Un Nouveau Point de Repère dans la Théorie des Formes Automorphes

Robert P. Langlands*

Verweilung, auch am Vertrautesten nicht,
ist uns gegeben; aus den erfüllten
Bildern stürzt der Geist zu plötzlich zu füllenden;

Rainer Maria Rilke "An Hölderlin"

Introduction. Ceux qui connaissent l'auteur et ses écrits, comme par exemple [P] et [W], savent que la notion de fonctorialité et les conjectures rattachées à celle-ci ont été introduites – en suivant ce que Artin avait fait pour un ensemble plus restreint de fonctions – pour aborder le problème de la prolongation analytique générale des fonctions L-automorphes. Ils savent en plus que je suis d'avis que seules les méthodes basées sur la formule des traces pourront aller au fond des problèmes. Il n'en reste pas moins que malgré de récents progrès importants sur le lemme fondamental et la formule des traces nous sommes bien loin de notre but.

Dans l'article [BE] j'ai essayé de dépasser les limites traditionelles, donc la comparaison de deux formules des traces, d'habitude dans le cadre de l'endoscopie, soit ordinaire soit tordue, quoique la présence de l'endoscopie ne soit pas toujours explicitement reconnue. On ne trouve dans [BE] que les premiers balbutiements d'une méthode nouvelle qui ne portera guère ses fruits avant longtemps. L'endoscopie et les comparaisons qu'elle suggère s'appuient sur des réflexions purement algébriques. Dans [BE], j'ai proposé en plus qu'avant d'entreprendre des comparaisons, on introduise un passage à la limite dans la formule des traces. Ce passage à la limite entraîne même dans certains cas des plus simples des problèmes analytiques graves et non résolus. Je les ai signalés dans [BE] sans pouvoir en entamer l'étude.

Je continue à y réfléchir et j'ai profité d'un colloque tenu à Toronto à l'occasion du $60^{iéme}$ anniversaire de naissance de James Arthur pour décrire mes conclusions des expériences numériques auxquelles j'ai fait allusion dans [BE] et surtout pour encourager autrui à poursuivre dans cette voie.

Le grand inconvénient de ce passage à la limite est la difficulté des problèmes analytiques qu'il pose; son grand avantage est qu'il nous permet de passer à un nouveau monde, à un paysage tout à fait différent où nous ne sommes plus hantés par les anciens problèmes, mais où nous pouvons aborder des questions nouvelles avec un esprit rafraîchi. Quoique nous restions au pied des mêmes montagnes, nous passons à un autre versant où nous pouvons chercher d'autres chemins.

---

* Au cours de mes réflexions sur les questions soulevées dans cet article, j'ai profité de conversations avec Mark Goresky, Nicolas Katz et Peter Sarnak à Princeton, avec Laurent Lafforgue à l'IHES, et avec Andrew Booker à ces deux endroits. Je leur en suis reconnaissant. Je suis aussi reconnaissant à Claude Levesque qui a lu attentivement la première version du texte. Grâce à ses suggestions nombreuses le style de l'article s'est fortement amélioré.

Dans cet article, je prétends à peu: je reprends tout simplement l'exposé de Toronto avec quelques suppléments. Je décrirai brièvement le nouveau repère auquel le titre fait référence, ensuite je donnerai un précis des conclusions tirées des résultats numériques, et enfin j'expliquerai de quel côté il me semble à présent le plus prometteur d'aborder les questions soulevées. Une connaissance des fondements de la théorie des formes automorphes sera exigée du lecteur.

Les nombres $m_\pi(\rho)$. Une fonction L-automorphe est définie provisoirement par un produit eulérien

$$L(s,\pi,\rho)=\prod_{\mathfrak{p}\notin S}\frac{1}{\det\left(\frac{1-\rho(\mathrm{A}_\mathfrak{p}(\pi))}{\mathrm{Np}^{\mathrm{s}}}\right)}. \tag{1}$$

Ici π est une représentation automorphe d'un groupe G sur un corps global F, qui au début est un corps de nombres, mais qui par la suite est aussi un corps de fonctions sur un corps fini; $\{A_\mathfrak{p}(\pi)\}$ est la classe de Frobenius-Hecke de π à la place $\mathfrak{p}$, et est souvent dite la classe de Satake, alors que ρ est une représentation du groupe ${}^LG$, dit le groupe L attaché à G. L'ensemble S est un ensemble fini qui contient toutes les places infinies et dont le choix précis n'a pas ici d'importance. Tôt ou tard on voudra une définition dans laquelle le produit est pris sur toutes les places finies, mais nous ne sommes pas arrivés à ce point.

À mon avis, la démonstration de la possibilité de prolonger analytiquement toutes ces fonctions passera par la fonctorialité. Cependant, plutôt que d'insister trop sur ce point, nous pouvons nous demander s'il y a éventuellement des conséquences à tirer de ce prolongement analytique, que nous pouvons aborder tout de suite et directement sans attendre une démonstration de la fonctorialité ou de l'existence de ces prolongements Ces conséquences pourraient même nous indiquer la voie à suivre pour trouver les démonstrations convoitées. Je rappelle, par exemple, que selon les conjectures importantes de Arthur ([A]) on devrait pouvoir, en développant la formule des traces et en utilisant un argument par récurrence, partager les représentations automorphes en deux classes: celles pour lesquelles on peut accepter et même s'attendre à ce que la conjecture de Ramanujan soit fausse; celles pour lesquelles toute théorie envisage à présent que la conjecture soit vraie. Pour ces dernières représentations, dites de type Ramanujan, l'ordre $m_\pi(\rho)$ du pôle de la fonction $L(s,\pi,\rho)$ au point $s=1$ a une signification majeure. J'ai proposé dans l'article [BE] qu'on cherche à introduire les nombres $m_\pi(\rho)$ directement par une voie qui évite le prolongement analytique, même si cette voie ne donnait peut-être à prime abord que des nombres réels, pour lesquels il faudrait ensuite démontrer que ce sont en fait des entiers non négatifs.

Plus précisement, j'ai proposé que l'on cherche à établir des formules non pas pour chacun des nombres $m_\pi(\rho)$ séparément, mais pour des sommes de la forme

$$\sum_\pi\prod_{v\in S}\mathrm{tr}\pi_\mathrm{v}(\mathrm{f}_\mathrm{v})\mathrm{m}_\pi(\rho). \tag{2}$$

Dans cette formule l'ensemble S est, comme celui de la formule (1), un ensemble fini de places qui contient toutes les places à l'infini. De plus, pour que la somme soit finie nous fixons un caractère central global unitaire χ

et n'admettons dans la somme que les représentations qui se transforment selon ce caractère et qui sont à la fois non ramifiées en dehors de S et de type Ramanujan. Enfin, à chaque place de S la fonction f est lisse de support compact modulo le centre de $G(F_v)$ et se transforme sous ce centre selon l'inverse de χ_v. Donc $f(zg) = \chi_v^{-1}(z)(g)$ pour z dans le centre. Ayant trouvé, à partir des méthodes de la formule des traces, une formule pour les sommes de (2), nous pourrons essayer, en comparant les formules pour divers ρ et divers G, non pas simplement d'établir que les nombres $m_\pi(\rho)$ sont des entiers, mais aussi d'établir la fonctorialité. Il s'agit certainement de problèmes difficiles, mais leur nouveauté nous force à sortir des chemins foulés.

Dans le travail [BE] j'ai essayé d'aborder ces problèmes numériquement. J'ai fait quelques observations encourageantes et les calculs d'Andrew Booker ont confirmé les miens, de sorte que je peux communiquer mes conclusions ici sans trop craindre qu'à cause des défauts de mes codes elles ne soient pas bien fondées. Les conclusions de l'article [BE] étaient cependant moins frappantes que celles des relations (9), (10) et (11) de la présente note et en même temps légèrement faussées par quelques petites erreurs de calculs. Je ne donne que les nouvelles conclusions. Le lecteur qui veut les comparer avec des données numériques est encouragé à consulter Andrew Booker ou à faire lui-même des calculs semblables. Après tout, des résultats numériques aux conclusions théoriques il y a un saut qui ne se fait pas sans un brin de foi. Il me semble cependant qu'il serait très utile de pousser plus loin ce genre de calculs, d'abord pour mieux se convaincre du bien-fondé de ce que j'affirme, ensuite pour mieux comprendre des cas plus généraux.

Conclusions des calculs numériques. Je rappelle le cadre de [BE]. Il s'agit d'arriver en substituant des fonctions convenables dans la formule des traces à une expression dont la limite est censée être la somme de (2). Je passe au cas le plus simple. Le corps F est $\mathbb{Q}$, le groupe G est $GL(2)$, l'ensemble S ne contient que la place infinie, et le caractère central est identiquement 1. Le groupe ${}^LG$ est $GL(2,\mathbb{C})$ et la représentation ρ est la représentation irréductible sur l'espace de tenseurs symétriques de degré m. Sa dimension est donc $m+1$. Il y a plusieurs contributions à la formule habituelle des traces: la contribution parabolique et la contribution elliptique. La contribution elliptique est la contribution principale, mais il faut toutefois soustraire la contribution de la représentation triviale, car elle n'est pas de type Ramanujan.

Dans l'article [BE] je suis arrivé à une somme sur $n > 0$ et $f > 0$, $n, f \in \mathbb{Z}$, $(n,f) = 1$, de l'expression de sa formule (70). Je la récris ici. Soit $N = \pm 4p^m$, avec p un nombre premier, m un entier positif, et soit $\theta_{n,f}(p,m)$ l'expression définie par

$$2\left\{\sum \left(\frac{D}{nf'}\right)\varphi(D,nf')\frac{\psi_\pm(x_r)}{\sqrt{|N|}}\Phi - \sqrt{|N|}\sum_\pm \epsilon_{n,f}(N)\int \psi_\pm(x)\sqrt{|x^2 \mp 1|}dx\right\}, \tag{3}$$

où

$$\Phi = \Phi_f = \prod_{q|f}\left(1 - \frac{\left(\frac{D}{q}\right)}{q}\right).$$

La première des sommes se fait sur des entiers positifs f' dont tous les diviseurs sont aussi des diviseurs de f, sur les signes $+1$ et -1, et sur $r \in \mathbb{Z}$ tels que $f|s$ où l'entier positif s est défini par la condition $r^2 - N = s^2 D$, D étant un discrimant fondamental. Nous rappelons brièvement les notations de [BE]. La fonction $\varphi(x,k)$ qui intervient dans l'équation fonctionnelle approximative dépend d'un nombre réel x et d'un entier positif k:

$$\varphi(x,k) = \begin{cases} \pi \mathrm{erfc}\left(\frac{\mathrm{k}\sqrt{\pi}}{\sqrt{|\mathrm{x}|}}\right) + \frac{\sqrt{|\mathrm{x}|}}{\mathrm{k}}\exp\left(\frac{-\pi \mathrm{k}^2}{|\mathrm{x}|}\right) & \text{si} \quad \mathrm{x} < 0, \\ \frac{\sqrt{x}}{k}\mathrm{erfc}\left(\frac{\mathrm{k}\sqrt{\pi}}{\sqrt{\mathrm{x}}}\right) + \mathrm{E}_1\left(\frac{\pi \mathrm{k}^2}{\mathrm{x}}\right) & \text{si} \quad \mathrm{x} > 0. \end{cases}$$

où

$$E_1(y) = -\gamma - \ln(y) + \sum_{j \geq 1}(-1)^{j-1}\frac{y^j}{j!j},$$

γ étant la constante d'Euler.

Le nombre réel $x_r = r/\sqrt{|N|}$. Le symbole

$$\left(\frac{a}{b}\right)$$

est celui de Kronecker. La fonction $\epsilon_{n,f}(N)$ est élémentaire, mais désagréable à exprimer explicitement et fastidieuse à définir précisément. Elle est égale à une valeur moyenne approximative de

$$\frac{f}{sn}\left(\frac{(r^2 - N)f^2/s^2)}{n}\right).$$

Elle est rendue nécessaire par la décomposition de la formule des traces en somme sur n et f, une décomposition suggérée par l'analyse et non pas par l'algèbre. La décomposition exige une décomposition pareille de la contribution à la trace de la représentation triviale, cette contribution devant être enlevée.

La formule (3) provient en effet de la somme sur le spectre discret des traces de $\pi(f)$, f étant une fonction produit sur $GL(2,\mathbb{A})$: $f = \prod_v f_v$ avec f_∞ positif homogène. Les fonctions $\psi_\pm$ sont les intégrales orbitales de f_∞ évaluées à une classe γ de norme ± 1 et de trace $2x$. Elles sont de support compact; ψ_- est lisse et ψ_+ est lisse sauf peut-être en ± 1 où son comportement est prescrit. À nos fins elles sont à peu près des fonctions lisses arbitraires à support compact. Les problèmes analytiques reliés à (3) doivent être résolus dans cette généralité sans s'occuper de la provenance des fonctions $\psi_\pm$, donc sans référence à la formule des traces.

Il sera alors utile par la suite de remplacer les fonctions $\psi_\pm(x)$ par $\psi_\pm(x)\sqrt{x^2 \mp 1} = \eta_\pm(x)$, aussi une fonction à toutes fins utiles arbitraire. Pour D grand la fonction $\varphi(D,n)$ se comporte comme $\sqrt{|D|}/n = \sqrt{|r^2 - N|}/sn$, de sorte que la première somme de (3) peut être remplacée par

$$2\sqrt{|N|}\sum \frac{f}{snf'}\left(\frac{D}{nf'}\right)\psi_\pm(x_r)\frac{\sqrt{|x_r \mp 1|}}{\sqrt{|N|}}\Phi$$

ou

$$2\sqrt{|N|}\sum \frac{f}{snf'}\left(\frac{D}{nf'}\right)\frac{\eta_\pm(x_r)}{\sqrt{|N|}}\Phi = 2\sum \frac{f}{sn}\left(\frac{D}{n}\right)\eta_\pm(x_r).$$

La somme à gauche porte toujours sur r, f' et $\pm$ et on exige toujours de r que $f|s$, s étant défini par $r^2 - N = s^2 D$. À droite il n'y plus de somme sur f'. Si $f = n = 1$, cette dernière expression n'est que

$$2\sum \frac{1}{s}\eta_\pm(x_r). \tag{4}$$

Il n'y a plus de condition sur r mais $1/s$ intervient dans la somme. Le deuxième terme de la différence devient

$$2\sqrt{|N|}\sum_\pm \epsilon_{1,1}(N)\int \eta_\pm(x)dx. \tag{5}$$

Je souligne encore que la formule (3) est la différence de deux termes dont le premier est donné par la formule des traces et dont le deuxième est, au moins après avoir sommé sur n et f, la contribution de la représentation triviale à la formule des traces. Elle doit être soustraite de la formule car la représentation triviale n'est pas de type Ramanujan. Celles qui restent et qui contribuent à la formule des traces sont de type Ramanujan. Nous nous attendons donc à ce que pour elles la conjecture de Ramanujan soit valable, mais cette hypothèse n'intervient pas dans les arguments. Soit

$$\Theta(p,m) = \sum_{n,f}\theta_{n,f}(p,m).$$

Puisque nous comprenons bien les fonctions L de Hecke pour $GL(2)$, nous pouvons certainement vérifier sans trop de peine que pour $m = 1$ la limite

$$\lim_{X\to\infty}\Xi(m,X) = \lim_{X\to\infty}\frac{\sum_{p<X}\ln(p)\Theta(p,m)}{X} \tag{6}$$

existe. Elle ne sera pas égale à (2) car il y a des contributions supplémentaires de termes paraboliques faciles à calculer. Elle sera égale toutefois à une expression assez simple dont nous comprendrons mieux la forme par la suite. Il ne s'agit pas toutefois d'exploiter des particularités du cas $m = 1$ mais de trouver une méthode uniforme qui ne fonctionne pas seulement pour $m = 1$ mais qui s'étend à tout m. C'est une nouvelle terre à défricher.

Cependant, pour la plupart des calculs je me suis restreint au cas $m = 1$ car même pour $m = 2$ la condition $p^m < X$ admet bien moins de nombres premiers que la condition $p < X$. Laissons alors tomber le symbole m et écrivons $\theta_{n,f}(p)$, $\Theta(p)$ et $\Xi(X)$. Puisque toute idée me manquait, j'avais par désespérance récrit le quotient de (6) comme

$$\sum_{n,f}\frac{\sum_{p<X}\ln(p)\theta_{n,f}(p)}{X}, \tag{7}$$

simplement parce que je me disais que

$$\xi_{n,f}(X) = \frac{\sum_{p<X}\ln(p)\theta_{n,f}(p)}{X} \tag{8}$$

est plus simple que (6). Dans (6) j'avais utilisé l'équation fonctionnelle approximative pour écarter les nombres de classes des extensions $\mathbb{Q}(\sqrt{D})$ qui interviennent dans la formule des traces mais ces extensions restaient implicites dans la somme sur n. Par contre, dans (8) elles sont absentes. Mais même si l'on réussit à traiter (8), il faut ensuite démontrer que l'ordre de la sommation peut être modifié comme dans (8) sans changer la limite, ce qui n'est guère évident.

Dans toutes ces expressions il y a les intégrales orbitales des fonctions f_v. Je me suis permis de ne considérer que le cas où l'ensemble S contient seulement la place ∞. Si des ensembles S plus grands étaient admis, peu serait changé. La somme se ferait non pas sur des r entiers mais sur des r à dénominateurs donnés. Donc les sommes de (6), (7) et (8) sont des distributions invariantes sur f_∞ et, par conséquent, des distributions sur l'intégrale orbitale de f_∞, donc sur la paire $\psi_\pm$, une fonction sur la réunion de deux lignes droites ou deux fonctions ψ_+ et ψ_- sur $\mathbb{R}$. On peut caractériser ces fonctions, mais pour nos fins numériques cela n'est guère nécessaire. Elles sont toutes les deux des fonctions à support compact, lisses sauf peut-être en ± 1 sur la ligne $+$. Les distributions définies par les sommes sont données par des mesures concentrées aux points $r/\sqrt{|N|}$, $r \in \mathbb{Z}$, et au premier abord on peut supposer que les limites sont aussi des mesures.

Avant de décrire mes observations, je rappelle qu'il y a quelques distributions invariantes sur les f_∞ qui sont d'une importance capitale pour la correspondance locale. Ce sont les caractères des représentations irréductibles admissibles de $GL(2,\mathbb{R})$ rattachées aux représentations de dimension deux du groupe de Galois $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Il y a trois représentations de ce genre. Comme distributions sur $\psi_\pm$ leurs caractères sont 0 sur l'intervalle $(-1,1)$ de la ligne $+$, qui correspond aux classes de conjugaison elliptiques. Sur la ligne $-$ et sur les deux intervalles $(-\infty,-1)$, $(1,\infty)$ de la ligne $+$, qui sont les ensembles correspondant aux classes de conjugaison hyperboliques, ces distributions sont des multiples constants cdx de la mesure de Lebesgue dx. Cela permet trois caractères linéairement indépendants, et il y en a effectivement trois car il y a trois représentations différentes de $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ dans $GL(2,\mathbb{C})$. Pour décrire un de ces caractères on a besoin de trois constantes, une pour la ligne $-$ et une pour chacun des deux intervalles hyperboliques sur la ligne $+$. Elles sont données dans [BE]. Par exemple, pour la représentation triviale du groupe de Galois, toutes ces constantes sont égales à 8. Cette mesure, que nous notons γ, interviendra par la suite. En effet, puisque la plus grosse irrégularité des nombres $m_\pi(\rho)$ est censée apparaître pour les π rattachées aux représentations de dimension deux du groupe de Galois, il faut attendre que ces trois caractères figurent d'une façon importante dans la limite (6). On les voit déjà dans la contribution parabolique, calculée dans [BE].

Je n'ai examiné que les mesures $\xi_{n,1}(X)$ que je note $\xi_n(X)$. Un examen plus étendu pour plusieurs valeurs de f serait souhaitable. L'espoir naïf que la mesure $\xi_n(X)$ ait une limite lorsque $X \to \infty$ s'avère faux. Il n'en reste pas moins que les expériences numériques suggèrent fortement un comportement frappant auquel je n'avais aucune raison de m'attendre. D'abord

$$\xi_n(X) \sim \alpha_n + \beta_n \ln X, \tag{9}$$

où α_n et β_n sont des mesures. Donc quoique $\xi_n(X)$ ne soit pas borné, sa valeur croît lentement. Par contre, les $\theta_{n,f}(p)$ qui sont fortement irréguliers semblent n'être majorés que par une puissance de p. Remarquons qu'ils sont la différence de deux termes d'ordre $p^{1/2}$. En plus, les termes logarithmiques interviennent déjà, au moins pour m pair, dans la contribution parabolique. Il faudra donc pour m pair que cette contribution soit annulée par une partie de la contribution elliptique. La présence du logarithme dans (9) n'est donc pas trop surprenante.

La relation (9) veut dire que la différence des deux côtés est $o(1)$ lorsque $X \to \infty$. Je ne peux pas affirmer que la somme sur n de ces différences reste $o(1)$ mais je suis tenté de l'espérer.

La conclusion la plus frappante de mes expériences numériques est que

$$\beta_n = b_n dx,$$

où b_n est une constante. De plus, si $n = n_1 n_2^2$ où n_1 est le produit de ν_{n_1} nombres premiers différents, alors il existe une constante c_{n_2} telle que

$$b_n = \frac{(-1)^{\nu_{n_1}}}{n_1} c_{n_2}. \tag{10}$$

L'évidence pour le dénominateur du premier facteur à droite est moins convaincante que celle pour le numérateur. La convergence est lente et les nombres $1/n_1$ sont petits, mais du signe il n'y a pas de doute. Grâce à un théorème important, pour l'histoire et pour la démonstration duquel je cite [N, Th. 5.20], si on fait fi des questions de convergence on a

$$\sum_n b_n = \sum_{n_2} c_{n_2} \sum_{n_1} \frac{(-1)^{\nu_{n_1}}}{n_1} = 0.$$

Le théorème bien connu trouvé dans [N] affirme que la somme intérieure est nulle.

Les résultats numériques pour la mesure α_n sont plus ambigus. Sur l'intervalle $(-1, 1)$ de la ligne $+$, donc pour les classes elliptiques, ils ont une interprétation évidente. La mesure α_n est un multiple constant $a_n dx$ de la mesure de Lebesgue et la constante a_n est de la même forme que b_n,

$$a_n = \frac{(-1)^{\nu_{n_1}}}{n_1} d_{n_2}.$$

On voudrait en plus que

$$\alpha_n = e_n dx + f_n \delta \tag{11}$$

sur les intervalles qui paramétrisent les éléments hyperboliques. Mais je n'ai pas su deviner quelles seront les constantes e_n ni quelle sera la mesure δ. Cependant, les données numériques n'établissent pas avec certitude qu'une formule semblable à (11) soit vraie.

Il serait donc utile de suppléer aux calculs numériques en démontrant des résultats théoriques. Mes tentatives d'entamer les questions de convergence dans [BE] ont été puériles. Elles n'ont révélé que mon manque d'expérience. Bien que les problèmes ne me dépassent pas tout à fait, mes conversations avec des spécialistes de la théorie analytique des nombres m'ont convaincu non seulement que je ne suis pas du tout en état de les aborder à présent mais qu'ils sont difficiles même pour des mathématiciens expérimentés. Les questions soulevées dans [BE] se posent aussi pour les corps de fonctions sur un corps fini et ne sont pas résolues, en autant que je sache, par les travaux de Lafforgue. Il est par conséquent tout à fait légitime de commencer avec eux et même avec les corps de fonctions rationnelles sur $\mathbb{F}_q$, où q est une puissance d'un nombre premier impair donné.

Corps de fonctions rationnelles. L'expression (70) de [BE] est une différence. Le second terme de la différence est évidemment de l'ordre de $\sqrt{|N|}$. Le premier terme est plus ou moins une somme de Riemann dont l'intégrale du second terme est une approximation. Il y a toutefois un hic. Dans l'expression (70) de [BE], il faut passer, par exemple dans $\varphi(D, nf')$, de $r^2 - N$ à D, $Ds^2 = r^2 - N$. L'entier s est à un facteur 2 près le plus grand entier qui divise $r^2 - N$. Pour $s \ll \sqrt{|N|}$ les nombres $r/\sqrt{|N|}$, r étant tel que $s^2|r^2 - N$, sont répartis uniformément, mais pour $s \sim \sqrt{|N|}$ cela n'est plus le cas. Par conséquent, la différence peut être assez grosse. Elle devient d'un ordre modeste seulement en prenant une moyenne pondérée sur N. Dans [BE], $N = \pm 4p^m$ avec $m > 0$ fixé et p premier, et le poids est $\ln(p)$. Rappelons que dans les faits $m + 1 = \deg\rho$. On prend la moyenne sur $p \leq X$, où $X \to \infty$. Mais jusqu'à présent l'évidence que cette moyenne se comporte bien est d'une part fondamentalement numérique et ne correspond d'autre part qu'au cas où $m = 1$.

Quoique le cadre formel reste pareil pour les corps de fonctions, en particulier pour un corps de fonctions rationnelles, les problèmes analytiques de [BE] se ramènent à des questions de comptage des points sur des variétés algébriques, plus précisément à la détermination de la cardinalité d'un sous-ensemble de ces points. Cela donne un tout autre goût au problème, et plutôt que de rappeler les arguments semblables à ceux qui mènent à la formule (70) de [BE], ou même à la formule qui en résulte, je veux expliquer des cas particuliers et concrets des questions qui se posent pour un corps de fonctions rationnelles. À mon avis, tant que l'on reste dans le cadre du corps des fonctions rationnelles ces cas particuliers sont aussi difficiles que le cas général. Cependant, pour un corps de fonctions quelconque, dont la fonction zêta aura des zéros non triviaux, il faut s'attendre à des problèmes supplémentaires.

Puisque nous examinons maintenant un corps de fonctions, j'utilise une notation différente, suggérée toutefois par celle de [BE]. Soient δ un entier (ou un demi-entier mais je ne considère ici que le cas où δ est entier) positif, N un polynôme unitaire de degré égal à 2δ, et $a \neq 0$ dans $\mathbb{F}_q$. Examinons d'abord la différence entre la somme

$$\frac{1}{q}\sum_R 1, \tag{12}$$

dans laquelle R parcourt l'ensemble des polynômes de degré au plus δ et tels que $R^2 - aN$ n'est pas divisible par le carré d'un polynôme non constant, et

$$q^\delta \prod_Q \left(1 - \frac{1 + \left(\frac{aN}{Q}\right)}{|Q|^2}\right), \qquad 13$$

où le produit se fait sur les polynômes unitaires premiers Q, où $|Q| = q^{\deg Q}$.

Cette différence est semblable à la différence entre (4) et (5), sauf que le corps de base est un corps de fonctions, et présente les mêmes problèmes. Nous avons encore pris $n = f = 1$ de sorte que le symbole de Kronecker est remplacé par 1. Le nombre N est remplacé par le polynôme aN et r par R. On ne peut plus normaliser les déterminants et les intégrales orbitales de la même façon car f_∞ devient une fonction sur $GL(2, F)$, F étant un corps de séries formelles sur $\mathbb{F}_q$. Nous supposons plutôt que les déterminants sont des polynômes de degré 2δ et que la fonction η qui remplace $\eta_\pm$ n'est que la fonction caractéristique de l'ensemble $|R^2/N| \leq 1$, donc une fonction lisse à support compact de R et de N, dont la valeur absolue $q^{-2\delta}$ est donnée. L'entier s est maintenant la valeur absolue $|S| = q^{\deg S}$ d'un polynôme S. La somme (12) est semblable à (4). La seule différence est que le facteur 2 n'est plus là et la somme est restreinte à $s = 1$ constant. L'équation fonctionnelle approximative se simplifie et $\varphi(D, nf')$ est remplacé par $1/q$. L'expression (13) contient q^δ qui remplace $\sqrt{|N|}$ et le produit sur Q remplace le facteur $\epsilon_{1,1}(N)$ de (5). Ce nouveau facteur est défini par le même genre de moyenne approximative que $\epsilon_{n,f}$ sauf que la moyenne est prise sur les r tels que S est une constante, c'est à dire $s = 1$. Évidemment cette nouvelle différence pose pour un corps de fonctions le même genre de difficulté que poserait (3) lui-même

Le comportement de la différence entre (12) et (13) lorsque N varie est irrégulier et pour avoir un comportement régulier il faudra passer à une moyenne, par exemple la somme des différences pour tout polynôme $N = P$ premier unitaire d'un degré donné 2δ et tout a, divisé par le nombre de termes dans la somme, ou, plus généralement, pour $N = P^m$, m donné, et $2\delta = m\deg P$. Cette moyenne remplace convenablement les moyennes pondérées

$$\frac{\sum_{p<X} \ln(p)\theta_{n,f}(p)}{X}$$

qui intervenaient pour le corps $\mathbb{Q}$. Maintenant considérons d'emblée la différence elle-même.

La somme (13) est égale à

$$\sum_{k=0}^{\infty} q^\delta \sum_{\deg A = k} (-1)^{\nu_A} \frac{\prod_{Q|A} \left(1 + \left(\frac{aN}{Q}\right)\right)}{q^{2\deg A}}.$$

Le polynôme unitaire A n'a pas de racine multiple et ν_A est le nombre de ses facteurs premiers. La somme (12) s'exprime d'une façon semblable comme

$$\frac{1}{q} \sum_R \sum_{A^2 | R^2 - aN} (-1)^{\nu_A}.$$

Une façon de majorer la différence est de majorer pour chaque k la différence entre

$$\frac{1}{q} \sum_{\deg A = k} \sum_{A^2|R^2-aN} (-1)^{\nu_A} = \frac{1}{q} \sum_{\deg A = k} (-1)^{\nu_A} \sum_{A^2|R^2-aN} 1, \tag{14}$$

la somme portant sur les R tels que $\deg R \leq \delta$, et

$$q^\delta \sum_{\deg A = k} (-1)^{\nu_A} \frac{\prod_{Q|A} \left(1 + \left(\frac{aN}{Q}\right)\right)}{q^{2\deg A}}. \tag{15}$$

Dans les expressions (14) et (15), A est unitaire et n'a pas de diviseur multiple.

Il y a trois intervalles. Il y a l'intervalle à gauche formé de petits k où $2k-1 \leq \delta$; un intervalle intermédiaire où $\delta < 2k-1$ et $k \leq \delta$; et enfin l'intervalle à droite formé de gros k où $k > \delta$. À droite la condition $k > \delta$ entraîne que la somme intérieure de l'expression (14) vaut 0 sauf que si aN est un carré, elle vaut $2(-1)^{\nu_A}$. Puisque

$$\sum_A \frac{(-1)^{\nu_A}}{|A|^s} = \prod_Q \left(1 - \frac{1}{|Q|^s}\right) = \frac{1}{(1-\frac{1}{q^s})\zeta(s)} = 1 - \frac{q}{q^s},$$

la somme sur A vaut alors 0 car $k > 1$ dans l'intervalle à droite. La somme de (15) sur $k > \delta$ est majorée par

$$q^\delta \sum_{\deg A = k > \delta} \frac{2^{\nu_A}}{q^{2k}}.$$

Cette somme est majorée par $O(\delta)$ et $\delta = \ln(q^\delta)/\ln(q) = O(\ln(q^{2\delta}))$. Puisque X devient $|N| = q^{2\delta}$, la contribution de l'intervalle à droite est donc $O(\ln X)$. On pourrait essayer de trouver de meilleures majorations pour la somme, mais celle-ci suffit à présent car elle est compatible avec (9) et je préfère passer aux contributions des deux autres intervalles.

La somme intérieure du côté droit de (14) donne le nombre de points d'une variété sur $\mathbb{F}_q$. Cette variété dépend du polynôme A qui est de degré k, unitaire et sans racine multiple. Examinons d'abord la variété $\mathfrak{B}$ définie dans l'espace affine de dimension $2k+1$ rattaché aux $k+1$ coefficients d'un polynôme S de degré k et aux coefficients de A. Les conditions sur ces $2k+1$ coefficients sont

$$S^2 - aN \equiv 0 \pmod{A}.$$

Pour le moment aN est donné. Pour un A donné il y a $k+1$ conditions sur S. Le nombre de S qui les satisfont pour un A donné est

$$\prod_{Q|A} \left(1 + \left(\frac{aN}{Q}\right)\right),$$

et le nombre de points sur $\mathfrak{B}$ est égal à

$$\sum_{\deg \mathrm{A} = \mathrm{k}} \prod_{Q|A} \left(1 + \left(\frac{aN}{Q}\right)\right).$$

Il y a une application rationnelle qui envoie $\mathfrak{B}$ sur l'espace vectoriel des polynômes de degré $k-1$, à savoir

$$\phi: (S, A) \to T = \frac{aN - S^2}{2A} \pmod{A}.$$

La somme intérieure de droite dans (14) est le nombre de points sur la variété $\mathfrak{V}$ définie par

$$R^2 - aN \equiv 0 \pmod{A^2}.$$

Pour $\delta - 2k + 1 \geq 0$, donc dans l'intervalle à gauche, chacun de ses points s'écrit $R = S + TA + UA^2$, avec un polynôme arbitraire de degré plus petit ou égal à $\delta - 2k$. Donc dans l'intervalle à gauche,

$$|\mathfrak{V}| = q^{\delta-2k+1}|\mathfrak{B}|. \tag{16}$$

En plus, chaque point de $\mathfrak{B}$ contribue le même montant à la somme, c'est-à-dire $q^{\delta-2k+1}$ divisé par q. Le facteur $(-1)^{\nu_A}$ ne posant pas de difficulté, la différence entre (14) et (15) est 0 dans l'intervalle à gauche, qui correspond à la région facile $s \leq \sqrt{|N|}$ dans le cas du corps $\mathbb{Q}$.

Dans l'intervalle intermédiaire, le polynôme U est nécessairement 0 et $\mathfrak{V}$ est l'image réciproque de l'espace vectoriel de dimension $\delta - k + 1$ défini par $\mathrm{degT} \leq \delta - \mathrm{k}$. Il serait peut-être difficile de trouver une formule même approximative pour le nombre de points de $\mathfrak{V}$. En plus il y a le poids $(-1)^{\nu_A}$ pour rendre les calculs plus difficiles. C'est donc dans cet intervalle intermédiaire qu'il faut passer à la moyenne sur $N = aP^m$.

La géométrie. Je ne veux pas cependant poursuivre ce problème à présent. Je ne l'ai pas résolu. Je veux seulement expliquer le genre de questions auxquelles il mène. Considérons l'équation

$$R^2 - DS^2 = aN, \qquad N = P^m. \tag{17}$$

Ici R et S sont des polynômes à coefficients dans $\mathbb{F}_q$, $\mathrm{degR} \leq \delta$, $\mathrm{degD} \leq 2\delta$, et D est un polynôme sans racine multiple. De plus, P est unitaire et $m\mathrm{degP} = 2\delta$. En examinant l'intervalle intermédiaire, pour lequel une moyenne sur P semble incontournable, on est mené au comptage des points sur la variété définie par (17). En fait, on ne veut compter que les points pour lesquels P est premier, mais dans l'espoir un peu incertain que le nombre pour P premier se déduise – au moins approximativement – du nombre pour P arbitraire en divisant par degP, je prends P arbitraire. Cet espoir n'est pas fou, mais insister sur trop de simplicité serait imprudent!

Le polynôme D définit une courbe hyperelliptique C_D, de genre $g = (\mathrm{degD} - 2)/2$ ou $g = (\mathrm{degD} - 1)/2$ selon la parité de degD et avec corps de fonctions engendré par Δ, $\Delta^2 = D$, sur le corps des fonctions rationnelles. Un élément typique de ce corps est $\phi = R + S\Delta$, R et S étant des fonctions rationnelles d'une variable que je note X. La courbe est alors définie par $Y^2 = D(X)$. La norme, $\mathrm{N(R + S\Delta)}$, de $R + S\Delta$ est $R^2 - DS^2$. Si degD est impair, il y a un seul point ∞ à l'infini sur cette courbe; si degD est pair, il y en a deux, ∞_1 et ∞_2. Soit $\bar{\phi} = R - S\Delta$ le conjugué de ϕ, de sorte que

$$\phi + \bar{\phi} = 2R, \qquad \phi - \bar{\phi} = 2S\Delta. \tag{18}$$

Si R et S sont des polynômes, alors ϕ n'a pas de pôle en dehors de l'infini. Si ϕ et, par conséquent, $\bar{\phi}$ n'ont pas de pôle en dehors des points à l'infini, alors ni R ni S n'ont de pôle en dehors de l'infini, car un pôle de S ne peut pas être annulé par un zéro de Δ. Ils sont donc des polynômes. Pour résoudre l'équation (17) en polynômes, nous cherchons par conséquent des fonctions ϕ dont les pôles sont à l'infini. De plus, puisque $m\mathrm{degP} = 2\delta$, si

$\mathrm{degR} \leq 2\delta$ on a $2\mathrm{degS} \leq 2\delta - \mathrm{degD}$. Par conséquent, le pôle de ϕ à l'infini est d'ordre 2δ si degD est impair. Si degD est pair il est de degré δ aux deux infinis. On exigera par la suite d'autres conditions sur S, par exemple qu'il soit de degré 0 ou qu'il soit d'un degré donné. Il s'agit de conditions linéaires sur ϕ à l'infini ou aux deux infinis que je mets de côté dans l'espoir que l'on pourra en tenir compte plus tard.

Nous pouvons donc écrire le diviseur de ϕ sous la forme

$$\begin{cases} m\sum\limits_{i=1}^{a}(x_i,y_i) + \frac{m}{2}\sum\limits_{i=a+1}^{a+b}\{(x_i,y_i)+(x_i,-y_i)\} - 2\delta\infty & \text{si degD est impair,} \\ m\sum\limits_{i=1}^{a}(x_i,y_i) + \frac{m}{2}\sum\limits_{i=a+1}^{a+b}\{(x_i,y_i)+(x_i,-y_i)\} - \delta\infty_1 - \delta\infty_2 & \text{si degD est pair.} \end{cases}$$

Dans les deux cas $a + 2b = \mathrm{degP}$. Les couples de points (x_i, y_i), (x_j, y_j), avec $i, j \leq a$ ne peuvent pas être en involution. Si $b > 0$, alors R et S doivent avoir un facteur premier en commun et, par conséquent, un facteur en commun qui est rationnel sur le corps de base $\mathbb{F}_q$. Si P est premier, il faudra que ce facteur soit P lui-même. Le comptage de ces points se ramène alors à un comptage pareil pour un δ plus petit. Je suppose par conséquent que $b = 0$.

Puisque je suis toujours au début de mes réflexions, je préfère ne considérer que le cas où degD et degP sont pairs. Alors $m|\delta$ et le diviseur de degré 0

$$\sigma = \sum_{i=1}^{a}(x_i, y_i) - \frac{\delta}{m}(\infty_1 + \infty_2) \tag{19}$$

est envoyé sur un point d'ordre m dans la jacobienne J_D.

Lorsque le point D varie, les points d'ordre m sur J_D forment un recouvrement non ramifié et aussi non connexe de l'espace $\tilde{\mathfrak{X}}$ des paramètres D. Cet espace de paramètres et son recouvrement peuvent être étudiés soit sur le corps des nombres complexes, soit sur les corps finis. Sur le corps des nombres complexes, ses propriétés primaires sont topologiques et cohomologiques. En particulier, il y a deux théories de cohomologie pertinentes, la cohomologie de de Rham, définie suivant Grothendieck, et la cohomologie habituelle d'un espace topologique, mettons à support compact, mais pourvue d'une structure de Hodge mixte, ce qui est possible même pour des variétiés qui ne sont pas propres. Sur les corps finis il y a la cohomologie étale qui est pertinente au problème du comptage. Les trois cohomologies sont reliées d'une façon mystérieuse qui me dépasse encore. Je trouve néanmoins utile de me faire guider, en essayant de compter le nombre de solutions des équations (17), par les balises que les idées couramment disponibles sur les motifs mixtes offrent même aux novices.

Les idées de base sont esquissées dans les premières pages de [Ha]. Pour le motif mixte $\tilde{\mathfrak{X}}$ qui nous intéresse présentement, il y a une discussion détaillée de sa structure topologique dans [Br], dont il est très profitable de tenir compte en réfléchissant sur l'équation (19) dans laquelle les paramètres sont un point D de $\tilde{\mathfrak{X}}$, un point d'ordre m de J_D et le diviseur σ. Je suis reconnaisant à Nicholas Katz qui a attiré mon attention non pas seulement sur cet article mais aussi sur une jolie formule de Michael Larsen, que je rappellerai par la suite.

Si nous voulons compter les points d'une variété sur un corps fini, il nous faudra, selon les conjectures de Weil, comprendre les valeurs propres de l'application de Frobenius sur sa cohomologie. Ceci est bien plus facile si ces valeurs propres sont toutes rationnelles et de la forme q^m avec m entier. Autant que j'aie compris, selon les principes qui règlent le passage du type Hodge du motif mixte d'une variété à l'action de son groupe de Galois, cela est plus probable, peut-être même certain, si la cohomologie dans les couches de la structure mixte est toute de type (p,p).

Considérons par exemple $\tilde{\mathfrak{X}}$ qui est le produit de la ligne droite avec le point 0 enlevé et de l'espace $\mathfrak{X}$ des paramètres D unitaires. La cohomologie à support compact, mettons sur $\mathbb{C}$, du premier facteur est $H_!^0 = 0$, $H_!^1 = \mathbb{C} = \mathbb{C}(0)$, de sorte qu'il est de type $(0,0)$, et $H_!^2 = \mathbb{C} = \mathbb{C}(-1)$, de sorte qu'il est de type $(1,1)$. Il n'est alors guère surprenant que le nombre de points sur la ligne droite avec 0 enlevé soit $q-1$. Ceci est une illustration simple des principes sur lesquels je m'appuierai sans encore les comprendre.

Le deuxième facteur $\mathfrak{X}$ est construit en enlevant les hyperplans $x_i = x_j$, $i \neq j$ du produit de $d = \mathrm{degD}$ lignes droites pour obtenir un espace $\mathfrak{Y}$ sur lequel le groupe W des permutations des indices agit, et en prenant ensuite le quotient par ce groupe. Brieskorn, suivant en partie Arnold, calcule la cohomologie de $\mathfrak{X}$ à partir de celle de $\mathfrak{Y}$ et d'une suite spectrale $H^p(W, H^q(\mathfrak{Y}))$ qui aboutit à $H^p(\mathfrak{X})$. Toute torsion mise de côté, le calcul donne des résultats simples. En effet, $H^0(\mathfrak{X},\mathbb{C}) = \mathbb{C}$, et en examinant de plus près les calculs on voit que ce $\mathbb{C}$ est $\mathbb{C}(0)$ et est donc de type $(0,0)$; de plus, $H^1(\mathfrak{X},\mathbb{C}) = \mathbb{C}$, mais ce $\mathbb{C}$ est $\mathbb{C}(-1)$ et est donc de type $(1,1)$. Pour $i > 1$, $H^i(\mathfrak{X},\mathbb{C}) = 0$. Par dualité, $H_!^d(\mathfrak{X},\mathbb{C}) = \mathbb{C}(-d)$, $H_!^{d-1}(\mathfrak{X},\mathbb{C}) = \mathbb{C}(-d+1)$. Cela mène à l'hypothèse que le nombre de points dans $\mathfrak{X}$ à coefficients dans $\mathbb{F}_q$ est égal à $q^d - q^{d-1}$. Le nombre dans $\tilde{\mathfrak{X}}$ sera alors $(q-1)(q^d-q^{d-1})$. En effet, cette observation et les calculs nécessaires ont été faits, indépendamment de toute théorie, par Michael Larsen.

Le nombre de points de $\mathfrak{X}$ dans $\mathbb{F}_q$ est le coefficient de q^{-ds} dans le développement du produit

$$\prod_Q \left(1 + \frac{1}{|Q|^s}\right) = \frac{\prod_Q \left(1 - 1|Q|^{2s}\right)}{\prod_Q \left(1 - \frac{1}{|Q|^s}\right)} = \frac{1 - \frac{1}{q^s}}{1 - \frac{1}{q^{2s}} \frac{\zeta(s)}{\zeta(2s)}}.$$

Dans le produit, Q parcourt l'ensemble des polynômes premiers unitaires et la fonction ζ est celle du corps des fonctions rationnelles. Elle est bien connue et se calcule facilement. Nous obtenons alors

$$\frac{1 - \frac{1}{q^s}}{1 - \frac{1}{q^{2s}}} \frac{\zeta(s)}{\zeta(2s)} = \frac{1 - \frac{q}{q^{2s}}}{1 - \frac{q}{q^s}} = 1 + \frac{q}{q^s} + \sum_{k=1}^{\infty} \frac{q^k - q^{k-1}}{q^{ks}}.$$

Les cas $d = 0$ et $d = 1$ sont exceptionnels, et ce, des deux côtés, car pour $d = 0$, $\mathfrak{X}$ se réduit à un seul point et pour $d = 1$, c'est la ligne droite. Donc la comparaison est toujours valable.

Si on croit aux principes suggérés par cette comparaison, on trouve sage de chercher à comprendre la structure topologique de l'ensemble des solutions de (19) en polynômes à coefficients complexes avant de passer au calcul du nombre de ses solutions en polynômes à coefficients dans $\mathbb{F}_q$. Nous avons vu qu'à chaque diviseur σ

sur C_D de la forme (19) qui est envoyé sur un point μ d'ordre m dans la jacobienne J_D est rattachée une solution $\phi = R + S\Delta$ de (17), définie à un multiple non nul près, telle que le diviseur des zéros et pôles de ϕ est $m\sigma$. C'est donc l'équation

$$\sigma \to \mu, \qquad m\mu = 0, \tag{20}$$

où σ est un diviseur de la forme (19) et $\mu \in J_D$ avec $D \in \tilde{\mathfrak{X}}$, que nous étudions.

Cette équation se résout en deux étapes, d'abord en trouvant les points d'ordre m et ensuite en trouvant les σ. Pour un μ donné, les σ forment un espace projectif et les ϕ un espace vectoriel. Donc pour compter le nombre de ϕ ou le nombre de σ, le premier nombre étant $q-1$ fois le deuxième, pour un μ donné il suffit de calculer la dimension de l'espace sous-jacent, qui se calcule à partir de la formule de Riemann-Roch dans laquelle il y a un entier qui peut dépendre de μ.

Si le polynôme P est rationnel sur le corps de base, alors σ l'est aussi. Donc (20) a une solution seulement si μ est rationnel et est par conséquent représenté par un diviseur ν rationnel sur le corps de base et de degré 0. Le diviseur $\sum_{i=1}^{a}(x_i, y_i)$ est alors linéairement équivalent à $\xi = \nu + \delta(\infty_1 + \infty_2)/m$. Quoiqu'il faille tôt ou tard revenir à la possibilité qu'il y ait des couples $(x_i, y_i), (x_j, y_j)$, $i \neq j$, en involution et en tenir compte, la dimension de l'espace projectif des diviseurs $\sum_{i=1}^{a}(x_i, y_i)$ est $dim\, H^0(\xi) - 1$ qui est égal à $a - g + dim\, H^0(\kappa - \xi) = \mathrm{degP} - \mathrm{g} + \mathrm{dim}\, \mathrm{H}^0(\kappa - \xi)$, où κ est un diviseur canonique. Si donc $\mathrm{degP} \geq \mathrm{g}$, l'espace n'est pas vide, mais sa dimension n'est pas tout à fait prévisible. Si en plus

$$dim\, H^0(\kappa - \xi) = 0, \tag{21}$$

donc en particulier si $\mathrm{deg}\xi = \mathrm{degP} = 2\delta/\mathrm{m} > 2\mathrm{g} - 2$, alors $dim\, H^0(\xi) = \mathrm{degP} - (\mathrm{degD} - 2)/2$, degD ayant été supposé pair.

Les deux comptages sont certainement liés, quoique notre comptage n'est plus tout à fait celui fait en développant (14) et (15) en séries alternées, car le quotient de $R^2 - aN$ par S^2 est censé être sans facteur carré tandis que nous n'exigeons en examinant (14) et (15) que la condition $A^2 | (R^2 - aN)$. Si $k = (2\delta - \mathrm{degD})/2$, alors $k \geq \mathrm{degS}$, avec souvent l'égalité, et l'intervalle intermédiaire est approximativement $\delta \geq k \geq \delta/2$ ou $\delta \geq \mathrm{degD} \geq 0$. Pour sa part, la condition $\mathrm{degP} \geq \mathrm{g}$ est $\mathrm{degP} \geq (\mathrm{degD} - 2)/2$ ou $4\delta/m \geq \mathrm{degD} - 2$, tandis que la condition $\mathrm{degP} > 2\mathrm{g} - 2$ est $\mathrm{degP} > \mathrm{degD} - 4$ ou $2\delta/m > \mathrm{degD} - 4$. Par conséquent, pour $m \leq 2$ nous savons non pas seulement que pour chaque μ tel que $m\mu = 0$, il y a une solution σ de (20), mais aussi que la dimension de l'espace projectif ne dépend pas de D si degD est fixé dans l'intervalle intermédiaire. Si $m \leq 4$ nous pouvons seulement affirmer qu'il y a toujours pour un D donné au moins une solution.

Simplement pour vérifier que les chiffres sont approximativement corrects dans les conditions les plus favorables, observons que le nombre de P est approximativement égal à $q^{\mathrm{degP}}/\mathrm{degP}$, le nombre de a égal à $q-1$, et le nombre de D, unitaires ou non, de l'ordre de $q^{\mathrm{degD}+1}$. Le nombre de μ doit être une constante fois ce même nombre. Si $\mathrm{degP} > 2\mathrm{g}-2$, le nombre de σ est $(q^{\mathrm{degP}-\mathrm{g}+1}-1)/(q-1)$ et le nombre moyen de solutions de (20) pour un P donné est de l'ordre

$$q^{\mathrm{degD}+1-\mathrm{g}} = q^{\delta-k+2}.$$

C'est l'ordre prédit par (16), car il faut toujours diviser par q. Observons que les nombres de (16) sont à sommer sur A. C'est de là que provient le facteur q^k supplémentaire.

Le cas $m=2$. En poursuivant l'examen des difficultés rattachées à nos problèmes nous examinons la structure du recouvrement de l'espace $\mathfrak{X}$ défini par les points μ d'ordre m de J_D, $D \in \mathfrak{X}$. Pour $m=1$, ce recouvrement est $\mathfrak{X}$ lui-même mais pour $m=2$ il devient plus intéressant. Même si on n'admet que des points strictement d'ordre 2 il n'est pas connexe. Je suppose toujours que degD est pair, mais exactement les mêmes conclusions sont valables pour degD impair.

Le polynôme D a $\mathrm{degD} = 2\mathrm{g}+2$ racines simples, $f_1, \ldots, f_{2g+2}$, qui sont les points de ramification de la courbe hyperelliptique C_D. Soit z_i le point $(f_i, 0)$ sur la courbe. Pour $i \neq j$ la fonction $(X-f_i)/(X-f_j)$ a $2(z_i - z_j)$ pour diviseur de zéros et pôles. Le point sur la jacobienne défini par $z_i - z_j$ est donc d'ordre deux; en particulier, $z_i - z_j \sim z_j - z_i$. Plus généralement, si A et B sont des sous-ensembles disjoints de $\{z_1, \ldots, z_{2g+2}\}$ et si $|A| = |B|$, alors

$$\chi_{A,B} = \sum_{i\in A} z_i - \sum_{j \in B} z_j$$

définit un point d'ordre deux dans la jacobienne. Si $|A| = g+1$, alors le diviseur de

$$\frac{\prod_{i\in A}(X-f_i)}{\Delta}$$

est $\chi_{A,B}$ de sorte que dans ce cas $\chi_{A,B} \sim 0$.

J'affirme que la collection de points rattachés à ces diviseurs donne tous les points d'ordre deux. Considérons l'ensemble de vecteurs $(m_1, \ldots, m_{2g+2})$ tels que $\sum_{i=1}^{2g+2} m_i = 0$ et divisons-le par les multiples entiers de $(1, \ldots, 1, -1, \ldots, -1)$, où il y a autant de -1 que de $+1$. On obtient un $\mathbb{Z}$-module M libre de rang $2g$. Alors $M/2M$ est un espace vectoriel de dimension $2g$ sur $\mathbb{F}_2$ et l'application

$$(m_1, \ldots, m_{2g+2}) \to \sum m_i z_i \to J_D$$

l'envoie dans l'ensemble des points d'ordre deux sur la jacobienne. Si elle est injective elle est aussi surjective.

Supposons qu'elle ne soit pas injective. Alors après avoir modifié la numérotation, un point dans le noyau s'écrit

$$(1, \ldots, 1, 0, \ldots, 0, -n), \tag{22}$$

avec n coordonnées 1. L'entier n n'est pas $2g+1$ car alors ce point serait égal à

$$(0,\ldots,0,2,-2) + (0,\ldots,0,2,0,-2) + \ldots + (0,\ldots,0,2,0,\ldots,0,-2) + (1,\ldots,1,-1,\ldots,-1),$$

avec le 2 à la position $g+2$ dans le vecteur pénultième. Ce vecteur est cependant zéro. Si une fonction dont le diviseur est l'image du vecteur (22) est écrite en fonction de $X' = X - f_{2g+2}$ et Δ, alors elle est de la forme $R(X') + S(X')\Delta$ avec $\mathrm{2degR} \leq \mathrm{n} \leq \mathrm{2g}$, $\mathrm{2degS} \leq \mathrm{2g} - \mathrm{degD} + 1$ de sorte que $S = 0$ et tous les zéros de R sont aux points $z_1, \ldots, z_n$, mais ils sont alors des zéros d'ordre pair, ce qui est impossible.

La structure du recouvrement défini par les points d'ordre deux devient alors plus évidente. Deux couples de diviseurs (A, B), (A', B') avec $|A| = |B| = |A'| = |B'|$, $|A \cap B| = |A' \cap B'| = 0$ et $|A \cup B| \leq g+1$ définissent le même point d'ordre deux sur la jacobienne si et seulement si $|A| = |A'|$, $|B| = |B'|$ et en plus $A \cup B = A' \cup B'$ pour $|A| + |B| < g+1$ mais $A \cup B$ égal à $A' \cup B'$ ou à son complément si $|A| + |B| = g+1$. Ces réflexions devront nous permettre de calculer soit le nombre de points sur le recouvrement, soit la structure de sa cohomologie au sens des structures de Hodge mixtes.

Pour compter il faudra d'abord observer que le point sur la jacobienne défini par (A, B) est rationnel pour $|A| + |B| < g+1$ si et seulement si le polynôme

$$\prod_{i \in A \cup B} (X - f_i)$$

est à coefficients rationnels, alors que pour $|A| + |B| = g+1$ il est rationnel si et seulement si les coefficients des deux polynômes

$$\prod_{i \in A \cup B} (X - f_i), \qquad \prod_{i \notin A \cup B} (X - f_i),$$

appartiennent à la même extension quadratique dans laquelle les deux polynômes sont conjugués. En principe, le comptage de ces polynômes se réduit à un problème tout à fait combinatoire. Observons à titre d'exemple que pour $g = 1$, il y a une seule possibilité pour $|A \cup B| = 0$ et il y a trois possibilités pour $|A \cup B| = 2$, chaque réunion étant équivalente à son complément. Pour tout g, les diverses composantes du recouvrement correspondent à un choix de $n = |A \cup B|$, et les D au-dessus desquels il y a des points rationnels dans cette composante sont les D qui ont un facteur rationnel sur $\mathbb{F}_q$ de degré n. Des facteurs rationnels différents permettent souvent l'existence de plusieurs diviseurs d'ordre m au-dessus du D donné. De toute façon, le comptage des μ au-dessus de D, et le comptage des D factorisables est certainement un problème combinatoire en principe élémentaire.

Du point de vue topologique et si on met le coefficient du terme de plus haut degré de D de côté, le recouvrement est une réunion de recouvrements connexes, dont chacun est un espace fibré défini à partir de la fibration $\mathfrak{Y} \to \mathfrak{X}$ à groupe W. L'ensemble des sous-ensembles de $\{1, \ldots, 2g+2\}$ ayant un nombre n donné d'éléments avec $n \leq g+1$, et identifiés à leurs compléments si $n = g+1$, est un ensemble F sur lequel le groupe W agit. Toute composante connexe du recouvrement est de la forme $\mathfrak{Y} \times_W F \to \mathfrak{X}$. Apparemment, selon les principes bien connus de la topologie et des espaces homogènes, sa cohomologie, et même sa structure de Hodge mixte, se calculent à partir d'une suite spectrale qui commence avec

$$H^p(W, H^q(\mathfrak{Y} \times F)).$$

Grâce à la description dans [Br] de la cohomologie de $\mathfrak{Y}$, il semble s'agir d'un problème combinatoire, mais je ne l'ai pas encore abordé.

Dans le cas particulier où $m = 2$, la dimension (de l'espace projectif) des solutions de (20) pour un D et un μ donnés se calcule explicitement. Nous continuons à supposer que degD et $a = 2r$ sont pairs. L'image de $\chi_{A,B}$ soit μ. Le quotient $\delta/m = r$ est entier et

$$\sum_{i=1}^{a}(x_i, y_i) - r\infty_1 - r\infty_2 \sim \chi_{A,B} = \sum_{i=1}^{\alpha} z_i - \sum_{i=\alpha+1}^{2\alpha} z_i, \qquad \alpha = |A| = |B|. \tag{23}$$

Le diviseur à gauche est censé être rationnel sur le corps de base, de sorte que le diviseur à droite doit avoir une image rationnelle dans la jacobienne.

Avant de continuer il y a une petite observation à faire. Si l'image de $\chi_{A,B}$ dans la jacobienne est rationnelle de sorte que $\chi_{A,B}$ et $s\chi_{A,B}$ sont linéairement équivalents pour n'importe quel élément du groupe de Galois, alors il y a un cocycle galoisien $s \to h_s$ à valeurs dans l'ensemble des fonctions rationnelles tel que $s\chi_{A,B} - \chi_{A,B} = (h_s)$ pour tout s. Alors si f est une fonction dont le diviseur est la différence des deux côtés de (23), on aura $sf/f = h_s$ à une constante près. Grâce au théorème 90 de Hilbert cette constante peut être supposée égale à 1. Donc la structure rationnelle naturelle sur l'espace vectoriel des solutions est $s: \ f \to h_s s(f)$.

Il est plus convenable de mettre l'équivalence (23) sous la forme

$$\sum_{i=1}^{a}(x_i, y_i) + \sum_{i=\alpha+1}^{2\alpha} z_i \sim \sum_{i=1}^{\alpha} z_i + r\infty_1 + r\infty_2. \tag{24}$$

Une fonction $R(X) + S(X)\Delta$, dont le diviseur des zéros est le diviseur à gauche et le diviseur des pôles est le diviseur à droite, est le produit de

$$Z = \frac{1}{\prod_{i=1}^{\alpha}(X - f_i)}$$

avec $A + B\Delta$, où A et B sont des polynômes en X. Puisque $R + S\Delta$ est de degré au plus r en ∞_1 et en ∞_2, nous avons $\mathrm{degA} \leq \mathrm{r} + \alpha$ et $\mathrm{degB} \leq \mathrm{r} + \alpha - \mathrm{d}/2$. De plus, $A + B\Delta$ s'annule en $z_1, \ldots, z_\alpha$. Puisque Δ s'annule au premier ordre en ces points, il faut que A s'annule aux points f_i, $1 \leq i \leq \alpha$. Voilà les conditions imposées par les pôles. La dimension des solutions est évidemment

$$r + \alpha + 1 - \alpha + r + \alpha + 1 - g - 1 = 2r + \alpha - g + 1 = p + \alpha - g + 1$$

si $r + \alpha \geq g + 1$ et elle est $r + 1$ si $r + \alpha < g + 1$. Mais il y a des conditions supplémentaires car le polynôme A s'annule en $f_1, \ldots, f_\alpha$. Ces conditions sont indépendantes si $r \geq \alpha$. Si $r < \alpha$ alors ces conditions ne sont satisfaites que pour $A = 0$. Les conditions supplémentaires ne contraignent pas B. La dimension de l'espace des fonctions admissibles est donc

(i) $\quad 0 \quad$ si $\quad r < \alpha$ et $r + \alpha < g + 1$,

(ii) $\quad r+\alpha-g \quad$ si $\quad r<\alpha$ et $r+\alpha \geq g+1$,

(iii) $\quad r-\alpha+1 \quad$ si $\quad r \geq \alpha$ et $r+\alpha<g+1$,

(iv) $\quad r+\alpha+1+r+\alpha-g=2r-g+1 \quad$ si $\quad r \geq \alpha$ et $r+\alpha \geq g+1$.

Rappelons que selon le théorème de Riemann-Roch il y a au moins deux valeurs de $a=2r$ pour lesquelles le comportement de la dimension des solutions de (20) change. Ce sont $a=g$ et $a=2g-2$. Puisque $\alpha \leq g$, les conditions en (i) entraînent que $a<g$ mais les conditions en (ii) n'entraînent pas encore que $a>g$. La dimension des solutions peut apparemment être néanmoins positive parce que $H^0(\kappa-\xi)$ n'est pas 0. Sous les conditions en (iv) la dimension est $\mathrm{degP}-\mathrm{g}+1$ de sorte que $H^0(\kappa-\xi)=0$. Ces conditions entraînent que $a \geq g+1$, mais non pas que $a \geq 2g-2$. Le théorème de Riemann-Roch donne apparemment des informations limitées dans l'intervalle $g \leq a \leq 2g-2$.

Nous avons posé $k=\delta-\mathrm{degD}/2=\delta-\mathrm{g}-1$ et avons constaté que l'intervalle intermédiaire était plus ou moins donné par $\delta=ma/2=a=2r \geq \mathrm{degD}=2\mathrm{g}+2$, donc $r \geq g+1$. Dès lors, il apparaît que dans l'intervalle intermédiaire, qui selon nos premiers calculs est la seule région difficile, c'est seulement le cas (iv) qui intervient. Curieux!

Les Recouvrements en général. Autant que je sache, pour $m>2$ il n'existe pas de description explicite des points d'ordre m sur les courbes jacobiennes J_D. Je n'aborde donc pas d'emblée le problème général de comptage. Ce qu'il importe de souligner ici, c'est que le premier geste à poser avant de les entamer est de comprendre du point de vue géométrique de [Br] les recouvrements de $\mathfrak{X}$ (et de $\tilde{\mathfrak{X}}$) définis par ces points. Puisque d'un point de vue topologique les D unitaires ne diffèrent guère des D à premiers coefficients arbitraires, nous ne considérerons dans cette section que $\mathfrak{X}$ et des D unitaires.

Selon [Br] et l'article [De] y cité, le recouvrement $\mathfrak{Y}$ de $\mathfrak{X}$ est un espace $K(\pi,1)$ à groupe fondamental le groupe $T(d)$ de tresses colorées et l'espace $\mathfrak{X}$ est un espace ayant comme groupe fondamental le groupe des tresses $S(d)$ avec $d=\mathrm{degD}$, $D \in \tilde{\mathfrak{X}}$. Soit $\mathfrak{Z}_m$ le recouvrement de $\mathfrak{X}$ défini par les points d'ordre m des jacobiennes J_D. Quoique je n'en aie qu'une connaissance superficielle et incomplète, je vais essayer d'expliquer brièvement les principes qui puissent permettre le calcul de la cohomologie de $\mathfrak{Z}_m$ et de sa structure de Hodge mixte. Choisissons un point de base $D_0 \in \mathfrak{X}$ et appelons $S'_m(d)$ le sous-groupe de $S(d)$ qui fixe tout point de l'ensemble F_m des points d'ordre m dans J_{D_0}. Soit $T'_m(d)=T(d)\cap S'_m(d)$. Soit en plus $\mathfrak{X}'_m$ le recouvrement de $\mathfrak{X}$ défini par $S'_m(d)$ et $\mathfrak{Y}'_m$ le recouvrement de $\mathfrak{Y}$ défini par $T'_m(d)$. Il y a alors un diagramme commutatif

$$\begin{array}{ccc}\mathfrak{Y}'_m & \longrightarrow & \mathfrak{Y}\\ \downarrow & & \downarrow\\ \mathfrak{X}'_m & \longrightarrow & \mathfrak{X}.\end{array}$$

Selon les théorèmes généraux de la théorie de l'homotopie ([Hu]), l'espace $\mathfrak{Y}'_m$ est aussi un espace $K(\pi, 1)$ dont le groupe fondamental est le groupe $T'_m(d)$. Son homologie et sa cohomologie sont alors calculées en termes de l'homologie et de la cohomologie du groupe $T'_m(d)$, donc en termes de $H_p(T'_m(d), \mathbb{Z})$ et $H^p(T'_m(d), \mathbb{Z})$. Il faut espérer que les renseignements précis sur $T(d)$ trouvés dans [De] et la description précise de l'action de $S(d)$ sur l'ensemble F_m nous permettront de les calculer.

Le groupe quotient fini $W' = T'_m(d)\backslash S(d)$ agit sur F_m et l'espace $\mathfrak{Z}_m$ est défini comme $\mathfrak{Z}_m = \mathfrak{Y}'_m \times_{W'} F_m$. L'espace $\mathfrak{Z}_m$ est donc le quotient de l'espace $\mathfrak{Z}'_m = \mathfrak{Y}'_m \times F_m$ par l'action du groupe W'. La cohomologie de $\mathfrak{Z}'_m$ se calcule immédiatement à partir de celle de $\mathfrak{Y}'_m$, Je rappelle qu'il y a une façon bien connue des spécialistes de calculer la cohomologie des espaces quotients à partir d'une suite spectrale. Brieskorn cite le résultat qui se déduit des théorèmes généraux de [Hu]. Rappelons le principe assez joli du calcul.

Soit U un espace $K(\pi, 1)$ pour un groupe π fini et V son recouvrement universel, qui est par conséquent homologiquement trivial. On a $U = \pi\backslash V$. Soit Z un espace sur lequel π agit librement et soit Z/π le quotient. On peut calculer la cohomologie de $Z \times_\pi V$ soit en utilisant l'application $Z \times_\pi V \to Z/\pi$ et sa suite spectrale, soit en utilisant l'application $Z \times_\pi V \to U$ et sa suite spectrale. La première commence avec le terme E^2 donné par $H^p(Z/\pi, H^q(V))$. Puisque la fibre est V, qui est cohomologiquement trivial, cela donne $H^p(Z/\pi)$. En utilisant l'autre suite spectrale, on a $H^p(U, H^q(Z)) = H^p(\pi, H^q(Z))$ car la cohomologie d'un espace $K(\pi, 1)$ est la cohomologie du groupe π. Pour nous Z sera $\mathfrak{Z}'_m$ et $\pi = W'$.

En principe donc, si nous comprenons l'action de W' sur l'ensemble des points d'ordre m, nous pouvons espérer calculer la cohomologie de $\mathfrak{Z}_m$ – peut-être même sa structure de Hodge mixte – en calculant d'abord la cohomologie de $\mathfrak{Y}'_m$ et en calculant ensuite la cohomologie du groupe W', mais seulement dans des modules sans torsion, en particulier dans des espaces vectoriels sur $\mathbb{Q}$.

Dans le cas topologique, le groupe des points d'ordre m sur la jacobienne J_D est le quotient $H_1(J_D)/mH_1(J_D)$. Pour trouver W' et son action sur F_m, il suffit donc de trouver l'action de $S(n)$ sur $H_1(J_D) \cong H_1(C_D)$. Rappelons d'abord la construction géométrique et intuitive de C_D, de son homologie et de l'action du groupe de tresses.

Choisissons une suite de couples $(f_1, f_2), \ldots, (f_{2g+1}, f_{2g+2})$ de points de ramification. Nous pouvons joindre les points de chaque couple par des courbes lisses sur la sphère de Riemann qui ne se coupent pas. Découpons le plan complexe le long de ces courbes pour obtenir un espace qui est géométriquement la sphère avec $g+1$ trous. La surface de Riemann définie par C_D s'obtient en collant les deux feuilles au-dessus du complément des coupures. La surface se représente topologiquement alors comme la jonction de ces deux sphères de Riemann trouées, le raccordement étant fait avec $g+1$ tuyaux.

Nous pouvons supposer qu'il y a aussi des courbes simples de f_{2i} à f_{2i+1}, avec $f_{2g+3} = f_1$, qui sont telles que la réunion de ces $2g+2$ courbes forme une courbe simple dans la sphère de Riemann. Nous dénotons la courbe de f_j à f_{j+1}, $f_{2g+3} = f_1$, par δ_j. Il y a alors sur C_D quelques cycles évidents, par exemple une courbe simple tracée sur un des tuyaux et qui le contourne une seule fois. Une autre possibilité est une courbe qui commence au point au-dessus de f_{2i} sur une des feuilles, qui fait une simple traversée du tuyau pour arriver au point sur l'autre feuille au-dessus de f_{2i}, puis passe à f_{2i+1} en restant au-dessus de δ_{2i}, et ensuite revient au point f_{2i} de départ en faisant d'abord une simple traversée du tuyau qui contient les deux points au-dessus de f_{2i+1} et en suivant enfin la courbe au-dessus de δ_{2i} qui joint f_{2i+1} à f_{2i}. Dénotons les premières courbes par α_i, $1 \le i \le g+1$, α_i se trouvant sur le tuyau qui passe par f_{2i-1}, et les deuxièmes par β_i, $1 \le i \le g+1$.

On a les conditions suivantes sur les nombres d'intersections des courbes, pourvu qu'une attention particulière soit accordée aux orientations

$$\begin{cases} \alpha_i \cdot \alpha_j &= 0, \qquad \beta_i \cdot \beta_j &= 0, \\ \alpha_i \cdot \beta_i &= 1, \qquad \alpha_{i+1} \cdot \beta_i &= -1. \end{cases} \tag{25}$$

Il est géométriquement évident que le cycle

$$\sum_{i=1}^{g+1} \alpha_i \tag{26}$$

est homologiquement trivial. Il n'exige guère plus de réflexion pour se convaincre que la somme

$$\sum_{i=1}^{g+1} \beta_i \tag{27}$$

est aussi triviale car la réunion des courbes au-dessus des δ_j sur l'une ou l'autre des deux feuilles la découpe en deux disques. Il est par conséquent évident que les cycles α_i et β_i engendrent le groupe $H_1(J_D)$ et que toutes les relations sont engendrées par (26) et (27) car sinon les relations (25) seraient impossibles.

Il y a une façon plus directe pour construire ces cycles. Si comme dans la théorie des surfaces de Riemann on regarde C_D comme un recouvrement ramifié à deux feuilles de la sphère de Riemann et si on trace sur ce recouvrement une courbe qui passe de f_j à f_{j+1} au-dessus de δ_j sur une des feuilles et qui revient à f_j sur l'autre en restant au-dessus de δ_j, alors la courbe ainsi obtenue est homotope soit à un α_i, soit à un β_i. Si l'on élargit un peu cette courbe, on obtient une courbe γ_j qui reste sur une seule feuille pour j impair mais qui passe d'une feuille à l'autre pour j pair et dont la projection sur la sphère de Riemann contient en son intérieur f_j, f_{j+1} et la courbe δ_j qui les joint, mais ne contient aucun point au-dessus de f'_j avec $j' \neq j, j+1$. La courbe γ_j rattachée à (f_j, f_{j+1}) ne coupe la courbe γ_{j+1} rattachée à (f_{j+1}, f_{j+2}) qu'une seule fois et l'orientation de l'intersection est négative. À part leurs orientations nous aurons $\alpha_i \sim \gamma_{2i}$ et $\beta_i \sim \gamma_{2i+1}$. Pour les orientations, rappelons qu'il y a une orientation positive naturelle en chaque point de la surface de Riemann C_D. On peut supposer que γ_j, qui fait un demi-tour autour de f_j et un demi-tour autour de f_{j+1}, les fait dans le sens positif. À chaque f_j il y aura γ_j et γ_{j+1} qui font un demi-tour. La courbe γ_j croise γ_{j+1}, soit en entrant dans le demi-tour, soit en en sortant. Puisqu'on a le choix, on peut supposer que c'est en sortant. Alors $\gamma_j \cdot \gamma_{j+1} = 1$. Ce n'est qu'à la toute fin, lorsque $j = 2g+2$, qu'il n'y a plus de choix, mais alors on vérifie facilement qu'à cause des autres conditions on a aussi $\gamma_{2g+2} \cdot \gamma_1 = 1$.

Selon [Br] le groupe fondamental de $\mathfrak{X}$ est engendré par des éléments h_i, $1 \leq i \leq 2g+2$, quoique le dernier h_{2g+2} s'avère superflu. Ces éléments agissent sur $\mathfrak{Y}$, qui est l'espace des paramètres $(f_1, \ldots, f_{2g+2})$, de la façon suivante. En ne touchant pas aux autres f_j, $j \neq i, i+1$, on déplace f_i de f_i à f_{i+1}, où $i+1$ est toujours pris dans le sens cyclique, en longeant un côté, mettons le côté droit, de la courbe fixée δ_i allant de f_i à f_{i+1} et en même temps on déplace f_{i+1} de f_{i+1} à f_i en longeant l'autre côté, donc le côté gauche. On arrive au même C_D mais les positions de f_i et de f_{i+1} ont été échangées.

Pendant cette homotopie il faut déplacer les courbes δ_{i-1}, δ_i et δ_{i+1} dont un des sommets est f_i ou f_{i+1} d'une façon continue pour que d'un côté elles suivent leurs sommets et de l'autre elles ne passent par aucune des autres courbes δ_j, $j \neq i-1, i, i+1$. La courbe δ_{i-1} allant de f_{i-1} à f_i est alors remplacée par la réunion de δ_{i-1} et d'une courbe qui longe δ_i à droite et passe comme δ_i de f_i à f_{i+1}. De la même façon, la courbe δ_{i+1} est remplacée par la réunion de δ_{i+1} et d'une courbe qui longe f_i à droite aussi mais en allant dans le sens inverse. Les deux extensions restent donc de deux côtés différents. La courbe δ_i elle-même est remplacée par δ_i dans le sens inverse. On voit que la géométrie ou la topologie sont telles que tout cela est possible.

Si on y réfléchit, on arrive à la conclusion que h_i remplace $\gamma_{i\pm1}$ par $\gamma_{i\pm1} \mp \gamma_i$, tandis que $h_i\gamma_j = \gamma_j$ si $j \neq i \pm 1$. Par exemple, γ_{i-1} et γ_i se coupent en un seul point, là où γ_i commence son demi-tour autour de f_i. À ce point on coupe les deux courbes et γ_{i-1} poursuit le chemin de γ_i et γ_i celui de γ_{i-1}. Les deux courbes simples deviennent de cette sorte une seule courbe qui contourne f_{i-1} et f_{i+1}, mais qui évite f_i et appartient à la classe de $\gamma_{i-1} + \gamma_i$. En général, $h_i(\gamma) = \gamma + (\gamma \cdot \gamma_i)\gamma_i$ de sorte que h_i est symplectique:

$$\{\gamma + (\gamma \cdot \gamma_i)\gamma_i\} \cdot \{\gamma' + (\gamma' \cdot \gamma_i)\gamma_i)\} = \gamma \cdot \gamma' + (\gamma' \cdot \gamma_i)(\gamma \cdot \gamma_i) + (\gamma \cdot \gamma_i)(\gamma_i \cdot \gamma') = \gamma \cdot \gamma'.$$

La moyenne sur les polynômes premiers. Le nombre de polynômes unitaires de degré n à coefficients dans $\mathbb{F}_q$ est q^n. Le nombre $\pi(n)$ de polynômes premiers (et unitaires) de même degré est $q^n/n + O(q^{n/2})$. Rappelons pourquoi. Le logarithme de la fonction ζ du corps des fonctions rationnelles sur $\mathbb{F}_q$ est d'une part

$$\sum_{k=1}^{\infty} \frac{1}{kq^{ks}} + \sum_P \sum_{k=1}^{\infty} \frac{1}{kq^{ks\deg P}},$$

et d'autre part, c'est

$$\sum_{k=1}^{\infty} \frac{1}{kq^{ks}} + \sum_{k=1}^{\infty} \frac{q^k}{kq^{ks}}.$$

Il en résulte que

$$\sum_{k|n} k\pi(k) = \sum_{\deg P|n} \deg P = q^n.$$

De cette relation on déduit assez facilement par récurrence que $\pi(n) = q^n/n + O(q^{n/2})$.

Pour que le polynôme P intervenant dans (17) soit premier, il faut et il suffit que le diviseur $\sum_{i=1}^{a}(x_i, y_i)$ de (19) qui définit σ dans (20) soit un diviseur premier. Nous verrons qu'un argument semblable est valable pour ces diviseurs pour un D et un μ donnés. Malheureusement, je ne sais pas à présent comment en tirer un argument utile pour le comptage sur D et μ car il y a un coefficient qui intervient, à savoir le nombre de points rationnels sur J_D, et qui varie avec D. Je ne le maîtrise pas.

Si $\rho = \sum_{i=1}^{a}(x_i, y_i)$ et si ξ est défini comme ci-dessus, alors l'équation (20) exige que $\rho \sim \xi$, donc que ρ soit linéairement équivalent à ξ. Leur différence est certainement de degré 0. Fixons n'importe quel diviseur rationnel δ de C_D de degré positif minimal. Nous étendons tout caractère θ de l'ensemble des diviseurs rationnels de degré 0 à un caractère sur l'ensemble de tous les diviseurs rationnels en exigeant que $\theta(\delta) = 1$. Soit K le nombre de classes de diviseurs rationnels de degré 0 modulo ceux linéairement équivalents à 0, donc le nombre de points rationnels sur J_D. Alors

$$\frac{1}{K}\sum_{\theta}\bar{\theta}(\xi)\ln L(s,\theta) = -\frac{1}{K}\sum_{\theta}\bar{\theta}(\xi)\left\{\sum_{\mathfrak{p}}\ln\left(1-\frac{\theta(\mathfrak{p})}{q^{s\deg\mathfrak{p}}}\right)\right\}. \tag{28}$$

Sauf pour ceux qui contiennent ∞_1 ou ∞_2, les $\mathfrak{p}$ sont exactement les diviseurs premiers parmi les diviseurs ρ. Ils ne sont toutefois pas soumis à la condition préalable d'être linéairement équivalents à ξ.

En développant les sommes du côté droit, nous obtenons d'une part

$$\frac{1}{K}\sum_{\theta}\sum_{\mathfrak{p}}\sum_{k=1}^{\infty}\frac{\bar{\theta}(\xi)\theta(\mathfrak{p}^k)}{k\mathrm{N}\mathfrak{p}^{\mathrm{ks}}} = \sum_{\mathfrak{p}}\sum_{\{k \mid \mathfrak{p}^k\sim\xi\}}\frac{1}{kq^{ks\deg\mathfrak{p}}}. \tag{29}$$

D'autre part,

$$L(s,\theta) = \prod_{j=1}^{m(\theta)}\left(1-\frac{\alpha_j(\theta)q^{1/2}}{q^s}\right)$$

si θ n'est pas trivial et

$$L(s,\theta) = \frac{\prod_{j=1}^{m(\theta)}\left(1-\frac{\alpha_j(\theta)q^{1/2}}{q^s}\right)}{\left(1-\frac{1}{q^s}\right)\left(1-\frac{q}{q^s}\right)}$$

si θ est trivial. Les racines $\alpha_j(\theta)$ sont toutes de valeur absolue 1. Donc le membre de gauche de (28) est égal à la somme de

$$\frac{1}{K}\sum_{k=1}^{\infty}\frac{1}{kq^{ks}} + \frac{1}{K}\sum_{k=1}^{\infty}\frac{q^k}{kq^{ks}} \tag{30}$$

et de

$$-\frac{1}{K}\sum_{k=1}^{\infty}\sum_{\theta}\sum_{j=1}^{m(\theta)}\frac{\bar{\theta}(\xi)\alpha_j(\theta)^k q^{k/2}}{kq^{ks}}. \tag{31}$$

Le nombre $\sum_\theta m(\theta)$ est $2g'$ si g' est le genre d'une extension maximale non ramifiée et abélienne du corps de fonctions C_D pour laquelle le corps fini de base reste $\mathbb{F}_q$. Ce nombre est facile à calculer à partir de K car $2g'-2 = K(2g-2)$. Le nombre K qui vaut souvent approximativement q^g reste toutefois inconnu. Ce manque de connaissance empêche l'utilisation efficace des équations (29), (30) et (31). On pourrait penser qu'en faisant la moyenne sur D on échapperait au besoin d'une connaissance précise de K mais jusqu'à présent je ne sais pas comment.

Conclusion. Il reste beaucoup à faire pour mener les suggestions de cette note à bonne fin. Il faudra suffisamment apprendre pour savoir exactement comment calculer l'action du groupe fondamental sur les recouvrements définis par les points d'un ordre donné et ensuite mener à bien tous les calculs proposés. Ayant compris les calculs topologiques il nous faudra alors savoir tout exprimer dans le cadre étale. Je n'ai jusqu'à présent rien fait dans cette direction. Dans ma discussion deux points sont restés flous: les conditions sur S dans $R^2 - DS^2 = aP^m$ et le passage de P unitaire, mais autrement arbitraire, à P premier et unitaire. Le premier problème sera sans doute fastidieux et l'issue des calculs est même incertaine, mais il n'y a pas de raison pour craindre de grosses difficultés. Le deuxième est cependant troublant.

La question majeure sera toutefois gardée pour la toute fin. Selon les principes esquissés dans [BE], ce que nous cherchons en passant au-delà de l'endoscopie, c'est une formule pour chaque somme de la forme

$$\sum_{\pi} m_\pi(\rho) \prod_{v \in S} \mathrm{tr}\pi_{\mathrm{v}}(\mathrm{f_v}), \tag{32}$$

la somme étant prise sur tous les π de type Ramanujan, avec caractères centraux donnés et non ramifiés en dehors de l'ensemble fini S. Considérons le groupe $GL(2)$ et ρ une représentation de son groupe L pris sans facteur galoisien. C'est le cas de cet article avec $\rho = \rho_m$ et $dim\, \rho_m = m + 1$.

Il y a trois sortes de représentations π pour lesquelles nous nous attendons à ce que l'application $m \to m_\pi(\rho_m)$ se comporte de trois façons différentes. D'abord pour la plupart des π, on s'attend à ce que $m_\pi(\rho_m) = 0$ si $m > 0$. Pour les π de type diédral on s'attend à ce que $m_\pi(\rho_m)$ soit 0 pour m impair, mais qu'il se comporte d'une façon régulière pour m pair. Donc on s'attend à ce que (32) s'exprime pour m pair comme une somme sur les extensions quadratiques du corps de base F, qui peut être un corps de nombres ou un corps de fonctions. Pour le corps des fonctions rationnelles nous n'avons pas mené les calculs préliminaires de cette note à un point tel que nous puissions être certains qu'en effet c'est le cas.

À plus forte raison, nous n'avons pas vu encore la contribution des représentations π pour lesquelles elle est la plus intéressante, à savoir celle des $\pi = \pi(\sigma)$, σ étant une représentation du groupe de Galois dans $GL(2, \mathbb{C})$ dont l'image est nécessairement finie. Dans nos calculs topologiques nous avons prévu le calcul précis des structures de Hodge. Nous nous attendons que ces structures soient assez simples, c'est-à-dire de type (p, p) pour la plupart. Lorsqu'on passe à la cohomologie étale on attend alors que les valeurs propres des éléments de Frobenius seront des nombres complexes assez simples, pas pires par exemple qu'une racine de l'unité fois q^k, k un entier. Ce qu'il faut espérer alors, c'est que dans la cohomologie des espaces de recouvrements des espaces $\mathfrak{X}$ ou $\tilde{\mathfrak{X}}$ il y ait juste assez de structure galoisienne qui persiste lorsque $\mathrm{degN} \to \infty$ pour qu'elle puisse apporter à la fin l'obole qui fera toute la différence et qui sera, sauf pour quelques précisions, égale à la contribution des $\pi = \pi(\sigma)$ à (32).

Il est évident de ces réflexions que pour moi et les autres qui croyons aux propos de cette note, il y a un long cheminement à faire avant que nous soyons sûrs que c'est vraiment la bonne voie

Bibliographie

[Br] Egbert Brieskorn *Sur les groupes de tresses*, Séminaire Bourbaki, 1971/72, No. 401

[De] Pierre Deligne *Les immeubles des groupes de tresses généralisés*, Inv. Math. **8** (1972) 273–302.

[Ha] Günter Harder *Eisensteinkohomologie und die Konstruktion gemischter Motive*, Springer-Verlag, 1991

[Hu] S-T. Hu *Homotopy Theory* Academic Press 1959

[P] R.P. Langlands *Problems in the Theory of Automorphic Forms* Lectures in Modern Analysis and Applications, SLN 170 (C. T. Taam, ed.), Springer-Verlag, 1970, pp. 18–86.

[W] ———, *Where stands functoriality today?* Representation Theory and Automorphic Forms (T.N. Bailey and A.W. Knapp, eds.) American Mathematical Society, 1991 pp. 457–471.

[BE] ———, *Beyond Endoscopy*, Contributions to Automorphic Forms, Geometry and Number Theory (H. Hida, D. Ramakrishnan, F. Shahidi, eds.), The Johns Hopkins University Press, 2004, pp. 611–698.

[N] W. Narkiewicz, *The Development of Prime Number Theory*, Springer-Verlag, 2000.