Les conjectures de Weil

David Hébert
Groupe de travail
Cohomologie étale

4 février 2009

Table des matières

Introduction.

Soient k un corps et X une variété algébrique projective sur k, c'est à dire la donnée d'un nombre fini (f_i) de polynômes homogènes de $\mathsf{k}[X_0, ..., X_n]$ pour un certain entier $n > 0$ tel que

$$X := \{P \in \mathbb{P}^n(\mathsf{k}) | \forall\, i \quad f_i(P) = 0\}.$$

Si $\mathbb{K}$ est un surcorps de k, on note

$$X(\mathbb{K}) := \{P \in \mathbb{P}^n(\mathbb{K}) | \forall\, i \quad f_i(P) = 0\}.$$

On note $\overline{X}$ pour $X(\overline{\mathsf{k}})$, où $\overline{\mathsf{k}}$ désigne une cloture algébrique de k.

Lorsque $\mathsf{k} = \mathbb{F}_q$ est le corps à q (=puissance d'un nombre premier) éléments, on s'intéresse à la cardinalité de $X(\mathbb{F}_{q^m})$ pour tout entier $m > 0$. Bien sûr ce nombre est fini car

$$\begin{array}{rcl} \mathsf{Card}(X(\mathbb{F}_{q^m})) & \leqslant & \mathsf{Card}(\mathbb{P}^n(\mathbb{F}_{q^m})) \\ & \leqslant & \dfrac{(q^m)^{n+1} - 1}{q^m - 1} \\ & \leqslant & \displaystyle\sum_{i=0}^{n} q^{im}. \end{array}$$

On note

$$N_m = \mathsf{Card}(X(\mathbb{F}_{q^m})).$$

Pour étudier ces nombres, on les rassemble dans une serie formelle, que l'on appelle fonction zeta :

$$Z(X,T) := \mathsf{exp}\left(\sum_{m=1}^{+\infty} N_m \frac{T^m}{m}\right).$$

Comme la fonction exponetielle admet une décomposition en série formelle à coefficient rationel, en la composant par la serie formelle logarithmique $\ln(Z(X,T))$, qui est elle aussi à coefficient rationel, on conclut que

$$Z(X,T) \in \mathbb{Q}[\![T]\!].$$

Etudions l'exemple de la variété $X = \mathbb{P}^n(\mathbb{F}_q)$.

$$\begin{aligned}
Z(X,T) &= \mathsf{exp}\left(\sum_{m=1}^{+\infty} N_m \frac{T^m}{m}\right) \\
&= \mathsf{exp}\left(\sum_{m=1}^{+\infty}\sum_{i=0}^{n} q^{im}\frac{T^m}{m}\right) \\
&= \mathsf{exp}\left(\sum_{i=0}^{n}\sum_{m=1}^{+\infty} \frac{(q^iT)^m}{m}\right) \\
&= \prod_{i=0}^{n} \mathsf{exp}\left(\sum_{m=1}^{+\infty} \frac{(q^iT)^m}{m}\right) \\
&= \prod_{i=0}^{n} \mathsf{exp}\left(-\ln(1-q^iT)\right) \\
&= \frac{1}{(1-T)(1-qT)(1-q^2T)...(1-q^nT)}.
\end{aligned}$$

La première observation, absolument innocente, que nous pouvons faire est que $Z(X,T) \in \mathbb{Z}(T)$. La seconde observation est

$$\begin{aligned}
Z\left(X, \frac{1}{q^nT}\right) &= \frac{1}{\left(1-\frac{1}{q^nT}\right)\left(1-\frac{1}{q^{n-1}T}\right)\left(1-\frac{1}{q^{n-2}T}\right)...\left(1-\frac{1}{T}\right)} \\
&= (-1)^{n+1}\frac{q^{\frac{n(n+1)}{2}}T^{n+1}}{(1-T)(1-qT)(1-q^2T)...(1-q^nT)} \\
&= (-1)^{n+1}q^{\frac{n(n+1)}{2}}T^{n+1}Z(X,T).
\end{aligned}$$

Ces résultats, ainsi que d'autres notemment sur les courbes, ont ammené Weil à énoncer des conjectures en 1949 :

Soit X une variété algébrique projective lisse de dimension n sur un corps fini k.

Rationalité.

Il existe des polynômes $P_i \in \mathbb{Z}[T]$ tels que

$$Z(X,T) = \frac{P_1(T)P_3(T)...P_{2n+1}(T)}{P_0(T)P_1(T)...P_{2n}(T)}.$$

De plus $P_0(T) = 1 - T$ et $P_{2n}(T) = 1 - q^nT$.

Equation fonctionnelle.

$$Z\left(X, \frac{1}{q^nT}\right) = \pm q^{\frac{n\chi}{2}}T^{\chi}Z(X,T).$$

Où $\chi = \sum_{i=0}^{2n}(-1)^i\mathsf{Deg}(P_i)$.

Analogue de l'hypothèse de Riemann.

Les conjugués des racines de P_i sont de module

$$q^{-\frac{i}{2}}$$

Nombre de Betti. ...

Weil suggère que si l'on dispose d'une bonne cohomologie alors on peut en déduire les conjectures. De telles cohomologies s'appellent les cohomologies de Weil. Dans un premier temps nous donnerons une description axiomatique de ces cohomologies ; nous en déduirons ensuite quelques résultats amenant aux conjectures. Nous nous interesserons ici à la rationalité et à l'équation fonctionnelle.

Chapitre 1

Cohomologies de Weil.

On fixe un corps $\mathbb{K}$ de caractéristique 0 qui se plonge dans $\mathbb{C}$

Définition 1.1. *Un foncteur contravariant* $\mathsf{H}^*(\bullet, \mathbb{K})$ *de la catégorie des variétés dans la catégorie des* $\mathbb{K}$ *algèbres graduées anti-commutatives de dimension finie est appelé* cohomologie de Weil *si les conditions suivantes sont vérifiées :*

A. Dualité de Poincaré. *Soit* n *la dimension de la varieté* X*.*

(i). *Pour tout entier* i *qui n'est pas compris entre* 0 *et* $2n$

$$\mathsf{H}^i(X, \mathbb{K}) = 0.$$

(ii). *Il existe un isomorphisme*

$$\mathsf{H}^{2n}(X, \mathbb{K}) \simeq \mathbb{K}$$

appelé isomorphisme d'orientation.

(iii). *Pour tout entier* i *entre* 0 *et* $2n$ *le produit de* $\mathsf{H}^*(X, \mathbb{K})$ *induit des applications bilinéaires non dégénérées*

$$Q_X^i : \mathsf{H}^i(X, \mathbb{K}) \times \mathsf{H}^{2n-i}(X, \mathbb{K}) \longrightarrow \mathsf{H}^{2n}(X, \mathbb{K}).$$

De plus ces transformations sont fonctorielles en X*.*

B. Formule de Künneth. *Si* X *et* Y *sont deux variétés on a un isomorphisme*

$$\mathsf{H}^*(X, \mathbb{K}) \otimes_{\mathbb{K}} \mathsf{H}^*(Y, \mathbb{K}) \simeq \mathsf{H}^*(X \times Y, \mathbb{K}).$$

C. Applications de cycles. *Pour toute variété* X*, il existe des morphismes de groupes*

$$\gamma_X : \mathsf{C}^p(X) \longrightarrow \mathsf{H}^{2p}(X, \mathbb{K})$$

qui vérifient

Fonctorialité. *Ces transformations sont fonctorielles en* X*.*

Multiplicativité. *Pour toutes variétés* X *et* Y *et tout cycles* Z *et* W *de respectivement* X *et* Y

$$\gamma_{X \times Y}(Z \times W) = \gamma_X(Z) \otimes \gamma_Y(W).$$

Non trivialité. *Si* P *est un point alors* γ_P *est l'inclusion de* $\mathbb{Z}$ *dans* $\mathbb{K}$*.*

Bien évidement la dualité de Poincaré implique que pour toute variété X de dimension n les $\mathbb{K}$ espaces vectoriels $\mathsf{H}^i(X, \mathbb{K})$ et $\mathsf{H}^{2n-i}(X, \mathbb{K})$ sont de même dimension et ce quelque soit l'entier i (il n'y aurait sinon aucun sens de parler de forme bilinéaire non dégénérée). En particulier $\mathsf{H}^0(X, \mathbb{K})$ et $\mathsf{H}^{2n}(X, \mathbb{K})$ sont de dimension 1.

Théorème 1.2. *Soient* $\mathsf{H}^*(\bullet, \mathbb{K})$ *une cohomologie de Weil,* X *une variété projective lisse de dimension* n *sur* $\mathbb{F}_q$ *et* $\mathsf{Fro} : \overline{X} \longrightarrow \overline{X}$ *l'endomorphisme de Frobéniüs :* $\mathsf{Fro}(x) = x^q$*. Alors pour tout entier* $m > 0$

$$N_m = \sum_{i=0}^{2n} (-1)^i \mathsf{Tr}(\mathsf{H}^i(\mathsf{Fro}^m, \mathbb{K})).$$

Admettons ce theorème pour le moment et déduisons en quelques résultats sur les conjectures de Weil. On fixe une cohomologie de Weil $\mathsf{H}^*(\bullet, \mathbb{K})$ que l'on note pour simplifier $\mathsf{H}^*(\bullet)$. On fixe de plus une variété projective lisse X sur $\mathsf{k} = \mathbb{F}_q$ de dimension n.

Lemme 1.3. *Soient* E *et* F *deux* $\mathbb{K}$*-espaces vectoriels de même dimension (fini) et*

$$\beta : E \times F \longrightarrow \mathbb{K}$$

une forme bilinéaire non dégénérée. Supposons qu'il existe

$$\varphi : E \longrightarrow E, \quad \psi : F \longrightarrow F, \quad \lambda \in \mathbb{K}^*$$

tel que pour tout $x \in E$ *et* $y \in F$

$$\beta(\varphi(x), \psi(y)) = \lambda \beta(x, y).$$

Alors

$$\mathsf{Det}(1 - \psi T) = \frac{(-\lambda T)^d}{\mathsf{Det}(\varphi)} \mathsf{Det}\left(1 - \frac{\varphi}{\lambda T}\right), \qquad \mathsf{Det}(\psi) = \frac{\lambda^d}{\mathsf{Det}(\varphi)}$$

où $\mathsf{Dim}_{\mathbb{K}}(E) = \mathsf{Dim}_{\mathbb{K}}(F) = d$*.*

Démonstration. Comme il s'agit d'un calcul de déterminant et que ce dernier est invariant par changement de base, on peut fixer une base et travailler avec les matrices. Soit donc M la matrice de β, c'est à dire

$$\forall X \in E,\ \forall Y \in F \quad \beta(X, Y) = {}^t X M Y$$

Entre autre la matrice M induit, grace à la non dégénéressence, un isomorphisme de F sur E. Notons A la matrice φ et B la matrice ψ. Alors la condition de l'énoncé devient

$${}^t A M B = \lambda M.$$

On en déduit en particulier que A est surjective donc bijective. Entre autre

$$B = \lambda M^{-1} {}^t A^{-1} M$$

Donc

$$\begin{aligned} \mathsf{Det}(\psi) &= \mathsf{Det}(B) \\ &= \mathsf{Det}(\lambda M^{-1} {}^t A^{-1} M) \\ &= \lambda^d \mathsf{Det}(A^{-1}) \\ &= \frac{\lambda^d}{\mathsf{Det}(\varphi)} \end{aligned}$$

$$
\begin{aligned}
\mathsf{Det}(1-\psi T) &= \mathsf{Det}(1-BT)\\
&= \mathsf{Det}(1-\lambda M^{-1t}A^{-1}MT)\\
&= \mathsf{Det}(1-\lambda^t A^{-1}T)\\
&= \mathsf{Det}(\lambda T^t A^{-1})\mathsf{Det}\left(\frac{A}{\lambda T}-1\right)\\
&= (\lambda T)^d \mathsf{Det}(A^{-1})(-1)^d \mathsf{Det}\left(1-\frac{A}{\lambda T}\right)\\
&= \frac{(-\lambda T)^d}{\mathsf{Det}(\varphi)}\mathsf{Det}\left(1-\frac{\varphi}{\lambda T}\right)
\end{aligned}
$$

□

Lemme 1.4. *Soient E un $\mathbb{K}$ espace vectoriel de dimension finie et u un endomorphisme de E. Alors*

$$
\mathsf{exp}\left(\sum_{m=1}^{+\infty}\mathsf{Tr}(u^m)\frac{T^m}{m}\right)=\mathsf{Det}(1-Tu)^{-1}.
$$

(L'identité de E étant notée 1).

Démonstration. Supposons E de dimension n. Comme le déterminant et la trace sont invariants par changement de base, on peut choisir une base, même complexe (ce qui est possible car $\mathbb{K}$ se plonge dans $\mathbb{C}$) telle que la matrice de l'endomorphisme soit triangulaire superieure :

$$
\begin{pmatrix}
\lambda_1 & & & & \\
 & \ddots & & * & \\
 & & \ddots & & \\
 & 0 & & \ddots & \\
 & & & & \lambda_n
\end{pmatrix}
$$

Ainsi $\mathsf{Det}(1-Tu)=\prod_{i=1}^n(1-\lambda_i T)$, et $\mathsf{Tr}(u^m)=\sum_{i=1}^n\lambda_i^m$. Alors

$$
\begin{aligned}
\sum_{m=1}^{+\infty} tr(u^m)\frac{T^m}{m} &= \sum_{m=1}^{+\infty}\sum_{i=1}^{n}\lambda_i^m\frac{T^m}{m}\\
&= \sum_{i=1}^{n}\sum_{m=1}^{+\infty}\frac{(\lambda_i T)^m}{m}\\
&= \sum_{i=1}^{n}-\ln(1-\lambda_i T)\\
&= \ln\left(\frac{1}{(1-\lambda_1 T)...(1-\lambda_n T)}\right).
\end{aligned}
$$

□

En substituant N_m dans la définition de la fonction zeta, on arrive à

$$\begin{aligned}
Z(X,T) &= \mathsf{exp}\left(\sum_{m=1}^{+\infty}\sum_{i=0}^{2n}(-1)^i \mathsf{Tr}(\mathsf{H}^i(\mathsf{Fro}^m))\frac{T^m}{m}\right) \\
&= \prod_{i=0}^{2n}\mathsf{exp}\left(\sum_{m=1}^{+\infty}\mathsf{Tr}(\mathsf{H}^i(\mathsf{Fro})^m)\frac{T^m}{m}\right)^{(-1)^i} \\
&\overset{1.4}{=} \prod_{i=0}^{2n}\mathsf{Det}(1-\mathsf{H}^i(\mathsf{Fro})T)^{(-1)^{i+1}}
\end{aligned}$$

En posant $P_i(T) = \mathsf{Det}(1-\mathsf{H}^i(\mathsf{Fro})T)$ on obtient la forme souhaitée pour la fonction zeta, bien que nous sachions juste que $Z(X,T) \in \mathbb{K}(T)$.

On note néanmoins que

$$\mathsf{Deg}(P_i) = \mathsf{Dim}_{\mathbb{K}}(\mathsf{H}^i(\overline{X})). \tag{1.1}$$

Posons $E_i = \mathsf{H}^i(\overline{X})$ et $\varphi_i = \mathsf{H}^i(\mathsf{Fro})$. La fonctorialité de la dualité de Poincaré (point (iii) de l'axiome A.) nous donne le diagramme commutatif suivant :

$$\begin{tikzcd}
E_i \times E_{2n-i} \arrow[r, "Q^i_{\overline{X}}"] \arrow[d, "\left(\begin{smallmatrix}\varphi_i & 0 \\ 0 & \varphi_{2n-i}\end{smallmatrix}\right)"'] & E_{2n} \arrow[d, "\varphi_{2n}"] \\
E_i \times E_{2n-i} \arrow[r, "Q^i_{\overline{X}}"'] & E_{2n}
\end{tikzcd}$$

En d'autre terme pour tout $x \in E_i$ et tout $y \in E_{2n-i}$

$$Q^i_{\overline{X}}(\varphi_i(x), \varphi_{2n-i}(y)) = \varphi_{2n}(Q^i_{\overline{X}}(x,y)).$$

Or l'endomorphisme linéaire φ_{2n} est nécessairement une homothétie (car par la dualité de Poincaré E_{2n} est de dimension 1). Notons

$$\mu \tag{1.2}$$

le coefficient, dans $\mathbb{K}^*$ (μ ne peut etre nul, grace à la non dégénérescence), de l'homothétie φ_{2n}. On peut alors appliquer le lemme 1.3 pour en déduire les relations suivantes :

$$\begin{aligned}
P_{2n-i}(T) &= \mathsf{Det}(1-\varphi_{2n-i}T) \\
&= \frac{(-\mu T)^{d_i}}{\mathsf{Det}(\varphi_i)}\mathsf{Det}\left(1-\frac{\varphi_i}{\mu T}\right) \\
&= \frac{(-\mu T)^{d_i}}{\mathsf{Det}(\varphi_i)}P_i\left(\frac{1}{\mu T}\right).
\end{aligned}$$

Où $d_i = \mathsf{Deg}(P_i) = \mathsf{Dim}_{\mathbb{K}}(E_i)$ (formule 1.1) ; ainsi

$$\begin{aligned} Z\left(X, \frac{1}{\mu T}\right) &= \prod_{i=1}^{2n} \left(P_i\left(\frac{1}{\mu T}\right)\right)^{(-1)^{i+1}} \\ &= \prod_{i=1}^{2n} \left(\frac{\frac{1}{(-T)^{d_i}}}{\mathsf{Det}(\varphi_i)} P_{2n-i}(T)\right)^{(-1)^{i+1}} \\ &= (-T)^{\chi} \left(\prod_{i=0}^{2n} \mathsf{Det}(\varphi_i)^{(-1)^i}\right) Z(X,T) \end{aligned}$$

où $\chi = \sum_{i=0}^{2n} (-1)^i \mathsf{Deg}(P_i) = \sum_{i=0}^{2n} (-1)^i \mathsf{Dim}_{\mathbb{K}}(E_i)$. En particulier comme $\mathsf{Dim}_{\mathbb{K}}(E_i) = \mathsf{Dim}_{\mathbb{K}}(E_{2n-i})$, on a la formule

$$\frac{\chi}{2} = \sum_{i=0}^{n-1} (-1)^i d_i + (-1)^n \frac{d_n}{2}.$$

D'après la deuxième relation du lemme 1.3 on en déduit la formule

$$\mathsf{Det}(\varphi_i)\mathsf{Det}(\varphi_{2n-i}) = \mu^{d_i}.$$

Pour $i = n$ on a en particulier que $\mathsf{Det}(\varphi_n)^2 = \mu^{d_n}$ d'où

$$\mathsf{Det}(\varphi_n) = \pm \mu^{\frac{d_n}{2}}.$$

Alors

$$\begin{aligned} \prod_{i=0}^{2n} \mathsf{Det}(\varphi_i)^{(-1)^i} &= \prod_{i=0}^{n-1} \mu^{(-1)^i d_i} . \pm \mu^{(-1)^n \frac{d_n}{2}} \\ &= \pm \mu^{\frac{\chi}{2}}. \end{aligned}$$

Ce qui prouve l'équation fonctionelle si $\mu = q^n$.

Observons que comme φ_{2n} est une homothétie de rapport μ dans un espace vectoriel de dimension 1 alors

$$P_{2n}(T) = 1 - \mu T.$$

De même si μ_0 est le rapport de l'homothétie φ_0 de l'espace de dimension 1 E_0 alors

$$P_0(T) = 1 - \mu_0 T.$$

Appliquons le diagramme précédent pour $i = 0$:

$$\begin{tikzcd} E_0 \times E_{2n} \arrow[r, "Q^0_{\overline{X}}"] \arrow[d, "\begin{pmatrix} \varphi_0 & 0 \\ 0 & \varphi_{2n} \end{pmatrix}"'] & E_{2n} \arrow[d, "\varphi_{2n}"] \\ E_0 \times E_{2n} \arrow[r, "Q^0_{\overline{X}}"'] & E_{2n} \end{tikzcd}$$

Ce qui donne pour tout $x \in E_0$ et tout $y \in E_n$:

$$Q^0_X(\varphi_0(x), \varphi_{2n}(y)) = \varphi_{2n}(Q^0_X(x, y)).$$

Soit encore, sachant que φ_0 et φ_{2n} correspondent respectivement à la multipication par μ_0 et μ :

$$Q^0_X(\mu_0 x, \mu y) = \mu Q^0_X(x, y).$$

La bilinéarité ainsi que la non dégénérescence de Q^0_X ammène à

$$\mu_0 \mu = \mu$$

et donc nécéssairement

$$\mu_0 = 1.$$

Ainsi φ_0 est l'identité sur E_0.

Nous admettrons que $\mu = q^n$.

Chapitre 2

Cohomologie étale.

On s'intéresse ici à la fin de la preuve de la rationnalité. On se place dans le cas d'une cohomologie de Weil particulière : la cohomologie étale.

2.1 Déterminant de Hankel.

On fixe dans ce paragraphe un corps $\mathbb{K}$.

Définition 2.1. *Soient n et k deux entiers positifs et $a = (a_i)_{i \geqslant 0}$ une suite d'éléments de $\mathbb{K}$. On définit le* déterminant de Hankel *de rang n et d'ordre k de la suite a la quantité*

$$\mathsf{D}_n^k(a) = \mathsf{Det}\left((a_{n+i+j})_{0 \leqslant i,j \leqslant k}\right).$$

Le déterminant $\mathsf{D}_0^n(a)$, aussi noté $\mathsf{D}^n(a)$ est appelé le n-ième déterminant de Kronecker *de la suite a.*

Proposition 2.2 (Relation de Sylvester)**.** *Soient n un entier positif et D le déterminant de la matrice $(a_{i,j})_{0 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{K})$. Pour toute paire d'entiers i et j entre 0 et n, D peut être vue comme un pôlynome en $a_{i,j}$ de degré au plus 1 ; on note $A_{i,j}$ le coefficient dominant de ces polynômes. Soit d le déterminant de la matrice $(a_{i,j})_{1 \leqslant i,j \leqslant n-1}$, extrait de D en supprimant les lignes et colonnes extrêmales. La relation de Sylvester est*

$$\mathsf{Dd} = A_{0,0}A_{n,n} - A_{0,n}A_{n,0}.$$

Démonstration. Considérons le déterminant D' de la matrice $(b_{i,j})_{0 \leqslant i,j \leqslant n}$ défini par $b_{0,j} = A_{0,j}$, $b_{n,j} = A_{n,j}$ et pour i qui n'est pas 0 ou n on pose $b_{i,j} = \delta_{i,j}$ le symbole de Kronecker.

$$\mathsf{D}' = \begin{vmatrix} A_{0,0} & A_{0,1} & \dots & A_{0,n-1} & A_{0,n} \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & \dots & & 1 & 0 \\ A_{n,0} & A_{n,1} & \dots & A_{n,n-1} & A_{n,n} \end{vmatrix}$$

En développant par rapport à la première colonne on arrive à

$$\mathsf{D}' = A_{0,0} \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & & 1 & 0 \\ A_{n,1} & \dots & A_{n,n-1} & A_{n,n} \end{vmatrix} + (-1)^{n+1} A_{n,0} \begin{vmatrix} A_{0,1} & \dots & A_{0,n-1} & A_{0,n} \\ 1 & 0 & \dots & 0 \\ 0 & \ddots & 0 & \vdots \\ 0 & \dots & 1 & 0 \end{vmatrix}$$

Enfin en développant par rapport à la dernière colonne, et sachant que le déterminant de l'identité est 1, on obtient

$$\mathsf{D}' = A_{0,0}A_{n,n} + (-1)^{n+1}(-1)^n A_{n,0}A_{0,n} = A_{0,0}A_{n,n} - A_{n,0}A_{0,n}.$$

Calculons ce determiant d'une autre manière. Commençons par observer dans un premier temps que par définition

$$\mathsf{D} = \sum a_{i,j}A_{i,j},$$

où, à j fixé, la somme porte sur l'indice i et inversement. Observons de plus que pour $k \neq j$

$$\sum_{i=0}^{n} a_{i,k}A_{i,j} = 0.$$

En effet cette somme correspond au calcul d'un déterminant où la colonne k et la colonne j sont identiques. On observe la même situation en inversant lignes et colonnes. Sachant que le determinant est une application multipicative de $\mathcal{M}_n(\mathbb{K})$ dans $\mathbb{K}$ et est invariant par transposé, pour calculer la quantité DD', il suffit de calculer le déterminant issu de la multiplication des deux matrices en présence. Les observations amènent donc

$$\mathsf{DD}' = \begin{vmatrix} \mathsf{D} & a_{0,1} & \dots & a_{0,n-1} & 0 \\ 0 & a_{1,1} & \dots & a_{1,n-1} & 0 \\ \vdots & \vdots & a_{i,j} & \vdots & \vdots \\ \vdots & a_{n-1,1} & \dots & a_{n-1,n-1} & 0 \\ 0 & a_{n,1} & \dots & a_{n,n-1} & \mathsf{D} \end{vmatrix}$$

ce qui prouve que $\mathsf{DD}' = \mathsf{D}^2\mathsf{d}$. Si D est non nul, on en déduit que $\mathsf{D}' = \mathsf{Dd}$. Si D est nul, on démontre très fastidieusement que $\mathsf{D}' = 0$. □

Corollaire 2.3. *Soient n et k deux entiers positifs tels que $k \geqslant 1$ et D_n^k le déterminant de Hankel de rang n d'ordre k d'une suite de $\mathbb{K}$. On a alors la relation*

$$\mathsf{D}_n^k\mathsf{D}_{n+2}^{k-2} = \mathsf{D}_{n+2}^{k-1}\mathsf{D}_n^{k-1} - \left(\mathsf{D}_{n+1}^{k-1}\right)^2$$

où l'on convient que $\mathsf{D}_n^{-1} = 1$.

Démonstration. Pour $k \geqslant 2$, c'est exactement la relation de Sylvester appliquée à la matrice de Hankel D_n^k. Pour $k = 1$, il faut voir que

$$\mathsf{D}_n^1 = \mathsf{D}_{n+2}^0\mathsf{D}_n^0 - \left(\mathsf{D}_{n+1}^0\right)^2$$

ce qui n'est qu'un gentil calcul de déterminant. □

Lemme 2.4. *Soit a une suite d'éléments de $\mathbb{K}$ non stationnaire, s'il existe k et n_0 tels que, pour tout $n \geqslant n_0$, $\mathsf{D}_n^k(a) = 0$ alors il existe h et n_1 tels que $\mathsf{D}_n^h(a) = 0$ pour $n \geqslant n_1$ et $\mathsf{D}_n^{h-1}(a) \neq 0$ pour $n \geqslant n_1 + 1$.*

Démonstration. Nous dirons que k est admissible si pour n suffisamment grand $\mathsf{D}_n^k(a) = 0$. Par hypothèse, il existe k admissible : soit h le plus petit entier admissible. Alors $h \neq 0$: en effet la suite étant non stationnaire les $D_n^0(a) = a_n$ sont non nuls pour n aussi grand soit-il. Ainsi $h \geqslant 1$. Soit n_1 le plus petit entier tel que $\mathsf{D}_n^h(a) = 0$ pour $n \geqslant n_1$. Il s'agit de voir que pour tout entier

$n \geqslant n_1 + 1$ on a $\mathsf{D}_n^{h-1} \neq 0$, supposons le contraire : il existe m_0 tel que $\mathsf{D}_{m_0}^{h-1} = 0$. Le corollaire 2.3 nous indique :

$$\mathsf{D}_{m_0}^h \mathsf{D}_{m_0+2}^{h-2} = \mathsf{D}_{m_0+2}^{h-1} \mathsf{D}_{m_0}^{h-1} - \left(\mathsf{D}_{m_0+1}^{h-1}\right)^2.$$

Or comme $m_0 \geqslant n_0 + 1$ on a $\mathsf{D}_{m_0}^h = 0$ et par hypothèse $\mathsf{D}_{m_0}^{h-1} = 0$, ce qui amène donc $\mathsf{D}_{m_0+1}^{h-1} = 0$. En continuant ainsi par récurrence, on prouve facilement que pour tout $m \geqslant m_0$ $\mathsf{D}_m^{h-1} = 0$, ce qui contredit la minimalité de h. □

Proposition 2.5. *Pour que la serie formelle*

$$f(X) = \sum_{n=0}^{+\infty} a_n X^n$$

à coefficient dans $\mathbb{K}$ *soit une fraction rationelle, il faut et il suffit qu'il existe* $k \in \mathbb{N}$ *tel que pour tout* n *assez grand* $\mathsf{D}_n^k(a) = 0$*, où* $a = (a_i)_{i \in \mathbb{N}}$*.*

Démonstration. Supposons que f soit rationelle. Soit $Q = \sum_{i=0}^{k} q_i X^i$ un dénominateur. Comme Qf est un pôlynome de degré d disons, en effectuant le produit

$$\left(\sum_{i=0}^{k} q_i X^i\right) \left(\sum_{n=0}^{+\infty} a_n X^n\right) = \sum_{n \geqslant 0} \left(\sum_{i+j=n} q_i a_j\right) X^n$$

on en déduit que $\sum_{i+j=n} q_i a_j = 0$ pour $n \geqslant d$. Ces relations de dépendance linéaire nous indique donc que pour $n + k > d$ les déterminants de Hankel $\mathsf{D}_n^k(a)$ sont nuls.

Montrons à présent la réciproque. Si la suite a est stationnaire, à partir du rang N par exemple, on a

$$f(X) = \sum_{n=0}^{N-1} a_n X^n + a_N \sum_{i=N}^{+\infty} X^i = \sum_{n=0}^{N-1} a_n X^n + a_N \frac{X^N}{1 - X}.$$

Ce qui prouve la rationalité. On peut donc supposer a non stationnaire. Les hypothèses nous permettent alors d'appliquer le lemme 2.4 : il existe $h \in \mathbb{N}_{>0}$ et $n_1 \in \mathbb{N}$ tels que $\mathsf{D}_n^h(a) = 0$ pour $n \geqslant n_1$ et $\mathsf{D}_n^{h-1}(a) \neq 0$ pour $n \geqslant n_1 + 1$. On considère alors le système linéaire d'inconnus $Y_0, ..., Y_h$

$$(E_n) \qquad \sum_{i=0}^{h} a_{n-i} Y_i = 0$$

pour n compris entre $N + h$ et $N + 2h$ pour un certain $N \geqslant n_1$. Le déterminant de la matrice associé étant $\mathsf{D}_N^h(a) = 0$; on en déduit qu'il existe une infinité de solutions à ce système. De plus le mineur $\mathsf{D}_{N+1}^{h-1}(a) \neq 0$ ce qui signifie que le rang de la matrice associé est $h - 1$. Il existe donc une unique solution telle que $Y_h = 1$. La solution de ce système pour $N = n_1$ est donc aussi une solution pour le système avec $N \geqslant n_1$. Posons

$$Q(X) = \sum_{k \geqslant 0} Y_k X^k$$

où $Y_h = 1$ et $Y_n = 0$ pour les $n > h$. Ainsi $Q(X) \in \mathbb{K}[X]$ de degré h. Mais alors

$$\begin{aligned} fQ &= \left(\sum_{n\geqslant 0} a_n X^n\right)\left(\sum_{k\geqslant 0} Y_k X^k\right) \\ &= \sum_{n\geqslant 0}\left(\sum_{i+j=n} a_i Y_j\right) X^n \\ &= \sum_{n=0}^{n_1}\left(\sum_{i+j=n} a_i Y_j\right) X^n \end{aligned}$$

car les Y_i sont solution de (E_n) pour $n \geqslant n_1$. Et donc f est une fraction rationelle. □

Corollaire 2.6. *Pour que la série formelle à coefficient dans* $\mathbb{K}$ *:*

$$f(X) = \sum_{n=0}^{+\infty} a_n X^n$$

soit une fraction rationelle, il faut et il suffit que pour tout n *assez grand le* n*-ième determiant de Kronecker* $\mathsf{D}^n(a)$ *soit nul ; où* $a = (a_i)_{i\in\mathbb{N}}$.

Démonstration. Posons

$$A_n^k(a) := {}^t(a_n, a_{n+1}, ..., a_{n+k}).$$

On raisonne comme dans la preuve de la proposition précédente : si $\sum_{i=0}^{k} q_i X^i$ est un dénominateur de f, alors pour n assez grand, on a une relation de dépendance linéaire. Comme les coefficients de cette dépendance linéaire sont les q_i, en prenant n suffisamment grand, on a

$$\sum_{i=0}^{k} q_i A_{n-k}^n(a) = 0.$$

On conclut en observant que $\mathsf{D}^n(a) = \mathsf{Det}\left((A_i^n(a))_{0\leqslant i\leqslant n}\right)$. Réciproquement, supposons que pour $n \geqslant n_0$ on ait $\mathsf{D}^n(a) = 0$. On va montrer par récurrence sur m que pour tout entier m positif $\mathsf{D}_m^n(a) = 0$. Le cas $m = 0$ correspond au n-ième determinant de Kronecker qui est nul par hypothèse ; supposons que pour un m quelconque fixé $\mathsf{D}_m^n(a) = 0$ (n désigne toujours un entier plus grand que n_0). Alors en appliquant le corollaire de la relation de Sylvester (corollaire 2.3) on obtient

$$\underbrace{\mathsf{D}_m^{n+1}(a)}_{=0}\,\mathsf{D}_{m+2}^{n-1}(a) = \mathsf{D}_{m+2}^n(a)\,\underbrace{\mathsf{D}_m^n(a)}_{=0} - \left(\mathsf{D}_{m+1}^n(a)\right)^2.$$

Ce qui prouve le résultat souhaité. Alors la proposition précédente justifie que f est une fraction rationelle. □

2.2 Fin de la preuve de la rationnalité.

Théorème 2.7. *Soit* X *une variété projective lisse sur un corps fini* $\mathbb{F}_q$*, où* q *est une puissance d'un nombre premier* p*. On définit une cohomologie sur le corps des nombres* l*-adiques où* l *est un nombre premier différent de* p*, appelé* cohomologie étale *comme*

$$\mathsf{H}^i_{ét}(X, \mathbb{Q}_l) := \varprojlim \mathsf{H}^i_{ét}(X, \mathbb{Z}/l^n\mathbb{Z}).$$

Les cohomologies étales (l variant et distinct de p) sont des cohomologies de Weil (lorsque l'on restreint la catégorie de départ à la catégorie des variétés projectives lisse sur $\mathbb{F}_q$).

On fixe une variété projective lisse X de dimension n sur $\mathbb{F}_q$ et une cohomologie étale $\mathsf{H}^*_{\text{ét}}(\bullet, \mathbb{Q}_l)$ que l'on note $\mathsf{H}^*(\bullet)$ (avec l distinct de la caractéristique de $\mathbb{F}_q$).

Nous avons démontrer que la fonction zeta s'écrit sous la forme

$$Z(X,T) = \frac{P_1(T)P_3(T)...P_{2n-1}(T)}{P_0(T)P_2(T)...P_{2n}(T)}$$

où $P_0(T) = 1-T$, $P_{2n}(T) = 1 - q^nT$ et pour $1 \leqslant i \leqslant 2n-1$ on a $P_i(T) = \mathsf{Det}(\mathsf{H}^i(\mathsf{Fro})) \in \mathbb{Q}_l[T]$. Nous avons de plus observé (dans l'introduction) que le développement en série entière de la fonctin zeta est à coefficient rationel.

Lorsque l'on regarde cette série dans $\mathbb{Q}_l[\![T]\!]$, on sait qu'il s'agit du développement d'une fraction rationelle, ce qui signifie que pour tout entier n suffisamment grand le n-ième déterminant de Kronecker de la suite $(a_k)_{k\in\mathbb{N}}$ est nul ; or comme ce déterminant vu dans $\mathbb{Q}_l$ vient d'un détermiant vu dans $\mathbb{Q}$, il est nul dans $\mathbb{Q}_l$ si et seulement si il l'est dans $\mathbb{Q}$. Donc pour tout n suffisamment grand le n-ième déterminant de Kronecker de la suite $(a_k)_{k\in\mathbb{N}}$ est nul dans $\mathbb{Q}$, donc il s'agit d'une fraction rationelle à coefficient rationel :

$$Z(X,T) \in \mathbb{Q}(T).$$

Supposons l'analogue de l'hypothèse Riemann vérifiée :

Lemme 2.8 (Deligne)**.** *Pour chaque i et chaque $l \neq p$, les valeurs propres de $\mathsf{H}^*(\mathsf{Fro}, \mathbb{Q}_l)$ sont des nombres algèbriques dont tous les conjugués complexes sont de valeur absolue*

$$q^{\frac{i}{2}}.$$

Considérons $\mathbb{K}$ le corps engendré sur $\mathbb{Q}$ par les racines des P_i (il s'agit donc d'un sous-corps de $\overline{\mathbb{Q}_l}$ une cloture algèbrique de $\mathbb{Q}_l$). Si l'on pose P le produit de P_i pour i impair et Q le produit des pairs. Alors $Z(X,T) = P/Q \in \mathbb{Q}(T)$ et grace au lemme on en déduit que les racines de P_i sont stables par le groupe de Galois de $\mathbb{K}$ sur $\mathbb{Q}$ et ainsi les P_i sont à coefficient rationel.

Chapitre 3

Formule de trace.

Ici, on esquisse une démonstration du théorème 1.2. On fixe toujours $\mathbb{K}$ un corps et $\mathsf{H}^*(\bullet)$ une cohomologie de Weil.

3.1 Généraltités.

Définition 3.1. *Soit X une variété. On définit une application degré*

$$\langle\rangle : \mathsf{H}^*(X) \longrightarrow \mathbb{K}$$

qui est nulle sur $\mathsf{H}^i(X)$ pour $i < 2\mathsf{Dim}(X)$ et est le morphisme d'orientation sur $\mathsf{H}^{2\mathsf{Dim}(X)}(X)$.

Définition 3.2. *Soient X et Y deux variétés de dimension respective n et m. Soit $u = a \otimes b \in \mathsf{H}^*(X \times Y) \simeq \mathsf{H}^*(X) \otimes_{\mathbb{K}} \mathsf{H}^*(Y)$. On définit*

$$\begin{array}{rcl} u^* : \mathsf{H}^*(X) & \longrightarrow & \mathsf{H}^*(Y) \\ c & \longmapsto & \langle Q_X^*(c, a)\rangle b. \end{array}$$

Explicitement : si $a \otimes b \in \mathsf{H}^\alpha(X) \otimes_{\mathbb{K}} \mathsf{H}^\beta(Y)$ alors $u^* = 0$ sur $\mathsf{H}^i(X)$ pour $i \neq 2n - \alpha$ et pour $c \in \mathsf{H}^{2n-\alpha}(X)$:

$$u^*(c) = \langle Q_X^{2n-\alpha}(c, a)\rangle b.$$

Théorème 3.3. *Soient X et Y deux variétés alors*

$$\begin{array}{rcl} \mathsf{H}^*(X \times Y) & \longrightarrow & \mathsf{Hom}_{\mathbb{K}}(\mathsf{H}^*(X), \mathsf{H}^*(Y)) \\ u & \longmapsto & u^* \end{array}$$

est un isomorphisme.

Démonstration. La dualité de Poincaré prouve que

$$\begin{array}{rcl} \mathsf{H}^{2n-i}(X) & \longrightarrow & \mathsf{Hom}_{\mathbb{K}}(\mathsf{H}^i(X), \mathbb{K}) \\ a & \longmapsto & \langle Q_X^i(\bullet, a)\rangle \end{array}$$

est un isomorphisme. La formule de Künneth et un résulat classique d'algèbre linéaire permettent alors de conclure. □

Ainsi, se donner un élément de $\mathsf{H}^*(X \times Y)$ pour deux variétés X et Y équivaut à se donner un morphisme $\mathbb{K}$ linéaire de $\mathsf{H}^*(X)$ dans $\mathsf{H}^*(Y)$, et réciproquement.

Définition 3.4. *Soient X et Y deux variétés et $u \in \mathsf{H}^*(X \times Y)$. On définit ${}^t u$ sur les composantes homogènes de la manière suivante. Pour $a \otimes b \in \mathsf{H}^\alpha(X) \otimes_{\mathbb{K}} \mathsf{H}^\beta(Y)$ on pose*

$${}^t(a \otimes b) = (-1)^{\alpha\beta} b \otimes a.$$

Théorème 3.5. *Soient X et Y deux variétés de dimension respective n et m et d un entier positif plus petit que $2m$. Alors pour tout $v \in \mathsf{H}^{2n+d}(X \times Y)$ et tout $w \in \mathsf{H}^{2m-d}(Y \times X)$*

$$\langle v.{}^t w\rangle = \sum_{i=0}^{2n} (-1)^i \mathsf{Tr}(w^* v^*_{|_{\mathsf{H}^i(X)}}).$$

Démonstration. Par linéarité, on se ramène au cas où

$$v \in \mathsf{H}^\alpha(X) \otimes_{\mathbb{K}} \mathsf{H}^\beta(Y),$$

$$w \in \mathsf{H}^{2m-\beta}(Y) \otimes_{\mathbb{K}} \mathsf{H}^{2n-\alpha}(X)$$

où $\alpha + \beta = 2n + d$. Il s'agit donc de démontrer que

$$Q_X^{\alpha+\beta}(v, {}^t w) = (-1)^{2n-\alpha} \mathsf{Tr}(w^* v^*_{|_{\mathsf{H}^{2n-\alpha}(X)}}).$$

(On identifie $\mathsf{H}^{2n}(X)$ à $\mathbb{K}$, on ommet donc les brackets $\langle\rangle$).

Fixons une base $\{e_1, ..., e_d\}$ de $\mathsf{H}^\alpha(X)$, où d est la dimension de ce $\mathbb{K}$ espace vectoriel. On choisit une base $\{f_1, ..., f_d\}$ de $H^{2n-\alpha}(X)$ telle que pour tout entier i compris entre 1 et d on ait $Q_X^\alpha(e_i, f_i) \neq 0$. En appliquant le procédé d'orthonormalisation de Gram-Schmidt on peut supposer que

$$\forall (i,j) \in [\![1, d]\!]^2, \quad Q_X^\alpha(e_i, f_j) = \delta_{i,j}.$$

En réordonnant les termes on peut écrire

$$v = \sum_{i=1}^{d} e_i \otimes b_i, \qquad w = \sum_{j=1}^{d} c_j \otimes f_j.$$

Où les b_i et c_j sont des vecteurs de respectivement $\mathsf{H}^\beta(Y)$ et $\mathsf{H}^{2m-i}(Y)$. En utilisant la fonctorialité de la dualité de Poincaré avec l'isomorphisme de Künneth on trouve la formule

$$Q_{X\times Y}^{\alpha+\beta}(e_i \otimes b_i, f_j \otimes c_j) = (-1)^{\alpha\beta} Q_X^\alpha(e_i, f_j) Q_Y^\beta(b_i, c_j).$$

Il suffit maintenant de calculer :

$$\begin{aligned}
Q_{X\times Y}^{\alpha+\beta}(v, {}^t w) &= Q_{X\times Y}^{\alpha+\beta}\left(\sum_{i=1}^{d} e_i \otimes b_i, (-1)^{\alpha\beta} \sum_{j=1}^{d} f_j \otimes c_j\right) \\
&= (-1)^{\alpha\beta} \sum_{0 \leqslant i,j \leqslant d} Q_{X\times Y}^{\alpha+\beta}(e_i \otimes b_i, c_j \otimes f_j) \\
&= \sum_{0 \leqslant i,j \leqslant d} Q_X^\alpha(e_i, f_j) Q_Y^\beta(b_i, c_j) \\
&= \sum_{i=1}^{d} Q_Y^\beta(b_i, c_j).
\end{aligned}$$

D'autre part

$$\begin{aligned}
w^*v^*(f_k) &= w^*\left(\sum_{i=1}^{d}(e_i\otimes b_i)^*(f_k)\right)\\
&= w^*\left(\sum_{i=1}^{d} Q_X^{2n-\alpha}(f_k,e_i)b_i\right)\\
&=^* (-1)^{2n-\alpha}w^*\left(\sum_{i=1}^{d} Q_X^{\alpha}(e_i,f_k)b_i\right)\\
&= (-1)^{2n-\alpha}w^*(b_k)\\
&= (-1)^{2n-\alpha}\sum_{j=1}^{d}(c_j\otimes f_j)^*(b_k)\\
&= (-1)^{2n-\alpha}\sum_{j=1}^{d} Q_Y^{\beta}(b_k,c_j)f_j.
\end{aligned}$$

[(*) : Axiomatiquement $\mathsf{H}^*(X)$ est une algèbre anti-commutative, et le morphisme Q_X^*, n'est autre que la multiplication.]

La trace étant la somme des coefficients diagonaux, c'est à dire la somme des coefficients associés à f_k dans $w^*v^*(f_k)$. C'est à dire la somme pour k entre 1 et d de $(-1)^{2n-\alpha}Q_Y^{\beta}(b_k,c_k)$, qui permet de conclure. □

3.2 Lien avec les cycles.

Définition 3.6. *Soit X une variété. On définit une application degré*

$$\langle\rangle : \mathsf{C}^*(X) \longrightarrow \mathbb{Z}$$

qui est nul pour les p-cycles, $p < \mathsf{Dim}(X)$ et $\langle\sum m_\alpha P_\alpha\rangle = \sum m_\alpha$ pour des $\mathsf{Dim}(X)$-cycles.

Soit $f : X \longrightarrow X$ un endomorphisme avec des points fixes isolés (typiquement le Frobenius). On note $L(f,X)$ la cardinalité de ses points fixes (comptés avec leur multiplicité). Notons Δ le cycle associé à l'image du morphisme diagonal $X \longrightarrow X\times X$ et Γ_f celui associé au graphe de f.

$$\Delta \in C^*(X\times X), \qquad \Gamma_f \in C^*(X\times X).$$

Naturellement le cycle $\Delta.\Gamma_f$ correspond aux points fixes de f. Précisement

$$L(f,X) = \langle\Delta.\Gamma_f\rangle$$

Lemme 3.7.

$$\left\langle\gamma(\Delta).{}^t\gamma(\Gamma_f)\right\rangle = \langle\Delta.\Gamma_f\rangle$$

où $\gamma = \gamma_{X\times X}$ est donné par l'axiome C des cohomologies de Weil.

Démonstration. Supposons que la partie homogène de degré n de $\Delta.\Gamma_f$ soit $\sum_\alpha m_\alpha P_\alpha$. C'est à dire que m_α est la multiplicité du point fixe P_α, et donc que

$$\langle\Delta.\Gamma_f\rangle = \sum_\alpha m_\alpha.$$

D'autre part il est évident que $\gamma(\Delta) = {}^t\gamma(\Delta)$. Ainsi

$$\begin{aligned}
\left\langle \gamma(\Delta).{}^t\gamma(\Gamma_f)\right\rangle &= \left\langle {}^t\gamma(\Delta).{}^t\gamma(\Gamma_f)\right\rangle \\
&= \left\langle {}^t\gamma(\Delta.\Gamma_f)\right\rangle \\
&= \langle \gamma(\Delta.\Gamma_f)\rangle \\
&= \sum_\alpha m_\alpha \underbrace{\gamma_{P_\alpha}(P_\alpha)}_{=1}
\end{aligned}$$

$\square$

Lemme 3.8. *Soient X une variété projective lisse sur $\mathbb{F}_q$ et $m \in \mathbb{N}_{>0}$, $x \in X$. Alors*

$$x \in X(\mathbb{F}_{q^m}) \Longleftrightarrow \mathsf{Fro}^m(x) = x.$$

Ce lemme très facile nous indique que la cardinalité de $X(\mathbb{F}_{q^m})$ correspond aux points fixes de la m-ième puissance du Frobenius. Les points fixes du Frobenius vérifient l'équation dans X : $x^q = x$, qui admet un nombre fini de solutions (car les x sont dans $\mathbb{P}^n(\mathbb{F}_q)$), donc les points fixes du Frobenius sont isolés, et il en va naturelement de même pour les itérés. En appliquant le théorème 3.5

$$N_m = L(\mathsf{Fro}^m, \overline{X}) = \sum_{i=0}^{2\mathsf{Dim}(X)} (-1)^i \mathsf{Tr}(\gamma(\Delta)^* \gamma(\Gamma_{\mathsf{Fro}^m})^*_{|_{\mathsf{H}^i(\overline{X})}}).$$

Nous admetterons le dernier pas qui mène au théorème 1.2 :

$$\mathsf{Tr}(\gamma(\Delta)^* \gamma(\Gamma_{\mathsf{Fro}^m})^*_{|_{\mathsf{H}^i(\overline{X})}}) = \mathsf{Tr}(\mathsf{H}^i(\mathsf{Fro}^m)).$$