *Let $P \in \mathbb{F}_{q^r}[X, \sigma]$ with nonzero constant coefficient. The polynomial $\Psi(P)(X^r)$ is a bound for P.*

Proof. — It follows directly from Theorem 3.2. □

II.4. The map Ψ and factorizations

In this section, we explain how the map Ψ can be used to find factorizations of a skew polynomial.

Let (D, φ) be an étale φ-module over $\mathbb{F}_{q^r}$.

Proposition 4.1. — *The map Ψ is constant on similarity classes.*

Proof. — Assume that the φ-module D is generated by some $x \in D$, and let $\chi_{\varphi,x}$ be the corresponding semi-characteristic polynomial of φ in the basis $x, \varphi(x), \ldots, \varphi^{d-1}(x)$. Then it is clear from the definition that $\Psi(\chi_{\varphi,x})$ is the characteristic polynomial of φ^r. Now, if two polynomials P and Q are similar, Q appears as the semi-characteristic polynomial of an element of D_P. Hence, there exists $x \in D_P$ such that $\chi_{\varphi,x} = Q$. In this case, $\Psi(Q)$ is the characteristic polynomial of φ^r, which also equals $\Psi(P)$, so $\Psi(P) = \Psi(Q)$. □

As we will see below, Ψ does not classify the similarity classes of polynomials, but it classifies the similarity classes of the factors appearing in the factorizations of a polynomial.

Proposition 4.2. — *Let $P, Q \in \mathbb{F}_{q^r}[X, \sigma]$ be two monic, nonconstant polynomials. Then $\Psi(PQ) = \Psi(P)\Psi(Q)$.*

Proof. — We translate Proposition 4.2 in terms of matrices: let $(e_0, \dots, e_{d-1})$ be the canonical basis of D_{PQ}, and let $y = Q(\varphi)(e_0)$. Let $\delta_1 = \deg P$ and $\delta_2 = \deg Q$, then $(y, \varphi(y), \dots, \varphi^{\delta_1 - 1}(y), e_0, \dots, e_{\delta_2 - 1})$ is a basis of D_{PQ} in which the matrix of φ is $H = \left(\begin{array}{c|c} G_P & (\star) \\ \hline 0 & G_Q \end{array}\right)$, where G_P (resp. G_Q) is the companion matrix of P (resp. of Q). Since this matrix is block-upper-triangular, the characteristic polynomial of $H\sigma(H)\cdots\sigma^{r-1}(H)$ is $\Psi(P)\Psi(Q)$. On the other hand, since H is the matrix of φ in some basis, this characteristic polynomial is $\Psi(PQ)$. □

Proposition 4.3. — *Let $P, Q \in \mathbb{F}_{q^r}[X, \sigma]$ be two monic polynomials with P irreducible. Then P is similar to a right-divisor of Q if and only if $\Psi(P)$ divides $\Psi(Q)$.*

Proof. — The case $P = X$ is obvious, so we treat the case where P has nonzero constant coefficient. If P is a right-divisor of Q, then Proposition 4.2 shows that $\Psi(P)$ divides $\Psi(Q)$. Conversely, if $\Psi(P)$ divides $\Psi(Q)$, we want to show that D_P is a quotient of D_Q, or equivalently, that V_P is a subrepresentation of V_Q. Let g be the Frobenius map $x \mapsto x^{q^r}$ acting on V_Q. We want to show that V_Q has a subspace stable under g, of dimension $\deg P$, on which the characteristic polynomial of g is $\Psi(P)$. By the Chinese remainders Theorem, we can assume that $\Psi(Q)$ is a power of $\Psi(P)$. Indeed, this Theorem shows that D_Q is the direct sum of subspaces stable under the action of g, and such that the characteristic polynomial of the action of g on each of these subspaces is a power of an irreducible polynomial. Now, assuming that $\Psi(Q)$ is a power of $\Psi(P)$, we see that the Jordan form of g on V_Q is a block-upper-triangular matrix whose diagonal blocks are all the same, equal to the companion matrix of $\Psi(P)$. Thus V_P appears as a subrepresentation of V_Q. □

Corollary 4.4. — *Let $P \in \mathbb{F}_{q^r}[X, \sigma]$. Then the similarity classes of irreducible factors of P appear in all possible orders in the factorizations of P.*

Proof. — If the similarity class of $P_0 \in K[X, \sigma]$ appears in some factorization of P, then $\Psi(P_0)$ is a divisor of $\Psi(P)$, and P has a right-divisor similar to P_0. For the general case, it is easy to see that if $Q \in \mathbb{F}_{q^r}[X, \sigma]$ is any polynomial, then there exists $\tilde{Q}$ similar to Q such that $XQ = \tilde{Q}X$. □

Corollary 4.5. — *Let $P, Q \in \mathbb{F}_{q^r}[X, \sigma]$ be two monic polynomials, with P irreducible. Then P and Q are similar if and only if $\Psi(P) = \Psi(Q)$.*

Proof. — Since we already know that Ψ is constant on similarity classes, it is enough to prove that if $\Psi(P) = \Psi(Q)$, then P and Q are similar. If $\Psi(P) = \Psi(Q)$, then Q has a

right-divisor that is similar to P. Since P and Q have the same degree, P is similar to Q. □

We note that this property is not true when P is not irreducible: this will be discussed in Remark 4.10 below.

Lemma 4.6. — *Every irreducible monic polynomial in $\mathbb{F}_q[Y]$ is the image of a monic irreducible polynomial by the map Ψ.*

Proof. — It is clear that Y is the image of X. Now assume that $R \in \mathbb{F}_q[Y]$ is irreducible, monic, with nonzero constant coefficient. Let V be the $\mathbb{F}_q$-representation of $G_{\mathbb{F}_{q^r}}$ whose dimension is the degree of R, and for which the matrix of the Frobenius map $x \mapsto x^{q^r}$ is the companion matrix of R. Let (D, φ) be the φ-module corresponding to V. Since R is irreducible, V is an irreducible representation, so (D, φ) is an irreducible φ-module. Let χ_φ be the semi-characteristic polynomial of φ at some nonzero $x \in D$. Theorem 1.6 shows that R is equal to the characteristic polynomial of φ^r, which is just $\Psi(\chi_\varphi)$ by definition. Moreover, the irreducibility of the φ-module D yields the irreducibility of $\chi_{\varphi,x}$. □

Corollary 4.7. — *Let $P \in \mathbb{F}_{q^r}[X, \sigma]$ be a monic polynomial. The polynomial P is irreducible if and only if $\Psi(P)$ is irreducible in $\mathbb{F}_q[Y]$.*

Since testing irreducibility of a polynomial of degree d over $\mathbb{F}_q$ can be done in $O(dMM(d))$ mulitplications in $\mathbb{F}_q$, we can test irreducibility of a polynomial in $\mathbb{F}_{q^r}[X, \sigma]$ of degree d in $O(d^2r^2 \log r \log q + MM(rd) + dMM(d))$ multiplications in $\mathbb{F}_q$.

Proof. — We can assume that P has nonzero constant coefficient. By Proposition 4.2, we know that if $\Psi(P)$ is irreducible, then so is P. Conversely, Lemma 4.6 shows that every irreducible divisor D of $\Psi(P)$ has an irreducible antecedent Q by Ψ. By Proposition 4.3, Q is similar to a right-divisor of P. Hence since P is irreducible, $Q = P$, and $\Psi(P) = D$, so $\Psi(P)$ is irreducible. □

Corollary 4.8. — *The map Ψ is surjective.*

Proof. — The result follows directly from Lemma 4.6 and Proposition 4.2. □

Corollary 4.9. — *The degrees of the factors in a factorization of a monic polynomial $P \in \mathbb{F}_{q^r}[X, \sigma]$ as a product of irreducibles are the same as the degrees of the factors of $\Psi(P)$ in a factorization as a product of irreducible polynomials in $\mathbb{F}_q[Y]$.*

Remark 4.10. — Let $P, Q \in \mathbb{F}_{q^r}[X, \sigma]$ be two monic polynomials, then $\Psi(P) = \Psi(Q)$ if and only if D_P and D_Q have the same semi-simplifications. Indeed, the similarity classes (with multiplicities) of the monic irreducible factors appearing in factorizations of P are

uniquely determined by $\Psi(P)$ because Ψ is multiplicative and by Ore's Theorem. On the other hand, these similarity classes are also uniquely determined by the semi-simplification of D_P again by multiplicativity of Ψ and by Theorem 4.4.

Now, we use the map Ψ to get more precise information about the factorization of $P \in \mathbb{F}_{q^r}[X, \sigma]$ from the factorization of $\Psi(P) \in \mathbb{F}_q[Y]$.

Proposition 4.11. — *Let $P \in \mathbb{F}_{q^r}[X, \sigma]$ be a monic polynomial. Assume $\Psi(P) = Q_1 \cdots Q_s$, with $Q_i \in \mathbb{F}_q[Y]$ distinct irreducible monic polynomials ($\Psi(P)$ is square-free). Then P has a unique right-divisor P_i such that $\Psi(P_i) = Q_i$. It is given by $P_i = rgcd(P, Q_i(X^r))$.*

Proof. — Assuming that the P_i's are irreducible, uniqueness is clear, since a right-divisor S of P such that $\Psi(S) = Q_i$ must divide both P and $Q_i(X^r)$. Let $1 \leq i \leq s$, and $P_i = rgcd(P, Q_i(X^r))$. Since $V_{\Psi(P)(X^r)} = V_P \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$, $\Psi(\Psi(P)(X^r)) = \Psi(P)(X)^r$. Hence, all divisors of $\Psi(P_i)$ are in the same similarity class, and $\Psi(P_i)$ is a power of Q_i, so its degree is divisible by $\deg Q_i$. But Q_i has only multiplicity one as a divisor of $\Psi(P)$, so $\Psi(P_i)$ is either 1 or Q_i. Since $\sum_i \deg P_i = \deg P$, $\Psi(P_i) = Q_i$ for all $1 \leq i \leq s$, and P_i has degree $\deg Q_i$ and is irreducible because Q_i is. □

Remark 4.12. — More generally, when $\Psi(P) = Q_1^{e_1} \cdots Q_s^{e_s}$, $P_i = rgcd(P, Q_i(X^r))$ has degree divisible by $\deg Q_i$, and $\Psi(P_i) = Q_i^{\varepsilon_i}$ for some $1 \leq \varepsilon_i \leq e_i$. This can sometimes provide a partial or even complete factorization for P, but not always: this will be better understood later when we count factorizations of a given polynomial.

II.5. Counting irreducible polynomials

Before counting factorizations of a given skew polynomial, we focus on finding the number of monic irreducible skew polynomials. This computation appears in **[CHH04]**, although it is obtained by very different methods. Here, it only comes from the computation of the cardinal of the fibers of Ψ.
Recall that a φ-module is called simple if it has no nontrivial subspaces stable by φ.

Lemma 5.1. — *Let D be a simple étale φ-module over $\mathbb{F}_{q^r}$ of dimension d. Then $End(D) = \mathbb{F}_q[\varphi^r] \simeq \mathbb{F}_{q^d}$.*

Proof. — Let $E = \mathrm{End}(D)$. It is clear that $\mathbb{F}_q[\varphi^r]$ is contained in E. Moreover, any $u \in E$ commutes with φ and therefore with φ^r. Since D is simple, φ^r has no nontrivial invariant subspace, so it is a result of elementary linear algebra that the commutant of φ^r is $\mathbb{F}_{q^r}[\varphi^r]$. Hence E is contained in $\mathbb{F}_{q^r}[\varphi^r]$. Now let $u = \sum_{i=0}^{d-1} a_i \varphi^r \in E$. The condition

that u commutes with φ yields $\left(\sum_{i=0}^{d-1}(a_i^q - a_i)\varphi^r\right)\varphi = 0$. Hence, the endomorphism $\sum_{i=0}^{d-1}(a_i^q - a_i)\varphi^r$ is zero on the image of φ. Since D is étale, $\sum_{i=0}^{d-1}(a_i^q - a_i)\varphi^r$ is zero, and since $(\mathrm{id}, \varphi^r, \ldots, \varphi^{(d-1)r})$ is a basis of the commutant of φ^r over $\mathbb{F}_{q^r}$, $a_i^q = a_i$ for all $0 \leq i \leq d-1$, so $u \in \mathbb{F}_q[\varphi^r]$. Hence E has dimension d over $\mathbb{F}_q$, and it is isomorphic to $\mathbb{F}_{q^d}$. □

Proposition 5.2. — *Let $Q \in \mathbb{F}_q[Y]$ be a monic irreducible polynomial of degree d. Then the number of monic polynomials $P \in \mathbb{F}_{q^r}[X, \sigma]$ such that $\Psi(P) = Q$ is $\frac{q^{dr}-1}{q^d-1}$.*

Proof. — By Corollary 4.5, it is enough to compute the number of polynomials P similar to a given P_0 such that $\Psi(P) = Q$. Let P be such a polynomial. Since Q is irreducible, so is P, and therefore the φ-module D_P is simple. We already know that any polynomial similar to P appears as a semi-characteristic polynomial of φ.

Now we want to characterize the nonzero $x, y \in D_P$ such that $\chi_{\varphi,x} = \chi_{\varphi,y}$. We claim that these are the nonzero x, y such that $y = u(x)$ for some $u \in \mathrm{End}(D_P)$. Indeed, it this is the case, then $\chi_{\varphi,x}(\varphi)(y) = u(\chi_{\varphi,x}(\varphi)(x)) = 0$, so $\chi_{\varphi,y} = \chi_{\varphi,x}$. Conversely, if $\chi_{\varphi,x} = \chi_{\varphi,y}$ then the map $x \mapsto y$ defines an automorphism of $\mathbb{F}_{q^r}$-vector space of D_P that is φ-equivariant thanks to this relation. This shows, using Lemma 5.1, that there is a natural bijection between D_P modulo the relation $\chi_{\varphi,x} = \chi_{\varphi,y}$ and D_P modulo the relation of $\mathrm{End}(D_P)$-colinearity.

Putting both parts together, we get the fact that $\{$Monic polynomials similar to $P\}$ is in bijection with $\{\mathrm{End}(D_P)$-lines in $D_P\}$, yielding the result. □

Corollary 5.3. — *The number of monic irreducible polynomials of degree d in $\mathbb{F}_{q^r}[X, \sigma]$ is*

$$\frac{q^{dr}-1}{d(q^d-1)} \sum_{i|d} \mu\left(\frac{i}{d}\right) q^i,$$

where μ is the Möbius function.

Proof. — It follows directly from Corollary 4.5, Proposition 5.2 and the classical formula for the number of irreducible monic polynomials in $\mathbb{F}_q[Y]$, that can be for instance found in [**LN94**]. As mentioned before, this formula already appeared in [**CHH04**]. □

II.6. A closer look at the structure of D_P

In this section, we consider the whole structure of the φ-module D_P instead of just looking at $\Psi(P)$. We address two different problems that both need a careful look at the structure of a φ-module D, or equivalently of the associated representation. Note that Proposition 4.11 shows that when $\Psi(P)$ has no square factors, for each choice of an order

of the similarity classes of the polynomials arising in a factorization of P, there is a unique factorization of P such that P has its factors in the chosen order. Therefore, there are exactly $s!$ factorizations of P as a product of irreducible monic polynomials in this case. The starting point of our discussion is Proposition 4.5. We rewrite it in our context, adding the formulation coming from representation theory. Let $P \in \mathbb{F}_{q^r}[X, \sigma]$ be a monic polynomial with nonzero constant coefficient. There are natural bijections between the following sets:

(i) The monic irreducible right-divisors of P;

(ii) The simple quotients of the φ-module D_P;

(iii) The irreducible subrepresentations of V_P.

Remark 6.1. — In this context, this result may sound surprising, because if $V_0 = V^{\oplus s}$ with V an irreducible representation of dimension d and $s > r$, V_0 has $\frac{q^{ds}-1}{q^d-1}$ distinct subrepresentations with irreducible quotient, whereas all the divisors of P are similar, and hence P has less than $\frac{q^{dr}-1}{q^d-1}$ monic irreducible right-divisors. There is no contradiction, however: the proposition just says that this case never happens, meaning that in this case V_0 is not some V_P, or, equivalently, that the φ-module associated to V_0 cannot be generated by a single element if $s \geq r$. We can give yet more precise information about whether there is a generator for a φ-module over a finite field: because of the equivalence of categories with the representations, the φ-module is a direct sum of φ-modules such that the composition factors of each summand are all the same, and the φ-module has a generator if and only if each of them has one. It remains to decide when a φ-module with isomorphic composition factors (that is, with semi-simplification isomorphic to a direct sum of copies of the same simple object) has a generator. We will introduce some definitions to discuss this matter. They will also be useful to count factorizations.

6.1. Generated φ-modules over finite fields. — We recall that an endomorphism is in Jordan form if its matrix is block-diagonal, where the blocks have the following form:

$$\begin{pmatrix} A & I & 0 & \dots & 0 \\ 0 & A & I & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \ddots & I \\ 0 & \dots & \dots & 0 & A \end{pmatrix},$$

where the characteristic polynomial of A is irreducible. These blocks are called the Jordan blocks, and the length of a Jordan block is the number of A in this writing (it is the length of the $\mathbb{F}_q[Y]$-module corresponding to the endomorphism whose matrix is the Jordan block).

Note that if the characteristic polynomial of the endomorphism is split, the matrices A that appear in its Jordan form are 1-dimensional. Assume that the minimal polynomial μ_g of g is a power of an irreducible polynomial π, say $\mu_g = \pi^t$, with $\deg \pi = \delta$. Let $W = \mathbb{F}_q^\delta$ endowed with the endomorphism whose matrix in the canonical basis is the companion matrix of π : any irreducible invariant subspace of g is isomorphic to W. We say that g has type $(t_1, \dots, t_m)$ if $t_1 \geq \cdots \geq t_m$ and the Jordan blocks of (the Jordan form of) g have lengths $t_1, \dots, t_m$. Of course, $t = t_1$. In general, if g has type $(t_1, \dots, t_m)$, then the map induced by g on any quotient of V by an irreducible invariant subspace has type $(t'_1, \dots, t'_m)$ where $t'_i = t_i$ except for one i for which $t'_i = t_i - 1$ (or possibly $m' = m - 1$ when $t_m = 1$).

Lemma 6.1. — *Let D be an étale φ-module over $\mathbb{F}_{q^r}$. Assume all the composition factors of D are isomorphic. Then D has a generator if and only if the number of Jordan blocks of the representation V associated to D is $\leq r$.*

Proof. — Since all the composition factors of D are isomorphic, it makes sense to talk about the type of the associated representation V, on which the Frobenius acts by g. The proof is done by induction on the type of g. The possible types for the considered endomorphisms have the form $(t_1, \dots, t_s)$ with $s \leq r$ by hypothesis. We complete the notation with zeros in order that the type is denoted by a r-tuple $(t_1, \dots, t_s, 0, \dots, 0)$. We order the types with respect to the lexicographical order. If g has type $(1, 0, \dots, 0)$, then D is simple, so it has a generator. Now assume g has type $(t_1, \dots, t_s, 0, \dots, 0)$. If every simple sub-$\varphi$-module of D is a direct factor of D, then g has type $(1, \dots, 1, 0, \dots, 0)$, and $D = D_0^{\oplus s}$ where D_0 is the only composition factor of D. But we know that $D_0^{\oplus s}$ has a generator since it is a quotient of $D_0^{\oplus r}$ which has one. Now, if D has a simple subobject D_0 that is not a direct factor, then we have an exact sequence

$$0 \to D_0 \to D \to D' \to 0$$

that is not split, and where the representation V' associated to D' has a smaller type than g. By induction hypothesis, there exists some $x_0 \in D'$ such that D' is generated by x_0. Let x be any lift of x_0 in D, and let D_x be the sub-φ-module of D generated by x. If $D_x \cap D_0 = \{0\}$, then $x_0 \mapsto x$ gives a splitting, which is not possible. Hence $D_0 \subset D_x$, and $D_x = D$, so D has a generator. □

6.2. Counting factorizations. — Now let us consider the problem of counting factorizations of a monic polynomial $P \in \mathbb{F}_{q^r}[X, \sigma]$ as a product of monic irreducible polynomials. The problem is reduced to that of computing the number of Jordan-Hölder sequences for an endomorphism g of an $\mathbb{F}_q$-vector space V. As before, first assume that the minimal

polynomial μ_g of g is a power of the irreducible polynomial π, say $\mu_g = \pi^t$, with $\deg \pi = \delta$, and let $W = \mathbb{F}_q^\delta$ endowed with the endomorphism whose matrix in the canonical basis is the companion matrix of π. There are $\frac{q^{\delta m}-1}{q^\delta-1}$ irreducible invariant subspaces for g because the intersection of such an invariant subspace with a Jordan block must be the only irreducible invariant subspace of this block, or zero, so $\mathrm{Hom}(W, V) = \mathrm{Hom}(W, W^{\oplus m})$. We want know how many quotients of V by an irreducible invariant subspace there are for each given possible type.

Lemma 6.1. — *Let $(t_1, \dots, t_m)$ be the type of g. Let $1 \leq i \leq m$ such that $i = m$ or $t_i > t_{i+1}$. Let i_0 be the smallest j such that $t_j = t_i$. Then there are $q^{\delta(i-1)} + q^{\delta i} + \cdots + q^{\delta(i_0-1)}$ invariant irreducible subspaces of V such that the quotient has type $(t_1, \dots, t_i - 1, t_{i+1}, \dots, t_m)$ (or $(t_1, \dots, t_{m-1})$ if $i = m$ and $t_m = 1$).*

Proof. — Denote by $(e_{1,1}, \dots, e_{1,\delta}, e_{2,1}, \dots, e_{2,\delta}, \dots)$ a basis of V in which the matrix of g has Jordan form. More precisely, for all $1 \leq i \leq m$, and for all $1 \leq j \leq t_i$ and $1 \leq l \leq \delta$, we have $g(e_{j,l}) = e_{j,l+1}$ if (j, l) is not of the shape $(j, 1)$ for some integer $j \geq 2$, or of the shape (j, δ) for some integer $j \geq 1$, $g(e_{j,1}) = e_{\delta u,\delta} + e_{\delta u+1,2}$ if $j \geq 2$, and $g(e_{j,\delta}) = \sum_{l=1}^{\delta} a_l e_{j,l}$, where $\sum_{l=1}^{\delta} a_l Y^{l-1} \in \mathbb{F}_q[Y]$ is an irreducible polynomial that does not depend of j (it is the characteristic polynomial of the induced endomorphism on any irreducible invariant subspace).

There are $i_0 - 1$ Jordan blocks of g whose length is greater than the length of the i-th block. For $\lambda = (\lambda_{1,1}, \dots, \lambda_{1,\delta}, \dots, \lambda_{i_0-1,\delta}) \in \mathbb{F}_q^{\delta(i_0-1)}$, let $v_\lambda = e_{i_0,1} + \sum_{j=1}^{i_0-1} \sum_{l=1}^{\delta} \lambda_{j,l} e_{j,l}$. Since two such vectors v_λ, v_μ are not colinear, they generate distinct invariant subspaces V_λ, V_μ, which are clearly isomorphic to W. Moreover, the quotient V/V_λ has the same type as $V/V_{(0)}$ because the map $V \to V$ that sends $e_{i_0,1}$ to v_λ and is the identity outside the invariant subspace generated by $e_{i_0,1}$ is an isomorphism (its matrix is upper triangular). One can build the same way invariant subspaces with quotients of the same type as generated by vectors of the shape $e_{i_0+1,1} + \sum_{j=1}^{i_0} \sum_{l=1}^{\delta} \lambda_{j,l} e_{j,l}, \dots, e_{i,1} + \sum_{j=1}^{i-1} \sum_{l=1}^{\delta} \lambda_{j,l} e_{j,l}$. There are exactly $q^{\delta i_0 - 1} + \cdots + q^{\delta i - 1}$ invariant subspaces that are built in this way. Doing such constructions for each i' satisfying the hypotheses of the lemma, we get exactly $\frac{q^{\delta m}-1}{q^\delta-1}$ irreducible invariant subspaces, which means all of them. Among these subspaces, the ones for which the quotient has the requested shape are exactly the $q^{\delta i_0 - 1} + \cdots + q^{\delta i - 1}$ built for the first i we considered. This proves the lemma. □

In order to compute the number of Jordan-Hölder sequences of g, consider the following diagram:

1	q^δ	$\dots$	$q^{\delta(m-1)}$
t_1	t_2	$\dots$	t_m

with $t_1 \geq \cdots \geq t_m$. An *admissible path* is a transformation of this table into another table

1	q^δ	$\dots$	$q^{\delta(m'-1)}$
t'_1	t'_2	$\dots$	$t'_{m'}$

such that

- either $m' = m-1$, $t'_j = t_j$ for $1 \leq j \leq m-1$, if $t_m = 1$;
- or $m' = m$, $t'_j = t_j$ for all $j \neq i$, with $1 \leq i \leq m$ such that $t_i > t_{i+1}$.

To such a path γ, we affect a weight $w(\gamma)$, which is the sum of the coefficients written above the cells of the first table containing the same number t_i as the cell whose coefficient was lowered in the second table. Here is an example of a table and all the admissible paths with the corresponding weights:

1	q^δ	$q^{2\delta}$	$q^{3\delta}$
3	2	2	1

$$\xrightarrow{1} \qquad \xrightarrow{q^\delta+q^{2\delta}} \qquad \xrightarrow{q^{3\delta}}$$

1	q^δ	$q^{2\delta}$	$q^{3\delta}$
2	2	2	1

1	q^δ	$q^{2\delta}$	$q^{3\delta}$
3	2	1	1

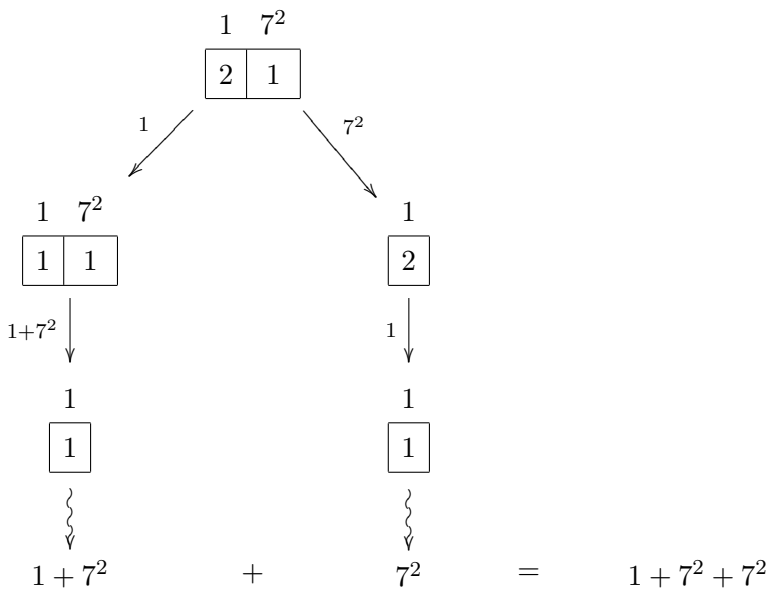
1	q^δ	$q^{2\delta}$
3	2	2

By Lemma 6.1, the weight of an admissible path from one table to another, is the number of irreducible invariant subspaces of an endomorphism g with type given by the first table such that the quotient has the type given by the second table. Therefore, a sequence of admissible paths ending to an empty table represents a class of Jordan-Hölder sequences. Thus the number of distinct sequences in this class is the product of the weights of the paths along the sequence. Hence, the number of Jordan-Hölder sequences for g is $\sum_{(\gamma_1,\dots\gamma_\tau)} \prod_{i=1}^{\tau} w(\gamma_i)$ the sum being taken on all sequences $(\gamma_1, \dots, \gamma_\tau)$ of admissible paths ending at the empty table (so $\tau = \sum_{j=1}^{m} t_j$).

In general, we do not know any simple formula for this computation (except in some particular cases that we shall discuss below), but a recursive algorithm can be used to compute the result. Given a table with coefficients $(t_1, \dots t_m)$, we need to compute the values associated to all tables that can be built out of this table through an admissible path. There are at most $t_1 \dots t_m$ such tables. According to Remark 6.1, there are at most r Jordan blocks for g. Using the notations above, this means $m \leq r$. Moreover, $\sum_{i=1}^{m} \delta t_i = \dim V$, so that $\tau \leq \frac{\dim V}{\delta}$. Then, by the arithmetic-geometric inequality, $t_1 \dots t_m \leq \left(\frac{\dim V}{\delta}\right)^r$, so the computation of the number of Jordan-Hölder sequences of g can be done in polynomial time in the dimension of V, when r is fixed.

Example 6.2. — Let us take a closer look at one particular example: assume that the type of g is $(1,\dots,1)$ (m terms). Then there is only one admissible path γ, that leads to $(1,\dots,1)$ ($m-1$ terms), and its weight is $\frac{q^{m\delta}-1}{q^{\delta}-1}$. Hence the number of Jordan-Hölder sequences of g is $\prod_{j=1}^{m}\frac{q^{\delta j}-1}{q^{\delta}-1}=[m]_{q^{\delta}}!$, the q^{δ}-factorial of m.

Example 6.3. — Let us look at an actual example. Let $q=7$, $r=2$, with $\mathbb{F}_{7^2}$ defined as $\mathbb{F}_7[Y]/(Y^2-Y+3)$, and let ω be the class of Y in $\mathbb{F}_{7^2}$. Consider the polynomial $P=X^6+\omega^3X^5+\omega^{17}X^4+\omega^3X^3+\omega^{27}X^2+\omega^{35}X+\omega^{36}$. The Jordan form of the matrix of φ^2 on D_P is $\begin{pmatrix} 0 & -4 & 0 & 0 & 0 & 0\\ 1 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & -4 & 0 & 0\\ 0 & 0 & 1 & -1 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & -4\\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$, so the endomorphism g has type $(2,1)$ with 2-dimensional irreducible blocks. We write the following diagram with all the admissible paths and their weights:



This shows that the number of factorizations of P as a product of monic irreducible polynomials is 99. An exhaustive research of all the factorizations with Magma gives the same result, but takes around one minute, whereas this computation is instantaneous.

Now, we need to look at the general case, with no further assumption on the minimal polynomial of g. In this case, by the Chinese remainders Theorem, V is a direct sum of invariant subspaces on which the induced endomorphisms have minimal polynomial that is a power of an irreducible. Here, the type of g is defined again as the data of

$((W_1, T_1), \dots, (W_s, T_s))$ where the W_l's are the distinct classes of irreducible invariant subspaces of V, and the T_l's are the tables representing the types of the endomorphisms induced on the corresponding subspaces of V. The notion of admissible path can be defined as previously.

Proposition 6.4. — *Let g be an endomorphism of an $\mathbb{F}_q$-vector space V. Assume that the type of g is $((W_1, T_1), \dots, (W_s, T_s))$. Denote by δ_i the dimension of W_i, and by τ_i the sum of the coefficients in table T_i. Then the number of Jordan-Hölder sequences of g is*

$$\frac{(\tau_1 + \cdots + \tau_s)!}{\tau_1! \cdots \tau_s!} \prod_{(\Gamma_1, \dots, \Gamma_s)} w(\Gamma_1) \cdots w(\Gamma_s),$$

the product being taken over all the s-uples $(\Gamma_1, \dots, \Gamma_s)$ of admissible path sequences ending at the empty tables.

Proof. — From a chain of admissible paths ending at $((W_1, \emptyset), \dots, (W_s, \emptyset))$, it is possible to extract its W_l-part Γ_l for all $1 \leq l \leq s$. By definition, it is the sequence of all the paths involving a change in the table associated to W_l. Such a chain is a sequence of admissible paths from T_l ending at the empty table. It is clear that the weight of the path sequence is the product of the weights of the Γ_l's. Therefore, it does not depend on the way the Γ_l's were combined together. The admissible path sequences that end at $((W_1, \emptyset), \dots, (W_s, \emptyset))$ are all the different ways to recombine admissible path sequences from all the (W_i, T_i) to the empty table. The weight of such a sequence is the product of the weights of the W_l-parts. There are as many recombinations as anagrams of a word that includes τ_l times the letter W_l for all $1 \leq l \leq s$, τ_l being the sum of the integers appearing in T_l. The result then follows directly from the previous discussion an the fact that the number of anagrams of a word that includes τ_l times the letter W_l is the multinomial coefficient $\frac{(\tau_1 + \cdots + \tau_s)!}{\tau_1! \dots \tau_s!}$. □

Example 6.5. — Assume g has type $((W_1, (t_1)), \dots, (W_s, (t_s)))$. It is easy to see that the only admissible path sequence for $(W_l, (t_l))$ has weight 1. Hence the number of Jordan-Hölder sequences of g is $\frac{(t_1 + \cdots + t_s)!}{t_1! \dots t_s!}$.

The previous discussions also allow us to explain how to find all factorizations of a given polynomial P using Giesbrecht's algorithm. A first factorization of P yields a Jordan-Hölder sequence for the φ-module D_P. All the simple sub-φ-modules of D_P can be constructed as in the proof of Lemma 6.1. Any such simple sub-φ-module yields a factorization of P as $P = P_1 Q$, with P_1 irreducible as in Theorem 4.2. By performing left-euclidean division in $\mathbb{F}_{q^r}[X, \sigma]$ (which is possible because $\mathbb{F}_{q^r}$ is perfect), we can find Q, which we factor again by Giesbrecht's algorithm. For each factorization we find, it takes as many uses of Giesbrecht's algorithm as factors there are in the polynomial. Since Giesbrecht's

algorithm is polynomial in the degree and in r, this quite naïve method gives all the factorizations of P with a complexity that is a polynomial in d and r times the number of factorizations of P.

Algorithm 2 AllFactorizations(P) returns all the factorizations of $P \in \mathbb{F}_{q^r}[X,\ \sigma]$

Input: $P \in \mathbb{F}_{q^r}[X,\ \sigma]$, monic
Output: List of all possible factorizations of P as product of monic irreducibles

```
Compute a factorization of P, P = P_1 ... P_s
if s = 1 then
  return [P]
else
  Let G be the companion matrix of P, compute a Jordan-Hölder sequence for the
  φ-module that has matrix G as in Proposition 4.2
  Let F_P = [ ]
  for each isomorphism class C of submodules of D_P do
    for x ∈ D_P such that the submodule generated by x is in C do
      Compute F = AllFactorizations(χ_{φ,x}^{-1} P)
      Add (χ_{φ,x}, F) to F_P, for all F ∈ F
    end for
  end for
  return F_P
end if
```

Note that the same kind of methods could also be used to find all the factorizations of a polynomial with prescribed orders of the similarity classes of the factors appearing in P, or of just some of them.

CHAPITRE III

UN ALGORITHME POUR LA RÉDUCTION DES ϕ-MODULES SUR $k(\!(u)\!)$

Dans ce chapitre, on étudie la catégorie des ϕ-modules sur $K = k(\!(u)\!)$, où k est un corps parfait de caractéristique $p > 0$. On appelle ϕ-module sur K la donnée d'un $k(\!(u)\!)$-espace vectoriel D de dimension finie muni d'un endomorphisme ϕ_D, semi-linéaire par rapport à un endomorphisme ϕ de $k(\!(u)\!)$, appelé endomorphisme de Frobenius. Un tel ϕ-module est dit *étale* si l'image de ϕ_D contient une base de D. Dans le cas le plus classique où $\phi(x) = x^p$ pour $x \in k(\!(u)\!)$, il est bien connu (voir **[Fon90]**, ainsi que l'introduction de cette thèse) que la catégorie des ϕ-modules sur $k(\!(u)\!)$ est équivalente à celle des $\mathbb{F}_p$-représentations de $G_K = \mathrm{Gal}(k(\!(u)\!)^{sep}/k(\!(u)\!))$, où $k(\!(u)\!)^{sep}$ désigne une clôture séparable de $k(\!(u)\!)$. Cette équivalence de catégories est une motivation importante pour l'étude des ϕ-modules sur $k(\!(u)\!)$, notamment dans une optique algorithmique ; en effet, un ϕ-module est donné par la matrice de ϕ_D dans une base, ce qui en fait un objet plus simple à manipuler que les représentations de G_K.

On se place ici dans un cadre un peu plus général que la théorie classique des ϕ-modules sur $k(\!(u)\!)$, en demandant que ϕ agisse sur k comme une puissance du Frobenius (éventuellement l'identité) et que $\phi(u) = u^b$ pour un entier $b \geq 2$. Dans ce cas, on note σ la restriction de ϕ à k. On démontre ici, généralisant le théorème principal de **[Car09a]**, un résultat de classification des objets simples de la catégorie des ϕ-modules sur $k(\!(u)\!)$ lorsque k est algébriquement clos (voir théorème 1.2.6) qui affirme que ce sont essentiellement les objets donnés par une matrice de la forme :

$$\begin{pmatrix} 0 & \cdots & 0 & \lambda u^s \\ 1 & \ddots & 0 & 0 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$

(avec une condition supplémentaire sur s et la dimension d, et avec $\lambda = 1$ si $\sigma \neq id$). On prouve de sucroît que les classes d'isomorphisme sont classifiées par les rationnels

$\frac{s}{b^d-1}$ (mod $\mathbb{Z}$), appelés *pentes*. En particulier, la semi-simplifiée d'un tel ϕ-module est déterminée par les pentes de ses quotients de Jordan-Hölder, que l'on appelle les pentes du ϕ-module. De ce théorème, on déduit l'existence (mais pas l'unicité) d'une filtration par les pentes lorsque k n'est pas nécessairement algébriquement clos (voir théorème 1.3.5). On réinterprète également les ϕ-modules et leurs pentes en termes de polynômes tordus et leurs polygones de Newton. On donne ensuite un algorithme de complexité $O(d^8\gamma^9)$ multiplications dans k (où d est la dimension et γ une constante liée aux diviseurs élémentaires de la matrice du ϕ-module) permettant de calculer explicitement une filtration par les pentes. La première difficulté pour analyser la complexité de cet algorithme est le fait que la manipulation algorithmique de séries formelles ne peut se faire qu'à une précision fixée, c'est-à-dire modulo une puissance fixée de u. En particulier, une grande partie de ce travail est consacrée à comprendre à quelle précision il est possible de tronquer les séries intervenant dans nos calculs sans perdre d'information sur notre objet de départ, et à contrôler les pertes de précision intervenant au gré des manipulations. Une autre difficulté majeure est le fait que le calcul dans des extensions du corps de base s'avère très coûteux en temps de calcul (notamment dans le cadre de ce travail, où les extensions considérées sont de degré *a priori* très grand), et une autre partie du travail algorithmique présenté ici est consacrée au contournement de ce problème.

Dans une première partie, on établit la classification précédente (qui généralise les résultats de [**Car09a**], où est traité le cas $k = \overline{\mathbb{F}}_p$). Cette classification nous permet d'établir le théorème de filtration par les pentes. Nous étudions également les ϕ-modules du point de vue des polynômes tordus, et on montre que les pentes d'un ϕ-module apparaissent aussi comme les pentes d'un polygone de Newton naturellement associé à ce ϕ-module, et qui est purement défini sur $k(\!(u)\!)$. La démonstration donnée pour la classification précédente donne un moyen assez explicite pour construire un sous-objet simple d'un ϕ-module donné. Cette démonstration est mise à contribution pour donner un algorithme de réduction.
Dans la deuxième partie, on se consacre à la description de l'algorithme de réduction. Nous établissons tout d'abord plusieurs lemmes traitant les problèmes liés au fait que les calculs sur machine ne se font qu'à précision finie, et qu'on ne peut donc travailler qu'avec des séries tronquées. Nous expliquons comment on peut se ramener à ne manipuler que des séries dont la valuation est suffisamment petite (c'est à dire, n'est pas exponentielle en la dimension) pour que la complexité des calculs demeure polynomiale. On présente ensuite l'algorithme proprement dit, dans les cas $\sigma \neq \mathrm{id}$ et $\sigma = \mathrm{id}$, qui sont sensiblement différents. En effet, dans le premier cas, calculer la réduction sur $\bar{k}(\!(u)\!)$ impose de faire des extensions de k dont le degré est exponentiel en la dimension du ϕ-module. Nous

montrons comment on peut calculer une réduction intéressante définie sur $k(\!(u)\!)$. Dans le deuxième cas, en revanche, on calcule une réduction définie sur $\bar{k}(\!(u)\!)$, car l'extension de k sur laquelle un ϕ-module peut être réduit sous une forme agréable n'est que de degré polynomial en la dimension du ϕ-module.
La troisième partie, assez brève, se consacre d'abord à l'étude détaillée du fonctionnement de l'algorithme sur un exemple, ainsi que de son application à un exemple naturel : si L est une extension finie de K, L a une structure naturelle de ϕ-module sur K. Nous choisissons un exemple de tel L et montrons comment la réduction précédente donne des informations sur L.

III.1. La catégorie des ϕ-modules sur $k(\!(u)\!)$

Soit $p > 0$ un nombre premier, et soit k un corps parfait de caractéristique p. On note $K = k(\!(u)\!)$ le corps des séries formelles à coefficients dans k. Soient σ une puissance du Frobenius sur k (éventuellement $\sigma = \mathrm{id}$), et $b > 1$ un entier. On munit K de l'endomorphisme ϕ défini par :

$$\phi\left(\sum_{n\in\mathbb{Z}} a_n u^n\right) = \sum_{n\in\mathbb{Z}} \sigma(a_n) u^{bn}.$$

1.1. Définition et premières propriétés. — On considère la catégorie des ϕ-modules $\mathrm{Mod}^{\phi}_{/K}$ dont les objets sont les K-espaces vectoriels D de dimension finie munis d'un endomorphisme ϕ-semi-linéaire $\phi_D : D \to D$. Les morphismes de $\mathrm{Mod}^{\phi}_{/K}$ sont les applications K-linéaires qui commutent avec ϕ_D. Nous allons étudier la sous-catégorie pleine des ϕ-modules étales $\mathrm{Mod}^{\phi}_{/K,\text{ét}}$, c'est à dire ceux pour lesquels l'image de l'application ϕ_D contient une base de D.
Pour le moment, nous souhaitons étudier les objets de cette catégorie, et en classifier les objets simples lorsque k est algébriquement clos. Cette étude a été initiée dans [**Car09a**] par Caruso, dont nous allons généraliser les résultats (qui donnent cette classification dans le cas pour le cas $k = \overline{\mathbb{F}}_p$). On rappelle ici la définition de certains objets de cette catégorie, ainsi que certaines de leurs propriétés.

Définition 1.1.1. — Soient $d \in \mathbb{N}^*$, $s \in \mathbb{Z}$, $\lambda \in k^\star$. On définit l'objet $D(d, s, \lambda)$ de $\mathrm{Mod}^{\phi}_{/\mathrm{K},\text{ét}}$ par :
- $D(d, s, \lambda) = Ke_1 \oplus Ke_2 \oplus \cdots \oplus Ke_d$;
- $\phi_D(e_i) = e_{i+1}$ pour $1 \leq i \leq d-1$;
- $\phi_D(e_d) = u^s \lambda e_1$.

On définit également $D(d, s) = D(d, s, 1)$.

À un ϕ-module D dont on a fixé une base $(e_1, \ldots, e_d)$ (en tant que K-espace vectoriel), on associe la matrice G de ϕ_D dans cette base, dont la i-ème colonne a pour coefficients les coordonnées de $\phi_D(e_i)$ dans cette base. En particulier, si $D = D(d, s, \lambda)$, la matrice G de ϕ_D dans la base $(e_1, \ldots, e_d)$ est la matrice carrée de taille d :

$$\begin{pmatrix} 0 & \cdots & 0 & \lambda u^s \\ 1 & \ddots & 0 & 0 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Notons par ailleurs que si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases de D, et si P est la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$, alors les matrices G et G' de ϕ_D dans les bases respectives $\mathcal{B}$ et $\mathcal{B}'$ sont liées par la relation $G' = P^{-1}G\phi(P)$, où l'écriture $\phi(P)$ indique que l'on a appliqué ϕ à chacun des coefficients de P. Ainsi, quitte à changer de base, on peut toujours supposer que le $k[\![u]\!]$-module engendré par les vecteurs de base est stable par ϕ_D, ce que nous ferons en général.

On suppose jusqu'à la fin de cette sous-partie que le corps k est algébriquement clos. Par ailleurs, lorsqu'il n'y a pas de confusion possible, on notera simplement ϕ à la place de ϕ_D.

Proposition 1.1.2. — *Soit (d, s, λ) avec $d \in \mathbb{N}^*$, $s \in \mathbb{Z}$, $\lambda \in k^\star$. On suppose qu'il existe $d' \in \mathbb{N}^*$ et $s' \in \mathbb{Z}$ tels que $t = \frac{d}{d'}$ soit un entier, et que $\frac{s}{b^d-1} = \frac{s'}{b^{d'}-1}$.*

(i) Si σ n'est pas l'identité, on a :

$$D(d, s, \lambda) \simeq D(d', s')^{\oplus t}.$$

(ii) Si σ est l'identité et si t est premier avec p, on a :

$$D(d, s, \lambda) \simeq D(d', s', \lambda'_1) \oplus D(d', s', \lambda'_2) \oplus \cdots \oplus D(d', s', \lambda'_t),$$

où les λ'_i sont les racines t-ièmes de λ.

(iii) Si σ est l'identité et $t = p$, il existe une suite croissante de sous-modules de $D(d, s, \lambda)$ stables par ϕ

$$0 = D_0 \subset D_1 \subset \cdots \subset D_p = D(d, s, \lambda)$$

pour laquelle tous les quotients D_m/D_{m-1} sont isomorphes à $D(d', s', \mu)$, μ étant l'unique racine p-ième de λ dans k.

Démonstration. — Les deux premiers points sont tout à fait semblables à la démonstration de la proposition 3 de [**Car09a**]. Démontrons l'assertion (iii). On note $r = \frac{s}{b^d-1} = \frac{s'}{b^{d'}-1}$ et μ l'unique racine p-ième de λ. Pour tous entiers $i \in \{1, \ldots, d'\}$ et $j \in \{0, \ldots, p-1\}$, on

pose :

$$f_{i,j} = \sum_{l=0}^{p-1} l^j \mu^{-s} u^{-rb^i(b^{ld'}-1)} e_{ld'+i},$$

et on définit D_m comme le sous-K-espace vectoriel de $D(d,s)$ engendré par les $f_{i,j}$ avec $1 \leq i \leq d'$ et $0 \leq j < m$. Un calcul de déterminant de Vandermonde montre que la famille des $f_{i,j}$ est libre, ce qui montre que la dimension de D_m sur K est md'. Par ailleurs, on a les relations $\phi(f_{i,m}) = f_{i+1,m}$ pour $i \in \{1, \ldots, d'-1\}$, et

$$\phi(f_{d',m}) = \mu u^{s'} \sum_{q=0}^{m} (-1)^{m-q} \binom{m}{q} f_{0,q} \equiv \mu u^{s'} f_{0,m} \pmod{D_{m-1}},$$

ce qui montre à la fois que D_m est stable par ϕ pour tout m, et que les quotients D_m/D_{m-1} sont tous isomorphes à $D(d', s', \mu)$. □

On note $\mathcal{R}_b$ l'ensemble quotient de $\mathbb{Z}_{(b)}$ (le localisé de $\mathbb{Z}$ en les puissances de b) par la relation d'équivalence :

$$x \sim y \Leftrightarrow (\exists l \in \mathbb{Z})\ x \equiv b^l y \pmod{\mathbb{Z}}.$$

Suivant [**Car09a**], pour $r = \frac{m}{t} \in \mathcal{R}_b$ (avec t premier avec b et $\frac{m}{t}$ irréductible), nous définissons $\ell(r)$ comme l'ordre de b modulo t (indépendant du choix du représentant irréductible). On note $\mathcal{N}(r)$ l'ensemble des entiers relatifs s pour lesquels $\frac{s}{b^{\ell(r)}-1}$ est un représentant de r. Les $D(\ell(r), s)$ pour $s \in \mathcal{N}(r)$ sont isomorphes entre eux, on note $D(r)$ un tel objet. Si σ est l'identité, on définit de même $D(r, \lambda) = D(\ell(r), s, \lambda)$ pour un s quelconque dans $\mathcal{N}(r)$. D'après le théorème 4 de [**Car09a**], dont la preuve se généralise immédiatement au cas k quelconque, les $D(r)$ (resp. $D(r, \lambda)$ si $\sigma = \mathrm{id}$) sont des objets simples de $\mathrm{Mod}^{\phi}_{/K,\text{ét}}$, deux à deux non isomorphes.

1.2. Classification des objets simples (k algébriquement clos). — On suppose que k est algébriquement clos. Dans cette partie, nous allons montrer que tout ϕ-module étale simple est isomorphe à un certain $D(r, \lambda)$. Dans la suite, nous noterons D un objet de la catégorie $\mathrm{Mod}^{\phi}_{/K,\text{ét}}$.

On étend naturellement l'application ϕ définie sur $k(\!(u)\!)$ en un automorphisme du corps $k\{\{u\}\}$ des séries de Puiseux en u à coefficients dans k.

Proposition 1.2.1. — *Soient $N \in \mathbb{N}^*$, $n_1, \dots, n_{N-1} \in \mathbb{N}$ et $\lambda_1, \dots, \lambda_N \in k(\!(u)\!)$ avec les λ_i non tous nuls. Pour tout $\mu \in k^\star$, on considère le système d'équations $(\mathcal{S}_\mu)$ suivant :*

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_1 \\ u^{n_1} & 0 & \cdots & 0 & \lambda_2 \\ 0 & u^{n_2} & \cdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & u^{n_{N-1}} & \lambda_N \end{pmatrix} \begin{pmatrix} \phi(\alpha_1) \\ \phi(\alpha_2) \\ \vdots \\ \vdots \\ \phi(\alpha_N) \end{pmatrix} = \mu \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_N \end{pmatrix}$$

Alors, il existe $j \in \{1, \dots, N\}$ tel que :

- *Si $\sigma \neq id$, $(\mathcal{S}_1)$ admet une solution non nulle avec $\alpha_1, \dots, \alpha_N \in k(\!(u^{\frac{1}{b^j-1}})\!)$;*
- *Si $\sigma = id$, il existe $\mu \in k^\star$ tel que $(\mathcal{S}_\mu)$ admette une solution non nulle avec $\alpha_1, \dots, \alpha_N \in k(\!(u^{\frac{1}{b^j-1}})\!)$.*

Démonstration. — Traitons d'abord le cas où $\sigma \neq id$, on fixe alors $\mu = 1$ et on s'intéresse au système $(\mathcal{S}_1)$. Supposons que l'on ait une solution donnée par $\alpha_1, \alpha_2, \dots, \alpha_N$ au système $(\mathcal{S}_1)$. Alors, partant de la première ligne du système $\alpha_1 = \lambda_1 \phi(\alpha_N)$ puis reportant ligne après ligne l'égalité obtenue dans la ligne suivante, on remarque que α_N doit être solution de l'équation

$$x = \sum_{j=0}^{N-1} \phi^j(\lambda_{N-j}) u^{b^{j-1} n_{N-j} + \cdots + n_{N-1}} \phi^{j+1}(x). \tag{1}$$

Pour $j \in \{1, \dots, N\}$, on note v_j la valuation u-adique de λ_j. On appelle J l'ensemble des entiers i dans $\{0, \dots, N-1\}$ tels que

$$\frac{b^i v_{N-i} + b^{i-1} n_{N-i} + \cdots + n_{N-1}}{b^{i+1} - 1} = \min_{j \mid \lambda_{N-j} \neq 0} \left\{ \frac{b^j v_{N-j} + b^{j-1} n_{N-j} + \cdots + n_{N-1}}{b^{j+1} - 1} \right\},$$

et soit $j_0 \in \{1, \dots, N\}$ tel que $j_0 - 1$ soit le plus petit élément de J. On note aussi $s = b^{j_0-1} v_{N-j_0+1} + b^{j_0-2} n_{N-j_0} + \cdots + n_{N-1}$.
Pour $j \in J$, on note $\lambda_j = u^{v_j}(\lambda_j^0 + \mu_j)$, avec $\lambda_j^0 \in k^\star$ et μ_j de valuation u-adique strictement positive. Soit alors α une solution non nulle de l'équation

$$\sum_{j \in J} \sigma^j(\lambda_{N-j}^0) \sigma^{j+1}(\alpha) = \alpha, \tag{2}$$

qui existe car σ est une puissance du Frobenius et $\sigma \neq id$. On cherche une solution à (1) sous la forme $x = u^{-\frac{s}{b^{j_0}-1}}(\alpha + y)$ avec $y \in k\{\{u\}\}$. Après quelques manipulations, on déduit

de (1) l'équation devant être vérifiée par y :

$$\begin{aligned} y &= \sum_{j\in J}\left[\phi^j(\mu_{N-j})\phi^{j+1}(\alpha+y)+\phi^j(\lambda^0_{N-j})\phi^{j+1}(y)\right] \\ &\quad + \sum_{\substack{0\le j\le N-1\\ j\notin J}} \sigma^j(\lambda_{N-j})u^{b^{j-1}n_{N-j}+\cdots+n_{N-1}-\frac{b^{j+1}-1}{b^{j_0-1}}s}(\phi^{j+1}(\alpha)+\phi^{j+1}(y)). \end{aligned} \tag{3}$$

Définissons par récurrence la suite $(y_i)_{i\in\mathbb{N}}$ par $y_0=0$, et pour $i\ge 0$,

$$\begin{aligned} y_{i+1} &= \sum_{j\in J}\left[\phi^j(\mu_{N-j})\phi^{j+1}(\alpha+y_i)+\phi^j(\lambda^0_{N-j})\phi^{j+1}(y_i)\right] \\ &\quad + \sum_{\substack{0\le j\le N-1\\ j\notin J}} \phi^j(\lambda_{N-j})u^{b^{j-1}n_{N-j}+\cdots+n_{N-1}-\frac{b^{j+1}-1}{b^{j_0-1}}s}(\phi^{j+1}(\alpha)+\phi^{j+1}(y_i)). \end{aligned}$$

On a alors pour $i\ge 2$,

$$\begin{aligned} y_{i+1}-y_i &= \sum_{j\in J}\phi^j(u^{-v_{N-j}}\lambda_{N-j})\phi^{j+1}(y_i-y_{i-1}) \\ &\quad + \sum_{\substack{0\le j\le N-1\\ j\notin J}} \phi^j(\lambda_{N-j})u^{b^{j-1}n_{N-j}+\cdots+n_{N-1}-\frac{b^{j+1}-1}{b^{j_0-1}}s}\phi^{j+1}(y_i-y_{i-1}). \end{aligned}$$

La valuation u-adique de y_1-y_0 étant strictement positive, la suite des valuations u-adiques de $y_{i+1}-y_i$ tend vers $+\infty$, ce qui prouve que la suite y_i converge dans $k\{\{u\}\}$. En notant y sa limite, on vérifie aisément que y est solution de l'équation (3) et par suite, en posant $x=u^{-\frac{s}{b^{j_0-1}}}(\alpha+y)$, que x est solution de (1). Il suffit alors de poser $\alpha_N=x$, $\alpha_1=\lambda_1u^Nx_N$, puis par récurrence, $\alpha_i=\phi(\alpha_{i-1})+\lambda_i\phi(\alpha_N)$ pour $2\le i\le N-1$, pour obtenir une solution non nulle au système.

Il nous reste à traiter le cas où $\sigma=id$. On ne suppose plus cette fois que $\mu=1$. Des calculs analogues aux précédents montrent que α_N doit être solution de l'équation :

$$x=\sum_{j=0}^{N-1}\frac{1}{\mu^{j+1}}\phi^j(\lambda_{N-j})u^{b^{j-1}n_{N-j}+\cdots+n_{N-1}}\phi^{j+1}(x). \tag{4}$$

On reprend les notations du cas $\sigma\neq id$ pour s,j_0,α^0_j et β_j. On choisit une solution μ de l'équation $\sum_{j\in J}\lambda^0_{N-j}\mu^{N-j-1}=1$, et on cherche une solution à (4) sous la forme $x=u^{-\frac{s}{b^{j_0-1}}}(1+y)$. On détermine et on résout l'équation devant être vérifiée par y de la même manière que dans le cas $\sigma\neq id$. □

Remarque 1.2.2. — Une récurrence permet de voir que, en gardant les notations de la proposition précédente, on a pour tout $i\ge 0$, $y_i\in\bigoplus_{j=0}^{j_0-1}u^{\theta_j}K$, avec pour $0\le j<j_0$,

$\theta_j = \frac{b^j s}{b^{j_0}-1}$. En effet, cela est clair pour y_0, et lorsque $f \in K$ et $l \in \mathbb{N}$, $\phi^l(u^{\theta_j} f) = u^{b^l \theta_j}\phi(f)$. En notant $l + j = j_0 n + m$ par division euclidienne par j_0 (avec $0 \leq m < j_0$), $b^{j+l}s = (b^{j_0 n} - 1)b^m s + b^m s$. Le premier terme de cette somme étant divisible par $b^{j_0} - 1$, $\frac{b^{l+j}s}{b^{j_0}-1} \in \theta_m + \mathbb{Z}$, ce qui montre que $\phi^l(u^{\theta_j} f) \in u^{\theta_m} K$. Il est ensuite facile de compléter la récurrence.

Remarque 1.2.3. — La proposition 1.2.1 est plus générale que l'usage que nous allons en faire dans l'immédiat, mais elle nous sera également utile dans la partie algorithmique. Nous réutiliserons souvent les notations de cette proposition, à laquelle nous ferons référence plusieurs fois dans la suite de cet article.

Proposition 1.2.4. — *Soit D un ϕ-module étale sur K. Alors, il existe $N \in \mathbb{N}$, $s \in \mathbb{Z}$, $\lambda \in k^\times$ et $x \in D$ non nul tels que $\phi^N(x) = \lambda u^s x$. Si de plus σ n'est pas l'identité, on peut choisir $\lambda = 1$.*

Démonstration. — Soit $y_1 \in D$. Pour $i \geq 0$, on pose $y_{i+1} = \phi^i(y_1)$. Soit N le plus petit entier tel que la famille $y_1, \ldots, y_N, y_{N+1}$ soit liée sur $k(\!(u)\!)$. Il existe alors $\lambda_1, \ldots, \lambda_N \in k(\!(u)\!)$ tels que $\phi(y_N) = \lambda_1 y_1 + \cdots + \lambda_N y_N$.

Fixons de tels $\lambda_1, \ldots, \lambda_N$. Soit $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{pmatrix}$ une solution non nulle de l'équation

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_1 \\ 1 & 0 & \cdots & 0 & \lambda_2 \\ 0 & 1 & \cdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & 1 & \lambda_N \end{pmatrix} \begin{pmatrix} \phi(\alpha_1) \\ \phi(\alpha_2) \\ \vdots \\ \vdots \\ \phi(\alpha_N) \end{pmatrix} = \mu \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_N \end{pmatrix}$$

comme dans la proposition 1.2.1 (on choisit en outre $\mu = 1$ si $\sigma \neq id$). Les α_i sont tous dans $k(\!(u^{\frac{1}{b^j-1}})\!)$. Soit $t : k(\!(u^{\frac{1}{b^j-1}})\!) \to k(\!(u)\!)$ l'application k-linéaire envoyant u^r sur u^r si r est entier, et sur 0 sinon. Comme $b^j - 1$ est premier avec b, cette application commute avec ϕ. Définissons maintenant :

$$x = t\left(u^{\frac{s}{b^j-1}}\alpha_1\right) y_1 + \cdots + t\left(u^{\frac{s}{b^j-1}}\alpha_N\right) y_N.$$

On a alors

$$\begin{aligned}\phi(x) &= t\left(u^{\frac{bs}{b^j-1}}(\phi(\alpha_1)+\lambda_2\phi(\alpha_N))\right)y_2\\ &\quad+\cdots+t\left(u^{\frac{bs}{b^j-1}}(\phi(\alpha_{N-1})+\lambda_N\phi(\alpha_N))\right)y_N+t\left(u^{\frac{bs}{b^j-1}}\lambda_1\phi(\alpha_N)\right)y_1\\ &= t\left(\mu u^{\frac{bs}{b^j-1}}\alpha_1\right)y_1+\cdots+t\left(\mu u^{\frac{bs}{b^j-1}}\alpha_N\right)y_N.\end{aligned}$$

En itérant les calculs, on voit que $\phi^j(x)=\mu^j u^s x$.

Il nous reste à vérifier que x est non nul. Cela découle du fait que la valuation u-adique de $u^{\frac{s}{b^j-1}}\alpha_N$ est nulle par construction, et donc que $t\left(u^{\frac{s}{b^j-1}}\alpha_N\right)\neq 0$, ce qui montre que $x\neq 0$ car la famille $y_1,\ldots,y_N$ est libre. □

Remarque 1.2.5. — Soit x une solution de l'équation précédente, construite à partir de $\xi=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_N\end{pmatrix}$. Alors on a :

$$\xi=u^{-\frac{s}{b^j-1}}x+\mu^{-1}u^{-\frac{bs}{b^j-1}}\phi(x)+\cdots+\mu^{-(j-1)}u^{-\frac{b^{j-1}s}{b^j-1}}\phi^{j-1}(x).$$

Théorème 1.2.6. — *Soit D un objet simple de $Mod^{\phi}_{/k((u)),ét}$.*

- *Si σ n'est pas l'identité, il existe $r\in\mathcal{R}_b$ tel que $D\simeq D(r)$.*
- *Si σ est l'identité, il existe $r\in\mathcal{R}_b$ et $a\in k^\star$ tel que $D\simeq D(r,a)$.*

Démonstration. — D'après la proposition 1.2.4, il existe des entiers $N\geq 0$, $s>0$, et $\lambda\in k^\star$ (λ étant égal à 1 si σ n'est pas l'identité) et un morphisme non nul de $D(N,s,\lambda)$ dans D. La simplicité de D assure que f est surjectif, donc que D se retrouve dans les constituants de Jordan-Hölder de $D(N,s,\lambda)$. On note $r=\frac{s}{b^N-1}$ sous la forme $r=\frac{n}{b^{\ell(r)}-1}$. On sait alors que $\ell(r)$ divise N.

Si σ n'est pas l'identité, $D(N,s,\lambda)$ est une somme directe de copies de $D(r)$. En particulier, les quotients de Jordan-Hölder sont tous isomorphes à $D(r)$, ce qui démontre le théorème dans ce cas.

Si σ est l'identité, notons $N=p^v t\ell(r)$, avec t non divisible par p. D'après la proposition 1.1.2 (en appliquant plusieurs fois le (iii)), $D(N,s,\lambda)$ admet une suite de composition dont les quotients sont tous isomorphes à des $D(p^{-v}N,s',\lambda')$ pour un certain entier n' et un $\lambda'\in k^\star$. Le (ii) de la même proposition montre alors que dans ce cas, les constituants de Jordan-Hölder sont tous isomorphes à des $D(r,a)$ pour certains $a\in k^\star$. On en déduit le théorème dans le cas où σ est l'identité. □

Une autre façon d'exprimer ce théorème est de dire qu'étant donné un ϕ-module étale D, il existe une unique famille $r_1, \ldots, r_n$ d'éléments de $\mathcal{R}_b$ (à l'ordre près), une famille $\lambda_1, \ldots, \lambda_n$ d'éléments de k, et une base de D (en tant que K-espace vectoriel) telle que la matrice de l'application ϕ dans cette base soit de la forme

$$\begin{pmatrix} \Delta_{r_1,\lambda_1} & (\star) & \cdots & (\star) \\ 0 & \Delta_{r_2,\lambda_2} & \ddots & (\star) \\ \vdots & \ddots & \ddots & (\star) \\ 0 & \cdots & 0 & \Delta_{r_n,\lambda_n} \end{pmatrix}$$

avec $\Delta_{r,\lambda} = \begin{pmatrix} 0 & \cdots & 0 & \lambda u^s \\ 1 & \ddots & 0 & 0 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}$ carrée de taille $\ell(r)$, si $r = \frac{s}{b^{\ell(r)}-1}$. Si $\sigma \neq id$, cela reste vrai même en prenant $\lambda_i = 1$ pour tout i. Par ailleurs, si $\sigma = \mathrm{id}$, les λ_i sont eux aussi uniquement déterminés.

Une première étape dans la caractérisation d'un ϕ-module est donc d'identifier les (r_i, λ_i) qui interviennent dans une telle décomposition. On appellera dans la suite *pentes* du ϕ-module D les r_i (ou, de manière équivalente, la donnée de $(s, \ell(r_i))$ ou celle des chiffres de l'écriture en base b de s tel que $r_i = \frac{s}{b^{\ell(r_i)-1}}$).

1.3. Filtration par les pentes (k quelconque). — On ne suppose plus désormais que k est algébriquement clos. Nous allons voir comment généraliser les résultats de la partie précédente. Une autre reformulation des résultats de cette partie est la suivante :

Corollaire 1.3.1. — *Soit D un ϕ-module étale sur $k(\!(u)\!)$. Si k est algébriquement clos, alors il existe une suite croissante de sous-ϕ-modules*

$$\{0\} = D_0 \subset D_1 \subset \cdots \subset D_n = D$$

telle que pour tout $1 \leq i \leq n$, il existe $r_i \in \mathcal{R}_b$ et $\lambda_i \in k^\times$ tels que le quotient D_i/D_{i-1} soit isomorphe à $D(r_i, \lambda_i)$.

C'est sous une forme analogue à l'énoncé de ce corollaire que nous allons donner une généralisation de ce qui précède. On ne suppose plus maintenant que k est algébriquement clos, mais seulement parfait.

Définition 1.3.2. — Soit D un ϕ-module sur $k(\!(u)\!)$. On dit que D est isocline de pente r s'il existe des $\lambda_i \in \bar{k}^\times$ tels que tous les quotients de Jordan-Hölder de $D \otimes_K \bar{k}(\!(u)\!)$ sont

isomorphes à l'un des $D(r, \lambda_i)$. Le ϕ-module D est dit isocline s'il existe $r \in \mathcal{R}_b$ tel que D soit isocline de pente r.

Lemme 1.3.3. — *Tout quotient et tout sous-objet d'un ϕ-module isocline de pente r est isocline de pente r.*
Toute extension d'un ϕ-module isocline de pente r par un ϕ-module isocline de même pente est isocline de pente r.

Démonstration. — Cela résulte immédiatement du fait que si on a une suite exacte $0 \to D' \to D \to D'' \to 0$, alors l'ensemble des quotients de Jordan-Hölder de D la réunion de l'ensemble de ceux de D' et ceux de D''. □

Lemme 1.3.4. — *Soit D un ϕ-module simple sur $k(\!(u)\!)$. Alors D est isocline.*

Démonstration. — On suppose que D est simple. Il existe une extension finie k' de k telle que les constituants de Jordan-Hölder de D sur $k'(\!(u)\!)$ soient simples sur $\bar{k}(\!(u)\!)$. On fixe un tel k', et on pose $\tilde{D} = D \otimes_K k'(\!(u)\!)$. Soit $D' \subset \tilde{D}$ un sous-ϕ-module simple sur $k'(\!(u)\!)$. Soit $G = \mathrm{Gal}(k'/k)$, le groupe G agit naturellement sur $\tilde{D}$, et on pose $\tilde{D}' = \sum_{g \in G} gD'$. Tous les gD' pour $g \in G$ sont isoclines de même pente que D, donc $\tilde{D}'$ l'est aussi. Comme $\tilde{D}'$ est stable par G, il admet d'après Hilbert 90 une base formée de vecteurs fixes par G. On a donc $(\tilde{D}')^G \subset D$, et par simplicité de D, $D = (\tilde{D}')^G$. En tant que sous-ϕ-module d'un ϕ-module isocline, D est isocline. □

***Théorème 1.3.5* (Filtration par les pentes)**. — *Soit D un ϕ-module sur k. Alors il existe une filtration par des sous-ϕ-modules*

$$\{0\} = D_0 \subset D_1 \subset \cdots \subset D_n = D$$

telle que pour tout $1 \leq i \leq n$, le quotient D_i/D_{i-1} soit isocline.

Démonstration. — Une suite de Jordan-Hölder de D fournit une telle filtration d'après le lemme 1.3.4. □

Remarque 1.3.6. — Une filtration par les pentes n'est pas unique en général, de même que les quotients d'une telle filtration ne sont pas uniquement déterminés.

Remarque 1.3.7. — Contrairement au cas de la théorie de Dieudonné-Manin, il peut exister des extensions non triviales entre deux ϕ-modules isoclines de pentes différentes. Par exemple (on suppose k algébriquement clos), si on note $D_1 = D(1, -1)$ et $D_2 = D(1, 0)$, ces deux ϕ-modules sont isoclines de pentes distinctes, et le ϕ-module D sur lequel la matrice de ϕ est donnée dans une base par $\begin{pmatrix} u^{-1} & 1 \\ 0 & 1 \end{pmatrix}$ est une extension de D_2 par D_1. Si la somme

était directe, D contiendrait un sous-ϕ-module isomorphe à D_2, et il y aurait dans D une solution non nulle à l'équation $\phi(x) = x$. Notant α, β les coordonnées de cette solution dans la base précédente, on aurait $\phi(\beta) = \beta$ et $u^{-1}\phi(\alpha) + \beta = \alpha$. On élimine d'abord le cas $\beta = 0$, ce qui impose $v(\beta) = 0$. On examine ensuite les valuations possibles pour α selon le signe de $bv(\alpha) - 1$, et on en conclut que cette équation n'a pas de solution non nulle.

Bien qu'une filtration par les pentes soit moins précise qu'une suite de Jordan-Hölder, l'intérêt d'une telle filtration est qu'elle est plus facile à obtenir algorithmiquement. De plus, du côté des représentations galoisiennes, les pentes d'un ϕ-module suffisent à donner les poids de l'inertie modérée de la représentation qui lui est associée, comme nous le verrons au chapitre IV.

1.4. Polynômes tordus et polygône de Newton. — Comme on l'a vu au chapitre I de cette thèse, un ϕ-module sur K peut être vu comme un module sur l'anneau des polynômes tordus $K[X, \phi]$. Cet anneau est l'anneau des polynômes à coefficients dans K, muni de son addition usuelle, la multiplication étant donnée par $X \cdot a = \phi(a)X$ lorsque $a \in K$. Le but de cette partie est de montrer que les pentes d'un ϕ-module s'interprètent comme les pentes d'un polygône de Newton.

1.4.1. Polynômes tordus et polynômes linéarisés sur $k(\!(u)\!)$: le cas classique. — Dans cette sous-partie, $\sigma = (x \mapsto x^q)$ et $b = q$, de sorte que pour $x \in k(\!(u)\!)$, $\phi(x) = x^q$. On considère l'anneau des polynômes tordus sur $K = k(\!(u)\!)$, noté $K[X, \phi]$.
Par ailleurs, on considère l'anneau des polynômes linéarisés à coefficients dans K : ce sont les polynômes de la forme $P(X) = \sum_{i=0}^{d} a_i X^{q^i}$, $a_i \in K$, sur lesquels l'addition est l'addition habituelle, et la multiplication est la composition. Il y a un isomorphisme d'anneaux naturel entre l'anneau des polynômes linéarisés et l'anneau des polynômes tordus, qui est donné par $P = \sum_{i=0}^{d} a_i X^i \in K[X, \phi] \mapsto L_P = \sum_{i=0}^{d} a_i X^{q^i}$. Remarquons au passage que les racines d'un polynôme linéarisé dans K^{sep} forment un $\mathbb{F}_q$-espace vectoriel dont la dimension est le degré du polynôme tordu associé.
Soient P un polynôme tordu et L_P le polynôme linéarisé associé. On note V_P le $\mathbb{F}_q$-espace vectoriel des racines de L_P. Cet espace est muni d'une filtration naturelle $(V_{P,v})_{v \in \mathbb{R}}$ définie par $V_{P,v} = \{x \in V_P \ / \ v(x) \geq v\}$. On note aussi $V_{P,v^+} = \{x \in V_P \ / \ v(x) > v\}$.

Définition 1.4.1. — Soit $P \in K[X, \phi]$. On dit que $v \in \mathbb{R}$ est une *pente* de P de multiplicité μ lorsque $\dim_{\mathbb{F}_q} \left(V_{P,v}/V_{P,v^+}\right) = \mu > 0$. On appelle *pentes caractéristiques* de P les pentes de P (comptées avec multiplicité), modulo la relation d'équivalence $v \sim v' \Leftrightarrow \exists m, n \in \mathbb{Z}$ tels que $p^m v \equiv p^n v' \pmod{\mathbb{Z}}$.

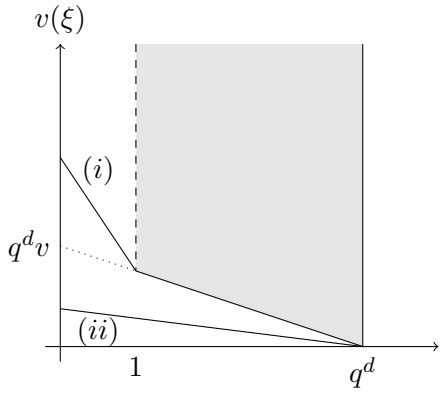
D'après la théorie classique du polygone de Newton, les pentes de P sont les opposés des pentes du polygone de Newton de L_P. La relation d'équivalence définissant les pentes caractéristiques est la même que celle qui définit l'équivalence entre pentes de ϕ-modules.

Lemme 1.4.2. — *Soit $P \in K[X, \phi]$ irréductible. Alors P a une seule pente.*

Démonstration. — On note $d = \deg P$. Supposons que P ait plusieurs pentes. Alors la filtration $V_{P,v}$ n'est pas constante, et il existe donc $v \in \mathbb{R}$ tel que $0 < \dim(V_{P,v}/V_{P,v^+}) < d$. Soit $L = \prod_{\xi \in V_{P,v}}(X - \xi)$ (le produit est pris au sens classique sur $K[X]$). Comme $V_{P,v}$ est un $\mathbb{F}_q$-espace vectoriel stable par G_K (puisque l'action de G_K préserve la valuation et que la somme de deux éléments de K^{sep} de valuation $\geq v$ est encore de valuation $\geq v$), L est un polynôme linéarisé (), associé à un polynôme tordu Q. Par ailleurs, il divise L_P au sens classique. Cela implique, via le lemme 3.1.1 de [**LB11a**]) qu'il divise L_P au sens des polynômes linéarisés, et donc que Q divise P, puis que P est réductible. □

Lemme 1.4.3. — *Soient $P, Q \in K[X, \phi]$. Alors les pentes caractéristiques de PQ (avec multiplicité) sont constituées de la réunion de celles de P et Q (avec multiplicité).*

Démonstration. — Par factorisation et récurrence, on peut supposer que Q est unitaire et a une seule pente. Notons $d = \deg Q$ et v la valeur de l'unique pente de Q (qui est donc de multiplicité d). On écrit $L_{PQ} = L_P \circ L_Q = \prod_{\xi \in V_P}(L_Q - \xi)$. Soit ξ une racine de L_P, on considère le polynôme $L_Q - \xi$. Son polygone de Newton a l'allure suivante (la partie grisée est le polygone de Newton de L_Q) :



On a représenté sur le dessin les deux cas possibles :

(i) si $v(\xi) > q^d v$, alors le polygone de Newton de $L_Q - \xi$ a deux pentes, l'une étant $-v$ et l'autre $-v(\xi) + (q^d - 1)v$;

(ii) si $v(\xi) \leq q^d v$, alors le polygone de Newton de $L_Q - \xi$ a une seule pente, égale à $-v(\xi)/q^d$.

Ainsi, dans le cas (i), $L_Q - \xi$ a dans K^{sep} une racine de valuation $v(\xi) - (q^d - 1)v$, et $q^d - 1$ racines de valuation v (comptées avec multiplicités). Dans le cas (ii), il a q^d racines de valuation $v(\xi)/q^d$.

Comptons maintenant le nombre de racines de L_{PQ} de valuation μ donnée. Si $\mu > v$, il y a une racine de L_{PQ} de valuation μ pour chaque racine de L_P de valuation $\mu + (q^d - 1)v$. Si $\mu = v$, il y a $(q^d - 1)$ racines de L_{PQ} de valuation μ pour chaque racine de L_P de valuation $> q^d v$, et q^d pour chaque racine de L_P de valuation $\leq q^d v$. Enfin, si $\mu < v$, il y a q^d racines de L_{PQ} de valuation μ pour chaque racine de L_P de valuation $q^d\mu$. Si on note m_μ la multiplicité de $\mu \in \mathbb{R}$ comme pente de P (éventuellement, $m_\mu = 0$), on voit que si $\mu > v$, L_{PQ} a exactement $q^{m_{\mu+(q^d-1)v}}$ racines de valuation $\geq \mu$. Si $\mu = v$, L_{PQ} a exactement $(q^d - 1)q^{m_{q^d v^+}} + q^d(q^{m_{q^d v}} - q^{m_{q^d v^+}}) + q^{m_{(v+(q^d-1)v)^+}} = q^{d+m_{q^d v}}$ racines de valuation $\geq \mu$. Enfin, si $\mu < v$, L_{PQ} a exactement $q^d q^{m_{q^d \mu}}$ racines de valuation $\geq \mu$. En conséquence, les pentes de PQ sont les μ_0/q^d pour μ_0 pente de P inférieure à $q^d v$ (avec multiplicité $d + m_{\mu_0}$), v (avec multiplicité $d + m_v$) et les $\mu_0 - (q^d - 1)v$ pour μ_0 pente de P supérieure strictement à $q^d v$ (avec multiplicité m_{μ_0}).

Il nous reste à remarquer que $\mu_0 \sim \mu_0/q^d$ et $\mu_0 - (q^d - 1)v \sim \mu_0$ pour terminer la démonstration. La première affirmation est claire. La deuxième découle du fait que $v = \frac{v(a_0)}{q^d-1}$, où a_0 est le coefficient constant de Q et donc $(q^d - 1)v \in \mathbb{Z}$. □

Proposition 1.4.4. — *Soit $P \in K[X, \phi]$. Soit $P = cP_1 \cdots P_s$ une factorisation de P comme produit de polynômes irréductibles unitaires P_i et d'une constante $c \in K$. Alors l'ensemble des pentes caractéristiques de P (avec multiplicité) est la réunion des ensembles des pentes caractéristiques des P_i (avec multiplicité), $1 \leq i \leq s$.*

Démonstration. — Le fait que les pentes de $P_1 \cdots P_s$ avec multiplicités soient celles des P_i résulte directement par récurrence du lemme 1.4.3, en utilisant le fait que les P_i ont une seule pente d'après le lemme 1.4.2. La proposition est donc vraie parce que la multiplication de P par une constante ne change pas le polygone de Newton de L_P. □

1.4.2. Cas général. — Dans cette sous-partie, $\sigma(a) = a^q$ lorsque $a \in k$, et $b \geq 2$ est un entier quelconque : on a donc $\phi(\sum a_i u^i) = \sum \sigma(a_i) u^{bi}$. On définit encore les pentes d'un polynôme dans $K[X, \phi]$, et on montre que ces pentes (modulo la relation d'équivalence convenable) sont les pentes des facteurs irréductibles du polynôme, comptées avec multiplicité. On suppose que le sous-corps de k fixé par σ est le corps à q éléments $\mathbb{F}_q$ (c'est à dire que $\mathbb{F}_q \subset k$).

Définition 1.4.5. — Soit $P \in K[X, \phi]$, $P = \sum_{i=0}^{d} a_i X^i$, on appelle *polygone de Newton* de P l'enveloppe convexe des points de coordonnées $(b^i, v(a_i))$ et d'un point à l'infini en

direction des ordonnées positives. Les *pentes* de P sont les pentes du polygone de Newton de P, la multiplicité d'une pente étant $i_1 - i_0$ si les extrémités du côté correspondant du polygone de Newton ont pour abscisses b^{i_0}, b^{i_1} (avec $i_0 \leq i_1$). Enfin, on appelle *pentes caractéristiques* de P l'ensemble des pentes de P, comptées avec multiplicités, modulo la relation d'équivalence $x \sim y \leftrightarrow \exists m, n \in \mathbb{Z}$ tels que $b^m x - b^n y \in \mathbb{Z}$.

Nous voulons comme précédemment montrer que les pentes d'un produit sont constituées de la réunion des pentes des facteurs (avec multiplicités). On ne dispose pas, comme dans le cas précédent, d'une théorie agréable reliant représentations et ϕ-modules, ce qui fait que l'on doit adapter les raisonnements à notre cadre. Si $P \in K[X, \phi]$, on note L_P l'application définie sur K^{sep}, définie par $L_P(x) = P(\phi)(x)$. Si $\xi \in K$, on définit le polygone de Newton de $L_P - \xi$ comme étant l'enveloppe convexe du polygone de Newton de P et du point de coordonnées $(0, v(\xi))$, les multiplicités étant définies comme avant. Par abus de notation, on considèrera même L_P pour $P \in K^{sep}[X, \phi]$.

On suppose que k est algébriquement clos : on voit tout de suite que, vu que nous nous intéressons aux pentes, nous pouvons faire cette hypothèse, car les pentes d'un polynôme ne changent pas par extension des scalaires à $\bar{k}(\!(u)\!)$. On remarque que les solutions d'une équation de la forme $L_P(x) = \xi$ forment un $\mathbb{F}_q$-espace affine, car la différence de deux d'entre elles est une solution de $L_P(x) = 0$, et les solutions de cette équation forment un sous-$\mathbb{F}_q$-espace vectoriel de K^{sep} car ϕ est $\mathbb{F}_q$-linéaire. On note

$$H_k = \left\{ \sum_{i \in I} a_i u^i \ / \ I \subset \mathbb{Q}, I \text{ est un ensemble bien ordonné}, a_i \in k \right\}.$$

Si $x = \sum_{i \in I} a_i u^i \in H_k$, on appelle *support* de x l'ensemble des $i \in I$ tels que $a_i \neq 0$. On remarque que H_k est un K-espace vectoriel, auquel ϕ et la valuation v s'étendent naturellement. Si le support de x est discret, alors la multiplication par x est bien définie dans H_k. On note $H_k[\phi] = \{\sum_{i=0}^d x_i \phi^i \ / \ x_i \in H_k\}$ (ce sont des sommes formelles, et par convention $\phi^0 = 1$). On définit le polygone de Newton d'un élément de $H_k[\phi]$ de la même manière que le polygone de Newton d'un élément de $K[X, \phi]$. Si l'on se donne $L = \sum_{i=0}^d x_i \phi^i \in H_k[\phi]$ dont tous les coefficients sont à support discret, cela a un sens de calculer $L(x) = \sum_{i=0}^d x_i \phi^i(x)$ pour $x \in H_k$. Enfin, on note H_k^+ (resp. H_k^{++}) l'ensemble des éléments de H_k dont le support est constitué d'éléments de valuation ≥ 0 (resp. > 0).

Lemme 1.4.6. — *Soient $P \in K[X, \phi]$ et $\xi \in K$. On suppose que le coefficient constant de P est non nul. Alors les pentes du polygone de Newton de $L_P - \xi$ sont les valuations des solutions non nulles $x \in H_k$ de l'équation $L_P(x) = \xi$. De plus, si $v_0 \in \mathbb{Q}$, la somme des*

multiplicités des pentes $\leq -v_0$ est égale à la dimension du $\mathbb{F}_q$-espace affine des solutions de l'équation dont la valuation est $\geq v_0$.

Démonstration. — Pour $L = \sum_{i=0}^{d} a_i \phi^i \in H_k[\phi]$, et $v \in \mathbb{Q}$, on définit $L_v = u^w \sum_{i=0}^{d} a_i u^{b^i v} \phi^i$, où $w \in \mathbb{Q}$ est choisi de sorte que tous les coefficients de Q_v soient de valuation positive ou nulle, et que l'un d'entre eux au moins soit de valuation nulle. On vérifie facilement que $\{$Pentes du polygone de Newton de $L_v\} = \{$Pentes du polygone de Newton de $L\} - v$, en comptant les multiplicités. Remarquons enfin que si les coefficients de L sont à support discret, alors ceux de L_v le sont aussi, et que cela a donc un sens de calculer $L_v(x)$ pour $x \in H_k$.

On note $L = L_P(\phi) - \xi \in H_k[\phi]$: tous les coefficients de L sont à support discret. On fixe $v_0 \in \mathbb{Q}$ tel que $-v_0$ soit une pente du polygone de Newton de P. Nous allons montrer que pour tout ordinal α, il existe $v_\alpha \in \mathbb{Q} \cup \{+\infty\}$, $x_\alpha \in H_k$, tels que :

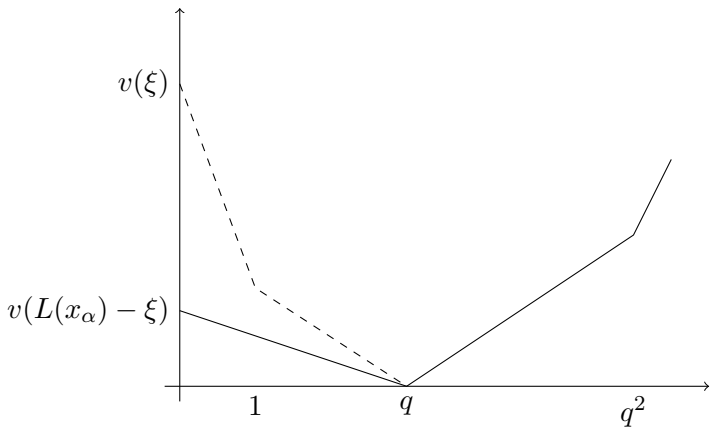
- pour tout ordinal $\beta < \alpha$, $v_\alpha > v_\beta$ et $v(x_\alpha - x_\beta) > v_\beta$;
- le polygone de Newton de $L - L(x_\alpha)$ a une pente $< -v_\alpha$ (éventuellement égale si $v_\alpha = +\infty$).

Nous en déduirons par induction transfinie que l'équation $L(x) = 0$ admet une solution $x \in H_k$ de valuation v_0, et nous compterons le nombre de solutions de cette équation ayant pour valuation v_0.

On pose $L_0 = L_{-v_0}$. Comme $-v_0$ est une pente du polygone de Newton de L, L_0 a au moins deux coefficients de valuation nulle. On considère $\bar{L}_0 = L \pmod{H_k^+}$. On a $\bar{L}_0 \in k[\sigma]$, $\bar{L}_0 = \sum_{i=s}^{t} \lambda_i \sigma^i$, avec $s < t$, $\lambda_s, \lambda_t \neq 0$. Soit ξ_0 une racine de $\bar{L}_0$ dans k. Nous remarquons au passage que le nombre de telles racines est q^{t-s} car k est algébriquement clos. On pose maintenant $x_0 = u^{-v_0}\xi_0$. Par construction, $L_0(\xi_0)$ est de valuation > 0, donc le polygone de Newton de $L - L(x_0)$ a une pente de valuation $< -v_0$. Soit maintenant α un ordinal, et supposons construits x_β, v_β vérifiant l'hypothèse d'induction pour $\beta < \alpha$. On note $x_{\beta^+} = \lim_{\beta<\alpha} x_\beta$: cela a un sens grâce à la première hypothèse. Soit $v_{\beta^+} = \sup_{\beta<\alpha} v_\beta$, alors le polygone de Newton de $L - L(x_{\beta^+})$ a une pente $\leq -v_{\beta^+}$ éventuellement égale à $-\infty$ (puisqu'il a une pente $< -v_\beta$ pour tout $\beta < \alpha$). Si cette pente est $-\infty$, il suffit de choisir $x_\alpha = x_{\beta^+}$ et $v_\alpha = +\infty$, car le coefficient constant de $L - L(x_\alpha)$ est alors nul. Sinon, soit $v_\alpha \in \mathbb{Q}$ tel que $-v_\alpha \leq -v_{\beta^+}$ soit une pente du polygone de Newton de $L_{\beta^+} = L - L(x_{\beta^+})$, et considérons $L_\alpha = (L_{\beta^+})_{v_\alpha}$. On sait alors que L_α se réduit modulo H_k^{++} sur un élément $\bar{L}_\alpha \in k[\sigma]$ ayant au moins deux coefficients non nuls. On fixe alors une racine ξ_α de ce polynôme, et par construction $L_\alpha(\xi_\alpha)$ est de valuation > 0, ce qui comme précédemment montre qu'en posant $x_\alpha = x_{\beta^+} + u^{v_\alpha}\xi_\alpha$, le polygone de Newton de $L - L(x_\alpha)$ a une pente $< -v_\alpha$. Si les v_α étaient tous des rationnels, alors ils formeraient une suite strictement

croissante de nombres réels indexée par tous les ordinaux, ce qui n'est pas possible. Par induction transfinie, il existe un ordinal α tel que le polygone de Newton de $L - L(x_\alpha)$ a un coefficient constant nul, c'est à dire précisément que $P(\phi)(x_\alpha) = \xi$. D'autre part, par construction, $v(x_\alpha) = v_0$.

Il nous reste à dénombrer les solutions de notre équation dans H_k. Il est déjà clair que les solutions de l'équation $L(x) = 0$ ont pour valuations des opposés de pentes du polygone de Newton de L, car si x est solution et a pour valuation $v \in \mathbb{Q}$, alors $L_{-v} = 0$ doit avoir une solution non nulle modulo H_k^{++}, ce qui signifie exactement que $-v$ est une pente du polygone de Newton de L. De la même manière, on voit que toute solution se construit de la manière décrite dans l'induction précédente, dont nous gardons les notations. Il nous reste donc à compter le nombre de solutions que l'on peut construire de cette façon. Le polygone de Newton de $L - L(x_\alpha)$ a l'allure suivante :



La partie en pointillés représente le polygone de Newton de L. On procède par récurrence sur le nombre ν de pentes finies du polygone de Newton de L_P (et non de L) qui sont $\leq -v_0$. Si $\nu = 0$, alors $-v_0$ est la plus petite pente du polygone de Newton de L, elle est de multiplicité 1 car le coefficient constant de P est non nul, et l'équation à résoudre à chaque étape de l'induction transfinie n'admet qu'une solution car elle est de la forme $\bar{x}^q = a$. Ainsi, l'équation $L(x) = 0$ n'admet qu'une solution. Supposons le résultat acquis pour un certain entier $\nu \geq 0$. On suppose que le polygone de Newton de L_P a $\nu + 1$ pentes finies qui sont $\leq -v_0$. L'équation modulaire $\bar{L}_0(\xi_0) = 0$ admet exactement q^{t-s} solutions, où q^t, q^s sont les abscisses des extrémités du segment correspondant à la pente $-v_0$ dans le polygone de Newton de L. On construit la famille (x_α) comme précédemment, ξ_0 étant fixé. Si $-v_0$ est une pente du polygone de Newton de L_P, alors ce polygone a au plus ν pentes qui sont $< -v_0$, et donc par hypothèse de récurrence, le nombre de solutions dans H_k de l'équation $L(x) - L(x_0) = 0$ dont la valuation est $> v_0$ est q^s. Par ailleurs, si $-v_0$ n'est pas une pente du polygone de Newton de L_P, alors $-v_0$ est la plus petite pente du polygone de Newton

de L, et l'équation $\bar{L}_0(\xi_0)$ a une seule solution. Dans ce cas, notons α le plus petit ordinal tel que l'équation résiduelle associée à $L - L(x_\alpha)$ ait plusieurs solutions. Les pentes du polygone de Newton de $L - L(x_\alpha)$ dont la pente est $< -v_0$ sont certaines pentes de L_P (en nombre non nul) et éventuellement une autre pente. Soit $-v$ la plus grande pente du polygone de Newton de L_P apparaissant dans ce polygone de Newton et inférieure à $-v_0$, le même raisonnnement que celui fait dans le cas où v_0 est une pente du polygone de Newton de L_P montre que le nombre de solutions de valuation $> v$ à l'équation $L(x) - L(x_\alpha) = 0$ est q^{m_v}, où q^{m_v} est l'abscisse de l'extrémité gauche du côté de pente $-v$ du polygone de Newton de L_P, et donc que le nombre de solutions de valuation $\geq v$ de cette équation est $q^{s-m_v}q^{m_v}$. Ainsi, l'équation $L(x) = 0$ a $q^s q^{t-s} = q^t$ solutions de valuation $\geq v_0$, ce qui termine la démonstration. □

Nous pouvons maintenant démontrer l'analogue du lemme 1.4.3 dans le cas général.

Lemme 1.4.7. — *Soient $P, Q \in K[X,\ \phi]$. Alors les pentes caractéristiques de PQ comptées avec multiplicités sont constituées de la réunion des pentes caractéristiques de P avec multiplicités et des pentes caractéristiques de Q avec multiplicités.*

Démonstration. — Si on suppose d'abord que Q a une seule pente, l'idée de la preuve est la même que dans le cas où $\phi(x) = x^q$. On note $L_P = P(\phi)$, $L_Q = Q(\phi)$. Remarquons d'abord que d'après le lemme 1.4.6, $x \in H_k$ vérifie $L_P(L_Q(x)) = 0$ si et seulement s'il existe $\xi \in H_k$ tel que $L_P(\xi) = 0$ et $L_Q(x) = \xi$. En fixant ξ solution de l'équation $L_P = 0$, et en examinant l'équation $L_Q(x) = \xi$, on peut calquer la démonstration du lemme 1.4.3 pour compter le nombre de solutions de cette équation. Le résultat en découle de la même manière. On peut alors en déduire le cas où Q a un nombre quelconque de pentes par récurrence sur ce nombre. □

Corollaire 1.4.8. — *Soit $P \in K[X, \phi]$ unitaire. Les pentes caractéristiques du polygone de Newton de P, comptées avec multiplicités, sont les mêmes que les pentes du ϕ-module associé à P.*

Corollaire 1.4.9. — *Soit D un ϕ-module étale sur K. Alors les pentes de D (avec multiplicités) ne dépendent pas de la façon dont on prolonge σ à $\overline{k}$.*

Démonstration. — Soit $x \in D$. On suppose que D est de dimension d sur K et que la famille $(x, \phi(x), \ldots, \phi^{d-1}(x))$ est une base de D (un tel x existe toujours). On écrit $\phi^d(x) = \sum_{i=0}^{d-1} \lambda_i \phi^i(x)$. Cette écriture est unique, et les pentes de D sont les pentes du polygone de Newton du polynôme tordu $X^d - \sum_{i=0}^{d-1} \lambda_i X^i$. Elles ne dépendent donc que de l'action de σ sur k, et non de la façon dont on choisit de la prolonger à $\overline{k}$ pour le calcul des pentes de $D \otimes_K \overline{k}(\!(u)\!)$. □

Remarque 1.4.10. — Ce résultat est surtout intéressant lorsque σ agit comme l'identité, car on peut calculer les pentes d'un ϕ-module indifféremment en prolongeant σ comme l'identité ou comme un Frobenius. On verra plus tard que les algorithmes proposés sont sensiblement différents dans ces deux cas.

III.2. Algorithme de réduction des ϕ-modules

Dans la suite, nous noterons D un objet de la catégorie $\mathrm{Mod}^{\phi}_{/K,\text{ét}}$, $(e_1, \ldots, e_d)$ une base, et $\mathfrak{D}$ le sous-k⟦u⟧-module engendré par les vecteurs de base. Nous supposons que $\mathfrak{D}$ est stable par ϕ. Nous noterons également G la matrice de ϕ dans la base $(e_1, \ldots, e_d)$. L'hypothèse de stabilité sur $\mathfrak{D}$ implique que G est à coefficients dans $k[\![u]\!]$. Nous noterons alors $0 \leq \gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_d = \gamma$ les valuations u-adiques des facteurs invariants de G. Le but de cette partie est de présenter un algorithme calculant une filtration par les pentes pour D. On suppose dans cette partie que $\sigma \neq id$.

2.1. Présentation générale de l'algorithme. —

2.1.1. Préliminaires. — L'idée de départ est de fixer $x \in D$ et de calculer le sous-ϕ-module de D engendré par x. On identifiera ensuite dans ce sous-ϕ-module un sous-ϕ-module isocline. Pour éviter l'explosion des valuations des coefficients apparaissant dans $x, \phi(x), \phi^2(x), \ldots$ (qui forment une famille génératrice du ϕ-module engendré par x), on va plutôt considérer la suite des itérés réduits de x, que l'on définit maintenant.

Définition 2.1.1. — Soit $x \in \mathfrak{D}$ tel que $x \notin u\mathfrak{D}$. On appelle respectivement *suite des itérés réduits* de x (notée $(x_i)_{i\geq 1}$) et *suite des exposants réducteurs* de x, (notée $(n_i)_{i\geq 1}$) les suites définies par récurrence par :

- $x_1 = x$,
- $\forall i \geq 1$, $n_i = \sup\{n \in \mathbb{N} \ / \ u^{-n}\phi(x_i) \in \mathfrak{D}\}$,
- $\forall i \geq 1$, $x_{i+1} = u^{-n_i}\phi(x_i)$.

Remarquons que ces suites sont construites de telle sorte que pour tout $i \geq 1$, $x_i \in \mathfrak{D} \backslash u\mathfrak{D}$.

Lemme 2.1.2. — *Soit $x \in \mathfrak{D} \setminus u\mathfrak{D}$, et soit $(n_i)_{i\geq 1}$ la suite des exposants réducteurs de x. Alors pour tout $i \geq 1$, $n_i \leq \gamma$.*

Démonstration. — Il suffit naturellement de prouver que si $x \in \mathfrak{D} \setminus u\mathfrak{D}$, alors $\phi(x) \notin u^{\gamma+1}\mathfrak{D}$. Par définition des facteurs invariants, il existe $H \in \mathcal{M}_d(k[\![u]\!])$ telle que $HG = u^{\gamma} I_d$. En particulier, si X est le vecteur colonne de x dans la base $(e_1, \ldots, e_d)$, on sait d'une part que l'un des coefficients de ce vecteur est de valuation u-adique nulle, et d'autre part que

les coordonnées de $\phi(x)$ dans cette base sont données par $G\phi(X)$. Ainsi, $HG\phi(X)$ est un vecteur à coefficients dans $u^\gamma k[\![u]\!]$, dont l'un au moins est de valuation γ. Il en résulte que l'un des coefficients de $G\phi(X)$ est de valuation $\leq \gamma$, c'est-à-dire que $\phi(x) \notin u^{\gamma+1}\mathfrak{D}$. □

Comme tous les calculs que nous effectuons en pratique se font à précision finie (c'est à dire modulo u^n pour un certain n qu'il faut fixer au préalable), nous devons comprendre quel est l'objectif à atteindre en termes de précision des calculs.

Lemme 2.1.3. — *Soit v un entier strictement supérieur à $\frac{b\gamma}{b-1}$ et H une matrice à coefficients dans $k[\![u]\!]$ congrue à G modulo u^v. Alors il existe $P \in GL_d(k[\![u]\!])$ telle que $PG\phi(P)^{-1} = H$.*

Démonstration. — Le théorème des facteurs invariants implique que l'inverse de G (dans $\mathcal{M}_d(K)$) est dans $u^{-\gamma}\mathcal{M}_d(k[\![u]\!])$. On définit une suite de matrices (P_i) par $P_0 = I_d$ et la formule de récurrence $P_{i+1} = H\phi(P)G^{-1}$. Par hypothèse, $P_1 \equiv I_d \pmod{u^{v-\gamma}}$. Pour tout $i \geq 1$, $P_{i+1} - P_i = H\phi(P_i - P_{i-1})G^{-1}$, donc si $P_i - P_{i-1}$ est divisible par u^α, alors $P_{i+1} - P_i$ est divisible par $b\alpha - \gamma$. Une récurrence immédiate montre alors que $P_{i+1} - P_i$ est divisible par u^{v_i}, où v_i est la suite définie par récurrence par $v_0 = v - \gamma$ et $v_{i+1} = bv_i - \gamma$. Comme $v_0 > \frac{\gamma}{b-1}$, la suite (v_i) est croissante et tend vers $+\infty$, ce qui implique que la suite des (P_i) converge pour la topologie u-adique vers une limite P, qui vérifie $PG\phi(P)^{-1} = H$ et qui est congrue à I_d modulo u (car chaque v_i est strictement positif), et est en conséquence inversible dans $k[\![u]\!]$. □

2.1.2. Plan de l'algorithme. — Maintenant que l'on a une idée plus claire de la précision à laquelle on doit obtenir le résultat, on peut présenter les idées de l'algorithme. Il s'agit donc de calculer une filtration par des ϕ-modules isoclines d'un ϕ-module D donné par la matrice G de son Frobenius. Nous détaillerons pas à pas les difficultés inhérentes à l'implémentation de chacune des étapes en donnant les outils mathématiques permettant de résoudre les problèmes qui apparaissent. On fixe γ comme ci-dessus et $\nu > \frac{\gamma}{b-1}$ un entier.

Étape 1. — On fixe $x \in \mathfrak{D} \setminus u\mathfrak{D}$, on calcule la suite $(x_i)_{i\in\mathbb{N}}$ des itérés réduit de x. On cherche alors $\lambda_0, \ldots, \lambda_N \in k$ tels que

$$\lambda_0 x_0 + \cdots + \lambda_N x_N \equiv x_{N+1} \pmod{u^\nu\mathfrak{D}},$$

ce qui est possible car $\mathfrak{D}/u^\nu\mathfrak{D}$ est de dimension finie sur k (on calcule bien des relations à coefficients dans k, et non $k(\!(u)\!)$). On montre alors (voir le lemme 2.2.1 ci-dessous) qu'il existe $\tilde{x}_0$ égal à x_0 modulo u^ν, dont la suite des itérés réduits est notée $(\tilde{x}_i)_{i\in\mathbb{N}}$, tel que

$$\lambda_0\tilde{x}_0 + \cdots + \lambda_N\tilde{x}_N = \tilde{x}_{N+1}.$$

Ainsi, le sous-ϕ-module de $\mathfrak{D}$ engendré par $\tilde{x}_0$ est un quotient du ϕ-module D' donné par $D' = \bigoplus_{i=0}^{N} Ke'_i$ avec $\phi(e'_i) = u^{n_i} e'_{i+1}$ pour $0 \leq i \leq N$ et $\phi(e'_N) = u^{n_N}(\lambda_0 e'_0 + \cdots + \lambda_N e'_N)$. Théoriquement, on connaît toutes les pentes de D' par la théorie du polygone de Newton.

Étape 2. — On veut identifier un sous-module isocline de D'. Pour cela, en utilisant le polygone de Newton de D', on détermine des entiers j, s et un polynôme P tels que pour toute racine α de P, $\exists x_\alpha \in D' \otimes_K k(\alpha)(\!(u)\!)$ tel que $\phi^j(x_\alpha) = u^s x_\alpha$: le rationnel $\frac{s}{b^j - 1}$ est une pente du polygone de Newton de D', et on sait alors qu'il existe un tel x_α. De plus, connaissant α, on peut calculer x_α à précision aussi grande que désiré (car on sait calculer les $\tilde{x}_i$ de l'étape 1 aussi précisément que l'on veut). Enfin, le sous-ϕ-module de D engendré par l'image de x_α est isocline.

Remarque 2.1.4. — Lorsque l'on détermine j, s tels que $\phi^j(x_\alpha) = u^s x_\alpha$, on peut s'assurer que $D(j, s)$ est simple.

Étape 3. — En pratique, on ne peut pas avoir accès à α car le degré de P est de l'ordre de $p^{\dim D}$, donc α peut avoir un degré de cet ordre sur k. Plutôt que de calculer un x_α, on calcule $x = \sum_\alpha \alpha^{-1} x_\alpha$, la somme portant sur les racines non nulles de P. Comme chaque x_α engendre un objet isocline, c'est aussi le cas de x. De plus, x est défini sur $k(\!(u)\!)$. Par des considérations sur les sommes de Newton associées à P, on peut calculer une approximation de x efficacement.

Étape 4. — On calcule l'image y de notre approximation de x dans le quotient D de D'. Cela nous donne une approximation d'un élément engendrant un sous-module isocline D_y de D. On détermine une base de D_y. Si y est une assez bonne approximation d'un élément engendrant un sous-objet isocline, on montre en fait que D_y est isocline.

Remarque 2.1.5. — Il se peut que l'image de x dans D soit 0. Dans ce cas, on peut quand même s'en sortir en construisant à partir de cette donnée un autre ϕ-module dont D est un quotient, et de dimension strictement inférieure à celle de D'. Par souci de simplicité, nous n'exposons pas cette construction dans notre première présentation de l'algorithme, mais elle sera détaillée plus loin.

Récurrence. — On détermine l'action de ϕ sur le quotient D/D_y, et on applique l'algorithme à ce quotient s'il est non nul.

2.2. Détails de l'algorithme. — Nous allons maintenant expliquer plus en détail les différentes parties de l'algorithme.

2.2.1. Étape 1. — Rappelons tout d'abord que la recherche d'une relation de dépendance linéaire entre les éléments de la suite des itérés réduits de $x \in \mathfrak{D} \setminus u\mathfrak{D}$ se fait parmi les

relations à coefficients dans k. Cela est dû au fait qu'il est plus difficile d'identifier une relation de dépendance linéaire à coefficients dans $k(\!(u)\!)$, car on manipule toujours des séries tronquées. En revanche, on a le résultat suivant :
Soit $x \in \mathfrak{D} \setminus u\mathfrak{D}$, et soient $(x_i)_{i\geq 1}$ la suite des itérés réduits de x et $(n_i)_{i\geq 1}$ la suite des exposants réducteurs de x. On note $\mathfrak{M}_x$ le sous-$k[\![u]\!]$-module de $\mathfrak{D}$ engendré par les x_i, qui est par construction stable par ϕ.

Lemme 2.2.1. — *Soient $\lambda_1, \ldots, \lambda_N \in K$, avec λ_1 de valuation finie μ, et soit*

$$c = \min\left\{0, -\frac{\mu}{b-1}\right\}.$$

On suppose que ν est un entier tel que $\nu > \frac{\gamma}{b-1} - c$, et que $\lambda_1 x_1 + \cdots + \lambda_N x_N \in u^{\mu+\nu}\mathfrak{D}$. Alors il existe $\tilde{x} \in \mathfrak{D} \setminus u\mathfrak{D}$, dont la suite des itérés réduits est notée $(\tilde{x}_i)_{i\geq 1}$, tel que la suite des exposants réducteurs de $\tilde{x}$ soit $(n_i)_{i\geq 1}$, que pour tout $i \geq 1$, $\tilde{x}_i \equiv x_i \pmod{u^\nu \mathfrak{D}}$, et tel que

$$\lambda_1 \tilde{x}_1 + \cdots + \lambda_N \tilde{x}_N = 0.$$

Démonstration. — Soit $z \in \mathfrak{D}$ tel que $\sum_{i=1}^N \lambda_i x_i = u^{\mu+\nu} z$. On pose $y = -\lambda_1^{-1} u^\mu z \in \mathfrak{D}$. Soit $x_1' = x_1 + u^\nu y$. On a alors $\phi(x_1') = u^{n_1} x_2 + u^{b\nu}\phi(y)$, et $b\nu \geq \nu + n_1$ car $\nu \geq \frac{\gamma}{b-1}$ et $n_1 \leq \gamma$. Ainsi, la suite des exposants réducteurs de x_1' est la même que celle de x. Si on note $(x_i')_{i\geq 1}$ la suite des itérés réduits de x_1', on vérifie facilement que pour $i \geq 2$,

$$x_i' = x_i + u^{b^{i-1}\nu - b^{i-2}n_1 - \cdots - n_{i-1}} \phi^{i-1}(y).$$

En particulier, si $i \geq 2$, on a $x_i' - x_i \in u^{c_i}\mathfrak{D}$, avec

$$\begin{aligned} c_i - (\mu+\nu) &\geq (b^{i-1}-1)\nu - \frac{b^{i-1}-1}{b-1}\gamma - \mu \\ &\geq (b^{i-1}-1)\left[\nu - \frac{\mu}{b^{i-1}-1} - \frac{\gamma}{b-1}\right] \\ &\geq (b^{i-1}-1)\left[\nu + c - \frac{\gamma}{b-1}\right] \\ &> 0. \end{aligned}$$

Ainsi, modulo $u^{\mu+\nu+1}\mathfrak{D}$, on a

$$\lambda_1 x_1' + \cdots + \lambda_N x_N' \equiv \lambda_1 x_1 + \cdots + \lambda_N x_N - u^{\mu+\nu} z \equiv 0 \pmod{u^{\mu+\nu+1}\mathfrak{D}}.$$

On construit de même par récurrence une suite $x_1^{(j)}$ telle que $x_1^{(j+1)} \equiv x_1^{(j)} \bmod (u^{\nu+j}\mathfrak{D})$, et $\sum_{i=1}^N \lambda_i x_i^{(j)} \equiv 0 \bmod (u^{\mu+\nu+j}\mathfrak{D})$ pour tout $j \geq 1$ (on note naturellement la suite des itérés réduits de $x_1^{(j)}$). Cette suite converge dans $\mathfrak{D}$ vers un élément $\tilde{x}$ vérifiant les propriétés annoncées. □

En particulier, si on obtient une relation $\sum_{i=1}^{N} \lambda_i x_i \equiv x_{N+1} \pmod{u^\nu}$ avec les λ_i dans k et $\lambda_1 \neq 0$, alors il existe $\tilde{x_1} \in \mathfrak{D} \setminus u\mathfrak{D}$, congru à x_1 modulo u^ν, dont la suite des exposants réducteurs est la même que celle de x_1, et dont la suite des itérés réduits, notée $(\tilde{x_i})_{i\geq 1}$, vérifie la relation $\sum_{i=1}^{N} \lambda_i \tilde{x}_i = \tilde{x}_{N+1}$. En outre, la démonstration précédente fournit un moyen de calculer une approximation de $\tilde{x}_1$ aussi précise que désiré.

2.2.2. Étape 2. — Selon que $\sigma = \mathrm{id}$ ou non, les choses se passent un peu différemment ensuite. Lorsque $\sigma = \mathrm{id}$, on doit résoudre une équation du type $\phi^j(x) = \mu u^s x$ pour un μ calculé préalablement comme solution d'une équation de degré au plus N à coefficients dans k. Les coefficients de x sont alors des séries formelles à coefficients dans $k(\mu)$, et le coût de la manipulation de tels objets reste polynômiale en la dimension car N l'est. On peut donc se permettre de faire tous les calculs explicitement sans sacrifier la complexité. Nous détaillerons plus loin la façon de procéder pour ce cas, et nous nous intéressons maintenant au cas $\sigma \neq \mathrm{id}$. Pour ce cas, on est amené à résoudre le système

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_1 u^{n_N} \\ u^{n_1} & 0 & \cdots & 0 & \lambda_2 u^{n_N} \\ 0 & u^{n_2} & \cdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & u^{n_{N-1}} & \lambda_N u^{n_N} \end{pmatrix} \begin{pmatrix} \phi(\alpha_1) \\ \phi(\alpha_2) \\ \vdots \\ \vdots \\ \phi(\alpha_N) \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_N \end{pmatrix},$$

puis à calculer $\sum_{i=1}^{N} t(u^r \alpha_i)\tilde{x}_i$. La démonstration de la proposition 1.2.1 permet de calculer une approximation aussi précise que désiré des α_i. Cependant, pour contrôler la précision de l'approximation de $\sum_{i=1}^{N} t(u^r \alpha_i)\tilde{x}_i$ que l'on va obtenir, il nous faut aussi contrôler la valuation des α_i. C'est la proposition suivante qui fournit ce contrôle :

Proposition 2.2.2. — *Soient $\lambda_1, \ldots, \lambda_N \in k(\!(u)\!)$ et $n_1, \ldots, n_{N-1} \in \mathbb{N}$. On suppose que :*

- $\forall 1 \leq i \leq N,\ n_i \leq \gamma$;
- $\forall 1 \leq i \leq N,\ v(\lambda_i) \geq c$ *(avec $c \leq 0$).*

On considère le système :

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_1 \\ u^{n_1} & 0 & \cdots & 0 & \lambda_2 \\ 0 & u^{n_2} & \cdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & u^{n_{N-1}} & \lambda_N \end{pmatrix} \begin{pmatrix} \phi(\alpha_1) \\ \phi(\alpha_2) \\ \vdots \\ \vdots \\ \phi(\alpha_N) \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_N \end{pmatrix}.$$

Soient $\alpha_1^0, \ldots, \alpha_N^0$ *une solution de ce système, et soit* $r = \frac{s}{b^{j_0}-1}$ *(dans les notations de la proposition 1.2.1). Alors, pour tout* $1 \leq i \leq N-1$,

$$v(u^r \alpha_i^0) \geq \left(1 - \frac{1}{b^i}\right) c - \frac{\gamma}{b-1}$$

En particulier, pour tout $1 \leq i \leq N-1$, $v(t(u^r \alpha_i^0)) \geq \left(1 - \frac{1}{b^N}\right) c - \frac{\gamma}{b-1}$.

Démonstration. — Par construction, $v(\alpha_N^0) = -r$. Comme $u^{n_{N-1}} \phi(\alpha_{N-1}^0) = \alpha_N^0 - \lambda_N \phi(\alpha_N^0)$, on a $n_{N-1} + bv(\alpha_{N-1}^0) \geq \min\{c - br, -r\}$, et par conséquent, $v(\alpha_{N-1}^0) \geq \min\left\{\frac{c-\gamma}{b} - r, \frac{-r-\gamma}{b}\right\}$. Un calcul tout à fait analogue permet de montrer par récurrence sur i que pour tout $1 \leq i \leq N-1$,

$$v(\alpha_{N-i}^0) \geq \min\left\{\min_{1 \leq j \leq i}\left\{\frac{c}{b^j} - \sum_{l=1}^{j} \frac{\gamma}{b^l} - \frac{r}{b^{j-1}}\right\}, -\frac{r}{b^i} - \sum_{l=1}^{i} \frac{\gamma}{b^l}\right\}.$$

En majorant pour $j \in \mathbb{N}^*$ la somme $\sum_{l=1}^{j} \frac{\gamma}{b^l}$ par $\frac{\gamma}{b-1}$, on obtient :

$$v(\alpha_{N-i}^0) \geq \min\left\{\min_{1 \leq j \leq i}\left\{\frac{c}{b^j} - \frac{\gamma}{b-1} - \frac{r}{b^{j-1}}\right\}, -\frac{r}{b^i} - \frac{\gamma}{b-1}\right\}.$$

De la minoration $r \geq c$ apparaissant dans la démonstration de la proposition 1.2.1 (par définition, $r = \min\left\{\frac{b^i v(\lambda_{N-i} + \sum_{l=0}^{i-1} b^l n_{N-l+1}}{b^{i+1}-1}\right\} \geq c$), on tire que $r - \frac{r}{b^i} \geq \left(1 - \frac{1}{b^i}\right) c$, et $r - \frac{r}{b^{j-1}} + \frac{c}{b^j} \geq \left(1 - \frac{1}{b^i}\right) c$ si $1 \leq j \leq i$. Cela démontre la proposition. □

À l'issue de cette étape, on a obtenu une approximation contrôlée de $\tilde{x} = \sum_{i=1}^{N} t(u^r \alpha_i^0) \tilde{x}_i$ vérifiant $\phi^j(\tilde{x}) = u^s \tilde{x}$, qui devrait nous permettre d'identifier un sous-ϕ-module isocline de D. Malheureusement, du fait que la relation trouvée au départ entre les itérés réduits de x_1 n'était *a priori* pas minimale, il se peut que $\tilde{x}$ soit nul. Comme $\tilde{x}$ est une approximation d'une combinaison linéaire des itérés réduits de x_1, s'il est nul on obtient une nouvelle relation de dépendance linéaire entre ces itérés réduits, qui est cette fois-ci à coefficients dans $k(\!(u)\!)$. Cette relation s'écrit :

$$\sum_{i=1}^{N-1} -t(u^r \alpha_i^0)/t(u^r \alpha_N^0) \tilde{x}_i = \tilde{x}_N$$

On peut alors écrire un nouveau système d'équations donné par cette relation pour chercher un vecteur vérifiant une relation du type $\phi^{j'}(x') = u^{s'} x'$, et la longueur de la relation a diminué de 1, ce qui va permettre de faire une récurrence. Deux difficultés apparaissent : comment, alors que l'on dispose seulement d'une approximation de $\tilde{x}$, s'assurer de sa nullité ? Et comment contrôler la précision envisageable pour les solutions nouveau système

qui va apparaître, alors que les coefficients que l'on peut manipuler ne sont que des approximations des coefficients du système qui nous intéresse ?
Il est facile de répondre à la première question grâce au lemme suivant :

Lemme 2.2.3. — *Soit $x \in D$ tel que $\phi^j(x) = u^s x$ pour certains entiers s, j. On suppose que $x \in u^n\mathfrak{D}$ avec $n > \frac{s}{b^j-1}$. Alors $x = 0$.*

Démonstration. — Supposons $x \neq 0$, et soit $n \in \mathbb{Z}$ tel que $x \in u^n\mathfrak{D} \setminus u^{n+1}\mathfrak{D}$. Écrivons $x = u^n y$ avec $y \in \mathfrak{D} \setminus u\mathfrak{D}$. On a alors $\phi^j(x) = u^{b^j n}\phi^j(y) = u^{n+s}y$. Ainsi, comme $y \notin u\mathfrak{D}$, on a $b^j n \leq s + n$, d'où $n \leq \frac{s}{b^j-1}$. □

La deuxième question est plus délicate, et la réponse est fournie par la proposition suivante :

Proposition 2.2.4. — *Soient $\lambda_1, \ldots, \lambda_N \in k(\!(u)\!)$ et $\tilde{\lambda}_1, \ldots, \tilde{\lambda}_N \in k(\!(u)\!)$, et $n_1, \ldots, n_{N-1} \in \mathbb{N}$ tels que*

- *$\forall 1 \leq i \leq N-1$, $n_i \leq \gamma$;*
- *$\forall 1 \leq i \leq N$, $v(\lambda_i) \geq c$, avec $c \leq 0$;*
- *$\forall 1 \leq i \leq N$, $\lambda_i \equiv \tilde{\lambda}_i$ (mod u^t) avec $t \geq -\frac{c}{b-1} + \frac{b\gamma}{b-1}$.*

Alors, il existe des solutions respectives $(\alpha_1, \ldots, \alpha_N)$ et $(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_N)$ aux systèmes $(\mathcal{S}_1)$ définis par les n_i et respectivement les λ_i et les $\tilde{\lambda}_i$ comme dans la proposition 1.2.1, tels que $v(\alpha_i - \tilde{\alpha}_i) \geq t - \frac{b\gamma}{b-1}$ pour tout $1 \leq i \leq N$.

Démonstration. — On cherche d'abord des solutions comme dans la proposition 1.2.1, dont on reprend les notations, notamment concernant l'ensemble J, et les entiers s et j_0. On pose $r = \frac{s}{b^{j_0}-1}$. On choisit $\alpha \in k$ solution non nulle de l'équation (2), ce qui définit de manière unique une solution à chacun des systèmes d'équations considérés. Nous notons $(\alpha_1^0, \ldots, \alpha_N^0)$ et $(\tilde{\alpha}_1^0, \ldots, \tilde{\alpha}_N^0)$ ces solutions respectives. Par construction, $\alpha_N^0 = u^{-r}(\alpha + y)$ et $\tilde{\alpha}_N^0 = u^{-r}(\alpha + \tilde{y})$, où y et $\tilde{y}$ sont solutions respectives des équations (3) définies par les λ_i et les $\tilde{\lambda}_i$.
Pour tout $j \in J$, on note $\lambda_{N-j} = u^{v_{N-j}}(\lambda_{N-j}^0 + \mu_{N-j})$, et $\tilde{\lambda}_{N-j} = u^{v_{N-j}}(\lambda_{N-j}^0 + \tilde{\mu}_{N-j})$. Remarquons maintenant que si $j \in J$, alors $(b^{j+1}-1)r = b^j v_{N-j} + b^j n_N + b^{j-1}n_{N-j} + \cdots + n_{N-1}$, donc $b^j v_{N-j} \leq (b^{j+1}-1)r \leq (b^{j+1}-1)\frac{\gamma}{b-1}$. Par conséquent, pour tout $j \in J$,

$$v\left(\phi^j(\mu_{N-j} - \tilde{\mu}_{N-j})\right) \geq b^j(t - v_{N-j}) \geq t - \gamma.$$

De manière similaire, on montre que si $j \notin J$, alors

$$v\left(\phi^j(\lambda_{N-j} - \tilde{\lambda}_{N-j})u^{b^j n_N + b^{j-1}n_{N-j} + \cdots + n_{N-j} - (b^{j+1}-1)r}\right) \geq b^j t - (b^{j+1}-1)r \geq t - \gamma.$$

On considère alors les suites $(y_i)_{i\geq 0}$ et $(\tilde{y_i})_{i\geq 0}$ définies comme dans la démonstration de la proposition 1.2.1. Les calculs précédents et une récurrence facile montrent immédiatement que pour tout $i \geq 1$, $v(y_i - \tilde{y_i}) \geq t - \gamma$. Il en résulte que $v(y - \tilde{y}) \geq t - \gamma$, et donc que $v(\alpha_N - \tilde{\alpha}_N) \geq t - \frac{\gamma}{b-1} - \gamma$. On en déduit que $v(\alpha_1 - \tilde{\alpha}_1) \geq \min\{t - \frac{b\gamma}{b-1}, c + bv(\alpha_N - \tilde{\alpha_N})\}$. L'hypothèse de minoration de t implique que $v(\alpha_1 - \tilde{\alpha}_1) \geq t - \frac{b\gamma}{b-1}$, et des calculs tout à fait similaires montrent que pour tout $1 \leq i \leq N$, $v(\alpha_i - \tilde{\alpha}_i) \geq t - \frac{b\gamma}{b-1}$. □

Expliquons maintenant la construction de relations de dépendance linéaire successives entre les itérés réduits de x_1. On construit des suites $(\lambda_1^{(l)}, \ldots, \lambda_{N-l}^{(l)})$ et $(\alpha_1^{(l)}, \ldots, \alpha_{N-l}^{(l)})$ de la manière suivante : les $(\lambda_1^{(0)}, \ldots, \lambda_N^{(0)})$ sont de la forme $\lambda_i^{(0)} = \lambda_i u^{n_N}$ pour certains $\lambda_i \in k$ (ceux qui sont calculés à l'étape 1), et $(\alpha_1^{(l)}, \ldots, \alpha_{N-l}^{(l)})$ sont construits comme dans la proposition 1.2.1 à partir du système défini par les n_i et les $\lambda_i^{(l)}$, de sorte que $\alpha_i^{(l)} = t(u^r \alpha_i^{(l),0})$. Tant que $\sum_{i=1}^{N-l} \alpha_i^{(l)} x_i = 0$, on définit pour $1 \leq i < N - l$, $\lambda_i^{(l+1)} = -\alpha_i^{(l)}/\alpha_{N-l}^{(l)}$.

D'après la proposition 2.2.4, on a pour tout $1 \leq i \leq N$, $v(\alpha_i^{(0)}) \geq -\frac{\gamma}{b-1}$, et $v(\alpha_N^{(0)}) = 0$. Tant que la famille $\lambda_i^{(l)}$ est bien définie, on note $c_l = \min\{\min\{v(\lambda_i^{(l)}) \mid 1 \leq i \leq N - l\}, 0\}$. La proposition 2.2.2 s'applique, et on a donc pour tout i, $v(\alpha_i^{(l)}) \geq \left(1 - \frac{1}{b^{N-l}}\right) c_l - \frac{\gamma}{b-1}$. Ainsi, $c_{l+1} \geq \left(1 - \frac{1}{b^{N-l}}\right) c_l - \frac{\gamma}{b-1}$ tant que les $\lambda_i^{(l+1)}$ sont bien définis. En outre, à chaque étape, r_l (correspondant dans les notations de la proposition 1.2.1 à $r = \frac{s}{b^{j_0}-1}$) vérifie $r_l < \frac{\gamma}{b-1}$, ce qui donne une majoration uniforme pour le lemme 2.2.3, ce qui permet de tester la nullité de $\sum_{i=1}^{N-l} \alpha_i^{(l)} x_i$.

Soit $(C_l)_{1\leq l\leq N-1}$ la suite définie par récurrence par $C_0 = 0$ et $C_{l+1} = \left(1 - \frac{1}{b^{N-l}}\right) C_l - \frac{\gamma}{b-1}$. Il est alors clair d'une part que, tant que les $\lambda_i^{(l)}$ sont définis, $v(\lambda_i^{(l)}) \geq C_l$ pour tout i, et d'autre part que $C_l \geq -\frac{l\gamma}{b-1}$. En particulier, pour tout $l \geq 0$ et pour tout $1 \leq i \leq N - l$, $v(\alpha_i^{(l)}) \geq -\frac{N\gamma}{b-1}$. Cette minoration permet de connaître la précision nécessaire pour les $\alpha_i^{(0)}$ de manière à ce que lorsque le processus s'arrête à la l-ème itération, les $\alpha_i^{(l)}$ soient encore connus à une précision suffisante.

2.2.3. Étape 3. — Pour obtenir enfin la réduction en isoclines, il nous faut encore redescendre tous les résultats obtenus sur le corps de base, par des calculs de traces. Il nous faut d'abord nous assurer du fait que ces calculs nous permettent bien de construire un sous-objet isocline de D. On souhaite également expliciter une méthode pour calculer ce résultat rapidement, c'est-à-dire sans passer par l'intermédiaire d'extensions de k, et vérifier que les méthodes et contrôles de précision explicités précédemment restent valables. En effet, comme on a supposé que $\sigma \neq \mathrm{id}$, les coefficients des séries formelles qui interviennent

vivent dans une extension de k dont le degré est *a priori* exponentiel en d, et on souhaite éviter de calculer ces solutions.

Nous allons commencer par expliquer comment éviter d'avoir recours à une extension du corps de base pour calculer directement une filtration d'un ϕ-module défini sur k. On étend ϕ à $k\{\{u\}\}[X]$ en imposant la relation $\phi(X) = X^q$ si $\sigma(x) = x^q$ pour $x \in k$. L'idée est que dans les calculs précédents, la solution de l'équation $\phi^j(x) = u^s x$ que l'on construit est donnée par un vecteur à coefficients dans $k(\alpha)(\!(u)\!)$, où α est racine d'un polynôme de la forme $P(X) = a_0X + a_1X^q + \cdots + a_NX^{q^N}$ (un polynôme linéarisé). Pour chaque racine α de P, on peut construire une solution x_α de l'équation $\phi^j(x) = u^s x$. On va alors calculer $\sum_{\{\alpha\neq 0 \mid P(\alpha)=0\}} \alpha^{-1}x_\alpha$. Comme les coefficients des x_α sont donnés par des polynômes en α, les coefficients ce cette somme s'obtiennent en calculant des sommes de Newton. La forme particulière de P et des coefficients qui interviennent dans les x_α vont nous permettre de faire ces calculs efficacement.

Lemme 2.2.5. — *Soient $P \in k[X]$ de la forme $P(X) = a_0X + a_1X^q + \cdots + a_nX^{q^n}$ et $l \geq 1$ un entier. On note $\hat{P} = \frac{a_0}{a_n} + \frac{a_1}{a_n}X + \cdots + X^n$. Alors la trace de la multiplication par X^{q^l} dans $k[X]/(P)$ est l'opposé du premier coefficient du vecteur ξ_l, où la suite ξ_i est définie comme suit. On note C_P la matrice compagne du polynôme , Pour $0 \leq i \leq n-1$, ξ_i est le vecteur de taille n ayant un 1 en $(i+1)$-ème position, et des zéros ailleurs. Ensuite, $\xi_n = \begin{pmatrix} -a_0/a_n \\ \vdots \\ -a_{n-1}/a_n \end{pmatrix}$. Enfin, pour $i \geq n$, $\xi_{i+1} = C_P\phi(\xi_i)$, où la notation $\phi(\xi)$ désigne simplement le fait que l'on a appliqué ϕ à tous les coefficients de ξ.*

Démonstration. — Remarquons tout d'abord que les polynômes de la forme $\mu_0X + \cdots + \mu_{n-1}X^{q^{n-1}}$ forment un sous-espace vectoriel de $k[X]/(P)$ stable par ϕ. En effet, soit $Q = \sum_{i=0}^{n-1} \mu_i X^{q^i}$. On a $\phi(Q) = \sum_{i=1}^{n-1} \left(\phi(\mu_{i-1}) - \frac{a_i}{a_n}\phi(y_{n-1})\right) X^{q^i}$. Ainsi, $\phi(Q) = (X, \ldots, X^{q^{N-1}}) \cdot M\phi(Y)$, où Y est le vecteur colonne contenant les coefficients de Q, et M est la matrice compagne associée au polynôme P. Ce calcul montre aussi comment calculer $\phi(Q)$. Remarquons maintenant que pour tout $i \geq 0$, le vecteur ξ_i défini dans l'énoncé du lemme correspond à $\phi^i(X)$ écrit sur la base $X, X^q, \ldots, X^{q^{n-1}}$ de ce sous-espace.

Commençons par montrer que le lemme est vrai pour $0 \leq l \leq n-1$. C'est évident pour $l = 0$, et pour $1 \leq l \leq n-1$, la trace de la multiplication par X^{q^l} est égale à $\sum_{P(\alpha)=0} \alpha^{q^l}$. C'est une somme de Newton associée à P, et les identités de Newton impliquent que cette somme est nulle. En effet, si $s_m = \sum_{P(\alpha)=0} \alpha^m$ et si σ_m désigne le m-ème polynôme symétrique élémentaire en les racines de P, alors $(-1)^m m\sigma_m = \sum_{i=0}^{m-1}(-1)^{i-1}\sigma_i s_{m-i}$. Si

m est divisible par p, cette formule se simplifie en $s_m = \sum_{i=1}^{m-1}(-1)^{i-1}\sigma_i s_{m-i}$. Comme les σ_i sont nuls pour $1 \leq i < q^{n-1}$, cela implique que $s_q = 0$, puis par récurrence que tous les s_{q^l} sont nuls pour $1 \leq l \leq n-1$.
Pour le cas général, notons que par linéarité de la trace, la trace de la multiplication par X^{q^l} est l'opposé du coefficient de X dans l'écriture de X^{q^l} sur la base $X, X^q, \ldots, X^{q^{n-1}}$. Le résultat découle alors du fait que les ξ_l calculent précisément les coefficients des X^{q^l} sur cette base. □

Plaçons-nous dans les notations des propositions 1.2.1 et 1.2.4, ainsi que du lemme 2.2.5. On a fixé $n_1, \ldots, n_{N-1} \in \mathbb{N}$ et $\lambda_1, \ldots, \lambda_N \in k(\!(u)\!)$, on suppose que la matrice de ϕ dans une base de D est

$$G = \begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_1 \\ u^{n_1} & 0 & \cdots & 0 & \lambda_2 \\ 0 & u^{n_2} & \cdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & u^{n_{N-1}} & \lambda_N \end{pmatrix}.$$

On considère alors le polynôme P défini comme dans la démonstration de la propostion 1.2.1 par $P(X) = \sum_{j\in J}\sigma^j(\lambda^0_{N-j})X^{q^j} - X \in k[X]$. Notons $n = \deg P$, on réécrit $P = \sum_{i=0}^{n} a_i X^{q^i}$. Avec les notations du lemme 2.2.5, on définit la matrice C_P et les vecteurs ξ_i. On pose aussi $M_1 = C_P$, et pour $i \geq 1$, $M_{i+1} = C_P\phi(M_i)$.
Pour $j \in J$, on pose comme dans la démonstration de 1.2.1, $\lambda_{N-j} = u^{v_{N-j}}(\lambda^0_{N-j} + \mu_{N-j})$.
Pour $j \notin J$, on pose $\beta_{N-j} = \phi^j(\lambda_{N-j})u^{b^j n_N + b^{j-1}n_{N-j}\cdots + n_{N-1} - (b^{j+1}-1)r}$.
Enfin, on définit par récurrence la suite $(Y_i)_{i\geq 1}$ par : $Y_1 = \sum_{j\in J}\phi^j(\mu_{N-j})\xi_{j+1} + \sum_{j\notin J}\beta_{N-j}\xi_{j+1}$, et pour $i \geq 1$,

$$Y_{i+1} = Y_1 + \sum_{j\in J}\phi^j(\lambda^0_{N-1} + \mu_{N-j})M_{j+1}\phi^{j+1}(Y_i) + \sum_{j\notin J}\beta_{N-j}M_{j+1}\phi^{j+1}(Y_i).$$

Si le vecteur Y représente l'élément y de $k(\!(u)\!)[X]/(P)$, alors $M_i\phi^i(Y)$ représente $\phi^i(y)$. La suite $(Y_i)_{i\geq 1}$ converge vers un élément Y_∞ de $(k[\![u]\!][X])^n$. En spécialisant Y_∞ en α racine non nulle de P, on retrouve le y intervenant dans la démonstration de 1.2.1.
Afin de mettre en évidence la dépendance de y en le choix de la racine α de P, on le notera ici $y(\alpha)$. On a alors $x_N(\alpha) = u^{-r}(\alpha + y(\alpha))$ solution de l'équation (1), dont on déduit un vecteur $\hat{x}_\alpha$ vérifiant $\phi(\hat{x}_\alpha) = \hat{x}_\alpha$, et $\phi^{j_0}(t(u^r\hat{x}_\alpha)) = u^s t(\hat{x}_\alpha)$. En particulier, $\sum_\alpha t(u^r\alpha^{-1}\hat{x}_\alpha)$ (la somme portant sur les racines non nulles de P) engendre un ϕ-module isocline de pente r ; nous allons voir comment calculer $\sum_\alpha t(u^r\alpha^{-1}\hat{x}_\alpha) = t(u^r\sum_\alpha \alpha^{-1}\hat{x}_\alpha)$, ce qui se ramène au calcul de $\sum_\alpha \alpha^{-1}\hat{x}_\alpha$. Pour obtenir $\sum_\alpha \alpha^{-1}\hat{x}_\alpha$, il suffit de calculer $x_N(X) = u^{-r}(X+Y_\infty)$, puis $x_1(X) = \lambda_1 u^{n_N}\phi(x_N(X))$, et les $x_i(X)$ par les formules de récurrence analogues et la

méthode décrite dans le lemme 2.2.5 pour appliquer ϕ. Le vecteur $\sum_\alpha \alpha^{-1}\hat{x}_\alpha$ est alors le vecteur colonne dont le i-ème coefficient est l'opposé du premier coefficient de $x_i(X)$.

Voyons maintenant quelle est la précision de l'approximation obtenue par le calcul des Y_i présenté plus haut. Tout d'abord, si $Y \equiv Y_\infty \pmod{u^t}$ avec $t \geq r$, alors $u^{-r}(X+Y) \equiv x_N(X) \pmod{u^{t-r}}$, et donc $u^{n_N}\lambda_1\phi(u^{-r}(X+Y)) \equiv x_1(X) \pmod{u^{t-r}}$. Une récurrence montre facilement que l'on obtient des congruences similaires pour les $x_i(X)$, et donc qu'après multiplication par u^r, on obtient une approximation d'un vecteur engendrant un sous-objet isocline, également modulo u^t. Il nous suffit donc de voir comment obtenir Y_∞ à une précision fixée, disons u^t. On a déjà $Y_1 \in u(k[\![u]\!])^N$. De plus, si $Y_i - Y_{i-1} \in u^v(k[\![u]\!])^N$, alors $Y_{i+1} - Y_i \in u^{bv}(k[\![u]\!])^N$. Ainsi, $Y_i - Y_\infty \in u^{b^i}(k[\![u]\!])^N$, et donc pour $i \geq \log_b(t)$, $Y_i - Y_\infty \in u^t(k[\![u]\!])^N$. En conclusion, après avoir mené un nombre d'itérations du calcul précédent supérieur à $\log_b(t + \frac{\gamma}{b-1})$, on obtient une approximation à u^t près de $x_N(X)$, donc une approximation du même ordre de tous les $x_i(X)$.

2.2.4. Étape 4. — Le calcul précédent fournit une approximation de $\sum_{\{\alpha \mid P(\alpha)=0\}} t(u^r\alpha^{-1}\hat{x}_\alpha)$, et l'on sait que $\sum_\alpha t(u^r\alpha^{-1}\hat{x}_\alpha)$ engendre un sous-ϕ-module isocline de D. Il nous reste à voir que cela suffit à obtenir la réduction en isoclines pour D. Soit $\tilde{x}_1 \in \mathfrak{D} \setminus u\mathfrak{D}$. On note $(x_i)_{i\geq 1}$ la suite des itérés réduits de x_1. Soit $\mu > \frac{2\gamma}{b-1}$ un entier. Il existe $j \geq 1$ et $\lambda_1, \ldots, \lambda_n \in k[\![u]\!]$ tels que $x_j - \sum_{i=1}^n \lambda_i x_{j+i} \in u^\mu\mathfrak{D}$. D'après la proposition 2.2.1, il existe $\tilde{x}_j \in \mathfrak{D} \setminus u\mathfrak{D}$, dont la suite des itérés réduits est notée $(\tilde{x}_i)_{i\geq j}$ tel que pour tout $i \geq j$, $x_i - \tilde{x}_j \in u^\mu\mathfrak{D}$ et tel que $\tilde{x}_j = \sum_{i=1}^n \lambda_i\tilde{x}_{j+i}$. On note $\mathfrak{M} = \sum_{i\geq j} k[\![u]\!]x_i$ et $\tilde{\mathfrak{M}} = \sum_{i\geq j} k[\![u]\!]\tilde{x}_i$. On suppose que le ϕ-module $\tilde{M} = \tilde{\mathfrak{M}}[1/u]$ est isocline.

Lemme 2.2.6. — *Les facteurs invariants du sous-ϕ-module $\tilde{\mathfrak{M}}$ de $\mathfrak{D}$ (c'est-à-dire les facteurs invariants de l'inclusion $\tilde{\mathfrak{M}} \subset \mathfrak{D}$) sont tous de valuation $\leq \frac{\gamma}{b-1}$. Par ailleurs, et $\mathfrak{M}\left[\frac{1}{u}\right]$ est isocline de même pente que $\tilde{M}$.*

Démonstration. — Posons $\tilde{\mathfrak{M}}' = \sum_{i\geq j+1} k[\![u]\!]\tilde{x}_i$ et remarquons alors que $u^\gamma\tilde{\mathfrak{M}}'$ est contenu dans le sous-$k[\![u]\!]$-module $\langle\phi(\tilde{\mathfrak{M}})\rangle$ engendré par $\phi(\tilde{\mathfrak{M}})$. En effet, pour tout $i \geq j$, il existe un entier $0 \leq n_i \leq \gamma$ tel que $u^{n_i}\tilde{x}_{i+1} = \phi(\tilde{x}_i)$. En particulier, $u^\gamma\tilde{x}_{i+1} = u^{\gamma-n_i}\phi(\tilde{x}_i) \in \langle\phi(\mathfrak{M})\rangle$. En outre, en raison de la relation $\tilde{x}_j = \sum_{i=1}^n \lambda_i\tilde{x}_{j+i}$, on a $\tilde{\mathfrak{M}} = \tilde{\mathfrak{M}}'$. Ainsi, $u^\gamma\tilde{\mathfrak{M}} \subset \langle\phi(\tilde{\mathfrak{M}})\rangle$. Si $y \in \tilde{\mathfrak{M}}$, le théorème des facteurs invariants montre que dès que $y \in u\langle\phi(\tilde{\mathfrak{M}})\rangle$, $y \in u\tilde{\mathfrak{M}}$. Par conséquent, si $y \in \tilde{\mathfrak{M}} \setminus u\tilde{\mathfrak{M}}$, alors $\phi(y) \notin u^{\gamma+1}\tilde{\mathfrak{M}}$. Soit alors δ la plus grande valuation d'un facteur invariant non nul de $\tilde{\mathfrak{M}}$, et $y \in \mathfrak{D}$ tel que $u^\delta y \in \tilde{\mathfrak{M}}$ et $u^{\delta-1}y \notin \tilde{\mathfrak{M}}$. On a alors $\phi^j(u^\delta y) \notin u^{\gamma+1}\tilde{\mathfrak{M}}$, et donc $b\delta \leq \gamma + \delta$, d'où on déduit que $\delta \leq \frac{\gamma}{b-1}$. On note ν l'entier immédiatement supérieur à $\frac{\gamma}{b-1}$.
Montrons maintenant que $\tilde{\mathfrak{M}}$ est isocline. Il existe une base $(\varepsilon_1, \ldots, \varepsilon_d)$ de $\mathfrak{D}$ et des entiers

naturels $\delta_1, \ldots, \delta_r$ tels que $(u^{\delta_1}\varepsilon_1, \ldots, u^{\delta_r}\varepsilon_r)$ soit une base de $\mathfrak{M}$. Soit $\tilde{r}$ le nombre de δ_i tels que $\delta_i \leq \delta$. Par construction de $\tilde{\mathfrak{M}}$, pour tout $1 \leq i \leq \tilde{r}$, il existe un élément ε'_i de $\tilde{\mathfrak{M}}$ tel que $u^{\delta_i}\varepsilon_i - \varepsilon'_i \in u^\nu\mathfrak{D}$. Comme $\delta_i \leq \delta < \nu$, $\varepsilon'_i \in u^{\delta_i}\mathfrak{D} \setminus u^{\delta_i+1}\mathfrak{D}$, et on peut donc écrire $\varepsilon'_i = u^{\delta_i}\tilde{\varepsilon}_i$, avec $\tilde{\varepsilon}_i \in \mathfrak{D}$ et $\varepsilon_i - \tilde{\varepsilon}_i \in u^{\nu-\delta}\mathfrak{D}$. Il est clair que $(u^{\delta_1}\tilde{\varepsilon}_1, \ldots, u^{\delta_{\tilde{r}}}\tilde{\varepsilon}_{\tilde{r}})$ est une famille libre dans $\tilde{\mathfrak{M}}$. Montrons qu'elle est également génératrice. Soit $y \in \tilde{\mathfrak{M}} \setminus u\tilde{\mathfrak{M}}$. Il existe $z \in \mathfrak{D}$ tel que $y' = y + u^\nu z \in \mathfrak{M}$. Ainsi, il existe $\alpha_1, \ldots, \alpha_r \in k[\![u]\!]$ tels que $y = \sum_{i=1}^r \alpha_i u^{\delta_i}\varepsilon_i + u^\nu z$. En utilisant les relations de congruences entre les ε_i et les $\tilde{\varepsilon}_i$, on voit qu'il existe $\tilde{z} \in \mathfrak{D}$ tel que $y = \sum_{i=1}^{\tilde{r}} \alpha_i u^{\delta_i}\tilde{\varepsilon}_i + u^{\delta+1}\tilde{z}$. Il en résulte que $u^{\delta+1}\tilde{z} \in u^{\delta+1}\mathfrak{D} \cap \tilde{\mathfrak{M}} \subset u\tilde{\mathfrak{M}}$ car tous les facteurs invariants de $\mathfrak{M}$ sont de valuation $\leq \delta$. Ainsi, $y - \sum_{i=1}^{\tilde{r}} \alpha_i u^{\delta_i}\tilde{\varepsilon}_i \in u\tilde{\mathfrak{M}}$. Par récurrence, en appliquant le même raisonnement, on construit ainsi des suites $(\alpha_i^{(l)})_{l\geq 1}$ convergeant respectivement dans $k[\![u]\!]$ vers $\alpha_i^{(\infty)}$, de telle sorte que $y = \sum_{i=1}^{\tilde{r}} \alpha_i^{(\infty)} u^{\delta_i}\tilde{\varepsilon}_i$. Il en résulte que $(u^{\delta_1}\tilde{\varepsilon}_1, \ldots, u^{\delta_{\tilde{r}}}\tilde{\varepsilon}_{\tilde{r}})$ est une base de $\tilde{\mathfrak{M}}$. Posons maintenant pour $i \geq \tilde{r}+1$, $\tilde{\varepsilon}_i = \varepsilon_i$. La famille $(\tilde{\varepsilon_1}, \ldots, \tilde{\varepsilon_d})$ est une base de $\mathfrak{D}$.

Enfin, notons G_1 (resp. G_2) la matrice de ϕ dans la base $(\varepsilon_1, \ldots, \varepsilon_d)$ (resp. $(\tilde{\varepsilon_1}, \ldots, \tilde{\varepsilon_d})$). Par construction, on sait que $G_1 \equiv G_2 \pmod{u^{b(\nu-\delta)}}$. Par ailleurs, $u^\gamma\mathfrak{D} \subset \langle\phi(\mathfrak{D})\rangle$. Comme $\mathfrak{M}_0 = \bigoplus_{i=1}^r k[\![u]\!]\varepsilon_i$ est stable par ϕ, on a également $u^\gamma\mathfrak{M}_0 \subset \langle\phi(\mathfrak{M}_0)\rangle$. Ainsi, notant H_1 la sous-matrice de G_1 formée des r premières lignes et colonnes, les facteurs invariants de H_1 sont tous de valuation $\leq \gamma$. Par suite, la matrice H_2 constituée des r premières lignes et colonnes de G_2, étant congrue à G_1 modulo $u^{b(\nu-\delta)}$ avec $b(\nu-\delta) > \frac{b\gamma}{b-1}$, définit un ϕ-module isomorphe à celui défini par H_1. C'est en particulier la matrice d'un ϕ-module isocline. La sous-matrice H'_2 de H_2 constituée des $\tilde{r}$ premières lignes et colonnes est donc également la matrice d'un ϕ-module isocline. C'est également la matrice de l'endomorphisme semi-linéaire induit par ϕ sur $\tilde{\mathfrak{M}}\left[\frac{1}{u}\right]$, ce qui achève la démonstration. $\square$

L'idée est d'appliquer ce lemme avec $x_1 = \sum_\alpha \alpha^{-1}\hat{x}_\alpha$. Si on dispose d'une approximation suffisamment précise de x_1, alors on peut calculer les $\tilde{x}_i$, et donc le ϕ-module $\tilde{\mathfrak{M}}[1/u]$. C'est ce ϕ-module qui nous fournit un sous-objet isocline de notre ϕ-module de départ, et on dispose d'une $k[\![u]\!]$-base du ϕ-module adaptée à ce sous-objet. En calculant la matrice de ϕ dans cette base, on n'a plus qu'à isoler la sous-matrice correspondant à l'action de ϕ sur le quotient et à lui réappliquer l'algorithme.

2.3. Algorithme de réduction ($\sigma \neq$ id). — On se donne un ϕ-module sous forme d'une matrice carrée G à coefficients dans $k[\![u]\!]$, correspondant à la matrice de ϕ dans une base $(e_1, \ldots, e_d)$. Les éléments du ϕ-module sont des vecteurs à coefficients dans $k(\!(u)\!)$. La plus grande valuation d'un facteur invariant de G est notée γ, on calcule la suite C_l comme définie précédemment par récurrence par $C_0 = 0$ et $C_{l+1} = \left(1 - \frac{1}{b^{N-l}}\right) C_l - \frac{\gamma}{b-1}$.. On rappelle que l'on suppose $\sigma \neq id$.

Étape 1. — Soient ν le plus petit entier immédiatement supérieur à $\frac{\gamma}{b-1}$, $N = d\nu$, $x_1 := e_1$, et t le plus petit entier supérieur à $((N+1)b+2)\nu + C_1 + \cdots + C_N$.
Tant que $x_1, x_2, \ldots, x_l$ vue comme famille d'éléments de $(k[\![u]\!]/(u^\nu))^d$ est libre, on calcule $n_l = \min\{n \in \mathbb{N} \ / \ u^{-n}\phi(x_l) \in \mathfrak{D}\}$, et $x_{l+1} = u^{-n_l}\phi(x_l)$.
Lorsque cette famille est liée, on obtient une relation

$$\lambda_1 x_1 + \cdots + \lambda_N x_N \equiv x_{N+1} \pmod{u^\nu \mathfrak{D}},$$

avec $\lambda_1 \neq 0$ (quitte à renuméroter).

Étape 2. — On calcule $\alpha_1(X)^0, \ldots, \alpha_N(X)^0 \in k\{\{u\}\}[X]/(P)$ approximations à u^t près des solutions de l'équation

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_1 u^{n_N} \\ u^{n_1} & 0 & \cdots & 0 & \lambda_2 u^{n_N} \\ 0 & u^{n_2} & \cdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & u^{n_{N-1}} & \lambda_N u^{n_N} \end{pmatrix} \begin{pmatrix} \phi(\alpha_1^0) \\ \phi(\alpha_2^0) \\ \vdots \\ \vdots \\ \phi(\alpha_N^0) \end{pmatrix} = \begin{pmatrix} \alpha_1^0 \\ \alpha_2^0 \\ \vdots \\ \vdots \\ \alpha_N^0 \end{pmatrix},$$

où P est le polynôme intervenant dans la démonstration de la proposition 1.2.1 . On utilise la méthode rapide pour appliquer ϕ modulo P, et une implémentation creuse des séries de Puiseux. Soient j, s tels que $v(\alpha_N^0) = \frac{s}{b^j-1}$, et pour $1 \leq i \leq N$, $\alpha_i = t(\mathrm{Tr}_{k(\!(u)\!)[X]/(X^{-1}P)/k(\!(u)\!)}(u^{-\frac{s}{b^j-1}}\alpha_i^0(X)/X))$.

Étape 3. — Soit $c = \min\{v(\alpha_i)\}$. Déterminer $(\tilde{x_i}) \in \mathfrak{D}$ comme dans la proposition 2.2.1 tels que la relation

$$\lambda_1 \tilde{x_1} + \cdots + \lambda_N \tilde{x_N} \equiv \tilde{x}_{N+1} \pmod{u^{\nu-c}\mathfrak{D}}.$$

Si $\sum_{i=1}^N \alpha_i \tilde{x_i} \in u^\nu \mathfrak{D}$, passer à l'étape 4. Sinon, remplacer t par l'entier immédiatement strictement supérieur à $t - \frac{\gamma - c}{b-1}$ et $\lambda_i = -\alpha_i/\alpha_N$ et retourner à l'étape 2 en remplaçant les nouveaux λ_i dans le système considéré (dont la dimension diminue de 1).

Étape 4. — Soit $\tilde{x} = \sum_{i=1}^N \alpha_i \tilde{x_i}$, et $x = u^n \tilde{x}$ de telle sorte que $x \in \mathfrak{D} \setminus u\mathfrak{D}$.
Calculer la suite des itérés réduits de x jusqu'à trouver une relation à coefficients dans k $x_i = \mu_1 x_{i+1} + \cdots + \mu_r x_{i+r}$. Calculer $X \in \mathcal{M}_{d,d}(k[\![u]\!])$ dont les colonnes sont les itérés réduits de x_i.
Appliquer l'algorithme des facteurs invariants à X pour obtenir TXQ diagonale, avec $T, Q \in GL_d(k[\![u]\!])$ déterminées à précision $u^{b\nu}$. Soit δ le nombre d'éléments de cette matrice de valuation $\leq \nu$.
Calculer $T^{-1}G\phi(T)$ et réappliquer l'algorithme à la sous-matrice $(d-\delta) \times (d-\delta)$ inférieure droite H.

2.4. Correction de l'algorithme. — Grâce au lemme 2.2.1, on sait qu'il existe $\hat{x}_1$ tel que, la suite des itérés réduits de $\hat{x}_1$ étant notée $(\hat{x}_i)$, $x_i - \hat{x}_i \in u^\nu \mathfrak{D}$ pour tout $1 \leq i \leq N$, et $\sum_{i=1}^N \lambda_i \hat{x}_i = \hat{x}_{N+1}$. Après le début du l-ème passage dans l'étape 3, pour tout i, $\tilde{x}_i - \hat{x}_i \in u^{\nu-c}\mathfrak{D}$.

Notons de même $\hat{\alpha}_i$ les solutions exactes de l'équation résolue au l-ème passage dans l'étape 2. Alors, $\sum \alpha_i \tilde{x}_i - \sum_{i=1} \hat{\alpha}_i \hat{x}_i \in u^{\min\{t_l - \frac{\gamma}{b-1}, \nu\}}\mathfrak{D}$. En particulier, si $\sum \hat{\alpha}_i \hat{x}_i = 0$, alors $\sum \alpha_i \tilde{x}_i \in u^\nu \mathfrak{D}$. En outre, les λ_i qui sont alors calculés dans l'étape 3 sont congrus modulo $u^{t_i - \frac{b\gamma}{b-1} - \frac{\gamma - c}{b-1}}\mathfrak{D}$ à des $\hat{\lambda}_i$ tels que $\sum \hat{\lambda}_i \hat{x}_i = \hat{x}_{N+1-l}$. Par conséquent, les α_i calculés au passage suivant à l'étape 2 sont bien congrus modulo $u^{t - \frac{(b+1)\gamma - c}{b-1}}\mathfrak{D}$ aux solutions de l'équation fournie par les $\hat{\lambda}_i$.

Enfin, au début de l'étape 4, $\tilde{x} - \sum \hat{\alpha}_i \hat{x}_i \in u^{(b+2)\nu}\mathfrak{D}$, donc $x - u^n \sum \hat{\alpha}_i \hat{x}_i \in u^{(b+1)\nu}\mathfrak{D}$ (car $n \leq \frac{\gamma}{b-1}$). Si on note $\hat{x} = u^n \sum \hat{\alpha}_i \hat{x}_i$, et $\hat{X}$ la matrice $d \times d$ dont les colonnes sont les itérés réduits de $\hat{x}$, alors $X - \hat{X} \in u^{(b+1)\nu}\mathcal{M}_d(k[\![u]\!])$. De plus, les facteurs invariants non nuls de $\hat{X}$ sont tous de valuation $< \frac{\gamma}{b-1}$, il en est donc de même de ceux de X. Il existe des matrices $\hat{T}$, $\hat{Q}$, inversibles dans $\mathcal{M}_d(k[\![u]\!])$, telles que $T - \hat{T} \in u^{b\nu}\mathcal{M}_d(k[\![u]\!])$, et telles que $\hat{T}\hat{X}\hat{Q}$ soit diagonale. Il suffit pour le voir d'appliquer l'algorithme des facteurs invariants à $T\hat{X}Q$.

Comme $\hat{x}$ engendre un ϕ-module isocline, les colonnes de la matrice $\hat{X}$ engendrent un ϕ-module isocline d'après le lemme 2.2.6. En outre, les δ premières colonnes de la matrice $\hat{T}^{-1}$ engendrent le même K-espace vectoriel que toutes les colonnes de $\hat{X}$, donc la matrice $\hat{T}G\phi(\hat{T}^{-1})$ est triangulaire par blocs, le bloc supérieur gauche correspondant à un sous-ϕ-module isocline. Enfin, $TG\phi(T^{-1}) - \hat{T}G\phi(\hat{T}^{-1}) \in u^{b\nu}\mathcal{M}_d(k[\![u]\!])$, donc ces deux matrices définissent des ϕ-modules isomorphes.

2.5. Complexité de l'algorithme. — Pour mener à bien l'étude de complexité, on note μ la complexité du calcul pour appliquer σ à un élément de k, β la complexité de calcul pour la multiplication de deux éléments de k, et $\beta(\alpha)$ la complexité de calcul pour la multiplication de deux éléments de $k[\![u]\!]$ à précision u^α. On se donne donc $G \in \mathcal{M}_d(k[\![u]\!])$, dont le déterminant est de valuation γ. On note ν l'entier immédiatement supérieur à $\frac{\gamma}{b-1}$, et t l'entier immédiatement supérieur (strictement) à $(b+2)\nu + C_1 + \cdots + C_N$. On ne compte que le nombre de multiplications d'éléments de k nécessaires.

2.5.1. Complexité des étapes. —

Appliquer ϕ. — Si $x \in \mathfrak{D}$ est donné sous forme d'un vecteur à coefficients dans $k[\![u]\!]$ modulo u^α, le calcul de $\phi(x)$ se fait en appliquant ϕ à chacun des coefficients de x, puis en multipliant le vecteur obtenu par G. Le nombre d'opérations nécessaires pour appliquer ϕ à un élément de $k[\![u]\!]/(u^\alpha)$ est $\frac{\alpha}{b}\mu$. Le calcul de $\phi(x)$ se fait donc en $O(d^2\beta(\alpha) + \frac{\alpha}{b}\mu)$.

Pour alléger l'écriture, nous noterons par la suite $f(\alpha)$ cette complexité. Pour appliquer ϕ (mod u^α) à un vecteur $d \times 1$ dont les coefficients sont des séries de Puiseux dont α termes sont non nuls, il faut compter $d^2\alpha^2$ multiplications dans k.

Algorithme des facteurs invariants dans $k[\![u]\!]$. — Cet algorithme exécuté à précision u^α demande à l'étape j (traitement des j-èmes ligne et colonne) $2((m-j+1)n+(n-j+1)m)$ multiplications dans $k[\![u]\!]/(u^\alpha)$ (on multiplie par 2 car chaque opération doit être faite sur deux matrices). Le coût de l'inversion d'un élément de $k[\![u]\!]/(u^\alpha)$ qui intervient à chaque étape, et est en $O(\alpha)$ multiplications dans k. Cela fait en tout $4\sum_{j=1}^{\min(m,n)}(mn-(j-1)(m+n)) = \min(m,n)(mn+(m+n)\frac{\min(m,n)-1}{2}) + O(n\alpha)$ opérations. Lorsqu'il y a δ facteurs invariants de valuation $\leq \alpha$, avec $\delta \leq n$, on doit faire en tout $6n\delta^2+2\delta^3-2\delta(n+\delta)+O(n\alpha)$ multiplications dans $k[\![u]\!]/u^\alpha$, ce qui fait $(6n\delta^2+2\delta^3-2\delta(n+\delta)+O(\alpha))\beta(\alpha)$.

Étape 1. — Pour faire un pivot de Gauss "dynamique" dans $k^{\nu d}$: on écrit $x_1 \mod u^\nu$ sur une k-base de $k[\![u]\!]/(u^\nu)$, on applique le pivot de Gauss à x_1 en stockant dans une matrice P les opérations nécessaires. On applique P à x_2, on y applique le pivot de Gauss, en continuant de stocker dans P les informations, jusqu'à ce que l'on trouve une famille liée et une relation. Cela se produit au bout de N étapes. À chaque étape du pivot de Gauss, on fait $d\nu$ opérations dans k pour les calculs sur les x_i, on en fait donc $2\nu dN$ en tout. On fait aussi $d^2\nu^2$ multiplications dans k pour appliquer P à chaque étape, donc $Nd^2\nu^2$ en tout. Enfin, on applique N fois la fonction ϕ à précision ν. La complexité de cette étape de l'algorithme est donc en $O(Nd^2\nu^2\beta + Nf(\nu))$.

Étape 2. — On ne tient pas compte des calculs préliminaires pour déterminer J, s, j_0 et P. On détermine tout d'abord la combinaison linéaire de $X, X^p, \ldots X^{p^{\deg P-1}}$ qui est égale à X^{p^i} pour $1 \leq i \leq N$, ce qui demande au plus N multiplications par une matrice de taille $\deg P$, et qui se fait donc en temps majoré par $N^2\beta$. Pour calculer les matrices A_i permettant d'appliquer ϕ^i de manière efficace dans $(k[\![u]\!]/(u^\alpha))[X]$, on calcule N matrices (pour les applications de ϕ à ϕ^N). L'ensemble de ces matrices est calculé en $N^4\beta$ opérations. On calcule ensuite $\alpha_N^0(X)$ par itérations successives. À la i-ème itération, on applique au plus N fois ϕ et on multiplie par une matrice à coefficients dans k un vecteur dont les coefficients sont des séries de Puiseux. D'après la remarque 1.2.2, il y a au plus Nt coefficients non nuls dans chacune des coordonnées de ce vecteur à chaque itération, ce qui donne $O(N^2t)$ opérations pour calculer les itérés par ϕ de ce vecteur, et $O(N^2t^2)$ opérations pour calculer l'itéré suivant. Il faut au plus $\log_b(t)$ itérations pour terminer le calcul. Cela fait donc $O(N^2t^2\log_b(t))$multiplications dans k.

Étape 3. — Relever les x_i d'une précision v à une précision $v+c$ se fait en $O\left(\log\left(\frac{c}{v-\nu}\right)\right)$ itérations du calcul décrit dans la démonstration du lemme 2.2.1. Si ce calcul se fait à

précision u^t, une itération demande N applications de ϕ à précision u^t, c'est-à-dire $Nf(t)$ opérations. L'étape se fait donc en $O\left(\log\left(\frac{c}{v-\nu}\right)Nf(t)\right)$ opérations.

Étape 4. — Pour l'étape 4, il faut refaire un calcul similaire à celui de l'étape 1 à précision $(b+2)\nu$, et appliquer une fois l'algorithme des facteurs invariants à précision ν.

2.5.2. Complexité globale. — Nous allons ici calculer cette complexité sous les hypothèses suivantes :

- La matrice $G \pmod{u^{b\nu}}$ est à coefficients dans $\mathbb{F}_q$, avec $q = p^v$, et σ est le Frobenius de $\overline{\mathbb{F}_q}$. On a alors $\beta = \widetilde{O}(\log p)$, $\mu = \widetilde{O}(v \log p)$.
- L'algorithme de multiplication dans $k[\![u]\!]/(u^\alpha)$ vérifie $\beta(\alpha) = \widetilde{O}(\alpha)$.

La taille de la matrice donnée en entrée est de l'ordre de $d^2 b\nu$.
L'entier t intervenant dans l'algorithme vérifie $t \leq (Nb + 2 + N^2)\nu$. Dans le cas le plus fréquent, on applique une seule fois l'étape 2, ce qui en fait cependant l'étape la plus coûteuse avec une complexité en $O(N^6\nu^2 \log_b(N))$. Dans ce pire cas, on procède $N-1$ fois à l'étape 2, et l'ensemble des passages dans l'étape 2 coûte $O(N^7\nu^2 \log_b(N))$.
Ainsi, pour calculer un sous-module isocline d'un objet de dimension d, il en coûte entre $O(d^6\nu^8 \log_b(d\nu))$ (dans le cas le plus fréquent) et $O(d^7\nu^8 \log_b(d\nu))$. En conséquence, l'exécution de tout l'algorithme de réduction se fait dans le cas le plus fréquent en $O(d^7\nu^8 \log_b(d\nu))$ et dans le pire cas en $O(d^8\nu^9 \log_b(d\nu))$.
Bien que les problèmes soient assez différents, on peut comparer cette complexité à celle du calcul de la forme de Frobenius pour une matrice à coefficients dans un corps fini : $O(d^3 \log d)$ en moyenne pour une matrice de taille $d \times d$, la taille de la matrice donnée en entrée étant donc d^2 dans **[AC94]**, et à celui de la forme de Jordan qui est en $O(d^4)$ multiplications dans le corps de base.

2.6. Algorithme de réduction (σ = id). — Nous allons maintenant présenter l'algorithme de réduction pour $\sigma = \mathrm{id}$, en rentrant un peu moins dans les détails que précédemment. La différence essentielle avec le cas $\sigma = \mathrm{id}$ est que l'on va ici s'autoriser à faire des extensions finies de k, ce qui nous évite toutes les complications liées aux calculs de sommes de Newton. En contrepartie, la complexité des calculs dans D augmente tandis que l'on étend les scalaires à des extensions finies de k.

Étape 1. — C'est la même que dans le cas $\sigma = \mathrm{id}$. On obtient une relation

$$\lambda_1 x_1 + \cdots + \lambda_N x_N \equiv x_{N+1} \pmod{u^\nu \mathfrak{D}}$$

avec $\lambda_1 \neq 0$.

Étape 2. — Dans les notations de la proposition 1.2.1, on pose $P(X) = \sum_{j\in J} \lambda^0_{N-j} X^{N-j-1} - 1$. On identifie les entiers j_0, s comme dans cette proposition. On fixe k' un corps de rupture de P, et on calcule maintenant dans $K' = k'(\!(u)\!)$. On détermine par récurrence une solution de l'équation $\phi^{j_0}(x) = \mu^{j_0} u^s x$ dans $D \otimes_K K'$. Les coordonnées de x sont notées $\alpha_1, \ldots, \alpha_d$.

Étape 3. — On pose $\mathfrak{D}' = \mathfrak{D} \otimes_k k'$. Soit $c = \min\{v(\alpha_i)\}$. Déterminer $(\tilde{x_i}) \in \mathfrak{D}$ comme dans la proposition 2.2.1 tels que la relation

$$\lambda_1 \tilde{x_1} + \cdots + \lambda_N \tilde{x_N} \equiv \tilde{x}_{N+1} \pmod{u^{\nu-c}\mathfrak{D}'}.$$

Si $\sum_{i=1}^N \alpha_i \tilde{x_i} \in u^\nu \mathfrak{D}'$, passer à l'étape 4. Sinon, poser $t > t - \frac{\gamma - c}{b-1}$ (t entier) et $\lambda_i = -\alpha_i/\alpha_N$ et retourner à l'étape 2 en remplaçant les nouveaux λ_i dans le système considéré (dont la dimension diminue de 1).

Étape 4. — Soit $\tilde{x} = \sum_{i=1}^N \alpha_i \tilde{x_i}$, et $x = u^n \tilde{x}$ de telle sorte que $x \in \mathfrak{D}' \setminus u\mathfrak{D}'$.
Calculer la suite des itérés réduits de x jusqu'à trouver une relation à coefficients dans k', $x_i = \mu_1 x_{i+1} + \cdots + \mu_r x_{i+r}$. Calculer $X \in \mathcal{M}_{d,d}(k'[\![u]\!])$ dont les colonnes sont les itérés réduits de x_i.
Appliquer l'algorithme des facteurs invariants à X pour obtenir TXQ diagonale, soit δ le nombre d'éléments de cette matrice de valuation $\leq \nu$.
Calculer $T^{-1}G\phi(T)$ et réappliquer l'algorithme à la sous-matrice $(d-\delta)\times(d-\delta)$ inférieure droite H.

La preuve de la correction de l'algorithme est la même que pour le cas $\sigma \neq \mathrm{id}$, mais cette fois le résultat renvoyé est une base de $D \otimes_K \bar{k}(\!(u)\!)$ telle que la matrice de ϕ dans cette base soit triangulaire supérieure par blocs, avec des blocs diagonaux de la forme

$$\begin{pmatrix} 0 & \cdots & 0 & \lambda^j u^s \\ 1 & \ddots & 0 & 0 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix},$$

où j est la taille du bloc. Dans le chapitre IV, nous verrons comment cela nous décrit immédiatement la semi-simplifiée de la $\overline{\mathbb{F}}_p$-représentation associée à D.
Calculons maintenant la complexité de cet algorithme. Nous reprenons les notations du paragraphe précédent, en prenant soin de noter $\beta(k')$ la complexité de la multiplication de deux éléments dans une extension finie k' de k, et $\beta(k', \alpha)$ la complexité de la multiplication de deux éléments de $k'[\![u]\!]/(u^\alpha)$. On notera également $f(k, \alpha)$ la complexité de l'application

de ϕ dans cet anneau : en fait, $f(k,\alpha)$ ne dépend pas de k, et ne nécessite pas de multiplication dans k. La complexité de l'étape 1 n'est pas modifiée : c'est $O(Nd^2\nu^2\beta(k)+Nf(k,\nu))$. Pour l'étape 2, on ne tient pas compte des calculs préliminaires pour déterminer J, s, j_0 et P. On note $F(N,k)$ la complexité de la factorisation d'un polynôme de degré N à coefficients dans k. Pour calculer x_μ, il s'agit d'appliquer $\phi,\ldots,\phi^N$ à un élément de $k[\![u^{\frac{1}{b^{j_0}-1}}]\!]$ pour lequel les seuls coefficients non nuls ont des valuations dans $\mathbb{N}+\{\frac{b^i s}{b^{j_0}-1}\}$, puis de calculer une combinaison linéaire de ces itérés. Chacune de ces applications a pour complexité $f(k',\alpha)$ (où $k'=k(\mu)$), le nombre de termes non nuls est au plus Nt, ce qui donne $O(Nt\beta(k'))$ multiplications pour calculer l'itéré suivant dans l'approximation de x_μ, soit en tout $O(Nt\beta(k')\log_b(t))$ multiplications pour le calcul de x_μ. Comme précédemment, l'étape 3 s'effectue en $O(\log\left(\frac{c}{v-\nu}\right)Nf(k',t)$ opérations.
La complexité du calcul d'un sous-objet (en ne conservant que les termes dominants) est donc $O(Nt\beta(k')\log(N^2\nu))$. Ce sous-objet, comme précédemment, peut être nul (l'expérience montre que ce cas se produit rarement) ; dans le pire des cas, on procède $N-1$ fois à cette étape, avec éventuellement des extensions successives du corps, ce qui donne une complexité dans le pire des cas en $O(N^2t\beta(k'')\log(N^2\nu))$, avec k'' une extension de k de degré au plus N^2. L'exécution de tout l'algorithme de réduction se fait donc dans le pire des cas en $O(N^8\nu\log(N^2\nu))$, et dans le cas le plus fréquent en $O(N^6\nu\log(N^2\nu))$. En exprimant cette complexité en fonction de d et ν, on obtient au pire $O(d^8\nu^9\log(d\nu))$ et le plus fréquemment $O(d^6\nu^7\log(d\nu))$.

III.3. Exemples

Nous traitons ici quelques exemples de calculs de réduction de ϕ-modules menés grâce à l'implémentation de l'algorithme précédent dans le logiciel de calcul formel Magma.

3.1. Un exemple pas à pas. — Nous considérons ici le ϕ-module sur $\mathbb{F}_7(\!(u)\!)$, avec $b=p=7$, dont la matrice est suivante, pour laquelle les pentes sont connues :

$$G_1=\begin{pmatrix}0&0&u^3&0&0\\0&1&0&0&0\\1&0&0&0&0\\0&0&0&0&u^6\\0&0&0&1&0\end{pmatrix}$$

Ici, il est clair que les pentes du ϕ-module considéré sont $\frac{3}{7^3-1}=\frac{1}{114}$ et $\frac{6}{7^2-1}=\frac{1}{8}$. On choisit aléatoirement une matrice P dans $GL_5(\mathbb{F}_7(\!(u)\!))$. On calcule alors $G_2=P^{-1}G_1\phi(P)$. Dans

notre exemple, on obtient :

$$\begin{pmatrix} u^{-2}+4+6u^9 & 2u^{-2}+4+6u^9 & 6u^2+u^3+u^5 & 6u^2+u^3+u^5 & u^5+5u^7 \\ 6u^{-4}+u^{-2}+3 & 5u^{-4}+6u^{-2}+3 & 6u^{-3}+1+u^2 & 6u^{-3}+1+u^2 & 6u^3+2u^7 \\ u^{-6}+3u^{-2}+3 & 2u^{-6}+3u^{-4}+2u^{-2}+3 & u^{-5}+6u^{-2}+6 & u^{-5}+6u^{-2}+6 & u^7+u^9 \\ 6u^{-6}+5u^{-2}+3 & 5u^{-6}+4u^{-4}+5 & 6u^{-5}+u^{-2}+u^{-1} & 6u^{-5}+u^{-2}+u^{-1} & 6u+6u^3+4u^5 \\ u^{-5}+5u^{-3}+6u^{-2} & 2u^{-5}+6u^{-3}+5u^{-2} & u^{-4}+u^{-2}+5u^{-1} & u^{-4}+u^{-2}+5u^{-1} & u^2+6u^4+6u^5 \end{pmatrix} + \cdots$$

Ici, on n'a pu écrire entièrement les séries donnant les coefficients de la matrice, faute de place, mais les calculs présentés tiennent compte des coefficients présents en réalité.
Tout d'abord, afin de se ramener au cas où tous les coefficients de la matrice sont dans $k[\![u]\!]$, on multiplie G_2 par une puissance de u adéquate. En faisant le changement de base donné par $u^n I$, on obtient $u^{-(b-1)n}G_2$. Il suffit donc de prendre $n = 1$, et $G = u^6 G_2$ et G_2 définissent des ϕ-modules isomorphes. On a $\gamma = 51$.
On calcule ensuite une relation modulo u^ν avec $\nu = 9$ (l'entier immédiatement supérieur à $51/6$), l'application ϕ étant donnée par G. On pose $x_1 = e_1$, on calcule la suite des itérés réduits de x_1 modulo u^ν. On obtient $x_3 = \begin{pmatrix} 2u^2 \\ 5u^2 \\ 2+5u^2 \\ 5+2u^2+2u^4 \\ 5u^4 \end{pmatrix}$ tel que $u^{16}x_4 = \phi(x_3)$, $u^{28}x_5 = \phi(x_2)$, et $u^{49}x_6 = \phi(x_5) \equiv x_3 \pmod{u^9}$. Cela fournit directement le fait qu'il existe un sous-module de dimension 3 engendré par un vecteur $\tilde{x}$ congru à x_3 modulo u^9 et de pente $\frac{16^2+28\times 7+49}{7^3-1} \sim \frac{3}{7^3-1}$. Il suffit de calculer un relevé $\tilde{x}_3$ de x_3 modulo $u^{9(7+2)}$. La matrice dont les colonnes sont $\tilde{x}_3, \tilde{x}_4 = u^{-16}\phi(\tilde{x}_3), \tilde{x}_5 = u^{-28}\phi(\tilde{x}_4)$ est

$$\begin{pmatrix} 2u^2+\cdots & 5u^4+\cdots & 2u^4+5u^6+\cdots \\ 5u^2+\cdots & 2u^2+2u^4+\cdots & 5u^2+5u^4+2u^6+\cdots \\ 2+5u^2+\cdots & 5+5u^2+2u^4+\cdots & 2+4u^2+3u^4+2u^6+\cdots \\ 5+2u^2+2u^4+\cdots & 2+2u^2+3u^4+5u^6+\cdots & 5+3u^2+6u^4+5u^8+\cdots \\ 5u^4+\cdots & 5u+2u^4+2u^6+\cdots & 2u+5u^4+5u^6+2u^8+\cdots \end{pmatrix}$$

La matrice de ϕ sur le quotient par le sous-objet engendré est :

$$\begin{pmatrix} 6u^6+6u^7+6u^9+6u^{10}+\cdots & 6u^{13}+6u^{14}+\cdots \\ u^5+u^7+u^8+u^{10}+\cdots & u^{12}+u^{14}+\cdots \end{pmatrix}$$

On recherche à nouveau un relation en partant de e_1, elle donne $x_3 = \begin{pmatrix} 6u+6u^2+6u^4+6u^5+6u^7+6u^8 \\ 1+u^2+u^3+u^5+u^6+u^8 \end{pmatrix}$, $x_4 = u^{-19}\phi(x_3)$, $x_5 = u^{-5}\phi(x_2) \equiv x_3 \pmod{u^9}$. Cela termine la décomposition, en montrant que le quotient précédent est isocline de pente $\frac{7\times 19+5}{7^2-1} \sim \frac{6}{7^2-1}$. Après le changement de base fourni par l'algorithme, on obtient la forme suivante :

$$\left(\begin{array}{ccc|cc} u^{49}+6u^{51} & u^9+u^{11} & 6+4u^2+u^4+u^{14} & u+6u^4+6u^6 & 2+3u^2+2u^4+3u^6 \\ 6u^{50}+3u^{52} & u^{12}+4u^{14} & 6u^5+3u^7+u^8 & 3u^4+2u^6+5u^7+2u^8 & 6u^5+3u^7+u^8 \\ 0 & u^{13}+u^{15} & 6u^6+6u^8+u^9 & 2u^5+4u^7+5u^8 & 6u^6+6u^8+u^9 \\ \hline 0 & 0 & 0 & 6u^6+6u^7+6u^9 & 6u^{13}+6u^{14}+6u^{16} \\ 0 & 0 & 0 & u^5+6u^{26} & u^{12}+u^{19} \end{array}\right) + \cdots$$

On peut remarquer que, bien que la forme la plus sympathique donnée par G_1 soit définie sur $\mathbb{F}_7(\!(u)\!)$, on n'obtient pas ici cette décomposition. On ne constate pas non plus le fait que la décomposition soit en fait une somme directe. En revanche, on a bien l'assurance que les blocs diagonaux encadrés définissent des ϕ-modules isoclines.
L'auteur a traité un certain nombre d'exemples à l'aide de Magma. Pour les petites dimensions et les petites valeurs de γ ($d \leq 10$, $\gamma \leq 5$, $p = b \leq 13$), le temps de calcul pour la réduction est de l'ordre de quelques secondes. Des exemples ont été traités jusqu'à $d = 100$, avec $p = 7$ et $\gamma \simeq p$, les temps de calcul étant de l'ordre de quelques dizaines de minutes (moins de 3 heures). Pour $d = 2$, on a également testé les grandes valeurs de p, γ étant choisi de l'ordre de p. Les temps de calcul restent raisonnables jusqu'à p de l'ordre de 1000, mais l'implémentation en Magma ne permet pas d'aller jusqu'à des p de l'ordre de 10000. Par ailleurs, on a aussi calculé des exemples avec de plus grandes valeurs de γ (plutôt de l'ordre de p^2). Les tableaux suivant récapitulent quelques temps de calculs effectués pour $p = 7$, $k = \mathbb{F}_{7^2}$.

$d = 2$

γ	7	41	62	70
Temps (sec)	0.22	0.37	0.42	0.43

$d = 3$

γ	6	19	40	80	98
Temps (sec)	0.26	0.41	0.96	1. 03	1.19

$d = 10$

γ	6	10	24	61
Temps (sec)	12.9	14.0	21.3	31.5

$d = 20$

γ	28	52
Temps	1m14s	2m48s

3.2. Un exemple provenant de l'arithmétique. — Soient L/K une extension finie, séparable, $\alpha \in \mathcal{O}_L$ tel que $L = K(\alpha)$, et P le polynôme minimal de α sur K. Le Frobenius sur L défini pour $x \in L$ par $\phi(x) = x^p$ munit naturellement L d'une structure de ϕ-module sur K (pour le même Frobenius sur K). La représentation galoisienne associée à L est donnée par $V = \mathrm{Hom}_{\phi,K}(L, K^{sep})$ (l'espace des K-homomorphismes de L vers une clôture séparable K^{sep} de K commutant au Frobenius) muni de l'action de $\mathcal{G} = \mathrm{Gal}(K^{sep}/K)$ induite par celle sur K^{sep}.

Proposition 3.2.1. — *La représentation associée à L s'identifie au $\mathbb{F}_p$-espace vectoriel dont une base est donnée par la famille des conjugués de α dans K^{sep}, muni de l'action naturelle de $\mathcal{G}$ sur cette base.*

Démonstration. — La représentation $V = \mathrm{Hom}_{\phi,K}(L, K^{sep})$ contient la famille des K-plongements de L vers K^{sep} puisqu'un tel plongement ψ commute avec ϕ. De plus, $\psi : L \to K^{sep}$ est déterminé par l'image de α, qui est nécessairement un conjugué de α. Soit $d = \deg P$, et notons $\alpha_1 = \alpha, \ldots, \alpha_d$ les conjugués de α dans K^{sep} et pour $1 \leq i \leq d$, $\psi_i : L \to K^{sep}$ le K-plongement défini par $\psi_i(\alpha) = \alpha_i$. La restriction à $L^\star$ des ψ_i fournit une famille de morphismes distincts $L^\star \to (K^{sep})^\star$. D'après le théorème d'indépendance linéaire des morphismes d'Artin, ces morphismes forment une famille libre dans V, et il en est donc de même des ψ_i. Comme V est un $\mathbb{F}_q$-espace vectoriel de dimension d, cette famille forme une base de V. L'action de $\mathcal{G}$ sur V est déterminée de la manière suivante : pour $g \in \mathcal{G}$, $(g\psi_i)(\alpha) = g\alpha_i$. Considérons maintenant W la $\mathbb{F}_q$-représentation de $\mathcal{G}$ dont une base est formée par les conjugués de α, munie de l'action naturelle de $\mathcal{G}$. L'application linéaire $f : W \to V$ envoyant α_i sur ψ_i commute avec l'action de $\mathcal{G}$, car si $g \in \mathcal{G}$, $f(g\alpha_i)$ est le morphisme $L \to K^{sep}$ envoyant α sur $g\alpha_i$, et $gf(\alpha_i) = g\psi_i$ est le morphisme envoyant α sur $g\alpha_i$ d'après la description précédente. Ainsi, les représentations V et W sont isomorphes, ce qui démontre la proposition. □

En particulier, si on note $\rho : \mathcal{G} \to GL(V)$ la représentation précédente, et L' une clôture galoisienne de L, alors $\ker \rho$ est le groupe de Galois $\mathcal{G}_{L'} = \mathrm{Gal}(K^{sep}/L')$ et l'image de ρ est isomorphe au quotient $\mathcal{G}/\mathcal{G}_{L'} \simeq \mathrm{Gal}(L'/K)$: c'est le groupe de Galois du polynôme P. En décrivant précisément l'image de ρ, on obtient donc la structure de $\mathrm{Gal}(L'/K)$. En général, on sait simplement que les facteurs de composition de $\mathrm{Gal}(L'/K)$ sont donnés par les représentations associées à des modules simples dont les pentes sont celles du ϕ-module L.

Pour faire un tel calcul en pratique, il est plus agréable de disposer d'une majoration de γ, que nous allons donner maintenant.

Lemme 3.2.2. — *Soit G la matrice de ϕ dans la base $1, \alpha, \ldots, \alpha^{d-1}$ de L, et γ la plus grande valuation d'un facteur invariant de G. On note $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0$. Alors :*

$$\gamma = \lceil qv(P'(\alpha)) - v(\mathfrak{d}_{L/K}) \rceil$$

où $\mathfrak{d}_{L/K}$ désigne la différente de l'extension L/K et $\lceil t \rceil$ désigne le plus petit entier supérieur ou égal à t. En particulier, si α est une uniformisante de $\mathcal{O}_L$,

$$\gamma = \lceil (q-1)v(P'(\alpha)) \rceil = \left\lceil (q-1) \min_{p \nmid i} \left\{ v(a_i) + \frac{i-1}{d} \right\} \right\rceil.$$

Démonstration. — Notons $\mathcal{O}_K[\alpha^q]$ la sous-$\mathcal{O}_K$-algèbre de $\mathcal{O}_L$ engendrée par α^q. Par définition, γ est le plus petit entier tel que pour $1 \leq i \leq d$, $u^\gamma \alpha^{i-1} \in \mathcal{O}_K[\alpha^q]$. Or, le conducteur de $\mathcal{O}_K[\alpha^q]$ dans $\mathcal{O}_L$ est l'idéal de $\mathcal{O}_K[\alpha^q]$ formé de l'ensemble des $x \in \mathcal{O}_K[\alpha^q]$

tels que $x\mathcal{O}_K \subset \mathcal{O}_K[\alpha^q]$. Cet idéal est déterminé par la valuation de l'un de ses générateurs, et γ est donc le plus petit entier supérieur ou égal à cette valuation. D'après **[Ser68]**, Chap. 3, §6, corollaire 1, le conducteur est l'idéal $Q'(\alpha^q)\mathfrak{d}_{L/K}$, où Q désigne le polynôme caractéristique de α^q. Par ailleurs, si on note u_α (respectivement u_{α^q}) l'application de multiplication par α (respectivement α^q) dans $\mathcal{O}_L$, le polynôme caractéristique Q de α^q vérifie $Q(X^q) = \det(u_{\alpha^q} - X^q I) = \det(u_\alpha - XI)^q = P(X)^q$. Ainsi, Q n'est autre que le polynôme déduit de P en appliquant le Frobenius à tous ses coefficients, ce qui démontre la première affirmation.

Si α est une uniformisante de $\mathcal{O}_L$, alors la différente de L/K n'est autre que l'idéal engendré par $P'(\alpha)$, ce qui démontre la première égalité de la deuxième assertion. Par ailleurs, $P'(X) = \sum_{p\nmid i} i a_i X^{i-1}$ (avec la convention $a_d = 1$). Comme $v(\alpha) = \frac{1}{d}$, on a $v(i a_i \alpha^{i-1}) = v(a_i) + \frac{i-1}{d}$, et toutes ces valeurs sont distinctes car si $1 \leq i \leq j \leq d$, sont tels que $v(a_i) + \frac{i-1}{d} = v(a_j) + \frac{j-1}{d}$, alors $0 \leq v(a_i) - v(a_j) = \frac{j-i}{d} < 1$. Comme $v(a_i)$ et $v(a_j)$ sont des entiers, $v(a_i) = v(a_j)$, d'où on déduit que $i = j$. Par conséquent, $v(P'(\alpha)) = \min_{p\nmid i}\left\{v(a_i) + \frac{i-1}{d}\right\}$, ce qui démontre la deuxième égalité. $\square$

Un exemple simple dans lequel on peut appliquer le résultat précédent est celui où α est une uniformisante de l'anneau des entiers de L. Le polynôme P est alors un polynôme d'Eisenstein E (pour l'idéal (u)). Prenons par exemple $K = \mathbb{F}_{3^3}(\!(u)\!)$, $\phi(x) = x^3$ et $E(X) = X^6 + u^2X^2 - uX - u$. L'extension L est une extension totalement ramifiée de degré 6. La matrice du Frobenius dans la base $1, \alpha, \ldots, \alpha^5$ est :

$$\begin{pmatrix} 1 & 0 & u & 0 & u^2 & u^4 \\ 0 & 0 & u & 0 & 2u^2 & u^4 + u^5 \\ 0 & 0 & 2u^2 & 0 & u^2 + u^3 & 0 \\ 0 & 1 & 0 & u & u^3 & u^2 + 2u^6 \\ 0 & 0 & 0 & u & u^4 & 2u^2 \\ 0 & 0 & 0 & 2u^2 & 0 & u^2 + u^3 \end{pmatrix}.$$

On a de plus $\gamma = 2$. L'algorithme de réduction donne une filtration $0 \subset L_1 \subset L_2 \subset L_3 \subset L_4 \subset L_5 = L$ avec $L_1 \simeq D(1,0)$, $L_2/L_1 \simeq D(1,1)$, $L_3/L_2 \simeq D(2,2)$, $L_4/L_3 \simeq D(1,1)$ et $L/L_4 \simeq D(1,2)$. Les pentes du ϕ-module L sont donc 0, $\frac{1}{4}$, $\frac{1}{2}$ (double) et 1. En particulier, $\mathrm{Gal}(E/K)$ s'identifie à un sous-groupe du groupe des matrices triangulaires supérieures par blocs) à coefficients dans $\mathbb{F}_3$, avec quatre blocs diagonaux de taille 1 et un bloc de taille 2.

CHAPITRE IV

APPLICATION AUX CALCULS EFFECTIFS POUR LES REPRÉSENTATIONS GALOISIENNES

Dans ce chapitre, nous donnons des applications de l'algorithme développé dans le chapitre III pour l'étude des représentations galoisiennes. Ces applications proviennent de plusieurs variations sur l'équivalence de catégories de Fontaine. Tout d'abord, nous donnons une description en fonction de certains paramètres des représentations irréductibles à coefficients dans un corps fini du groupe de Galois absolu G_K d'un corps K complet pour une valuation discrète, et dont le corps résiduel est fini. Ensuite, nous montrons comment on peut décrire la représentation de G_K (c'est à dire, donner les paramètres correspondants dans la classification précédente) associée à un ϕ-module donné, lorsque ϕ agit comme un Frobenius (ces ϕ-modules correspondent aux E-représentations pour un corps $E \subset k$), ou par élévation à la puissance q sur u et trivialement sur les coefficients (ces ϕ-modules correspondent aux $\overline{\mathbb{F}}_p$-représentations de G_K si $k = \mathbb{F}_q$). Nous nous intéressons ensuite rapidement au cas des modules de Kisin en caractéristique p, qui sont des ϕ-modules décrivant des représentations modulo p de groupes de Galois p-adiques, puis au cas des modules de Wach, qui jouent le même rôle mais sont des (ϕ, Γ)-modules. Nous expliquons en particulier comment calculer la semi-simplifée d'un (ϕ, Γ)-module, ainsi que la semi-simplifiée de la représentation associée.

IV.1. Description des représentations irréductibles de G_K

Soit k un corps fini de caractéristique $p > 0$, on note q le cardinal de k. Soit K un corps complet pour une valuation discrète, dont le corps résiduel est k. On note π une uniformisante de K. Soit K^{sep} une clôture séparable de K, et $G_K = \mathrm{Gal}(K^{sep}/K)$ le groupe de Galois absolu de K. Si $r \geq 1$ est un entier, on note en général $\mathbb{F}_{p^r}$ le corps à p^r éléments contenu dans le corps résiduel de K^{sep}.
Si V est une représentation irréductible de G_K, de dimension d, à coefficients dans $\mathbb{F}_{p^r}$, le sous-groupe d'inertie sauvage étant un pro-p-groupe, il agit trivialement sur V. Ainsi, V est une représentation irréductible de $G_K/I_p = R_K$ (la notation R_K n'est pas standard,

mais il n'existe à vrai dire pas de notation standard pour ce groupe). Le groupe R_K est le produit semi-direct du groupe d'inertie modérée I_t, et du groupe de Galois absolu de k, G_k. Plus précisément, G_k est un groupe procyclique, isomorphe au complété profini de $\mathbb{Z}$ noté $\hat{\mathbb{Z}}$. Le groupe G_k est engendré par le morphisme de Frobenius Frob_q, qui n'est autre que l'élévation à la puissance q. Le groupe I_t, lui, est le groupe de Galois $\mathrm{Gal}(K^{mr}/K^{nr})$ de l'extension maximale modérément ramifiée de K sur l'extension maximale non ramifiée de K. Il est isomorphe à $\prod_{\ell \neq p} \mathbb{Z}_\ell$, le produit portant sur tous les nombres premiers $\ell \neq p$. On fixe $(\varpi_n)_{n\in\mathbb{N}}$ une suite de racines $p^n - 1$-èmes de l'uniformisante. Le corps K^{mr} n'est rien d'autre que le corps engendré sur K^{nr} par tous les ϖ_n. Si $g \in I_t$, alors $\frac{g\varpi_n}{\varpi_n} \equiv \omega_n(g) \pmod{\varpi_n}$, avec $\omega_n(g)^{p^n-1} = 1$, donc $\omega_n(g) \in \mathbb{F}_{p^n}^\times \subset \bar{k}^\times$. Cela montre que si $\sigma \in R_K$ est envoyé sur Frob_q par la projection canonique, et $g \in I_t$, alors $\sigma g \sigma^{-1} = g^q$.

Soit V une représentation irréductible de H_K à coefficients dans $\mathbb{F}_{p^r}$, la restriction de G à I_t est semi-simple car I_t est une limite projective de groupes d'ordre premier à p. Nous allons donc commencer par essayer de comprendre les $\mathbb{F}_{p^r}$-représentations irréductibles de I_t. Soit donc W une telle représentation, que l'on suppose de dimension δ. L'anneau des endomorphismes I_t-équivariants $E = \mathrm{End}_{I_t}(W)$ est une algèbre à division d'après le lemme de Schur ; c'est aussi un ensemble fini, et donc un corps d'après le théorème de Wedderburn. La représentation W hérite d'une structure naturelle de représentation E-linéaire. La dimension de cette E-représentation est 1 car l'action de E sur W est transitive (la commutativité de I_t implique que ses éléments agissent de manière I_t-équivariante). Ainsi, $[E : \mathbb{F}_{p^r}] = \dim_{\mathbb{F}_{p^r}} W = \delta$ et E est isomorphe à $\mathbb{F}_{p^{r\delta}}$ en tant que $\mathbb{F}_{p^r}$ espace vectoriel. On fixe un isomorphisme réalisant cette identification (un tel isomorphisme n'est pas canonique), ce qui fait que W s'identifie à un caractère $\chi : I_t \to \mathbb{F}_{p^{r\delta}}^\times$. Remarquons au passage que si on choisit un autre isomorphisme $\mathbb{F}_{p^r}$-linéaire $E \to \mathbb{F}_{p^{r\delta}}$, alors on obtient un autre caractère $\tilde{\chi}$, qui est obtenu en composant χ avec un automorphisme $\mathbb{F}_{p^r}$-linéaire de $\mathbb{F}_{p^{r\delta}}$, ce qui veut dire que $\tilde{\chi} = \chi^{p^{rm}}$ pour un $0 \leq m \leq \delta - 1$. Par ailleurs, comme I_t est un groupe procyclique, les caractères $I_t \to \mathbb{F}_{p^{r\delta}}^\times$ sont exactement les puissances du caractère fondamental $\omega_{r\delta} : g \mapsto \frac{g\varpi_{r\delta}}{\varpi_{r\delta}} \pmod{\varpi_{r\delta}}$: il existe $0 \leq s \leq p^{r\delta-2}$ tel que $\chi = \omega_{r\delta}^s$. Modulo la relation d'équivalence $s \sim s'$ lorsqu'il existe $0 \leq m \leq \delta - 1$ tel que $s \equiv p^{rm} s' \pmod{p^{r\delta} - 1}$, l'entier s défini ainsi ne dépend que de la représentation W. Les chiffres de l'écriture de s en base p^r sont appelés *poids de l'inertie modérée* de la représentation W.

Revenons maintenant à notre représentation irréductible de H_K, V, qui est de dimension d à coefficients dans $\mathbb{F}_{p^r}$. D'après l'étude précédente, la restriction à I_t de V est isomorphe à la somme directe $\omega_{r\delta_1}^{s_1} \oplus \cdots \oplus \omega_{r\delta_t}^{s_t}$, pour certains entiers t, $\delta_1, \ldots, \delta_t$, et $s_1, \ldots, s_t$. Ici,

les caractères $\omega_{r\delta_i}$ sont vus comme des $\mathbb{F}_{p^r}$-représentations irréductibles de dimensions respectives δ_i, c'est à dire que $V = V_1 \oplus \cdots \oplus V_t$, avec V_i sous-espace de dimension δ_i stable par l'action de I_t, et sur lequel le choix d'un isomorphisme vers $\mathbb{F}_{q^{r\delta_i}}$ identifie l'action de I_t à l'action par le caractère $\omega_{r\delta_i}^{s_i}$: l'entier s_i est donc bien défini modulo la relation du paragraphe précédent. Soit $\sigma \in H_K$ tel que la réduction modulo I_t de σ soit Frob_q et agissant trivialement sur les racines de l'uniformisante. Remarquons que l'action de σ sur V vue comme $\mathbb{F}_{p^{r\delta}}$-espace vectoriel n'est en général pas linéaire. Le sous-espace σV_1 est stable sous l'action de I_t. En effet, si $g \in I_t$, $g\sigma^{-1}V_1 = \sigma^{-1}g^qV_1 = \sigma^{-1}V_1$. Soit s un entier, maximal pour la propriété « la somme $V_1 + \cdots + \sigma^{s-1}V_1$ est directe ». On a alors $\sigma^s V_1 \cap (V_1 \oplus \sigma V_1 \oplus \cdots \oplus \sigma^{s-1}V_1) \neq \{0\}$, et comme la représentation $\sigma^s V_1$ est une représentation irréductible de I_t, $\sigma^s V_1 \subset V_1 \oplus \sigma V_1 \oplus \cdots \oplus \sigma^{s-1}V_1$. Donc $V_1 \oplus \cdots \oplus \sigma^{s-1}V_1$ est stable sous l'action de σ et celle de I_t, c'est donc une sous-représentation non nulle de V, et

$$V = V_1 \oplus \cdots \oplus \sigma^{s-1}V_1.$$

En particulier, $s = t$. Fixons $x_1 \in V_1$, on a $\sigma^s x_1 = \lambda_1 x_1 + \cdots + \lambda_{s-1}\sigma^{s-1}x_1$, avec les $\lambda_i \in E$. Comme $\sigma^s V_1$ est isomorphe en tant que $\mathbb{F}_{p^r}$-représentation à V_1, on a $\lambda_i = 0$ dès que $p^r - 1$ ne divise pas $q^i - 1$. Si on note τ l'ordre de q modulo $p^r - 1$, cela se traduit par $\lambda_i = 0$ si τ ne divise pas i. On note $t = \tau\ell$, et $P = X^\ell - \sum_{i=0}^{\ell-1} \lambda_i X^i \in E[X, \sigma^\tau]$. Ce polynôme tordu (au sens du chapitre I de cette thèse) est irréductible. En effet, si $P = P_1P_2$ avec P_1 non constant, alors $P_1(\sigma^\tau)P_2(\sigma^\tau)(x_1) = 0$, donc $P_2(\sigma^\tau)(x_1)$ est annulé par $P_1(\sigma^\tau)$. Mais $P_2(\sigma^\tau)(x_1)$ engendre une représentation V_1' de I_t isomorphe à V_1, donc la représentation $V_1' \oplus \sigma V_1' \oplus \cdots \oplus \sigma^{\tau \deg P_1 - 1}V_1'$ est une sous-représentation de V, qui est stricte puisque P_1 est non constant. On définit certaines représentations de la manière suivante :

Définition 1.0.3. — Soit τ l'ordre de q modulo p^r. Soient $\delta \in \mathbb{N}^*$, $t \in \mathbb{N}^*$ multiple de τ, s_1 un entier primitif pour $r\delta$. Soit $E = \mathrm{End}_{I_t}(\omega_{r\delta}^{s_1})$, et soit $P \in E[X, \sigma^\tau]$. On note $V_{\delta,t,s_1,P}$ la représentation décrite de la manière suivante : $V_1 = \omega_{r\delta}^{s_1}$, $V = V_1 \oplus \sigma V_1 \oplus \cdots \oplus \sigma^t V_1$, et il existe $x_1 \in V_1$ tel que $\sigma^t(V_1) = P(\sigma^\tau)(x_1)$.

On a alors :

Proposition 1.0.4. — *Toute représentation irréductible de G_K à coefficients dans $\mathbb{F}_{p^r}$ est isomorphe à une représentation de la forme $V_{\delta,t,s,P}$. De plus, si $P \in \mathbb{F}_{p^r}[X, \sigma^\tau]$ et $i \in \mathbb{N}$, on note $P^{(q^i)}$ le polynôme où on a élevé les coefficients de P à la puissance q^i. Alors les isomorphismes entre représentations de la forme $V_{\delta,t,s,P}$ sont donnés par $V_{\delta,t,s_1,P} \simeq V_{\delta,t,q^i s_1,\tilde{P}^{(q^i)}}$ avec $0 \leq i \leq \tau - 1$ et $\tilde{P}$ similaire à P.*

Démonstration. — On a déjà vu que les représentations irréductibles se décrivent de cette manière. Il nous reste à donner les isomorphismes entre deux telles représentations. Pour que V_1' soit une sous-I_t-représentation de V isomorphe à V_1, il faut et il suffit que V_1 contienne un vecteur de la forme $x_1' = Q(\sigma^\tau)(x_1)$ avec $Q \in E[X, \sigma^\tau]$. Fixons un tel Q, et notons $\tilde{P}Q$ le plus petit multiple commun à droite de P et Q. Comme P est irréductible, $\tilde{P}$ est similaire à P, et $\tilde{P}(\sigma^\tau)(x_1') = 0$. Un autre paramétrage de la représentation est donc donné par $(\delta, t, s_1, \tilde{P})$.

Par ailleurs, on peut aussi décrire notre représentation en partant de σx_1 au lieu de x_1, ce qui conduit au paramétrage $(\delta, t, qs_1, P^{(q)})$. D'une manière générale, si V_1^0 est une sous-I_t-représentation irréductible de V, et si $x \in V_1^0$, alors il existe un entier i tel que $\sigma^i x$ engendre une représentation de I_t isomorphe à V_1. Cela montre que les isomorphismes possibles sont ceux annoncés. □

IV.2. Calcul de la semi-simplifiée de la représentation associée à un ϕ-module

Nous allons maintenant expliquer comment décrire la semi-simplifiée de la représentation associée à un ϕ-module sur $K = \mathbb{F}_q(\!(u)\!)$, dans deux cas particuliers : celui où $\phi(x) = x^{p^r}$, et $\mathbb{F}_{p^r} \subset \mathbb{F}_q$ (qui correspond aux $\mathbb{F}_{p^r}$-représentations de G_K), et celui où $\sigma = id$ et $\phi(u) = u^q$ (qui correspond aux $\overline{\mathbb{F}_p}$-représentations de G_K).

2.1. Le cas des $\mathbb{F}_{p^r}$-représentations, avec $\mathbb{F}_{p^r} \subset K$. — Rappelons que parmi ces représentations, celles qui sont irréductibles sont décrites par :

- des entiers δ, t tels que $\delta t = \dim V$, δ étant la dimension d'une sous-représentation irréductible V_1 de la restriction de V à l'inertie modérée ;
- une identification $E = \mathrm{End}(V_1) \simeq \mathbb{F}_{p^{r\delta}}$;
- d'un entier s tel que $V_1 \simeq \omega_{r\delta}^s$;
- un polynôme $P = X^t - \lambda_{t-1}X^{t-1} - \cdots - \lambda_0 \in E[X, \sigma]$ tels que pour un $x_1 \in V_1$, $\sigma^t x_1 = \sum_{i=0}^{t-1} \lambda_i \sigma^i x_1$.

On note $V_{\delta,s,P}$ la représentation correspondante.

On se donne maintenant un ϕ-module simple sur K, que l'on note D. Il s'agit de déterminer la représentation associée à D. Si D est de pente $\frac{s}{p^{r\delta}-1}$, on connaît déjà la restriction à l'inertie modérée de la représentation associée. De plus, on sait qu'il existe un polynôme P à coefficients dans $\mathbb{F}_q$, de la forme $\sum_{i=0}^N \mu_i X^{p^{ri}}$, tel que pour toute racine α de P, on sache construire (au moins théoriquement) un élément x_α de $D \otimes_K K(\alpha)$ tel que $\phi^\delta(x_\alpha) = u^s x_\alpha$. On notera D_α le ϕ-module engendré par x_α : c'est un ϕ-module simple sur K^{nr}. Comme précédemment, notons σ un élément de G_K relevant le Frobenius sur $\mathbb{F}_q$, et n'agissant pas sur $u^{1/n}$ lorsque p et n sont premiers entre eux. On peut faire agir σ sur les x_α précédents,

et on a $\sigma x_\alpha = x_{\alpha^q}$ par construction. Par conséquent, on a aussi $\sigma D_\alpha = D_{\alpha^q}$. Soit t minimal tel que $\sigma^t D_\alpha \subset D_\alpha + \cdots + \sigma^{t-1} D_\alpha$. En tant que ϕ-module sur K^{nr}, D est isomorphe à $D_\alpha \oplus \cdots \oplus \sigma^{t-1} D_\alpha$ (car D_α est simple), et $\sigma^t x_\alpha$ s'écrit comme une combinaison linéaire à coefficients dans K^{nr} d'éléments de $D_\alpha \oplus \cdots \oplus \sigma^{t-1} D_\alpha$. Il existe donc des éléments λ_{ij} de K^{nr} tels que :

$$x_{\alpha^{q^t}} = \sum_{0 \leq i \leq \delta - 1} \sum_{0 \leq j \leq t-1} \lambda_{ij} \phi^i (x_{\alpha^{q^j}}).$$

De la relation $\phi^\delta(x_{\alpha^{q^j}}) = u^s x_{\alpha^{q^j}}$ pour tout $0 \leq j \leq t$, on tire $\lambda_{ij} = 0$ si $i \neq 0$, et $\lambda_{0j}^{p^{r\delta}} = \lambda_{0j}$. Par conséquent, $x_{\alpha^{q^s}}$ s'écrit comme combinaison linéaire à coefficients dans $\mathbb{F}_{p^{r\delta}}$ des $x_{\alpha^{q^j}}$ pour $0 \leq j \leq \delta - 1$. On pose $\lambda_j = \lambda_{0j}$. Cette relation sur les $x_{\alpha^{q^j}}$ impose une relation analogue sur les α^{q^j}, car α apparaît comme coefficient constant de l'une des coordonnées de x_α dans une base de $D \otimes_K K^{\mathrm{nr}}$ (la même pour tous les α). On a donc :

$$\alpha^{q^t} = \lambda_0 \alpha + \cdots + \lambda_{t-1} \alpha^{q^{t-1}}.$$

Le ϕ-module D est déterminé par la donnée de sa pente ainsi que des éléments $(\lambda_0, \ldots, \lambda_{t-1})$. On pose $P = X^t - \sum_{i=0}^{t-1} \lambda_i X^i \in \mathbb{F}_{p^{r\delta}}[X, \phi]$.

Proposition 2.1.1. — *La représentation V associée à D est $V_{\delta,s,P}$.*

Démonstration. — Fixons α comme précédemment. Rappelons que x_α est construit à partir d'un $\xi_\alpha \in D \otimes_K K^{\mathrm{mr}}$ vérifiant $\phi(\xi_\alpha) = \xi_\alpha$, et que ξ_α se retrouve à partir de x_α *via* la formule :

$$\xi_\alpha = u^{-\frac{s}{p^{r\delta}-1}} x_\alpha + \cdots + u^{-\frac{sp^{r(\delta-1)}}{p^{r\delta}-1}} \phi^{\delta-1}(x_\alpha).$$

Cette écriture plus le fait que $\phi(\xi_\alpha) = \xi_\alpha$ montre que $\xi_\alpha \in (D_\alpha \otimes_{K(\alpha)} K^{\mathrm{sep}})^{\phi=1}$, qui est une représentation de I_t isomorphe à la représentation associée à D_α, notée V_α. Munissons V_α d'une structure de $\mathbb{F}_{p^{r\delta}}$-espace vectoriel par la formule suivante : si $\mu \in \mathbb{F}_{p^{r\delta}}$, $\mu \cdot \xi_\alpha = \sum_{i=0}^{\delta-1} \mu^{p^{ri}} u^{-\frac{sp^{ri}}{p^{r\delta}-1}} \phi^i(x_\alpha)$, puis par $\mu g \xi_\alpha = g(\mu \xi_\alpha)$ si $g \in I_t$. Comme V_α est irréductible, cela munit bien tout V_α d'une structure de $\mathbb{F}_{p^{r\delta}}$. Cette action est coïncide sur $\mathbb{F}_{p^r}$ avec la structure naturelle de $\mathbb{F}_{p^r}$-espace vectoriel de V_α, et si $\gamma \in I_t$, on a $\gamma \cdot \xi_\alpha = \omega_{r\delta}^h(\gamma) \cdot \xi_\alpha$. Cette structure identifie donc chaque élément de $\mathbb{F}_{p^{r\delta}}$ à un élément de $\mathrm{End}_{I_t}(V_\alpha)$.
Par ailleurs, σ agit sur V, et cette action vérifie $\sigma \xi_\alpha = \xi_{\alpha^q}$. Un calcul immédiat utilisant l'expression de ξ_α dans D_α et la relation entre les $x_{\alpha^{q^j}}$, montre que

$$\sigma^t \xi_\alpha = \sum_{j=0}^{t-1} \lambda_j \xi_{\alpha^{q^j}},$$

avec les mêmes λ_j que précédemment. Cela donne bien la description annoncée pour V. $\square$

Remarque 2.1.2. — Pour déterminer complètement la semi-simplifiée de la représentation associée à un ϕ-module algorithmiquement, il serait intéressant de pouvoir déterminer ces λ_i. Cela est assez facile si on s'autorise à calculer dans $\mathbb{F}_q(\alpha)$. En effet, il suffit alors de calculer une relation de dépendance linéaire sur $\mathbb{F}_{p^{r\delta}}$ minimale entre les α^{q^j}. Malheureusement, une telle approche n'est pas efficace ($\mathbb{F}_q(\alpha)$ est *a priori* de degré exponentiel en δ sur $\mathbb{F}_q$).

2.2. Le cas des $\overline{\mathbb{F}}_p$-représentations. — Ce point de vue est en quelque sorte l'opposé du précédent : cette fois, c'est le corps des coefficients qui est grand. On suppose que $K = \mathbb{F}_p(\!(u)\!)$, et on s'intéresse aux $\mathbb{F}_{p^r}$-représentations de G_K avec $\mathbb{F}_q \subset \mathbb{F}_{p^r}$. On suppose dans cette partie que $\sigma = \mathrm{id}$ et que $b = q$. On a alors une anti-équivalence de catégories entre la catégorie des $\mathbb{F}_{p^r}$-représentations de G_K et celle des ϕ-modules étales sur K munis d'une action de $\mathbb{F}_{p^r}$ commutant à celle de ϕ. La donnée d'un tel ϕ-module est exactement la même que celle d'un ϕ-module étale sur $\mathbb{F}_{p^r}(\!(u)\!)$, l'action de ϕ étant celle donnée préalablement. Nous savons que les ϕ-modules simples sur $\overline{\mathbb{F}}_p(\!(u)\!)$ sont de la forme $D(d, s, \lambda)$ avec $\lambda \in \overline{\mathbb{F}}_p^\times$. Nous allons calculer la représentation associée à cet objet.

Lemme 2.2.1. — *Soient $d \in \mathbb{N}^*$, $s \in \mathbb{Z}$, et $\lambda \in \overline{\mathbb{F}}_p^\times$. On note $q = p^a$. Alors la représentation de G_K associée à $D(d, s, \lambda^d)$ est :*

$$\left(ind\, {}^{G_K}_{G_{\mathbb{F}_{q^d}(\!(u)\!)}} \omega_{ad}^s \right) \otimes \chi_\lambda,$$

où χ_λ est le caractère non ramifié envoyant le Frobenius sur λ.

Démonstration. — Rappelons que le foncteur réalisant l'équivalence de catégories précédente est $D \mapsto V(D) = \mathrm{Hom}_{K,\phi}(D, K^{\mathrm{sep}})$, $V(D)$ étant muni de l'action de $\overline{\mathbb{F}}_p$ héritée de celle sur D par la formule $\lambda \cdot f(x) = f(\lambda x)$. Remarquons tout d'abord que $D(d, s, \lambda^d) \simeq D(d, s, 1) \otimes D_\lambda$, où D_λ est le ϕ-module défini par $D_\lambda = Ke$ avec $\phi(e) = \lambda e$. Comme la représentation associée à D_λ est χ_λ, et que l'équivalence de catégories précédente est une $\otimes$-équivalence de catégories, il nous suffit de montrer le résultat pour $\lambda = 1$. On suppose dorénavant que $D = D(d, s, 1)$. Si on note $(e_1, \ldots, e_d)$ la base canonique de D, alors un élément $f \in V$ est entièrement déterminé par l'application $\xi_f : \overline{\mathbb{F}}_p \to K^{\mathrm{sep}}$ définie par $\xi_f(\alpha) = f(\alpha e_0)$. En effet, on a alors pour $1 \leq i \leq d-1$, $f(\alpha e_i) = \phi^i(f(\alpha e_1)) = \xi_f(\alpha)^{q^i}$. De plus, l'application $f \mapsto \xi_f$ est un isomorphisme de représentations de V sur l'ensemble $W = \{\ \xi : \overline{\mathbb{F}}_p \to K^{\mathrm{sep}}$ telles que $\xi(\alpha)^{q^d} = u^s \xi(\alpha)$ pour tout $\alpha \in \overline{\mathbb{F}}_p\}$(l'action de G_K provenant de son action sur K^{sep}). Soit F un supplémentaire de $\mathbb{F}_{q^d}$ dans $\overline{\mathbb{F}}_p$, et soit π la projection de $\overline{\mathbb{F}}_p$ sur $\mathbb{F}_{q^d}$ correspondante. On note ξ l'application définie sur $\overline{\mathbb{F}}_p$ par $\xi(\alpha) = \pi(\alpha) u^{\frac{s}{q^d-1}}$. Alors $\xi \in W$, et on note W_0 le sous-$\overline{\mathbb{F}}_p$-espace vectoriel engendré par ξ.

Ce sous-espace est stable sous l'action de $G_{\mathbb{F}_{q^d}(\!(u)\!)}$, et $G_{\mathbb{F}_{q^d}(\!(u)\!)}$ agit sur W_0 par ω_{ad}^s. Comme V est irréductible, le critère de MacKey montre que $\mathrm{ind}_{G_{\mathbb{F}_{q^d}(\!(u)\!)}}^{G_K} W_0 = V$. □

Ainsi, en partant d'un ϕ-module quelconque, pour déterminer la semi-simplifiée de la représentation associée, il suffit de calculer une suite de composition du ϕ-module en utilisant l'algorithme du chapitre III, puis d'utiliser le lemme précédent pour connaître les facteurs de composition de la représentation associée.

IV.3. Modules de Kisin et modules de Wach en caractéristique p

Les ϕ-modules sur $k(\!(u)\!)$ apparaissent, comme on l'a vu, dans l'étude des représentations du groupe de Galois absolu de $k(\!(u)\!)$. Dans cette partie, nous commençons par détailler cette approche, en montrant comment on peut déterminer la semi-simplifiée de la représentation modulo p associée à un ϕ-module sur $k(\!(u)\!)$. Par ailleurs, l'une des utilisations les plus intéressantes des ϕ-modules sur $k(\!(u)\!)$ ou $k[\![u]\!]$ réside dans l'application l'étude des représentations de groupes de Galois p-adiques, par l'intermédiaire de la théorie de Hodge p-adique. Nous allons aussi voir comment les calculs de décomposition précédents fournissent des invariants de telles représentations.

3.1. Modules de Kisin. — L'approche des modules de Kisin, bien que moins habituelle que celle des (ϕ, Γ)-modules (présentée au paragraphe suivant), est la mieux adaptée à notre problème.

Soit $\mathcal{K}$ une extension finie de $\mathbb{Q}_p$, dont le corps résiduel est k, et soit $(\pi_n)_{n\geq 0}$ une suite compatible de racines p^n-èmes de l'uniformisante. Pour tout $n \geq 0$, on note $\mathcal{K}'_n = \mathcal{K}(\pi_n)$. On pose $\mathcal{K}'_\infty = \bigcup_{n\geq 0} \mathcal{K}'_n$. On fixe une clôture algébrique $\overline{\mathcal{K}}$ de $\mathcal{K}$ contenant $\mathcal{K}'_\infty$. On appelle G_∞ le groupe $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K}'_\infty)$. Notons que la théorie du corps des normes (voir [**Win83**]) montre que $G_\infty \simeq G_{k(\!(u)\!)}$. Rappelons que l'action du sous-groupe d'inertie sauvage I_p de $G_\mathcal{K}$ est triviale sur les $\mathbb{F}_p$-représentations irréductibles de $G_\mathcal{K}$. Par ailleurs, on a $G_\infty/(G_\infty \cap I_p) \simeq G_\mathcal{K}/I_p$, donc les représentations irréductibles de $G_\mathcal{K}$ sont les mêmes que les représentations irréductibles de G_∞. En particulier, la semi-simplifiée d'une $\mathbb{F}_p$-représentation de $G_\mathcal{K}$ ne dépend que de sa restriction à G_∞, et les poids de l'inertie modérée de cette représentation sont donnés par les poids de l'inertie modérée de la représentation de $G_{k(\!(u)\!)}$ correspondante. En fait, si V est une $\mathbb{Q}_p$-représentation de $G_\mathcal{K}$, le choix d'un réseau $T \subset V$ fournit, par réduction modulo p, une $\mathbb{F}_p$-représentation de $G_\mathcal{K}$ (dont la semi-simplifiée ne dépend pas du choix de réseau par le théorème de Brauer-Nesbitt). Par ailleurs, Kisin (voir [**Kis06**], Lemma 2.1.15) construit un foncteur qui associe à chaque réseau stable par G_∞ dans une telle représentation V un ϕ-module sur $\mathfrak{S} = W(k)[[u]]$ (ici, ϕ agit comme le Frobenius sur $W(k)$, et comme $u \mapsto u^p$ sur u, et un ϕ-module est simplement un $\mathfrak{S}$-module libre de rang

fini muni d'un endomorphisme ϕ-semi-linéaire). La représentation de $G_{k(\!(u)\!)}$ correspondant à la réduction modulo p de ce ϕ-module n'est autre que la réduction modulo p du réseau de départ.

3.2. Modules de Wach. — Soit $\mathcal{K}$ une extension finie de $\mathbb{Q}_p$, dont le corps résiduel est k, et soit $(\varepsilon_n)_{n\geq 0}$ une suite compatible de racines primitives p^n-èmes de l'unité. Pour tout $n \geq 0$, on note $\mathcal{K}_n = \mathcal{K}(\varepsilon_n)$. On pose $\mathcal{K}_\infty = \bigcup_{n\geq 0} \mathcal{K}_n$. On fixe une clôture algébrique $\overline{\mathcal{K}}$ de $\mathcal{K}$ contenant $\mathcal{K}_\infty$. Le groupe $H_\mathcal{K}$ est, par définition, $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K}_\infty)$. C'est un sous-groupe distingué de $G_\mathcal{K}$, on note $\Gamma = G_\mathcal{K}/H_\mathcal{K}$. La théorie des (ϕ, Γ)-modules permet de comprendre les représentations de $G_\mathcal{K}$, en voyant une telle représentation comme la donnée d'une représentation de $H_\mathcal{K}$ munie d'une action de Γ, puis en voyant une représentation de $H_\mathcal{K}$ comme représentation de $G_{k(\!(u)\!)}$ par l'intermédiaire de la théorie du corps des normes. On obtient alors un ϕ-module sur $\mathcal{K}$ muni d'une action de Γ. La théorie des modules de Wach, initiée par Wach puis largement étudiée par Berger, permet l'étude des représentations p-adiques cristallines de $G_\mathcal{K}$. On munit $k[\![u]\!]$ de son Frobenius naturel ϕ, et de l'action de Γ donnée par la formule suivante : pour $\gamma \in \Gamma$, $\gamma u = (1+u)^{\chi(\gamma)} - 1$ (où χ désigne le caractère cyclotomique).

Définition 3.2.1. — On appelle *module de Wach* sur k la donnée d'un $k[\![u]\!]$-module libre de rang fini N, muni d'un opérateur ϕ et d'une action de Γ, ayant les propriétés suivantes :
- les actions de ϕ et Γ sur N sont semi-linéaires par rapport aux actions correspondantes sur $k[\![u]\!]$;
- les actions de ϕ et Γ commutent ;
- il existe $r \geq 0$ tel que le sous-$k[\![u]\!]$-module de N engendré par l'image de ϕ contient $u^{(p-1)r}N$.

Étant donnée une représentation de $G_\mathcal{K}$, on peut lui associer (ϕ, Γ)-module (si elle est cristalline, on peut directement lui associer un module de Wach). On peut réduire ce (ϕ, Γ)-module modulo p, ce qui donne un (ϕ, Γ)-module sur $k(\!(u)\!)$. La représentation correspondante est la réduction modulo p d'un réseau stable dans la représentation cristalline de départ. Par ailleurs, il existe dans le (ϕ, Γ)-module modulo p des modules de Wach. Nous allons maintenant montrer comment récupérer les poids de l'inertie modérée de la représentation associée à ce (ϕ, Γ)-module à partir de la donnée d'un module de Wach sur k à l'intérieur de ce (ϕ, Γ)-module. Tout d'abord, soient ω_d le caractère de Serre de niveau d de $G_{\mathbb{Q}_{p^d}}$, et $h \in \mathbb{Z}$. Soit V est la $\mathbb{F}_p$-représentation induite par ω_d^h à $G_{\mathbb{Q}_p}$, alors le (ϕ, Γ)-module associé est donné dans une bonne base par (voir [**Ber09**], Proposition

10.2.2) :

$$\mathrm{Mat}(\phi) = \begin{pmatrix} 0 & \cdots & \cdots & \pm u^{h(p-1)} \\ 1 & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \vdots \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\mathrm{Mat}(\gamma) = \begin{pmatrix} \lambda_\gamma^{\frac{h(p-1)}{(p^d-1)}} & 0 & \cdots & 0 \\ 0 & \lambda_\gamma^{\frac{hp(p-1)}{(p^d-1)}} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \lambda_\gamma^{\frac{hp^{d-1}(p-1)}{(p^d-1)}} \end{pmatrix},$$

où $\lambda_\gamma = \frac{\omega_1(\gamma)u}{\gamma(u)}$.

Dans cette base, les poids de l'inertie modérée de la représentation sont déterminés par $h \pmod{p^d-1}$. Remarquons que lorsque $\mathcal{K}/\mathbb{Q}_p$ est non ramifiée, la théorie de Fontaine-Laffaille montre que les poids de l'inertie modérée sont exactement les poids de Hodge-Tate de la représentation.

On rappelle que si $d \in \mathbb{N}^*$, $s \in \mathbb{Z}$, on note $D(d,s)$ le ϕ-module sur $k(\!(u)\!)$ dont une base est $(e_0, \ldots, e_{d-1})$, l'application ϕ étant donnée par $\phi(e_i) = e_{i+1}$ pour $0 \leq i \leq d-2$, et $\phi(e_{d-1}) = u^s e_0$. Lorsqu'on considère $D(d,s)$, on fixe une telle base, que l'on appelle base canonique de $D(d,s)$.

Proposition 3.2.2. — *On suppose $p \neq 2$. Soit s un entier divisible par $p-1$, alors il existe $p-1$ façons de munir $D(d,s)$ d'une structure de (ϕ,Γ)-module. Si on note $(e_0, \ldots, e_{d-1})$ la base canonique de $D(d,s)$, et si on note θ la solution de l'équation $\phi^d(\theta) = \left(\frac{\gamma(u)}{u}\right)^s \theta$ dont le coefficient constant (en tant que série formelle) est 1, alors les actions de γ correspondantes sont données par $\gamma(e_i) = a\theta^{p^i} e_i$, avec $a \in \mathbb{F}_p^\times$.*

Démonstration. — Le cas $d = 1$ est facile, on suppose donc $d \geq 2$. Soit $(e_0, \ldots, e_{d-1})$ la base canonique de $D(d,s)$. Supposons donnée une action de γ munissant D d'une structure de (ϕ,Γ)-module. On pose $x_i = \theta^{-p^i}\gamma(e_i)$. On a alors $\phi^d(x_0) = u^s x_0$.

Écrivons $x_0 = \sum_{i=0}^{d-1} a_i e_i$, avec $a_i \in \overline{\mathbb{F}}_p(\!(u)\!)$. Nous allons montrer que $a_i = 0$ si $i \neq 0$. Remarquons tout d'abord que la relation $\phi^d(x_0) = u^s x_0$ impose que pour tout $0 \leq i \leq d-1$ tel que $a_i \neq 0$, $\frac{\phi^d(a_i)}{a_i} = u^{(p^i-1)s}$. Cela impose que si $a_i \neq 0$, $v(a_i) = \frac{p^i-1}{p^d-1}s$, qui doit donc être entier. Soit δ le plus petit entier strictement positif tel que $\frac{p^\delta-1}{p^d-1}s \in \mathbb{Z}$. Alors $\{j \in \mathbb{Z} \mid \frac{p^j-1}{p^d-1}s \in \mathbb{Z}\} = \delta\mathbb{Z}$. En effet, soit j un entier tel que $\frac{p^j-1}{p^d-1}s \in \mathbb{Z}$, écrivons $j = m\delta + r$

la division euclidienne de j par δ. On a alors

$$\frac{p^{m\delta+r}-1}{p^d-1}s = \frac{p^{m\delta}(p^r-1)}{p^d-1}s + \frac{(p^\delta-1)(1+p^\delta+\cdots+p^{\delta(m-1)})}{p^d-1}s,$$

donc $\frac{p^{m\delta}(p^r-1)}{p^d-1}s \in \mathbb{Z}$. Comme $p^{m\delta}$ et p^d-1 sont premiers entre eux, $\frac{p^r-1}{p^d-1}s \in \mathbb{Z}$, ce qui montre que $r=0$.

Soit maintenant $j \in \delta\mathbb{Z}$, montrons que les solutions de $\phi^d(a_j) = u^{p^j-1}a_j$ sont les éléments de la forme $a_j = \lambda_j u^{\frac{p^j-1}{p^d-1}s}$, avec $\lambda_j \in \overline{\mathbb{F}_p}$. Il est clair qu'un tel élément est solution. Réciproquement, si a_j est une solution non nulle, alors $v(a_j) = \frac{p^j-1}{p^d-1}s$, et il existe $\lambda \in \overline{\mathbb{F}}_p$ tel que $v(a_j - \lambda u^{\frac{p^j-1}{p^d-1}s}) > \frac{p^j-1}{p^d-1}s$. Comme $a_j - \lambda u^{\frac{p^j-1}{p^d-1}s}$ est solution de la même équation, il est nécessairement nul.

Les considérations précédentes montrent donc qu'il existe un entier t et des $\lambda_j \in \overline{\mathbb{F}}_p$ tels que :

$$\gamma e_0 = \theta x_0 = \sum_{j=0}^{t-1} a_j e_{\delta j},$$

avec $\delta t \leq d$ et $a_j = \lambda_j \theta u^{\frac{p^j-1}{p^d-1}s}$.

On pose pour tout $i \in \mathbb{N}$, $e_i = \phi^i(e_0)$ (cela nous permettra de simplifier les calculs dans un premier temps). Nous allons exprimer le fait que $\gamma^{p-1} = \mathrm{id}$. On a déjà, pour tout $i \in \mathbb{N}$,

$$\gamma e_i = \sum_{j=0}^{t-1} \phi^i(a_j) e_{\delta j+i}.$$

On a donc l'égalité :

$$\gamma^2(e_0) = \sum_{j_1=0}^{t-1} \gamma(a_{j_1}) \sum_{j_2=0}^{t-1} \phi^{\delta j_1}(a_{j_2}) e_{\delta(j_1+j_2)}.$$

Par récurrence, on montre alors que :

$$\gamma^{p-1}e_0 = \sum_{j_1=0}^{t-1} \cdots \sum_{j_{p-1}=0}^{t-1} \gamma^{p-2}(a_{j_1})\phi^{\delta j_1}(\gamma^{p-3}(a_{j_2}))\cdots\phi^{\delta(j_1+\cdots+j_{p-1})}(a_{j_{p-1}})e_{\delta(j_1+\cdots+j_{p-1})}.$$

Si $(j_1,\ldots,j_{p-1}) \in \{0,\ldots t-1\}^{p-1}$, on note

$$\alpha_{j_1,\ldots j_{p-1}} = \gamma^{p-2}(a_{j_1})\phi^{\delta j_1}(\gamma^{p-3}(a_{j_2}))\cdots\phi^{\delta(j_1+\cdots+j_{p-1})}(a_{j_{p-1}}).$$

On vérifie alors que si $\alpha_{j_1,\ldots,j_{p-1}} \neq 0$, on a $v(\alpha_{j_1,\ldots,j_{p-1}}) = \frac{s}{p^d-1}(p^{\delta(j_1+\cdots+j_{p-1})}-1)$. Par ailleurs, si $\delta(j_1+\cdots+j_{p-1}) = md+r$ est la division euclidienne de $\delta(j_1+\cdots+j_{p-1})$ par d, alors $e_{\delta(j_1+\cdots+j_{p-1})} = u^{p^m s}e_r$. Soient maintenant $(j_1,\ldots j_{p-1})$ et $(j'_1,\ldots,j'_{p-1})$ deux tels $(p-1)$-uplets d'entiers. On suppose que $j_1+\cdots+j_{p-1} < j'_1+\cdots+j'_{p-1}$. Nous allons vérifier qu'alors, $v(\alpha_{j_1,\ldots,j_{p-1}}) + p^m s \neq v(\alpha_{j'_1,\ldots,j'_{p-1}}) + p^{m'}s$, où m et m' sont les quotients

respectifs des divisions euclidiennes de $\delta(j_1+\cdots+j_{p-1})$ et de $\delta(j'_1+\cdots+j'_{p-1})$ par d. Supposons donc qu'il y ait égalité, on a alors :

$$v(\alpha_{j_1,\ldots,j_{p-1}})-v(\alpha_{j'_1,\ldots,j'_{p-1}})=s(p^{m'}-p^m).$$

Cette égalité s'écrit encore $p^{\delta(j_1+\cdots+j_{p-1})}-p^{\delta(j'_1+\cdots+j'_{p-1})}=(p^d-1)(p^{m'}-p^m)$. Comme $\delta(j_1+\cdots+j_{p-1})<\delta(j'_1+\cdots+j'_{p-1})$, la valuation p-adique du membre de gauche de cette égalité est $\delta(j_1+\cdots+j_{p-1})$. Comme $m\leq m'$, la valuation p-adique du membre de droite est $+\infty$ (si $m=m'$) ou m. Le premier cas étant impossible, on a nécessairement $m=\delta(j_1+\cdots+j_{p_1})$. Comme $d\geq 2$ et que m est le quotient de la division de $\delta(j_1+\cdots+j_{p-1})$ par d, on a nécessairement $m=0$, et par suite tous les j_i sont nuls. Mais alors, on obtient $1-v(\alpha_{j'_1,\ldots,j'_{p-1}})=(p^d-1)(p^{m'}-1)$, qui à son tour impose que tous les j'_i sont nuls. C'est une contradiction, ce qui prouve notre affirmation.

Remarquons maintenant que, si on note pour éviter les confusions $m_{j_1,\ldots,j_{p-1}}$ le quotient de la division de $\delta(j_1+\cdots+j_p)$ par d, le calcul précédent de $\gamma^{p-1}e_0$ se récrit :

$$\gamma^{p-1}e_0=\sum_{r=0}^{d-1}\left(\sum_{\delta(j_1+\cdots+j_{p-1})\equiv r[d]}\alpha_{j_1,\ldots,j_{p-1}}u^{p^{m_{j_1,\ldots,j_{p-1}}}s}\right)e_r.$$

Pour $r\in\{0,\ldots,d-1\}$ fixé, les termes (non nuls) intervenant dans la somme

$$\sum_{\delta(j_1+\cdots+j_{p-1})\equiv r[d]}\alpha_{j_1,\ldots,j_{p-1}}u^{p^{m_{j_1,\ldots,j_{p-1}}}s}$$

sont tous de valuations distinctes. On sait que $\gamma^{p-1}e_0=e_0$. Cela impose que pour $r=0$, on a $\sum_{\delta(j_1+\cdots+j_{p-1})\equiv 0[d]}\alpha_{j_1,\ldots,j_{p-1}}u^{p^{m_{j_1,\ldots,j_{p-1}}}s}=1$. Cette somme a un seul terme de valuation 0, qui est $\alpha_{0,0,\ldots,0}=\lambda_0^{p-1}\theta\gamma(\theta)\cdots\gamma^{p-2}(\theta)=\lambda_0^{p-1}$. On doit donc avoir λ_0^{p-1} d'une part, et $\alpha_{j_1,\cdots,j_{p-1}}=0$ d'autre part si les j_i sont non tous nuls.

Par ailleurs, pour $r\neq 0$, on a $\sum_{\delta(j_1+\cdots+j_{p-1})\equiv r[d]}\alpha_{j_1,\ldots,j_{p-1}}u^{p^{m_{j_1,\ldots,j_{p-1}}}s}=0$, ce qui impose aussi que les $\alpha_{j_1,\ldots,j_{p-1}}$ sont tous nuls. Le cas $r=1$ impose alors que a_1 soit nul. On montre alors par récurrence que tous les a_i $(i\geq 1)$ sont nuls. En conclusion, il existe $\lambda_0\in\mathbb{F}_p^\times$ tel que $\gamma e_0=\lambda_0\theta e_0$, c'est-à-dire que $\gamma(\phi^i(e_0))=\lambda_0\theta^{p^i}\phi^i(e_0)$ pour $0\leq i\leq d-1$. □

Lemme 3.2.3. — *Soient D un ϕ-module simple sur $\overline{\mathbb{F}}_p((u))$ et $D_0=D(d_0,s_0,\mu_0)$ un ϕ-module sur $\overline{\mathbb{F}}_p((u))$ muni d'une action de Γ qui en fait un (ϕ,Γ)-module simple. On suppose que D est un sous-ϕ-module de D_0. Soient d,s,μ tels que $D\simeq D(d,s,\mu)$, et soit $a=\frac{p-1}{pgcd(p-1,s)}$. On note α une racine primitive a-ème de l'unité. Alors $D_0\simeq\bigoplus_{i=0}^{a-1}D(d,s,\mu\alpha^i)$, et $\mu^a=\mu_0$.*

Démonstration. — Comme $D\subset D_0$ et comme $D+\gamma D+\cdots+\gamma^{p-2}D=D_0$, D_0 est isocline de même pente que D. Comme D est simple, d divise d_0. Soit $m=d_0/d$. Puisque $m\leq p-1$,

le lemme III1.1.2 montre que $D_0 \simeq \bigoplus_{i=0}^{m-1} D(d,s,\mu\beta^i)$, avec β une racine primitive m-ème de l'unité. Par ailleurs, pour tout $0 \leq i \leq a-1$, le sous-ϕ-module de D_0 engendré par $\gamma^i D$ est isomorphe à $D(d,s,\mu\omega(\gamma)^{si})$, donc les quotients de Jordan-Hölder du ϕ-module D_0 sont les $D(d,s,\mu\omega(\gamma)^{si})$. Ainsi, $m=a$, et la conclusion en découle. □

Lemme 3.2.4. — *Soient $d \in \mathbb{N}$, $s \in (p-1)\mathbb{Z}$, et $\mu \in \overline{\mathbb{F}}_p$. Soit D un (ϕ,Γ)-module sur $\overline{\mathbb{F}}_p(\!(u)\!)$. On suppose qu'il existe $e_0 \in D$ non nul tel que $\phi^d(e_0) = u^s e_0$. Alors, D admet un sous-(ϕ,Γ)-module simple dont le ϕ-module sous-jacent est de la forme $D(d,s,\mu)$.*

Démonstration. — Soit $\theta \in \overline{\mathbb{F}}_p(\!(u)\!)$ tel que $\phi^d(\theta) = \left(\frac{\gamma u}{u}\right)^s \theta$ et dont le coefficient constant est 1. Nous allons montrer qu'il existe $x \neq 0$ dans D tel que $\phi^d(x) = u^s x$ et $\gamma(x) = \varepsilon^{-1}\theta x$ pour un certain $\varepsilon \in \mathbb{F}_p^\times$. Pour $\varepsilon \in \mathbb{F}_p^\times$, on pose

$$x_\varepsilon = e_0 + \varepsilon\theta^{-1}\gamma(e_0) + \varepsilon^2\theta^{-1}\gamma(\theta^{-1})\gamma^2(e_0) + \cdots + \varepsilon^{p-2}\theta^{-1}\cdots\gamma^{p-3}(\theta^{-1})\gamma^{p-2}(e_0).$$

D'une part, du fait que $\theta\gamma(\theta)\ldots\gamma^{p-1}(\theta) = 1$, on a $\varepsilon\theta^{-1}\gamma(x_\varepsilon) = x_\varepsilon$. D'autre part, pour $0 \leq i \leq p-2$, on a :

$$\phi^d(\theta^{-1}\cdots\gamma^{i-1}(\theta^{-1})\gamma^i(e_0)) = \left(\frac{u}{\gamma(u)}\frac{\gamma(u)}{\gamma^2(u)}\cdots\frac{\gamma^{i-1}(u)}{\gamma^i(u)}\right)^s \gamma^i(u)^s\gamma^i(e_0) = u^s\gamma^i(e_0).$$

Ainsi, on a $\phi^d(x_\varepsilon) = u^s x_\varepsilon$. Il nous reste à vérifier que l'un des x_ε est non nul. Il suffit pour cela de remarquer que $\sum_{\varepsilon\in\mathbb{F}_p^\times} x_\varepsilon = -e_0$. □

Il nous reste donc à voir comment calculer un sous-module de Wach dont le ϕ-module sous-jacent soit isocline à l'intérieur d'un module de Wach donné.

Lemme 3.2.5. — *Soient $\mathfrak{D}_1, \mathfrak{D}_2$ deux ϕ-modules sur $\overline{\mathbb{F}}_p[\![u]\!]$, et soit $f : \mathfrak{D}_1 \to \mathfrak{D}_2$ un morphisme de ϕ-modules. On note $g = \gamma(\mathfrak{D}_1)$ (la plus grande valuation d'un diviseur élémentaire de l'inclusion $\mathfrak{D}_1 \hookrightarrow \langle\phi(\mathfrak{D}_1)\rangle$), et ν un entier strictement plus grand que $\frac{g}{p-1}$. On suppose que $f(\mathfrak{D}_1) \subset u^\nu\mathfrak{D}_2$. Alors $f = 0$.*

Démonstration. — Quitte à quotienter $\mathfrak{D}_1$ par le noyau de f, on peut supposer que f est injective, et donc que $\mathfrak{D}_1 \subset \mathfrak{D}_2$. On est alors ramené à démontrer que $\mathfrak{D}_1 = 0$. On suppose $\mathfrak{D}_1 \neq 0$. Soit $(e_1,\ldots,e_n)$ une base de $\mathfrak{D}_2$ adaptée à l'inclusion $\mathfrak{D}_1 \subset \mathfrak{D}_2$, c'est-à-dire telle qu'il existe des entiers $\mu_1 \leq \cdots \leq \mu_s$ tels que $(u^{\mu_1}e_1,\ldots,u^{\mu_s}e_s)$ soit une base de $\mathfrak{D}_1$, avec $1 \leq s \leq n$. Par hypothèse, on a $\nu \leq \mu_1$. Écrivons maintenant $\phi(e_1) = \sum_{i=1}^d a_i e_i$ avec les $a_i \in \overline{\mathbb{F}}_p[\![u]\!]$. Comme $\mathfrak{D}_1$ est stable par ϕ, $a_i = 0$ pour $i > s$. On a alors $\phi(u^{\mu_1}e_1) = \sum_{i=1}^s u^{b\mu_1}a_i e_i$. Par défintion de g, $\phi(u^{\mu_1}e_1) \notin u^{g+1}\mathfrak{D}_1$. Ainsi, il existe $1 \leq i \leq s$ tel que $(p-1)\mu_1 + v(a_i) \leq g$, et donc $\mu_1 \leq \frac{g}{p-1} < \nu$, ce qui n'est pas. Donc $\mathfrak{D}_1 = 0$. □

Soit $\mathfrak{N}$ un module de Wach sur $\overline{\mathbb{F}}_p[\![u]\!]$, et soit $\mathfrak{D} \subset \mathfrak{N}$ un sous-ϕ-module de $\mathfrak{N}$. On note $\nu = \nu(\mathfrak{D})$ le plus petit entier immédiatement supérieur à $\frac{g}{p-1}$ (où g est la plus grande valuation d'un diviseur élémentaire de l'inclusion $\mathfrak{D} \hookrightarrow \langle \phi(\mathfrak{D}) \rangle$). On fixe un générateur γ de Γ.

Proposition 3.2.6. — *Soit $(e_1, \ldots, e_d)$ une base de $\mathfrak{D}$ sur $\overline{\mathbb{F}}_p[\![u]\!]$. On suppose que $\mathfrak{N}/\mathfrak{D}$ est sans torsion, et que pour tout $1 \leq i \leq d$, il existe $y_i \in \mathfrak{D}$ tel que $\gamma(e_i) - y_i \in u^\nu \mathfrak{N}$. Alors $\mathfrak{D}$ est stable par Γ.*

Démonstration. — Soit π la projection canonique de $\mathfrak{N}$ sur $\mathfrak{N}/\mathfrak{D}$. L'hypothèse d'existence des y_i implique que pour tout $x \in \mathfrak{D}$, il existe $y \in \mathfrak{D}$ tel que $\gamma(x) - y \in u^\nu \mathfrak{N}$. Soit $\gamma(\mathfrak{D})$ l'image de $\mathfrak{D}$ par γ : c'est un sous-ϕ-module de $\mathfrak{N}$. On sait alors que $\pi(\gamma(\mathfrak{D})) \subset u^\nu \mathfrak{N}/\mathfrak{D}$. D'après le lemme 3.2.5, il nous suffit de montrer que $g(\mathfrak{D}) = g(\gamma(\mathfrak{D}))$, car ce lemme (appliqué à $\pi : \gamma(\mathfrak{D}) \to \mathfrak{N}/\mathfrak{D}$) impliquera alors que $\gamma(\mathfrak{D}) \subset \mathfrak{D}$, et donc que $\mathfrak{D}$ est stable par Γ.
On a en fait $\gamma(\mathfrak{D}) = \bigoplus_{i=1}^d \overline{\mathbb{F}}_p[\![u]\!]\gamma(e_i)$. En effet, si la base $(e'_1, \ldots, e'_d)$ de $\mathfrak{D}$ est adaptée à l'inclusion $\mathfrak{D} \hookrightarrow \langle \phi(\mathfrak{D}) \rangle$ (avec pour diviseurs élémentaires $(u^{\mu_1}, \ldots, u^{\mu_d})$, alors la base $(\gamma(e'_1), \ldots, \gamma(e'_d))$ est adaptée à l'inclusion $\gamma(\mathfrak{D}) \hookrightarrow \langle \phi(\gamma(\mathfrak{D})) \rangle$, et les diviseurs élémentaires correspondants sont $(\gamma(u)^{\mu_1}, \ldots, \gamma(u)^{\mu_d})$. □

Cette proposition ainsi que les explications précédentes montrent comment déterminer les poids de l'inertie modérée de la représentation associée à un (ϕ, Γ)-module $\mathfrak{N}$ sur $\overline{\mathbb{F}}_p[\![u]\!]$ d'une manière algorithmique. Il suffit alors de calculer un sous-ϕ-module simple $\mathfrak{D}_0$ en utilisant l'algorithme du chapitre III, puis de construire par récurrence une suite $(\mathfrak{D}_i)$ de sous-ϕ-modules de $\mathfrak{N}$, où $\mathfrak{D}_i$ se déduit de $\mathfrak{D}_{i-1}$ en y ajoutant les images par γ des vecteurs de base de $\mathfrak{D}_{i-1}$, tant que celles-ci ne sont pas toutes congrues modulo u^ν à des éléments de $\mathfrak{D}_{i-1}$, et en saturant $\mathfrak{D}_i$ de sorte que $\mathfrak{N}/\mathfrak{D}_i$ soit sans torsion.

3.3. Réduction des (ϕ, Γ)-modules. — On présente ici une ébauche d'algorithme pour la réduction des (ϕ, Γ)-modules sur $\overline{\mathbb{F}}_p(\!(u)\!)$, ainsi que le calcul de la semi-simplifiée de la représentation associée. On se donne un (ϕ, Γ)-module N de la manière suivante : on fixe une base de N, et on se donne la matrice G de ϕ dans cette base ainsi que la matrice M de γ dans la même base (on suppose que dans cette base, G et M sont à coefficients dans $\overline{\mathbb{F}}_p[\![u]\!]$). On note $\mathfrak{N}$ le sous-$\overline{\mathbb{F}}_p[\![u]\!]$-module engendré par les vecteurs de cette base. Soit g la plus grande valuation d'un diviseur élémentaire de G, et ν un entier strictement supérieur à $\frac{g}{p-1}$. Si $\dim N = d$, les matrices G et M peuvent être remplacées par leurs réductions modulo $u^{p(d+1)\nu}$.

Étape 1. — Calculer par l'algorithme de réduction des ϕ-modules un sous-ϕ-module $\mathfrak{D}$ de $\mathfrak{N}$, de sorte que $D = \mathfrak{D}[1/u]$ soit isomorphe à $D(d, s, \mu)$. Calculer $a = \frac{p-1}{\mathrm{pgcd}(p-1,s)}$ et remplacer $\mathfrak{D}$ par $\mathfrak{N} \cap (D + \gamma D + \cdots + \gamma^{a-1} D)$. Calculer une $\overline{\mathbb{F}}_p[\![u]\!]$-base $\mathcal{B}$ de $\mathfrak{N}$ adaptée à l'inclusion $\mathfrak{D} \subset \mathfrak{N}$.

Remarque 3.3.1. — Pour calculer $\mathfrak{N} \cap (D + \gamma D + \cdots + \gamma^{a-1} D)$, on se contente de déterminer une approximation d'une base de ce ϕ-module. Si $(e_0, \cdots, e_{\delta-1})$ est une base de $\mathfrak{D}$ au départ, on applique l'algorithme des diviseurs élémentaires à la famille des $\{\gamma^i(e_j)\}$ (qui est connue modulo $u^{2p\nu}$), et on obtient une base du nouveau $\mathfrak{D}$ connue modulo $u^{(p(d+1)-1)\nu}$.

Étape 2. — Si la matrice de γ dans la base $\mathcal{B}$ est congrue modulo u^ν à une matrice stabilisant $\mathfrak{D}$, passer à l'étape 3. Sinon, remplacer $\mathfrak{D}$ par $\mathfrak{N} \cap (D + \gamma^a D)$, calculer une $\overline{\mathbb{F}}_p[\![u]\!]$-base de $\mathfrak{N}$ adaptée à l'inclusion $\mathfrak{D} \subset \mathfrak{N}$ et $x_0 \in D$ vérifiant $\phi^{2ad}(x_0) = \mu^{2a} u^{\frac{(p^{2ad}-1)s}{p^{ad}-1}} x_0$ (quitte à remplacer s par un multiple de la forme $p^i s$, on peut supposer que $x_0 \in \mathfrak{D} \setminus u\mathfrak{D}$) et recommencer l'étape 2.

Remarque 3.3.2. — On procède comme à l'étape 1 pour calculer le nouveau $\mathfrak{D}$. À chaque passage dans l'étape 2, la perte de précision sur les vecteurs de base de $\mathfrak{D}$ est au plus u^ν. Comme le nombre de passages est $\leq p-1$, on obtient une approximation d'une base de $\mathfrak{D}$ à $u^{(pd+1)\nu}$ près.

Étape 3. — Déterminer $\theta \in \overline{\mathbb{F}}_p[\![u]\!]$, de coefficient constant 1, tel que $\phi^d(\theta) = \left(\frac{\gamma(u)}{u}\right)^s \theta$. Déterminer $\varepsilon \in \mathbb{F}_p^\times$ tel que

$$x_\varepsilon = x_0 + \varepsilon\theta^{-1}\gamma(x_0) + \cdots + \varepsilon^{p-2}\theta^{-1}\cdots\gamma^{p-3}(\theta^{-1})\gamma^{p-2}(x_0) \neq 0.$$

Il suffit de tester cette relation modulo u^ν. Calculer le sous-ϕ-module N_ε de N engendré par x_ε, c'est un (ϕ, Γ)-module simple. La représentation associée à N_ε est ind $\omega_{ad}^{s/p-1} \otimes \omega_\varepsilon \otimes \chi_\mu$, où ω_ε est la puissance du caractère cyclotomique modulo p envoyant γ sur ε et χ_μ est le caractère non ramifié envoyant le Frobenius sur μ.

Récurrence. — Calculer $\mathfrak{N}_\varepsilon = \mathfrak{N} \cap N_\varepsilon$. Déterminer les actions de ϕ et γ sur le quotient $\mathfrak{N}/\mathfrak{N}_\varepsilon$ et réappliquer l'algorithme à ce quotient.
Le calcul de $\mathfrak{N}_\varepsilon$ fait diminuer de ν la précision, la nouvelle base de $\mathfrak{N}$ est donc connue à $u^{pd\nu}$ près, et les actions de ϕ et γ sur $\mathfrak{N}/\mathfrak{N}_\varepsilon$ aussi. Comme $\dim \mathfrak{N}/\mathfrak{N}_\varepsilon < d$, on obtient par récurrence une base de $\mathfrak{N}$ déterminée à $u^{p\nu}$ près, dans laquelle le (ϕ, Γ)-module est réduit.

CHAPITRE V

OPTIMISATION DU THÉORÈME D'AX-SEN-TATE APPLIQUÉE À UN CALCUL DE COHOMOLOGIE GALOISIENNE

Ce chapitre reprend l'article Optimisation du théorème d'Ax-Sen-Tate et application à un calcul de cohomologie galoisienne p-adique, *publié aux* Annales de l'Institut Fourier ([**LB10**]).

V.1. Introduction

Soit p un nombre premier, k un corps parfait de caractéristique p, et $F = \mathrm{Frac}\ \mathrm{W}(k)$. Soit K une extension finie totalement ramifiée de F. On note $\mathcal{O}_K$ l'anneau des entiers de K, $\mathfrak{m}_K$ son unique idéal maximal, et π_K (ou π s'il n'y a pas de confusion possible) une uniformisante de K. L'indice de ramification de K sur F est noté e (c'est le degré de K sur F). Enfin, on note $\bar{K}$ une clôture algébrique de K, et C le complété de $\bar{K}$, auquel on étend la valuation de F notée v, et normalisée par $v(p) = 1$. Le théorème d'Ax-Sen-Tate dit que les points fixes de C sous l'action de $G = \mathrm{Gal}(\bar{K}/K)$ sont exactement les éléments de K. La démonstration d'Ax (voir [**Ax70**]) de ce théorème s'appuie sur le résultat suivant :

***Théorème V.1* (Ax).** — *Soit $x \in C$ et $A \in \mathbb{R}$. On suppose que pour tout $\sigma \in G$, $v(\sigma x - x) \geq A$. Alors, il existe $y \in K$ tel que $v(x - y) \geq A - \frac{p}{(p-1)^2}$.*

Ax pose sans y répondre la question de l'optimalité de la constante $\frac{p}{(p-1)^2}$ intervenant dans le théorème précédent, en précisant qu'une borne inférieure pour cette constante optimale est effectivement $\frac{1}{p-1}$. Pour traiter cette question nous introduisons ici la tour d'extensions K_m de K par les racines p^m-ièmes de l'uniformisante, et $K_\infty = \cup_{m \geq 0} K_m$. La première partie est consacrée à l'étude de l'extension K_∞/K. Dans sa démonstration du théorème d'Ax-Sen-Tate (voir [**Tat67**]), Tate présente des calculs de la cohomologie galoisienne à coefficients dans l'extension cyclotomique de K. Dans cet article, nous démontrons des résultats du même type lorsque K_∞ est une extension arithmétiquement profinie (APF) de K (intervenant dans les travaux de Fontaine et Wintenberger sur la théorie du corps des normes, voir [**Win83**]). Ces résultats s'appliquent à l'extension K_∞,

et une étude *ad hoc* de l'extension K_∞/K, qui constitue la partie essentiellement originale de cet article, nous permettra de démontrer le :

***Théorème V.2* (Théorème 2.3.1).** — *Soit $x \in C$ et $A \in \mathbb{R}$. Si on suppose que pour tout $\sigma \in G$, $v(\sigma x - x) \geq A$, alors, pour tout $m \in \mathbb{N}$, il existe $y_m \in K_m$ tel que $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$. Réciproquement, si pour tout $m \in \mathbb{N}$ il existe $y_m \in K_m$ tel que $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$, alors pour tout $\sigma \in G$, $v(\sigma x - x) \geq A$.*

Le cas particulier où $m = 0$ implique que la constante optimale dans le théorème d'Ax est $\frac{1}{p-1}$. Le cas $m = 1$ est utilisé par Caruso (voir [**Car09a**], théorème 3.5.4) pour prouver une formule de réciprocité explicite entre un (ϕ, N)-module filtré de torsion et la $\mathbb{F}_p$-représentation de G_K associée ; la version d'Ax du théorème, et même le cas $m = 0$ de notre théorème 2.3.1, s'avèrent insuffisants pour l'utilisation faite par Caruso dans le cas général.
La caractérisation donnée par le théorème nous permet en outre de décrire la structure de $H^1(G, \mathcal{O}_{\bar{K}})$. La deuxième partie est dédiée à cette étude. Nous redémontrons notamment un résultat dû à Sen (voir [**Sen69**], théorème 3) qui dit que si l'entier n vérifie $n \geq \frac{e}{p-1}$, alors $H^1(G, \mathcal{O}_{\bar{K}})$ est tué par π_K^n. Dans le cas où $K = F$, on montre que $H^1(G, \mathcal{O}_{\bar{K}})$ est isomorphe au sous-espace de $k^{\mathbb{N}}$ formée des suites vérifiant une relation de récurrence linéaire tordue par le Frobenius, introduites sous le nom de suites *twist-récurrentes* par Kedlaya dans le but de donner une description de $\bar{K}$. On donne finalement quelques indications pour obtenir une description analogue dans le cas ramifié, qui pourrait être le point de départ à un analogue en torsion de la théorie de Sen.

V.2. Optimisation du théorème d'Ax

Nous démontrons dans cette partie le théorème 2.3.1 de l'introduction. Nous introduisons l'extension de K par les racines d'ordre une puissance de p de π, que nous étudions à l'aide de la théorie des extensions APF. Nous étudions en détail les propriétés de K_∞, et nous en déduisons une caractérisation des éléments de K_∞ vérifiant une condition du type « Pour tout $\sigma \in G$, $v(\sigma x - x) \geq A$ ».

2.1. Extensions APF. — Soit K_∞ une extension infinie, arithmétiquement profinie (APF) (cf. [**Win83**], §1) de K. On se propose dans cette partie de décrire la cohomologie de $\mathrm{Gal}(\bar{K}/K_\infty)$ à coefficients dans C, en cherchant à généraliser les résultats de [**Tat67**] concernant l'extension cyclotomique de K. On utilise la numérotation supérieure des groupes de ramification, comme défini dans [**Ser68**], chap. IV. Pour $\mu \geq -1$, si M est

une extension finie de K, on pose

$$M^\mu = M \cap \bar{K}^{\mathrm{Gal}(\bar{K}/K)^\mu}.$$

Si e désigne l'indice de ramification absolu de K, on sait d'après **[Cola]**, proposition 3.22, que

$$v(\mathfrak{d}_{M/K}) = \frac{1}{e}\int_{-1}^{+\infty}\left(1 - \frac{1}{[M : M^\mu]}\right) d\mu.$$

Proposition 2.1.1. — *Soit L_∞ une extension galoisienne finie de K_∞. Alors $Tr_{L_\infty/K_\infty}(\mathcal{O}_{L_\infty}) \supset \mathfrak{m}_{K_\infty}$.*

Démonstration. — Suivant **[Win83]** §1, nous notons $(K_n)_{n\in\mathbb{N}}$ la tour des extensions élémentaires de K_∞ et nous définissons comme dans *loc. cit.* la suite μ_n comme la suite strictement croissante des $\mu \in \mathbb{R}_+$ tels que pour tout $\varepsilon > 0$,

$$\mathrm{Gal}(\bar{K}/K)^\mu \mathrm{Gal}(\bar{K}/K_\infty) \neq \mathrm{Gal}(\bar{K}/K)^{\mu+\varepsilon}\mathrm{Gal}(\bar{K}/K_\infty). \tag{5}$$

Quitte à remplacer K par l'un des K_n, on sait d'après **[Ser68]**, Chap V, §4, Lemme 6, qu'il existe une extension L de K telle que $L_\infty = LK_\infty$. On note pour tout $n \in \mathbb{N}$, $L_n = LK_n$. La configuration des extensions considérées est la suivante :

$$\begin{tikzcd}
 & L_n \arrow[d, dash] \\
K_n \arrow[ur, dash] \arrow[d, dash] & L_n^\mu \arrow[d, dash] \\
K_n^\mu \arrow[ur, dash] \arrow[d, dash] & L \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Suivons pas à pas la méthode de Colmez (**[Colb]**, 1.4.) : pour tout $\mu \geq -1$, $[K_n : K_n^\mu] = [K_nL_n^\mu : L_n^\mu]$ (car $K_n^\mu = K_n \cap L_n^\mu$). On a bien sûr $v(\mathfrak{d}_{L_n/K_n}) = v(\mathfrak{d}_{L_n/K}) - (\mathfrak{d}_{K_n/K})$. Ainsi, en appliquant la formule pour le calcul de la valuation de la différente, il vient :

$$\begin{aligned}
v(\mathfrak{d}_{L_n/K_n}) &= \frac{1}{e}\int_{-1}^{+\infty}\left(\frac{1}{[K_n : K_n^\mu]} - \frac{1}{[L_n : L_n^\mu]}\right) d\mu \\
&= \frac{1}{e[K_n : K]}\int_{-1}^{+\infty}[K_n^\mu : K]\left(1 - \frac{1}{[L_n : K_nL_n^\mu]}\right) d\mu.
\end{aligned}$$

Soit n_0 entier tel que $L^{n_0} = L$. Si $\mu \geq n \geq n_0$, alors $L^\mu = L \subset L_n^\mu$. Ainsi, $L_n = K_n L \subset K_n L_n^\mu$, c'est à dire $[L_n : K_n L_n^\mu] = 1$. Par conséquent,

$$\begin{aligned} e[K_n : K]v(\mathfrak{d}_{L_n/K_n}) &= \int_{-1}^{n_0} [K_n^\mu : K] \left(1 - \frac{1}{[L_n : K_n L_n^\mu]}\right) d\mu \\ &\leq \int_{-1}^{n_0} [K_n^\mu : K] d\mu, \end{aligned}$$

Pour $\mu \leq \mu_n$, et pour $m \leq n$, $K_n^\mu = K_m^\mu$. Comme K_∞/K est APF, μ_n tend vers $+\infty$, et on a pour n assez grand :

$$\int_{-1}^{n_0} [K_n^\mu : K] d\mu = \int_{-1}^{n_0} [K_{n_0}^\mu : K] d\mu,$$

qui est une constante. Par conséquent, $v(\mathfrak{d}_{L_n/K_n}) = O\left(\frac{1}{[K_n:K]}\right)$. On a alors ([**Ser68**], Chap V, §3, Lemme 4) :

$$v(Tr_{L_n/K_n}(\mathfrak{m}_{L_n})) = O([K_n : K]^{-1}),$$

et donc un élément de $\mathfrak{m}_{K_\infty}$ se trouve dans $Tr_{L_n/K_n}(\mathfrak{m}_{L_n})$ pour n assez grand, et par conséquent dans $Tr_{L_\infty/K_\infty}(\mathcal{O}_{L_\infty})$. □

Il résulte immédiatement de cette proposition qu'étant donné $\varepsilon > 0$, il existe $y_\varepsilon \in \mathcal{O}_L$ tel que $v(Tr_{L/K_\infty}(y_\varepsilon)) > \varepsilon$.

Corollaire 2.1.2. — *Soit L une extension galoisienne finie de K_∞ de groupe de Galois G, et soit $x \in L$ et $\varepsilon > 0$. Alors il existe $y \in L$ tel que*

$$v(x - Tr_{L/K_\infty}(y)) \geq \min_{\sigma \in G} v(\sigma x - x) - \varepsilon \text{ et } v(y) \geq v(x) - \varepsilon.$$

Démonstration. — Soit $y_\varepsilon \in \mathcal{O}_L$ tel que $v(Tr_{L/K_\infty}(y_\varepsilon)) > \varepsilon$, et soit $z = Tr_{L/K_\infty}(y_\varepsilon)$. On pose $y = \frac{1}{z} x y_\varepsilon$. Alors $v(y) \geq v(x) - \varepsilon$ et

$$Tr_{L/K\infty}(y) = \frac{1}{z} \sum_{\sigma \in G} \sigma(y_\varepsilon)\sigma(x) = \frac{1}{z} \sum_{\sigma \in G} \sigma(y_0)(\sigma x - x + x) = x + \frac{1}{z} \sum_{\sigma \in G} \sigma(y_0)(\sigma x - x).$$

Ainsi, $v(Tr_{L/K_\infty}(y) - x) \geq \min_{\sigma \in G} v(\sigma x - x) - \varepsilon$. □

Donnons au passage une proposition qui ne nous servira pas par la suite, mais qui découle directement du corollaire 2.1.2 en reprenant les arguments de [**Tat67**], dont elle généralise la proposition 10 aux extensions APF.

Proposition 2.1.3. — *Soit K_∞/K une extension APF, on note $\mathcal{H} = Gal(\bar{K}/K_\infty)$, et $\widehat{K_\infty}$ la fermeture de K_∞ dans C. Alors :*

$$H^0(\mathcal{H}, C) = \widehat{K_\infty} \text{ et } H^r(\mathcal{H}, C) = 0 \text{ pour } r \geq 1.$$

2.2. Etude de l'extension K_∞/K. — On peut maintenant appliquer le résultat précédent à une extension APF bien choisie. On définit $\pi_0 = \pi$, pour tout $n \in \mathbb{N}$, π_{n+1} une racine p-ième de π_n, $K_n = K(\pi_n)$, et $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$. L'extension K_∞, étudiée par Breuil dans [**Bre99b**] est APF. Nous redonnons ici une démonstration plus élémentaire (dans le sens ou elle n'a pas recours aux groupes de Lie p-adiques) de ce résultat, qui est le lemme 2.1.1 de *loc. cit.*

Proposition 2.2.1. — *L'extension K_∞/K est APF.*

Démonstration. — On sait que $v(\mathfrak{d}_{K_n/K}) = e(n+1) - \frac{e}{p^n}$. Un rapide calcul à partir de l'expression intégrale de $v(\mathfrak{d}_{K_n/K})$ et une récurrence immédiate montrent alors que pour tout $n \geq 1$, la famille $(\mu_n)_{n\in\mathbb{N}}$ étant définie comme en (5),

$$\mu_n = ne - 1 + \frac{pe}{p-1}.$$

La suite μ_n tend vers $+\infty$, il résulte de [**Win83**], 1.4.2. que K_∞/K est APF et que (K_n) est la tour d'extensions élémentaires de K_∞. □

On a le corollaire suivant :

Corollaire 2.2.2. — *Soit $\varepsilon > 0$, soit $x \in \bar{K}$ tel que pour tout $\sigma \in G$, $v(\sigma x - x) \geq A$. Il existe $y_\varepsilon \in K_\infty$ tel que $v(x - y_\varepsilon) \geq A - \varepsilon$.*

Démonstration. — On note M la clôture galoisienne de $K_\infty(x)$, alors $\mathrm{Gal}(\bar{K}/M)$ agit trivialement sur x, et donc pour tout $\sigma \in \mathrm{Gal}(M/K)$, $v(\sigma x - x) \geq A$, et en particulier pour tout $\sigma \in \mathrm{Gal}(M/K_\infty)$, $v(\sigma x - x) \geq A$. D'après le corollaire 2.1.2, il existe pour tout $\varepsilon > 0$ un $z_\varepsilon \in K_\infty$ tel que

$$v(x - z_\varepsilon) \geq A - \varepsilon \text{ et } v(z_\varepsilon) \geq v(x) - \varepsilon. \quad \square$$

Théorème 2.2.3. — *Soit $x \in K_\infty$. Les deux assertions suivantes sont équivalentes :*

(i) $\forall \sigma \in G = Gal(\bar{K}/K)$, $v(\sigma x - x) \geq A$

(ii) $\forall m \in \mathbb{N}$, $\exists y_m \in K_m$ *tel que* $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$.

En particulier, si x vérifie (i), il existe $y \in K$ tel que $v(x - y) \geq A - \frac{1}{p-1}$.

Démonstration. — Pour simplifier l'écriture, on notera $A_m = A - \frac{1}{p^m(p-1)}$.
$(i) \Rightarrow (ii)$. Soit $n \in \mathbb{N}$ tel que $x \in K_n \setminus K_{n-1}$. L'élément x s'écrit

$$x = \sum_{i=0}^{p^n-1} a_i \pi_n^i,$$

avec les a_i dans K. Pour $\sigma \in G$, $\sigma\pi_n$ est de la forme $\zeta\pi_n$, avec ζ racine p^n-ième de l'unité. De plus, il existe $\sigma \in G$ tel que ζ soit une racine *primitive* p^n-ième de l'unité. Fixons un

tel σ. On a :

$$\sigma x - x = \sum_{i=1}^{p^n-1} a_i \pi_n^i (\zeta^i - 1).$$

L'ordre de ζ^i en tant que racine de l'unité est $p^{n-v(i)}$. En effet, écrivant $i = p^{v(i)}d$ avec d non divisible par p. Alors $\zeta^i = (\zeta^d)^{p^{v(i)}}$, ζ^d est une racine primitive p^n-ième de 1, donc $(\zeta^d)^{p^{v(i)}}$ est une racine primitive $p^{n-v(i)}$-ième de 1.

Par conséquent, pour $i \in \{1, \ldots, p^n - 1\}$, on a

$$v(a_i \pi_n^i (\zeta^i - 1)) = v(a_i) + \frac{i}{ep^n} + \frac{1}{p^{n-v(i)-1}(p-1)}.$$

Soient $i, j \in \{1, \ldots, p^n - 1\}$ tels que $v(a_i \pi_n^i (\zeta^i - 1)) = v(a_j \pi_n^j (\zeta^j - 1))$. Alors

$$\frac{i-j}{ep^n} + \frac{p^{v(i)} - p^{v(j)}}{p^{n-1}(p-1)} = v(a_j) - v(a_i) \in \frac{1}{e}\mathbb{Z}.$$

Les entiers $v(i)$ et $v(j)$ sont inférieurs à $n-1$, on peut de plus supposer que $v(i) \leq v(j)$. On a alors $(i-j)(p-1) - ep^{v(i)+1}(1 - p^{v(j)-v(i)}) \in p^n(p-1)\mathbb{Z}$. Si $v(i) < v(j)$, alors

$$v((i-j)(p-1)) = v(i), \text{ et } v(ep^{v(i)+1}(1 - p^{v(j)-v(i)})) = v(e) + v(i) + 1.$$

Par conséquent, $v((i-j)(p-1) - ep^{v(i)+1}(1 - p^{v(j)-v(i)})) = v(i) < n-1$.

On a donc nécessairement $v(i) = v(j)$. Ainsi, $\frac{i-j}{p^n} \in \mathbb{Z}$, et comme i et j sont inférieurs à p^n, $i = j$. Finalement,

$$v(a_i \pi_n^i (\zeta^i - 1)) = v(a_j \pi_n^j (\zeta^j - 1)) \Leftrightarrow i = j.$$

En particulier,

$$v(\sigma x - x) = \min_{1 \leq i \leq p^n - 1} \left(v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)} \right).$$

Par conséquent, si $i \in \{1, \ldots, p^{n-1}\}$ et $v(i) < n-m$, on a sous les hypothèses du théorème :

$$v(a_i) + \frac{i}{ep^n} \geq A - \frac{p^{n-m-1}}{p^{n-1}(p-1)} \geq A_m.$$

D'autre part,

$$y_m = \sum_{\substack{0 \leq j \leq p^n - 1 \\ p^{n-m} | j}} a_j \pi_n^j = \sum_{j=0}^{p^m - 1} a_{p^{n-m} j} \pi_m^j \in K_m.$$

Finalement, on a

$$v(x - y_m) = \min_{\substack{1 \leq j \leq p^n - 1 \\ p^{n-m} \nmid j}} v(a_j \pi_n^j) = \min_{\substack{1 \leq j \leq p^n - 1 \\ v(j) < n-m}} \left(v(a_j) + \frac{j}{ep^n} \right) \geq A_m,$$

avec $y_m \in K_m$.

Réciproquement, $(ii) \Rightarrow (i)$: On suppose que $x \in K_n \setminus K_{n-1}$. On écrit $x = \sum_{i=0}^{p^n-1} a_i \pi_n^i$. On fixe $\sigma_0 \in \mathrm{Gal}(\bar{K}/K)$ tel que $\sigma_0 x = \zeta x$ avec ζ racine primitive p^n-ième de l'unité. On pose pour tout $m < n$:

$$z_m = \sum_{j=0}^{p^m-1} a_{p^{n-m}j} \pi_m^j.$$

La démonstration comporte trois étapes : tout d'abord, on montre que $v(\sigma x - x) \geq v(\sigma_0 x - x)$ pour tout $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Ensuite, on vérifie que $v(x - z) \leq v(x - z_m)$ pour tout $z \in K_m$. Enfin, on montre qu'il existe $m < n$ tel que $v(x - z_m) \leq v(\sigma_0 x - x) - \frac{1}{p^m(p-1)}$, et on conclut.

Soit $\sigma \in G$. Il existe une racine p^n-ième de l'unité ω telle que $\sigma \pi_n = \omega \pi_n$. Notons p^r l'ordre de ω en tant que racine de l'unité. On a alors $\sigma x - x = \sum_{i=1}^{p^n-1} a_i \pi_n^i (\omega^i - 1)$. Pour tout $i \in \{1, \ldots, p-1\}$, $v(a_i \pi_n^i (\omega^i - 1)) = v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{r-1}(p-1)}$. Or $r \leq n$, donc

$$\forall i \in \{1, \ldots, p-1\},\ v(a_i \pi_n^i (\omega^i - 1)) \geq v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)}.$$

Or on sait que $v(\sigma_0 x - x) = \min_{1 \leq i \leq p^n - 1} \left(v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)} \right)$, et donc

$$v(\sigma x - x) \geq \min_{1 \leq i \leq p^n - 1} \left(v(a_i \pi_n^i (\omega^i - 1)) \right) \geq v(\sigma_0 x - x).$$

Soit $z \in K_m$. On va montrer que $v(z - z_m) \neq v(x - z_m)$. Tout d'abord, comme z et z_m sont dans K_m, $v(z - z_m) \in \frac{1}{ep^m}\mathbb{Z}$. D'autre part, $v(x - z_m) = \min_{v(i) < n-m} \left(v(a_i) + \frac{i}{ep^n} \right)$. Ainsi,

$$ep^m v(x - z_m) = \min_{v(i) < n-m} \left(ep^m v(a_i) + \frac{i}{p^{n-m}} \right).$$

Si $v(i) < n - m$, $\frac{i}{p^{n-m}} \notin \mathbb{Z}$. Comme $ev(a_i) \in \mathbb{Z}$ pour tout i, on en déduit que $ep^m v(x - z_m) \notin \mathbb{Z}$, et donc que $v(z - z_m) \neq v(x - z_m)$. Par conséquent, $v(x - z) = \min(v(x - z_m), v(z - z_m)) \leq v(x - z_m)$.

On sait que $v(\sigma_0 x - x) = \min_{1 \leq i \leq p^n - 1} \left(v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)} \right)$. Notons i_0 l'indice pour lequel ce minimum est atteint ; soit $m \in \{0, \ldots, n-1\}$ tel que $v(i_0) = n - 1 - m$. On a

$$v(x - z_m) = \min_{v(i) < n-m} \left(v(a_i) + \frac{i}{ep^n} \right) \leq v(a_{i_0}) + \frac{i_0}{ep^n}.$$

Or, par définition de i_0, $v(\sigma_0 x - x) = v(a_{i_0}) + \frac{i_0}{ep^n} + \frac{1}{p^m(p-1)}$, et donc $v(x - z_m) \leq v(\sigma_0 x - x) - \frac{1}{p^m(p-1)}$.

Fixons-nous maintenant $\sigma \in G$. D'après les hypothèses du théorème, il existe un $y_m \in K_m$ tel que $v(x - y_m) \geq A_m$. On fixe un tel y_m, a en particulier $v(x - z_m) \geq A_m$. Ainsi,

$$v(\sigma x - x) \geq v(\sigma_0 x - x) \geq v(x - z_m) + \frac{1}{p^m(p-1)} \geq A. \quad \square$$

2.3. Optimisation du théorème d'Ax. — Dans cette partie, on utilise les résultats de la partie précédente et de l'étude menée sur les extensions APF pour donner la constante optimale dans le théorème d'Ax. Remarquons d'emblée que la constante optimale est minorée par $\frac{1}{p-1}$. En effet, $v(\sigma\pi_1 - \pi_1) = v(\pi_1) + \frac{1}{p-1}$, et $\inf_{y \in K} v(\pi_1 - y) = v(\pi_1)$. On va montrer que $\frac{1}{p-1}$ est en fait la constante optimale.

Théorème 2.3.1. — *Soit $x \in C$. Les deux assertions suivantes sont équivalentes :*

(i) $\forall \sigma \in G = Gal(\bar{K}/K)$, $v(\sigma x - x) \geq A$

(ii) $\forall m \in \mathbb{N}$, $\exists y_m \in K_m$ *tel que* $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$.

En particulier, si x vérifie (i), il existe $y \in K$ tel que $v(x - y) \geq A - \frac{1}{p-1}$.

Démonstration. — $(i) \Rightarrow (ii)$ On commence par supposer $x \in \bar{K}$. Pour tout $\varepsilon > 0$, on fixe $z_\varepsilon \in K_\infty$ tel que tel que $v(x - z_\varepsilon) \geq A - \varepsilon$, comme dans le corollaire 2.2.2. On a $v(\sigma z_\varepsilon - z_\varepsilon) \geq A - \varepsilon$.
Soit $m \in \mathbb{N}$. D'après le théorème 2.2.3, il existe $y_\varepsilon \in K_m$ tel que $v(z_\varepsilon - y_\varepsilon) \geq A_m - \varepsilon$. Fixons un tel y_ε, on a alors $v(x - y_\varepsilon) \geq A_m - \varepsilon$.
Si $0 < \varepsilon' < \varepsilon$,

$$v(y_\varepsilon - y_{\varepsilon'}) \geq A_m - \varepsilon.$$

Mais $ep^m v\,(y_\varepsilon - y_{\varepsilon'}) \in \mathbb{Z}$. Ainsi, pour ε suffisamment petit (de manière à ce que les entiers immédiatement supérieurs à $ep^m(A_m - \varepsilon)$ et à $ep^m A_m$ soient égaux), on a $v(y_\varepsilon - y_{\varepsilon'}) \geq A_m$. Fixons un tel ε et posons $y_m = y_\varepsilon$. Alors, pour tout $0 < \varepsilon' < \varepsilon$,

$$v(x - y_m) \geq \min(v(x - y_{\varepsilon'}), v(y_{\varepsilon'} - y_m)) \geq A_m - \varepsilon'.$$

Cette minoration étant valable pour tout ε', on a $v(x - y_m) \geq A_m$. Maintenant, lorsque $x \in C$, soit $y \in \bar{K}$ tel que $v(x - y) \geq A$. On a alors pour tout $\sigma \in G$, $v(\sigma y - y) \geq A$. Par conséquent, il existe pour tout m un $y_m \in K_m$ tel que $v(y - y_m) \geq A_m$, et on a pour tout $m \in \mathbb{N}$,

$$v(x - y_m) \geq A - \frac{1}{p^m(p-1)}.$$

$(ii) \Rightarrow (i)$ Supposons d'abord $x \in \bar{K}$. Soit $n \in \mathbb{N}$, pour $m < n$ on pose $z_m = y_m$, et pour $m \geq n$, on pose $z_m = y_n$. On a alors, pour tout $m \in \mathbb{N}$, $z_m \in K_m$ et $v(y_n - z_m) \geq A_m$. D'après le théorème 2.2.3, pour tout $\sigma \in G$, on a $v(\sigma y_n - y_n) \geq A$. On en déduit

immédiatement que pour tout $\sigma \in G$,

$$v(\sigma x - x) \geq \min(v(\sigma y_n - y_n), v(\sigma(x - y_n)), v(x - y_n)) \geq A_n.$$

Cette inégalité étant vraie pour tout $n \in \mathbb{N}$, il en résulte que $v(\sigma x - x) \geq A$ quel que soit $\sigma \in G$.
On en déduit le résultat pour $x \in C$ comme précédemment. □

Le théorème 2.3.1 peut se reformuler de la manière suivante :

Corollaire 2.3.2. — *Soit $x \in C$. Alors :*

$$\inf_{\sigma \in G} v(\sigma x - x) = \sup_{n \in \mathbb{N}} \inf_{y \in K_n} \left\{ v(x - y) + \frac{1}{p^n(p-1)} \right\}.$$

V.3. Application au calcul de $H^1(G, \mathcal{O}_{\bar{K}})$

On a la suite exacte $0 \to \mathcal{O}_{\bar{K}} \to \bar{K} \to \bar{K}/\mathcal{O}_{\bar{K}} \to 0$. En passant aux points fixes par $G = \mathrm{Gal}(\bar{K}/K)$, on a :

$$0 \to K/\mathcal{O}_K \to \left(\bar{K}/\mathcal{O}_{\bar{K}}\right)^G \to H^1(G, \mathcal{O}_{\bar{K}}) \to 0$$

car $H^1(G, \bar{K}) = 0$ (ici, $H^1(G, \mathcal{O}_{\bar{K}})$ est muni de la topologie discrète). Il en résulte que $H^1(G, \mathcal{O}_{\bar{K}})$ est isomorphe au quotient $\left(\bar{K}/\mathcal{O}_{\bar{K}}\right)^G / (K/\mathcal{O}_K)$, identification que l'on fera par la suite. On a déjà le résultat suivant :

Proposition 3.0.3. — *Soit n un entier $\geq \frac{e}{p-1}$. Alors $H^1(G, \mathcal{O}_{\bar{K}})$ est tué par π^n. En particulier, $H^1(G, \mathcal{O}_{\bar{K}})$ est tué par p.*

Démonstration. — Soit $x \in \left(\bar{K}/\mathcal{O}_{\bar{K}}\right)^G$. C'est l'image modulo $\mathcal{O}_{\bar{K}}$ d'un élément ξ de $\bar{K}$ vérifiant pour tout $\sigma \in G$, $v(\sigma\xi - \xi) \geq 0$. Il existe $y \in K$ tel que $v(\xi - y) \geq -\frac{1}{p-1}$. On a alors $v(\pi^n \xi - \pi^n y) \geq \frac{n}{e} - \frac{1}{p-1} \geq 0$, donc $\pi^n \xi = 0$ dans $H^1(G, \mathcal{O}_{\bar{K}})$, c'est à dire $\pi^n x = 0$. □

Remarque 3.0.4. — Ce résultat était déjà connu de Sen, voir [**Sen69**], théorème 3. Il n'implique pas le théorème 2.3.1, ni même l'obtention de la constante optimale dans le théorème d'Ax, car n est supposé être entier. Cependant, bien que Sen n'en dise rien, il semble possible d'adapter sa preuve du théorème 3 de [**Sen69**] pour en déduire la constante optimale dans le théorème d'Ax, en montrant d'abord que si $x \in \bar{K}$ et $\sigma x - x \in \mathcal{O}_{\bar{K}}$ pour tout $\sigma \in G$, alors il existe $y \in K$ tel que $v(x - y) \geq -\frac{1}{p-1}$.

Dans la suite, on note

$$\mathfrak{a}_n = \left\{ z \in \bar{K} \ / \ v(z) \geq -\frac{1}{p^n(p-1)} \right\}.$$

3.1. Cas non ramifié. — Dans cette sous-partie, on suppose que $K = F$, c'est à dire K/F absolument non ramifiée.
On rappelle que l'on identifie $\left(\bar{K}/\mathcal{O}_{\bar{K}}\right)^G / (K/\mathcal{O}_K)$ et $H^1(G, \mathcal{O}_{\bar{K}})$. On va montrer que l'on peut associer à $x \in H^1(G, \mathcal{O}_{\bar{K}})$ une suite d'éléments de k dont nous étudierons ensuite les propriétés. Pour $n \in \mathbb{N}$, on note $\eta_n = \pi_n^{-1}$.

Proposition 3.1.1. — *Soit $x \in H^1(G, \mathcal{O}_{\bar{K}})$, il existe un antécédent ξ de x dans $\bar{K}$ et une unique suite $(x_n)_{n\in\mathbb{N}^*}$ d'éléments de k telle que pour tout $n \in \mathbb{N}$,*

$$\xi = \sum_{i=1}^{n} [x_i]\eta_i \mod \mathfrak{a}_n,$$

où pour tout i, $[x_i]$ est le représentant de Teichmüller de x_i. De plus, la suite (x_n) ne dépend que de x.

Démonstration. — Soit ξ un antécédent de x dans $\bar{K}$. D'après le théorème 2.3.1, il existe pour tout $m \in \mathbb{N}$ un $y_m \in K_m$ tel que $\xi = y_m \mod \mathfrak{a}_m$. On fixe une telle famille (y_m). Comme $v(\xi - y_0) \geq -\frac{1}{p-1}$, on peut supposer, quitte à remplacer ξ par $\xi - y_0$, que $v(\xi) \geq -\frac{1}{p-1}$. On construit la suite $(x_n)_{n\in\mathbb{N}}$ par récurrence. Le cas $n = 0$ est trivial.
On suppose construite la suite jusqu'à l'indice n, et on écrit :

$$\xi = [x_1]\eta_1 + \cdots + [x_n]\eta_n + z, \text{ avec } z \in \mathfrak{a}_n, \text{ et } y_{n+1} = \sum_{i\geq -n_0} c'_i \pi_{n+1}^i,$$

où les c'_i sont pris parmi les représentants de Teichmüller des éléments de k et $n_0 \geq 0$. En posant $c_i = c'_{-i}$, on a $y_{n+1} = \sum_{i=1}^{n_0} c_i \eta_{n+1}^i \mod \mathcal{O}_{\bar{K}}$. Il en résulte que $\xi = \sum_{i=1}^{n_0} c_i \eta_{n+1}^i + z'$, avec $z' \in \mathfrak{a}_{n+1}$. Pour $k \geq 1$,

$$\eta_{n+1}^k \in \mathfrak{a}_n \Leftrightarrow (p \geq 3 \text{ et } k = 1) \text{ ou } (p = 2 \text{ et } k \in \{1, 2\}).$$

Ainsi, pour $p \geq 3$, en réduisant modulo $\mathfrak{a}_n$, on a $\sum_{i=2}^{n_0} c_i \eta_{n+1}^i = \alpha_1\eta_1 + \cdots + \alpha_n\eta_n \mod \mathfrak{a}_n$. Par conséquent, en identifiant les coefficients dans K_{n+1}, on a

$$x = [x_1]\eta_1 + \cdots + [x_n]\eta_n + c_1\eta_{n+1} + z',$$

ce qui achève la récurrence en posant $x_{n+1} = c_1 \mod p$.
Lorsque $p = 2$, on a (toujours en réduisant modulo $\mathfrak{a}_n$) $\sum_{i=3}^{n_0} c_i \eta_{n+1}^i = [x_1]\eta_1 + \cdots + [x_{n-1}]\eta_{n-1}$. Ainsi, $\xi = c_1\eta_{n+1} + c_2\eta_{n+1}^2 + [x_1]\eta_1 + \cdots + [x_{n-1}]\eta_{n-1} + z'$. Mais $\eta_{n+1}^2 = \eta_n$, et donc ξ s'écrit encore $\xi = [x_1]\eta_1 + \cdots + [x_n]\eta_n \mod \mathfrak{a}_{n+1}$ (car $\eta_{n+1} \in \mathfrak{a}_{n+1}$).
La suite $(x_n)_{n\in\mathbb{N}}$ ainsi associée à $x \in H^1(G, \mathcal{O}_{\bar{K}})$ ne dépend pas de $\xi \in \mathfrak{a}_0$. De plus si ξ

mod $\mathfrak{a}_n = \sum_{i=1}^n [x_i]\eta_i = \sum_{i=1}^n [x'_i]\eta_i$, alors en réduisant modulo $\mathfrak{a}_i$, on a

$$\sum_{j=1}^{i}[x_j]\eta_j = \sum_{j=1}^{i}[x'_j]\eta_j \text{ si } p \geq 3, \text{ et } \sum_{j=1}^{i-1}[x_j]\eta_j = \sum_{j=1}^{i-1}[x'_j]\eta_j \text{ si } p = 2.$$

On en déduit par récurrence sur i que pour tout $i \in \mathbb{N}$, $v([x_i] - [x'_i]) \geq \frac{1}{p^i} > 0$. Comme les $[x_i]$ sont dans K, ils sont égaux modulo p, et la suite (x_n) est unique. □

On peut donc définir l'application

$$\begin{array}{rccc} \psi : & H^1(G,\mathcal{O}_{\bar{K}}) & \longrightarrow & k^{\mathbb{N}^*} \\ & x & \mapsto & (x_n)_{n\in\mathbb{N}^*} \end{array}$$

telle que pour tout $n \in \mathbb{N}^*$, $x - \sum_{i=1}^n [x_i]\eta_i \in \mathfrak{a}_n$. C'est un morphisme $\mathcal{O}_K$-linéaire (ou k-linéaire puisque $H^1(G,\mathcal{O}_{\bar{K}})$ est tué par p), injectif. Il nous reste à identifier son image. On va adapter à notre cas des constructions proposées par Kedlaya dans un cadre une peu différent (il s'agissait de donner une description d'une clôture algébrique de $\bar{\mathbb{F}}_p((t))$, voir [**Ked01a**]). Compte tenu du fait que nous étudions des objets plus simples, nous avons préféré réécrire l'étude de Kedlaya dans le langage de notre problème.

Définition 3.1.2. — Soit $(x_n)_{n\in\mathbb{N}^*} \in k^{\mathbb{N}^*}$. On dit que la suite (x_n) est *twist-récurrente* s'il existe $d_0, \ldots, d_r \in k$ non tous nuls tels que

$$\forall n \in \mathbb{N}^*,\ d_0 x_n + d_1 x_{n+1}^p + \cdots + d_r x_{n+r}^{p^r} = 0.$$

Proposition 3.1.3. — *L'application ψ définie précédemment induit un isomorphisme de $H^1(G,\mathcal{O}_{\bar{K}})$ sur le sous-espace de $k^{\mathbb{N}^*}$ formé des suites twist-récurrentes.*

Démonstration. — On commence par montrer que si $x \in H^1(G,\mathcal{O}_{\bar{K}})$, alors $\psi(x)$ est twist-récurrente. L'élément x provient d'un élément $\xi_0 \in \bar{K}$, que l'on peut supposer de valuation $\geq -\frac{1}{p-1}$. Calculons ξ_0^p lorsque $\psi(x) = (x_n)$. Soit $n \in \mathbb{N}^*$, écrivons $\xi_0 = \sum_{i=1}^n [x_i]\eta_i + z$, avec $z \in \mathfrak{a}_n$ et les $[x_i]$ les représentants de Teichmüller. Alors $\xi_0^p = \sum_{i=0}^{n-1}[x_{i+1}]^p\eta_i + \tilde{z}$, avec $\tilde{z} = \sum_{j=1}^p \binom{p}{j} \left(\sum_{i=1}^n [x_i]\eta_i\right)^{p-j} z^j$. Or pour tout $j \in \{1, \ldots, p-1\}$,

$$v\left(\binom{p}{j}\left(\sum_{i=1}^{n}[x_i]\eta_i\right)^{p-j} z^j\right) \geq 1 - \frac{j}{p^n(p-1)} - \frac{p-j}{p^n} \geq 0.$$

Ainsi, $\xi_0^p = [x_1]^p\eta_0 + \sum_{i=1}^{n-1}[x_{i+1}]^p\eta_i \mod \mathfrak{a}_{n-1}$. En particulier, ξ_0^p vérifie $v(\sigma\xi_0^p - \xi_0^p) \geq 0$ pour tout $\sigma \in G$, et se réduit dans $H^1(G,\mathcal{O}_{\bar{K}})$ sur un élément dont l'image par ψ est (x_{n+1}^p). Pour tout $s \in \mathbb{N}$, on pose $\xi_{s+1} = \xi_s^p - [x_s]^{p^s}\eta_0$. On vérifie facilement que $v(\sigma\xi_s^p - \xi_s^p) \geq 0$ pour tout $\sigma \in G$, et que la réduction dans $H^1(G,\mathcal{O}_{\bar{K}})$ a pour image par ψ la suite $[x_{n+s}]^{p^s}$. Comme par ailleurs tous les ξ_s sont dans $K(\xi_0)$, ils forment une famille liée sur K. Il existe

donc $\delta_0, \dots, \delta_r \in K$ tels que $\delta_0\xi_0 + \cdots + \delta_r\xi_r = 0$. Quitte à multiplier par une puissance de p, on peut supposer que les δ_s sont dans $\mathcal{O}_K$ et qu'au moins l'un d'entre eux est non divisible par p. L'application ψ étant $\mathcal{O}_K$-linéaire, on en déduit que pour tout $n \in \mathbb{N}^*$,

$$d_0x_n + d_1x_{n+1}^p + \cdots + d_rx_{n+r}^{p^r} = 0,$$

où d_s désigne la réduction de δ_s modulo p. Donc (x_n) est twist-récurrente.

Réciproquement, il nous reste à prouver que si $(x_n)_{n\in\mathbb{N}^*}$ est twist-récurrente, alors c'est l'image par ψ d'un élément de $H^1(G, \mathcal{O}_{\bar{K}})$. Soit donc $(x_n)_{n\in N^*}$ twist-récurrente et soient $d_0, \dots, d_r \in k$ non tous nuls tels que

$$\forall n \in \mathbb{N}^*,\ d_0x_n + \cdots + d_rx_{n+r}^{p^r} = 0.$$

On note $\delta_0, \dots, \delta_r$ des relevés des d_k dans $\mathcal{O}_K$, pour $n \geq 1$, on note $[x_n]$ le représentant de Teichmüller de x_n dans $\mathcal{O}_K$, et on considère le polynôme

$$P = -\left(\delta_r[x_r]^{p^r}\eta_1 + \cdots + (\delta_1[x_r]^p + \cdots + \delta_r[x_{2r-1}]^{p^r})\eta_r\right) + \delta_0X + \cdots + \delta_rX^{p^r}.$$

On va montrer qu'il admet une racine dans $\mathcal{O}_{\bar{K}}$ dont l'image dans $H^1(G, \mathcal{O}_{\bar{K}})$ s'envoie par ψ sur la suite $(0, \dots, x_{r+1}, x_{r+1}, \dots)$. On fixe $n \geq 1$ et on cherche une racine ξ de P sous la forme $\xi = [x_{r+1}]\eta_{r+1} + \cdots + [x_{n+r}]\eta_{n+r} + y\eta_{n+r+1}$ avec $y \in \mathcal{O}_{\bar{K}}$.
Tout d'abord, on a pour $0 \leq s \leq r$,

$$\xi^{p^s} = \left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^{p^s} + \eta_{n+r+1}^{p^s}y^{p^s} + \sum_{j=1}^{p^s-1}\binom{p^s}{j}\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^{p^s-j}\eta_{n+r+1}^jy^j.$$

Comme $P(\xi) = 0$, on a :

$$\sum_{k=0}^{r}\delta_k\left[\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^{p^k} + \sum_{j=1}^{p^k-1}\binom{p^k}{j}\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^{p^k-j}\eta_{n+r+1}^jy^j + \eta_{n+r+1}^{p^k}y^{p^k}\right]$$
$$= \delta_r[x_r]^{p^r}\eta_1 + \cdots + (\delta_1[x_r]^p + \cdots + \delta_r[x_{2r-1}]^{p^r})\eta_r.$$

On voit donc que y est annulé par un polynôme Q de degré p^r, dont le coefficient constant est

$$\sum_{k=0}^{r}\delta_k\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^{p^k} - (\delta_r[x_r]^{p^r}\eta_1 + \cdots + (\delta_1[x_r]^p + \cdots + \delta_r[x_{2r-1}]^{p^r})\eta_r),$$

et dont le coefficient dominant est $\delta_r\eta_{n+r+1}^{p^r} = \delta_r\eta_{n+1}$. Par ailleurs, on a :

$$\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^p = \sum_{\varepsilon_1+\cdots+\varepsilon_n=p}\frac{p!}{\varepsilon_1!\dots\varepsilon_n!}[x_{r+1}]^{\varepsilon_1}\dots[x_{n+r}]^{\varepsilon_n}\eta_{r+1}^{\varepsilon_1}\dots\eta_{n+r}^{\varepsilon_n}.$$

On remarque que si tous les ε_i sont $< p$, $v(\frac{p!}{\varepsilon_1!\dots\varepsilon_n!}) = 1$ et $v(\eta_{r+1}^{\varepsilon_1}\dots\eta_{n+r}^{\varepsilon_n}) = -\frac{\varepsilon_1}{p^{r+1}} - \dots - \frac{\varepsilon_n}{p^{n+r}} > -1$. Donc tous les termes correspondants de la somme sont nuls modulo $\mathcal{O}_{\bar{K}}$, et donc

$$\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^p = [x_{r+1}]^p\eta_r + [x_{r+2}]^p\eta_{r+1} + \dots + [x_{n+r}]^p\eta_{n+r-1} \mod \mathcal{O}_{\bar{K}}.$$

Le fait que la série commence à $[x_{r+1}]\eta_{r+1}+\cdots$ permet de montrer, par un calcul analogue, que pour tout $s \in \{1,\dots,r\}$, on a :

$$\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^{p^s} = [x_{r+1}]^p\eta_{r+1-s} + [x_{r+2}]^p\eta_{r+2-s} + \dots + [x_{n+r}]^p\eta_{r+n-s} \mod \mathcal{O}_{\bar{K}}.$$

En additionnant, on a donc :

$$\sum_{s=0}^{r}\delta_s\left(\sum_{i=r+1}^{n+r}[x_i]\eta_i\right)^{p^s} = \delta_r[x_r]^{p^r}\eta_1 + \dots + (\delta_1[x_r]^p + \dots + \delta_r[x_{2r-1}]^{p^r})\eta_r + \eta_{n+1}z,$$

avec $z \in \mathcal{O}_{\bar{K}}$. Le coefficient constant de Q est donc de valuation $\geq -\frac{1}{p^{n+1}}$ qui est la valuation de son coefficient dominant. En traçant son polygone de Newton, on en déduit que ce polynôme a une racine de valuation positive. Le polynôme P a donc bien une racine de la forme $x = [x_{r+1}]\eta_{r+1} + \dots + [x_{n+r}]\eta_{n+r} + y\eta_{n+r+1}$ avec $y \in \mathcal{O}_{\bar{K}}$. Comme P a p^r racines, il y a au moins l'une d'entre elles qui est obtenue pour une infinité de n à l'aide de la construction précédente. Notons ξ_0 une telle racine. En réduisant modulo $\mathfrak{a}_n$, on voit que pour *tout* $n \in \mathbb{N}^*$, on a $\xi_0 - \sum_{i=r+1}^{r+n}[x_i]\eta_i \in \mathfrak{a}_n$. On a donc $\xi_0 \in H^1(G,\mathcal{O}_{\bar{K}})$, et $\psi(\xi_0) = (0,0,\dots,0,x_{r+1},x_{r+2},\dots,x_n,\dots)$. Comme $(x_1,\dots,x_r,0,0,\dots)$ est l'image de $\sum_{i=1}^{r}[x_i]\eta_i \in H^1(G,\mathcal{O}_{\bar{K}})$, on en déduit que (x_n) est dans l'image de ψ. □

Corollaire 3.1.4. — *Si $K = F$, $H^1(G,\mathcal{O}_{\bar{K}})$ est un k-espace vectoriel de dimension infinie. Plus précisément, si k est fini, la dimension de $H^1(G,\mathcal{O}_{\bar{K}})$ est dénombrable. Si k est infini, elle est égale à la cardinalité de k.*

Démonstration. — $H^1(G,\mathcal{O}_{\bar{K}})$ est l'ensemble des suites twist-récurrentes à valeurs dans k. Pour $d_0,\dots,d_r$ non tous nuls fixés, l'ensemble des suites vérifiant la relation de twist-récurrence

$$\forall n \in \mathbb{N},\ d_0x_n + \dots + d_rx_{n+r}^{p^r} = 0$$

forme un k-espace vectoriel de dimension finie. La réunion des espaces déterminés par l'ensemble des $(d_0,\dots,d_r) \in k^{r+1}$, pour $r \geq 0$, est de dimension dénombrable si k est fini, et de dimension la cardinalité de k si k est infini. □

3.2. Le cas ramifié. — Dans cette partie, on entame une étude analogue à la précédente, en ne supposant plus cette fois-ci que $e = 1$.

3.2.1. Cas $e \leq p-1$.— On étudie ici le cas où $e \leq p-1$, pour lequel les constructions proposées dans le cas non ramifié s'adaptent facilement. La proposition précédente nous dit que $H^1(G, \mathcal{O}_{\bar{K}})$ est tué par π, en particulier il a une structure naturelle de k-espace vectoriel. On peut en fait associer à un élément de $H^1(G, \mathcal{O}_{\bar{K}})$ une famille de suites d'éléments de k.

Proposition 3.2.1. — *Soit $x \in H^1(G, \mathcal{O}_{\bar{K}})$, il existe e suites $(x_{1,n}), \ldots, (x_{e,n})$ d'éléments de k telles que pour tout $n \in \mathbb{N}$, $x = \sum_{i=1}^{n} \sum_{j=1}^{e} [x_{j,i}]\eta_i^j \mod \mathfrak{a}_n$, $[x_{j,n}]$ désignant le représentant de Teichmüller de $x_{j,n}$.*

Démonstration. — On procède comme dans le cas non ramifié, la différence ici étant que la réduction modulo $\mathfrak{a}_n$ de y_{n+1} ne tue plus seulement $c_1\eta_{n+1}$ mais la somme $c_1\eta_{n+1} + \cdots + c_e\eta_{n+1}^{\rho}$ lorsque $e < p-1$, ρ désignant le plus grand entier inférieur à $\frac{ep}{p-1}$. Le cas $e = p-1$ entraîne la même modification que dans le cas $e = 1, p = 2$. □

On a donc comme précédemment une application :

$$\begin{array}{rccc} \psi : & H^1(G, \mathcal{O}_{\bar{K}}) & \longrightarrow & \left(k^{\mathbb{N}^*}\right)^e \\ & x & \mapsto & ((x_{1,n})_{n\in\mathbb{N}^*}, \ldots, (x_{e,n})_{n\in\mathbb{N}^*}) \end{array}$$

Théorème 3.2.2. — *L'application qui à $x \in H^1(G, \mathcal{O}_{\bar{K}})$ associe $((x_{1,n}), (x_{2,n}), \ldots, (x_{e,n}))$ est injective, et son image est l'ensemble des e-uplets de suites twist-récurrentes à valeurs dans k, qui est donc isomorphe à $H^1(G, \mathcal{O}_{\bar{K}})$.*

Démonstration. — Nous ne donnerons pas ici la démonstration de ce résultat, les idées sont similaires à celles de la preuve dans le cas non ramifié. □

3.2.2. Cas général.— Il nous reste à traiter le cas $e \geq p$. $H^1(G, \mathcal{O}_{\bar{K}})$ n'est pas tué par π. On note $\tau = \left\lfloor \frac{e}{p-1} \right\rfloor$ et $\rho = \left\lfloor \frac{ep}{p-1} \right\rfloor$ (où $\lfloor t \rfloor$ désigne le plus grand entier inférieur ou égal à t). Un calcul direct montre que $\rho - \tau = e$. Soit $x \in H^1(G, \mathcal{O}_{\bar{K}})$. On dispose d'une suite (y_n) avec pour tout $n \in \mathbb{N}$, $y_n \in K_n$ et $x = y_n \mod \mathfrak{a}_n$. On écrit pour tout $n \in \mathbb{N}$ que $y_n = \sum_{j=1}^{N_n} c_{j,n}\eta_n^j$, avec les $c_{j,n}$ pris dans une famille de représentants des éléments de k dans $\mathcal{O}_K$ de valuation nulle ou infinie (attention, il ne s'agit plus ici de représentants de Teichmüller). Pour tout $n \in \mathbb{N}^*$, il existe $z_n \in \mathfrak{a}_n$ tel que $x = \sum_{j=1}^{N_n} c_{j,n}\eta_n^j + z_n$. On remarque que $\eta_n^j \in \mathfrak{a}_n$ si et seulement si $j \leq \tau$, on peut donc supposer que la somme commence à $j = \tau + 1$.

Réduisons modulo $\mathfrak{a}_n$ l'égalité précédente écrite aux rangs n et $n+1$. On a pour $j \geq 1$:

$$\eta_{n+1}^j \in \mathfrak{a}_n \Leftrightarrow \frac{j}{ep^{n+1}} \leq \frac{1}{p^n(p-1)} \Leftrightarrow j \leq \frac{ep}{p-1} \Leftrightarrow j \leq \rho.$$

Par conséquent,

$$\sum_{j=\tau+1}^{N_n} c_{j,n}\eta_n^j = \sum_{j=\rho+1}^{N_{n+1}} c_{j,n+1}\eta_{n+1}^j \mod \mathfrak{a}_n$$

Il découle de ces calculs la proposition suivante :

Proposition 3.2.3. — *Soit $x \in H^1(G, \mathcal{O}_{\bar{K}})$. Il existe e suites $(\alpha_{n,\tau+1})_{n\in\mathbb{N}^*}, \ldots, (\alpha_{n,\rho})_{n\in\mathbb{N}^*}$ d'éléments de $\mathcal{O}_K$ telles que pour tout $n \in \mathbb{N}^*$, $x = \sum_{i=1}^n \sum_{j=\tau+1}^{\rho} \alpha_{i,j}\eta_i^j \mod \mathfrak{a}_n$.*

Démonstration. — On procède par récurrence, en conservant les notations précédentes. Le cas $n = 1$ est immédiat, compte tenu du fait que pour $j \geq \rho$, $\eta_1^j \in K$.
Pour $n \geq 1$, on a $\sum_{j=\rho+1}^{N_{n+1}} c_{j,n+1}\eta_{n+1}^i = \sum_{i=1}^n \sum_{j=\tau+1}^{\rho} \alpha_{i,j}\eta_i^j \mod \mathfrak{a}_n$ par hypothèse de récurrence, et donc

$$x = \sum_{k=\tau+1}^{\rho} c_{k,n+1}\eta_i^k + \sum_{i=1}^{n}\sum_{k=\tau+1}^{\rho} \alpha_{i,k}\eta_i^k + z_{n+1},$$

ce qui prouve la proposition en posant $\alpha_{n+1,j} = c_{j,n+1}$. □

Remarquons que dans cette écriture, un η_i^j n'apparaît qu'une fois ; autrement dit, il n'existe pas de couples (i, j), (i', j') distincts d'indices dans cette somme tels que $\eta_i^j = \eta_{i'}^{j'}$. En effet, on a :

$$p(\tau+1) > p\frac{e}{p-1} \geq \rho.$$

En conséquence, si $j, j' \in \{\tau+1, \ldots, \rho\}$ et $j < j'$, on a $pj > j'$, et donc $p^{i'}j \neq p^i j'$ pour tous i, i'. De plus, comme on calcule modulo K, on peut supprimer de cette somme les $\alpha_{j,i}$ tels que $j|p^i$; on peut également regrouper les termes indexés par $(i, j - \lambda p^i)$ pour $\lambda \in \mathbb{N}$ car alors $\eta_i^{j-\lambda p^i} = \pi^\lambda \eta_i^j$. Pour $i \in \mathbb{N}^*$ et $j \in \{\tau+1, \ldots, \rho\}, j \nmid p^i$, on note $\gamma_{i,j} = \max\{s \in \{\tau+1, \ldots, \rho\} \,/\, p^i \mid s-j\}$ et $I = \{(i, \gamma_{i,j}) \,/\, i \in \mathbb{N}^*, j \in \{\tau+1, \ldots, \rho\}, p^i \nmid \gamma\}$. On peut encore écrire pour tout $n \in \mathbb{N}$,

$$x = \sum_{(i,\gamma)\in I, i\leq n} \beta_{i,\gamma}\eta_i^\gamma \mod \mathfrak{a}_n,$$

en regroupant les termes comme expliqué précédemment. Une telle écriture est alors unique : il n'y a aucune sous-somme finie de $\sum_{(i,\gamma)\in I} \beta_{i,\gamma}\eta_i^\gamma$ égale à un élément non nul de K, et aucun $\beta_{i,\gamma}\eta_i^\gamma$ non nul n'est de valuation positive. En effet, si $\gamma - \lambda p^i \in \{\tau+1, \ldots, \rho\}$ et $\gamma - (\lambda+1)p^i \notin \{\tau+1, \ldots, \rho\}$, alors dès que $\beta_{i,\gamma}$ est non nul, on a $ev(\beta_{i,\gamma}) \leq \lambda$, et donc $ev(\beta_{i,\gamma}) < \lambda + \frac{\tau}{p^i} \leq -ev(\eta_i^\gamma)$. On peut donc bien définir une application de $H^1(G, \mathcal{O}_{\bar{K}})$ vers $\mathcal{O}_K^I$, qui à x associe les $\beta_{i,\gamma}$.

Proposition 3.2.4. — *Soit $r \geq 1$ et H_{π^r} le sous-module de π^r-torsion de $H^1(G, \mathcal{O}_{\bar{K}})$, alors $H^1(G, \mathcal{O}_{\bar{K}})/H_{\pi^r}$ est un $\mathcal{O}_K$-module de type fini engendré par au plus $\frac{pe}{r(p-1)^2}$ éléments.*

Démonstration. — On note $I_r = \{(i, \gamma) \in I,\ rp^i < \gamma\}$. La π^r-torsion de $H^1(G, \mathcal{O}_{\bar{K}})$ est l'ensemble des $x \in H^1(G, \mathcal{O}_{\bar{K}})$ tels que $\pi^r x = 0$, c'est à dire $v(\pi^r x) \geq 0$. En associant à x la famille des $\beta_{i,\gamma}$ et en considérant les valuations, $\pi^r x = 0$ si et seulement si pour tout $(i, \gamma) \in I$, $\frac{r}{e} + v(\beta_{i,\gamma}) \geq \frac{\gamma}{ep^i}$. Notons H_{π^r} le sous-module de π^r-torsion de $H^1(G, \mathcal{O}_{\bar{K}})$, la proposition et les calculs précédents montrent que l'application composée

$$\mathcal{O}_K^{I_r} \to \sum_{(i,\gamma) \in I_r} \eta_i^\gamma \mathcal{O}_K \to H^1(G, \mathcal{O}_{\bar{K}})/H_{\pi^r}$$

est surjective. Le $\mathcal{O}_K$-module $H^1(G, \mathcal{O}_{\bar{K}})/H_{\pi^r}$ est donc de type fini, engendré par des éléments en nombre fini majoré par le cardinal de I_r. À i fixé, il y a au plus p^i éléments de la forme (i, γ) dans I. De plus, si $(i, \gamma) \in I_r$, $p^i < \frac{\rho}{r}$ et donc $i < \log_p(\rho/r)$. Le cardinal de I_r est donc majoré par $\sum_{1 \leq i < \log_p(\rho/r)} p^i$. Cette somme est majorée par $\frac{\log_p(\rho/r)}{p-1} \leq \frac{pe}{r(p-1)^2}$. □

Remarque 3.2.5. — Le $\mathcal{O}_K$-module H_π a une structure naturelle de k-espace vectoriel, on a un morphisme injectif $H_\pi \to k^{\mathbb{N}}$, et il semble possible d'espérer que les résultats de Kedlaya s'adaptent pour montrer que l'image de cette injection peut se décrire en terme de suites twist-récurrentes dans leur définition la plus générale (voir [**Ked01a**] et [**Ked01b**]). Nous ne ferons pas ici cette interprétation.

Remarque 3.2.6. — Les méthodes utilisées dans cet article peuvent peut-être se généraliser au calcul de $H^1(G, GL_n(\mathcal{O}_{\bar{K}}))$. En effet, en utilisant la forme de Smith des éléments de $GL_n(\mathcal{O}_{\bar{K}})$, on devrait pouvoir donner une description de $H^1(G, GL_n(\mathcal{O}_{\bar{K}}))$, ce qui pourrait donner un avatar de la théorie de Sen dans le cas des représentations de torsion.

BIBLIOGRAPHIE

[AC94] Daniel Augot and Paul Camion, *Forme de Frobenius et vecteurs cycliques*, C. R. Acad. Sci. Paris Sér. I Math. **318** (1994), no. 2, 183–188. MR 1260335 (94m :65090)

[Ax70] James Ax, *Zeros of polynomials over local fields—The Galois action*, J. Algebra **15** (1970), 417–428. MR 0263786 (41 #8386)

[BB10] Laurent Berger and Christophe Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbf{Q}_p)$, Astérisque (2010), no. 330, 155–211. MR 2642406

[Ber04] Laurent Berger, *Limites de représentations cristallines*, Compos. Math. **140** (2004), no. 6, 1473–1498. MR 2098398 (2006c :11138)

[Ber09] ———, *Galois representations and* (φ, Γ)*-modules*, Cours à l'Institut Henri Poincaré, 2009.

[Bre99a] Christophe Breuil, *Représentations semi-stables et modules fortement divisibles*, Invent. Math. **136** (1999), no. 1, 89–122. MR 1681105 (2000c :14024)

[Bre99b] ———, *Une application de corps des normes*, Compositio Math. **117** (1999), no. 2, 189–203. MR 1695849 (2000f :11157)

[BU09] Delphine Boucher and Felix Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. **44** (2009), no. 12, 1644–1656. MR 2553570 (2010j :94085)

[Car09a] Xavier Caruso, $\mathbb{F}_p$*-représentations semi-stables*, à paraître dans Annales de l'Institut Fourier, 2009.

[Car09b] ———, *Sur la classification de quelques* ϕ*-modules simples*, Mosc. Math. J. **9** (2009), no. 3, 562–568, back matter. MR 2562793 (2011d :11119)

[CF00] Pierre Colmez and Jean-Marc Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), no. 1, 1–43. MR 1779803 (2001g :11184)

[CHH04] Robert S. Coulter, George Havas, and Marie Henderson, *On decomposition of sub-linearised polynomials*, J. Aust. Math. Soc. **76** (2004), no. 3, 317–328. MR 2053506 (2005b :13013)

[CL09] Xavier Caruso and Tong Liu, *Quasi-semi-stable representations*, Bull. Soc. Math. France **137** (2009), no. 2, 185–223. MR 2543474 (2011c :11086)

[Cola] Pierre Colmez, *Notes du cours de M2, Corps locaux*, http ://www.math.jussieu.fr/ colmez/CL.pdf.

[Colb] _____, *Notes du cours de M2, Introduction aux anneaux de Fontaine*, http ://www.math.jussieu.fr/ colmez/Fontaine.pdf.

[Col10] _____, *Représentations de* $\mathrm{GL}_2(\mathbf{Q}_p)$ *et* (ϕ, Γ)*-modules*, Astérisque (2010), no. 330, 281–509. MR 2642409 (2011j :11224)

[Eme11] Matthew Emerton, *Local-global compatibility in the p-adic langlands program for* $GL_{2/\mathbb{Q}}$, prépublication, 2011.

[Fal88] Gerd Faltings, *p-adic Hodge theory*, J. Amer. Math. Soc. **1** (1988), no. 1, 255–299. MR 924705 (89g :14008)

[FL82] Jean-Marc Fontaine and Guy Laffaille, *Construction de représentations p-adiques*, Ann. Sci. École Norm. Sup. (4) **15** (1982), no. 4, 547–608 (1983). MR 707328 (85c :14028)

[FM87] Jean-Marc Fontaine and William Messing, *p-adic periods and p-adic étale cohomology*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 179–207. MR 902593 (89g :14009)

[FM95] Jean-Marc Fontaine and Barry Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 41–78. MR 1363495 (96h :11049)

[Fon90] Jean-Marc Fontaine, *Représentations p-adiques des corps locaux. I*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 249–309. MR 1106901 (92i :11125)

[Fon94] _____, *Représentations p-adiques semi-stables*, Astérisque (1994), no. 223, 113–184, With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988). MR 1293972 (95g :14024)

[Gie95] Mark Giesbrecht, *Nearly optimal algorithms for canonical matrix forms*, SIAM J. Comput. **24** (1995), no. 5, 948–969. MR 1350753 (96f :65180)

[Gie98] _____, *Factoring in skew-polynomial rings over finite fields*, J. Symbolic Comput. **26** (1998), no. 4, 463–486. MR 1646671 (99i :16053)

[Jac96] Nathan Jacobson, *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996. MR 1439248 (98a :16024)

[Ked01a] Kiran S. Kedlaya, *The algebraic closure of the power series field in positive characteristic*, Proc. Amer. Math. Soc. **129** (2001), no. 12, 3461–3470 (electronic). MR 1860477 (2003a :13025)

[Ked01b] _____, *Power series and p-adic algebraic closures*, J. Number Theory **89** (2001), no. 2, 324–339. MR 1845241 (2002i :11116)

[Ked08] ———, *Slope filtrations for relative Frobenius*, Astérisque (2008), no. 319, 259–301, Représentations p-adiques de groupes p-adiques. I. Représentations galoisiennes et (ϕ, Γ)-modules. MR 2493220 (2010c :14024)

[KG85] Walter Keller-Gehrig, *Fast algorithms for the characteristic polynomial*, Theoret. Comput. Sci. **36** (1985), no. 2-3, 309–317. MR 796306 (86i :65020)

[Kis06] Mark Kisin, *Crystalline representations and F-crystals*, Algebraic geometry and number theory, Progr. Math., vol. 253, Birkhäuser Boston, Boston, MA, 2006, pp. 459–496. MR 2263197 (2007j :11163)

[Kis07] ———, *What is... a Galois representation ?*, Notices Amer. Math. Soc. **54** (2007), no. 6, 718–719. MR 2327973 (2008d :11049)

[Kis09] ———, *The Fontaine-Mazur conjecture for* GL_2, J. Amer. Math. Soc. **22** (2009), no. 3, 641–690. MR 2505297 (2010j :11084)

[Lau02] Gérard Laumon, *La correspondance de Langlands sur les corps de fonctions (d'après Laurent Lafforgue)*, Astérisque (2002), no. 276, 207–265, Séminaire Bourbaki, Vol. 1999/2000. MR 1886762 (2003b :11052)

[LB10] Jérémy Le Borgne, *Optimisation du théorème d'Ax-Sen-Tate et application à un calcul de cohomologie galoisienne p-adique*, Ann. Inst. Fourier (Grenoble) **60** (2010), no. 3, 1105–1123. MR 2680825

[LB11a] ———, *Semi-characteristic polynomials, φ-modules and skew polynomials*, prépublication, 2011.

[LB11b] ———, *Un algorithme pour la réduction des ϕ-modules sur $k(\!(u)\!)$*, en préparation, 2011.

[LN94] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994. MR 1294139 (95f :11098)

[Ore33] Oystein Ore, *Theory of non-commutative polynomials*, Ann. of Math. (2) **34** (1933), no. 3, 480–508. MR 1503119

[Sen69] Shankar Sen, *On automorphisms of local fields*, Ann. of Math. (2) **90** (1969), 33–46. MR 0244214 (39 #5531)

[Ser68] Jean-Pierre Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII. MR 0354618 (50 #7096)

[Ser72] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR 0387283 (52 #8126)

[Ser89] ———, *Abelian l-adic representations and elliptic curves*, second ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989, With the collaboration of Willem Kuyk and John Labute. MR 1043865 (91b :11071)

[Tat67] John Tate, *$p-$ divisible groups.*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158–183. MR 0231827 (38 #155)

[Tsu99] Takeshi Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. Math. **137** (1999), no. 2, 233–411. MR 1705837 (2000m :14024)

[Wac96] Nathalie Wach, *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France **124** (1996), no. 3, 375–400. MR 1415732 (98b :11119)

[Win83] Jean-Pierre Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux ; applications*, Ann. Sci. École Norm. Sup. (4) **16** (1983), no. 1, 59–89. MR 719763 (85e :11098)

Résumé. — Nous nous intéressons aux aspects algorithmiques de la théorie des représentations modulo p de groupes de Galois p-adiques. À cet effet, l'un des outils introduits par Fontaine est la théorie de φ-modules : un φ-module sur un corps K de caractéristique p est la donnée d'un espace vectoriel de dimension finie sur K muni d'un endomorphisme φ, semi-linéaire par rapport au morphisme de Frobenius sur K. Les représentations à coefficients dans un corps fini du groupe de Galois absolu de K forment une catégorie équivalente à la catégorie des φ-modules dits « étales » sur K.
Le but des travaux rassemblés ici est donner des algorithmes pour décrire le plus complètement possible la représentation associée à un φ-module donné. Nous étudions en préambule les φ-modules sur les corps finis, ce qui nous permet d'obtenir de nouveaux résultats décrivant les polynômes tordus sur un corps fini, qui sont des objets utilisés notamment en théorie des codes correcteurs. Cela nous permet d'améliorer en partie l'algorithme dû à Giesbrecht pour la factorisation de ces polynômes. Nous nous intéressons ensuite à la catégorie des φ-modules sur un corps de séries formelles de caractéristique p. Nous donnons une classification des objets simples de cette catégorie lorsque le corps résiduel est algébriquement clos, et décrivons un algorithme efficace pour décomposer un φ-module en φ-modules « isoclines ». Nous donnons des applications à l'étude algorithmique des représentations de p-torsion de groupes de Galois p-adiques.

Abstract. — We study algorithmic aspects of the theory of modular representations of p-adic Galois groups. For this purpose, one of the tools introduced by Fontaine is the theory of φ-modules. A φ-modles over a field K of positive characteristic is the data of a finite-dimensional vector space over K, endowed with an endomorphism φ that is semilinear with respect to the Frobenius morphism on K. The category of representations of the absolute galois group of K with coefficients in a finite field is equivalent to that of *étale* φ-modules over K.
The aim of the works collected here is to give algorithms to decribe the representation associated to a given φ-module as completely as possible. First, we study the φ-modules over finite fields, which allows us new results describing the so-called skew polynomials over a finite field. These are objets used for example in the theory of error-correcting codes. We improve a part of the algorithm of Giesbrecht for the factorizations of these polynomials. We the consider the category of φ-modules over a field of formal power series of characteristic p. We give a classification of the simple objects of this category when the residue field is algebraically closed. We decribe an efficient algorithm to decompose a φ-module with *isocline* φ-modules. We give applications to the algorithmic study of p-torsion representations of p-adic Galois groups.