Contribution à l'étude p-adique des sommes de caractères

Régis Blache

Mémoire d'Habilitation à Diriger les Recherches

Contribution à l'étude p-adique des sommes de caractères

François-Régis Blache

Laboratoire AOC
Université des Antilles et de la Guyane
Mèl : rblache@univ-ag.fr
Adresse : IUFM de Guadeloupe, BP 399, 97159 Pointe à Pitre CEDEX

RÉSUMÉ : Dans ce mémoire, on se propose de décrire certains résultats de l'auteur sur les propriétés p-adiques des fonctions L associées à des caractères sur les corps finis, à la suite des travaux de Dwork, Robba, Adolphson et Sperber, Wan, entre autres. On parlera aussi de sommes de caractères (et de leurs fonctions L) définies sur certains anneaux locaux.

MSC2000 : 11,14

MOTS CLÉS : Sommes de caractères, rationalité des fonctions L, racines et pôles réciproques de ces fonctions, nombres de Weil, polygones de Newton génériques, polygone de Hodge et de Hodge Stickelberger, polyèdres de Newton, cohomologies étales et p-adiques, fonctions de Dwork

Table des matières

CHAPITRE 1

Introduction

1. Guide de lecture

Ce mémoire d'Habilitation à Diriger les Recherches repose sur les travaux de l'auteur concernant les sommes de caractères sur les corps finis et les propriétés p-adiques, ainsi que le sommes de caractères sur les anneaux finis. On y expose de façon assez détaillée le contenu des articles **[B3]**, **[BF]**, **[B4]**, **[B2]**, **[B1]** et **[BFZ]**. Pour préserver l'unité de ce mémoire, on ne parlera pas des travaux portant sur

(1) les sommes incomplètes sur les courbes définies sur certains anneaux **[B6]**, **[B5]**, plus précisément le degré de leurs fonctions L ;

(2) la construction de cryptosystèmes provenant des jacobiennes de courbes sur un corps fini, en particulier l'interprétation géométrique de l'addition dans le groupe des points rationnels de ces jacobiennes **[BCE]**, **[BEP]** ;

(3) la conjecture de Gauss sur l'existence d'une infinité de courbes hyperelliptiques ayant un certain anneau de fonctions régulières principal **[AB]**.

On a fait le choix, pour rendre ce mémoire aussi autonome que possible, d'expliquer assez précisément les idées en jeu, ainsi que les techniques utilisées. Toutefois, très peu de démonstrations sont données, on renvoie le lecteur curieux aux articles cités dans la bibliographie.

Pour souligner ces idées, le chapitre 2 tente de retracer (rapidement) certaines des questions principales qui sous-tendent l'étude des sommes de caractères depuis Gauss. Il est aussi l'occasion d'introduire les principaux outils d'étude de ces objets mathématiques, ainsi que des résultats fondamentaux pour la suite. On presse donc de lecteur de commencer la lecture par ce chapitre, en espérant que l'exposition le rende d'une lecture agréable. Les chapitres suivants peuvent être abordés de façon séparée et dans l'ordre qu'on veut. Toutefois, certains des résultats du chapitre 3 sont utilisés dans le chapitre 4, le chapitre 5 utilise les outils décrits à la section 1, et les sommes de Gauss p-adiques (Définition 2.5) sont utilisées dans le chapitre 8.

Les cinq chapitres 3, 4, 5, 6 et 7 sont centrés autour de l'étude p-adique des sommes de caractères, et se situent (tout du moins l'auteur l'espère) dans la lignée des travaux de Dwork, Robba, Adolphson-Sperber et Wan. Le chapitre 6 s'inscrit aussi dans la lignée des résultats de Ax, Chevalley, Katz et Warning.

Le dernier est assez différent, où l'on se préoccupe de sommes sur les anneaux. Ces sommes sont beaucoup moins étudiées que les sommes sur les corps finis, et l'auteur ne prétend pas en donner une étude systématique. On présente quelques calculs explicites, ainsi que des similarités avec le cas classique des corps finis.

2. Remerciements.

J'ai la chance immense de pouvoir faire un métier qui est aussi une passion. Pour ne rien gâter je l'exerce dans de très beaux endroits. C'est un plaisir de remercier ceux que j'ai croisés, plus ou moins longtemps, plus ou moins souvent, et qui ont permis cette heureuse conjonction.

Une importante partie des travaux exposés dans ce mémoire ont été faits quand j'étais en poste à l'Université de Polynésie Française. Je tiens à remercier Stéphane Ballet, Jean Chaumine, Éric Férard et Jean-Marie Goursaud pour m'avoir acceuilli et avoir contribué à créer un cadre propice à l'exigeante activité de recherche.

L'Institut de Mathématiques de Luminy m'a toujours soutenu, ceci depuis le début. Son directeur actuel, Gilles Lachaud était mon directeur de thèse. Je tiens à le remercier pour la confiance qu'il m'a accordée, en m'appuyant quand je me suis lancé dans cette aventure, et à de nombreuses reprises depuis.

Merci encore à Robert Rolland pour avoir maintenu ce lien vivace (il continue tout en étant en retraite !), ainsi qu'à Yves Aubry pour son enthousiasme, à François Rodier pour son attention renouvelée. Merci enfin à tous ceux qui ont rendu mes séjours à Luminy agréables, et fructueux par l'ambiance scientifique qui y règne. Gilles Lachaud et François Rodier me font l'honneur de participer à ce jury d'habilitation, réaffirmant ainsi le lien tissé avec l'IML, et je les en remercie.

J'ai conçu tous mes autres travaux mathématiques en Guadeloupe, et cela n'aurait pas été possible sans le soutien de certains collègues. Jean Pierre Cherdieu a toujours été un soutien précieux, il a su lui aussi créer une ambiance propice au travail. Je lui dois beaucoup plus, et je l'en remercie. Alain Pietrus, en tant que directeur du laoratoire, me permet de présenter ce mémoire dans de bonnes conditions, qu'il trouve ici l'expression de ma gratitude. Le personnel de l'IUFM de Guadeloupe, où je suis arrivé l'année dernière, m'a acceuilli comme si je n'étais jamais parti, et je lui en sais gré. Antoine Delcroix, Dany-Jack Mercier pour ne citer qu'eux, m'ont permis de me réadapter sans effort. Ils sont bien nombreux ceux que je pourrais remercier, autant à l'Université ou à l'IUFM qu'ailleurs, qu'ils sachent que je ne les oublie pas.

Felipe Voloch a accepté la charge de rapporteur du mémoire d'Habilitation à Diriger les Recherches. Noam Elkies et René Schoof participent au jury. C'est un grand honneur qu'ils me font tous, et un immense plaisir de pouvoir associer à ces remerciements des mathématiciens dont les noms ont bercé ma formation à la recherche.

Merci à tous les personnels administratifs et techniques qui nous permettent de travailler l'esprit dégagé de la plupart des problèmes matériels.

Salut à tous les étudiants ! Si ce mémoire, par sa forme même, ne porte que sur la recherche, je n'oublie que notre autre mission est leur formation. Qu'ils soient chaque année plus exigeants et plus curieux.

Les derniers mais non les moindres. Merci à ma famille et à ma belle famille pour avoir été un point d'ancrage au long de ces années, merci à Isado, Césaire, Charlélie, Aimée et Rose pour m'avoir suivi et assisté dans ces pérégrinations, entouré de leur amour et de leur confiance.

Il me reste à souhaiter, de façon assez égoïste, que ces bonnes conditions restent réunies pour me permettre de pouvoir exercer ma curiosité encore longtemps !

CHAPITRE 2

Sommes de caractères et fonctions L : généralités

On va essayer d'expliquer dans cette section les différentes idées qu'ont suivies les mathématiciens dans l'étude des sommes de caractères provenant de la géométrie algébrique, ainsi que les principaux résultats connus sur ces objets mathématiques. L'auteur ne prétend pas donner un compte rendu exhaustif des travaux menés sur le sujet - c'est un travail qui dépasserait de loin, en volume et en temps, l'objectif de ce mémoire - mais dégager les principaux problèmes qui se posent et essayer ainsi d'aider le lecteur à entrer dans la problématique qui sous-tend ce travail.

La première partie est consacrée aux sommes de Gauss, qui sont l'exemple le plus simple de sommes de caractères. Elles en sont pourtant un archétype, puisqu'elles permettent, à travers un certain nombre de résultats classiques (relation de Davenport Hasse, congruences de Stickelrberger) d'observer la plupart des phénomènes qui vont nous intéresser. La seconde donne des résultats plus généraux à l'aide de la géométrie algébrique et de la cohomologie étale, à la suite des travaux de Weil, Grothendieck et Deligne. La troisième expose les principales idées de Dwork dans sa démonstration de la rationalité des fonctions zêta (on ne respecte pas l'ordre chronologique des résultats). Dans la quatrième partie, on décrira des polygones combinatoires donnant des informations sur les valuations p-adiques des sommes de caractères, puis des applications de ces idées dans la cinquième. La dernière est un résumé très rapide des contributions de l'auteur, qu'on espère avoir ainsi remises dans leur contexte.

1. Sommes de Gauss

La plus connue des familles de sommes de caractères est sans doute la famille des **sommes quadratiques de Gauss**, qu'on retrouvera plusieurs fois dans ce mémoire. Il s'agit des sommes suivantes (où p désigne un nombre premier) :

$$\mathscr{G}_p = \sum_{n=0}^{p-1} \exp\left(\frac{2i\pi n^2}{p}\right).$$

Elles ont été étudiées en 1801 par Gauss dans ses Disquitiones Arithmeticae [**21**] pour sa démonstration de la loi de réciprocité quadratique. Il a montré que ce nombre complexe est de module $|\mathscr{G}_p| = \sqrt{p}$. Quelques années plus tard, Gauss a fini de les calculer, obtenant la formule

$$\mathscr{G}_p = \begin{cases} \sqrt{p} & \text{si} \quad p \equiv 1 \mod 4 \\ i\sqrt{p} & \text{si} \quad p \equiv 3 \mod 4 \end{cases}$$

On va voir que cette formule est archétypale des résultats qui vont nous intéresser ici.

Commençons par élargir un peu le cadre. Notons $k = \mathbb{F}_q$, le corps fini à $q = p^m$ éléments. Soit $\psi := \psi_y$ le caractère additif (non trivial) de k défini par $x \mapsto \exp\left(\frac{2i\pi}{p}\mathrm{Tr}(xy)\right)$ pour un certain $y \in k^\times$, et Tr la trace de $k/\mathbb{F}_p$. De même soit χ un caractère multiplicatif de $k^\times$, d'ordre s un diviseur de $q-1$. On définit alors la **somme de Gauss associée à ces deux caractères** par

$$\mathscr{G}(\psi, \chi) := \sum_{x \in k} \psi(x)\chi(x).$$

C'est une conséquence élémentaire de la formule de Poisson qu'on a $\mathscr{G}(\psi_1, \chi_2) = \mathscr{G}_p$ quand $k = \mathbb{F}_p$, et χ_2 le caractère quadratique (d'ordre 2). On a donc obtenu une généralisation de la somme de Gauss quadratique.

Un résultat bien connu sur ces sommes est la **relation de Davenport Hasse**. Si k_r est l'extension algébrique de degré r de k, $\psi_r := \psi \circ \mathrm{Tr}_{k_r/k}$ et $\chi_r := \chi \circ \mathrm{N}_{k_r/k}$ les extensions des caractères ψ et χ à k_r, alors on a

$$-\mathscr{G}(\psi_r, \chi_r) = \left(-\mathscr{G}(\psi, \chi)\right)^r.$$

En d'autres termes, à partir la famille de sommes de Gauss $(\mathscr{G}(\psi_r,\chi_r))_{r\geq 1}$, on peut former la **fonction** L

$$L(\mathscr{G}(\psi,\chi);T) := \exp\left(\sum_{r\geq 1}\mathscr{G}(\psi_r,\chi_r)\frac{T^r}{r}\right) = 1-\mathscr{G}(\psi,\chi)T$$

qui possède la propriété remarquable d'être un polynôme de degré 1, dont la racine réciproque est la somme de Gauss originelle.

On va maintenant s'intéresser aux propriétés de divisibilité des sommes de Gauss, en donnant les **congruences de Stickelberger** (*cf.* [**8**], [**63**]). La somme de Gauss $\mathscr{G}(\psi,\chi)$ est un entier algébrique du corps de nombres $K := \mathbb{Q}(\zeta_p,\zeta_{q-1})$. On sait que l'idéal premier (p) se décompose en produits d'idéaux premiers $(p) = \mathfrak{p}_1\dots\mathfrak{p}_g$ dans l'anneau des entiers $\mathcal{O}_K := \mathbb{Z}[\zeta_p,\zeta_{q-1}]$ de K. Choisissons $\mathfrak{p}$, l'un des $\mathfrak{p}_i$, et notons ω le caractère de Teichmüller associé à $\mathfrak{p}$, c'est à dire le caractère d'ordre $q-1$ de $k\simeq\mathcal{O}_K/\mathfrak{p}$ qui envoie la classe de ζ_{q-1} sur ζ_{q-1}. Pour $0\leq a\leq q-2$ un entier, on sait alors

$$\mathscr{G}(\psi,\omega^{-a}) \equiv -\frac{(\zeta_p-1)^{\sigma_p(a)}}{p(a)}\ [\mathfrak{p}^{s(a)+1}], \tag{1}$$

où $\sigma_p(a)$ désigne la somme des chiffres p-adiques de a, et $p(a)$ le produit de leurs factorielles. On peut reformuler ce résultat de deux autres façons, un peu moins précises, mais qui reflètent bien un certain nombre de résultats de ce mémoire

(1) dans $K_{\mathfrak{p}}$, le corps p-adique obtenu en complétant K le long de la place $\mathfrak{p}$, la somme de Gauss $\mathscr{G}(\psi,\omega^{-a})$ est de valuation p-adique $\frac{\sigma_p(a)}{p-1}$ (puisque le premier (p) est ramifié d'indice $p-1$ dans K) ;
(2) le polygône de Newton (pour la valuation p-adique) de la fonction $L(\mathscr{G}(\psi,\chi);T)$ est constitué d'un segment de longueur (horizontale) 1 et de pente $\frac{\sigma_p(a)}{p-1}$.

On renvoie le lecteur désireux d'avoir plus de détails sur les sommes de Gauss (et bien d'autres) au livre de Berndt, Evans et Williams [**8**].

2. Sommes provenant de la géométrie algébrique

Continuons d'élargir le cadre. Soit X un schéma séparé et de type fini (une variété algébrique) sur le corps fini k, de dimension d. On supposera dans la suite que f est une fonction régulière sur X, c'est à dire un élément de $\Gamma(X,\mathcal{O}_X)$, et g une fonction régulière sans zéro sur X, $g\in\Gamma(X,\mathcal{O}_X^\times)$, ce qui est toujours possible quitte à restreindre X à un de ses ouverts. On note alors $X(k_r)$ l'ensemble des k_r-points de X, c'est à dire des morphismes de X vers Spec k_r sur Spec k.

On définit les sommes de caractères

$$S_r(X,f,g) := \sum_{x\in X(k_r)}\psi_r(f(x))\chi_r(g(x)),$$

et on leur associe la fonction L définie par

$$L(X,f,g;T) := \exp\left(\sum_{r\geq 1}S_r(X,f,g)\frac{T^r}{r}\right).$$

Dans le cas où X est une courbe (une variété de dimension 1), il résulte des travaux de Weil que cette fonction est un polynôme, dont on sait exprimer le degré à l'aide du genre de X et des diviseurs $(f)_\infty$ (des pôles de f) et $(g)_0,(g)_\infty$ (respectivement des zéros et des pôles de g) sur la courbe complète $\overline{X}$. De plus toutes les racines réciproques sont des q-nombres de Weil de poids 1.

Définition 2.1. *Soit w un entier positif. On appelle q-nombre de Weil de poids w un entier algébrique de module complexe $q^{\frac{w}{2}}$, dont tous les conjugués par un automorphisme de $\overline{\mathbb{Q}}$ sont de module complexe $q^{\frac{w}{2}}$.*

On va voir comment ces résultats ont été généralisés en dimension supérieure par Grothendieck et Deligne. C'est Dwork qui, le premier, a montré la rationalité des fonctions L dans le cas général, et on décrira ses méthodes un peu plus loin.

Remarque 2.1. *Notons que les fonctions L contiennent les fonctions zêta des variétés algébriques sur les corps finis comme cas particulier. Par exemple, si X est la variété affine définie dans $\mathbb{A}^n$ par l'annulation de t polynômes $f_1, \dots, f_t \in k[x_1, \dots, x_n]$ (ce qui revient au même, X est l'intersection des hypersurfaces H_i d'équations respectives $f_i = 0$), on peut compter son nombre de points à l'aide de sommes de caractères (additifs) associées au polynôme*

$$g(x_1, \dots, x_{n+t}) := x_{n+1}f_1 + \cdots + x_{n+t}f_t.$$

En effet il résulte des relations d'orthogonalité des caractères additifs que la somme $\sum_{x_{n+1},\dots,x_{n+t}\in k} \psi(g(x_i))$ est non nulle ssi $(x_1, \dots, x_n)$ est un point de X, auquel cas elle vaut q^t. On en déduit la relation

$$Z(X/k; q^tT) = L(g; T),$$

et on pourrait faire de même pour des variétés toriques ou projectives. La méthode qu'on vient de décrire est proche de la méthode originale de Dwork. Elle a par exemple été utilisée dans [**5**] *pour montrer la conjecture de Katz sur les polygones de Hodge et Newton dans le cas affine.*

2.1. Interprétation en cohomologie étale. Dans ce numéro, on va décrire la fonction $L(X, f, g; T)$ définie plus haut à l'aide de la cohomologie étale de X à valeurs dans un certain faisceau ℓ-adique. On en déduira quelques unes des propriétés de la fonction. L'exposition est proche de [**14**, Sommes Trig.], le lecteur intéressé trouvera une autre belle introduction à ce sujet dans [**32**, Ch III].

Notons $\mathbb{G}_a = \mathbb{A}^1$ (*resp.* $\mathbb{G}_m$) la variété en groupes (affine) du groupe additif (*resp.* multiplicatif), définie sur k, et F le morphisme de Frobenius sur ces variétés, relatif à k, défini par $x \mapsto x^q$. Soit L_a l'isogénie de Lang sur $\mathbb{G}_a$, c'est à dire $L_a = F - Id_{G_a}$; elle est surjective, et on obtient le suite exacte suivante de variétés en groupes

$$0 \longrightarrow \mathbb{G}_a(k) \longrightarrow \mathbb{G}_a \xrightarrow{L_a} \mathbb{G}_a \longrightarrow 0.$$

Notons $\mathcal{L}_a$ le $\mathbb{G}_a(k) = k$-torseur sur $\mathbb{G}_a$ défini par cette suite exacte (cf. [**14**, 1.7]). De même on définit l'isogénie de Lang sur $\mathbb{G}_m$ par $L_m(x) = x^{q-1}$, et on note $\mathcal{L}_m$ le $\mathbb{G}_m(k) = k^\times$-torseur sur $\mathbb{G}_m$ défini par la suite exacte

$$0 \longrightarrow \mathbb{G}_m(k) \longrightarrow \mathbb{G}_m \xrightarrow{L_m} \mathbb{G}_m \longrightarrow 0.$$

Fixons un nombre premier ℓ distinct de p, et notons encore ψ le caractère d'ordre p de k vers $\overline{\mathbb{Q}}_\ell^\times$ correspondant à ψ par un plongement fixé une fois pour toutes de $\overline{\mathbb{Q}}_\ell$ dans $\mathbb{C}$. Au torseur $\mathcal{L}_a$, on associe un $\overline{\mathbb{Q}}_\ell$-faisceau, lisse et de rang 1, $\mathcal{L}_\psi := \psi(\mathcal{L}_a)$ sur $\mathbb{A}^1$. De même, pour χ un caractère multiplicatif de $k^\times$, on définit le $\overline{\mathbb{Q}}_\ell$-faisceau, lisse et de rang 1, $\mathcal{L}_\chi := \chi(\mathcal{L}_m)$ sur $\mathbb{G}_m$.

Soient f et g deux fonctions sur X comme plus haut. Considérons le faisceau $\mathcal{F} = f^*\mathcal{L}_\psi \otimes g^*\mathcal{L}_\chi$ sur X. Pour x un point fermé de X, disons $x \in X(k_r)$, soit $\overline{x}$ un point géométrique au dessus de x. La fibre $\mathcal{F}_{\overline{x}}$ est un $\overline{\mathbb{Q}}_\ell$-espace vectoriel de dimension 1, sur lequel agit le groupe $\mathrm{Gal}(k(\overline{x})/k(x))$. L'action du Frobenius géométrique relatif à $k(x)$, $F_{\overline{x}}$, est la multiplication par $\psi(\mathrm{Tr}_{k_r/k}(f(x)))\chi(N_{k_r/k}(g(x)))$; en d'autres termes la trace de l'action de $F_{\overline{x}}$ sur $\mathcal{F}_{\overline{x}}$ est cette racine de l'unité.

Notons $H^i_c(X, \mathcal{F})$, $0 \le i \le 2d$, les $\overline{\mathbb{Q}}_\ell$-espaces vectoriels de dimension finie provenant de la cohomologie à supports compacts de X, à valeurs dans le faisceau ℓ-adique $\mathcal{F}$. Le morphisme de Frobenius F_X associé à X agit linéairement sur ces espaces, et la formule des traces de Lefschetz [**23**] nous assure, pour tout $r \ge 1$, l'égalité

$$S_r(X, f, g) = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(F_X^r | H^i_c(X, \mathcal{F})).$$

L'avatar, pour les fonctions L, de cette formule, est

$$L(X, f, g; T) = \prod_{i=0}^{2d} \det(1 - TF_X | H^i_c(X, \mathcal{F}))^{(-1)^{i+1}}. \tag{2}$$

et on en déduit en particulier la rationalité de la fonction L. En d'autres termes, celle-ci s'écrit sous la forme

$$L(X, f, g; T) = \frac{P_1(T) \dots P_{2d-1}(T)}{P_0(T) \dots P_{2d}(T)},$$

où les P_i sont des polynômes de degré $b_i = \dim H^i_c(X, \mathcal{F})$, le i-ième *nombre de Betti*.

2.2. Pôles et racines réciproques. On vient d'obtenir la rationalité des fonctions L. Dans cette section, on va recenser les informations sur les racines et zéros réciproques de ces fonctions.

Pour chaque $0 \leq i \leq 2d$, notons $P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}Y)$. Il résulte du théorème pricipal de Deligne, Weil II [**15**] que puisque $\mathcal{F}$ est un faisceau ponctuellement pur de poids nul, toutes les valeurs propres de l'action de Frobenius sur $H^i_c(X, \mathcal{F})$ sont des entiers algébriques, et pour chacune il existe un entier $m \leq i$ tel que tous ses conjugués complexes soient de module $q^{\frac{m}{2}}$. En d'autres termes, les racines réciproques de $P_i(T)$ sont des q-nombres de Weil de poids inférieur à i.

D'autre part, la dualité de Poincaré assure qu'il y a une dualité entre les espaces $H^i_c(X, \mathcal{F})$ et $H^{2d-i}_c(X, \mathcal{F}^\vee(d))$, où $\mathcal{F}^\vee$ désigne le faisceau dual de $\mathcal{F}$. En particulier les valeurs propres du Frobenius agissant sur ce dernier espace sont les $\frac{q^d}{\alpha_{ij}}$, et les deux nombres α_{ij} et $\frac{q^d}{\alpha_{ij}}$ sont des entiers algébriques. En conséquence, pour tout $\ell \neq p$, ces nombres sont des unités ℓ-adiques.

Il reste à se poser la question de leurs valuations p-adiques.

3. Intreprétation p-adique et polygones de Newton ; les idées de Dwork

On a vu un certain nombre de propriétés des nombres de Weil des sommes de caractères. Dans cette section, on va s'intéresser à leurs valuations p-adiques. Le prototype de ces résultats est le théorème de Stickelberger sur les sommes de Gauss. Dans un premier temps, on va décrire les travaux de Dwork, qui lui ont permis de montrer la rationalité des fonctions zêta. Dans les deux sections suivantes, on va insister sur leurs conséquences en termes de valuations des nombres de Weil associés à des sommes de caractères. Finalement, on va illustrer leur importance en décrivant deux familles de résultats classiques qui reposent sur la connaissance des valuations p-adiques des nombres de Weil, puis en expliquant rapidement l'utilisation récente des idées de Dwork pour compter effectivement le nombre de points d'une variété algébrique sur un corps fini.

Remarque 3.1. *Commençons par remarquer que si α est un nombre de Weil associé à un faisceau construit comme à la section précédente, l'intégrité simultanée de α et $\frac{q^d}{\alpha}$ assure que* $0 \leq \mathrm{ord}_q(\alpha) \leq d$.

On va maintenant rappeler la définition des polygones de Newton. Dans toute la suite on note ord_p (*resp.* ord_q) la valuation p-adique normalisée par $\mathrm{ord}_p(p) = 1$ (*resp.* $\mathrm{ord}_q(q) = 1$)

Définition 3.1. *Soit $P(T) = \sum_{i=0}^d a_i T^i \in K[T]$ un polynôme à coefficients dans un corps p-adique K. Le polygone de Newton de P pour la valuation* ord_p *est le graphe de la plus grande fonction f convexe et affine par morceaux sur $[0, d]$ telle que tous les points de coordonnées $(i, \mathrm{ord}_p(a_i))$ soient dans l'épigraphe de f. On le note* $\mathrm{NP}_p(P)$.

On définirait de même $\mathrm{NP}_q(P)$*, le polygone de Newton de P pour la valuation* ord_q.

Le lien entre le polygone de Newton et les racines réciproques d'un polynôme est donné par le théorème suivant. C'est une conséquence de l'expression des coefficients d'un polynôme à l'aide des polynômes symétriques élémentaires, évalués en les racines.

Théorème 3.1. *Le nombre de racines réciproques α de P de valuation* $\mathrm{ord}_p(\alpha) = r$ *est égal à la longueur horizontale du segment de pente r dans le polygone* $\mathrm{NP}_p(P)$.

C'est à dire que pour connaître les valuations p-adiques des racines (réciproques) d'un polynôme P, il suffit de construire son polygone de Newton. C'est ce qu'on fera généralement dans la suite.

Pour le rôle fondateur qu'elles ont joué dans le développement des théories cohomologiques p-adiques, nous décrivons maintenant les idées mises en œuvre par Dwork dans sa démonstration de la rationalité des fonctions L. On peut dire sans galvauder le terme qu'il s'agissait alors (à la fin des années cinquante) d'idées révolutionnaires, puisque les mathématiciens espéraient plutôt une démonstration cohomologique (à la Weil) de ce résultat.

Prenons l'exemple d'une hypersurface X de $\mathbb{A}^n$ d'équation $F(x) = 0$ (auquel se ramène Dwork). Par les relations d'orthogonalité des caractères additifs, et un argument d'inclusion-exclusion, il y a un lien entre le nombre de points de X dont aucune des coordonnées n'est nulle et la somme

$$\sum_{x \in (k^\times)^n,\ y \in k^\times} \psi(yF(x)).$$

3.1. Fonctions de Dwork. La première idée de Dwork est de construire des séries entières p-adiques, qui représentent le caractère ψ en ce sens que (on se réfèrera au chapitre 7 pour des définitions précises, et une généralisation de ces fonctions)

Définition 3.2. *On appelle fonction de Dwork pour k une série entière p-adique θ surconvergente (de rayon de convergence > 1) telle que, si pour tout x de k_r, $\widetilde{x}$ désigne son relèvement au Teichmüller $\mathcal{T}_{mr}$, alors*

1. *la fonction $x \mapsto \theta(\widetilde{x})$ est un caractère additif non trivial ψ de k, à valeurs dans $\mathbb{Q}_p(\zeta_p)$;*
2. *Pour chaque $r \geq 1$, le caractère additif ψ_r de k_r obtenu en composant ψ avec la trace de k_r sur k admet la représentation suivante :*

$$\forall x \in k_r,\ \psi_r(x) = \prod_{i=0}^{r-1} \theta(\widetilde{x}^{p^i}).$$

Si $F(x) = \sum_{\mathbf{i}} a_{\mathbf{i}} x^{\mathbf{i}}$, on a donc $\psi(yF(x)) = \Theta(\widetilde{x}, \widetilde{y})$, pour Θ la série $\Theta(T,U) = \theta(U)\prod_{\mathbf{i}} \theta(\widetilde{a}_{\mathbf{i}} T^{\mathbf{i}}) = \sum_{\mathbf{i}=(\mathbf{i}_1,\mathbf{i}_2)} h_{\mathbf{i}} T^{\mathbf{i}_1} U^{\mathbf{i}_2}$. A partir d'une telle fonction, on sait maintenant écrire le nombre de points à l'aide de la somme

$$\sum_{x \in (\mathcal{T}^\times)^n,\ y \in \mathcal{T}^\times} \Theta(x,y).$$

3.2. La formule des traces. La seconde idée est d'exprimer la somme qu'on vient d'exhiber comme la trace d'un endomorphisme complètement continu d'un espace de Banach p-adique. Dwork définit un opérateur sur l'espace des séries entières p-adiques par

$$\Psi_q(\sum_{\mathbf{i}} a_{\mathbf{i}} x^{\mathbf{i}}) = \sum_{\mathbf{i}} a_{q\mathbf{i}} x^{\mathbf{i}}.$$

Alors l'endomorphisme $\Psi_q \circ \Theta$ sur un espace de séries entières p-adiques surconvergentes (où Θ est la multiplication par la série entière Θ) a pour trace

$$\begin{array}{rcl} \mathrm{Tr}(\Psi_q \circ \Theta) & = & \mathrm{Tr}\left(\Psi_q \circ \sum h_{\mathbf{i}} T^{\mathbf{i}_1} U^{\mathbf{i}_2}\right) \\ & = & \sum_{\mathbf{i}} h_{\mathbf{i}} \mathrm{Tr}\left(\Psi_q \circ T^{\mathbf{i}_1} U^{\mathbf{i}_2}\right) \\ & = & \sum_{\mathbf{i}} h_{(q-1)\mathbf{i}}\ ; \end{array}$$

(la somme converge puisque la fonction Θ est surconvergente). D'autre part la somme qu'on vient d'écrire s'interprète comme somme des valeurs de Θ en les racines $(q-1)$-ièmes de l'unité, c'est à dire en les points du Teichmüller

$$(q-1)^{n+1} \sum_{\mathbf{i}} h_{(q-1)\mathbf{i}} = \sum_{x \in (\mathcal{T}^\times)^n,\ y \in \mathcal{T}^\times} \Theta(x,y),$$

et de la même façon le r-ième itéré de $\Psi_q \circ \Theta$ donnera le nombre de points de X sur l'extension k_r. On en déduit que la fonction zêta de X est, à peu de choses près, la "série entière caractéristique" de la matrice (de taille infinie, en fait c'est un déterminant de Fredholm, et on pourra consulter avec profit l'article de Serre [**61**] sur ce point) de $\Psi_q \circ \Theta$.

3.3. Rationalité. La vision de Dwork à cette époque est souvent qualifiée de "pré cohomologique", en ce sens qu'elle n'utilise pas de cohomologie, mais lui ouvre la voie. En deux mots, à partir des séries entières qu'il vient de construire, et de certaines de leurs propriétés (elles sont à coefficients entiers, quotients de fonctions entières, et de rayon de convergence non nul), Dwork montre la rationalité en généralisant un ancien résultat de É. Borel.

À la suite de ces résultats, des théories cohomologiques ont été développées (cohomologie de Monsky Washnitzer, cristalline, etc...). Le principe est le suivant : dans certains cas, on peut construire des opérateurs différentiels commutant avec l'opérateur $\Psi_q \circ \Theta$. À l'aide des conoyaux de ces opérateurs (la cohomologie de de Rham), ou de complexes de Koszül construits sur ces opérateurs, on peut ainsi construire des espaces vectoriels p-adiques de dimension finie (quand on sait démontrer toutefois que les opérateurs différentiels ont un indice). La fonction L est alors le polynôme caractéristique d'une matrice. Une estimation des valuations p-adiques des coefficients des matrices qu'on obtient donne alors des estimations pour les valuations des nombres de Weil.

Ces résultats auront une grande importance dans la suite, on va rappeler certains d'entre eux dans la section qui vient.

4. Sommes de caractères associées à des polynômes de Laurent

Les résultats qu'on vient de donner sont très généraux, et on ne sait en général pas calculer les nombres de Betti, ou déterminer exactement les poids des nombres de Weil. Dans cette section, on va décrire un cas particulier dans lequel on sait, sous certaines hypothèses,

(1) que la cohomologie est concentrée en dimension médiane (c'est à dire que seul l'espace $H_c^d(X, \mathcal{F})$ est non nul) ;

(2) calculer la dimension de cet espace ;

(3) calculer les poids des nombres de Weil ;

(4) donner une borne inférieure pour le polygone de Newton du polynôme $P_d^{(-1)^{n-1}}$.

C'est surtout ce dernier résultat qu'on va expliciter dans ce chapitre.

Soit $f \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ un polynôme de Laurent en n variables. Considérons les sommes de caractères

$$S_r(f) = \sum_{\mathbf{x} \in \mathbb{G}_m^n(k_r)} \psi(f(\mathbf{x})),$$

et la fonction $L(f;T)$ associée. De même si χ est un caractère multiplicatif de $(k^\times)^n$, on note $L(f, \chi; T)$ la fonction L associée aux sommes de caractères (qu'on appellera *tordues* dans la suite)

$$S_r(f, \chi) = \sum_{\mathbf{x} \in \mathbb{G}_m^n(k_r)} \psi(f(\mathbf{x}))\chi(\mathbf{x}).$$

Ce cas particulier couvre de nombreux cas intéressants, parmi lesquels celui des fonctions zêta de variétés affines, toriques ou projectives (voir la remarque 2.1).

Le premier résultat dans ce sens est dû à Deligne. Il a montré à l'aide de la cohomologie étale (*cf.* [**13**]) que si f est un polynôme de degré d en n variables dont la partie homogène de plus haut degré définit une hypersurface lisse de l'espace projectif, alors la première propriété ci-dessus est vérifiée, et la dimension de $H_c^n(\mathbb{G}_m^n, f^*\mathcal{L}_\psi)$ est $(d-1)^n$.

Dans le cas général, ce théorème se réinterprète de la façon suivante (les résultats qu'on va décrire sont dûs à Adolphson et Sperber [**2**], et proviennent de l'acyclicité d'un complexe de Koszül, montrée sur $\mathbb{C}$ par Kouchnirenko [**39**]). Soit Δ le *polyèdre de Newton à l'infini de* f : si $f = \sum_{\mathbf{i} \in \mathbb{Z}^n} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$ (la somme est finie), alors Δ est l'enveloppe convexe dans $\mathbb{R}^n$ des points $\mathbf{i}$ de $\mathbb{Z}^n$ tels que le monôme $\mathbf{x}^{\mathbf{i}}$ apparaisse effectivement dans l'écriture de f, et de l'origine. En particulier Δ est un polyèdre convexe et entier.

Soit σ une face de Δ ; on note f_σ la restriction de f à la face σ, c'est à dire le polynôme $\sum_{\mathbf{i} \in \sigma} a_{\mathbf{i}} x^{\mathbf{i}}$. Quand f est *non-dégénéré par rapport à* Δ, c'est à dire quand pour toute face σ de Δ ne contenant pas l'origine, le sous-schéma de $\mathbb{G}_m^n/k$ défini par

$$\frac{\partial f_\sigma}{\partial x_1} = \dots = \frac{\partial f_\sigma}{\partial x_n} = 0$$

est vide, on a les résultats suivants (*cf.* [**2**], [**17**])

Théorème 4.1. *Supposons que* Δ *engendre* $\mathbb{R}^n$ *; si* Vol *désigne le volume sur* $\mathbb{R}^n$ *provenant de la mesure usuelle, alors*

(1) *Pour tout* $i \neq n$, $H_c^i(\mathbb{G}_m^n, f^*\mathcal{L}_\psi) = 0$ *;*

(2) $\dim H_c^n(\mathbb{G}_m^n, f^*\mathcal{L}_\psi) = n!\mathrm{Vol}(\Delta)$ *;*

(3) *Si l'origine est un point intérieur à* Δ*, ce dernier espace est pur de poids* n *(toutes les valeurs propres de l'action de Frobenius sont des* q*-nombres de Weil de poids* n*).*

Dans le cas général, Denef et Loeser décrivent les poids des valeurs propres de Frobenius [**17**, Theorem 1.8]. On a donc une réponse précise aux premières questions de ce chapitre. Il ne manque que la description du polygone de Newton de la fonction L.

C'est une question difficile, car ces polygones varient beaucoup avec le polynôme. On va expliciter des polygones combinatoires (improprement) appelés polygones de Hodge dans la littérature, et qui donnent de bonnes bornes inférieures pour les polygones de Newton des fonctions L qu'on vient de décrire, puis décrire les liens entre ces polygones et les "vrais" polygones de Newton, liens en grande partie conjecturaux.

Comme d'habitude, on identifie les valuations q-adiques des racines réciproques d'un polynôme avec les pentes des segments de son polygone de Newton q-adique. Pour simplifier les notations, nous noterons $\mathrm{NP}_q(f)$ (*resp.* $\mathrm{NP}_q(f,\chi)$) le polygone de Newton q-adique de $L(f;T)^{(-1)^{n-1}}$ (*resp.* de $L(f,\chi;T)^{(-1)^{n-1}}$) dans la suite.

Si Π est un polygone convexe de longueur l, c'est à dire le graphe d'une fonction convexe, continue sur l'intervalle $[0,l]$ et affine par morceaux sur chacun des intervalles $[i-1,i]$, on notera $\Pi=(\pi_i)_{1\leq i\leq l}$ quand sa pente sur $[i-1,i]$ est π_i. Si Π_1 et Π_2 sont deux polygones convexes de longueur l, on écrira $\Pi_1\preceq\Pi_2$ quand Π_1 est au dessus de Π_2, et que leurs extrémités coïncident.

4.1. Polygones pour les sommes additives. Adolphson et Sperber ont prouvé [**2**, Theorem 3.10] l'existence d'une borne inférieure pour les polygones de Newton des fonctions $L(f;T)^{(-1)^{n-1}}$ quand f décrit l'ensemble des polynômes non dégénérés de polyèdre Δ. Cette borne est souvent appelée *polygone de Hodge*, et notée $\mathrm{HP}(\Delta)$. Il s'agit d'un invariant ne dépendant que de Δ, que nous allons maintenant décrire. Remarquons qu'il ne s'agit en général ni du polygone de Hodge d'un cristal comme dans [**31**], ni d'un polygone de Hodge géométrique, ces deux familles de polygones ayant toutes leurs pentes entières, comme on le verra dans la section 5.2. En revanche ces derniers sont des cas particuliers de la construction suivante, puisqu'ils proviennent de fonctions zêta qui sont des cas particuliers de fonctions L.

Notons $C(\Delta):=\mathbb{R}_+\Delta$ le cône de Δ dans $\mathbb{R}^n$, $M_\Delta:=C(\Delta)\cap\mathbb{Z}^n$ le monoïde associé à ce cône, et $\mathcal{A}_\Delta$ l'algèbre $k[M_\Delta]$. On peut définir une application de $C(\Delta)$ dans $\mathbb{R}_+$, le *poids associé à* Δ par

$$w_\Delta(\mathbf{u})=\min\{\rho\in\mathbb{R}_+,\ \mathbf{u}\in\rho\Delta\}.$$

Les sommets du polyèdre Δ étant dans $\mathbb{Z}^n$, l'image de M_Δ par w_Δ est contenue dans $\mathbb{Q}_+$, et plus précisément dans $\frac{1}{D}\mathbb{N}$ pour un certain entier $D>0$, minimal, qu'on appellera dans la suite le *dénominateur de* Δ. Le poids w_Δ fait de l'algèbre $\mathcal{A}_\Delta$ une algèbre graduée

$$\mathcal{A}_\Delta=\oplus_{i\geq 0}\mathcal{A}_{\Delta,\frac{i}{D}},\ \mathcal{A}_{\Delta,\frac{i}{D}}=\mathrm{Vect}\{\mathbf{x}^{\mathbf{u}},\ w_\Delta(\mathbf{u})=\frac{i}{D}\}$$

à laquelle on associe sa série de Poincaré

$$P_{\mathcal{A}_\Delta}(t):=\sum_{i\geq 0}\dim\mathcal{A}_{\Delta,\frac{i}{D}}t^i.$$

On sait [**39**, Lemme 2.9] que cette série est en fait une fraction rationnelle. Plus précisément, $P_\Delta(t):=(1-t^D)^nP_{\mathcal{A}_\Delta}(t)$ est un polynôme de degré inférieur ou égal à nD, à coefficients entiers positifs ou nuls, et qui vérifie $P_\Delta(0)=1$, $P_\Delta(1)=n!V(\Delta)$. Si on note $P_\Delta(t):=\sum\ell_it^{s_i}$, le polygone $\mathrm{HP}(\Delta)$ est alors le polygone convexe commençant à l'origine, et formé de la juxtaposition des segments de longueur horizontale ℓ_i et de pente $\frac{s_i}{D}$. Par commodité, on l'appellera aussi dans la suite le *polygone issu de la série de Poincaré* $P_{\mathcal{A}_\Delta}$. Le résultat d'Adolphson et Sperber se réécrit donc ainsi : pour tout polynôme f de $k[\mathbf{x},\mathbf{x}^{-1}]$ de polyèdre Δ et non dégénéré, on a $\mathrm{NP}_q(f)\preceq\mathrm{HP}(\Delta)$.

Il est maintenant naturel de se demander comment varient les polygones $\mathrm{NP}_q(f)$ quand f varie parmi les polynômes de polyèdre fixé, non dégénérés. Malheureusement ces variations sont très difficiles à contrôler ; des calculs explicites dans le cas de polynômes de petit degré en une variable montrent qu'il est illusoire d'espérer donner une réponse complète à cette question (*cf.* [**26**], [**27**]). Pour contourner cette difficulté, on préfère parler de *polygone de Newton générique* ; c'est la borne inférieure des $\mathrm{NP}_q(f)$ quand f décrit les polygônes de polyèdre fixé à coefficients dans $\mathbb{F}_q$, n'importe quel sous corps de $\overline{\mathbb{F}}_p$. Le théorème de spécialisation de Grothendieck [**31**] assure que cette borne inférieure existe. Ce polygone ne dépend pas de q, mais seulement de p, et on le note $\mathrm{GNP}(\Delta,p)$. Dans le cas de la dimension 1, on sait calculer explicitement ce polygone **[BF]**, [**46**], ainsi que le polynôme de Hasse, qui détermine l'hypersurface de l'espace des polynômes hors de laquelle on a $\mathrm{NP}_q(f)=\mathrm{GNP}(\Delta,p)$.

On se pose donc la question du comportement du polygone de Newton générique. Pour des raisons liées à la ramification, il est aisé de voir qu'une condition nécessaire pour qu'il coïncide avec le polygone de Hodge est d'avoir $p\equiv 1 \mod D$. Adolphson et Sperber ont conjecturé que cette condition est suffisante.

La conjecture est avérée en dimension $n \leq 3$, mais elle est fausse en dimension supérieure, où il faut remplacer D par un multiple D^* en général strict, comme l'a démontré Wan [**65**], [**66**] (en revanche, dans certains cas, comme celui du polynôme g de la remarque 2.1, on a $D^* = D$, ce qui permet à Wan de retrouver l'ordinarité générique des intersections complètes). Donc on a $\liminf_{p\to\infty} \mathrm{GNP}(\Delta, p) = \mathrm{HP}(\Delta)$. Wan a conjecturé [**66**, Conjecture 1.11] que la limite existe sous certaines hypothèses, c'est à dire que $\lim_{p\to\infty} \mathrm{GNP}(\Delta, p) = \mathrm{HP}(\Delta)$.

Une autre question, plus difficile, est la suivante : choisissons un polynôme de Laurent $\widetilde{f}$ à coefficients dans $\overline{\mathbb{Q}}$, et soit $\mathbb{Q}_{\widetilde{f}}$ l'extension de $\mathbb{Q}$ engendrée par les coefficients de $\widetilde{f}$. Pour chaque premier p de $\mathbb{Q}$, on choisit $\mathfrak{p}$ un premier au dessus de p dans le corps $\mathbb{Q}_{\widetilde{f}}$, de corps résiduel $\mathbb{F}_q$. On se demande comment varient les polygones de Newton $\mathrm{NP}_q(\widetilde{f} \mod \mathfrak{p})$ des réductions modulo $\mathfrak{p}$ de $\widetilde{f}$ quand p tend vers l'infini. Considérons l'espace des polynômes à coefficients dans $\overline{\mathbb{Q}}$, de polyèdre de Newton Δ, et de monômes prescrits de façon à ce que le sous-monoïde de M_Δ engendré par les exposants des monômes prescrits contienne tous les éléments de M_Δ à l'exception d'un nombre fini. Alors Wan conjecture [**66**, Conjecture 1.12] qu'il existe un ouvert dense défini sur $\mathbb{Q}$ de l'espace de ces polynômes tel que pour tout $\widetilde{f}$ de cet ouvert on ait

$$\lim_{p\to\infty} \mathrm{NP}_q(\widetilde{f} \mod \mathfrak{p}) = \mathrm{HP}(\Delta).$$

Ce résultat est connu pour l'espace de tous les polynômes de degré d en une variable [**71**, Theorem 1.3], ainsi que pour l'espace des polynômes de Laurent de degrés d et d' en une variable [**43**].

4.2. Polygones pour les sommes tordues. Dans le cas où χ n'est pas trivial, la situation est un peu plus compliquée.

Soit ω le caractère de Teichmüller de $k^\times$, qui est un générateur du groupe des caractères de $k^\times$. Pour un n-uplet d'entiers $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_n)$, on note $\chi = \omega^{\boldsymbol{\delta}}$ le caractère de $(k^\times)^n$ défini par $\chi(x_1, \ldots, x_n) = \omega(x_1)^{\delta_1} \ldots \omega(x_n)^{\delta_n}$.

Adolphson et Sperber ont montré, toujours sous des conditions de non-dégénérescence, que la fonction L a le même degré que dans le cas additif (*cf.* [**3**], [**4**]). Ils ont aussi donné une borne inférieure pour son polygone de Newton [**4**, Theorem 3.17], qu'on appellera dans la suite *polygone de Hodge associé à* Δ *et* $\boldsymbol{\delta}$, et qu'on notera $\mathrm{HP}(\Delta, \frac{\boldsymbol{\delta}}{q-1})$. On va décrire cette borne inférieure à l'aide de séries de Poincaré, mais on va voir qu'elle dépend maintenant du résidu de p modulo l'ordre du caractère χ. En particulier quand on fixe l'ordre du caractère, on ne peut plus espérer obtenir une limite quand p tend vers ∞, à moins de supposer que le caractère est d'ordre deux.

Nous allons décrire le polygone $\mathrm{HP}(\Delta, \frac{\boldsymbol{\delta}}{q-1})$, dans le cas où le polyèdre Δ engendre l'espace $\mathbb{R}^n$. Pour deux entiers i et $0 \leq \delta \leq q-2$, on note $\delta^{(i)}$ le reste modulo $q-1$ de l'entier $p^i\delta$; remarquons que la suite $(\delta^{(i)})_i$ est périodique : on a $\delta^{(m)} = \delta$, où $m = \log_p q$. On note encore $\boldsymbol{\delta}^{(i)} = (\delta_1^{(i)}, \ldots, \delta_n^{(i)})$.

Soit maintenant $N^{(i)}$ le réseau $\frac{\boldsymbol{\delta}^{(i)}}{q-1} + \mathbb{Z}^n$ de $\mathbb{R}^n$. On note $M_{\Delta,\boldsymbol{\delta}^{(i)}} := C(\Delta) \cap N^{(i)}$, et $\mathcal{A}_{\Delta,\boldsymbol{\delta}^{(i)}}$ le $\mathcal{A}_\Delta$-module $k[M_{\Delta,\boldsymbol{\delta}^{(i)}}]$. Il existe alors un entier positif D, minimal, tel que l'image de tous les $M_{\Delta,\boldsymbol{\delta}^{(i)}}$, $0 \leq i \leq m-1$ par w_Δ soit contenue dans $\frac{1}{D}\mathbb{N}$; on appellera cet entier le *dénominateur de* $(\Delta, \boldsymbol{\delta})$ dans la suite. Muni de ce poids, $\mathcal{A}_{\Delta,\boldsymbol{\delta}^{(i)}}$ devient un $\mathcal{A}_\Delta$-module gradué, auquel on peut associer une série de Poincaré et un polynôme $P_{\Delta,\boldsymbol{\delta}^{(i)}}$ comme plus haut. Notons $\Pi^{(i)}$ le polygone issu de cette série. De plus chacun des polynômes $P_{\Delta,\boldsymbol{\delta}^{(i)}}$ est de degré plus petit que nD, et vérifie $P_{\Delta,\boldsymbol{\delta}^{(i)}}(1) = n!V(\Delta)$. On a ainsi une famille de polygones $\Pi^{(i)}$ pour $0 \leq i \leq a$, tous de même longueur $n!V(\Delta)$.

Définition 4.1. *Si* Π *et* Π' *sont deux polygones de même longueur, on note* $\Pi + \Pi'$ *le polygone dont la pente sur le segment* $[i, i+1]$ *est la somme des pentes de* Π *et* Π' *sur ce segment ; d'autre part, pour un réel* $r > 0$*, on désigne par* $r\Pi$ *le polygone obtenu à partir de* Π *en multipliant toute ses pentes par* r *(c'est en fait l'image de* Π *par l'affinité orthogonale d'axe* Ox*, de direction* Oy *et de rapport* r*).*

Avec ces notations, on sait alors décrire le polygone de Hodge

$$\mathrm{HP}(\Delta, \frac{\boldsymbol{\delta}}{q-1}) = \frac{1}{m} \sum_{i=0}^{m-1} \Pi^{(i)}.$$

On renvoie au chapitre 4 pour une autre construction (qu'on appellera *polygone de Hodge-Stickelberger* et les questions de comportement asymptotique.

5. Applications des estimations p-adiques

On va décrire (rapidement) ici trois des principales conséquences des résultats qu'on vient de décrire. Il s'agit de la divisibilité du nombre de points d'une variété algébrique sur un corps fini de caractérisitique p, de la question de l'ordinarité de ces variétés, et des calculs explicites qui ont vu un développement rapide ces dernières années.

5.1. Valuation p-adique du nombre de points d'une variété. (cf. chapitre 6) Une question importante est la question de la divisibilité du nombre de points des variétés algébriques sur un corps fini. Le théorème de Chevalley-Warning [**67**] est le premier de ces résultats

Théorème 5.1. *Soit $F \in \mathbb{Z}[X_1, \ldots, X_n]$ un polynôme en n variables de degré d. Si $n > d$, alors le nombre de solutions de la congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \mod p$$

est divisible par p.

Ce résultat a été amélioré par Ax [**7**] dans le cas des hypersurfaces, puis par Katz [**29**] dans le cas général.

Théorème 5.2. *Soient $F_i \in k[X_1, \ldots, X_n]$, $1 \leq i \leq t$ des polynômes en n variables de degrés respectifs d_i, et X l'intersection des hypersurfaces d'équation $F_i = 0$. Alors si b est le plus petit entier tel que*

$$b \geq \frac{n - \sum_{i=1}^{t} d_i}{\max_{1 \leq i \leq t} d_i},$$

le nombre de points de X sur k est divisible par q^b.

Le résultat le plus abouti dans cette direction est sans doute dû à Adolphson et Sperber [**1**], et s'interprète élégamment à l'aide des polyèdres de Newton. On en donne la version pour les sommes exponentielles, on pourrait l'appliquer aux nombres de points à l'aide de la remarque 2.1

Théorème 5.3. *Soit $f \in k[X_1, \ldots, X_n]$ un polynôme de polyèdre de Newton à l'infini Δ, et $S(f)$ la somme*

$$\sum_{x \in k^n} \psi(f(x)).$$

Alors si μ est le plus petit rationnel tel que $\mu\Delta$ – l'image de Δ par l'homothétie de centre O et de rapport μ– contienne un point de $\mathbb{N}^n$ dont toutes les coordonnées sont strictement positives, on a

$$\mathrm{ord}_q(S(f)) \geq \mu.$$

5.2. Ordinarité. On va maintenant décrire les conjectures de Katz sur l'ordinarité générique des variétés algébriques sur un corps fini.

Commençons par rappeler une conjecture de Katz, prouvée par Mazur [**50**], qui assure qu'un certain polygone de Newton associé à la fonction zêta d'une variété est au dessus d'un polygone défini par les nombres de Hodge de cette variété. On sait que dans le cas d'une variété projective X, d'intersection complète et lisse de dimension d sur k, la cohomologie étale est donnée par

$$H_c^i(X, \mathbb{Q}_\ell) = \begin{cases} 0 & \text{si} \quad i \text{ impair}, \ i \neq d \\ \mathbb{Q}_\ell\left(-\frac{i}{2}\right) & \text{si} \quad i \text{ pair}, \ i \neq d \\ H_c^d(X, \mathbb{Q}_\ell) & \text{si} \quad i = d \end{cases}$$

c'est à dire que le seul espace "intéressant" est $H_c^d(X, \mathbb{Q}_\ell)$. La conjecture de Katz donne une borne inférieure pour le polygone de Newton de P_d, le polynôme caractéristique de l'action de Frobenius sur cet espace

Théorème 5.4. *Soit X/k une intersection complète, projective et lisse de dimension d. Alors le polygone de Newton de P_d est au dessus du polygone de Hodge, qui est le polygone de Newton du polynôme défini par les nombres de Hodge $h^{i,n-i}$*

$$\prod_{i=0}^{d}(1-q^iT)^{h^{i,n-i}},\ h^{i,n-i}=\dim_k H^{n-i}(X,\Omega^i_{X/k}).$$

Remarque 5.1. *On rencontre aussi ce théorème avec la convention $h^{i,n-i}=\dim_k H^{n-i}(X,\Omega^i_{X/k})-\delta_{i,n-i}$, ce qui signifie que dans ce cas on s'intéresse à l'action de Frobenius sur la cohomologie primitive, et plus sur l'espace $H^d_c(X,\mathbb{Q}_\ell)$ tout entier.*

Ce théorème a été étendu aux intersections complètes dans l'espace affine (ou dans $\mathbb{G}_m^{n_1}\times\mathbb{A}^{n_2}$) par Adolphson et Sperber [**5**]. En fait cette borne inférieure est en général atteinte.

Définition 5.1. *On dit qu'une intersection complète projective lisse de dimension d est ordinaire quand les deux polygones décrits ci-dessus coïncident.*

Alors les intersections complètes sont génériquement ordinaires. En d'autres termes, si S est le k-schéma paramétrant les intersections complètes lisses de multidegré $(n_1,\dots,n_r)$ dans $\mathbb{P}^{d+r}$, et $X\to S$ la famille universelle, alors

Théorème 5.5. *Il existe un ouvert U non vide de S tel que pour tout s de S, la variété X_s est ordinaire.*

Ce théorème a été démontré par Illusie [**28**] dans le cas général, puis par Wan à l'aide des polygones de Newton de sommes de caractères associées à des polynômes de Laurent [**65**].

Remarquons que dans le cas des courbes il admet une expression particulièrement simple (grâce à la dualité de Serre). Ici les deux seuls nombres de Hodge sont $h^{0,1}=h^{1,0}=g$, le genre de la courbe. Le polygone de Hodge est formé de deux segments de longueur g, l'un de pente nulle, l'autre de pente 1. On retrouve bien sûr la définition usuelle des courbes ordinaires à l'aide du p-rang de la jacobienne. L'ordinarité générique des courbes a été prouvée par Koblitz [**37**].

Ces théorèmes ont un lien très fort avec le *théorème de spécialisation de Grothendieck*, dont on se servira souvent dans la suite, selon lequel dans une famille propre et lisse, le polygone de Newton croît par spécialisation.

5.3. Calcul explicite des fonctions zêta. L'intérêt pour les courbes sur les corps finis s'est renouvelé ces dernières années. On a commencé à construire des cryptosystèmes à l'aide des groupes de points rationnels des jacobiennes de telles courbes. Le problème du logarithme discret est difficile dans certains de ces groupes, ce qui explique leur utilisation dans ce cadre.

On sait que le nombre de points rationnels sur k de la jacobienne de C est donné par $P(1)$, où P est le polynôme numérateur de la fonction zêta de C sur k (de degré $2g$). Le premier, Kedlaya [**36**] a montré comment calculer ces fonctions L de façon efficace à l'aide de la cohomologie de Monsky-Washnitzer dans le cas des courbes hyperelliptiques. À sa suite Denef et Vercauteren [**18**] ont généralisé ce travail aux courbes C_{ab}, puis, avec Castryk [**11**] aux courbes non dégénérées. Des algorithmes similaires ont été écrits par Lauder et Wan dans le cas des courbes d'Artin Schreier [**41**], [**42**]. Le principe de ces algorithmes est que les coefficients des matrices de Frobenius (dont le polynôme caractéristique est le numérateur de la fonction zêta) sont assez faciles à calculer avec une certaine précision p-adique. À l'aide des bornes de Weil sur le nombre de points de C, on fixe alors une précision suffisante.

Lauder [**40**] a aussi écrit de tels algorithmes pour des hypersurfaces en s'inspirant des idées de Dwork. On plonge une hypersurface donnée X dans une famille contenant une hypersurface diagonale (calculer le nombre de points d'une hypersurface diagonale est aisé), puis on écrit l'équation différentielle qui décrit la variation de la cohomologie le long d'une telle famille, et on la résout avec une certaine précision p-adique comme plus haut.

6. Contributions de l'auteur

Le reste de ce mémoire est consacré à décrire, assez précisément, mais souvent sans les démonstrations, les résultats de l'auteur autour des questions qu'on vient de décrire.

Le chapitre 3 est consacré à une description des polygones de Newton génériques des fonctions L associés aux sommes provenant des polynômes en une variable. Ces résultats ont été obtenus en collaboration avec Éric Férard d'abord, puis avec Hui June Zhu. Ils sont consignés dans les articles [**BF**], [**BFZ**], et la prépublication [**BF2**].

Le chapitre 4 donne les premiers (à la connaissance de l'auteur) résultats sur le comportement asymptotique des polygones de Newton pour les polynômes en plusieurs variables, quand le dénominateur du polyèdre de Newton est différent de 1, 2. Ces résultats proviennent d'une prépublication [**B2**].

Les chapitres 5 et 6 sont les seuls dans lesquels on ait présenté les démonstrations. Ils sont récents et n'ont été publiés, ou postés, nulle part.

Le chapitre 5 reprend des résultats connus sur la structure de l'opérateur de Frobenius pour certaines sommes exponentielles. Seule la démarche est originale, puisqu'au lieu d'utiliser la transformée de Fourier des faisceaux ℓ-adiques, on utilise ici la cohomologie de Monsky-Washnitzer, à la Robba.

Le chapitre 6 définit un certain invariant, la p-densité, qui est bien adapté à l'étude p-adique des sommes exponentielles ; on y donne de nouvelles minorations pour leur valuation p-adique, et le théorème de Chevalley-Warning qui en découle. On y donne aussi la première pente générique de certaines familles assez générales de courbes d'Artin-Schreier.

Le chapitre 7 contient les premiers travaux de l'auteur [**B4**] autour des idées de Dwork. Il présente une généralisation des "splitting functions" de ce dernier à la représentation de caractères d'ordre une puissance de p, et un théorème à la Stickelberger pour des sommes de Gauss incomplètes. On donne aussi une minoration de la valuation p-adique des sommes incomplètes sur un anneau.

Le dernier chapitre est assez différent puisqu'il est le seul à ne pas utiliser les méthodes p-adiques. On s'y intéresse aux sommes de caractères, cette fois-ci sur certains anneaux. On y démontre la rationalité des fonctions L associées à ces sommes, puis on donne les degrés ainsi que les pôles et racines réciproques de ces fonctions dans quelques cas particuliers. Ces résultats proviennent de [**B3**], [**B1**].

CHAPITRE 3

Etude p-adique des sommes de caractères en une variable, comportement asymptotique des polygones de Newton

1. Interprétation des fonctions L (une variable)

On note $f(x) = \sum_{i=-d_0}^{d_\infty} a_i x^i \in k[x, x^{-1}]$ un polynôme de Laurent en une variable, avec $a_{-d_0} a_{d_\infty} \neq 0$, et ψ un caractère additif non trivial de k. Soit ω un caractère multiplicatif de $k^\times$ d'ordre $q-1$, et $0 \leq e \leq q-2$ un entier. On va décrire une interprétation de la fonction $L(f, \omega^e; T)$ comme polynôme caractéristique d'un endomorphisme dans un espace vectoriel p-adique. On sait [**68**] que c'est un polynôme de degré $d := d_0 + d_\infty$, dont toutes les racines réciproques sont des nombres de Weil de poids 1.

On note K l'extension non ramifiée de degré m de $\mathbb{Q}_p$, $\mathcal{O}$ son anneau de valuation et $\mathcal{T}^\times$ le sous groupe formé des éléments d'ordre fini de $K^\times$. C'est un groupe fini d'ordre $q-1$, et on note $\mathcal{T} := \mathcal{T}^\times \cup \{0\}$. On appelle *relèvement de Teichmüller* l'unique application de k dans $\mathcal{T}$ qui est une section de la réduction modulo p de $\mathcal{O}^\times$ vers k. Soit $\widetilde{f}(x) = \sum_{i=-d_0}^{d_\infty} \widetilde{a}_i x^i$ le relèvement (coefficient par coefficient) de Teichmüller de f. Soit $\mathbb{C}_p$ la complétion d'une clotûre algébrique de $\mathbb{Q}_p$, et Ω un corps algébriquement clos contenant $\mathbb{C}_p$, complet pour une valuation étendant celle de $\mathbb{C}_p$, et tel que le corps résiduel de Ω soit une extension transcendante de $\mathbb{F}_p$. Pour tout $x \in \Omega$, $r \in \mathbb{R}_+$, on note $B(x, r^+)$ (*resp.* $B(x, r^-)$) la boule fermée (*resp.* ouverte) dans Ω de centre x et de rayon r.

On note $A := B(0,1^+) \backslash B(0,1^-)$, et on considère $\mathscr{H}^\dagger(A)$ l'anneau des fonctions analytiques surconvergentes sur A. Soit $\pi \in \mathbb{C}_p$ une racine du polynôme $X^{p-1}+p$. Considérons la fonction $F := X^{\frac{e}{1-q}} \exp(\pi \widetilde{f}(X))$; comme le rayon de convergence de $X \mapsto \exp(\pi X)$ est 1, F n'est pas dans $\mathscr{H}^\dagger(A)$. Soit ∂_F l'opérateur différentiel (où une fonction agit sur $\mathscr{H}^\dagger(A)$ par multiplication)

$$\partial_F := X\frac{d}{dX} + \pi X \widetilde{f}'(X) + \frac{e}{1-q} \quad \left(= F^{-1} \circ X\frac{d}{dX} \circ F \right).$$

Puisque F n'est pas dans $\mathscr{H}^\dagger(A)$, ∂_F est injectif dans $\mathscr{H}^\dagger(A)$. Donc l'indice de ∂_F dans $\mathscr{H}^\dagger(A)$ est la dimension du conoyau. D'après [**55**, Proposition 5.4.3], il est de dimension d.

Définissons la série entière $\theta(X) := \exp(\pi X - \pi X^p)$; c'est une *splitting function* au sens de Dwork [**20**, p 55]. Ses valeurs aux racines $(p-1)$-ièmes de l'unité sont les racines p-ièmes non triviales de l'unité ; en d'autres termes cette fonction est une représentation analytique d'un caractère d'ordre p. Il est bien connu que θ converge pour tout x de $\mathbb{C}_p$ tel que $v_p(x) > -\frac{p-1}{p^2}$, et en particulier on a $\theta \in \mathscr{H}^\dagger(A)$.

Posons $G(X) := \prod_{i=-d_0}^{d_\infty} \theta(a_i X^i) := \sum_{n \geq 0} h_n X^n$, et $H(X) := X^e \prod_{i=0}^{m-1} G^{\tau^i}(X^{p^i})$, où τ est un relèvement du Frobenius de k à $\mathbb{C}_p$ qui laisse π fixé ; puisque θ est surconvergente, G et H le sont aussi et on a $H \in \mathscr{H}^\dagger(A)$.

On considère maintenant l'application ψ_q, définie par $\psi_q f(x) := \frac{1}{q} \sum_{z^q = x} f(z)$ sur $\mathscr{H}^\dagger(A)$; si $f(X) = \sum b_n X^n$, alors $\psi_q f(X) = \sum b_{qn} X^n$. Posons $\alpha := \psi_q \circ H$; les opérateurs ∂_F et α commutent à un facteur q près sur $\mathscr{H}^\dagger(A)$, et on obtient le diagramme commutatif suivant, dont les lignes sont exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{H}^\dagger(A) & \xrightarrow{\partial_F} & \mathscr{H}^\dagger(A) & \longrightarrow & \mathscr{H}^\dagger(A)/\partial_F \mathscr{H}^\dagger(A) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle q\alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \overline{\alpha}} & & \\ 0 & \longrightarrow & \mathscr{H}^\dagger(A) & \xrightarrow{\partial_F} & \mathscr{H}^\dagger(A) & \longrightarrow & \mathscr{H}^\dagger(A)/\partial_F \mathscr{H}^\dagger(A) & \longrightarrow & 0 \end{array} \tag{3}$$

La formule des traces de Dwork assure que pour tout $r \geq 1$, $(q^r-1)S_{k_r}(f,\omega^e)$ est la trace de l'opérateur α^r. On en déduit l'expression suivante pour la fonction L [**55**, p 235]

$$L(f,\omega^e;T) = \frac{\det(1-T\alpha)}{\det(1-qT\alpha)} = \det(1-T\overline{\alpha}).$$

On a donc réécrit la fonction L associée à notre famille de sommes exponentielles comme le polynôme caractéristique d'un endomorphisme d'un espace vectoriel p-adique de dimension finie.

D'autre part on a la factorisation suivante de l'endomorphisme $\overline{\alpha}$: notons $e = \sum_{i=0}^{m-1} p^i e_i$ l'écriture en base p de l'entier e. Si α_i, $0 \leq i \leq m-1$ est l'endomorphisme de $\mathscr{H}^\dagger(A)$ défini par $\alpha_i = \psi_p \circ x^{e_i} G$, et ∂_i l'opérateur différentiel défini par $\partial_i := X\frac{d}{dX} + \pi X\widehat{f}^{\tau^i}(X)' + \frac{e_i}{1-q}$, on a la relation de commutation entre les α_i et les ∂_i suivante : $\alpha_i \circ \partial_i = p\partial_{i+1} \circ \alpha_i$, à un facteur p près, et $\tau^{-1} \circ \alpha_i$ passe au quotient, ce qui nous donne un endomorphisme $\overline{\tau^{-1} \circ \alpha_i}$ de W, le $\mathbb{C}_p$-espace vectoriel de base $\mathcal{B} = \{X^{-d_0}, \ldots, X^{d_\infty - 1}\}$. Donc α_i induit $\overline{\alpha}_i$ de W dans W^τ, le $\mathbb{C}_p$-espace vectoriel W où la multiplication externe est donnée par $\lambda \cdot w = \lambda^\tau w$. D'autre part on a $\alpha = \alpha_{m-1}^{\tau^{m-1}} \ldots \alpha_1^\tau \alpha_0$. Ceci nous donne la relation suivante entre le morphisme τ^m-linéaire $\overline{\alpha}$ de W et les morphismes τ-linéaires $\overline{\alpha}_i$

$$\overline{\alpha} = \overline{\alpha}_{m-1}^{\tau^{m-1}} \ldots \overline{\alpha}_1^\tau \overline{\alpha}_0.$$

2. Polygône de Newton des sommes de caractères purement additives

Dans cette section, on considère un polynôme $f(x) = x^d + \cdots + a_1 x \in k[x]$ et son relèvement de Teichmüller $\widetilde{f}(x) = x^d + \cdots + \alpha_1 x \in K[x]$, unitaire et de degré d. On va utiliser la description de la fonction L associée aux sommes de caractères

$$S_r(f,\psi) := \sum_{x \in k_r} \psi_r(f(x))$$

comme polynôme caractéristique d'un endomorphisme pour calculer le polygone de Newton générique des polynômes de degré d sur k. De même on va calculer le polynôme de Hasse de la famille des polynômes de degré d sur k, c'est à dire l'equation de l'hypersurface de l'espace (affine) de ces polynômes hors de laquelle le polygone de Newton coïncide avec le polygone de Newton générique. On conclura sur le comportement asymptotique des polygones de Newton génériques.

La stratégie est la suivante (on reprend les notations du numéro précédent, tout en remarquant que comme on somme maintenant sur $\mathbb{A}^1$, on considère les restrictions de $\overline{\alpha}$ et $\overline{\alpha}_1$ au sous espace vectoriel engendré par $\mathcal{B}' := \{X, \ldots, X^{d-1}\}$) : si M est la matrice de $\overline{\alpha}$ dans la base $\mathcal{B}'$, alors la fonction L s'écrit

$$L(f;T) = 1 + \sum_{n=1}^{d-1} M_n T^n,$$

où M_n est la somme des mineurs $n \times n$ principaux de M. On va commencer par utiliser la décomposition de $\overline{\alpha}$ vue plus haut, avant de s'intéresser à la fonction L elle même.

Ici la décomposition de $\overline{\alpha}$ s'écrit $\overline{\alpha} = \overline{\alpha}_1^{\tau^{m-1}} \ldots \overline{\alpha}_1^\tau \overline{\alpha}_1$, où α_1 est l'endomorphisme $\alpha_1 = \psi_p \circ G$ avec les notations du numéro précédent. Il est nécessaire d'avoir une idée précise des coefficients, puis des mineurs de la matrice M_1 de $\overline{\alpha}_1$, avant d'utiliser la relation précédente pour "passer" à $\overline{\alpha}$.

2.1. Valuations des coefficients et des mineurs de M_1. Commençons par exprimer l'image du monôme X^n dans la base $\mathcal{B}$ de $\mathscr{H}^\dagger(A)/\partial_F\mathscr{H}^\dagger(A)$. Puisque ∂_F est aussi un opérateur différentiel agissant sur $\mathbb{C}_p[X, \frac{1}{X}]$, on sait [**55**, Theorem 5.6] qu'un supplémentaire de $\partial_F\mathbb{C}_p[X, \frac{1}{X}]$ dans $\mathbb{C}_p[X, \frac{1}{X}]$ est encore un supplémentaire de l'image de ∂_F, $\partial_F\mathscr{H}^\dagger(A)$, dans $\mathscr{H}^\dagger(A)$. On a, pour tout $n \in \mathbb{Z}$

$$\partial_F X^{n-d} = (n-d)X^{n-d} + \pi \sum_{i=1}^{d} i\alpha_i X^{i+n-d},$$

et comme cette fonction poynômiale est dans $\partial_F\mathscr{H}^\dagger(A)$, on obtient les relations, pour tout $n \geq d$

$$X^n \equiv -\frac{n-d}{\pi} X^{n-d} - \sum_{i=1}^{d-1} i\alpha_i X^{i+n-d} \qquad \mod \partial\mathscr{H}^\dagger(A),$$

et pour $n<0$, $X^n \equiv -\frac{\pi}{n}\sum_{i=1}^{d} i\alpha_i X^{i+n} \mod \partial_F \mathscr{H}^\dagger(A)$. Donc pour tout $n\in\mathbb{Z}$, X^n s'écrit

$$X^n \equiv \sum_{i=0}^{d-1} a_{ni}X^i \qquad \mod \partial_F\mathscr{H}^\dagger(A),$$

pour certains $a_{ni}\in K(\pi)$, $0\leq i\leq d-1$. On aura besoin des informations suivantes sur les valuations π-adiques de ces nombres [**55**, Lemma 7.7]

Lemme 2.1. *Les nombres a_{ni} vérifient*
i) $a_{ni}=\delta_{ni}$ pour $0\leq n\leq d-1$,
ii) $v(a_{ni})\geq -\lfloor\frac{n-i}{d}\rfloor$ pour $n\geq d$, $1\leq i\leq d-1$
iii) $a_{n0}=0$ pour tout $n>0$, où v désigne la valuation π-adique, normalisée par $v_\pi(\pi)=1$.

Intéressons nous maintenant aux coefficients de la série $G(X)=\sum_{n\geq 0}h_nX^n$. On a le résultat suivant, qui repose sur la connaissance des coefficients de degré $\leq p-1$ de la série $\theta(X)$:

Lemme 2.2. *Supposons $p\geq d$, et soit $0\leq n\leq (p-1)d$; si pour un polynôme P on note $\{P\}_n$ son coefficient de degré n, les coefficients de G satisfont les congruences suivantes*

$$h_n \equiv \sum_{k=\lceil\frac{n}{d}\rceil}^{p-1} \left\{g^k\right\}_n \frac{\pi^k}{k!} \qquad \mod p\pi.$$

Finalement si on note m_{ij} les coefficients de la matrice M, on a l'expression $m_{ij}=h_{pi-j}+\sum_{n\geq d}h_{np-j}a_{ni}$. (*cf.* [**55**]), et les deux lemmes précédents donnent

Lemme 2.3. *Supposons $p\geq d+3$, alors pour $1\leq i,j\leq d-1$ on a*

$$m_{ij}\equiv h_{pi-j}\equiv \sum_{k=\lceil\frac{pi-j}{d}\rceil}^{p-1}\left\{g^k\right\}_{pi-j}\frac{\pi^k}{k!} \qquad \mod p\pi.$$

Venons en aux mineurs de la matrice M_1 ; on sait que le coefficient de degré n du polynôme caractéristique $\det(\mathbf{I}-T\overline{\alpha}_1)$ est donné par la somme des mineurs $n\times n$ principaux de M_1. D'après la description des coefficients, c'est le mineur correspondant aux n premières lignes (et colonnes) qui va donner la partie principale du coefficient. Commençons par introduire quelques notations.

Définition 2.1. *i/ Dans la suite, on pose $Y_n:=\sum_{k=1}^{n}\lceil\frac{pk-n}{d}\rceil$, et*

$$\Sigma_n := \{\sigma\in S_n,\ \sum_{k=1}^{n}\left\lceil\frac{pk-\sigma(k)}{d}\right\rceil = Y_n\}.$$

ii/ Soit $g(X)=\sum_{i=1}^{d}t_iX^i$ un polynôme de degré d à coefficients dans un anneau A de caractéristique 0. Pour tout $1\leq n\leq d-1$ on note $\mathcal{P}_n$ le polynôme de $\mathbb{Z}[X_1,\ldots,X_d]$ défini par

$$\mathcal{P}_n(t_1,\ldots,t_d) := \sum_{\sigma\in\Sigma_n} sgn(\sigma)\prod_{i=1}^{n}\left\{g^{\lceil\frac{pi-\sigma(i)}{d}\rceil}\right\}_{pi-\sigma(i)}.$$

Notons qu'on peut montrer la propriété suivante, qui nous sera utile dans la suite

Aucun des polynômes $\mathcal{P}_n$, $1\leq n\leq d-1$, n'est identiquement nul. (P)

A l'aide de ces notations, on obtient une congruence pour $M_n^{(1)}$, le mineur de M_1 associé aux lignes et colonnes $\{1,\ldots,n\}$, puis pour le coefficient de degré n de $\det(\mathbf{I}-T\overline{\alpha}_1)$. Précisément

Proposition 2.1. *Posons $\det(\mathbf{I}-T\overline{\alpha}_1):=1+\sum_{n=1}^{d-1}b_nt^n$. Alors pour tout $p\geq 3d$, et tout $1\leq n\leq d-1$, on a les congruences*

$$b_n\equiv M_n^{(1)}\equiv u\mathcal{P}_n(\alpha_1,\ldots,\alpha_d)\pi^{Y_n} \qquad \mod \pi^{Y_n+1},$$

pour une certaine unité u de $\mathbb{Z}_p$.

2.2. Mineurs de M et polygone de Newton générique. On rappelle la relation

$$M = M_1^{\tau^{m-1}} M_1^{\tau^{m-2}} \cdots M_1,$$

qui va nous permettre de déduire le polygone de Newton de $\det(\mathbf{I} - TM)$ de celui de $\det(\mathbf{I} - TM_1)$. On montre le résultat suivant

Proposition 2.2. *Posons $L(f;T) = \det(\mathbf{I} - T\overline{\alpha}) := 1 + \sum_{n=1}^{d-1} B_n t^n$. Alors pour tout $p \geq 3d$, et tout $1 \leq n \leq d-1$, on a les congruences*

$$B_n \equiv u^n \prod_{i=0}^{m-1} \mathcal{P}_n(\alpha_1^{\tau^i}, \ldots, \alpha_d^{\tau^i}) \pi^{mY_n} \qquad \mod \pi^{mY_n+1},$$

pour une certaine unité u de $\mathbb{Z}_p$.

On pourrait réinterpréter ce résultat dans l'esprit de [**71**, Theorem 3.3] de la façon suivante. Soit M_1 une matrice de taille $(d-1) \times (d-1)$ à coefficients dans l'anneau de valuation d'un corps d'indice de ramification n sur $\mathbb{Q}_p$, et qui satisfait aux hypothèses suivantes

(1) il y a une permutation de $\{1, \ldots, d-1\}$, σ, telle que le long de la ligne i, les coefficients m_{ij} sont de valuation $\geq v_i$ pour $j < \sigma(i)$, et $\geq v_i - 1$ pour $j \geq \sigma(i)$;

(2) $v_{i+1} - v_i \geq \frac{3}{n}$;

(3) la valuation du mineur formé des n premières lignes et colonnes est la somme pour i allant de 1 à n des $\min_{1 \leq j \leq n} \mathrm{ord}(m_{ij})$.

alors pour $M = M_1^{\tau^{m-1}} M_1^{\tau^{m-2}} \cdots M_1$, on a

$$\mathrm{NP}_q(\det(\mathbf{I} - TM)) = \mathrm{NP}_p(\det(\mathbf{I} - TM_1)).$$

Nous allons maintenant définir le polygone de Newton générique pour les fonctions L associées à des polynômes de degré d, ainsi que le polynôme de Hasse associé

Définition 2.2. *i/ Posons $Y_0 := 0$. Le polygone de Newton générique pour les sommes de caractères associées aux polynômes de degré d dans k, $GNP([0,d],p)$, est l'enveloppe convexe inférieure des points*

$$\left\{ (n, \frac{Y_n}{p-1}) \right\}_{0 \leq n \leq d-1},$$

qui ne dépend que de d et p, et pas de q.

ii/ On note $P_n \in \mathbb{F}_p[X_1, \ldots, X_d]$ la réduction modulo p de $\mathcal{P}_n$, et $P_{d,p} := \prod_{i=1}^{\lfloor \frac{d}{2} \rfloor} P_i$. Finalement, on définit le polynôme de Hasse $H_{[0,d],p} \in \mathbb{F}_p[X_1, \ldots, X_{d-1}]$ pour les polynômes de degré d comme

$$H_{[0,d],p}(X_1, \ldots, X_{d-1}) := P_{d,p}(X_1, \ldots, X_{d-1}, 1).$$

A l'aide de ces notations, on exprime le résultat principal de cette section :

Théorème 2.1. *Soit $p \geq 3d$ un nombre premier, et $f \in k[X]$ un polynôme unitaire de degré d. On a alors l'égalité $NP_q(f) = GNP([0,d],p)$ exactement quand les coefficients de f appartiennent à l'ouvert de Zariski $U_{[0,d],p} := D(H_{[0,d],p})$. De plus pour tout polynôme de degré d sur k, le polygone de Newton vérifie $NP_q(f) \preceq GNP([0,d],p)$.*

2.3. Comportement asymptotique. Une première conséquence du théorème 2.1 est qu'on a

$$\lim_{p \to \infty} \mathrm{GNP}([0,d],p) = \mathrm{HP}(d),$$

c'est à dire que le polygone de Newton générique tend vers le polygone de Hodge quand p tend vers l'infini.

Une question plus fine est la suivante : choisissons un polynôme (en une variable) de degré d, $\widetilde{f}$ à coefficients dans $\overline{\mathbb{Q}}$, et soit $\mathbb{Q}_{\widetilde{f}}$ l'extension de $\mathbb{Q}$ engendrée par les coefficients de $\widetilde{f}$. Pour chaque premier p de $\mathbb{Q}$, on choisit $\mathfrak{p}$ un premier au dessus de p dans le corps $\mathbb{Q}_{\widetilde{f}}$, de corps résiduel $\mathbb{F}_q$. On se demande comment varient les polygones de Newton $\mathrm{NP}_q(\widetilde{f} \mod \mathfrak{p})$ des réductions modulo $\mathfrak{p}$ de $\widetilde{f}$ quand p tend vers

l'infini. Wan conjecture [**66**, Conjecture 1.12] qu'il existe un ouvert dense $\mathcal{U}_d$ défini sur $\mathbb{Q}$ de l'espace des polynômes de degré d sur $\overline{\mathbb{Q}}$ tel que pour tout $\widetilde{f}$ de cet ouvert on ait

$$\lim_{p\to\infty} \mathrm{NP}_q(\widetilde{f} \mod \mathfrak{p}) = \mathrm{HP}([0,d]).$$

Zhu démontre cette conjecture dans [**70**], et on peut le retrouver avec les résultats donnés ci dessus. En examinant attentivement les polynômes $\mathcal{P}_n$ définis plus haut, on se rend compte qu'il existe, pour tout résidu r modulo d premier à d, un polynôme $\mathscr{H}_{[0,d],r}$ de $\mathbb{Q}[X_1,\dots,X_{d-1}]$ tel que pour tout $p \equiv r \mod d$ assez grand, l'image de $\mathscr{H}_{[0,d],r}$ dans $\mathbb{F}_p[X_1,\dots,X_{d-1}]$ est $H_{[0,d],p}$. On a obtenu

Théorème 2.2. *Posons $\mathscr{H}_{[0,d]} := \prod_{r\in(\mathbb{Z}/d\mathbb{Z})^\times} \mathscr{H}_{[0,d],r}$. Alors pour tout polynôme unitaire de degré d à coefficients dans $\overline{\mathbb{Q}}[X]$, dans l'ouvert $\mathcal{U}_{[0,d]}$ défini comme le complémentaire de l'hypersurface d'équation $\mathscr{H}_{[0,d]} = 0$, la limite des $\mathrm{NP}_q(\widetilde{f} \mod \mathfrak{p})$ existe et vaut $\mathrm{HP}([0,d])$.*

3. Le cas des sommes tordues

Soit ω le caractère de Teichmüller de $k^\times$, il s'agit d'un caractère multiplicatif d'ordre $q-1$, et $f = \sum_{i=-d_0}^{d_\infty} a_i x^i \in k[x,x^{-1}]$ un polynôme de Laurent ayant son pôle en 0 d'ordre d_0 son pôle en l'∞ d'ordre d_∞. On note $d := d_0 + d_\infty$ dans cette section.

Dans cette section on s'intéresse aux polygones de Newton des fonctions $L(f,\omega^e;T)$ associées aux sommes de caractères tordues

$$S_r(f,\omega^e) = \sum_{x\in k_r^\times} \psi_r(f(x))\omega^e(\mathrm{N}(x)).$$

On en déduit les polygones de Newton génériques, ainsi que les polynômes de Hasse correspondants. Comme les méthodes sont les mêmes que celles utilisées pour les sommes additives, on va se contenter d'exposer rapidement les résultats, puis on va insister sur les différences qui apparaissent pour le comportement asymptotique. Si on fixe e et qu'on fait varier p, la situation est similaire au cas additif.

En revanche, on verra dans l'étude d'un cas non générique dans la section 4 qu'il est utile de considérer la situation suivante : on fixe deux entiers $s \geq 2$ et $1 \leq r \leq s-1$, et on pose $e = \frac{(q-1)r}{s}$ pour une puissance convenable de p, $q \equiv 1 \mod s$. C'est à dire qu'on fixe l'ordre de χ quand p varie. Alors on n'a plus un seul polygone combinatoire, mais un pour chaque résidu inversible modulo s, ce sont les **polygones de Hodge Stickelberger** définis dans la section 4. En conséquence, le comportement asymptotique des polygones de Newton génériques ne peut plus être uniforme comme dans le cas additif. On montre que la limite de ces polygones existe, à condition de se restreindre aux nombres premiers de résidu modulo s fixé, et que cette limite est le polygone de Hodge Stickelberger.

3.1. Polygones de Newton pour les sommes tordues.

Dans le cas présent, le polygone de Hodge défini en 4.2 (voir aussi [**4**], [**3**]) est le polygone de longueur d qui est la juxtaposition des segments de longueur 1 et de pentes

$$\{\frac{m-\lambda}{d_\infty}\}_{1\leq m\leq d_\infty} \cup \{\frac{m+\lambda}{d_0}\}_{0\leq m\leq d_0-1},$$

où $\lambda := \frac{\sigma_p(e)}{m(p-1)}$, $\sigma_p(n)$ désignant la somme des chiffres de l'écriture en base p de n.

Rappelons la factorisation de l'endomorphisme $\overline{\alpha}$: si $e = \sum_{i=0}^{m-1} p^i e_i$ est l'écriture en base p de l'entier e, et α_i, $0 \leq i \leq m-1$ l'endomorphisme de $\mathscr{H}^\dagger(A)$ défini par $\alpha_i = \psi_p \circ x^{e_i} G$, alors on a

$$\overline{\alpha} = \overline{\alpha}_{m-1}^{\tau^{m-1}} \dots \overline{\alpha}_1^\tau \overline{\alpha}_0.$$

On note M_i la matrice de $\overline{\alpha}_i$ dans la base $\mathcal{B} = \{x^{-d_0},\dots,x^{d_\infty-1}\}$. Commençons par nous ramener à une situation semblable à celle de la section précédente. Notons $\mathcal{B}_0 := \{x^{-d_0},\dots,x^{-1}\}$ et $\mathcal{B}_\infty := \{1,\dots,x^{d_\infty-1}\}$. De même on note $f_0 = \sum_{i=-d_0}^{-1} a_i x^i$, $f_\infty = \sum_{i=0}^{d_\infty} a_i x^i$, on construit les séries entières G_0 et G_∞ respectivement associées à ces polynômes, puis $\alpha_{i0} := \psi_p \circ x^{e_i} G_0$ et $\alpha_{i\infty} := \psi_p \circ x^{e_i} G_\infty$. Si M_{i0} (*resp.* $M_{i\infty}$) désigne la matrice de α_{i0} dans la base $\mathcal{B}_0$ (*resp.* de $\alpha_{i\infty}$ dans la base $\mathcal{B}_\infty$), alors on peut montrer que, dans le cas générique, et pour p assez grand, on a

$$M_{in} \equiv M_{in_0}^{(0)} M_{in_\infty}^{(\infty)}$$

modulo une puissance convenable de l'uniformisante π. Ici $M_{in}^{(*)}$ désigne le mineur $n \times n$ formé des n premières lignes et colonnes de la matrice M_{i*}, et (n_0, n_∞) est une partition de n telle que les n plus petits nombres de $\{\frac{m-\lambda}{d_\infty}\}_{1\leq m\leq d_\infty} \cup \{\frac{m+\lambda}{d_0}, 1)\}_{0\leq m\leq d_0-1}$, soient exactement les $\{\frac{m+1-\lambda}{d_\infty}\}_{1\leq m\leq n_\infty} \cup \{\frac{m-1+\lambda}{d_0}, 1)\}_{0\leq m\leq n_0-1}$.

On est donc ramenés à peu de choses près (en fait à la puissance x^{e_i} qui apparaît dans G) à la situation étudiée dans la section précédente. On va donner quelques définitions

Définition 3.1. *i/ On pose, pour tout* $1 \leq n \leq d$

$$Y_n^{(i)}(e) := \sum_{k=1}^{n_\infty} \lceil \frac{pk - e_i - n}{d} \rceil + \sum_{k=0}^{n_0-1} \lceil \frac{pk + e_i - n}{d} \rceil,$$

et $Y_n(e) := \frac{1}{m}\sum_{i=0}^{m-1} Y_n^{(i)}(e)$, $Y_0(e) := 0$.

ii/ A l'aide de ces rationnels, on définit le polygone de Newton générique associé aux polynômes de Laurent de degrés (d_0, d_∞) *sur* k *tordus par* ω^e *comme le polygone* $\mathrm{GNP}([-d_0, d_\infty], \frac{e}{q-1})$ *de sommets*

$$\left\{(n, \frac{1}{p-1}Y_n(e))\right\}_{0\leq n\leq d}.$$

On pourrait de même définir un polynôme de Hasse, qu'on note $H_{[-d_0,d_\infty],\frac{e}{q-1},p}$, dans $\mathbb{F}_p[X_{-d_0}, \ldots, X_{d_\infty}]$ de façon très semblable à celle de la section précédente. On obtient alors le résultat suivant

Théorème 3.1. *Pour* p *un nombre premier assez grand, et* $f \in k[X, X^{-1}]$ *un polynôme de Laurent de degré* (d_0, d_∞)*, on a l'égalité de polygones de Newton*

$$NP_q(f, \omega^e) = GNP([-d_0, d_\infty], \frac{e}{q-1})$$

exactement quand les coefficients de f *appartiennent à l'ouvert de Zariski*

$$U_{[-d_0,d_\infty],\frac{e}{q-1}} := D(H_{[-d_0,d_\infty],\frac{e}{q-1}}).$$

De plus pour tout polynôme de Laurent de degrés (d_0, d_∞) *sur* k*, le polygone de Newton vérifie* $NP_q(f, \omega^e) \preceq GNP([-d_0, d_\infty], \frac{e}{q-1})$.

3.2. Comportement asymptotique. Il est naturel, au vu des résultats précédents, et par analogie avec le cas des sommes additives, de s'intéresser au comportement asymptotique des polygones de Newton génériques associés aux sommes tordues, ou des polygones de Newton des réductions d'un polynôme de Laurent à coefficients dans $\overline{\mathbb{Q}}$. On peut procéder de deux façons.

1. L'entier e est fixé. La première question est ici celle du comportement asymptotique des

$$GNP([-d_0, d_\infty], \frac{e}{q-1})$$

quand p diverge, q étant une puissance quelconque de p. Puisque la suite $\sigma_p(e)$ est stationnaire de limite e dans ce cas, il est aisé de vérifier que la constante λ_p (le λ du paragraphe précedent, dont on veut souligner la dépendance en p) tend vers 0, et donc que les polygones de Newton génériques tendent vers le polygone de Hodge **additif** $HP([-d_0, d_\infty])$.

La seconde est celle du comportement générique de $\lim_{p\to\infty} \mathrm{NP}(f, \omega^e \mod \mathfrak{p})$. On montre ici encore qu'il existe un ouvert dense et défini sur $\mathbb{Q}$ de l'espace des polynômes de Laurent de degrés (d_0, d_∞) fixés tel que pour tout polynôme de cet ouvert, la limite existe et soit exactement $HP([-d_0, d_\infty])$.

On retrouve donc les mêmes propriétés asymptotiques que pour les sommes additives. En fait ce n'est pas ce cas qui nous intéresse le plus.

2. L'ordre du caractère multiplicatif reste fixé. Ici on fixe deux entiers, r positif, et $s \geq 2$, et on pose $e_p = \frac{(q-1)r}{s}$, pour q une puissance convenable de p, qui varie avec p, et $\chi_p := \omega^{\frac{(q-1)r}{s}}$.

On sait alors réécrire le rationnel λ_p de la façon suivante. Si σ désigne la permutation de l'ensemble $\{0, \ldots, s-1\}$ induite par la multiplication par p dans $\mathbb{Z}/s\mathbb{Z}$, et si σ_i est le cycle, de longueur ℓ_i, de σ contenant r, alors on a $\lambda = \frac{\sum_{j\in\sigma_i} j}{s\ell_i}$. Il est fondamental de remarquer que λ_p ne dépend plus que de r, s, et du résidu de p modulo s. Cette remarque revêt une grande importance, on va donc modifier légèrement

nos notations. On se réfèrera à **[BF2]** pour une définition précise du polynôme de Hasse dans le cas des polynômes.

Définition 3.2. *i/ On appelle le polygone de longueur d,* $\mathrm{HP}([-d_0, d_\infty], \frac{(q-1)r}{s})$ polygone de Hodge Stickelberger associé au polyèdre $[-d', d]$, au rationnel $\frac{r}{s}$ et au résidu ν. *On le note dorénavant*

$$\mathrm{HS}([-d_0, d_\infty], \frac{r}{s}, \nu),$$

où ν est le résidu de p modulo s.

ii/ On définit comme dans le cas additif un polynôme de Hasse $\mathscr{H}_{[-d_0,d_\infty],\frac{r}{s},\nu}$ dans $\mathbb{Q}[X_{-d_0}, \dots, X_{d_\infty}]$.

Remarquons qu'on a maintenant $\varphi(s)$ polygones distincts, où φ est comme d'habitude l'indicatrice d'Euler. En particulier il ne faut plus espérer de limite aussi uniforme que dans le cas additif. En revanche, si on se restreint aux premiers de résidu modulo s fixé, on retrouve l'existence d'une limite pour les polygones de Newton génériques, et d'une limite générique pour les polygones de Newton $\mathrm{NP}(f, \chi_p \mod \mathfrak{p})$, f parcourant l'espace des polynômes de Laurent de degrés $(-d_0, d_\infty)$ à coefficients dans $\overline{\mathbb{Q}}$.

Théorème 3.2. *Soit $\nu \in (\mathbb{Z}/s\mathbb{Z})^\times$.*

i/ Quand p tend vers ∞ le long de la classe ν, alors on a

$$\lim \mathrm{GNP}([-d_0, d_\infty], \frac{r}{s}, p) = \mathrm{HS}([-d_0, d_\infty], \frac{r}{s}, \nu).$$

ii/ Il existe un ouvert de Zariski non vide $\mathcal{U}_{[-d_0,d_\infty],\frac{r}{s},\nu} = D(\mathscr{H}_{[-d_0,d_\infty],\frac{r}{s},\nu})$ de l'espace des polynômes de Laurent de degrés $(-d_0, d_\infty)$ sur $\overline{\mathbb{Q}}$ tel que pour tout f de $\mathcal{U}_{[-d_0,d_\infty],\frac{r}{s},\nu}$, la limite quand p tend vers ∞ le long de la classe ν existe et vaut $\mathrm{HS}([-d_0, d_\infty], \frac{r}{s}, \nu)$.

Ces résultats peuvent paraître peu naturels, mais on va voir dès le prochain chapitre leur intérêt dans l'étude d'un cas non générique des polynômes de Laurent.

4. Un cas non générique des polynômes de Laurent

On va déduire ici les polygones de Newton génériques associés aux polynômes de Laurent de la forme $f(x^s)$ des résultats qu'on vient de voir. Les calculs menés dans le cas additif montrent que pour $s > 2$, et q non congru à 1 modulo s, le polygone de Hodge n'est plus une bonne borne inférieure pour les polygones de Newton de ces polynômes (on va décrire un nouveau polygone de Hodge Stickelberger qui est alors la "bonne" borne inférieure). C'est aussi une conséquence du fait que pour une infinité d'extensions k_r de k, le polynôme $x \mapsto x^s$ est un polynôme de permutation pour k_r, et que la somme associée à $f(x^s)$ est la même que celle associée à $f(x)$.

La formule de Poisson, appliquée aux sous-groupes $(k_r^\times)^s$, $r \geq 1$, donne le lien entre les fonctions L des sommes associées à $f(x^s)$ et celles des sommes tordues associées à $f(x)$. Plus précisément, notons comme plus haut σ la permutation de $\{0, \dots, s-1\}$ induite par la multiplication par p modulo s, et $\sigma = \prod_{i=1}^u \sigma_i$ sa décomposition en produit de cycles à supports disjoints, où σ_i est de longueur ℓ_i. Alors la permutation σ^m se décompose en $\sigma^m = \prod_{i=1}^u \sigma_i^m = \prod_{i=1}^u \prod_{j=1}^{\ell_i/\ell_i'} \sigma_{ij}$ pour σ_{ij} des cycles de longueur ℓ_i', avec $\ell_i' | \ell_i$. En fait chaque cycle σ_i se décompose en produit de ℓ_i/ℓ_i' cycles de même longueur ℓ_i'. Si f est un polynôme de Laurent quelconque, on note, pour chaque cycle σ_i,

$$L_i(T) \quad := \quad \prod_{j=1}^{\ell_i/\ell_i'} L(f/k_{\ell_i'}, \chi_s^{r_{ij}}; T^{\ell_i'}), \tag{4}$$

où r_{ij} est un élément du support de σ_{ij}, et la notation $L(f/k_{\ell_i'}, \dots)$ signifie qu'on considère la fonction L sur le corps $k_{\ell_i'}$, et plus sur k. Avec ces notations, on sait maintenant relier les fonctions L des sommes associées à f, tordues par les caractères d'ordre s, et celle des sommes additives associées à $f(x^s)$

Lemme 4.1. *On a l'égalité*

$$L(f(x^s); T) \quad = \quad \prod_{i=1}^u L_i(T). \tag{5}$$

En d'autres termes, le polygone de Newton $\mathrm{NP}(f(x^s))$ est une juxtaposition de polygones de Newton de la forme $\mathrm{NP}(f,\chi)$, où χ parcourt les caractères d'ordre s de $\overline{k}^\times$. Il est donc naturel de définir un nouveau polygone de Hodge Stickelberger de la façon suivante.

Définition 4.1. *i/ Si Π_1 et Π_2 sont deux polygones convexes de pentes respectives $(s_i)_{1\leq i\leq a}$ et $(s'_i)_{1\leq i\leq b}$, leur juxtaposition est le polygone convexe $\Pi_1 \coprod \Pi_2$ de pentes $(s_i, s'_j)_{1\leq i\leq a, 1\leq j\leq b}$.*

ii/ Le polygone de Hodge Stickelberger associé aux polynômes de Laurent de la forme $f(x^s)$ sur k, *pour f de degré (d_0, d_∞) est le polygone défini par*

$$\mathrm{HS}([-d_0,d_\infty],s,\nu)=\coprod_{i=1}^{u} h_{\ell_i}\left(\mathrm{HS}([-d_0,d_\infty],\frac{r_i}{s},\nu)\right),$$

où h_n est l'homothétie de centre l'origine et de rapport n, r_i est un élément du support du cycle σ_i, et ν est le reste de la division euclidienne de p par s.

iii/ On définit de même le polygone de Newton générique associé aux polynômes de Laurent de la forme $f(x^s)$ sur k, pour f de degré (d_0, d_∞),

$$\mathrm{GNP}([-d_0,d_\infty],s,p)=\coprod_{i=1}^{u} h_{\ell_i}\left(\mathrm{GNP}([-d_0,d_\infty],\frac{r_i}{s},p)\right),$$

à partir des polygones de Newton génériques définis dans la section précédente.

iv/ Le polynôme de Hasse des polynômes de Laurent de la forme $f(x^s)$ sur k, pour f de degré (d_0, d_∞), est le polynôme de $\mathbb{Q}[X_{-d_0}, \ldots, X_{d_\infty}]$ défini par

$$\mathscr{H}_{[-d_0,d_\infty],s,\nu}=\prod_{i=1}^{u}\mathscr{H}_{[-d_0,d_\infty],\frac{r_i}{s},\nu}$$

Le résultat suivant est simplement obtenu en combinant le lemme précédent avec le théorème 3.2

Théorème 4.1. *Le comportement asymptotique des polygones de Newton associés aux polynômes de Laurent $f(x^s)$, pour f de degré (d_0, d_∞), est donné par*

i/ quand p tend vers ∞ le long de la classe ν, alors on a

$$\lim \mathrm{GNP}([-d_0,d_\infty],s,p)=\mathrm{HS}([-d_0,d_\infty],s,\nu).$$

ii/ il existe un ouvert de Zariski non vide $\mathcal{U}_{[-d_0,d_\infty],s,\nu}$ de l'espace des polynômes de Laurent de degré (d_0, d_∞) sur $\overline{\mathbb{Q}}$ tel que pour tout $\widetilde{f}$ de $\mathcal{U}_{[-d_0,d_\infty],s,\nu}$, la limite de $\mathrm{NP}_q(\widetilde{f},\chi \mod \mathfrak{p})$ quand p tend vers ∞ le long de la classe ν existe et vaut $\mathrm{HS}([-d_0,d_\infty],s,\nu)$.

5. Conclusion et questions

On va présenter ici quelques questions et résultats, proposant d'une part de recadrer le problème dans une théorie plus large et mieux établie, celle des cristaux, d'autre part de tenter de préciser le cas non générique des polynômes, c'est à dire de déterminer exactement les polynômes sur $\overline{\mathbb{Q}}$ de degré fixé pour lesquels la limite de $\mathrm{NP}(f \mod \mathfrak{p})$ n'est pas le polygone de Hodge.

5.1. Cristaux. Les objets qu'on vient de manipuler sont en fait des F-isocristaux. En effet, l'application semi linéaire $\overline{\alpha}_1$ est un endomorphisme de $\mathscr{M}$, un $\mathcal{O}$-module libre (pour $\mathcal{O}$ l'anneau de valuation du corps $K(\pi)$), τ-linéaire, et qui devient un isomorphisme quand on le considère comme un endomorphisme de $\mathscr{M}\otimes K(\pi)$. On sait associer à un tel cristal deux polygones (*cf.* [**31**])

(1) le polygone de Hodge, qui décrit les diviseurs élémentaires de l'endomorphisme ;

(2) le polygone de Newton (du polynôme caractéristique) défini comme plus haut, et qui permet la classification de Dieudonné-Manin des isocristaux de rang fixé à isomorphisme près.

On a donc calculé les polygones de Newton d'isocristaux associés à des sommes de caractères. Quant aux polygones de Hodge, on a déjà souligné dans l'introduction que leur appellation est impropre. Par exemple, on peut vérifier que pour p assez grand, le polygone de Hodge (pour la valuation ord_p) du cristal $(\mathcal{O}^{d-1}, \overline{\alpha}_1)$

provenant de la somme de caractères associée à un polynôme de degré d est indépendant du choix de f, et a pour pentes

$$\frac{1}{p-1}\lfloor\frac{p-1}{d}\rfloor,\ldots,\frac{1}{p-1}\lfloor(d-1)\frac{p-1}{d}\rfloor.$$

Ce n'est donc pas le polygone de Hodge $\mathrm{HP}([0,d])$ qu'on a manipulé. En fait le "vrai" polygone de Hodge converge vers le polygone de Hodge combinatoire (par en dessous) quand p tend vers $+\infty$.

On peut aussi remarquer que la construction du polygone de Hodge des sommes tordues à partir des polygones de Hodge provenant de séries de Poincaré, décrite à la section 4.2, est la même que celle des polygones de Hodge μ-ordinaires à partir des polygones de Hodge classiques, décrite dans [**38**, Section 2.8] ou [**54**, Theorem 1.15 iii/].

Il est donc naturel de vouloir répondre à la question suivante.

Question 1. Plonger l'étude des polygones de Newton de sommes de caractères dans la théorie des isocristaux.

A la connaissance de l'auteur, ce travail n'a pas été fait, et l'étude précédente ne pourrait que s'enrichir en étant confrontée avec une théorie bien établie.

5.2. Polynômes non génériques. On appellera *polynôme de Laurent non générique* un polynôme f à coefficients dans $\overline{\mathbb{Q}}$ qui ne satisfait pas la propriété

$$\lim_{p\to\infty}\mathrm{NP}(f \bmod \mathfrak{p}) = \mathrm{HP}([-d_0, d_\infty])$$

On va décrire ici quelques exemples connus, en se restreignant aux polynômes à coefficients dans $\mathbb{Q}$ par souci de simplifier l'exposition.

Pour n un entier positif, soit $D_n(x,y)$ l'unique polynôme de $\mathbb{Z}[x,y]$ tel que $D_n(u+v,uv) = u^n + v^n$. Pour tout $c \in \mathbb{N}$ le polynôme (unitaire et de degré n) $D_n(x,c)$ de $\mathbb{Q}[x]$ est un *polynôme de Dickson de degré n* sur $\mathbb{Q}$. Si p divise c, alors la réduction modulo p de $D_n(x,c)$ est x^n, un monôme, et la fonction polynômiale associée est une permutation de $\mathbb{F}_p$ exactement quand $\mathrm{pgcd}(n, p-1) = 1$. Si p ne divise pas c, la fonction polynômiale est une permutation de $\mathbb{F}_p$ quand $\gcd(n, p^2-1) = 1$ (voir [**19**], ou [**45**, Chapter 7]).

Pour tout $l \geq 1$, on appelle *polynôme de permutation global sur $\mathbb{Q}$ de niveau l* un polynôme $h(x) \in \mathbb{Q}[x]$ tel que l'application $x \mapsto h(x)$ soit une permutation de chacun des corps finis $\mathbb{F}_p, \ldots, \mathbb{F}_{p^l}$ pour une infinité de nombres premiers p. Par exemple, $D_n(x,c)$ est un polynôme de permutation global sur $\mathbb{Q}$ de niveau l si et seulement si tout facteur premier Q de n vérifie $Q > l+1$ (pour $c = 0$), ou $Q > 2l+1$ (pour $c \neq 0$). Pour le niveau 1 cela signifie que n est impair (pour $c = 0$) et que $\mathrm{pgcd}(n,6) = 1$ (pour $c \neq 0$). On sait que tout polynôme de permutation global sur $\mathbb{Q}$ est la composée de polynômes de Dickson $D_n(x,c)$ sur $\mathbb{Q}$ et de polynômes linéaires sur certaines extensions de $\mathbb{Q}$.

Revenons aux polynômes non génériques. Les résultats précédents impliquent que pour tout polynôme de Laurent $f(x)$ sur $\overline{\mathbb{Q}}$ contenant $x^s = D_s(x,0)$, $s > 2$ comme facteur de composition à droite, (c'est à dire $f(x) = P(x^s)$), la limite des polygones de Newton p-adiques n'existe pas quand $p \to \infty$. Un argument de Wan montre que si $f(x)$ est un polynôme de Laurent contenant un polynôme de permutation global sur $\mathbb{Q}$ de niveau 3 comme facteur de composition à droite, alors la limite $\lim_{p\to\infty}\mathrm{NP}(f(x) \bmod p)$ n'existe pas. Ceci l'amène à énoncer la conjecture suivante (*cf.* [**69**, Chapter 5]).

Si f est un polynôme de Laurent de $\mathbb{Q}[x, x^{-1}]$ qui ne contient pas de polynôme de permutation global sur $\mathbb{Q}$ de niveau 3 comme facteur de composition à droite, alors la limite $\lim_{p\to\infty}\mathrm{NP}_p(f \bmod p)$ existe et est le polygone de Hodge associé.

On a énoncé dans [**BFZ,** Section 6] la conjecture suivante, pour $f(x) \in \mathbb{Q}[x]$ un polynôme de degré $d \geq 2$, $S(f(x) \bmod p) = \sum_{x\in F_p}\psi(f(x))$ la somme de caractères associée mod p, et $\varepsilon > 0$

Question 3. Si $\mathrm{ord}_p S(f(x) \bmod p) > \frac{1}{d} + \varepsilon$ pour une infinité de nombres premiers p, alors $f(x) = P(D_s(x,c))$ pour un certain $P \in \mathbb{Q}[x]$ et un polynôme de Dickson D_s de degré $s > 2$ (à des facteurs de composition linéaires près).

On peut voir cette conjecture comme une généralisation de la conjecture de Schur sur les polynômes de permutation globaux. En effet, on peut réécrire cette dernière : "Pour tout $f \in \mathbb{Q}[x]$, si $S(f(x) \bmod p) = 0$ (c'est à dire $\mathrm{ord}_p(S(f(x) \bmod p)) = +\infty$) pour une infinité de nombres premiers p, alors $f(x)$ est un polynôme de Dickson" (à des facteurs de composition linéaires près) (*cf.* [**45**, Chapter 7]).

On peut montrer le résultat suivant (où on a posé

$$\Gamma_n := \left\{(k_1,\dots,k_{d-1}) \in \mathbb{N}^{d-1},\ (d-1)k_1 + \cdots + k_{d-1} = (n+1)d - r + 1\right\},$$

pour n un entier naturel, $2 \leq r \leq d-1$ un entier premier à d, et $Q_n^r \in \mathbb{Q}[X_1,\dots,X_{d-1}]$ le polynôme

$$Q_n^r := \sum_{(k_1,\dots,k_{d-1})\in\Gamma_n} \binom{n+1-\frac{r}{d}}{k_1,\dots,k_{d-1}} \prod_{i=1}^{d-1} X_i^{k_i}.)$$

Proposition 5.1. *Si $f(X) := X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{Z}[X]$ est un polynôme de degré d vérifiant les hypothèses de la question ci-dessus, alors on peut trouver un entier r comme plus haut, tel que pour tout entier $n \geq 0$, on ait*

$$Q_n^r(a_1,\dots,a_{d-1}) = 0.$$

On aurait ainsi obtenu une caractérisation (comme intersection d'hypersurfaces dans l'espace des polynômes) de l'ensemble des polynômes de la forme $P \circ D_s$. Par exemple si d est premier, on ne devrait retrouver (pour p distinct de 1, -1 modulo d, c'est à dire $r \neq d-1$) que les polynômes de Dickson de degré p. On peut vérifier sur de petits cas, par exemple $d = 5$, que c'est bien le cas.

5.3. Cas des fractions rationnelles. On sait définir des polygones de Hodge pour des fractions rationnelles quelconques [**72**]. Au prix de quelques complications théoriques, on obtient le polygone de Hodge comme une juxtaposition (pour chaque pôle de la fraction rationnelle) de polygônes de Hodge de polynômes (dont le degré est l'ordre du pôle) comme décrits dans ce chapitre. On sait aussi [**43**] que le comportement générique est semblable à celui des polynômes.

Il serait souhaitable de déterminer les polygones de Newton génériques et les polynômes de Hasse dans cette situation. Vraisemblablement ce seront respectivement des juxtapositions et des produits de polygones de Newton et de polynômes de Hasse "locaux" (c'est à dire associés à un seul pôle, en fonction des coefficients de la décomposition en éléments simples en ce pôle). Les calculs de Liu [**46**] donnent ce résultat dans le cas des polynômes de Laurent.

CHAPITRE 4

Comportement asymptotique des polygones de Newton associés aux sommes de caractères à plusieurs variables

1. Introduction

Dans tout ce chapitre, f désigne un polynôme de Laurent en n variables, c'est à dire un élément de $k[x_1, \ldots, x_n, (x_1, \ldots x_n)^{-1}]$. Considérons les sommes de caractères

$$S_r(f) = \sum_{\mathbf{x} \in \mathbb{G}_m^n(k_r)} \psi(f(\mathbf{x})),$$

et la fonction $L(f;T)$ associée. De même si χ est un caractère multiplicatif de $(k^\times)^n$, on note $L(f, \chi; T)$ la fonction L associée aux sommes de caractères

$$S_r(f, \chi) = \sum_{\mathbf{x} \in \mathbb{G}_m^n(k_r)} \psi(f(\mathbf{x}))\chi(\mathbf{x}).$$

On renvoie à la section 4 du chapitre sur les généralités pour les notations utilisées dans ce chapitre. On note $\mathrm{GNP}(\Delta, p)$ le polygone de Newton générique associé aux fonctions L définies ci-dessus avec χ trivial (*resp.* $\mathrm{GNP}(\Delta, \frac{e}{q-1})$ quand $\chi = \omega^e$), quand f parcourt l'espace des polynômes de Laurent de polyèdre de Newton Δ, non dégénérés. On note $\mathrm{HP}(\Delta)$ (*resp.* $\mathrm{HP}(\Delta, \frac{e}{q-1})$ quand $\chi = \omega^e$) les polygones de Hodge correspondants.

On va étudier le comportement asymptotique des polygones $\mathrm{GNP}(\Delta, p)$ dans deux cas

(1) quand Δ est l'enveloppe convexe de points de la forme $\{d_i\mathbf{e}_i, -d'_i\mathbf{e}_i\}_{1 \leq i \leq n}$, avec $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ une base du $\mathbb{Z}$-module $\mathbb{Z}^n$; ce sera le théorème 4.1.

(2) quand Δ est l'enveloppe convexe de points de la forme $\{d_i\mathbf{f}_i, -d'_i\mathbf{f}_i\}_{1 \leq i \leq n}$, où $\mathbf{f}_1, \ldots, \mathbf{f}_n$ engendrent un sous module M de $\mathbb{Z}^n$ tel que $2\mathbb{Z}^n \subset M$; ce sera le théorème 6.1.

Ce sont à notre connaissance les premiers résultats sur le comportement asymptotique de sommes de caractères associées à des polynômes de plusieurs variables, quand le dénominateur du polyèdre Δ est strictement plus grand que 2.

Dans le cas où χ n'est pas trivial, et d'ordre fixé, on ne peut plus espérer obtenir une limite quand p tend vers ∞, à moins de supposer que le caractère est d'ordre deux (c'est ce résultat qui nous permet de prouver le cas (2) ci-dessus). En revanche, quand p tend vers ∞ le long d'une classe modulo l'ordre du caractère, on retrouve l'existence d'une limite, généralisant ainsi les résultats en dimension 1 de **[BFZ]**. Ces résultats font l'objet des théorèmes 5.1 et 5.2.

Ce chapitre est organisé de la façon suivante : dans la première section, nous utilisons la somme directe de polyèdres convexes, et calculons le polygone de Hodge associé. Dans la seconde nous utilisons des résultats de cohomologie ℓ-adique (principalement la formule de Künneth) pour exprimer les polygones de Newton de (fonctions L de) sommes associées à certains polynômes en plusieurs variables à l'aide des polygones de Newton associés à des polynômes plus simples. Dans la section 3 sont démontrées les conjectures de Wan dans le cas (1) : on y utilise les résultats du chapitre 3 sur les polynômes de Laurent en une variable, dont on déduit les théorèmes 4.1 et 4.2. Ensuite, dans la quatrième section, on donne quelques applications au cas des sommes mixtes, tordues par un caractère multiplicatif. Finalement, on utilise les deux résultats et la formule de Poisson pour déduire les conjectures de Wan pour le cas (2) dans la dernière section.

2. Sommes directes de polyèdres

Dans toute cette section, on fixe deux polyèdres convexes Δ_1 de $\mathbb{R}^{n_1}$ et Δ_2 de $\mathbb{R}^{n_2}$. On va rappeler la définition de leur *somme directe* $\Delta_1 \oplus \Delta_2$, et donner certaines de ses propriétés ; on exprimera ensuite

la série de Poincaré de l'algèbre graduée $\mathcal{A}_{\Delta_1\oplus\Delta_2}$ à l'aide de celles des algèbres graduées $\mathcal{A}_{\Delta_1}$ et $\mathcal{A}_{\Delta_2}$, de façon à calculer le polygone de Hodge de $\Delta_1 \oplus \Delta_2$ en fonction de ceux de Δ_1 et Δ_2.

Commençons par définir la somme directe de polyèdres (*cf.* [**25**, 16.1.3]) ; dans toute la suite, on va supposer que les polyèdres qui interviennent sont de dimension maximale, c'est à dire que l'espace affine qu'ils engendrent est l'espace ambiant.

Définition 2.1. *Soient deux polyèdres convexes Δ_1 et Δ_2, respectivement dans $\mathbb{R}^{n_1}$ et $\mathbb{R}^{n_2}$. Leur* somme directe *est le polyèdre convexe de $\mathbb{R}^{n_1+n_2}$ qui est l'enveloppe convexe de $\Delta_1 \times \{0\} \cup \{0\} \times \Delta_2$. On le note $\Delta_1 \oplus \Delta_2$.*

Remarque 2.1. *Il ne faut pas confondre l'opération qu'on vient de définir avec la somme usuelle de polyèdres (ou somme de Minkowski). Par exemple, si $\Delta_1 = [0, d_1] \subset \mathbb{R}$ et $\Delta_2 = [0, d_2] \subset \mathbb{R}$, alors $\Delta_1 \oplus \Delta_2$ est le triangle de sommets $(0,0), (d_1, 0)$ et $(0, d_2)$, alors que la somme usuelle de ces polyèdres donne le rectangle de sommets $(0,0), (d_1, 0), (0, d_2)$ et (d_1, d_2).*

En revanche ces opérations sont duales l'une de l'autre sous la dualité usuelle des polytopes.

On sait exprimer les invariants associés à Δ à l'aide de ceux associés à Δ_1 et Δ_2, c'est l'objet du

Lemme 2.1. *Soient Δ_1 et Δ_2 deux polyèdres convexes contenant l'origine, et Δ leur somme directe. On note σ_i une face de Δ_i. Alors*

1. *le cône $C(\sigma_1 \oplus \sigma_2)$ dans $\mathbb{R}^{n_1+n_2}$ est égal au produit $C(\sigma_1) \times C(\sigma_2)$;*
2. *le monoïde M_Δ est égal au monoïde $M_{\Delta_1} \times M_{\Delta_2}$ de $\mathbb{Z}^{n_1+n_2}$;*
3. *le poids w_Δ est l'application $w_{\Delta_1} + w_{\Delta_2}$ de $C(\Delta)$ dans $\mathbb{R}_+$ qui à $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2)$ associe $w_{\Delta_1}(\mathbf{u}_1) + w_{\Delta_2}(\mathbf{u}_2)$*
4. *le dénominateur D de Δ est le plus petit commun multiple des dénominateurs D_1 et D_2 de Δ_1 et Δ_2.*

On déduit de l'assertion (2) que l'algèbre $\mathcal{A}_\Delta$ est isomorphe au produit tensoriel (sur k) des algèbres $\mathcal{A}_{\Delta_1}$ et $\mathcal{A}_{\Delta_2}$. Venons en à la graduation ; si $\mathbf{x}_i^{\mathbf{u}_i}$ est dans $\mathcal{A}_{\Delta_i, \frac{k_i}{D_i}}$, alors d'après l'assertion (3), le monôme $\mathbf{x}^{\mathbf{u}} = \mathbf{x}_1^{\mathbf{u}_1}\mathbf{x}_2^{\mathbf{u}_2}$ est dans $\mathcal{A}_{\Delta, \frac{k}{D}}$, avec

$$\frac{k_1}{D_1} + \frac{k_2}{D_2} = \frac{k}{D}.$$

On obtient la décomposition suivante pour chaque pièce de la graduation de $\mathcal{A}_\Delta$:

$$\mathcal{A}_{\Delta, \frac{k}{D}} = \bigoplus_{\frac{k_1}{D_1}+\frac{k_2}{D_2}=\frac{k}{D}} \mathcal{A}_{\Delta_1, \frac{k_1}{D_1}} \otimes \mathcal{A}_{\Delta, \frac{k_2}{D_2}},$$

puis la factorisation de la série de Poincaré de $\mathcal{A}_\Delta$ à l'aide de celles de $\mathcal{A}_{\Delta_1}$ et $\mathcal{A}_{\Delta_2}$

$$P_{\mathcal{A}_\Delta}(t) = P_{\mathcal{A}_{\Delta_1}}(t^{\frac{D}{D_1}}) P_{\mathcal{A}_{\Delta_2}}(t^{\frac{D}{D_2}}),$$

et finalement la factorisation $P_\Delta(t) = P_{\Delta_1}(t^{\frac{D}{D_1}}) P_{\Delta_2}(t^{\frac{D}{D_2}})$.

Nous terminons cette section en démontrant, à l'aide de la formule précédente, que le polygone de Hodge de la somme directe $\Delta = \Delta_1 \oplus \Delta_2$ s'exprime à l'aide des polygones de Hodge de chacun des facteurs. Pour cela nous avons besoin d'introduire une nouvelle opération sur les polygones convexes. Rappelons qu'on a choisi de noter un polygone convexe d'origine O par $(s_i)_{1\le i\le a}$ quand il est formé par la juxtaposition des segments de longueur horizontale 1 et de pente s_i.

Définition 2.2. *Soient deux polygones convexes Π_1 et Π_2. Alors si*

$$\Pi_1 = (s_i)_{1\le i\le a},\ \Pi_2 = (s'_i)_{1\le i\le b},$$

on définit le produit de Π_1 et Π_2, et on note $\Pi_1 \times \Pi_2$ le polygone convexe d'origine O défini par

$$\Pi = (s_i + s'_j)_{1\le i\le a,\ 1\le j\le b}.$$

Remarquons que la longueur horizontale de Π est le produit des longueurs horizontales de Π_1 et Π_2, mais aussi que la longueur horizontale du segment de pente s dans Π est

$$\ell = \sum_{s_i + s'_j = s} \ell_i \ell'_j,$$

où ℓ_i (*resp.* ℓ'_j) est la longueur horizontale du segment de pente s_i (*resp.* s'_j) de Π_1 (*resp.* Π_2).

On en déduit la décomposition suivante pour le polygone $\mathrm{HP}(\Delta)$.

Proposition 2.1. *Soient Δ_1 et Δ_2 deux polyèdres convexes, et Δ leur somme directe. Alors le polygone de Hodge de Δ est le produit des polygones de Hodge de ses facteurs*

$$\mathrm{HP}(\Delta) = \mathrm{HP}(\Delta_1) \times \mathrm{HP}(\Delta_2).$$

3. Sommes exponentielles

Ici on considère deux polynômes de Laurent sur k, f_1 et f_2 respectivement en n_1 et n_2 variables, d'indéterminées $\mathbf{x}_1$ et $\mathbf{x}_2$, et on appelle $f = (f_1, f_2)$ le polynôme de Laurent en les $n := n_1 + n_2$ variables $\mathbf{x} = (x_1, \dots, x_{n_1+n_2})$ tel que $f(\mathbf{x}) = f_1(x_1, \dots, x_{n_1}) + f_2(x_{n_1+1}, \dots, x_{n_1+n_2})$. Il résulte immédiatement de la définition 2.1 que si Δ_1 et Δ_2 sont les polyèdres de Newton respectifs de f_1 et f_2 dans $\mathbb{R}^{n_1}$ et $\mathbb{R}^{n_2}$, alors le polyèdre de f est Δ, la somme directe de Δ_1 et Δ_2.

On va dans ce numéro réexprimer les espaces vectoriels de cohomologie étale associés aux sommes exponentielles provenant de f à l'aide de la formule de Künneth, et de ceux associés à f_1 et f_2 ; ensuite on en déduira des bornes pour les polygones de Newton génériques associés à Δ en fonction de ceux associés à Δ_1 et Δ_2.

Commençons par remarquer que la condition de non dégénérescence se transmet de f_1 et f_2 à f.

Lemme 3.1. *Soient f_1 et f_2 deux polynômes non dégénérés respectivement pour Δ_1 et Δ_2. Alors le polynôme $f = (f_1, f_2)$ est non dégénéré pour Δ.*

Soit ψ un caractère additif non trivial sur k, et $\mathcal{L}_\psi$ le $\overline{\mathbb{Q}}_\ell$-faisceau sur $\mathbb{A}^1_k$ associé à ψ et au recouvrement d'Artin-Schreier $y^q - y = x$. De même on note χ un caractère de $k^\times$ et $\mathcal{L}_\chi$ le $\overline{\mathbb{Q}}_\ell$-faisceau sur $\mathbb{G}_{m,k}$ associé à χ.

Si X est un schéma de type fini sur k, f une fonction régulière sur X (c'est à dire un morphisme $f : X \to \mathbb{A}^1$), et g une fonction régulière qui ne s'annule pas sur X, on peut construire comme dans l'introduction la fonction $L(X, f, g; T)$, et la formule des traces de Grothendieck nous permet de la réinterpréter à l'aide des polynômes caractéristiques de l'action du Frobenius sur les groupes de cohomologie à supports compacts de X à valeurs dans le faisceau $f^*\mathcal{L}_\psi \otimes g^*\mathcal{L}_\chi$

$$L(X, f, g; T) = \prod_i \det\left(I - TF | H^i_c(X \otimes \overline{k}, f^*\mathcal{L}_\psi \otimes g^*\mathcal{L}_\chi)\right)^{(-1)^{i-1}}.$$

Revenons à la situation qui nous intéresse. On a ici les trois fonctions $f_i : \mathbb{G}_m^{n_i} \to \mathbb{A}^1$, $1 \le i \le 2$, et $f = (f_1, f_2) : \mathbb{G}_m^n \to \mathbb{A}^1$. On fixe un caractère χ_1 (*resp.* χ_2) de $(k^\times)^{n_1}$ (*resp.* $(k^\times)^{n_2}$), et on note χ le caractère (χ_1, χ_2) de $(k^\times)^n$. D'après la définition de f, on a, en notant pr_i les projections canoniques de $\mathbb{G}_m^n = \mathbb{G}_m^{n_1} \times \mathbb{G}_m^{n_2}$ sur chacun de ses facteurs, que $f^*\mathcal{L}_\psi \otimes \mathcal{L}_\chi = \bigotimes_{i=1}^2 \mathrm{pr}_i^*\left(f_i^*\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_i}\right)$ est le produit tensoriel externe des deux faisceaux $f_i^*\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_i}$. Alors la formule de Künneth nous assure qu'on a un isomorphisme

$$H^\bullet_c(\mathbb{G}_m^n, f^*\mathcal{L}_\psi \otimes \mathcal{L}_\chi) = H^\bullet_c(\mathbb{G}_m^{n_1}, f_1^*\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_1}) \otimes H^\bullet_c(\mathbb{G}_m^{n_2}, f_2^*\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2}).$$

On a vu que f est non dégénéré quand f_1 et f_2 le sont ; dans ce cas l'isomorphisme précédent se réécrit simplement

$$H^n_c(\mathbb{G}_m^n, f^*\mathcal{L}_\psi \otimes \mathcal{L}_\chi) = H^{n_1}_c(\mathbb{G}_m^{n_1}, f_1^*\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_1}) \otimes H^{n_2}_c(\mathbb{G}_m^{n_2}, f_2^*\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2})$$

d'après des résultats de Denef et Loeser [**17**, Theorem 1.3]. En d'autres termes, la fonction $L(f, \chi; T)^{(-1)^{n-1}}$ est le polynôme dont les racines réciproques sont les produits des couples de racines réciproques des polynômes $L(f_1, \chi_1; T)^{(-1)^{n_1-1}}$ et $L(f_2, \chi_2; T)^{(-1)^{n_2-1}}$.

Rappelons que pour un polynôme de Laurent f on note $\mathrm{NP}_q(f,\chi)$ le polygone de Newton du polynôme $L(f,\chi;T)^{(-1)^{n-1}}$. On déduit en particulier des résultats précédents une factorisation de $\mathrm{NP}_q(f,\chi)$ qui nous sera utile un peu plus loin.

Lemme 3.2. *On a l'égalité de polygones de Newton*

$$\mathrm{NP}_q(f,\chi) = \mathrm{NP}_q(f_1,\chi_1) \times NP(f_2,\chi_2).$$

Pour un polyèdre Δ de dimension n, et χ un caractère multiplicatif comme ci-dessus, on a défini le polygone de Newton générique $\mathrm{GNP}(\Delta,\chi,p)$ comme la borne inférieure des polygones de Newton $\mathrm{NP}_q(f,\chi)$ quand f parcourt l'ensemble des polynômes de polyèdre Δ, non dégénérés. Quand Δ est une somme directe, on peut déduire des résultats précédents une borne pour ce polygone à l'aide des polygones de Newton génériques des facteurs de Δ.

Corollaire 3.1. *Soient Δ_1 et Δ_2 deux polyèdres convexes, et Δ leur somme directe. Alors on a*

$$\mathrm{GNP}(\Delta_1,\chi_1,p) \times \mathrm{GNP}(\Delta_2,\chi_2,p) \preceq \mathrm{GNP}(\Delta,\chi,p).$$

4. Comportement asymptotique, cas additif

On se place dans la situation suivante : on fixe un entier n, et on note $(\mathbf{e}_1,\dots,\mathbf{e}_n)$ une base du $\mathbb{Z}$-module $\mathbb{Z}^n$. D'autre part on choisit des entiers naturels $d_1,d_1',\dots,d_n,d_n'$ tels que pour chaque i on ait $(d_i,d_i') \neq (0,0)$ (sinon la situation qu'on va décrire peut se ramener en dimension inférieure). On note Δ le polyèdre convexe de $\mathbb{R}^n$ qui est l'enveloppe convexe de l'ensemble des points $\{d_i\mathbf{e}_i, -d_i'\mathbf{e}_i\}_{1\leq i\leq n}$ et de l'origine si nécessaire.

On va montrer le résultat suivant :

Théorème 4.1. *Quand p tend vers l'infini, le polygone de Newton générique de Δ associé au premier p,* $\mathrm{GNP}(\Delta,p)$*, tend vers le polygone de Hodge* $\mathrm{HP}(\Delta)$*.*

Démonstration. Commençons par réduire le problème au cas où $\mathbf{e}_i$ est le i-ème vecteur de la base canonique de $\mathbb{R}^n$. On peut définir une action à gauche de $\mathbf{M}_n(\mathbb{Z})$ sur l'espace des polynômes de Laurent en n variables, qui au polynôme $f(\mathbf{x}) = \sum a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}$ et à la matrice M associe le polynôme ${}^Mf(\mathbf{x}) = f({}^M\mathbf{x}) = \sum a_{\mathbf{i}}({}^M\mathbf{x})^{\mathbf{i}} = \sum a_{\mathbf{i}}\mathbf{x}^{M\mathbf{i}}$, où ${}^M\mathbf{x}$ est le n-uplet de variables dont la i-ème est $\prod_{j=1}^n x_j^{m_{ji}}$, et $M\mathbf{i}$ désigne la multiplication usuelle de la matrice M par le vecteur (colonne) $\mathbf{i}$. D'autre part, si M est dans $\mathbf{GL}_n(\mathbb{Z})$, l'application $\mathbf{x} \mapsto {}^M\mathbf{x}$ est une bijection de $(k^\times)^n$, ainsi que de chacune de ses extensions. Donc on obtient $L({}^Mf;T) = L(f;T)$.

Soit maintenant f un polynôme de Laurent de la forme $f(\mathbf{x}) = \sum_{i=1}^n \sum_{j=-d_i'}^{d_i} a_{ij}\mathbf{x}^{j\mathbf{e}_i}$, dont le polyèdre convexe est Δ. En choisissant pour M la matrice de passage de la base $\{\mathbf{e}_1,\dots,\mathbf{e}_n\}$ à la base canonique, on voit que ${}^Mf(\mathbf{x}) = \sum_{i=1}^n \sum_{j=-d_i'}^{d_i} a_{ij}x_i^j$, dont le polyèdre associé est l'enveloppe convexe des points de coordonnées

$$(d_1,0,\dots,0),(-d_1',0,\dots,0),\dots,(0,\dots,0,d_n),(0,\dots,0,-d_n').$$

Mais ce dernier polyèdre est la somme directe des segments $[-d_i',d_i]$, $1\leq i\leq n$, et le corollaire 3.1 nous assure que

$$\mathrm{GNP}([-d_1',d_1],p) \times \cdots \times \mathrm{GNP}([-d_n',d_n],p) \preceq \mathrm{GNP}(\Delta,p).$$

D'autre part, d'après la proposition 2.1, on a $\mathrm{HP}(\Delta) = \mathrm{HP}([-d_1',d_1]) \times \cdots \times \mathrm{HP}([d_n',d_n])$. Le résultat découle maintenant du fait que pour chaque i, le polygone $\mathrm{GNP}([-d_i',d_i],p)$ tend vers $\mathrm{HP}([-d_i',d_i])$ quand p tend vers ∞ : le polygone $\mathrm{GNP}(\Delta,p)$ est encadré entre deux polygones ayant la même limite. □

Remarque 4.1. *Dans le cas où $p \equiv 1$ modulo* $\mathrm{ppcm}(d,d')$*, on sait (cf.* [**55**]*) que les polygones* $\mathrm{GNP}([-d',d],p)$ *et* $\mathrm{HP}([-d',d])$ *coïncident. En particulier, si $p \equiv 1$ modulo $D = \mathrm{ppcm}(d_i,d_i')_{1\leq i\leq n}$, on en déduit que les polygones* $\mathrm{GNP}(\Delta,p)$ *et* $\mathrm{HP}(\Delta)$ *coïncident, et la conjecture d'Adolphson et Sperber* [**2**, p. 386] *est vérifiée dans ce cas.*

Considérons maintenant la seconde question, à savoir l'existence d'un ouvert dense $\mathcal{U}_\Delta$ défini sur $\mathbb{Q}$ de l'espace des polynômes à coefficients dans $\overline{\mathbb{Q}}$ de polyèdre de Newton Δ tel que pour tout f de $\mathcal{U}_\Delta$, on ait $\lim_{p\to\infty} \mathrm{NP}_q(f \mod \mathfrak{p}) = \mathrm{HP}(\Delta)$, où $\mathfrak{p}$ est un premier au dessus de p dans le corps $\mathbb{Q}_f$ engendré par les coefficients de f. Comme on ne considère pas tous les polynômes de polyèdre Δ, on ne peut répondre à cette question. En revanche, pour les sous-familles que nous avons utilisées, on obtient le résultat suivant :

Théorème 4.2. *Il existe un ouvert dense $\mathcal{U}$ défini sur $\mathbb{Q}$ de l'espace des polynômes de la forme $f(x) = \sum_{i=1}^{n}\sum_{j=-d_i'}^{d_i} A_{ij}\mathbf{x}^{je_i}$ à coefficients dans $\overline{\mathbb{Q}}$ tel que pour tout polynôme dans $\mathcal{U}$, on ait*

$$\lim_{p\to\infty} \mathrm{NP}_q(f \mod \mathfrak{p}) = \mathrm{HP}(\Delta).$$

Remarque 4.2. *Le polynôme de Hasse qui définit $\mathcal{U}$ est le produit des $\mathscr{H}_{[-d_i',d_i]}$ du chapitre précédent (voir aussi* [**46**]*).*

5. Comportement asymptotique des sommes tordues

Dans cette section, on note encore $(\mathbf{e}_1,\dots,\mathbf{e}_n)$ une base du $\mathbb{Z}$-module $\mathbb{Z}^n$, et Δ le polyèdre convexe de $\mathbb{R}^n$ qui est l'enveloppe convexe de l'ensemble des points $\{d_i\mathbf{e}_i, -d_i'\mathbf{e}_i\}_{1\le i\le n}$ et de l'origine si nécessaire. On va étudier le comportement asymptotique des polygones de Newton de la forme $\mathrm{NP}_q(f,\chi)$ et des $\mathrm{GNP}(\Delta,\chi,p)$ pour f comme plus haut, et χ un caractère multiplicatif de $(k^\times)^n$ d'ordre fixé. Cette étude a été menée en dimension 1 dans la section 3, et nous allons la généraliser ici. Comme dans le cas des polynômes en une variable, les résultats sont assez différents du cas additif puisque qu'il n'y a plus de limite, mais une limite pour chaque classe inversible modulo l'ordre du caractère.

On sait exprimer le polygone de Hodge associé à une somme directe de polyèdres et à deux caractères multiplicatifs, à l'aide des polygones de Hodge associés à ses facteurs. C'est l'exacte transposition de la proposition 2.1 dans ce nouveau cadre, la démonstration en est très similaire au cas du polygone de Hodge de l'algèbre $\mathcal{A}_\Delta$.

Proposition 5.1. *Soient Δ_1 et Δ_2 deux polyèdres convexes, respectivement dans $\mathbb{R}^{n_1}$ et $\mathbb{R}^{n_2}$, et Δ leur somme directe. Si on pose*

$$\boldsymbol{\delta}_1 = (\delta_1,\dots,\delta_{n_1}),\ \boldsymbol{\delta}_2 = (\delta_{n_1+1},\dots,\delta_{n_1+n_2}),\ \text{et } \boldsymbol{\delta} = (\boldsymbol{\delta}_1,\boldsymbol{\delta}_2) = (\delta_1,\dots,\delta_{n_1+n_2}),$$

alors le polygone de Hodge $\mathrm{HP}(\Delta, \frac{\boldsymbol{\delta}}{q-1})$ est le produit des polygones de Hodge de ses facteurs

$$\mathrm{HP}(\Delta, \frac{\boldsymbol{\delta}}{q-1}) = \mathrm{HP}(\Delta_1, \frac{\boldsymbol{\delta}_1}{q-1}) \times \mathrm{HP}(\Delta_2, \frac{\boldsymbol{\delta}_2}{q-1}).$$

On peut définir des polygones de Hodge-Stickelberger dans ce nouveau cadre :

Définition 5.1. *On pose, pour Δ un polyèdre convexe, $\frac{\mathbf{r}}{\mathbf{s}} = (\frac{r_1}{s_1},\dots,\frac{r_n}{s_n})$, p un premier de résidu ν modulo $s = \mathrm{ppcm}(s_1,\dots,s_n)$ et q une puissance de p telle que $q \equiv 1 \mod s$*

$$\mathrm{HS}(\Delta, \frac{\mathbf{r}}{\mathbf{s}}, \nu) := \mathrm{HP}(\Delta, \frac{\boldsymbol{\delta}}{q-1})$$

avec $\boldsymbol{\delta} = \left(\frac{(q-1)r_1}{s_1},\dots,\frac{(q-1)r_n}{s_n}\right)$.

Remarque 5.1. *On vérifie aisément, à l'aide de la définition qu'on en a donné, que ce polygone ne dépend pas de q, la puissance de p qu'on choisit. D'autre part il ne dépend ici encore que du reste de p modulo s, ce qui justifie notre notation.*

A l'aide de ces notations, les transpositions des théorèmes 4.1 et 4.2 à cette nouvelle situation s'écrivent :

Théorème 5.1. *Quand p tend vers l'infini, le polygone de Newton générique de Δ associé au premier p et au caractère χ, $\mathrm{GNP}(\Delta,\chi,p)$, tend vers le polygone de Hodge-Stickelberger $\mathrm{HS}(\Delta,\frac{\mathbf{r}}{\mathbf{s}},\nu)$ quand p tend vers $+\infty$ avec $p \equiv \nu\ [s]$.*

Théorème 5.2. *Il existe un ouvert dense $\mathcal{U}$ défini sur $\mathbb{Q}$ de l'espace des polynômes de la forme $f(x) = \sum_{i=1}^{n}\sum_{j=-d_i'}^{d_i} a_{ij}\mathbf{x}^{j\mathbf{e}_i}$ à coefficients dans $\overline{\mathbb{Q}}$ tel que pour tout polynôme dans $\mathcal{U}$, on ait*

$$\lim_{\substack{p\to+\infty \\ p\equiv\nu\ [s]}} \mathrm{NP}_q(f \mod \mathfrak{p}, \chi_p) = \mathrm{HS}(\Delta, \frac{\mathbf{r}}{\mathbf{s}}, \nu).$$

Remarque 5.2. *Dans le cas où tous les chiffres p-adiques de $\frac{(q-1)r}{s}$ sont divisibles par $\mathrm{ppcm}(d,d')$, et en particulier quand $p \equiv 1$ modulo $\mathrm{ppcm}(d,d',s)$, on sait (cf.* [**BFZ**]*) que les polygones $\mathrm{GNP}([-d',d],\chi,p)$ et $\mathrm{HS}([-d',d],\frac{r}{s},1)$ coïncident. En particulier, si pour tout $1 \le i \le n$ les chiffres p-adiques de $\frac{(q-1)r_i}{s_i}$ sont*

divisibles par $\mathrm{ppcm}(d_i, d_i')$*, ce qui se produit quand* $p \equiv 1$ *modulo* $D = \mathrm{ppcm}(d_i, d_i', s_i)_{1\leq i\leq n}$*, on en déduit que les polygones* $\mathrm{GNP}(\Delta, \chi, p)$ *et* $\mathrm{HP}(\Delta, \frac{\mathbf{r}}{\mathbf{s}}, 1)$ *coïncident, et on a vérifié dans ce cas une extension de la conjecture d'Adolphson et Sperber aux sommes tordues.*

Terminons ce chapitre par le cas particulier $s = 2$. Pour un nombre premier impair p fixé, on note χ_2 le caractère quadratique, défini sur $k^\times$ par $\chi_2(x) = \omega^{\frac{q-1}{2}}(x)$. Tous les caractères multiplicatifs d'ordre 2 de $(k^\times)^n$ sont de la forme $\chi_2^{\boldsymbol{\varepsilon}}$, avec $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n$, et $\chi_2^{\boldsymbol{\varepsilon}}(x_1, \ldots, x_n) = \chi_2^{\varepsilon_1}(x_1) \ldots \chi_2^{\varepsilon_n}(x_n)$. Puisque (presque) tous les premiers sont impairs, le polygone de Hodge-Stickelberger ne dépend plus que de $\boldsymbol{\varepsilon}$, on le note $\mathrm{HS}(\Delta, \frac{\boldsymbol{\varepsilon}}{2})$. Pour la même raison, on peut décrire directement ce polygone à l'aide d'une série de Poincaré.

Lemme 5.1. *Soit* Δ *un polyèdre convexe de* $\mathbb{R}^n$ *(et qui l'engendre),* $\mathcal{A}_{\Delta, \frac{\boldsymbol{\varepsilon}}{2}}$ *le* $\mathcal{A}_\Delta$*-module gradué défini à la section 4.2. Alors le polygone* $\mathrm{HS}(\Delta, \frac{\boldsymbol{\varepsilon}}{2})$ *est le polygone issu de la série de Poincaré de* $\mathcal{A}_{\Delta, \frac{\boldsymbol{\varepsilon}}{2}}$*.*

L'indépendance du polygone de Hodge par rapport à p nous permet de retrouver l'existence d'une limite.

Corollaire 5.1. *Quand* p *tend vers l'infini, le polygone de Newton générique de* Δ *associé au premier* p *et au caractère quadratique* χ_2*,* $\mathrm{GNP}(\Delta, \chi_2, p)$*, tend vers le polygone de Hodge-Stickelberger* $\mathrm{HS}(\Delta, \frac{\boldsymbol{\varepsilon}}{2})$ *quand* p *tend vers* $+\infty$*.*

Corollaire 5.2. *Il existe un ouvert dense* $\mathcal{U}$ *défini sur* $\mathbb{Q}$ *de l'espace des polynômes de la forme* $f(x) = \sum_{i=1}^n \sum_{j=-d_i'}^{d_i} a_{ij} \mathbf{x}^{j\mathbf{e}_i}$ *à coefficients dans* $\overline{\mathbb{Q}}$ *tel que pour tout polynôme dans* $\mathcal{U}$*, on ait*

$$\lim_{p\to+\infty} \mathrm{NP}_q(f \mod \mathfrak{p}, \chi_2) = \mathrm{HS}(\Delta, \frac{\boldsymbol{\varepsilon}}{2}).$$

6. Polynômes de polyèdres d'exposant deux

Dans cette partie on étend les principaux résultats à des polyèdres un peu plus généraux : on fixe un entier n, et on note $(\mathbf{f}_1, \ldots, \mathbf{f}_n)$ une famille libre de $\mathbb{Z}^n$, qui engendre un sous-module N contenant $2\mathbb{Z}^n$. Comme dans les sections précédentes on choisit des entiers naturels $d_1, d_1', \ldots, d_n, d_n'$. On note Δ le polyèdre convexe de $\mathbb{R}^n$ qui est l'enveloppe convexe de l'ensemble des points $\{d_i\mathbf{f}_i, -d_i'\mathbf{f}_i\}_{1\leq i\leq n}$ et de l'origine si nécessaire. On va réexprimer les sommes additives associées à certains polynômes de polyèdre Δ à l'aide de sommes mixtes étudiées dans le chapitre précédent ; on utilisera ensuite les corollaires 5.1 et 5.2 pour obtenir la limite.

Dans toute la suite, on suppose que p est un nombre premier impair.

Soit $\mathcal{F} = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ une famille libre de $\mathbb{Z}^n$, qui engendre un sous-module N de $\mathbb{Z}^n$ tel que le quotient $\mathbb{Z}^n/N$ soit un groupe d'exposant 2. On note $M = (f_{ij})$ la matrice de passage de la base canonique à la famille $\mathcal{F}$ dans $\mathbf{M}_n(\mathbb{Z})$, et k la dimension comme $\mathbb{F}_2$-espace vectoriel de $\mathbb{Z}^n/N$. On a donc la suite exacte

$$0 \to \mathbb{Z}^n \to \mathbb{Z}^n \to \mathbb{Z}^n/N \simeq \mathbb{F}_2^k \to 0, \tag{6}$$

où la première flèche est l'action de M.

On peut trouver une base $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ de $\mathbb{Z}^n$ (comme $\mathbb{Z}$-module) telle que la famille

$$\mathbf{e}_1, \ldots, \mathbf{e}_{n-k}, 2\mathbf{e}_{n-k+1}, \ldots, 2\mathbf{e}_n$$

soit une base de N. En d'autres termes la matrice M est équivalente, sur $\mathbf{M}_n(\mathbb{Z})$, à la matrice diagonale dont les $n-k$ premiers coefficients diagonaux valent 1, et les k derniers valent 2 ; remarquons qu'on doit avoir $\det M = 2^k$.

Définition 6.1. *On note* M_2 *l'application linéaire de* $\mathbb{F}_2^n$ *induite par la réduction modulo* 2 *de la matrice* M*. Soit* $\overline{E}$ *son noyau, et pour tout* $\overline{\boldsymbol{\varepsilon}} = (\overline{\varepsilon}_1, \ldots, \overline{\varepsilon}_n) \in \overline{E}$*, notons* $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n)$ *le relèvement de* $\overline{\boldsymbol{\varepsilon}}$ *à* $\{0,1\}^n$*. Finalement, soit* E *le sous ensemble de* $\{0,1\}^n$ *formé des* $\boldsymbol{\varepsilon}$ *quand* $\overline{\boldsymbol{\varepsilon}}$ *décrit* $\overline{E}$*.*

L'ensemble E qu'on vient de définir va nous servir à décrire les points entiers d'un domaine fondamental de $\mathbb{Z}^n/N$. D'autre part, rappelons que si $\mathbf{x} = (x_1, \ldots, x_n)$, on note ${}^M\mathbf{x} = (y_1, \ldots, y_n)$, avec $y_i = \prod_{j=1}^n x_j^{f_{ji}}$. L'ensemble E va aussi nous servir à décrire l'image du morphisme $\varphi_M : \mathbf{x} \mapsto {}^M\mathbf{x}$ de $(k^\times)^n$ dans lui-même, et à réexprimer les sommes pures, (ainsi que leurs fonctions L et groupes de cohomologie) associées au

polynôme $f({}^M\mathbf{x})$ en fonction de sommes associées au polynôme f tordues par certains caractères quadratiques. On rappelle qu'on note $\chi_2^{\boldsymbol{\varepsilon}}$, avec $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n) \in \{0,1\}^n$, le caractère (multiplicatif) de $k^{\times n}$ défini par $\chi_2^{\boldsymbol{\varepsilon}}(x_1, \dots, x_n) = \chi_2^{\varepsilon_1}(x_1) \dots \chi_2^{\varepsilon_n}(x_n)$.

Lemme 6.1. (1) *L'ensemble des points entiers contenus dans le polyèdre*

$$[0,1[\mathbf{f}_1 \times \cdots \times [0,1[\mathbf{f}_n = \left\{ \sum_{i=1^n} x_i \mathbf{f}_i,\ 0 \leq x_i < 1 \right\}$$

est $\{\mathbf{f}_{\boldsymbol{\varepsilon}} := \frac{1}{2}\sum_{i=1}^n \varepsilon_i \mathbf{f}_i,\ \boldsymbol{\varepsilon} \in E\}$.

(2) *Le sous-groupe du groupe des caractères multiplicatifs de* $(k^\times)^n$ *orthogonal à l'image du morphisme* φ_M *est*

$$(\mathrm{Im}\varphi_M)^\perp = \{\chi_2^{\boldsymbol{\varepsilon}},\ \boldsymbol{\varepsilon} \in E\}\,.$$

La formule de Poisson permet de réexprimer les sommes pures associées à un polynôme de Laurent de la forme $f({}^M\mathbf{x})$.

Proposition 6.1. *Soit* $f \in k[\mathbf{x}, \mathbf{x}^{-1}]$ *un polynôme de Laurent, et* M *comme précédemment ; on rappelle que* ${}^M f$ *est le polynôme de Laurent* $f({}^M x)$. *On a les décompositions suivantes*

(1) *des sommes de caractères*

$$\sum_{\boldsymbol{x} \in k_r^{\times n}} \psi({}^M f(\mathbf{x})) = \sum_{\boldsymbol{\varepsilon} \in E} \sum_{\boldsymbol{x} \in k_r^{\times n}} \psi(f(\mathbf{x}))\chi_2^{\boldsymbol{\varepsilon}}(\mathbf{x})\ ;$$

(2) *de la fonction L*

$$L({}^M f, T) = \prod_{\boldsymbol{\varepsilon} \in E} L(f, \chi_2^{\boldsymbol{\varepsilon}}; T)\ ;$$

(3) *de la suite exacte longue de cohomologie*

$$H_c^\bullet(\mathbb{G}_m^n, ({}^M f)^* \mathcal{L}_\psi) = \bigoplus_{\boldsymbol{\varepsilon} \in E} H_c^\bullet(\mathbb{G}_m^n, f^* \mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2^{\boldsymbol{\varepsilon}}}).$$

On va en déduire une décomposition pour le polygone de Newton

Corollaire 6.1. *Le polygone de Newton associé au polynôme* ${}^M f$ *est la juxtaposition des polygônes de Newton associés au polynôme* f *et aux caractères* $\chi_2^{\boldsymbol{\varepsilon}}$ *quand* $\boldsymbol{\varepsilon}$ *décrit* E

$$\mathrm{NP}_q({}^M f) = \coprod_{\boldsymbol{\varepsilon} \in E} \mathrm{NP}_q(f, \chi_2^{\boldsymbol{\varepsilon}}).$$

Nous allons maintenant réécrire le polygone de Hodge $\mathrm{HP}(\Delta)$ à l'aide des polygones des sections précédentes :

Lemme 6.2. *Soit* Δ_0 *le polyèdre convexe de* $\mathbb{R}^n$ *qui est l'enveloppe convexe de l'ensemble des points* $\{d_i\mathbf{e}_i, -d_i'\mathbf{e}_i\}_{1 \leq i \leq n}$ *et de l'origine si nécessaire, pour* $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ *une base du* $\mathbb{Z}$*-module* $\mathbb{Z}^n$. *On a la décomposition suivante du polygone de Hodge associé à* Δ *:*

$$\mathrm{HP}(\Delta) = \mathrm{HP}(\Delta_0) \coprod \left(\coprod_{\boldsymbol{\varepsilon} \in E \setminus \{0,\dots,0\}} \mathrm{HS}(\Delta_0, \frac{\boldsymbol{\varepsilon}}{2}) \right).$$

Nous pouvons démontrer le résultat suivant

Théorème 6.1. *Quand* p *tend vers l'infini, le polygone de Newton générique de* Δ *associé au premier* p, $\mathrm{GNP}(\Delta, p)$, *tend vers le polygone de Hodge* $\mathrm{HP}(\Delta)$.

Démonstration. Remarquons d'abord que

$$f(\mathbf{x}) = \sum_{i=1}^n \sum_{j=-d_i'}^{d_i} a_{ij}\mathbf{x}^{j\mathbf{f}_i} =^M g(x),$$

pour le polynôme $g(\mathbf{x}) = \sum_{i=1}^{n} \sum_{j=-d_i'}^{d_i} a_{ij} x_i^j$. D'après le corollaire 6.1, le polygone de Newton générique de la famille des polynômes $f(\mathbf{x}) = \sum_{i=1}^{n} \sum_{j=-d_i'}^{d_i} a_{ij} x^{j\mathbf{f}_i},\ a_{ij} \in k$ est donné par

$$\mathrm{GNP}(\Delta_0, p) \coprod \left(\coprod_{\boldsymbol{\varepsilon} \in E \setminus \{0,\dots,0\}} \mathrm{GNP}(\Delta_0, \frac{\boldsymbol{\varepsilon}}{2}, p) \right)$$

pour p assez grand puisqu'alors les ouverts de Hasse en jeu ont forcément une intersection non vide.

Le théorème de spécialisation de Grothendieck assure que le polygone de Newton générique de la famille de tous les polynômes de polyèdre Δ vérifie

$$\mathrm{GNP}(\Delta_0, p) \coprod \left(\coprod_{\boldsymbol{\varepsilon} \in E \setminus \{0,\dots,0\}} \mathrm{GNP}(\Delta_0, \frac{\boldsymbol{\varepsilon}}{2}, p) \right) \preceq \mathrm{GNP}(\Delta, p) \preceq \mathrm{HP}(\Delta).$$

Finalement le lemme 6.2, joint au théorème 4.1 appliqué au polyèdre Δ_0, et au corollaire 5.1 nous assurent que le membre de gauche tend vers le membre de droite quand p tend vers ∞. Donc le polygone $GNP(\Delta, p)$ tend vers $\mathrm{HP}(\Delta)$ quand p tend vers ∞. □

De même on obtient, pour l'autre conjecture

Théorème 6.2. *Il existe un ouvert dense $\mathcal{U}$ défini sur $\mathbb{Q}$ de l'espace des polynômes de la forme $f(x) = \sum_{i=1}^{n} \sum_{j=-d_i'}^{d_i} a_{ij} \mathbf{x}^{j\mathbf{f}_i}$ à coefficients dans $\overline{\mathbb{Q}}$ tel que pour tout polynôme dans $\mathcal{U}$, on ait*

$$\lim_{p \to \infty} \mathrm{NP}_q(f \mod \mathfrak{p}) = \mathrm{HP}(\Delta).$$

7. Conclusion et questions

Ce sont les premiers exemples, en dimension supérieure et quand le dénominateur n'est pas $D = 1$ ou 2, sur lesquels les conjectures sur le comportement asymptotique des polygones de Newton sont vérifiées. Ceci dit, il est clair qu'on est loin d'avoir démontré ces conjectures dans le cas général. On a seulement utilisé quelques propriétés bien connues des sommes de caractères pour se ramener au résultat en dimension 1. Un peu plus généralement, on peut montrer que si les polygones de Newton génériques $\mathrm{GNP}(\Delta_1, p)$ et $\mathrm{GNP}(\Delta_2, p)$ associés à deux polyèdres Δ_1 et Δ_2 convergent vers les polygones de Hodge respectifs, alors il en est de même pour $\mathrm{GNP}(\Delta, p)$ avec $\Delta = \Delta_1 \oplus \Delta_2$. Cela donne quelques exemples supplémentaires à l'aide des cas démontrés par Wan pour $D = 1$ ou $D = 2$ (*cf.* [**65**]).

Il n'est pas étonnant qu'on se soit appuyé sur les résultats en dimension 1. En fait il ne faut pas espérer travailler sur des polynômes à plusieurs variables avec les idées qu'on a utilisées jusqu'ici. Il y a plusieurs raisons à cela

(1) le problème combinatoire de montrer qu'un certain polynôme de Hasse est non nul devient très compliqué. Il était déjà astucieux de montrer l'existence d'un monôme non nul en dimension 1, mais à partir de la dimension 2 cette question devient extrèmement compliquée ;

(2) on a beaucoup utilisé la description explicite des coefficients de l'exponentielle d'Artin-Hasse de valuation p-adique ≤ 1 (voir en particulier le lemme 2.2). Cela nous a donné les pentes en dimension 1 sans problème, puisqu'elles sont toutes plus petites que 1. En revanche, en dimension supérieure, les nouvelles pentes peuvent dépasser 1, et on aurait besoin d'une description suffisamment explicite de tous les coefficients de la série AH.

Remarquons que les estimations explicites des coefficients peuvent servir dans un autre contexte. Dans le cas d'une hypersurface de l'espace (affine ou projectif), on sait donner une formule de congruence modulo p pour la fonction zêta [**30**]. Dans le cas des courbes, cette formule provient du calcul du polynôme caractéristique de la matrice de Hasse Witt. En dimension supérieure, on sait généraliser cette matrice [**51**] pour obtenir l'action de l'endomorphisme de Frobenius dans une base de $H^n(X, \mathcal{O}_{X/k})$, et on retrouve la formule de congruence par les mêmes calculs. On retrouve ces résultats avec les idées exposées ici, à l'aide de la remarque 2.1, de la description de la partie de poids 1 de l'homologie du complexe de Koszül et du lemme 2.2 qui s'étend en dimension supérieure. Il serait intéressant de pouvoir généraliser (au cas des intersections complètes) ces matrices pour obtenir des bases pour les espaces $H^{n-i}(X, \Omega^i_{X/k})$, une matrice

de l'action de Frobenius dans chacun de ces espaces, et en déduire des congruences pour les "parties de pente fixée" de la fonction zêta.

Pour en revenir aux idées qui nous ont plus particulièrement intéressés dans ce chapitre, il serait intéressant d'obtenir des théorèmes de décomposition du polygone de Newton générique plus généraux que ceux donnés ici. C'est la stratégie de Wan pour étudier la coïncidence du polygone de Newton générique avec le polygone de Hodge. Malheureusement ses méthodes ne se généralisent pas dans le cas où les deux polygones sont distincts : ils reposent sur le fait que le poids est sous additif, qu'il est additif exactement pour les points cofaciaux. Cette propriété n'est plus utile ici comme le polygone de Newton générique ne coïncide plus avec le polygone de Hodge.

CHAPITRE 5

Propriétés d'orthogonalité pour l'opérateur de Frobenius associé à certaines sommes de caractères.

On va essayer ici d'aller un peu plus loin que la borne de Weil dans le cas suivant : $f(t) \in k[t, t^{-1}]$ désigne un polynôme de Laurent en une variable, et χ un caractère multiplicatif de $k^\times$; on note d_0 (*resp.* d_∞) l'ordre de son pôle en 0 (*resp.* en ∞). On sait alors que la fonction L

$$L(f, \chi, T) := \exp\left(\sum_{r\geq 1} S_r(f, \chi)\frac{T^r}{r}\right)$$

est un polynôme de degré $d := d_0 + d_\infty$ ($d-1$ quand f admet un seul pôle et χ est trivial), dont les racines réciproques $\alpha_1, \ldots, \alpha_d$ sont des entiers algébriques ayant tous leurs conjugués complexes de module $q^{\frac{1}{2}}$. Une conséquence directe de ce résultat est la majoration (souvent appelée borne de Weil)

$$|S_r(f, \chi)| \leq d\sqrt{q^r}.$$

Intuitivement, si on arrive à prouver que les points d'affixe α_i sont bien distribués sur le cercle de rayon $\sqrt{q}$, la somme de caractères sera petite. C'est malheureusement une question difficile, et la remarque qu'on va faire ici ne donne qu'une réponse très partielle : quand le polynôme f est impair, et χ le caractère quadratique, on va montrer que deux des racines réciproques sont opposées, ce qui conduit à l'amélioration suivante de la borne de Weil

$$|S_r(f, \chi)| \leq (d-2)\sqrt{q}.$$

Ce résultat n'est pas nouveau, sa manifestation la plus célèbre est l'annulation de certaines sommes de Salié (qu'on peut cependant montrer de façon beaucoup plus élémentaire) ; donnons en une explication rapide. On sait associer à la situation qu'on vient de décrire un espace de dimension d (le H^1 d'une certaine suite de cohomologie de de Rham p-adique dans cet article –*cf.* section 1– ou le H^1 étale d'un certain faisceau ℓ-adique – *cf.* section 2.1), et une application linéaire F (l'application de Dwork dans le premier cas, le Frobenius dans le second) dont la fonction L est le polynôme caractéristique. Dans [**34**] (voir aussi [**33**]), Katz parvient à déterminer les groupes de monodromie associés à certaines familles de sommes de caractères indexées par des familles à un paramètre, c'est à dire les groupes engendrés par les applications linéaires $\frac{1}{\mathscr{G}_q}F_x$ quand x décrit une famille à un paramètre (ici $\mathscr{G}_q$ représente la somme de Gauss quadratique sur k). Dans les cas particuliers qui nous intéressent (par exemple la famille $f_x(t) = f(t) + xt$), il parvient à prouver que ce groupe est

(1) le groupe symplectique $\mathbf{Sp}(d)$ quand le caractère multiplicatif χ est trivial et le polynôme f est impair.

(2) le groupe orthogonal $\mathbf{O}(d)$ quand le caractère multiplicatif χ est le caractère quadratique χ_2 et le polynôme f est impair.

On trouve aussi une démonstration, à l'aide de la dualité de Poincaré, du fait que dans le premier cas l'opérateur est symplectique dans [**14**, Sommes Trig. p 25]. Dans le second cas, quand le déterminant de $\frac{1}{\mathscr{G}_q}F_x$ est -1, le résultat est une conséquence du fait qu'un endomorphisme orthogonal en un nombre pair de variables, et de déterminant -1, possède comme valeurs propres à la fois 1 et -1 ; sa trace est donc majorée par $d-2$. Puisqu'on a $S_r(f, \chi) = \mathrm{Tr}(F)$, on en déduit le résultat.

On va retrouver ces résultats à l'aide des méthodes p-adiques initiées par Dwork, en s'inspirant des travaux de Robba. On sait associer un module différentiel sur un anneau de séries surconvergentes à notre situation, puis une suite de cohomologie de de Rham p-adique. Son H^1 est muni d'un endomorphisme $\overline{\alpha}$ dont

le polynôme caractéristisque est la fonction L recherchée. On dispose d'autre part d'un module différentiel dual. Dans les cas qui nous intéressent, on peut exhiber un isomorphisme entre le module différentiel et son dual, à l'aide duquel on construit une forme bilinéaire non dégénérée, alternée quand le caractère χ est trivial, symétrique quand c'est le caractère quadratique. L'endomorphisme $\frac{1}{\mathscr{G}_q}\overline{\alpha}$ conserve cette forme, redonnant ainsi une partie du résultat de Katz.

Nous conseillons au lecteur de lire la section 1 du chapitre 3 avant ce qui suit.

1. Dualité

On va décrire et utiliser ici certains des résultats de [**57**] relatifs à la théorie de Dwork duale. On va les expliciter dans le cas où A est la couronne $B(0,1)^+\backslash B(0,1)^-$ puisque les applications qu'on en donnera ne concernent que des sommes définies sur $k^\times$.

Commençons par définir quelques anneaux de fonctions analytiques

$$\mathscr{R}'_0 = \{\text{fonctions analytiques sur une couronne } r < |x| < 1,\ r < 1\};$$

$$\mathscr{R}'_\infty = \{\text{fonctions analytiques sur une couronne } 1 < |x| < \frac{1}{r},\ r < 1\ \};$$

$$\mathscr{R}_0 = \{\text{fonctions analytiques sur la boule } |x| < 1\};$$

$$\mathscr{R}_\infty = \{\text{fonctions analytiques sur la "boule" } |x| > 1, \text{ et nulles en } \infty\}.$$

Le premier est communément appelé "anneau de Robba".

On pose $\mathscr{R}(A) := \mathscr{R}_0 \oplus \mathscr{R}_\infty$ et $\mathscr{R}'(A) := \mathscr{R}'_0 \oplus \mathscr{R}'_\infty$. D'après le théorème de Mittag Loeffler, on a les sommes directes

$$\mathscr{R}'_0 = \mathscr{H}_0^\dagger(B(\infty,1)) \oplus \mathscr{R}_0; \quad \mathscr{R}'_\infty = \mathscr{H}^\dagger(B(0,1)) \oplus \mathscr{R}_\infty;$$
$$\mathscr{H}^\dagger(A) = \mathscr{H}^\dagger(B(0,1)) \oplus \mathscr{H}_0^\dagger(B(\infty,1)).$$

où l'anneau $\mathscr{H}_0^\dagger(B(\infty,1))$ est celui des fonctions analytiques sur une "boule" de la forme $|x| > r,\ r < 1$, et nulles en ∞. On en déduit la suite exacte

$$0 \to \mathscr{R}(A) \to \mathscr{R}'(A) \to \mathscr{H}^\dagger(A) \to 0.$$

Plus précisément, si $f_0 = \sum_{n\in\mathbb{Z}} a_n t^n \in \mathscr{R}'_0$, et $f_\infty = \sum_{n\in\mathbb{Z}} b_n t^n \in \mathscr{R}'_\infty$, la projection de (f_0, f_∞) sur $\mathscr{H}^\dagger(A)$ est h, pour la série $h = \sum_{n<0} a_n t^n + \sum_{n\geq 0} b_n t^n$, et sa projection sur $\mathscr{R}(A)$ est le couple (g_0, g_∞), avec $g_0 = \sum_{n\geq 0}(a_n - b_n)t^n$ et $g_\infty = \sum_{n<0}(b_n - a_n)t^n$. Cette suite exacte est scindée par le plongement diagonal $h \mapsto (h, h)$ de $\mathscr{H}^\dagger(A)$ dans $\mathscr{R}'(A)$.

On va maintenant définir une forme bilinéaire (sur $\mathbb{C}_p$) symétrique sur $\mathscr{R}'(A)$. Commençons par définir des résidus de façon similaire à celle des fonctions analytiques sur $\mathbb{C}$. Pour $u = \sum a_n t^n \in \mathscr{R}'_0$, on pose $\mathrm{Res}_0(u\frac{\mathrm{d}t}{t}) = a_0$, et pour $u = \sum a_n t^n \in \mathscr{R}'_\infty$, on pose $\mathrm{Res}_\infty(u\frac{\mathrm{d}t}{t}) = -a_0$. D'autre part on pose, pour $u = (u_0, u_\infty) \in \mathscr{R}'(A)$,

$$\int u\frac{\mathrm{d}t}{t} = \mathrm{Res}_0(u\frac{\mathrm{d}t}{t}) + \mathrm{Res}_\infty(u\frac{\mathrm{d}t}{t}).$$

On a une formule à la Cauchy : si $u \in \mathscr{H}^\dagger(A)$, alors $\int u\frac{\mathrm{d}t}{t} = 0$.

On définit la forme bilinéaire $(\cdot,\cdot)$ sur $\mathscr{R}'(A)$ par

$$(u, v) = \int uv\frac{\mathrm{d}t}{t}.$$

On peut vérifier qu'elle est non dégénérée, et que $\mathscr{R}'(A)$ s'identifie ainsi à son dual topologique. D'après la formule de Cauchy, on voit aussi que $\mathscr{H}^\dagger(A)$ est égal à son orthogonal.

Considérons le module différentiel $\mathscr{M} = F\mathscr{H}^\dagger(A)$, avec $F(t) = t^{\frac{e}{1-q}}\exp(\pi f(t))$. On note $\mathscr{M}^* = \mathrm{Hom}_{\mathscr{H}^\dagger(A)}(\mathscr{M}, \mathscr{H}^\dagger(A))$ son module dual sur $\mathscr{H}^\dagger(A)$, qui s'identifie à $F^{-1}\mathscr{H}^\dagger(A)$. On a vu (*cf.* 1) que $\mathscr{M}$ d'identifie à $\mathscr{H}^\dagger(A)$ muni de la différentiation

$$\partial_F = t\frac{\mathrm{d}}{\mathrm{d}t} + \pi t f'(t) + \frac{e}{1-q}.$$

De la même façon, $\mathscr{M}^*$ s'identifie à $\mathscr{H}^\dagger(A)$ muni de la différentiation

$$\partial_{F^{-1}} = t\frac{\mathrm{d}}{\mathrm{d}t} - \pi t f'(t) - \frac{e}{1-q}.$$

Si maintenant $\widehat{\mathscr{M}} := \mathscr{M} \otimes_{\mathscr{H}^\dagger(A)} \mathscr{R}'(A)$, on peut identifier $(\widehat{\mathscr{M}})^*$, le dual du $\mathscr{R}'(A)$-module $\widehat{\mathscr{M}}$, avec $\widehat{(\mathscr{M}^*)} = \mathscr{M}^* \otimes_{\mathscr{H}^\dagger(A)} \mathscr{R}'(A)$, et on notera simplement ce module $\widehat{\mathscr{M}^*}$. La dualité est définie par la forme bilinéaire (sur $\mathscr{R}'(A)$)

$$\forall u \in \widehat{\mathscr{M}}, u^* \in \widehat{\mathscr{M}^*},\ \langle u, u^*\rangle = uu^*.$$

En combinant les deux formes bilinéaires qu'on vient de décrire, on peut définir une nouvelle forme bilinéaire (sur $\mathbb{C}_p$) $(\cdot|\cdot)$ sur $\widehat{\mathscr{M}} \times \widehat{\mathscr{M}^*}\frac{\mathrm{d}t}{t}$ par

$$(u|u^*\frac{\mathrm{d}t}{t}) = \int \langle u, u^*\rangle \frac{\mathrm{d}t}{t} = \int uu^*\frac{\mathrm{d}t}{t}.$$

On en déduit une dualité entre $\widehat{\mathscr{M}}$ et $\widehat{\mathscr{M}^*}\frac{\mathrm{d}t}{t}$, dans laquelle le dual de $\mathscr{M}$ est le quotient $\widehat{\mathscr{M}^*}\frac{\mathrm{d}t}{t}/\mathscr{M}^*\frac{\mathrm{d}t}{t}$. De même on a une dualité (sur $\mathbb{C}_p$) entre $\widehat{\mathscr{M}^*}$ et $\widehat{\mathscr{M}}\frac{\mathrm{d}t}{t}$, dans laquelle le dual de $\mathscr{M}\frac{\mathrm{d}t}{t}$ est $\widehat{\mathscr{M}^*}/\mathscr{M}^*$.

Revenons aux anneaux $\mathscr{H}^\dagger(A)$ et $\mathscr{R}'(A)$. La transposée de la différentiation $\partial_F : \mathscr{R}'(A) \to \mathscr{R}'(A)\frac{\mathrm{d}t}{t}$ est la différentiation $-\partial_{F^{-1}} : \mathscr{R}'(A) \to \mathscr{R}'(A)\frac{\mathrm{d}t}{t}$, et puisque $\partial_{F^{-1}}$ envoie $\mathscr{H}^\dagger(A)$ dans $\mathscr{H}^\dagger(A)\frac{\mathrm{d}t}{t}$, on obtient par passage au quotient une application

$$\overline{\partial}_{F^{-1}} : \mathscr{R}'(A)/\mathscr{H}^\dagger(A) \to \mathscr{R}'(A)\frac{\mathrm{d}t}{t}/\mathscr{H}^\dagger(A)\frac{\mathrm{d}t}{t}.$$

En conséquence l'application $-\overline{\partial}_{F^{-1}}$ est la transposée de $\partial_F : \mathscr{H}^\dagger(A) \to \mathscr{H}^\dagger(A)\frac{\mathrm{d}t}{t}$.

Puisque $H^1_F = \mathscr{H}^\dagger(A)\frac{\mathrm{d}t}{t}/\partial_F\mathscr{H}^\dagger(A)$ est de dimension finie, son dual s'identifie au noyau K de $\overline{\partial}_{F^{-1}}$. D'autre part, l'application $\overline{\partial}_{F^{-1}}$ induit un morphisme $\delta : K \to H^1_{F^{-1}}$, et on a la suite exacte

$$0 \to \mathrm{Ker}_{\mathscr{H}^\dagger(A)}\partial_{F^{-1}} \to \mathrm{Ker}_{\mathscr{R}'(A)}\partial_{F^{-1}} \to \mathrm{Ker}\ \delta \to 0.$$

Comme F^{-1} n'est ni dans $\mathscr{H}^\dagger(A)$, ni dans $\mathscr{R}'(A)$, l'opérateur $\partial_{F^{-1}}$ est injectif sur ces deux espaces, et δ est lui aussi injectif. Mais puisque $H^1_{F^{-1}}$ et H^1_F sont de même dimension, et que ce dernier espace est le dual de K, l'application δ est un isomorphisme.

On a donc démontré

Lemme 1.1. *Via l'isomorphisme δ, le dual de l'espace H^1_F pour la forme bilinéaire $(\cdot|\cdot)$ est l'espace $H^1_{F^{-1}}$.*

2. Action de Frobenius

Dans ce chapitre, on va déterminer l'adjoint de l'opérateur de Dwork $\overline{\alpha}$ pour la forme bilinéaire $(\cdot|\cdot)$. On se restreindra ensuite aux cas qui nous intéressent ; on va définir sur l'espace H^1_F une forme bilinéaire symétrique $\langle\cdot|\cdot\rangle$ dont on va démontrer qu'elle est symétrique ou alternée suivant que la somme est tordue ou non par le caractère quadratique. Finalement on en déduira que l'opérateur $\overline{\alpha}$ est une similitude dans le premier cas, une similitude symplectique dans le second. On va ainsi retrouver, à l'aide des outils p-adiques, certains des résultats de [**33**, Chapter 7].

2.1. L'opérateur de Frobenius, adjoint de $\overline{\alpha}$. On sait définir sur les espaces de fonctions définis au chapitre précédent une application ϕ_q, étendant par linéarité l'application $x^n \mapsto x^{qn}$. En particulier on remarque que $\psi_q \circ \phi_q = Id$, ψ_q est un inverse à gauche de ϕ_q. L'application ϕ_q (*resp.* ψ_q) est appelée "application de Frobenius" (*resp.* "de Dwork") par Robba. On a de plus les règles de commutation suivantes avec la différentiation extérieure $t\frac{\mathrm{d}t}{t}$

$$qt\frac{\mathrm{d}t}{t} \circ \psi_q = \psi_q \circ t\frac{\mathrm{d}t}{t} \ ; \ t\frac{\mathrm{d}t}{t} \circ \phi_q = q\phi_q \circ t\frac{\mathrm{d}t}{t}.$$

L'action de ψ_q s'étend à une application du module différentiel $\mathscr{M} = F(t)\mathscr{H}^\dagger(A)$ dans le module différentiel $\mathscr{M}^s = F(t^q)\mathscr{H}^\dagger(A)$. Mais la série $H(t) := F(t)/F(t^q)$ est surconvergente, et les deux modules différentiels sont isomorphes. Via cet isomorphisme, l'application ϕ_q (*resp.* ψ_q) sur $\mathscr{M}$ induit l'application $\beta := H^{-1} \circ \phi_q$ (*resp.* $\alpha := \psi_q \circ H$) sur $\mathscr{H}^\dagger(A)$. Comme plus haut, β est un inverse à gauche de α, et ces applications commutent à la différentiation extérieure ∂_F de la façon suivante

$$q\partial_F \circ \alpha = \alpha \circ \partial_F \ ; \ \partial_F \circ \beta = q\beta \circ \partial_F.$$

On en déduit un nouveau diagramme commutatif qui montre que l'application β passe au quotient, pour donner un endomorphisme $\overline{\beta}$ de H^1_F

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{H}^\dagger(A) & \xrightarrow{\partial_F} & \mathscr{H}^\dagger(A) & \longrightarrow & H^1_F & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle q\beta} & & \downarrow{\scriptstyle \overline{\beta}} & & \\ 0 & \longrightarrow & \mathscr{H}^\dagger(A) & \xrightarrow{\partial_F} & \mathscr{H}^\dagger(A) & \longrightarrow & H^1_F & \longrightarrow & 0 \end{array}$$

En conséquence, comme on le voit en "composant" le diagramme ci-dessus avec le précédent, on a

Lemme 2.1. *Les endomorphismes $\overline{\alpha}$ et $\overline{\beta}$ de l'espace de cohomologie de de Rham H^1_F vérifient $\overline{\alpha} \circ \overline{\beta} = qId$.*

Notons α^* et β^* les applications définies comme plus haut sur $\mathscr{H}^\dagger(A)$, mais provenant du module différentiel dual $\mathscr{M}^*$. On les étend à $\mathscr{R}'(A)$. Elles passent au quotient $\widehat{\mathscr{M}^*}/\mathscr{M}^*$, et laissent K, le noyau de $\overline{\partial}_{F^{-1}}$, stable d'après les formules de commutation ci dessus. Alors la transposée de $\overline{\alpha}$ (*resp.* $\overline{\beta}$) pour la forme bilinéaire $(\cdot|\cdot)$ est $\beta^*_{|K}$ (*resp.* $\alpha^*_{|K}$). D'autre part les diagrammes

$$\begin{array}{ccc} K & \xrightarrow{\delta} & H^1_{F^{-1}} \\ {\scriptstyle \alpha^*_{|K}}\downarrow & & \downarrow{\scriptstyle \overline{\alpha^*}} \\ K & \xrightarrow{\delta} & H^1_{F^{-1}} \end{array} \qquad \text{et} \qquad \begin{array}{ccc} K & \xrightarrow{\delta} & H^1_{F^{-1}} \\ {\scriptstyle \beta^*_{|K}}\downarrow & & \downarrow{\scriptstyle \overline{\beta^*}} \\ K & \xrightarrow{\delta} & H^1_{F^{-1}} \end{array}$$

sont commutatifs.

Nous résumons ces résultats dans une proposition (à l'aide du lemme 1.1, on identifie le dual de H^1_F à $H^1_{F^{-1}}$)

Proposition 2.1. *La transposée (pour la forme bilinéaire $(\cdot|\cdot)$) de l'endomorphisme $\overline{\alpha}$ de H^1_F est l'endomorphisme $\overline{\beta^*}$ de $H^1_{F^{-1}}$.*

De même, la transposée de l'endomorphisme $\overline{\beta}$ de H^1_F est l'endomorphisme $\overline{\alpha^*}$ de $H^1_{F^{-1}}$.

2.2. Une nouvelle forme bilinéaire sur H^1_F. Dans toute la suite de ce chapitre on se place dans l'un des cas suivants

(1) *Cas i/* f est un polynôme impair, et $e = \frac{q-1}{2}$;
(2) *Cas ii/* f est un polynôme impair, et $e = 0$.

On définit l'application $\theta : \mathscr{H}^\dagger(A) \to \mathscr{H}^\dagger(A)$ par

(1) $\eta(t^n) = (-1)^n t^{n-1}$ dans le cas *i/*;
(2) $\eta(t^n) = (-1)^n t^n$ dans le cas *ii/*.

On a donc obtenu un isomorphisme de $\mathscr{H}^\dagger(A)$, qu'on peut encore décrire par $\eta(u(t)) = \frac{u(-t)}{t}$ dans le cas (1), et $\eta(u(t)) = u(-t)$ dans le cas (2). Il s'étend à un isomorphisme $\widehat{\eta} : \mathscr{R}'(A) \to \mathscr{R}'(A)$ dans les deux cas. Un calcul facile montre qu'il commute aux différentiations $\partial_{F^{-1}}$ et ∂_F. En d'autres termes, il provient d'un isomorphisme entre le module différentiel $\mathscr{M}$ et son dual $\mathscr{M}^*$.

Lemme 2.2. *On a les relations $\partial_{F^{-1}} \circ \eta = \eta \circ \partial_F$ et $\partial_{F^{-1}} \circ \widehat{\eta} = \widehat{\eta} \circ \partial_F$. En conséquence de la première, l'isomorphisme η induit un isomorphisme $\overline{\eta}$ de H^1_F sur $H^1_{F^{-1}}$.*

On utilise $\overline{\eta}$ pour définir une nouvelle forme bilinéaire sur H^1_F

Définition 2.1. *On définit sur $H^1_F \times H^1_F$ la forme bilinéaire non dégénérée*

$$\begin{array}{rccc} \langle\cdot|\cdot\rangle & : & H^1_F \times H^1_F & \to & \mathbb{C}_p \\ & & (\overline{u}, \overline{v}) & \mapsto & (\overline{u}|\overline{\eta}(\overline{v}))\,. \end{array}$$

L'objet de ce paragraphe est de démontrer

Lemme 2.3. *La forme bilinéaire non dégénérée $\langle\cdot|\cdot\rangle$ est symétrique dans le cas* (1)*, et alternée dans le cas* (2)*.*

Démonstration. Revenons à la définition de la forme bilinéaire. Si $\overline{u}$ et $\overline{v}$ sont dans H^1_F, soit $u \in \mathscr{H}^\dagger(A)$ un relèvement de $\overline{u}$, u' un élément de K tel que $\delta(u') = \overline{\eta}(\overline{u})$, et $\widehat{u}$ un relèvement de u' à $\mathscr{R}'(A)$. On définit de même $v, v', \widehat{v}$ à partir de $\overline{v}$. Par définition de la forme bilinéaire, on a

$$\langle\overline{u}|\overline{v}\rangle = \int u\widehat{v}\frac{\mathrm{d}t}{t}\ ;\ \langle\overline{v}|\overline{u}\rangle = \int v\widehat{u}\frac{\mathrm{d}t}{t}.$$

Par construction de δ, on a $\partial_{F^{-1}}\widehat{v} \equiv \eta(v) \mod \mathscr{H}^\dagger(A)$, et $\langle\overline{v}|\overline{u}\rangle = \int \eta^{-1}(\partial_{F^{-1}}\widehat{v})\widehat{u}\frac{\mathrm{d}t}{t}$. Puisque $\partial_{F^{-1}} \circ \widehat{\eta} = \widehat{\eta} \circ \partial_F$, on en déduit que $\langle\overline{v}|\overline{u}\rangle = \int \partial_F(\eta^{-1}\widehat{v})\widehat{u}\frac{\mathrm{d}t}{t}$. Mais on a vu que l'adjoint de ∂_F est $-\partial_{F^{-1}}$, et on obtient $\langle\overline{v}|\overline{u}\rangle = -\int \eta^{-1}(\widehat{v})\partial_{F^{-1}}\widehat{u}\frac{\mathrm{d}t}{t}$. Finalement on a $\partial_{F^{-1}}\widehat{u} \equiv \eta(u) \mod \mathscr{H}^\dagger(A)$, et on trouve

$$\langle\overline{v}|\overline{u}\rangle = -\int \eta^{-1}(\widehat{v})\eta(u)\frac{\mathrm{d}t}{t} = \begin{cases} \int u(-t)\widehat{v}(-t)\frac{\mathrm{d}t}{t} & \text{dans le cas (1)} \\ -\int u(-t)\widehat{v}(-t)\frac{\mathrm{d}t}{t} & \text{dans le cas (2)} \end{cases}$$

la dernière égalité provenant de la définition de η. Il reste à remarquer que d'après la définition de $\int a\frac{\mathrm{d}t}{t}$ à l'aide des coefficients constants de a_0 et a_∞, ce nombre est inchangé en remplaçant a par $a(-t)$.

□

2.3. Action de $\overline{\alpha}$ sur la forme bilinéaire. Commençons par montrer que α commute avec l'isomorphisme η. C'est encore une conséquence du fait que η provient d'un isomorphisme entre le module différentiel $\mathscr{M}$ et son dual $\mathscr{M}^*$.

Lemme 2.4. *On a les relations suivantes :*

(1) $\eta \circ \alpha = (-1)^{\frac{q-1}{2}}\alpha^* \circ \eta$ *dans le cas* (1)*;*

(2) $\eta \circ \alpha = \alpha^* \circ \eta$ *dans le cas* (2)*.*

En particulier, quand on passe au quotient, on a le diagramme commutatif suivant

$$\begin{array}{ccc} H^1_F & \xrightarrow{\overline{\alpha}} & H^1_F \\ \overline{\eta}\downarrow & & \downarrow\overline{\eta} \\ H^1_{F^{-1}} & \xrightarrow{\varepsilon\overline{\alpha^*}} & H^1_{F^{-1}} \end{array}$$

où $\varepsilon = (-1)^{\frac{q-1}{2}}$ dans le cas (1) *et $\varepsilon = 1$ dans le cas* (2)*.*

Démonstration. Montrons la relation dans le cas (1), la démonstration dans le cas (2) est semblable. Comme plus haut, on note $H(t) = \sum_{i\in\mathbb{Z}} h_i t^i$; d'une part on a

$$\eta(\alpha(t^n)) = \eta\left(\sum_{i\in\mathbb{Z}} h_{qi-n-\frac{q-1}{2}}t^i\right) = \sum_{i\in\mathbb{Z}}(-1)^{i+1}h_{qi-n+\frac{q-1}{2}+1}t^i.$$

D'autre part

$$\alpha^*(\eta(t^n)) = (-1)^n \alpha^*(t^{n-1}) = (-1)^n \sum_{i\in\mathbb{Z}} (-1)^{qi+1-n+\frac{q-1}{2}} h_{qi-n+\frac{q-1}{2}+1} t^i,$$

et le résultat provient du fait que q étant impair, on a $(-1)^{qi} = (-1)^i$. □

On peut résumer les résultats précédents en disant que $\overline{\alpha}$ est une similitude pour la forme bilinéaire $\langle\cdot|\cdot\rangle$.

Théorème 2.1. *L'endomorphisme $\overline{\alpha}$ de H_F^1 est une similitude (orthogonale dans le cas* (1)*, symplectique dans le cas* (2)*) de multiplicateur εq, où $\varepsilon = (-1)^{\frac{q-1}{2}}$ dans le cas* (1) *et $\varepsilon = 1$ dans le cas* (2)*.*

Démonstration. C'est une conséquence des différents résultats qu'on vient de présenter. On a en effet la suite d'égalités :

$$\begin{array}{rcll} \langle\overline{\alpha}(\overline{u})|\overline{\alpha}(\overline{v})\rangle & = & (\overline{\alpha}(\overline{u})|\overline{\eta\alpha}(\overline{v})) & \text{(Définition 2.1)} \\ & = & \varepsilon\left(\overline{\alpha}(\overline{u})|\overline{\alpha^*\eta}(\overline{v})\right) & \text{(Lemme 2.4)} \\ & = & \varepsilon\left(\overline{\beta\alpha}(\overline{u})|\overline{\eta}(\overline{v})\right) & \text{(Proposition 2.1)} \\ & = & \varepsilon q\left(\overline{u}|\overline{\eta}(\overline{v})\right) & \text{(Lemme 2.1)} \\ & = & \varepsilon q\langle\overline{u}|\overline{v}\rangle & \text{(Définition 2.1)} \end{array}$$

qui donne le résultat recherché. □

Corollaire 2.1. *Rappelons qu'on note $\mathscr{G}_q$ la somme de Gauss quadratique sur k. L'endomorphisme A de H_F^1 défini par*

$$A = \begin{cases} \frac{1}{\mathscr{G}_q}\overline{\alpha} & (\textit{dans le cas (1)}) \\ q^{-\frac{1}{2}}\overline{\alpha} & (\textit{dans le cas (2)}) \end{cases}$$

est orthogonal dans le cas (1)*, symplectique dans le cas* (2)*.*

3. Calcul du déterminant et applications

On va montrer dans cette section les majorations de sommes de caractères qu'on a annoncées dans l'introduction. Dans un premier temps, on va calculer (partiellement) la variation de la cohomologie de façon à montrer que le déterminant de la matrice de l'application $\overline{\alpha}$ est constant dans une certaine famille. On l'estimera précisément à l'aide de la méthode de Davenport-Hasse. Puis on conclura à l'aide des résultats obtenus tout au long de ce chapitre.

3.1. Variation de la cohomologie. Dans ce chapitre, on va étudier la variation des applications décrites précédemment quand le polynôme f décrit une famille à un paramètre. Plus précisément, si $f(t) = \sum_{-d_0}^{d_\infty} a_i t^i$, et $\widetilde{f}(t) = \sum_{-d_0}^{d_\infty} \widetilde{a}_i t^i$ est son relèvement de Teichmüller, on va poser pour $x \in \mathbb{C}_p$, $\widetilde{f}_x = \widetilde{a}_{-d_0} t^{-d_0} + x\left(\sum_{-d_0+1}^{d_\infty-1} \widetilde{a}_i t^i\right) + \widetilde{a}_{d_\infty} t^{d_\infty}$ (notons que $f_1 = \widetilde{f}$). On note encore F_x, α_x et $\beta_x, \ldots$ les objets décrits plus haut, dont on veut souligner la dépendance en le paramètre x.

D'autre part, on note $\mathscr{H}$ l'anneau des fonctions analytiques en les variables x et t sur une couronne $r < |t| < \frac{1}{r}$, $|x| < \frac{1}{r}$ ($0 < r < 1$ quelconque), et $\mathscr{K}$ l'anneau des fonctions analytiques sur une boule $|x| < \frac{1}{r}$ en la variable x.

On reprend ici l'exposition de [**56**].

On a une suite exacte (où on note maintenant ∂_t l'application ∂_F pour exprimer que c'est une différentiation par rapport à t)

$$0 \longrightarrow \mathscr{H} \xrightarrow{\partial_t} \mathscr{H} \longrightarrow W \longrightarrow 0$$

et W est un $\mathscr{K}$-module libre de rang $d_0 + d_\infty$. On choisit désormais de travailler dans la base suivante

$$\left(u_i := \left[t^i\right]\right)_{-d_0 \le i \le d_\infty - 1}.$$

La dérivation $\frac{\partial}{\partial x}$ agit sur $F\mathscr{H}$ via $\frac{\partial}{\partial x}(uF) = \left(\frac{\partial u}{\partial x} + \frac{u}{F}\frac{\partial F}{\partial x}\right)F$. On notera ∂_x l'application $u \mapsto \frac{\partial u}{\partial x} + \frac{u}{F}\frac{\partial F}{\partial x}$ induite sur $\mathscr{H}$. Alors ∂_x commute avec ∂_t et passe au quotient, faisant de W un $\mathscr{K}$-module différentiel.

On va expliciter la connexion ∇, c'est à dire la matrice de $\frac{\partial}{\partial x}$ dans la base (u_i). D'après la description de ∂_x, on obtient

$$\partial_x t^i = \frac{t^i}{F}\frac{\partial F}{\partial x} = \sum_{j=-d_0+1}^{d_\infty-1} \widetilde{a}_j t^{i+j},$$

et en passant à W, si on note pour tout $i \in \mathbb{Z}$, $[t^i] = \sum_{-d_0 \le i \le d_\infty - 1} b_{ik}(x)[t^k]$, où $b_{ik}(x) \in \mathscr{K}$ (c'est un polynôme en x), on trouve

$$\partial_x u_i = \sum_{k=-d_0}^{d_\infty-1} \left(\sum_{j=-d_0+1}^{d_\infty-1} \widetilde{a}_j b_{i+j,k}(x) \right) u_k, \tag{7}$$

et on remarque que cette application linéaire est induite par la multiplication par $\sum_{j=-d_0+1}^{d_\infty-1} \widetilde{a}_i t^i$ sur W.

Dans toute la suite, on note $G(x) \in \mathbf{M}_d(K[x])$ la matrice dont on vient de décrire les coefficients. On va donner un résultat qui nous sera utile un peu plus loin.

Lemme 3.1. *Supposons f impair. Alors la trace de G est nulle.*

Démonstration. Commençons par glaner quelques informations sur les b_{ik}. Soient $0 \le n < k \le d_\infty - 2$; on commence par remarquer que si $n \equiv k \mod 2$, alors $b_{d_\infty+n,k} = 0$. On sait que $b_{ik} = \delta_{ik}$ pour $-d_0 \le i, k \le d_\infty - 1$. D'autre part on a la relation suivante, obtenue en calculant $\partial_t(t^n)$

$$\left(n + \frac{e}{1-q}\right) b_{n,k} + d_\infty \widetilde{a}_{d_\infty} b_{d_\infty+n,k} - d_0 \widetilde{a}_{d_0} b_{d_0+n,k} + \pi x \sum_{i=-d_0+1}^{d_\infty-1} i\widehat{a}_i b_{i+n,k} = 0,$$

qui permet d'obtenir l'assertion par récurrence sur n.

Venons en aux coefficients de G. Supposons maintenant $0 < i \le d_\infty - 1$; le coefficient g_{ii} de la matrice G est donné, d'après (7), par

$$g_{ii} = \sum_{j=-d_0+1}^{d_\infty-1} \widetilde{a}_j b_{i+j,i}(x).$$

Il est clair que si $i + j \le d_\infty - 1$, le terme est nul (on ne peut avoir $i + j = i$ puisque j est impair par hypothèse). Si $i + j \ge d_\infty$, on peut réécrire ce terme $b_{d_\infty+k,i}$, avec $k = i + j - d_\infty < i$, et $k \equiv i \mod 2$, ce terme est encore nul d'après la remarque précédente.

On démontrerait de même que $g_{ii} = 0$ pour $-d_0 < i < 0$, et c'est évident pour $i = 0$. □

Considérons maintenant l'application $\overline{\alpha}_{1x}$, et notons $A(x)$ sa matrice dans la base décrite ci dessus. On vérifie (comme dans [**BF,**Section 2.1]) que les coefficients de $A(x)$ sont des éléments de $\mathscr{K}$, ce qui en fait un isomorphisme de $\mathscr{K}$-modules de $W(x)$ dans $W^\tau(x^p)$ (qui est le $\mathbb{C}_p$ espace vectoriel $W(x^p)$ muni de la multiplication externe $\lambda \cdot w = \lambda^\tau w$ pour tout $\lambda \in \mathbb{C}_p$). D'autre part $\overline{\alpha}_{1x}$ commute avec ∂_x, ce qui en fait un isomorphisme de $\mathscr{K}$-modules différentiels.

Fixons $x_0 \in \mathbb{C}_p$, $|x_0| \le 1$; pour tout x de $\mathbb{C}_p$, $|x - x_0| < 1$, soit $u(x_0, x)$ la multiplication par

$$\frac{F_x}{F_{x_0}} = \exp\left(\pi(x - x_0) \sum_{j=-d_0+1}^{d_\infty-1} \widetilde{a}_i t^i\right)$$

dans $\mathscr{H}$. On déduit de la décomposition formelle de ∂_{F_x} la commutation suivante

$$u(x_0, x) \circ \partial_{F_x} = \partial_{F_{x_0}} \circ u(x_0, x),$$

et l'application $u(x_0, x)$ induit une application linéaire de $H^1_{F_x}$ dans $H^1_{F_{x_0}}$, qu'on note $\overline{u}(x_0, x)$. Regardons ce qui se passe quand on fait varier x : on voit que $\partial_x \overline{u}(x_0, x)$ est la multiplication par $\sum_{j=-d_0+1}^{d_\infty-1} \widetilde{a}_i t^i \frac{F_x}{F_{x_0}}$. On

en déduit que la matrice de $\overline{u}(x_0,x)$ dans la base décrite plus haut est $U(x_0,x)$ la matrice de $\mathbf{M}_{d_0+d_\infty}(\mathscr{R}_{x_0})$ définie pour $|x-x_0|<1$ par

$$\frac{\mathrm{d}}{\mathrm{d}x}U(x_0,x)=G(x)U(x_0,x),\ U(x_0,x_0)=\mathbf{I}. \tag{8}$$

Enfin, on voit qu'en désignant par $u^\tau(x_0^p,x^p)$ la multiplication par $\frac{F_x^\tau}{F_{x_0}^\tau}$, on a la commutation $\overline{\alpha}_{1x_0}\circ\overline{u}(x_0,x)=\overline{u}^\tau(x_0^p,x^p)\circ\overline{\alpha}_{1x}$, ce qui donne en terme de matrices

$$U^\tau(x_0^p,x^p)A(x)=A(x_0)U(x_0,x),\ |x-x_0|<1. \tag{9}$$

Nous allons utiliser ces relations pour montrer le résultat suivant

Lemme 3.2. *Supposons que le polynôme f est impair. Alors la fonction (analytique sur un disque de la forme $|x|\leq\frac{1}{r}$, $0<r<1$) $x\mapsto\det A(x)$ est constante.*

Démonstration. On a vu au lemme 3.1 que la trace de G est nulle. D'après (8), le déterminant de U satisfait l'équation différentielle

$$\frac{\mathrm{d}}{\mathrm{d}x}\det U(x_0,x)=\mathrm{Tr}(G(x))\det U(x_0,x),$$

et il est constant, égal à 1, pour $|x-x_0|<1$. En prenant $x_0=0$ et en prenant les déterminants dans la relation (9), on voit que pour tout x, $|x|<1$, on a $\det A(x)=\det A(0)$. Mais la fonction $x\mapsto\det A(x)$ est dans $\mathscr{K}$, c'est à dire analytique sur une boule de la forme $|x|<\frac{1}{r}$; elle est donc constante sur cette boule, et c'est le résultat recherché. □

3.2. Estimation du déterminant : la méthode de Davenport-Hasse. On va calculer ici le déterminant de l'endomorphisme α_0, c'est à dire le coefficient de degré $d:=d_0+d_\infty$ de la fonction $L(f,\chi_2;T)$ à l'aide de la méthode de Davenport-Hasse. Commençons par en rappeler le principe. Ce paragraphe es très inspiré par la première section de [**35**].

Quand on développe l'expression de la fonction L ci dessus comme produit eulérien

$$L(f,\chi_2;T)=\prod_{\mathfrak{p}}\frac{1}{1-\chi_2(\mathfrak{p})\psi_{\deg\mathfrak{p}}(f(\mathfrak{p}))T^{\deg\mathfrak{p}}},$$

où le produit porte sur les idéaux premiers de $k[X]$ distincts de (X), ou ce qui revient au même sur les places de $\mathbb{G}_m$, on obtient l'expression suivante pour le coefficient de degré n

$$c_n=\sum_{\substack{h\in k[x]\text{unitaire}\\ \deg h=r,\ h(0)\neq 0}}\chi_2\left(\prod_{\text{racines de }h}\alpha\right)\psi\left(\sum_{\text{racines de }h}a\alpha^{d_\infty}+b\alpha^{-d_0}\right).$$

La méthode de Davenport-Hasse [**12**] consiste maintenant à calculer le coefficient de plus haut degré de la fonction L, c'est à dire c_d. Les arguments des caractères dans cette dernière expression sont des polynômes symétriques en les racines de h, et s'écrivent à l'aide des polynômes symétriques élémentaires, c'est à dire à l'aide des coefficients de h ; rappelons que si s_i, $1\leq i\leq d$ désigne le polynôme symétrique élémentaire de degré i en les variables $x_1,\dots,x_d$, alors on a pour un polynôme unitaire de degré d, $h(x)=x^d+\sum_{i=1}^d(-1)^i s_i x^{d-i}$. C'est très simple pour l'argument du caractère multiplicatif, qui est $(-1)^d s_d=s_d$, le coefficient constant de h. Pour celui du caractère additif, on fait appel aux polynômes de Newton définis par

$$N_k(s_1,\dots,s_d):=\sum_{\text{racines de }h}\alpha^k,\ k\in\mathbb{N}.$$

Pour $k<0$ un entier, on remarque que le polynôme unitaire dont les racines sont les inverses de celles de h est le polynôme $h^*(x)=\frac{(-1)^d}{s_d}x^dP\left(\frac{1}{x}\right)$, ce dont on déduit que le polynôme symétrique élémentaire de degré i en les $\frac{1}{x_1},\dots,\frac{1}{x_d}$ est $s_i^*=\frac{s_{d-i}}{s_d}$. On en déduit

$$N_{-k}\left(\frac{s_{d-1}}{s_d},\dots,\frac{1}{s_d}\right)=\sum_{\text{racines de }h}\alpha^k,\ k\in\mathbb{Z}\backslash\mathbb{N}.$$

A l'aide de ces notations, on sait réexprimer le coefficient c_d de la façon suivante :

$$c_d = \sum_{\substack{s_1,\dots,s_d \in k \\ s_d \neq 0}} \chi_2(s_d)\psi\left(aN_{d_\infty}(s_1,\dots,s_d) + bN_{d_0}\left(\frac{s_{d-1}}{s_d},\dots,\frac{1}{s_d}\right)\right). \tag{10}$$

On va calculer cette dernière somme, en utilisant des arguments de linéarité donnés par Katz [**35**, Corollary 2.5]. Posons $d_\infty := 2n_\infty + 1$ et $d_0 := 2n_0 + 1$. Alors en remarquant que le polynôme $N_{d_\infty}(s_1,\dots,s_d)$ est isobare de poids d_∞ (pour s_i de poids i), Katz montre qu'il est linéaire en les variables s_i, $n_\infty \leq i \leq 2n_\infty$, et que son seul monôme en s_{d_∞} est $(-1)^{d_\infty+1}d_\infty s_{d_\infty} = d_\infty s_{d_\infty}$. De même, le polynôme $N_{d_0}\left(\frac{s_{d-1}}{s_d},\dots,\frac{1}{s_d}\right)$ est linéaire en les $\frac{s_{d_\infty}}{s_d},\dots,\frac{s_{d_\infty+n_0}}{s_d}$ et son seul monôme en s_{d_∞} est $d_0\frac{s_{d_\infty}}{s_d}$. On peut donc écrire, pour P_i, R des polynômes en les variables $s_1,\dots,s_{n_\infty},s_{d_\infty+n_0+1},\dots,s_d$, et Q_i, S des fractions rationnelles en ces mêmes variables de dénominateur une puissance de s_d

$$N_{d_\infty}(s_1,\dots,s_d) = \sum_{i=n_\infty}^{2n_\infty} s_iP_i(s_j) + R(s_j)\ ;\ N_{d_0}\left(\frac{s_{d-1}}{s_d},\dots,\frac{1}{s_d}\right) = \sum_{i=d_\infty}^{d_\infty+n_0} s_iQ_i(s_j) + S(s_j).$$

On sait maintenant réécrire la somme (10) de la façon suivante

$$c_d = \sum_{\substack{s_1,\dots,s_{n_\infty}, \\ s_{d_\infty+n_0+1},\dots,s_d \in k, s_d\neq 0}} \chi_2(s_d)\psi\left(R(s_j)+S(s_j)\right) \sum_{s_{n_\infty+1},\dots,s_{d_\infty+n_0}} \psi\left(s_iP_i(s_j)+s_iQ_i(s_j)\right).$$

De plus le coefficient de s_{d_∞} est $ad_\infty + b\frac{d_0}{s_d}$, et on vérifie comme Katz que la somme interne est non nulle exactement quand ce terme est nul (soit pour $s_d = -\frac{bd_0}{ad_\infty}$), ainsi que les $s_1,\dots,s_{n_\infty},s_{d_\infty+n_0+1},\dots,s_{d-1}$; alors cette somme vaut $q^{n_0+n_\infty+1} = q^{\frac{d}{2}}$, c'est à dire que $c_d = \chi_2(-\frac{bd_0}{ad_\infty})q^{\frac{d}{2}} = \chi_2(-abd_0d_\infty)q^{\frac{d}{2}}$.

En résumé on a obtenu le résultat suivant (on reprend les notations du chapitre précédent)

Proposition 3.1. *Pour tout x de $\mathbb{C}_p$, on a*

$$\det \overline{\alpha}_x = \chi_2(-abd_0d_\infty)q^{\frac{d}{2}}.$$

3.3. Amélioration de la borne de Weil. Le résultat qui suit est une conséquence du fait que dans le groupe orthogonal en un nombre pair de variables, un élément de déterminant -1 possède simultanément 1 et -1 comme valeurs propres. En conséquence la trace d'une telle matrice $d \times d$ est plus petite que $d-2$. Puisque la somme de caractères qui nous intéresse est la trace du Frobenius, on obtient donc

Théorème 3.1. *Soit $f(t) = \sum_{-d_0}^{d_\infty} a_it^i$ un polynôme de Laurent impair. Si χ_2 désigne le caractère quadratique de $k^\times$, et si $\chi_2(-abd_0d_\infty) = -1$, on a la majoration*

$$\left|\sum_{x\in k^\times} \psi(f(x))\chi_2(x)\right| \leq (d-2)\sqrt{q}.$$

Corollaire 3.1. *Soit f comme ci-dessus. Le nombre N de points rationnels de la courbe d'Artin Schreier d'équation $y^p - y = f(x^2)$ vérifie*

$$|N-(q+1)| \leq (p-1)\left(2(d_0+d_\infty)-1\right)\sqrt{q}.$$

Démonstration. Il est clair par la formule de Poisson, et par des résultats classiques sur les courbes d'Artin-Schreier [**9**, Section VI] que le numérateur de la fonction zêta de la courbe ci-dessus est le produit des normes (de $\mathbb{Q}(\zeta_p)$ sur $\mathbb{Q}$) des fonctions $L(f;T)$ et $L(f,\chi_2;T)$ associées aux différents caractères additifs de k. Il suffit maintenant d'appliquer les résultats précédents au second membre. □

4. Conclusion et questions

Il serait intéressant de rechercher des résultats d'équidistribution comme dans [**35**], pour obtenir des majorations en moyenne des sommes considérées plus haut.

Un autre objectif est de chercher des propriétés des fonctions L associées aux puissances symétriques des cristaux associés à une famille de sommes exponentielles (indexée par $\mathbb{A}^1$) comme dans [**56**] ou dans [**24**]. Malheureusement l'équation différentielle régissant la cohomologie est beaucoup moins classique que dans les cas considérés dans les travaux qu'on vient de citer.

Mentionnons finalement la construction de graphes de Ramanujan à l'aide de petites sommes considérées plus haut (par exemple pour $d_0 = 1,\ d_\infty = 3$).

CHAPITRE 6

p-densité et applications

L'objet de cette partie est d'étudier la valuation p-adique des sommes exponentielles sur un corps fini de caractéristique p. Un résultat classique dans ce domaine est le théorème de Stickelberger sur la valuation p-adique des sommes de Gauss [**63**]. En général, cette question est intimement liée à celle de l'existence de points sur des variétés algébriques définies sur un corps fini, plus précisément à la divisibilité par la caractéristique de ce nombre de points. La première question de ce type, posée par E. Artin, a été résolue par Chevalley, puis précisée par Warning [**67**], qui a obtenu ce qu'on appelle aujourd'hui le théorème de Chevalley-Warning. Pendant les années 60, l'émergence des idées de Dwork a permis des améliorations de ce résultat, d'abord par Ax [**7**], puis par Katz [**29**]. Les deux ont déduit leurs résultats d'une minoration convenable de la valuation p-adique des sommes d'exponentielles, et leurs bornes ne dépendent que des degrés des polynômes dont l'annulation définit la variété algébrique. Plus récemment, Adolphson et Sperber ont précisé ces résultats, en considérant un polyèdre de Newton, qui permet de cerner plus finement les monômes apparaissant dans les polynômes [**1**].

Toutes ces bornes sont indépendantes du premier p, et chacune est optimale dans le sens suivant : si on choisit un degré (resp. un polyèdre de Newton), alors pour chaque premier p on peut trouver un polynôme tel que la valuation de la somme exponentielle associée à ce polynôme soit égale à la borne.

Dans les années 90, Moreno et Moreno ont pris le premier p en compte. En utilisant une méthode de réduction au sous-corps premier, ils sont capables de remplacer les degrés des polynômes par leurs poids en base p (la somme des chiffres de l'écriture en base p), ce qui donne une nouvelle borne, qui améliore les précédentes dans certains cas [**52**]. Récemment, dans un travail commun avec Castro, Kumar et Shum, O. Moreno a réduit le problème de l'estimation de la valuation p-adique d'une somme exponentielle à celui d'estimer le poids en base p minimal des solutions d'un système d'équations modulaires [**53**]. Ici encore la borne est optimale, en un sens encore plus fort : c'est la première qui ne prend en compte que les monômes apparaissant effectivement dans le polynôme. Quand on fixe un degré ou un polyèdre de Newton, on considère un convexe qui peut contenir bien d'autres exposants que ceux d'origine.

Soyons plus précis : pour un premier p, et l'une de ses puissances q, soit $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ un polynôme ; notons D l'ensemble des exposants (dans $\mathbb{N}^r$) des monomes de f. Le système introduit par Moreno et al. pour donner une borne pour la valuation p-adique de la somme associée à f sur $\mathbb{F}_q$ est formé d'équations modulo $q-1$, dont les coefficients sont les éléments de D. Moreno et al. donnent dans certains cas des minorations pour le poids en base p d'une solution, ce qui suffit à donner des améliorations des résultats déjà connus.

On va définir la p-densité d'un sous-ensemble fini D de $\mathbb{N}^r$. C'est un minorant pour les poids en base p des solutions du système de Moreno et al., qui dépend seulement du premier p et de l'ensemble D. Il est optimal en ce sens qu'il existe un nombre infini de puissances q de p tels qu'il soit atteint pour le module $q-1$. En conséquence il permet de donner une borne uniforme (elle ne dépend que de p et D) de la valuation. On sait aussi borner la première puissance pour laquelle il est atteint.

Au delà des théorèmes de type Chevalley-Warning, les minorations de la valuation p-adique des sommes exponentielles ont de nombreuses applications. Dans cet article on détermine la première pente générique (des polygones de Newton des numérateurs des fonctions zêta) de certaines familles de courbes d'Artin-Schreier. Rappelons que ce sont les courbes définies sur $\mathbb{F}_q$, possédant une équation affine de la forme

$$y^p - y = f(x),\ f \in \mathbb{F}_q[x],$$

i.e. des revêtements cycliques d'ordre p de la droite projective, ramifiés seulement à l'infini. On montre que quand f parcourt l'espace des polynômes unitaires dont les exposants sont dans $D \subset \mathbb{N}$, alors la première pente du polygone de Newton générique est exactement la p-densité de D. Par exemple, on

peut ainsi montrer très rapidement que certaines familles de courbes d'Artin-Schreier de petit genre sont supersingulières.

En un sens, ces résultats sont une généralisation du théorème de Stickelberger : quand D contient un seul entier d, la p-densité est la valuation minimale d'une somme de Gauss sur une extension de $\mathbb{F}_p$, associée à un caractère multiplicatif d'ordre divisant d. Cela rejoint le résultat sur les courbes d'Artin-Schreier, puisque pour un tel D on considère seulement la coubre d'équation $y^p - y = x^d$, et que les racines réciproques du numérateur de sa fonction zêta s'expriment à l'aide des sommes de Gauss dont on vient de parler.

Ces bornes ont encore bien d'autres applications, à des problèmes mathématiques classiques comme le problème de Waring ou les bornes de Serre Weil, mais aussi en théorie mathématique de l'information, où elles sont utilisées pour l'estimation de certains invariants des codes, des fonctions booléennes...

Ce travail est organisé de la manière suivante : dans la première section on définit la p-densité d'un sous ensemble fini $D \subset \mathbb{N}^r$, on donne certaines de ses propriétés, et on montre qu'elle améliore la borne d'Adolphson et Sperber. On en déduit à la section 2 le résultat principal sur la valuation des sommes exponentielles, et un théorème à la Chevalley-Warning-Ax-Katz. Dans la dernière section, on lie la première pente générique des familles de courbes d'Artin-Schreier à la p-densité.

1. p-densité

Dans cette section, on fixe un premier p, et un sous ensemble fini et non vide de $\mathbb{N}^r\backslash\{0,\dots,0\}$, $D = \{\mathbf{d}_i\}_{1\leq i\leq n}$, avec $\mathbf{d}_i = (d_{i1},\dots,d_{ir})$. On suppose que D n'est contenu dans aucun des hyperplans $x_j = 0$ de $\mathbb{R}^d$, pour $1 \leq j \leq r$; ce cas se ramène immédiatement en dimension inférieure.

Pour n un entier naturel, on note $\sigma_p(n)$ le poids en base p de n : c'est à dire que si on a $n = n_0 + pn_1 + \cdots + p^t n_t$, avec $0 \leq n_i \leq p-1$, le poids est donné par $\sigma_p(n) = n_0 + \cdots + n_t$.

1.1. Equations modulaires et définition de la p-densité.

On commence par définir un certain nombre d'objets, et par donner certaines de leurs propriétés. Elles nous seront utiles dans la définition de la p-densité à la fin de la section.

Définition 1.1. *Soit D comme ci dessus, et $m > 0$ un entier.*

i/ On note $E_D(m)$ l'ensemble des n-uplets $U = (u_1,\dots,u_n) \in \{0,\dots,p^m-1\}^n\backslash\{0,\dots,0\}$ vérifiant les équations modulaires

$$\sum_{i=1}^{n} u_i \mathbf{d}_i \equiv 0 \ [p^m-1],\ \sum_{i=1}^{n} u_i d_{ij} > 0,\ \text{pour tout } 1 \leq j \leq r.$$

Pour $U \in E_D(m)$, le poids en base p de U *est l'entier $\sigma_p(U) := \sum_{i=1}^n \sigma_p(u_i)$, et la* longueur de U *est $\ell(U) := m$.*

ii/ On pose $\sigma_p(D,m) := \min_{U\in E_D(m)} \sigma_p(U)$.

*iii/ Soit δ_m le m-*décalage*, de l'ensemble $\{0,\dots,p^m-1\}$ dans lui-même, qui envoie un entier $0 \leq n \leq p^m-2$ sur le reste de la division euclidienne de pn par p^m-1, et p^m-1 sur lui-même. On l'étend, coordonnée par coordonnée, à l'ensemble $\{0,\dots,p^m-1\}^n$.*

iv/ Définissons une application

$$\begin{array}{rccc} \varphi & : & E_D(m) & \to & \mathbb{N}^r \\ & & U & \mapsto & \frac{1}{p^m-1}\sum_{i=1}^n u_i \mathbf{d}_i \end{array}$$

v/ Pour tout $U \in E_D(m)$, on pose $\Phi(U) := \{\varphi(\delta_m^k(U)),\ 0,\leq k \leq m-1\}$.

Remarque 1.1. *i/ L'ensemble $E_D(m)$ étant fini, le nombre $\sigma_p(D,m)$ est bien défini.*

ii/ L'application δ_m décale les chiffres de l'écriture en base p de l'entier n, son nom vient de là. En conséquence, elle préserve le poids en base p. D'autre part, on a la congruence $\delta(U) \equiv pU\ [p^m-1]$, et $\delta_m^m = Id$: la m-ième itérée de l'application δ_m est l'identité. Finalement, pour tout $n \in \{0,\dots,p^m-1\}$ on a l'égalité

$$\sum_{k=0}^{m-1} \delta_m^k(n) = \frac{p^m-1}{p-1}\sigma_p(n).$$

iii/ On suppose dans la suite que pour tout $1 \leq i \leq n$ le premier p ne divise pas $\mathbf{d}_i$. Cela ne change rien : si $\mathbf{d}_i = p\mathbf{d}'_i$, l'application qui envoie $U = (u_1, \ldots, u_i, \ldots, u_n)$ vers $U' = (u_1, \ldots, \delta_m(u_i), \ldots, u_n)$ est une bijection de $E_D(m)$ sur $E_{D'}(m)$, avec $D' = (\mathbf{d}_1, \ldots, \mathbf{d}'_i, \ldots, \mathbf{d}_n)$, qui préserve le poids.

iv/ On sera souvent amenés à travailler dans l'ensemble $\mathbb{N}^r$ (resp. $\mathbb{N}^n$) ; de façon à simplifier les notations, on considère ces ensembles comme des sous-ensembles du $\mathbb{Z}$-module $\mathbb{Z}^r$ (resp. $\mathbb{Z}^n$), et on utilise les lois usuelles de ces modules.

Commençons par donner quelques propriétés des objets que nous avons défini. Nous ne les prouvons pas puisqu'elles découlent immédiatement des définitions.

Lemme 1.1. *Soient D, m comme ci-dessus. Pour tout $1 \leq j \leq r$, soit $D_j = \sum_{i=1}^n d_{ij}$ le degré total de D sur sa j-ème coordonnée.*

i/ L'application δ envoie $E_D(m)$ sur lui même, en préservant le poids en base p.

ii/ Pour tout $U = (u_1, \ldots, u_n) \in \{0, \ldots, p^m - 1\}^n$, on a

$$\sum_{k=0}^{m-1} \delta_m^k(U) = \frac{p^m - 1}{p - 1}(\sigma_p(u_1), \ldots, \sigma_p(u_n)).$$

iii/ L'image de φ est contenue dans $\prod_{j=1}^r \{1, \ldots, D_j\}$.

Voici d'autres conséquences des définitions, que nous allons utiliser pour définir la p-densité de l'ensemble D.

Lemme 1.2. *Soient D, m comme ci-dessus, et $U = (u_1, \ldots, u_n) \in E_D(m)$. Soit $1 \leq t \leq m - 1$ un entier, et pour tout $1 \leq i \leq n$ écrivons $u_i = p^t w_i + v_i$, le résultat de la division euclidienne de u_i par p^t.*

i/ On a l'égalité

$$\sum_{i=1}^n \sigma_p(u_i)\mathbf{d}_i = (p-1)\sum_{k=0}^{m-1} \varphi(\delta_m^k(U)).$$

ii/ Pour t comme ci-dessus, on a :

$$\sum_{i=1}^n v_i\mathbf{d}_i = p^t\varphi(\delta_m^{-t}(U)) - \varphi(U) \ ; \ \sum_{i=1}^n w_i\mathbf{d}_i = p^{m-t}\varphi(U) - \varphi(\delta_m^{-t}(U)).$$

DÉMONSTRATION. L'assertion i/ est une conséquence directe des définitions : d'après le lemme 1.1 ii/, on a $\sum_{i=1}^n \sum_{k=0}^{m-1} \delta_m^k(u_i)\mathbf{d}_i = \frac{q-1}{p-1}\sum_{i=1}^n \sigma_p(u_i)\mathbf{d}_i$. D'autre part, $\sum_{i=1}^n \delta_m^k(u_i)\mathbf{d}_i = (q-1)\varphi(\delta_m^k(U))$ par la définition de l'application φ.

Montrons ii/. Pour chaque $1 \leq i \leq n$, notons $u_i = \sum_{k=0}^{m-1} u_{ik}p^k$, $0 \leq u_{ik} \leq p-1$, l'écriture en base p de u_i. Pour U comme ci-dessus, et $0 \leq k \leq m-1$, on pose $U_k := (u_{1k}, \ldots, u_{nk})$. Un calcul rapide montre que pour tout i on a $pu_i - \delta(u_i) = (q-1)u_{i,m-1}$, et

$$(q-1)\left(p\varphi(U) - \varphi(\delta_m(U))\right) = p\sum_{i=1}^n u_i\mathbf{d}_i - \sum_{i=1}^n \delta(u_i)\mathbf{d}_i = (q-1)\sum_{i=1}^n u_{i,m-1}\mathbf{d}_i.$$

En d'autres termes on a : $\sum_{i=1}^n u_{i,m-1}\mathbf{d}_i = p\varphi(U) - \varphi(\delta_m(U))$. Mais d'après la définition de w_i comme quotient d'une division euclidienne, on a $w_i = \sum_{k=t}^{m-1} u_{ik}p^{k-t}$. On obtient donc

$$\begin{array}{rcl} \sum_{i=1}^n w_i\mathbf{d}_i & = & \sum_{k=t}^{m-1} p^{k-t}\sum_{i=1}^n u_{ik}\mathbf{d}_i \\ & = & \sum_{k=t}^{m-1} p^{k-t}\left(p\varphi(\delta_m^{m-1-k}(U)) - \varphi(\delta_m^{m-k}(U))\right) \\ & = & p^{m-t}\varphi(U) - \varphi(\delta_m^{-t}(U)) \end{array}$$

La preuve de l'assertion concernant les v_i est similaire. □

Nous montrons maintenant le résultat principal de cette section, qui va nous permettre de définir la p-densité.

Proposition 1.1. *L'ensemble $\left\{\frac{\sigma_p(D,m)}{m}\right\}_{m\geq 1}$ admet un minimum ; celui-ci est atteint en l'un au moins des entiers $m \leq \prod_{j=1}^r D_i$.*

DÉMONSTRATION. Fixons un entier $m > \prod_{j=1}^{r} D_i$, et soit $U = (u_1, \ldots, u_n) \in E_D(m)$ tel que $\sigma_p(U) = \sigma_p(D, m)$. On a posé $\Phi(U) := \{\varphi(\delta_m^k(U))\}_{0 \leq k \leq m-1}$. C'est un sous ensemble de $Im(\varphi)$. D'après le lemme 1.1 iii/, et le principe des paires de chaussettes, on peut trouver deux entiers $t_1 < t_2$ dans $\{0, \ldots, m-1\}$ tels que $\varphi(\delta_m^{t_1}(U)) = \varphi(\delta_m^{t_2}(U))$. Remplaçons U par $\delta_m^{t_1}(U)$ (ils ont le même poids en base p) ; on a donc $0 < t \leq m-1$ tel que $\varphi(U) = \varphi(\delta_m^t(U))$.

Pour chaque $1 \leq i \leq n$, on note encore $u_i = p^{m-t} w_i + v_i$ le résultat de la division euclidienne de u_i par p^{m-t}, et on pose $V = (v_1, \ldots, v_n)$, $W = (w_1, \ldots, w_n)$. D'après le lemme 1.2 ii/ et le fait que $\varphi(U) = \varphi(\delta_m^t(U))$, on a

$$\sum_{i=1}^{n} v_i \mathbf{d}_i = (p^{m-t} - 1)\varphi(U) \ ; \ \sum_{i=1}^{n} w_i \mathbf{d}_i = (p^t - 1)\varphi(U).$$

Donc $V \in E_D(m-t)$ et $W \in E_D(t)$. D'après les définitions, on a les inégalités $\sigma_p(V) \geq \sigma_p(D, m-t)$, et $\sigma_p(W) \geq \sigma_p(D, t)$. Maintenant, pour chaque i on a $\sigma_p(u_i) = \sigma_p(v_i) + \sigma_p(w_i)$, d'où $\sigma_p(U) = \sigma_p(V) + \sigma_p(W)$. Notre choix de U assure donc $\sigma_p(D, m) = \sigma_p(V) + \sigma_p(W) \geq \sigma_p(D, m-t) + \sigma_p(D, t)$, c'est à dire

$$\frac{\sigma_p(D, m)}{m} \geq \left(1 - \frac{t}{m}\right) \frac{\sigma_p(D, m-t)}{m-t} + \frac{t}{m} \frac{\sigma_p(D, t)}{t}.$$

En conséquence on a montré l'inégalité $\frac{\sigma_p(D,m)}{m} \geq \min(\frac{\sigma_p(D,m-t)}{m-t}, \frac{\sigma_p(D,t)}{t})$. Si t ou $m-t$ est plus grand que $\prod_{j=1}^{r} D_i$, on utilise le même procédé pour V ou W. Finalement on obtient :

$$\frac{\sigma_p(D, m)}{m} \geq \min_{t \leq \prod_{j=1}^{r} D_i} \left\{ \frac{\sigma_p(D, t)}{t} \right\},$$

ce qui est le résultat recherché. □

Nous pouvons définir la p-densité de l'ensemble D.

Définition 1.2. *i/ Soient D, p comme plus haut. La* p-densité de l'ensemble D *est le rationnel*

$$\pi_p(D) := \frac{1}{p-1} \min_{m \geq 1} \left\{ \frac{\sigma_p(D, m)}{m} \right\}.$$

ii/ La densité d'un élément $U \in E_D(m)$ est $\pi(U) := \frac{\sigma_p(U)}{(p-1)m}$. L'élément U est minimal *quand $\pi(U) = \pi_p(D)$.*

1.2. Propriétés de la p-densité. On garde dans cette section les notations de la précédente.

Nous allons donner quelques propriétés de la p-densité d'un sous-ensemble fini de $\mathbb{N}^r$. Commençons par une définition

Définition 1.3. *i/ Soit $D \subset \mathbb{N}^r$; le* poids en base p de D *est le plus grand des poids en base p des coordonnées de ses éléments ; on le note*

$$\sigma_p(D) := \max\{\sigma_p(d_{ij}),\ 1 \leq i \leq n, 1 \leq j \leq r\}.$$

ii/ Pour chaque $1 \leq i \leq n$ soit $\sigma_p(\mathbf{d}_i)$ le vecteur $(\sigma_p(d_{i1}), \ldots, \sigma_p(d_{ir})) \in \mathbb{N}^r$. On note $\sigma_p(D)$ l'ensemble $\{\sigma_p(\mathbf{d}_1), \ldots, \sigma_p(\mathbf{d}_n)\}$.

A l'aide de ces définitions, on obtient :

Lemme 1.3. *Soient $D_1, D_2, D \subset \mathbb{N}^r$, aucun de leurs éléments n'étant multiple de p.*

i/ Si $D_1 \subset D_2$, on a $\pi_p(D_1) \geq \pi_p(D_2)$.

ii/ Posons $D = \{\mathbf{d}_1, \ldots, \mathbf{d}_n\}$. Soit $\mathbf{v}(v_1, \ldots, v_r) \in \mathbb{R}^r$ un vecteur tel que pour tout $1 \leq i \leq n$ le produit scalaire $\mathbf{v} \cdot \mathbf{d}_i$ soit plus petit que 1. On a l'inégalité

$$\pi_p(D) \geq \sum_{j=1}^{r} v_j.$$

iii/ On conserve les notations du ii/. Soit $\mathbf{v}(v_1, \ldots, v_r) \in \mathbb{R}^r$ un vecteur tel que pour tout $1 \leq i \leq n$ le produit scalaire $\mathbf{v} \cdot \sigma_p(\mathbf{d}_i)$ soit plus petit que 1. On a l'inégalité

$$\pi_p(D) \geq \sum_{j=1}^{r} v_j.$$

iv/ On a l'inégalité : $\pi_p(D) \geq \frac{1}{\sigma_p(D)}$.

DÉMONSTRATION. L'assertion i/ vient des définitions, puisque pour chaque m, on a $E_{D_1}(m) \subset E_{D_2}(m)$.

Montrons ii/. Soit $U = (u_1, \ldots, u_n) \in E_D(m)$. Pour tout $1 \leq j \leq r$, on a $\sum_{i=1}^n u_i d_{ij} = a_j(q-1)$ pour un certain entier naturel non nul a_j. D'après [**53**, Proposition 11 iv/], on a $\sigma_p(a(p^m-1)) \geq m(p-1)$. Mais pour chaque $1 \leq j \leq r$, on a les inégalités

$$\sigma_p(\sum_{i=1}^n u_i d_{ij}) \leq \sum_{i=1}^n \sigma_p(u_i d_{ij}) \leq \sum_{i=1}^n \sigma_p(u_i) d_{ij}. \tag{11}$$

On en déduit

$$\sigma_p(U) = \sum_{i=1}^n \sigma_p(u_i) \geq \sum_{i=1}^n \sigma_p(u_i) \sum_{j=1}^r v_j d_{ij} \geq \sum_{j=1}^r v_j \sum_{i=1}^n \sigma_p(u_i) d_{ij} \geq m(p-1) \sum_{j=1}^r v_j.$$

C'est ce que nous voulions. L'assertion iii/ provient des mêmes raisonnements, en remplaçant l'inégalité (11) par

$$\sigma_p(\sum_{i=1}^n u_i d_{ij}) \leq \sum_{i=1}^n \sigma_p(u_i)\sigma_p(d_{ij}).$$

Finalement, iv/ est un cas particulier de iii/, quand $\mathbf{v}$ est le vecteur dont toutes les coordonnées valent $\frac{1}{d\sigma_p(D)}$. □

Nous allons maintenant donner une minoration de $\pi_p(D)$ qui ne dépend que de l'enveloppe convexe $D \cup \{0, \ldots, 0\}$ dans $\mathbb{R}^r$. Cette borne apparaît dans les travaux de Adolphson et Sperber (*cf.* [**1**, page 546])

Définition 1.4. *Soit $D \subset \mathbb{N}^r$ comme ci-dessus. Notons $\Delta(D)$ l'enveloppe convexe des points de D et de l'origine dans $\mathbb{R}^r$. On définit $\omega(D)$ comme le plus petit nombre tel que $\omega(D)\Delta(D)$, l'image de $\Delta(D)$ par l'homothétie de rapport $\omega(D)$ et de centre l'origine, contient un point de $(\mathbb{N}^*)^r$.*

Proposition 1.2. *On a la minoration $\pi_p(D) \geq \omega(D)$.*

DÉMONSTRATION. Soit $U \in E_D(m)$. Alors $\varphi(U) = \frac{1}{p^m-1}\sum_{i=1}^n u_i \mathbf{d}_i$ est un point de $(\mathbb{N}^*)^r$. D'après la définition de $\omega(D)$, on a donc $\sum_{i=1}^n u_i \geq (p^m-1)\omega(D)$. De la même façon, pour chaque $0 \leq k \leq m-1$ on obtient $\sum_{i=1}^n \delta_m^k(u_i) \geq (p^m-1)\omega(D)$. En sommant sur k on trouve $\sum_{k=0}^{m-1}\sum_{i=1}^n \delta_m^k(u_i) \geq m(p^m-1)\omega(D)$. D'après le lemme 1.1 ii/ on a $\sum_{k=0}^{m-1}\delta_m^k(u_i) = \frac{p^m-1}{p-1}\sigma_p(u_i)$, et finalement $\sum_{i=1}^n \sigma_p(u_i) \geq m(p-1)\omega(D)$, c'est à dire $\pi(U) \geq \omega(D)$. C'est l'assertion recherchée. □

On termine ces propriétés par une dernière minoration.

Lemme 1.4. *Soit T un sous ensemble de $\{1, \ldots, r\}$, de cardinal t. On note D_T la projection suivante de D sur $\mathscr{R}^t$*

$$D_T = \{\mathbf{d}'_i,\ 1 \leq i \leq n\},\ \mathbf{d}'_i := (d_{ij})_{j \in T}.$$

Alors on a $\pi_p(D) \geq \pi_p(D_T)$.

DÉMONSTRATION. Il suffit de remarquer que si S est le complémentaire de T dans $\{1, \ldots, r\}$, alors pour chaque $m \geq 1$ on a $E_D(m) = E_{D_S}(m) \cap E_{D_T}(m)$: on a juste scindé le système d'équations modulaires en deux sous-systèmes. L'assertion est maintenant une conséquence directe des définitions. □

1.3. Le cas $r = 1$. Commençons par le cas le plus simple : $D = \{d\}$, avec $d > 1$ un entier premier à p.

Définition 1.5. *Pour tout rationnel $x \in \mathbb{Q}$, on note $\langle x \rangle := x - [x]$ sa partie fractionnaire. Soit ℓ l'ordre de p dans le groupe multiplicatif $(\mathbb{Z}/d\mathbb{Z})^\times$. Pour chaque entier $1 \leq a \leq d-1$, on définit*

$$\tau_d(a) = \frac{1}{\ell}\sum_{i=0}^{\ell-1}\langle \frac{ap^i}{d} \rangle.$$

Remarque 1.2. *Le rationnel $\tau(a)$ est bien connu. Soit m un entier tel que $p^m \equiv 1\ [d]$. Si ω est le caractère de Teichmüller du corps fini $\mathbb{F}_{p^m}$, d'après le théorème de Stickelberger* [**8**]*, $\tau(a)$ est la p^m-valuation de la somme de Gauss sur $\mathbb{F}_{p^m}$ associée au caractère $\omega^{-a\frac{p^m-1}{d}}$.*

Proposition 1.3. *Supposons que $D = \{d\}$, $d \neq 1$. On a l'égalité*

$$\pi_p(D) = \min_{1 \leq a \leq d-1} \{\tau_d(a)\}.$$

DÉMONSTRATION. Soit $u \in E_D(m)$. On a donc $ud = a(p^m - 1)$. Posons $d_m := \gcd(d, p^m - 1)$: on doit avoir $u = a'(p^m - 1)/d_m$ et $a = a'd/d_m$ pour un certain $a' \in \{1, \ldots, d_m - 1\}$. D'après [**8**, Theorem 11.2.7], on sait que

$$\sigma_p(u) = (p-1) \sum_{i=0}^{m-1} \langle \frac{a'p^i}{d_m} \rangle.$$

Si ℓ_m est l'ordre de p dans le groupe multiplicatif $(\mathbb{Z}/d_m\mathbb{Z})^\times$, on a aussi $\ell_m | m$, et on en déduit $\sigma_p(u) = (p-1)\frac{m}{\ell_m} \sum_{i=0}^{\ell_m - 1} < \frac{a'p^i}{d_m} >$. D'autre part on sait que $\ell_m | \ell$, d'où l'égalité

$$\sigma_p(u) = (p-1)\frac{m}{\ell} \sum_{i=0}^{\ell-1} \langle \frac{a'p^i}{d_m} \rangle = (p-1)\frac{m}{\ell} \sum_{i=0}^{\ell-1} \langle \frac{ap^i}{d} \rangle = m(p-1)\tau_d(a).$$

Le résultat provient maintenant de la définition de $\pi_p(D)$. □

Remarquons la symétrie suivante : $\tau_d(a) + \tau_d(d-a) = 1$. En conséquence pour chaque a l'un de ces deux nombres est plus petit que $\frac{1}{2}$. D'après le lemme 1.3 on obtient les bornes suivantes en dimension 1

Corollaire 1.1. *Soit $D \subset \mathbb{N}\backslash\{0\}$, tel que $D \neq \{1\}$, et D ne contient aucun multiple de p ; on a les inégalités*

$$\frac{1}{\sigma_p(D)} \leq \pi_p(D) \leq \frac{1}{2}.$$

Remarque 1.3. *Quand $D = \{d\}$ et p est semi primitif modulo d, c'est à dire quand l'une des puissances de p vaut -1 modulo d, on a l'égalité de droite dans le corollaire ci-dessus.*

Terminons cette section par un résultat pratique, qui facilite le calcul numérique de la p-densité de petits sous-ensembles pour un petit premier.

Lemme 1.5. *Soit $U \in E_D(m)$ de densité π, tel que $\Phi(U)$ contienne m éléments deux à deux distincts. Si $d = \max D$, on a*

$$m \leq 2d\pi - 1.$$

DÉMONSTRATION. D'après le lemme 1.2 i/, on a

$$\sum_{i=1}^{n} \sigma_p(u_i) d_i = (p-1) \sum_{k=0}^{m-1} \varphi(\delta_m^k(U)).$$

Les nombres $\varphi(\delta_m^k(U))$ sont les éléments de $\Phi(U)$; puisqu'ils sont strictement positifs et deux à deux distincts, le second membre est plus grand que $m(m+1)/2$.

D'autre part, on a la majoration $\sum_{i=1}^{n} \sigma_p(u_i) d_i \leq d \sum_{i=1}^{n} \sigma_p(u_i) = d\sigma_p(U) = dm(p-1)\pi$. Le résultat découle de la combinaison de ces deux inégalités. □

2. Valuation des sommes exponentielles.

Dans ce chapitre on choisit un polynôme $f \in \overline{\mathbb{F}}_p[x_1, \ldots, x_r]$ tel que toutes les variables apparaissent dans f (sinon on se ramène en dimension inférieure), et on note $D := D(f)$ l'ensemble des exposants des monômes de f dans $\mathbb{N}^r$.

Supposons que $f \in k[x_1, \ldots, x_r]$. Notons ψ un caractère additif non trivial de k. La somme exponentielle associée à f sur k est la somme

$$S_q(f) := \sum_{(x_1, \ldots, x_r) \in k^r} \psi(f(x_1, \ldots, x_r)).$$

Notre principal résultat est l'estimation suivante de la valuation q-adique de la somme $S(f)$

Théorème 2.1. *Soient p, f, D comme ci-dessus. Si v_q désigne la valuation q-adique, on a la minoration*

$$v_q(S_q(f)) \geq \pi_p(D).$$

De plus cette inégalité est optimale en ce sens que si p et D sont fixés, il existe une puissance q de p et un polynôme f défini sur k, ayant ses exposants dans D, tels qu'on ait l'égalité.

Démonstration. La minoration provient de [**53**, Theorem 8] : le nombre L défini dans ce théorème est égal à $\sigma_D(m) \geq m(p-1)\pi_p(D)$. Puisque le nombre π du même théorème est de valuation $v_q(\pi) = \frac{1}{m(p-1)}$, on obtient le résultat.

L'optimalité provient de [**53**, Theorem 9] : d'après la proposition 1.1 on peut choisir $m \geq 1$ tel que $\sigma_D(m) = m(p-1)\pi_p(D)$. Alors le nombre L vaut exactement $m(p-1)\pi_p(D)$, et il y a au moins un polynôme f avec ses coefficients dans $\mathbb{F}_{p^m}$ et ses exposants dans D tel que $S(f)$ soit exactement de valuation q-adique égale à $\pi_p(D)$. □

Remarque 2.1. *D'après la proposition 1.2, on obtient donc une meilleure minoration que dans* [**1**, Theorem 1.2]. *Le prix à payer est la dépendance en p de la nouvelle borne, alors que celle de* [**1**] *n'en dépend pas.*

Comme d'habitude, on déduit du résultat précédent un théorème à la Chevalley-Warning-Ax-Katz. Commençons par fixer quelques notations.

Soient $f_1, \ldots, f_s \in k[x_1, \ldots, x_r]$ des polynômes en r variables sur k. Pour tout $1 \leq i \leq s$, soit D_i l'ensemble des exposants de f_i dans $\mathbb{N}^r$. Notons X la sous-variété de l'espace affine $\mathbb{A}^r$ (sur k) définie par l'annulation simultanée des f_i, $1 \leq i \leq s$. On note $D(X)$ le sous ensemble de $\mathbb{N}^{r+s}$ défini comme l'union sur $1 \leq i \leq s$ des $D_i \times \{0, \ldots, 0, 1, 0, \ldots, 0\}$, où le 1 est à la i-ème place. On a alors

Théorème 2.2. *Le nombre de points rationnels sur $\mathbb{F}_q$ de X, $N_q(X)$ satisfait*

$$v_q(N_q(X)) \geq \pi_p(D(X)) - s.$$

Démonstration. La preuve est très classique. Considérons le polynome

$$g(x_1, \ldots, x_r, y_1, \ldots, y_s) := \sum_{i=1}^{s} y_i f_i(x_1, \ldots, x_r) \ \in \ k[x_1, \ldots, x_r, y_1, \ldots, y_s];$$

à partir des relations d'orthogonalité sur les caractères additifs, on a la relation $S_q(g) = q^s N_q(X)$. Mais l'ensemble des exposants de g est exactement $D(X)$, et le résultat provient du théorème 2.1. □

3. La première pente générique des courbes d'Artin Schreier

Communément, une courbe d'Artin-Schreier C est un revêtement cyclique de degré p de la droite projective sur un corps de caractéristique p. En d'autres termes, une telle courbe admet un modèle affine d'équation $y^p - y = f(x)$, avec $f \in k(x)$ une fraction rationnelle. Si f admet au moins deux pôles, la formule de Deuring-Shafarevic assure que le p-rang de la jacobienne de C est strictement positif : le premier segment du polygone de Newton du numérateur de sa fonction zêta est horizontal.

Nous supposons donc dans la suite que f admet un pôle unique, à l'infini, c'est à dire que f est un polynôme. Dans ce cas, on déduit le polygone de Newton du numérateur de la fonction zêta de celui de la fonction L associée aux sommes exponentielles (et à n'importe quel caractère additif non trivial)

$$S_r(f) = \sum_{x \in k_r} \psi(\mathrm{Tr}_{k_r/k}(f(x))), \ r \geq 1$$

par l'homothétie de centre O et de rapport $p-1$. Le reste de ce chapitre est donc consacré à l'étude du polygone de Newton q-adique de cette fonction.

Commençons par préciser le sens de "première pente générique". On paramètre l'espace des polynômes dont les exposants sont dans D, $D = \{d_1, \ldots, d_n\}$ par l'espace affine $\mathbb{A}_D$ de dimension $n-1$, en associant le point $(a_1, \ldots, a_{n-1})$ et le polynôme $f(x) = x^{d_n} + a_{n-1}x^{d_{n-1}} + \cdots + a_1 x^{d_1}$. D'après le théorème de spécialisation de Grothendieck [**31**, Corollary 2.3.2], quand f parcourt l'espace des polynômes dont les exposants sont dans D, et à coefficients dans $\overline{\mathbb{F}}_p$, il y a un ouvert, Zariski-dense, $U_{D,p}$ de cet espace, et un *polygone de Newton générique* $GNP(D,p)$, tels que pour tout $f \in U_{D,p}(\mathbb{F}_q)$, on ait $NP_q(f) = GNP(D,p)$, et $NP_q(f) \preceq GNP(D,p)$ pour tout $f \in \mathbb{A}_D(\mathbb{F}_q)$.

Définition 3.1. *La* première pente générique *de la famille des polynômes unitaires dont les exposants sont dans D et les coefficients dans $\overline{\mathbb{F}}_p$ est la première pente du polygone de Newton générique $GNP(D,p)$. On la note $s_1(D,p)$.*

Une nouvelle interprétation de la p-densité est

Théorème 3.1. *On a la relation $s_1(D,p) = \pi_p(D)$.*

Démonstration. L'inégalité $s_1(D,p) \geq \pi_p(D)$ provient du Théorème 2.1 joint à l'argument de [**7**, Introduction] : pour tout $f \in \mathbb{A}_D(\mathbb{F}_q)$, et tout $r \geq 1$, on a $v_q(S_r(f)) \geq r\pi_p(D)$, donc toute racine réciproque de $L(f,T)$ est de valuation q-adique supérieure à $\pi_p(D)$. En conséquence, pour tout $f \in \mathbb{A}_D$, la première pente du polygone de Newton q-adique de $L(f,T)$ est plus grande que la p-densité de D.

Montrons maintenant l'autre inégalité. D'après la définition, il suffit de montrer qu'il existe une puissance q de p, et un polynôme f à coefficients dans $\mathbb{F}_q$ tels que la première pente du polygone de Newton q-adique de $L(f,T)$ soit plus petite que $\pi_p(D)$. La seconde assertion du théorème 2.1, affirme l'existence de tels objets, satisfaisant $v_q(S(f)) = \pi_p(D)$. Dans ce cas l'une au moins des racines réciproques de $L(f,T)$ est de valuation q-adique plus petite que $\pi_p(D)$, ce que nous recherchions. □

Appliquons ce théorème pour construire des familles de courbes d'Artin-Schreier supersingulières. On rappelle qu'une courbe est *supersingulière* exactement quand son polygone de Newton est formé d'un seul segment, de longueur (horizontale) $2g$ et de pente $\frac{1}{2}$. D'après le résultat que nous venons de prouver, on obtient

Corollaire 3.1. *i/ La famille de courbes d'Artin-Schreier $y^p - y = f(x)$, $f \in \mathbb{A}_D(\overline{\mathbb{F}}_p)$, est supersingulière exactement quand la p-densité de D vaut $\frac{1}{2}$.*

ii/ (cf. [**64**] *pour $p = 2$) Quand D est un sous ensemble fini de $\{1, p^i + 1\}_{i \geq 0}$, la famille du i/ est supersingulière sur $\overline{\mathbb{F}}_p$.*

Remarque 3.1. *D'après le lemme 1.5, on a $\pi_p(D) = \frac{1}{2}$ ssi pour tout $1 \leq m \leq \max D - 1$, et tout $U \in E_D(m)$, on a $\pi(U) \geq \frac{1}{2}$. En conséquence, pour les corps de petite caractéristique, et les polynômes de petit degré (ils semblent être les plus à même de produire des familles de courbes supersingulières), une recherche exhaustive par ordinateur suffit à prouver la supersingularité.*

Example 3.1. *En plus de celles exhibées au corollaire précédent, les familles suivantes sont supersingulières (la dernière colonne donne une référence pour les familles déjà connues)*

p	D	Reference
2	$\{11,3,1\}$	[**59**]
2	$\{13,3,1\}$	[**59**]
3	$\{7,2,1\}$	[**73**]
3	$\{14,2,1\}$	
5	$\{7,1\}$	[**73**]
7	$\{5,2\}$	[**73**]

Notons que le seul nouvel exemple n'est pas très intéressant, puisque la courbe d'équation $y^3 - y = x^{28} + ax^4 + bx^2$ est un revêtement de degré 2, supersingulier par le corollaire 3.1 de la courbe d'équation $y^3 - y = x^{14} + ax^2 + bx$.

CHAPITRE 7

Sommes incomplètes sur les anneaux

On va présenter dans ce chapitre les résultats de [**B4**], et en donner une application à la valuation p-adique de sommes incomplètes sur les anneaux p-adiques dans la section 3.

1. Anneaux de Galois et vecteurs de Witt

Dans tout ce chapitre (et le suivant), on fixe un premier p. On note K l'extension non ramifiée de degré m du corps $\mathbb{Q}_p$, et $\mathcal{O}$ son anneau de valuation. C'est un anneau de valuation discrète d'idéal maximal $p\mathcal{O}$, et de corps résiduel $k = \mathbb{F}_q$, $q = p^m$. On note $\mathcal{T}^\times$ le sous groupe multiplicatif de $\mathcal{O}^\times$ formé des éléments d'ordre fini (des racines $q-1$-ièmes de l'unité), c'est le *sous groupe de Teichmüller* de $\mathcal{O}^\times$. On note R l'anneau $\mathcal{O}/p^l\mathcal{O}$, qu'on appelle parfois dans la littérature "anneau de Galois" (on rencontre aussi la notation $\mathrm{GR}(p^l, m)$). On désigne encore par $\mathcal{T}^\times$ l'image du sous groupe de Teichmüller dans R, et on appelle Teichmüller de R le sous ensemble $\mathcal{T} := \mathcal{T}^\times \cup \{0\}$. On pourrait aussi écrire

$$\mathcal{T} = \{x \in R,\ x^q = x\}\,.$$

Tout élément de R s'écrit de façon unique sous la forme $x := t_0 + pt_1 + \cdots + p^{l-1}t^{l-1}$, pour $t_0, \ldots, t_{l-1} \in \mathcal{T}$.

Pour tout $r \geq 1$, on note K_r l'extension non ramifiée de degré r de K, $\mathcal{O}_r$ son anneau de valuation et $R_r := \mathcal{O}_r/p^l\mathcal{O}_r$. De même $\mathcal{T}_r^\times$ désigne indifféremment le sous groupe de Teichmüller de $\mathcal{O}_r$ ou son image dans R_r, et $\mathcal{T}_r$ le Teichmüller de R_r. Le groupe $\mathrm{Gal}(K_r/K) \simeq \mathbb{Z}/r\mathbb{Z}$, engendré par le Frobenius, agit sur R_r en fixant R, et permet de considérer R_r comme une extension de degré r de R. On peut décrire l'action du Frobenius τ sur R_r à l'aide de la décomposition $x := t_0 + pt_1 + \cdots + p^{l-1}t_{l-1}$, pour $t_0, \ldots, t_{l-1} \in \mathcal{T}$: pour x comme ci-dessus

$$x^\tau := t_0^q + pt_1^q + \cdots + p^{l-1}t_{l-1}^q.$$

Fixons une racine p^l-ième primitive de l'unité $\zeta_{p^l} \in \overline{\mathbb{Q}}_p$. Alors l'application $n \mapsto \zeta_{p^l}^n$ se prolonge en un caractère Ψ_0 de $\mathbb{Z}_p$, d'ordre p^l. Si Ψ_l désigne le caractère additif d'ordre p^l de $\mathcal{O}$ défini en composant Ψ_0 avec la trace de K sur $\mathbb{Q}_p$, son passage au quotient devient un caractère Ψ d'ordre p^l de R, et son extension $\Psi_l^{(r)}$ via la trace donne un caractère Ψ_r de R_r d'ordre p^l.

Nous allons maintenant décrire cette situation d'une autre façon, à l'aide des vecteurs de Witt. Le lecteur intéressé par plus de détails et par les preuves de nos assertions pourra consulter [**62**] ou [**10**].

Les *polynômes de Witt* $\Phi_0, \ldots, \Phi_n, \ldots$ sont les polynômes de $\mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ définis par :

$$\Phi_0(X_0) = X_0, \ldots, \Phi_n(X_0, \ldots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n, \ldots$$

Il existe deux familles de polynômes $(S_i)_{i\in\mathbb{N}}$, $(P_i)_{i\in\mathbb{N}}$ dans $\mathbb{Z}[(X_i, Y_i)_{i\in\mathbb{N}}]$ tels que, pour tout $n \geq 0$:

$$\Phi_n(X_0, \ldots, X_n) + \Phi_n(Y_0, \ldots, Y_n) = \Phi_n(S_0, \ldots, S_n)\ ;$$

$$\Phi_n(X_0, \ldots, X_n)\Phi_n(Y_0, \ldots, Y_n) = \Phi_n(P_0, \ldots, P_n).$$

Remarquons qu'en assignant le poids p^j aux variables X_j, Y_j, le polynôme S_i est isobare de poids p^i, et le polynôme P_i isobare de poids $2p^i$.

Ces polynômes nous permettent de définir les opérations des anneaux de Witt

Définition 1.1. *Soit A un anneau commutatif. L'anneau des vecteurs de Witt de longueur l, à coefficients dans A, $W_l(A)$, est l'ensemble A^l, muni de l'addition et de la multiplication définies par :*

$$(a_0, \ldots, a_{l-1}) + (b_0, \ldots, b_{l-1}) := (S_0(a_0, b_0), \ldots, S_{l-1}(a_0, \ldots, b_{l-1}))\ ;$$

$$(a_0, \ldots, a_{l-1}) \times (b_0, \ldots, b_{l-1}) := (P_0(a_0, b_0), \ldots, P_{l-1}(a_0, \ldots, b_{l-1})).$$

On note V l'application de $W_l(A)$ définie par $V(a_0,\dots,a_{l-1}) = (0,a_0,\dots,a_{l-2})$, qu'on appelle *Verschiebung* (du mot allemand pour *décalage*) ; V est un endomorphisme de groupes additifs, mais pas d'anneaux. Notons que pour tout $(a_0,\dots,a_{l-1})$ dans $W_l(A)$, on a l'égalité de vecteurs de Witt :

$$(a_0,\dots,a_{l-1}) = \sum_{i=0}^{l-1} V^i(a_i,0,\dots,0).$$

Finalement, si $\phi : A \to B$ est un morphisme d'anneaux, l'application $W_l(\phi)$ de $W_l(A)$ vers $W_l(B)$ qui envoie $(a_0,\dots,a_{l-1})$ vers $(\phi(a_0),\dots,\phi(a_{l-1}))$ est encore un endomorphisme d'anneaux. En particulier, quand A est de caractéristique p, le Frobenius de A, qui associe à un élément sa puissance p-ième, induit un morphisme de $W_l(A)$, envoyant $(a_0,\dots,a_{l-1})$ sur $(a_0^p,\dots,a_{l-1}^p)$. On va noter ce morphisme F, c'est le *Frobenius de* $W_l(A)$.

Les morphismes F et V commutent, et pour tout x de $W_l(A)$, (a,b) de $\mathbb{N}^2$ on a les relations

$$FVx = VFx = px;\ V^a x V^b y = V^{a+b}\left(F^b x F^a y\right).$$

Terminons en faisant le lien entre les différents objets qu'on vient de décrire. Ce lien donné par les isomorphismes

$$\begin{array}{rccc} w_r & : & R_r & \to & W_l(k_r) \\ & & x = t_0 + \cdots + p^{l-1}t_{l-1} & \mapsto & (\bar{t}_0,\dots,\bar{t}_{l-1}^{p^{l-1}}) \end{array}$$

Via cet isomorphisme, le Frobenius τ de R correspond au Frobenius F de $W_l(k)$, et la multiplication par p dans R au morphisme (de groupes additifs) FV.

2. Les fonctions de Dwork de niveau supérieur

On se propose ici de décrire une généralisation des fonctions de Dwork. On va commencer par rappeler la construction de Dwork.

L'**exponentielle d'Artin-Hasse** est la série entière p-adique définie par

$$\mathrm{AH}(x) = \exp\left(\sum_{i\geq 0}\frac{X^{p^i}}{p^i}\right) \in \mathbb{Q}_p[[X]].$$

On sait (par exemple à l'aide du lemme de Dwork) que la série $\mathrm{AH}(X)$ est en fait dans $\mathbb{Z}_p[[X]]$, et que son rayon de convergence est 1. Choisissons π_1 un zéro de la série $\sum_{i\geq 0}\frac{X^{p^i}}{p^i}$, de valuation $\frac{1}{p-1}$. Alors la fonction $\theta_1(x) := \mathrm{AH}(\pi_1 x)$ est surconvergente, de rayon de convergence $p^{\frac{1}{p-1}}$. De même on définit la fonction

$$\theta_1^{(m)}(x) := \prod_{i=0}^{m-1}\theta_1(x^{p^i}),$$

qui est encore une série surconvergente (qui converge en particulier sur la boule unité fermée de $\mathbb{C}_p$). La fonction $\theta_1^{(m)}$ représente un caractère additif de k, de la façon suivante.

Définition 2.1. *On appelle fonction de Dwork (de niveau 1) pour k une série entière p-adique θ surconvergente telle que, si pour tout x de k_r, $\widetilde{x}$ désigne son relèvement au Teichmüller $\mathcal{T}_r$, alors*

1. *la fonction $x \mapsto \theta(\widetilde{x})$ est un caractère additif non trivial ψ de k, à valeurs dans $\mathbb{Q}_p(\zeta_p)$;*
2. *Pour chaque $r \geq 1$, le caractère additif ψ_r de k_r obtenu en composant ψ avec la trace de k_r sur k admet la représentation suivante :*

$$\forall x \in k_r,\ \psi_r(x) = \prod_{i=0}^{r-1}\theta(\widetilde{x}^{p^i}).$$

L'objet de ce chapitre est de définir des fonctions de Dwork de niveau supérieur : on va copier la définition précédente, en s'aidant de la représentation des éléments de R comme des vecteurs de Witt pour obtenir un caractère additif de l'anneau R.

Définition 2.2. *Pour tout x de R, d'image $(x_0,\dots,x_{l-1})$ dans $W_l(k)$, on note $\widehat{x}=(\widetilde{x}_0,\dots,\widetilde{x}_{l-1})\in\mathbb{C}_p^l$, et $\widehat{x}^p=(\widetilde{x}_0^p,\dots,\widetilde{x}_{l-1}^p)$. Une* fonction de Dwork (de niveau l) pour R, Θ, *est une fonction analytique p-adique surconvergente en l variables qui converge sur un ouvert de $\mathbb{C}_p^l$ de la forme $D(0,r_1)\times\cdots\times D(0,r_l)$, avec $r_1,\dots,r_l>1$, et qui satisfait aux deux conditions suivantes :*

1. *La fonction de R vers $\mathbb{C}_p$ définie par $x\mapsto\Theta(\widetilde{x})$ est un caractère additif Ψ d'ordre p^l de R, à valeurs dans $\mathbb{Q}_p(\zeta_{p^l})$;*
2. *Pour chaque $r\geq 1$, le caractère additif Ψ_r de R_r obtenu en composant Ψ avec la trace de R_r sur R admet la représentation analytique suivante :*

$$\Psi_r(x)=\prod_{i=0}^{r-1}\Theta(\widehat{x}^{p^i}).$$

2.1. Représentation analytique des racines p^l-ièmes de l'unité. Rappelons que Dwork obtient ses fonctions à l'aide de l'exponentielle d'Artin Hasse AH et des zéros de valuation $\frac{1}{p-1}$ de la série $\sum_{i\geq 0}\frac{X^{p^i}}{p^i}$; on va définir leurs généralisations simplement en considérant les autres zéros de cette série. On peut vérifier en construisant son polygone de Newton que la série $\sum_{i\geq 0}\frac{X^{p^i}}{p^i}$ admet $p-1$ zéros de valuation $\frac{1}{p-1}$, $\varphi(p^2)=p^2-p$ zéros de valuation $\frac{1}{p(p-1)}$, etc...

On sait que le corps Ω_l, obtenu en adjoignant à $\mathbb{Q}_p$ les racines p^l-ièmes de l'unité (c'est à dire que $\Omega_l=\mathbb{Q}_p(\zeta_{p^l})$), est une extension totalement ramifiée de $\mathbb{Q}_p$ de degré $\varphi(p^l)=p^{l-1}(p-1)$. Introduisons une définition

Définition 2.3. *Pour tout $0\leq k\leq l$, soit ζ_{p^k} une racine p^k-ième de l'unité dans $\mathbb{C}_p$. On dit que la famille $(\zeta_{p^k})_{0\leq k\leq l}$ est un* système compatible de racines p^k-ièmes de l'unité dans $\mathbb{C}_p$ *si les conditions suivantes sont vérifiées :*

1. *ζ_{p^k} est une racine primitive p^k-ième de l'unité ;*
2. *on a $\zeta_{p^k}^p=\zeta_{p^{k-1}}$ pour tout $1\leq k\leq l$.*

Nous allons construire un système de racines de $\sum_{i\geq 0}\frac{X^{p^i}}{p^i}$, satisfaisant lui même une relation de compatibilité, et qui nous servira tout à l'heure à représenter analytiquement un système compatible de racines p^k-ièmes de l'unité dans $\mathbb{C}_p$.

Lemme 2.1. *Soit π_l un zéro de $\sum_{i\geq 0}\frac{X^{p^i}}{p^i}$ avec $v_p(\pi_l)=(p^l-p^{l-1})^{-1}$, $l\geq 2$. Alors cette série admet un unique zéro π_{l-1}, de valuation $(p^{l-1}-p^{l-2})^{-1}$, tel que $\pi_{l-1}\equiv\ \pi_l^p[p\pi_l]$.*

A l'aide de ce résultat, on choisit une fois pour toutes π_l, un zéro de valuation $(p^l-p^{l-1})^{-1}$, puis on définit de proche en proche π_k pour $1\leq k\leq l-1$, par la condition $\pi_{k-1}\equiv\ \pi_k^p[p\pi_k]$. On va construire une famille de fonctions analytiques surconvergentes à l'aide de l'exponentielle d'Artin-Hasse et des zéros qu'on vient de choisir.

Définition 2.4. *Supposons les éléments π_k, $1\leq k\leq l-1$, choisis comme ci dessus. Pour tout k, on définit la fonction $\theta_k(x):=\mathrm{AH}(\pi_k x)$.*

On utilisera dans le prochain numéro ces fonctions pour définir les fonctions de Dwork pour R. On montre comme dans le cas classique que les valeurs de la fonction θ_k aux racines $p-1$-ièmes de l'unité sont des racines p^k-ièmes primitives de l'unité (c'est à dire qu'on prouve d'abord que pour $t\in\boldsymbol{\mu}_{p-1}$, on a $v_p(\theta_k(t)-1)=\frac{1}{p^{k-1}(p-1)}$, puis que $\theta(t)^{p^k}=1$). La construction qu'on a faite des π_k donne un peu plus que cela.

Lemme 2.2. *La famille $(\theta_k(1))_{0\leq k\leq l}$ est un système compatible de racines p^l-ièmes de l'unité.*

2.2. Fonctions de Dwork pour R. L'objet de ce numéro est de montrer

Théorème 2.1. *L'application définie par*

$$\begin{array}{rccc}\Theta & : & \prod_{i=1}^l B(0,p^{(p^{i-1}(p-1))^{-1}}) & \to & \mathbb{C}_p\\ & & (x_0,\dots,x_{l-1}) & \mapsto & \theta_l(x_0)\dots\theta_1(x_{l-1})\end{array}$$

est une fonction de Dwork pour R.

Avant de donner une idée de la démonstration, commençons par deux lemmes cruciaux. La forme de la série $\sum_{i\geq 0}\frac{X^{p^i}}{p^i}$ rappelle beaucoup les polynômes de Witt. Une conséquence de ce lien est

Lemme 2.3. *Pour tout entier $k\geq 0$, posons*

$$R_k(X,Y) := S_k(X,0,\dots,0;Y,0,\dots,0),$$

où les polynômes S_k sont ceux définis dans la section 1 (en particulier R_k est homogène de degré p^k). On a alors l'égalité de séries formelles, dans $\mathbb{Z}_p[[X,Y]]$

$$AH(X)AH(Y)=\prod_{k\geq 0}AH(R_k(X,Y)).$$

De ce lemme, on déduit par récurrence sur l (le cas $l=1$ provient de la construction de Dwork)

Lemme 2.4. *Soient $x_0,\dots,x_{l-1},y_0,\dots,y_{l-1}$ des éléments de k_r, et $z_0,\dots,z_{l-1}\in k_r$ définis par l'égalité de vecteurs de Witt $(z_0,\dots,z_{l-1})=(x_0,\dots,x_{l-1})+(y_0,\dots,y_{l-1})$ dans $W_l(k_r)$; alors si $\widetilde{x}$ désigne le représentant de Teichmüller de x, on a la congruence*

$$\Theta(\widetilde{x}_0,\dots,\widetilde{x}_{l-1})\Theta(\widetilde{y}_0,\dots,\widetilde{y}_{l-1})\equiv\Theta(\widetilde{z}_0,\dots,\widetilde{z}_{l-1})\ [p\pi_l].$$

Nous pouvons maintenant esquisser la démonstration du théorème 2.1

Démonstration. On fait la démonstration en deux étapes, correspondant aux deux propriétés que doit satisfaire la fonction Θ. Commençons par remarquer qu'il est suffisant de prouver ce théorème pour $m=1$ (c'est à dire pour $R=\mathbb{Z}/p^l\mathbb{Z}$) d'après la description des caractères de R à l'aide de la trace de R sur $\mathbb{Z}/p^l\mathbb{Z}$.

i/ Il est facile de vérifier que pour tout $t\in\boldsymbol{\mu}_{p-1}$, $t\pi_k$ est encore un zéro de $\sum_{i\geq 0}\frac{X^{p^i}}{p^i}$, et que $\theta_k(t)=\mathrm{AH}(t\pi_k)$ est encore une racine p^k-ième primitive de l'unité. Les valeurs de Θ aux l-uplets d'éléments de $\boldsymbol{\mu}_{p-1}$ est donc une racine p^l-ième de l'unité. Finalement, le lemme 2.4 assure qu'on a bien défini un caractère (c'est à dire un morphisme de groupes) car deux racines p^l-ièmes de l'unité qui satisfont la congruence de ce lemme sont égales.

ii/ C'est un calcul à faire à l'aide du lemme 2.4. En fait on a pour tout $x_0,\dots,x_{l-1}\in k_r$:

$$\prod_{i=0}^{r-1}\Theta(\widetilde{x}_0^{p^i},\dots,\widetilde{x}_{l-1}^{p^i})\equiv\Theta(\widetilde{y}_0,\dots,\widetilde{y}_{l-1})\ [p\pi_l],$$

où on a posé, dans $W_l(k_r)$:

$$(y_0,\dots,y_{l-1})=\sum_{i=0}^{r-1}(x_0^{p^i},\dots,x_{l-1}^{p^i})=\mathrm{Tr}_{W_l(k_r)/W_l(k)}(x_0,\dots,x_{l-1}).$$

Et le résultat en découle en utilisant l'isomorphisme w_r. □

2.3. Une généralisation du théorème de Stickelberger. L'objet de cette section est de démontrer une généralisation à la situation des sommes de Gauss p-adiques de la célèbre congruence de Stickelberger (*cf.* 1). Fixons ω le caractère de Teichmüller pour $R^\times$ (qui est la projection de la réduction de $R^\times$ sur $\mathcal{T}^\times$). On note encore Ψ le caractère de R défini à la section précédente, et Θ la fonction qui le représente analytiquement ; en particulier on pose $\zeta_{p^l}:=\Psi(1)$, c'est une racine primitive p^l-ième de l'unité. On va s'intéresser à certaines sommes de caractères incomplètes

Définition 2.5. *On appelle somme de Gauss p-adique associée à Ψ et ω la somme incomplète*

$$\mathscr{G}_{\mathcal{T}^\times}(\Psi,\omega^{-a}):=\sum_{x\in\mathcal{T}^\times}\Psi(x)\omega^{-a}(x).$$

Ces sommes vérifient la congruence suivante

Théorème 2.2. *Soit $1\leq a\leq q-2$ un entier. Dans $\mathbb{Q}_p(\zeta_{p^l})$, on a la congruence*

$$\mathscr{G}_{\mathcal{T}^\times}(\Psi,\omega^{-a})\equiv-\frac{(\zeta_{p^l}-1)^{s(a)}}{p(a)}\ [(\zeta_{p^l}-1)^{s(a)+1}],$$

où $s(a)$ désigne la somme des chiffres p-adiques de a, et $p(a)$ le produit de leurs factorielles.

DÉMONSTRATION. On utilise la représentation analytique p-adique du caractère Ψ par la fonction de Dwork Θ, et certaines propriétés des coefficients de Θ qu'on va rappeler maintenant.

Rappelons qu'on a $\Theta(x_0,\dots,x_{l-1}) = \theta_l(x_0)\dots\theta_1(x_{l-1})$, avec $\theta_k(x) = \mathrm{AH}(\pi_k x)$. La connaissance des coefficients de AH nous donne les informations suivantes sur ceux des fonctions θ_k, $1 \le k \le l$

$$\theta_k(x) = \sum_{n\ge 0} \lambda_{nk} x^n,\ \mathrm{ord}_p(\lambda_{nk}) \ge \frac{n}{p^{k-1}(p-1)}\ n \ge 0,\ \lambda_{nk} = \frac{\pi_k^n}{n!},\ 0 \le n \le p-1.$$

Puisque le caractère Ψ est décrit, pour tout x de R, par $\Psi(x) = \prod_{i=0}^{m-1} \Theta(\widehat{x}^{p^i})$, et que (comme $x \in \mathcal{T}$) $\Theta(\widehat{x}) = \theta_l(\widetilde{x})$, on peut écrire dans $\mathbb{C}_p$

$$\begin{aligned} G_{\mathcal{T}^\times}(\omega^{-a},\Psi) &= \textstyle\sum_{x\in\mathcal{T}^\times} x^{-a}\theta_l(x)\dots\theta_l(x^{p^{m-1}}) \\ &= \textstyle\sum_{x\in\mathcal{T}^\times} x^{-a}\left(\sum_{n\ge0}\lambda_{nl}x^n\right)\dots\left(\sum_{n\ge0}\lambda_{nl}x^{np^{m-1}}\right) \\ &= \textstyle\sum_{n_0,\dots,n_{m-1}\ge0} \lambda_{n_0 l}\dots\lambda_{n_{m-1}l}\sum_{x\in\mathcal{T}^\times} x^{n_0+\dots+p^{m-1}n_{m-1}-a} \\ &= (p^m-1)\sum_{\substack{n_0,\dots,n_{m-1}\ge0 \\ n_0+\dots+p^{m-1}n_{m-1}\equiv a\ [p^m-1]}} \lambda_{n_0 l}\dots\lambda_{n_{m-1}l}, \end{aligned}$$

et le théorème résulte maintenant du fait suivant : si $n_0,\dots,n_{m-1}$ sont m entiers naturels tels que :

$$n_0 + \dots + p^{m-1}n_{m-1} \equiv a\ [p^m-1].$$

Alors on a :

$$n_0 + \dots + n_{m-1} \ge s(a) = a_0 + \dots + a_{m-1},$$

et on a égalité si, et seulement si on a les égalités $n_0 = a_0,\dots,n_{m-1} = a_{m-1}$ □

3. Valuation des sommes incomplètes

Dans cette section, on va appliquer le théorème de Stickelberger qu'on vient de prouver, pour donner une minoration de la valuation p-adique des sommes incomplètes sur les anneaux de la forme

$$S_{\mathcal{T}_m}(f,\Psi) := \sum_{(x_1,\dots,x_r)\in\mathcal{T}_m^r} \Psi(f(x_1,\dots,x_r)),$$

pour Ψ un caractère d'ordre p^l et f un polynôme de $R[x_1,\dots,x_r]$, dans l'esprit de [**53**].

3.1. Polynômes d'Ax pour les caractères d'ordre p^l. Soit Ψ comme plus haut. Dans ce paragraphe, on définit le *polynôme d'Ax associé à* Ψ, et on donne la valuation p-adique valuation de ses coefficients.

Définition 3.1. *Le* polynôme d'Ax du caractère Ψ *est l'unique polynôme P de $\Omega_m[T]$ de degré au plus p^m-1 tel que pour tout $t \in \mathcal{T}$ on ait*

$$\Psi(t) := P(t).$$

L'unicité provient de l'interpolation de Lagrange. On a

Lemme 3.1. *Soit P le polynôme d'Ax pour le caractère Ψ ; posons $P(x) = \sum_{i=0}^{p^m-1} c_i x^i$. Pour tout $0 \le i \le p^m-1$, on a*

$$v_p(c_i) = \frac{\sigma_p(i)}{p^{l-1}(p-1)},$$

où $\sigma_p(i)$ est la somme des chiffres en base p de l'entier i.

DÉMONSTRATION. Elle suit les mêmes lignes que celles d'Ax dans [**7**], en s'appuyant sur le théorème de Stickelberger qu'on a montré dans la section précédente. □

3.2. Valuation p-adique des sommes incomplètes. Dans cette section on utilise les notations du chapitre 6.

Soit A un anneau ; on note $A[\mathbf{x}]_D$ l'ensemble des polynômes de la forme

$$R[\mathbf{x}]_D := \left\{ f(\mathbf{x}) = \sum_{i=1}^{n} a_i \mathbf{x}^{\mathbf{d}_i},\ a_i \in R \right\},$$

où on a posé $\mathbf{x}^{\mathbf{d}_i} := x_1^{d_{i1}} \cdots x_r^{d_{ir}}$.

En raisonnant comme dans [**53**, Section 3.2], et puisqu'on suppose que D n'est contenu dans aucun des sous ensembles $\{x_j = 0\}$, on obtient le

Théorème 3.1. *Soit $f \in R[\mathbf{x}]_D$ un polynôme ayant ses exposants dans D. On a*

$$v_p\left(S_{\mathcal{T}_m}(f,\Psi)\right) \geq \frac{\sigma_p(D,m)}{p^{l-1}(p-1)}.$$

Cette borne est optimale : il existe au moins un polynôme de $\mathcal{O}_m[\mathbf{x}]_D$ tel qu'elle soit atteinte.

Démonstration. On utilise les mêmes outils que dans les preuves des théorèmes 7, 8 et 9 de [**53**]. En particulier, d'après la preuve du théorème 7 on obtient

$$S_{\mathcal{T}_m}(f,\Psi) \equiv \left(\sum_{\substack{U=(u_1,\ldots,u_n)\in E_D(m),\\ \sigma_p(U)=\sigma_p(D,m)}} \prod_{i=1}^{n} \frac{a_i^{u_i}}{p(u_i)} \right) \pi^{\sigma_p(D,m)} \left[\pi^{\sigma_p(D,m)+1}\right], \tag{12}$$

avec $p(n) := n_0! \ldots n_{m-1}!$, pour $n = n_0 + \cdots + p^{m-1} n_{m-1}$, $0 \leq n_i \leq p-1$.

D'après (12), si f est fixé, la borne est atteinte pour un certain l si, et seulement si elle est atteinte pour tout $l \geq 1$, puisque la partie principale ne dépend que de l (*cf.* [**48**]). □

En utilisant la p-densité de l'ensemble D, on obtient une borne qui ne dépend plus que de p et D

Corollaire 3.1. *Soit $f \in R[\mathbf{x}]_D$ un polynôme ayant ses exposants dans D. Alors on a*

$$v_{p^m}\left(S_{\mathcal{T}_m}(f,\Psi)\right) \geq \frac{\pi_p(D)}{p^{l-1}},$$

où v_{p^m} est la valuation p-adique normalisée par $v_{p^m}(p^m) = 1$.

4. Conclusion et questions

La contruction qu'on vient de décrire a été utilisée par Liu et Wei [**49**] pour étudier les sommes incomplètes associées à des polynômes en plusieurs variables. Ces résultats étaient connus en dimension 1 pour la droite projective [**44**] et les courbes [**B5**]. L'idée, une fois généralisées les fonctions de Dwork, est de reproduire les travaux d'Adolphson et Sperber [**2**] dans ce nouveau cadre. On construit un complexe de Koszül, dont on vérifie l'acyclicité (excepté en dimension nulle), et la dimension du H_0 qu'on obtient est le degré de la fonction L. Cet invariant s'exprime encore comme le volume d'un polyèdre de Newton, construit cette fois à l'aide des degrés des monômes, pondérés par des puissances de p. De la même façon que dans 4, on construit un polygone de Hodge à partir du polyèdre de Newton et on obtient une borne inférieure pour le polygone de Newton de la fonction L.

Liu [**47**] a ensuite étendu ces résultats aux sommes tordues dans l'esprit de [**4**], [**3**]. En particulier, il obtient le polygone de Newton exact de la fonction L pour les sommes de Gauss p-adiques, généralisant le résultat qu'on vient d'exposer (cette fonction L est de degré p^l, et la congruence démontrée ci dessus ne donne que la première pente).

Récemment, Liu et Wan [**48**] ont proposé l'idée suivante : considérer le nombre $\zeta_{p^l} - 1$ comme un paramètre T, et considérer maintenant la fonction associée aux sommes

$$S_k(T) = \frac{1}{(q^k-1)^n} \sum_{x \in \boldsymbol{\mu}_{q^k-1}^n} (1+T)^{\mathrm{Tr} f(x)},\ k \geq 1.$$

Les auteurs obtiennent ainsi une fonction $L_f(s,T)$, dont ils prouvent qu'elle est entière (en s), et qui, spécialisée (en T), redonne toutes les fonctions L associées aux sommes incomplètes.

Par ailleurs, cette construction donne le cadre correct pour étudier le comportement asymptotique des polygones de Newton, en étudiant le polygone de Newton T-adique de la fonction $L_f(s,T)$. En effet, on ne peut espérer étudier le comportement asymptotique des polygones de Newton des fonctions L associées aux sommes incomplètes puisque leur longueur diverge (linéairement en p^{ln}), et le polygone de Newton T-adique (de longueur infinie) les remplace avantageusement. Son étude permet ainsi de généraliser aux sommes incomplètes les notions d'ordinarité et les questions de comportement asymptotique.

CHAPITRE 8

Sommes sur les anneaux

1. Introduction et notations

On reprend les notations du chapitre précédent. On va s'intéresser ici aux sommes, associées à une fonction réguliére définie sur un schéma sur R. Ici on somme sur l'ensemble de tous les R-points du schéma, non plus sur l'image d'une section de la réduction modulo p comme auparavant. La situation est très différente : au lieu d'utiliser des revêtements de courbes, et l'hypothèse de Riemann sur les corps finis [**B5**], on montre que les sommes sont "concentrées" sur les fibres de la réduction modulo p où la fonction admet une singularité. C'est une conséquence de la formule de la phase stationnaire, qu'on va exploiter pour décrire explicitement la fonction L dans deux cas, celui de la droite affine, et celui des courbes. Dans le premier cas, on va déterminer explicitement les fonctions L pour l assez grand, en montrant que les sommes de caractères s'expriment à l'aide de sommes de Gauss. Dans le second, on va trouver une factorisation de la fonction L, et montrer que le cas générique, on retrouve des résultats proches de ceux des corps finis.

Soit X un schéma défini sur R, et f une fonction régulière sur X (un morphisme de X dans $\mathbb{A}^1_R$). On va s'intéresser aux sommes

$$S_r(X,f) := \sum_{\Pi \in X(R_r)} \Psi_r(f(\Pi)),$$

où $X(R_r)$ désigne l'ensemble des R_r-points de X, c'est à dire l'ensemble des morphismes de Spec R_r vers X. Comme toujours, on leur associe la fonction L

$$L(X,f;T) := \exp\left(\sum_{r\geq 1} S_r(X,f)\frac{T^r}{r}\right).$$

On va essayer de répondre aux questions suivantes : rationalité, degré, poids des racines réciproques,. On va y répondre ici dans certains cas particuliers, essentiellement pour X de dimension 1 (une courbe).

Commençons par montrer la rationalité des fonctions L définies ci dessus dans un cadre très général.

2. Rationalité des fonctions L

Soit X un schéma de type fini sur R, et $f \in \Gamma(X,\mathcal{O}_X)$ une fonction régulière sur X. On va montrer ici que la fonction L associée à X et f est en fait une fraction rationnelle.

2.1. Foncteur de Greenberg. Commençons par rappeler quelques résultats sur le foncteur de Greenberg [**22**]. A tout schéma Y sur k, on associe fonctoriellement un schéma WY au dessus de Spec R, ayant le même espace topologique sous-jacent, et dont le faisceau structural $\mathcal{O}_{WY} = W_l(\mathcal{O}_Y)$ est défini pour tout ouvert U de Y par

$$\Gamma(U,\mathcal{O}_{WY}) = W_l(\Gamma(U,\mathcal{O}_Y)).$$

Si X est un schéma sur R, le foncteur qui associe $\mathrm{Hom}_R(WY,X)$ à un schéma Y sur k se représente par un schéma $\mathcal{F}X$ sur k : on obtient un isomorphisme fonctoriel

$$\mathrm{Hom}_R(WY,X) = \mathrm{Hom}_k(Y,\mathcal{F}X).$$

Le foncteur de Greenberg est maintenant le foncteur $X \mapsto \mathcal{F}X$ de la catégorie des schémas sur R vers celle des schémas sur k. Remarquons qu'on obtient en particulier un morphisme $\lambda_X : W\mathcal{F}X \to X$ correspondant à l'identité de $\mathcal{F}X$ par la formule d'adjonction ; notons $\gamma_X : \Gamma(X,\mathcal{O}_X) \to W_l(\Gamma(\mathcal{F}X,\mathcal{O}_{\mathcal{F}X}))$ le morphisme induit par λ_X sur les sections globales.

Puisque pour tout $r \geq 1$ on a $W\mathrm{Spec}\ k_r = \mathrm{Spec}\ R_r$, la formule d'adjonction fournit une bijection, (qu'on appellera *bijection de Greenberg* dans la suite)

$$X(R_r) = \mathcal{F}X(k_r),$$

de l'ensemble des R_r-points de X vers l'ensemble des k_r-points de $\mathcal{F}X$. De plus, si $\Pi \in X(R_r)$, et $P \in \mathcal{F}X(k_r)$ est son image par cette bijection, alors le diagramme suivant commute

$$\begin{array}{ccc} \Gamma(X, \mathcal{O}_X) & \xrightarrow{\gamma_X} & W_l(\Gamma(\mathcal{F}X, \mathcal{O}_{\mathcal{F}X})) \\ {\scriptstyle \Gamma(\Pi)}\downarrow & & \downarrow{\scriptstyle W_l(\Gamma(P))} \\ R & \xrightarrow{\quad w \quad} & W_l(k) \end{array}$$

En d'autres termes, pour toute fonction $f \in \Gamma(X, \mathcal{O}_X)$ d'image $\gamma_X(f) := (f_0, \ldots, f_{l-1})$ dans $W_l(\Gamma(\mathcal{F}X, \mathcal{O}_{\mathcal{F}X}))$, et tout R_r-point Π de X, correspondant au k_r-point P de $\mathcal{F}X$, on a $f(\Pi) = w^{-1}(\gamma_X(f)(P)) = w^{-1}(f_0(P), \ldots, f_{l-1}(P))$. On peut donc réécrire la somme S_r à l'aide de la bijection de Greenberg

$$S_r(X, f) = S_r(\mathcal{F}X, \gamma_X f) := \sum_{P \in \mathcal{F}X(k_r)} \Psi_r(w^{-1}\gamma_X f(P)),$$

et la fonction $L(X, f; t)$ devient

$$L(X, f; T) = \exp\left(\sum_{r \geq 1} S_r(\mathcal{F}X, \gamma_X f)\frac{T^r}{r}\right) = L(\mathcal{F}X, \gamma_X f; T) \tag{13}$$

On va réinterpréter cette nouvelle fonction.

2.2. Interprétation ℓ-adique et rationalité. Notons $\mathbb{W}_l$ la variété en groupes (affine) des vecteurs de Witt de longueur l, définie sur k (on a en particulier un isomorphisme de variétés algébriques $\mathbb{W}_l = \mathbb{A}^l$), et par F le morphisme de Frobenius sur $\mathbb{W}_l$ relatif à k, défini par $(X_0, \ldots, X_{l-1}) \mapsto (X_0^q, \ldots, X_{l-1}^q)$. Soit L l'isogénie de Lang sur $\mathbb{W}_l$, c'est à dire $L = F - Id_{W_l}$; elle est surjective, et on obtient le suite exacte suivante de variétés en groupes

$$0 \longrightarrow \mathbb{W}_l(k) \longrightarrow \mathbb{W}_l \xrightarrow{L} \mathbb{W}_l \longrightarrow 0.$$

Notons $\mathcal{L}$ le $\mathbb{W}_l(k) = W_l(k)$-torseur sur $\mathbb{W}_l$ défini par cette suite exacte (cf. [**14**], 1.7).

Fixons un nombre premier ℓ distinct de p, et soit ψ_l le caractère d'ordre p^l de $W_l(\mathbb{F}_q)$ vers $\overline{\mathbb{Q}}_\ell^\times$ correspondant à $\Psi \circ w^{-1}$ par un plongement fixé une fois pour toutes de $\overline{\mathbb{Q}}_\ell$ dans $\mathbb{C}$. Au torseur $\mathcal{L}$, on associe un $\overline{\mathbb{Q}}_\ell$-faisceau, lisse et de rang 1, $\mathcal{L}_{\psi_l} := \psi_l(\mathcal{L})$ sur $\mathbb{W}_l$.

Soit $g : Y \to \mathbb{W}_l$ un morphisme de variétés sur k. Considérons le faisceau $g^*\mathcal{L}_{\psi_l}$ sur Y. Pour y un point fermé de Y, disons $y \in Y(k_r)$, soit $\overline{y}$ un point géométrique au dessus de y. La fibre $g^*\mathcal{L}_{\psi_l,\overline{y}}$ est un $\overline{\mathbb{Q}}_\ell$-espace vectoriel de dimension 1, sur lequel agit le groupe $\mathrm{Gal}(k(\overline{y})/k(y))$. L'action du Frobenius géométrique relatif à $k(y)$, $F_{\overline{y}}$, est la multiplication par $\psi_l(\mathrm{Tr}_{W_l(k_r)/W_l(k)}(g(y)))$; c'est à dire que la trace de l'action de $F_{\overline{y}}$ sur $g^*\mathcal{L}_{\psi_l,\overline{y}}$ est cette racine de l'unité.

Notons $H_c^i(Y, g^*\mathcal{L}_{\psi_l})$, $0 \leq i \leq 2\dim Y$ les $\overline{\mathbb{Q}}_\ell$-espaces vectoriels de dimension finie provenant de la cohomologie à supports compacts de Y, à valeurs dans le faisceau ℓ-adique $g^*\mathcal{L}_{\psi_l}$. Le morphisme de Frobenius F_Y associé à Y agit linéairement sur ces espaces, et la formule des traces de Lefschetz [**23**] nous assure, pour tout $r \geq 1$, l'égalité

$$\sum_{y \in Y(k_r)} \psi_l(\mathrm{Tr}_{W_l(k_r)/W_l(k)} g(y)) = \sum_{i=0}^{2\dim Y} (-1)^i \mathrm{Tr}(F_Y^r | H_c^i(Y, g^*\mathcal{L}_{\psi_l})).$$

L'avatar, pour les fonctions L, de cette formule, est

$$L(Y, g; T) = \prod_{i=0}^{2\dim Y} \det(1 - TF_Y | H_c^i(Y, g^*\mathcal{L}_{\psi_l}))^{(-1)^{i+1}}, \tag{14}$$

qui, appliquée à la variété algébrique $Y = \mathcal{F}X$ et à la "fonction" $g = \gamma_X f$, donne le

Théorème 2.1. *Soit X un schema de type fini sur R, et f une fonction régulière sur X ; alors la fonction $L(X, f; T)$ est une fraction rationnelle.*

On va maintenant essayer de déterminer les degrés, racines et pôles réciproques de ces fonctions dans des cas particuliers.

3. Cas de la droite affine

Soit $f \in R[X]$ un polynôme. On va s'intéresser dans ce chapitre aux sommes de la forme

$$S_R(f) = \sum_{x \in R} \Psi(f(x)),$$

ainsi qu'aux fontions L qui leurs sont associées. Comme on va souvent être amenés à faire varier l, il est plus simple de supposer que f est la réduction modulo p^l d'une série entière restreinte de $\mathcal{O}\{X\}$ (par exemple l'anneau $\mathbb{Z}_p\{X\}$ est la complétion p-adique de l'anneau $\mathbb{Z}[X]$). On notera encore f une telle série.

Le résultat principal de ce numéro (qu'on n'obtiendra malheureusement pas par les méthodes du numéro précédent) est la détermination explicite des fonctions L quand l est assez grand. On va en effet montrer que les racines et pôles réciproques de ces fonctions sont des sommes de Gauss, à la fois classiques et p-adiques. On reprend ici les résultats de [**B3**].

On se ramène d'abord à des calculs d'intégrales, qui seront plus faciles à manipuler.

Lemme 3.1. *Soit $f \in \mathcal{O}\{X\}$ une série entière restreinte ; on a alors l'égalité*

$$S_{l,r}(f) := \sum_{x \in R_r} \Psi_r(f(x)) = q^{rl} \int_{\mathcal{O}_r} \Psi_{r,l}(f(x))|dx| := q^{rl} I_{l,r}(f),$$

où $|dx|$ est la mesure de Haar normalisée sur K_r. D'autre part, si

$$L_I(\Psi_l, f; T) := \exp\left(\sum_{r \geq 1} I_{l,r}(f)\frac{T^r}{r}\right),\ L_S(\Psi, f; T) := \exp\left(\sum_{r \geq 1} S_{l,r}(f)\frac{T^r}{r}\right)$$

désignent les fonctions L attachées respectivement aux sommes et aux intégrales, alors on a la relation

$$L_S(\Psi, f; T) = L_I(\Psi_l, f; q^l T).$$

3.1. Voisinages critiques. On va définir un *voisinage critique* associé à f, hors duquel les intégrales ci dessus s'annulent pour l assez grand. Notons $\overline{K}$ et $\widetilde{K}$ respectivement une clôture algébrique fixée de K, et l'extension maximale non ramifiée de K dans $\overline{K}$. Soient $\overline{\mathcal{O}}$ et $\widetilde{\mathcal{O}}$ les anneaux de valuation de ces corps.

Commençons par définir une *distance critique*. On note, pour $r \geq 1$

$$\Sigma_r^+(f) := \{x \in \mathcal{O}_r,\ f'(x) = 0\}\ ;\ \widetilde{\Sigma}^+(f) := \{x \in \widetilde{\mathcal{O}},\ f'(x) = 0\}\ ;$$
$$\overline{\Sigma}^+(f) := \{x \in \overline{\mathcal{O}},\ f'(x) = 0\}.$$

Ce sont des ensembles de points critiques de f, finis et rangés ci dessus du plus petit au plus grand. La *valuation critique de f*, $\mathcal{V}(f)$, est le plus petit entier tel que la famille des boules de $\overline{K}$ de rayon $|p|^{-\Delta(f)}$

(1) sépare deux éléments quelconques de $\overline{\Sigma}^+(f)$;
(2) sépare les éléments de $\overline{\Sigma}^+(f) \backslash \widetilde{\Sigma}^+(f)$ de $\widetilde{\mathcal{O}}$;
(3) sépare tout élément de $\widetilde{\Sigma}^+(f)$ de tout sous corps de $\widetilde{K}$ qui ne le contient pas ;
(4) sépare les points de n'importe quel sous ensemble de la forme $Z_\alpha^+(f) := \{x \in \overline{\mathcal{O}},\ f(x) = f(\alpha),\ x \neq \alpha\}$, pour $\alpha \in \widetilde{\Sigma}^+(f)$.

Définition 3.1. *Le voisinage critique de f, $U(f)$, est l'ensemble*

$$U(f) := \bigcup_{\alpha \in \widetilde{\Sigma}^+(f)} \left\{x \in \widetilde{\mathcal{O}},\ v(x - \alpha) > \mathcal{V}(f)\right\}.$$

Cet ensemble possède deux propriétés agréables : sa trace sur $\mathcal{O}_r$ ne dépend que des points critiques de f dans $\mathcal{O}_r$, et en dehors de $U(f)$, la dérivée de f n'est jamais trop proche de 0. Plus précisément

i/ Pour tout $r \geq 1$ on a (les boules sont fermées ici)

$$U(f) \cap \mathcal{O}_r = \coprod_{\alpha \in \Sigma_r^+(f)} \{x \in \mathcal{O}_r,\ v(x-\alpha) > \mathcal{V}(f)\} = \coprod_{\alpha \in \Sigma_r^+(f)} B(\alpha, |p|_{K_r}^{\lceil \mathcal{V}(f) \rceil}),$$

ii/ Si on peut écrire $f'(x) = p^e g(x)$ pour une série $g \in \mathcal{O}\{X\} \backslash p\mathcal{O}\{X\}$ dont la réduction modulo p est de degré d_0, alors on a

$$\forall x \in \widetilde{\mathcal{O}} \backslash U(f), \quad v(f'(x)) \leq e + [d_0 \mathcal{V}(f)]\,.$$

On déduit de ces résultats, et du fait que, hors du voisinage critique, f agit bijectivement sur chaque boule assez petite, le

Théorème 3.1. *Posons*

$$\Lambda_0(f) := \max\left(\lceil \mathcal{V}(f) \rceil, [d_0 \mathcal{V}(f)] + 1 + \delta_{p2}\right) + e + [d_0 \mathcal{V}(f)] + 1,$$

avec $\delta_{p2} = 1$ si $p = 2$, 0 sinon. Alors pour tous entiers $l \geq \Lambda_0(f)$, $r \geq 1$, on a

$$I_{l,r}(f) = \int_{\mathcal{O}_r \cap U(f)} \Psi_l^{(r)}(f(x))|dx| = \sum_{\alpha \in \Sigma_r^+(f)} \int_{B(\alpha, |p|_{K_r}^{\lceil \mathcal{V}(f) \rceil})} \Psi_l^{(r)}(f(x))|dx|.$$

3.2. Séries à monôme dominant. On souhaite étudier les restrictions de la série f à chacune des boules de son voisinage critique. On introduit pour cela une nouvelle notion

Définition 3.2. *Soit $f \in \mathcal{O}\{X\}$ une série entière restreinte, et m un entier positif; on dit f est une série entière restreinte à monôme dominant de degré $m+1$ quand f est de la forme $f(X) = \alpha_0 + \sum_{n \geq m+1} \alpha_n X^n$, les α_i vérifiant*

$$v(\alpha_n) > v(\alpha_{m+1}),\ \text{et}\ v(n\alpha_n) > v((m+1)\alpha_{m+1})\ \text{pour tout}\ n > m+1.$$

On note $e := e(f') = v((m+1)\alpha_{m+1})$ la multiplicité artihmétique de f'.

L'idée est qu'une série entière restreinte à monôme dominant va se comporter comme le monôme dominant $\alpha_{m+1}X^{m+1}$ sur une boule de centre 0, et que sa dérivée hors de cette boule est suffisamment éloignée de 0.

Introduisons quelques notations :

(1) Pour deux entiers a et b, soit $[a]_b$ le reste de la division euclidienne de a par b ;

(2) Pour un élément α de $K^\times$, soit $\mathrm{ac}(\alpha)$ sa composante angulaire, c'est à dire sa projection sur le sous groupe de Teichmüller $\mathcal{T}_d$;

(3) Pour un entier $l' \geq 1$, soit $L_{\mathcal{T}}(\Psi_{l'}, \alpha x^{m+1}; T)$ la fonction L provenant des sommes de caractères sur $\mathcal{T}$, associées au caractère $\Psi_{l'}$ et à ses extensions, et à la fonction αx^{m+1}. C'est un produit de fonctions L associées à des sommes de Gauss, classiques pour $l' = 1$, p-adiques sinon.

Alors la fonction L associée à une série entière à monôme dominant a une forme particulièrement simple :

Lemme 3.2. *Soit $p \geq 3$ un nombre premier, et $f \in \mathcal{O}\{X\}$ une série entière à monôme dominant de degré $m+1$, et de multiplicité arithmétique e. Soit $l \geq e+2$ un entier ; posons $n := \left[\frac{l-e-2}{m+1}\right]$. Si $m+1 = p^u b$, $(b,p) = 1$, la fonction L associée aux sommes provenant de Ψ et f s'écrit*

i) quand $0 \leq [l-e-2]_{m+1} \leq m-u-1$,

$$L_S(\Psi, f; T) = \frac{1}{1 - q^{l-n-1}\Psi(f(0))T}\ ;$$

ii) quand $m-u \leq [l-e-2]_{m+1} \leq m$, si on pose $l' = l - ((m+1)(n+1) + e - u)$,

$$L_S(\Psi, f; T) = L_{\mathcal{T}}(\Psi_{l'}, \mathrm{ac}(\alpha_{m+1})x^b; q^{l-n-2}\Psi(f(0))T).$$

On a un résultat similaire pour $p = 2$, avec quelques complications techniques **[B3, Theorem 4.12]**.

3.3. Cas général. Revenons à une série entière restreinte f quelconque. La dernière vertu de la définition du voisinage critique est que sur chacune de ses boules, la restriction de f est à monôme dominant : précisément la série entière $f_\alpha(X) := f(\alpha + p^{\lceil \mathcal{V}(f) \rceil} X)$ est à monôme dominant de degré $m_\alpha + 1$, pour m_α la multiplicité de α en tant que racine de f'. En regroupant les résultats précédents, on obtient la description explicite des fonctions L associées à f pour l assez grand :

Théorème 3.2. *Pour tout $l \geq \Lambda(f)$, la fonction $L_S(\Psi, f; T)$ s'écrit*

$$L_S(\Psi, f; T) = \prod_{i=1}^{s} L_S\left(\Psi^{(d_i)}, f_{\sigma_i}; (q^{-\lceil \mathcal{V}(f) \rceil} T)^{d_i}\right),$$

où $\sigma_1, \ldots, \sigma_s$ sont les orbites de l'action de $G = \mathrm{Gal}(\widetilde{K}/K)$ sur $\widetilde{\Sigma}^+(f)$, avec $\#\sigma_i = d_i$, $f_{\sigma_i} := f_{\alpha_i}$ pour un α_i de σ_i, et les fonctions $L_S\left(\Psi^{(d_i)}, f_{\sigma_i}; T\right)$ décrites au Lemme 3.2.

En faisant varier p, on déduit que si $P \in \mathbb{Z}[X]$ est un polynôme, alors pour presque tous les premiers p les fonctions L provenant de Ψ_l, un caractère d'ordre p^l de $\mathbb{Z}_p$, et P ont le même degré, dépendant de l'odre des points critiques de P dans $\overline{\mathbb{Q}}$, une clôture algébrique de $\mathbb{Q}$. Ce résultat est un analogue en dimension 1 de [**16**, Theorem 4.5.2] où le degré de la fonction L associée à Ψ_l et à f un polynôme en $n \geq 2$ variables avec des points critiques isolés est donné en termes des valeurs propres de l'action de la monodromie aux points critiques de f.

Corollaire 3.1. *Choisissons un polynôme*

$$P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X], \text{ avec } P'(X) = c(P') \prod_{i=1}^{s} P_i(X)^{m_i}$$

la décomposition en facteurs irréductibles de sa dérivée dans $\mathbb{Z}[X]$, où $c(P')$ désigne le contenu de P' ; si on pose

$$D(P) := n a_n \mathrm{disc}(P_1 \ldots P_s) \prod_{i=1}^{s} (m_i + 1),$$

alors pour tout premier p ne divisant pas $D(P)$, et tout $l \geq 2$, la fonction $L_S(\Psi, P; T)$ est de degré (où $\boldsymbol{\mu}_n$ est le groupe des racines n-ièmes de l'unité)

$$\sum_{i=1}^{s} \deg(P_i) \sum_{\zeta \in \boldsymbol{\mu}_{m_i+1} \setminus \{1\}} \zeta^{l-1}.$$

4. Cas des courbes

Dans toute cette section, on note C un schéma projectif, irréductible et lisse de dimension relative 1 sur Spec R. Par commodité, on appellera dans la suite "courbe sur R" un tel schéma.

Soit f une fonction sur C, c'est à dire un morphisme de C dans $\mathbb{P}^1_R$ la droite projective sur R ; on se propose de décrire une décomposition des sommes de caractères suivantes :

$$S_r(C, f) := \sum_{\Pi \in C_f(R_r)} \Psi_r(f(\Pi)),$$

où $C_f(R_r)$ désigne l'ensemble des R_r-points de C en lesquels f n'a pas de pôle. On en déduira ensuite une factorisation de la fonction

$$L(C, f; T) := \exp\left(\sum_{r \geq 1} S_r(C, f) \frac{T^r}{r}\right).$$

Dans le cas particulier où f est une fonction de Morse (c'est à dire que ses points critiques sont d'ordre 1), on va aussi obtenir le degré de cette fonction, le poids des nombres de Weil qui sont ses racines réciproques, et une majoration de la somme $S_r(C, f)$.

4.1. Géométrie des courbes sur un anneau. Notons $C_k := C \times_{\mathrm{Spec}\ R} \mathrm{Spec}\ k$ la "réduction modulo p" de C ; c'est une courbe irréductible et lisse sur Spec k, et pour tout $r \geq 1$, on a une bijection entre $C(k_r)$ et $C_k(k_r)$. Notons encore $C_r := C \times_{\mathrm{Spec}\ R} \mathrm{Spec}\ R_r$ et $C_{k_r} := C \times_{\mathrm{Spec}\ R} \mathrm{Spec}\ k_r$ les courbes obtenues par extension des scalaires. Alors le morphisme $\rho : \mathrm{Spec}\ k_r \to \mathrm{Spec}\ R_r$ induit par la réduction modulo p associe à tout point $\Pi \in C_r(R_r)$ un unique point $P \in C_r(k_r)$ via $P = \Pi \circ \rho$. Inversement, par lissité du morphisme structural, tout point de $C_r(k_r)$ provient d'un point de $C_r(R_r)$ de cette façon. On en déduit

Lemme 4.1. *Pour tout $r \geq 1$, on a l'union disjointe :*

$$C_r(R_r) = \coprod_{P \in C_r(k_r)} (\mathrm{Spec}\ \mathcal{O}_{C_r,P})(R_r),$$

où $(\mathrm{Spec}\ \mathcal{O}_{C_r,P})(R_r)$ *est l'ensemble des R_r-points du schéma* $\mathrm{Spec}\ \mathcal{O}_{C_r,P}$ *sur R.*

On est donc ramenés, dans l'estimation des sommes de caractères, à décomposer celles-ci comme des sommes sur les fibres de la réduction modulo p. On va étudier ces fibres plus précisément. Commençons par rappeler la définition d'un paramètre local pour un R-point de C. Le faisceau d'idéaux associé à un R-point Π de C (vu comme un sous-schéma de C) est localement principal, et il existe un élément $t \in \mathcal{O}_{C,P}$ qui engendre le noyau du morphisme $\Pi : \mathcal{O}_{C,P} \to R$. On appelle un tel élément un *paramètre local* pour C en Π. Soit m_P l'idéal maximal de l'anneau local $\mathcal{O}_{C,P}$; alors un paramètre local possède les propriétés suivantes

(1) t n'est pas diviseur de zéro dans $\mathcal{O}_{C,P}$;
(2) $t \in m_P \backslash m_P^2$;
(3) $\mathcal{O}_{C,P}/(t^n)$ est un R-module libre de base $1, t, t^2, \ldots, t^{n-1}$;
(4) l'anneau des fractions de $\mathcal{O}_{C,P}$, K_C, est un $\mathcal{O}_{C,P}$-module engendré par $1, t^{-1}, \ldots$.

On se servira de ces propriétés pour écrire des développements locaux de la fonction f tout à l'heure. Pour l'instant, on va utiliser les paramètres locaux pour décrire précisément les fibres de la réduction modulo p.

Proposition 4.1. *Soit C une courbe lisse sur R, P un point de $C(k)$, et t un paramètre local pour un R-point de* $\mathrm{Spec}\ \mathcal{O}_{C,P}(R)$. *Alors l'application $t \mapsto t(\Pi)$ de* $\mathrm{Spec}\ \mathcal{O}_{C,P}(R)$ *vers R est une bijection sur pR.*

4.2. Factorisation de la fonction L en produit de facteurs locaux. Réécrivons maintenant la somme $S_r(C, f)$; d'après le Lemme 4.1, on a

$$S_r(C, f) := \sum_{P \in C(k_r) \backslash P_f(k_r)} S_P(C, f), \quad S_P(C, f) := \sum_{\Pi \in \mathrm{Spec}\ \mathcal{O}_{C \otimes R_r, P}(R_r)} \Psi(f(\Pi)).$$

D'autre part, si Π_P est un R_r-point de C au dessus de P, et t_P un paramètre local en Π_P, notons $f_l(t) := \alpha_0 + \alpha_1 t + \cdots + \alpha_{l-1} t^{l-1}$ l'image de f dans l'anneau $\mathcal{O}_{C \otimes R_r, P}/(t_P^l)$.

Définition 4.1. *Le polynôme local associé à f en Π_P est le polynôme de $R_r[T]$ défini par*

$$f_{\Pi_P}(T) = \alpha_1 T + p\alpha_2 T^2 \cdots + p^{l-2} \alpha_{l-1} T^{l-1}.$$

Si on note R_r' l'anneau $R_r \otimes \mathbb{Z}/p^{l-1}\mathbb{Z}$, on obtient, à l'aide de la Proposition 4.1, l'écriture suivante pour les sommes locales :

$$S_P(f) = \Psi(f(\Pi_P)) \sum_{x \in R_r'} \Psi(f_{\Pi_P}(x)).$$

On s'est donc ramenés à étudier des sommes sur la droite affine $\mathbb{A}^1_{R'}$. Comme plus haut, toutes ces sommes sont nulles dès que f permute la fibre. Une condition suffisante pour observer ce phénomène est que le coefficient α_1 soit inversible, c'est à dire que le diviseur de la différentielle $d\overline{f}$ n'ait pas de zéro en P. Cela motive la définition suivante.

Définition 4.2. *Soit $g \in K(C_k)$ une fonction sur C_k ; on dit que g a un point critique en $P \in C_k(\overline{k})$ si le diviseur dg a un zéro en P. L'ordre du point critique de g en P est la multiplicité du diviseur $(dg)_0$ en P.*

On note Σ_g le support de $(dg)_0$, c'est à dire l'ensemble des points critiques de g.

La discussion précédente nous assure que la somme $S_P(f)$ est nulle dès que $P \notin \Sigma_{\overline{f}}$. On en déduit la factorisation suivante de la fonction L

Théorème 4.1. *Soit f une fonction sur C, et $\mathcal{P}_1, \dots, \mathcal{P}_t$ un ensemble de représentants pour les orbites de l'action de $\mathrm{Gal}(\overline{k}/k)$ sur $\Sigma_{\rho_K(f)} \backslash \mathbb{P}_f(\overline{k})$. Si $\deg(P_i) = d_i$, choisissons Π_i un R_{d_i}-point au dessus de l'un des points de $C(k_{d_i})$ dans l'orbite de $\mathcal{P}_i$; La fonction L associée à f admet la factorisation en facteurs locaux*

$$L(C, f; T) = \prod_{i=1}^{t} L'(\mathbb{A}^1_{R'_{d_i}}, f_{\Pi_i}; \Psi^{(d_i)}(f(\Pi_i))T^{d_i})$$

où pour chaque $1 \leq i \leq t$, f_{Π_i} est le polynôme local associé à f en Π_i.

4.3. Cas des fonctions de Morse : où l'on retrouve des résultats classiques. Dans la suite on note ρ_K la réduction modulo p, de l'anneau total des fonctions de C vers le corps des fonctions de C_k. Commençons par nous restreindre à certaines fonctions

Définition 4.3. *On dit que f est une fonction de Morse sur C si la différentielle $d\rho_K(f)$ n'admet que des zéros simples (quand tous les points de $(d\rho_K(f))_0$ sont de multiplicité 1), et si f n'a de pôle en aucun point du support de $(d\rho_K(f))_0$.*

Il est aisé de voir qu'une fonction de Morse est (dans la terminologie du chapitre précédent) une série entière restreinte à monôme dominant de degré 2. On sait donc exprimer la somme locale associée à une telle fonction sur la fibre au dessus d'une de ses singularités de façon simple, à l'aide de la somme de Gauss quadratique $\mathscr{G}_q$. La fonction L s'écrit aussi simplement, et on obtient

Théorème 4.2. *Soit f une fonction de Morse sur C ; la fonction $L(C, f; t)$ est de degré $(-1)^{l-1} \deg(d\rho_K(f))_0$, et toutes ses racines réciproques sont des nombres de Weil de poids l.*

Fixons maintenant le diviseur polaire de $\overline{f}$. Pour peu que les ordres polaires soient premiers à p, cela fixe le diviseur polaire de la différentielle $d\overline{f}$, et donc le degré de $(d\overline{f})_0$, c'est à dire le nombre de points critiques (comptés avec leurs multiplicités) puisque la fonction est de Morse. En menant le calcul on trouve le résultat suivant, qui est presque mot pour mot la réécriture du résultat en caractéristique p

Corollaire 4.1. *Soit f une fonction de Morse, telle que les ordres polaires de $\overline{f}$ soient premiers à la caractéristique. Alors si le diviseur polaire de $\rho_K(f)$ est $\sum_{i=1}^{k} n_i P_i^\infty$, la fonction $L(C, f; t)$ est de degré*

$$(-1)^{l-1} \left(2g - 2 + \sum_{i=1}^{k} (n_i + 1) \deg(P_i^\infty) \right),$$

et toutes ses racines réciproques sont des nombres de Weil de poids l.

En conséquence, on a la borne

$$|S_r(C, f)| \leq \left(2g - 2 + \sum_{i=1}^{k} (n_i + 1) \deg(P_i^\infty) \right) q^{\frac{lr}{2}}.$$

5. Conclusion et questions

Hormis le résultat très général de la section 2.1, mais qui ne donne aucune information précise, on a surtout travaillé dans des cas particuliers. Le principe que la somme se concentre en les fibres au dessus des points critiques de la fonction est général, et se démontre sans grande difficulté en dimension supérieure. En découle, comme dans la section 4, la factorisation des fonctions L en produits de facteurs locaux associés à un certain polynôme local sur un espace affine.

C'est à dire que la situation se ramène par des raisonnements locaux à celle de l'espace affine, où elle a été étudiée dans le cadre de la fonction zêta d'Igusa [**16**, Section 4.5]. On trouvera par exemple dans ce texte le degré de la fonction L associée à un polynôme en $n \geq 2$ variables et possédant des points critiques isolés. Il est exprimé à l'aide des valeurs propres de l'action de la monodromie sur les H^{n-1} de chaque fibre en un des points critiques. On l'a retrouvé en dimension 1 comme conséquence de nos calculs de la section 3. Il reste les questions suivantes

Questions. *i/* Que peut on dire (dans le cas de points critiques isolés) des racines et des pôles réciproques de la fonction L sur l'espace affine de dimension ≥ 2.

ii/ Que se passe-t-il quand les points critiques ne sont plus isolés ?

Il semble que pour la question *i/*, les nombres de Weil puissent s'exprimer, pour l assez grand, à l'aide des racines et des pôles réciproques des fonctions L associées à des polynômes homogènes (sur k) de degré l'ordre du point critique. En général, il serait intéressant de transposer des questions dans le cadre des conjectures d'Igusa sur les majorations uniformes de sommes de caractères associées à des polynômes en plusieurs variables [**16**, Corollary 1.4.5], qui donnent des résultats en termes de résolution des singularités, qu'on doit pouvoir réinterpréter.

Mais la géométrie du schéma X semble aussi prendre une part importante. Dans le cas des courbes il est remarquable qu'en recollant ces informations locales, on retombe sur la même information globale. Le théorème 4.2, regardé sous l'éclairage de la section 2.1 donne envie de répondre par l'affirmative aux questions suivantes

Questions. *i/* Pour f une fonction de Morse sur C une courbe lisse sur R, le faisceau ℓ-adique $(\gamma_C f)^*\mathcal{L}_{\psi_l}$ est il pur de poids l ?

ii/ Dans la même situation, peut on comparer les groupes $H^l_c(\mathcal{F}C, (\gamma_C f)^*\mathcal{L}_{\psi_l})$ et $H^1_c(C\otimes k, \rho_K(f)^*\mathcal{L}_{\psi_1})$?

La description particulièrement simple de $\mathcal{F}X$ comme fibré en espaces affines au dessus de $X \otimes k$ peut sans doute aider à la résolution de ces questions, mais elles restent pour l'instant hors de portée de l'auteur...

CHAPITRE 9

Publications de l'auteur

[**AB**] Y. Aubry, R. Blache – On a question related to the Gauss conjecture for function fields, *Journal of Number Theory* **128** (2008), p. 2053–2062.

[**B1**] R. Blache – L-functions of character sums on curves over rings, prépublication.

[**B2**] ———, Polygones de Newton de certaines sommes de caractères et séries de Poincaré, en ligne à l'adresse `http://arxiv.org/abs/0802.3889`.

[**B3**] ———, On certain character sums over p-adic rings and their L-functions, *Mathematische Nachrichten* **180** (2007), p. 1681–1697.

[**B4**] ———, A Stickelberger theorem for p-adic Gauss sums, *Acta Arithmetica* **118** (2005), p. 11–26.

[**B5**] ———, Exponential sums over lifts of points, *Journal of Number Theory* **105** (2004), p. 361–386.

[**B6**] ———, Majorations de sommes exponentielles sur les anneaux de Galois, *Comptes Rendus de l'Académie des Sciences Série I - Mathématiques* **332** (2001), p. 427–430.

[**BCE**] R. Blache, J.-P. Cherdieu, J. Estrada Sarlabous – Some computational aspects of jacobians of curves in the family $y^3 = \gamma x^5 + \delta$ over $\mathbb{F}_q$, *Finite Fields and their Applications* **13** (2007), p. 348–365.

[**BF**] R. Blache, E. Férard – Newton stratification for polynomials : the open stratum, *Journal of Number Theory* **123** (2007), p. 456–472.

[**BF2**] ———, Newton polygons for twisted exponential sums and polynomials $P(x^d)$, en ligne à l'adresse `http://arxiv.org/abs/math/0702502`.

[**BFZ**] R. Blache, E. Férard, H. Zhu – Hodge-Stickelberger polygons for L-functions of exponential sums of $P(x^s)$, *Math. Res. Letters*, **15** (2008), p. 1053–1071.

[**BEP**] R. Blache, J. Estrada Sarlabous, M. Petkova – A geometric interpretation of reduction in the jacobians of C_{ab} curves, *Arithmetic, Geometry and Coding Theory 2005 (AGCT 10)*, Société Mathématique de France.

Bibliographie

[1] A. Adolphson, S. Sperber – On the zeta function of a complete intersection, *Ann. Sc. ENS* **20** (1987), p. 545–556.

[2] _____, Exponential sums and Newton polyhedra : Cohomology and estimates, *Ann. Math.* **130** (1989), p. 367–408.

[3] _____, On twisted exponential sums, *Math. Ann.* **290** (1991), p. 713–726.

[4] _____, Twisted exponential sums and Newton polyhedra, *J. reine angew. Math.* **443** (1993), p. 151–177.

[5] _____, On the zeta function of a complete intersection, *Ann. Sc. ENS* **29** (1996), p. 287–328.

[6] Y. Aubry, R. Blache – On a question related to the Gauss conjecture for function fields, *Journal of Number Theory* **128** (2008), p. 2053–2062.

[7] J. Ax – Zeroes of polynomials over finite fields, *Amer. J. Math.* **86** (1964), p. 255–261.

[8] B. Berndt, R. Evans, K. Williams – *Gauss and Jacobi sums*, Wiley-Interscience, New York, 1998.

[9] E. Bombieri – On exponential sums in finite fields, *Amer. J. Math.* **88** (1966), p. 71–105.

[10] N. Bourbaki – *Algèbre commutative ix*, Hermann, Paris, 1962.

[11] W. Castryk, J. Denef, F. Vercauteren – Computing zeta functions of nondegenerate curves., *Int. Math. Res. Papers* **12** (2006), p. 1–57.

[12] H. Davenport, H. Hasse – Die Nullstellen der Kongruenzzetafunktionen in Gewissen Zyklischen Fällen, *J. Reine Angew. Math.* **172** (1934), p. 151–182.

[13] P. Deligne – La conjecture de Weil : I., *Publ. Math. IHES* **43** (1974), p. 273–307.

[14] _____, Application de la formule des traces aux sommes trigonométriques., *Lecture Notes in Math.* **569** (1977).

[15] _____, La conjecture de Weil : II, *Publ. Math. IHES* **52** (1980), p. 137–252.

[16] J. Denef – Report on Igusa local zeta function, *Séminaire Bourbaki* **33** (1990/91), p. 359–386.

[17] J. Denef, F. Loeser – Weights of exponential sums, intersection cohomology, and Newton polyhedra., *Inv. Math.* **106** (1991), p. 275–294.

[18] J. Denef, F. Vercauteren – Computing zeta functions of C_{ab} curves using Monsky-Washnitzer cohomology., *Finite Fields Appl.* **12** (2006), p. 78–102.

[19] L. Dickson – The analytic representation of substitutions on a power of a prime number with a discussion of the linear group, *Ann. Math.* **11** (1896/97), p. 65–120.

[20] B. Dwork – On the zeta function of a hypersurface., *Publ. Math. IHES* **12** (1962), p. 5–68.

[21] C. Gauss – *Disquitiones arithmeticae*, 1801.

[22] M. Greenberg – Schemata over local rings, *Annals of Mathematics* **73** (1961), p. 624–648.

[23] A. Grothendieck – Formule de Lefschetz et rationalité des fonctions L, *Séminaire Bourbaki, exposé 279*, 1964/65.

[24] C. D. Haessig – L-functions of symmetric powers of cubic exponential sums, Soumis, en ligne à l'adresse `http://arxiv.org/abs/math/0608521`.

[25] M. Henk, J. Richter-Gebert, G. Ziegler – *Handbook of discrete and computational geometry*, CRC Press, 1997.

[26] S. Hong – Newton polygons of L-functions associated with exponential sums of polynomials of degree 4 over finite fields, *Finite Fields Appl.* **7** (2001), p. 205–237.

[27] _____, Newton polygons of L-functions associated with exponential sums of polynomials of degree 4 over finite field, *J. Number Th.* **97** (2002), p. 368–396.

[28] L. Illusie – Ordinarité des intersections complètes générales, *The Grothendieck festschrift*, Progress in Math., vol. 87, Birkhaüser, 1990.

[29] N. Katz – On a theorem of Ax, *Amer. Jour. Math.* **93** (1971).

[30] _____, *Une formule de congruence pour la fonction zêta*, Lecture Notes in Math., vol. 340, Springer, 1973.

[31] _____, Slope filtration of F-crystals, *Astérisque* **63** (1979), p. 113–164.

[32] _____, Sommes exponentielles, *Astérisque* **79** (1980).

[33] _____, *Differential equations and exponential sums*, Graduate Texts in Mathematics, vol. 58, Princeton University Press, 1984.

[34] ———, Monodromy groups attached to families of exponential sums, *Duke Math. Jour.* **54** (1987), p. 41–56.

[35] ———, Notes on G2, determinants, and equidistribution, *Finite Fields Appl.* **10** (2004), p. 221–269.

[36] K. Kedlaya – Counting points on hyperelliptic curves using Washnitzer-Monsky cohomology, *J. Ramahujan Math. Soc.* **16** (2001), p. 323–338.

[37] N. Koblitz – p-adic variation of the zeta function over families of varieties defined over finite fields, *Comp. Math.* **31** (1975), p. 119–218.

[38] R. Kottwitz – Isocrystals with additional structure, *Compos. Math.* **56** (1985), p. 201–220.

[39] A. Kouchnirenko – Polyèdres de Newton et nombres de Milnor, *Inv. Math.* **32** (1976), p. 1–31.

[40] A. Lauder – Counting solutions to equations in many variables over finite fields, *Found. Comp. Math.* **4** (2004), p. 221–267.

[41] A. Lauder, D. Wan – Computing zeta functions of Artin-Schreier curves over finite fields, *LMS J. Comput. Math.* **5** (2002), p. 34–55.

[42] ———, Computing zeta functions of Artin-Schreier curves over finite fields ii, *J. Complexity* **20** (2004), p. 331–349.

[43] H. Li, H. J. Zhu – Zeta functions of totally ramified p-covers of the projective line, *Rend. Sem. Mat. Univ. Padova* **113** (2005), p. 203–225.

[44] W.-C. W. Li – Character sums over p-adic fields, *Jour. Numb. Th.* **74** (1999), p. 181–229.

[45] R. Lidl, H. Niederreiter – *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing company, 1983.

[46] C. Liu – Generic exponential sums associated to Laurent polynomials in one variable, En ligne à l'adresse `http://arxiv.org/abs/0802.0271`.

[47] ———, The L-function of twisted Witt extensions, *J. Number Th.* **125** (2007), p. 267–284.

[48] C. Liu, D. Wan – T-adic L-functions of p-adic exponential sums, En ligne à l'adresse `http://arxiv.org/abs/0802.2589`.

[49] C. Liu, D. Wei – The L-function of Witt coverings, *Math. Z.* **255** (2007), p. 95–115.

[50] B. Mazur – Frobenius and the Hodge filtration, *Bull. Amer. Math. Soc.* **78** (1972), p. 653–667.

[51] L. Miller – The Hasse-Witt matrix of special projective varieties, *Pac. J. Math.* **43** (1972), p. 443–455.

[52] O. Moreno, C.J. Moreno – Improvements of the Chevalley-Warning and Ax-Katz theorems, *Amer. J. Math.* **117** (1995), p. 241–244.

[53] O. Moreno, K.W. Shum, F.N. Castro, P.V. Kumar – Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications, *Proc. Lond. Math. Soc.* **88** (2004), p. 545–564.

[54] M. Rapoport, M. Richartz – On the classification and specialization of F-isocrystals with additional structure, *Comp. Math.* **103** (1996), p. 153–181.

[55] P. Robba – Index of p-adic differential operators III. Applications to twisted exponential sums, *Astérisque* **119-120** (1984), p. 191–266.

[56] ———, Symmetric powers of the p-adic Bessel equation, *J. Reine. Angew. Math.* **366** (1986), p. 194–220.

[57] ———, Une introduction naïve aux cohomologies de Dwork, *Mémoires SMF* **23** (1986), p. 61–105.

[58] J. Scholten, H. J. Zhu – Hyperelliptic curves in characteristic 2, *Int. Math. Res. Not.* **17** (2002), p. 905–917.

[59] ———, Families of supersingular curves in characteristic 2, *Math. Res. Let.* **8** (2002), p. 414–419.

[60] ———, Slope estimates of Artin-Schreier curves, *Comp.Math.* **137** (2003), p. 275–292.

[61] J. P. Serre – Endomorphismes complètement continus des espaces de Banach p-adiques, *Publi. Math. IHES* **12** (1962), p. 69–85.

[62] ———, *Corps locaux*, Hermann, Paris, 1963.

[63] J. Stickelberger – Uber eine Verallgemeinerung der Kreistheilung, *Math. Ann.* **37** (1890), p. 321–367.

[64] G. Van der Geer, M. Van der Vlugt – Reed Müller codes and supersingular curves I, *Comp. Math.* **84** (1992), p. 333–367.

[65] D. Wan – Newton polygons for zeta and L-functions, *Ann. Math.* **137** (1993), p. 249–296.

[66] ———, Variation of p-adic Newton polygons for L-functions of exponential sums, *Asian J. Math.* **8** (2004), p. 427–472.

[67] E. Warning – Bemerkung zur Verstehenden Arbeit von Herr Chevalley, *Abh. Math. Sem. Univ. Hamburg* **11** (1936), p. 249–296.

[68] A. Weil – On some exponential sums, *Proc. Nat. Acad. Sci. USA* **34** (1948), p. 204–207.

[69] R. Yang – Newton polygons of L-functions of polynomials of the form $x^d + \lambda x$, *Finite Fields Appl.* **9** (2003), p. 59–88.

[70] H. J. Zhu – p-adic variation of L-functions of one variable exponential sums, i., *Amer. J. Math.* **125** (2003), p. 219–233.

[71] ———, Asymptotic variation of L-functions of one-variable exponential sums, *J. Reine Angew. Math.* **572** (2004), p. 219–233.

[72] ———, L-functions of exponential sums over one dimensional affinoids : Newton over Hodge, *Int. Math. Res. Not.* **30** (2004), p. 1529–1550.

[73] ———, Some families of supersingular curves in characteristic > 2, En ligne à l'adresse `http://arxiv.org/abs/0809.0104`.