La fonction zéta d'Igusa d'un polynôme à une variable

Leonardo Zapponi

1. Notations

Dans la suite, pour tout nombre premier p, on note $\mathbb{Z}_p$ l'anneau des entiers p-adiques, d'idéal maximal $\mathfrak{p} = p\mathbb{Z}_p$ et de corps des fractions $\mathbb{Q}_p$. On désigne par $v : \mathbb{Q}_p^\times \to \mathbb{Z}$ la valuation p-adique. Muni de la norme

$$|x| = p^{-v(x)},$$

l'ensemble $\mathbb{Z}_p$ est alors un anneau complet, compact et totalement discontinu. On note de plus μ l'unique mesure de Haar sur $\mathbb{Z}_p$ telle que $\mu(\mathbb{Z}_p) = 1$. Pour tout $x \in \mathbb{Z}_p$ et tout entier naturel n, soit finalement

$$D(x,n) = x + \mathfrak{p}^n = \{y \in \mathbb{Z}_p \mid v(y-x) \geq n\}$$

le disque (ouvert et fermé) centré en x de rayon (et mesure) p^{-n}. Cet ensemble ne dépendant que de la classe $a \in \mathbb{Z}/p^n\mathbb{Z}$ de x modulo $\mathfrak{p}^n$, on le notera également $D(a)$.

2. La fonction L de Igusa d'un polynôme

Soit f un polynôme à oefficients entiers. Pour tout entier $n > 0$, notons $N_n(f)$ le nombre de racines de f dans $\mathbb{Z}/n\mathbb{Z}$, c'est à dire le cardinal de l'ensemble

$$Z_n(f) = \{x \in \mathbb{Z}/n\mathbb{Z} \mid f(x) = 0\}.$$

On pose de même $N_0(f) = 1$. Si m divise n, on a une application naturelle de $Z_n(f)$ dans $Z_m(f)$. Le théorène des restes chinois affirme que l'on a l'identité

$$N_{nm}(f) = N_n(f)N_m(f)$$

lorsque les entiers n et m sont premiers entre eux. La série de Dirichlet

$$L(s,f) = \sum_{n>0} \frac{N_n(f)}{n^s}.$$

est convergente pour s assez grand et la propriété multiplicative de $N_n(f)$ implique que l'on a un produit eulérien

$$L(s,f) = \prod_p P_p(p^{-s}, f),$$

avec

$$P_p(T,f) = \sum_{n\geq 0} N_{p^n}(f)T \in \mathbb{Q}[\![T]\!].$$

Dans la suite, nous dirons que le polynôme f est *separable* sur $\mathbb{Z}_p$ si toutes ses racines dans $\mathbb{Z}_p$ sont simples. Le but de cette note est de démontrer le résultat suivant.

***Théorème 1* (Igusa).** — *Pour tout polynôme $f \in \mathbb{Z}_p[X]$, on a l'identité*

$$P_p(p^{-s}, f) = \frac{1 - p^{-s}\int_{\mathbb{Z}_p} |f(x)|^{s-1}dx}{1-p^{-s}}.$$

De plus, si f est séparable sur $\mathbb{Z}_p$ alors $P_p(T,f)$ est une fraction rationnelle ayant au plus un pôle simple en 1.

3. Estimations p-adiques

Dans ce paragraphe nous démontrons deux résultats élémentaires mais cruciaux pour la suite.

Lemme 2. — *Si un polynôme $f \in \mathbb{Z}_p[X]$ ne possède pas de racine dans $\mathbb{Z}_p$ alors $v(f(x))$ est borné pour tout $x \in \mathbb{Z}_p$.*

Démonstration. — S'il existait une suite (x_n) d'éléments de $\mathbb{Z}_p$ tels que $v(f(x_n))$ diverge, ce qui revient à affirmer que $f(x_n)$ converge vers 0, on pourrait en extraire une sous-suite convergente (y_n). Une application polynômiale étant continue pour la topologie p-adique, la limite de (y_n) serait alors une racine de f, ce qui est exclu. □

Soit $x \in \mathbb{Z}_p$ une racine d'un polynôme non nul $f \in Z_p[X]$. On a donc l'identité

$$f = (X-x)^e g,$$

où e est la multiplicité de x et $g \in \mathbb{Z}_p[X]$ est univoquement déterminé et ne s'annule pas en x. L'entier

$$d_f(x) = v(g(x))$$

est appelé *valuation de la différente* de f en x. On remarquera que si x est une racine simple de f alors $d_f(x)$ est la valuation p-adique de l'élément $f'(x)$, où f' désigne le polynôme dérivé de f.

Lemme 3. — *Soit $x \in \mathbb{Z}_p$ une racine d'un polynôme non nul $f \in \mathbb{Z}_p[X]$ et notons e sa multiplicité. Pour tout $y \in \mathbb{Z}_p$ tel que $v(y-x) > d_f(x)$, on a l'identité*

$$v(f(y)) = ev(y-x) + d_f(x).$$

Démonstration. — En suivant les notations et les hypothèses ci-dessus, on a l'identité

$$g = g(x) + (X-x)h,$$

avec $h \in \mathbb{Z}_p[X]$. En particulier, pour $v(y-x) > d_f(x)$, on a les relations

$$v(g(y)) = v((g(x) + (y-x)h(y)) = v(g(x)) = d_f(x),$$

d'où les identités

$$v(f(y)) = v((y-x)^e g(y)) = v((y-x)^e) + v(g(y)) = ev(y-x) + d_f(x).$$

□

4. Deux recouvrements

Pour tout polynôme $f \in \mathbb{Z}_p[X]$, posons

$$D_n(f) = \{x \in \mathbb{Z}_p \mid v(f(x)) \geq n\} = f^{-1}(D(0,n)).$$

Dans ce paragraphe, nous présentons deux descpriptions cet esemble en tant qu'union de disques p-adiques. La première est valable de manière générale, la seconde pour de grandes valeurs de n. En comparant les expressions de la mesure de $D_n(f)$ ainsi obtenues, on en déduit alors une expression asymptotique pour $N_{p^n}(f)$.

Proposition 4. — *Pour tout polynôme $f \in \mathbb{Z}_p[X]$ et tout entier naturel n, on a une décomposition en union disjointe*

$$D_n(f) = \bigcup_{a \in Z_{p^n}(f)} D(a).$$

En particulier, on en déduit l'identité

$$\mu(D_n(f)) = N_{p^n}(f)p^{-n}.$$

Démonstration. — On a une décomposition en union disjointe (classes latérales modulo $\mathfrak{p}^n$)

$$\mathbb{Z}_p = \bigcup_{a \in \mathbb{Z}/p^n\mathbb{Z}} D_a,$$

L'ensemble D_a étant le translaté de $D_0 = \mathfrak{p}^n$, on a donc l'identité

$$\mu(D_a) = \mu(\mathfrak{p}^n) = p^{-n}.$$

Il suffit maintenant de remarquer qu'un élément $x \in D(a)$ appartient à $D_n(f)$ si et seulement si l'image de $f(x)$ dans $\mathbb{Z}/p^n\mathbb{Z}$, qui coïncide avec $f(a)$, est nulle, ou encore si a appartient à $Z_{p^n}(f)$. □

Proposition 5. — *Soient $x_1, \ldots, x_r \in \mathbb{Z}_p$ les racines d'un polynôme $f \in \mathbb{Z}_p[X]$ séparable sur $\mathbb{Z}_p$. Pour n assez grand, l'ensemble $D_n(f)$ se décompose en une union disjointe*

$$D_n(f) = \bigcup_{i=1}^{r} D(x_i, n - d_f(x_i)).$$

Démonstration. — On a la factorisation

$$f = \prod_{i=1}^{r} (X - x_i)^{e_i} g,$$

avec $g \in \mathbb{Z}_p[X]$ sans racine dans $\mathbb{Z}_p$. D'après le lemme 2, pour tout $x \in \mathbb{Z}_p$, la valuation de $g(x)$ est majorée par un entier M. Posons $N = \max_i\{d_f(x_i)\}$ et supposons que l'on ait l'inégalité

$$n > (d+1)\max\{N, M\},$$

où d désigne le degré de f. Dans ce cas, pour $x \in D(x_i, p^{-(n-d_f(x_i))/e_i})$, on obtient les relations

$$v(x - x_i) \geq (n - d_f(x_i))/e_i \geq (n - d_f(x_i))/d > ((d+1)d_f(x_i) - d_f(x_i)/d = d_f(x_i)$$

et, en appliquant le lemme 3, on en déduit les relations

$$v(f(x)) = e_i v(x - x_i) + d_f(x_i) \geq n,$$

d'où l'inclusion $D(x_i, p^{-(n-d_f(x_i))/e_i}) \subset D_n(f)$. Réciproquement, pour $x \in D_n(f)$, la factorisation de f décrite précédemment amène aux relations

$$v(f(x)) = \sum_{i=1}^{r} e_i v(x - x_i) + v(g(x)) \geq n.$$

La somme ci-dessus possédant au plus d termes, l'un d'entre eux est supérieur ou égal à n/d. Tout d'abord, les inégalités

$$v(g(x)) \leq M < \frac{d+1}{d} M < \frac{n}{d}$$

impliquent qu'il existe i tel que $v(x - x_i) \geq n/d$. Les relations

$$\frac{n}{d} > \frac{d+1}{d} M > M \geq d_f(x_i)$$

permettent d'appliquer le lemme 3, ce qui amène finalement aux relations

$$v(f(x)) = e_i v(x - x_i) + d_f(x_i) \geq n$$

et l'élément x appartient bien au disque centré en x_i de rayon $p^{-(n-d_f(x_i))/e_i}$. □

Corollaire 6. — *Soit $f \in \mathbb{Z}_p[X]$ un poynôme séparable sur $\mathbb{Z}_p$ et notons $x_1, \ldots, x_r \in \mathbb{Z}_p$ ses racines. Pour tout entier n assez grand, on a l'identité*

$$N_{p^n}(f) = \sum_{i=1}^{r} p^{d_f(x_i)}.$$

En particulier, la suite $(N_{p^n}(f))_n$ est ultimement stationnaire.

Démonstration. — C'est une conséquence de la proposition. En effet, les éléments d'un disque $D(x_i, p^{d_f(x_i)-n})$ définissent $p^{d_f(x_i)}$ éléments dans $\mathbb{Z}/p^n\mathbb{Z}$. □

5. Démonstration du théorème

Considérons la série formelle $P_f \in \mathbb{Q}[\![T]\!]$ définie par

$$P_f = \sum_{n\geq 0} p^{-n} N_n(f) T^n,$$

où l'on a posé $N_0(f) = 1$.

Théorème 7. — *Soit $f \in \mathbb{Z}_p[X]$ un polynôme séparable sur $\mathbb{Z}_p$ et notons $x_1, \ldots, x_r \in \mathbb{Z}_p$ ses racines. En posant*

$$N = \sum_{i=1}^{r} p^{d_f(x_i)},$$

on a l'identité

$$P_f = g + \frac{pN}{p-T},$$

avec $g \in \mathbb{Q}[T]$. En particulier, P_f est une fraction rationnelle.

Démonstration. — En effet, d'après le corollaire 5, il existe un polynôme $g \in \mathbb{Q}[T]$ tel que

$$P_f - g = \sum_{n\geq 0} p^{-n} N T^n = \frac{pN}{p-T}.$$

□

Posons

$$\zeta_f(s) = \int_{\mathbb{Z}_p} |f(x)|^s dx$$

L'ensemble

$$U_n(f) = D_n(f) - D_{n+1}(f) = \{x \in \mathbb{Z}_p \mid v(f(x)) = n\}$$

est mesurable et, d'après le lemme 1, on a l'identité

$$\mu(U_n(f)) = N_n(f)p^{-n} - N_{n+1}(f)p^{-n-1}.$$

On en déduit alors les relations

$$\begin{aligned}
\int_{\mathbb{Z}_p} |f(x)|^s dx &= \sum_{n\geq 0} \int_{U_n(f)} |f(x)|^s dx = \sum_{n\geq 0} p^{-ns}\mu(U_n(f)) = \\
&= \sum_{n\geq 0} p^{-n} N_n(f) p^{-ns} - \sum_{n\geq 0} p^{-n-1} N_{n+1}(f) p^{-ns} = \\
&= P_f(p^{-s}) - p^s(P_f(p^{-s}) - 1) = \\
&= (1-p^s)P_f(p^{-s}) + p^s = \\
&= \frac{t-1}{t} P_f(t) + \frac{1}{t}.
\end{aligned}$$

6. Un exemple explicite

Nous allons conclure cette note avec le calcul de la fonction $L(s, f)$ dans quelques cas particuliers. Commençons en considérant le polynôme $f = X(X - 1)$. Pour tout entier $n > 0$, on a la relation $N_n(f) = 2^{\omega(n)}$, où $\omega(n)$ désigne le nombre de diviseurs premiers de n (comptés sans multiplicité). Pour les facteurs locaux, on obtient les expressions

$$P_p(T, f) = \frac{1 + T}{1 - T} = \frac{1 - T^2}{(1 - T)^2},$$

d'où les l'identités

$$L(s, f) = \sum_{n>10} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta(s)^2}{\zeta(2s)}.$$

---

26 mai 2019

LEONARDO ZAPPONI • *E-mail :* leonardo.zapponi@imj-prg.fr