Les conjectures de Weil

Bernard Le Stum

Université de Rennes 1

24 décembre 2012

Sommaire

Exemple

On cherche le nombre de couples $(x, y) \in \mathbf{F}_q^\times$ tels que $y^2 = x^3 + x$. Ici $\mathbf{F}_q$ désigne un corps fini avec q impair.

On considère alors la courbe affine X définie par

$$y^2 = x^3 + x, \quad y \neq 0 \quad \subset \quad \mathbf{A}^2_{\mathbf{F}_q}$$

ainsi que sa fermeture projective $\overline{X}$ définie par

$$y^2 z = x^3 + xz^2 \quad \subset \quad \mathbf{P}^2_{\mathbf{F}_q}.$$

On cherche donc le nombre de points rationnels de X. Et il revient au même de compter ceux de $\overline{X}$: on a

$$N(\overline{X}) = N(X) + |\{a \in \mathbf{F}_q, a^3 + a = 0\}| + |\{a \in \mathbf{F}_q, a^3 = 0\}|$$

$$= \begin{cases} N(X) + 1 + 1 & \text{si} \quad \sqrt{-1} \notin \mathbf{F}_q \quad (q \equiv -1 \mod 4) \\ N(X) + 3 + 1 & \text{si} \quad \sqrt{-1} \in F_q \quad (q \equiv 1 \mod 4) \end{cases}$$

Exemple (suite)

On rappelle qu'il y a exactement $\frac{q-1}{2}$ carrés dans $\mathbf{F}_q^\times$.

Cas $q \equiv -1 \mod 4$ (i.e. $q = 3, 7, 27, \ldots$) : puisque -1 nest pas un carré dans $\mathbf{F}_q$, si $c \in \mathbf{F}_q^\times$, on aura

$$c \text{ ou } -c \text{ est un carré mais pas les deux.}$$

On voit donc que si $a \in \mathbf{F}_q$, alors

$a^3 + a$ ou $(-a)^3 + (-a) = -(a^3 + a)$ est un carré mais pas les deux.

Il y a donc $\frac{q-1}{2}$ fois où $a^3 + a$ est de la forme b^2. Et quand cela arrive, il y a exactement 2 possibilités pour b. On a donc

$$N(X) = 2 \times \frac{q-1}{2} = q - 1 \quad \text{et} \quad N(\overline{X}) = (q-1) + 2 = q + 1.$$

Le cas ou $q \equiv 1 \mod 4$ (i.e. $q = 5, 9, 25, \ldots$) ne se traite pas

Exemple (fin)

Cas $q = 5$: on dresse la table

a	-2	-1	1	2
a^2	-1	1	1	-1
a^3	2	-1	1	-2
$a^3 + a$	0	-2	2	0

On voit donc qu'un élément de la form $a^3 + a$ ne peut pas être un carré non nul si bien que $N(X) = 0$ et $N(\overline{X}) = 4$.

Cas $q = 9$: On écrit $\mathbf{F}_9 = \mathbf{F}_3[\sqrt{-1}]$ et on calcule

$$a^3 + a = \overline{a} + a = 2\mathrm{Re}(a) = -\mathrm{Re}(a) \in \mathbf{F}_3 = \{-1, 0, 1\}.$$

C'est toujours un carré dans $\mathbf{F}_9$ et il est non nul si et seulement si $\mathrm{Re}(a) \neq 0$. On obtient ainsi $9 - 3 = 6$ possibilités pour a. On a donc

$$N(X) = 2 \times 6 = 12 \quad \text{et} \quad N(\overline{X}) = 12 + 4 = 16.$$

Compter les points

On se donne plus généralement une variété algébrique X sur $\mathbf{F}_q$ ou $\mathbf{F}_q$ est un corps fini avec q elements (q une puissance d'un nombre premier p).

On veut faire la chose suivante :

- Calculer le nombre de points rationnels $N(X) := |X(\mathbf{F}_q)|$ de X

Plus généralement, si $\mathbf{F}_{q^r}/\mathbf{F}_q$ est une extension finie, on veut calculer le nombre

$$N_r(X) := |X(\mathbf{F}_{q^r})| \quad \Big(= N(X \otimes_{\mathbf{F}_q} \mathbf{F}_{q^r})\Big)$$

de points de X à valeur dans $\mathbf{F}_{q^r}$.

On appellera *nombre de Weil* de poids $m \in \mathbf{N}$, un nombre algébrique dont les valeurs absolues archimédiennes valent $q^{\frac{m}{2}}$ ($1 + 2\sqrt{-1}$ par exemple si $q = 5$).

On peut alors énoncer les conjectures de Weil ([4]) :

Conjectures de Weil

Théorème (Rationalité, version additive)

Il existe un nombre fini d'entiers algébriques α_i, β_j tels que pour tout r, on ait $N_r(X) = \sum \alpha_i^r - \sum \beta_j^r$.

Théorème (Équation fonctionnelle, version additive)

Si X est propre et lisse de pure dimension d, alors l'application $\gamma \mapsto q^d/\gamma$ induit une permutations des α_i et une permutation des β_j.

Théorème (Pureté, version additive)

Si X est de dimension d, les entiers algébriques α_i et β_j sont des nombres de Weil de poids $\in [0, 2d]$. Si X est propre et lisse, les poids sont pairs pour les α_i et impairs pour les β_j.

Partie topologique des conjectures

On dira que X (propre et lisse) provient par réduction d'une variété algébrique complexe V si on peut écrire

$$X = \mathcal{X} \otimes_R \mathbf{F}_q \quad \text{et} \quad V = \mathcal{X} \otimes_R \mathbf{C}$$

avec $\mathbf{F}_q \twoheadleftarrow R \hookrightarrow \mathbf{C}$ et $\mathcal{X}$ schéma propre et lisse sur R.

Si c'est le cas, on aura pour m pair :

$$|\{\alpha_i, \quad \text{poids}(\alpha_i) = m\}| = \text{rang } \mathrm{H}_m(V)$$

et pour m impair :

$$|\{\beta_i, \quad \text{poids}(\beta_i) = m\}| = \text{rang } \mathrm{H}_m(V).$$

Les conjectures de Weil ont été démontrée par Dwork (rationalité, [2]), Grothendieck (équation fonctionnelle, [3]) et Deligne (pureté, [1]).

Exemple

On considère de nouveau la courbe (q impair)

$$\overline{X}: \quad y^2z = x^3 + xz^2 \quad \subset \quad \mathbf{P}^2_{\mathbf{F}_q}.$$

Les nombre de Weil de poids 0 et 2 sont 1 et q, respectivement. Et il y a deux nombres de Weil de poids 1 dont le produit vaut q. Si $q \equiv -1 \mod 4$, on trouve $\pm\sqrt{-q}$. On aura donc bien

$$N(\overline{X}) = 1 + q - \sqrt{-q} + \sqrt{-q} = q + 1.$$

Le cas $q = 9$ est le N_2 du cas $q = 3$ et on a bien

$$1^2 + 3^2 - (\sqrt{-3})^2 - (-\sqrt{-3})^2 = 1 + 9 + 3 + 3 = 16.$$

Lorsque $q = 5$, ont peut montrer que les nombres de Weil de poids 1 sont $1 \pm 2\sqrt{-1}$. On retrouve bien $N(\overline{X}) = 4$ et on découvre $N_2(\overline{X}) = 32$ (on a donc 28 solutions avec $x, y \neq 0$ pour $y^2 = x^3 + x$ sur $\mathbf{F}_{25} = \mathbf{F}_5[\sqrt{2}]$).

Séries de Dirichlet

L'*anneau des séries de Dirichlet* est l'algèbre complète A du monoïde multiplicatif $\mathbf{N} \setminus \{0\}$ sur $\mathbf{Z}$ (ensemble des suites $(a_n)_{n>0}$ dans $\mathbf{Z}$ avec

$$(a_n)(b_n) = (c_n) \Leftrightarrow c_n = \sum_{ij=n} a_i b_j \quad).$$

C'est un anneau séparé complet ($\mathbf{Z}$ muni de la topologie discrète et $A = \prod_{\mathbf{N}\setminus\{0\}} \mathbf{Z}$) et on note traditionnellement $n^{-s} \in A$ les vecteurs de la base orthogonale canonique (la suite qui vaut 1 à la n-ème place et 0 ailleurs). Tout élément de A s'écrit donc de manière unique $\sum a_n n^{-s}$ et on a la formule $n^{-s} m^{-s} = (nm)^{-s}$.

On peut remarquer que si P désigne l'ensemble des nombres premiers, on a

$$A \simeq \mathbf{Z}[[\{p^{-s}\}_{p\in P}]]$$

(utiliser simplement le fait que P est une base du monoïde $\mathbf{N} \setminus \{0\}$).

Fonctions zêta arithmétiques

On désignera par $|X|$ l'ensemble des points fermés d'un schéma X. Lorsque X est un schéma de type fini sur $\mathbf{Z}$, on voit aisément que $x \in |X|$ si et seulement si son corps résiduel $k(x)$ est fini. On pose alors

$$N(x) = |k(x)|.$$

La série de Dirichlet $1 - N(x)^{-s}$ est inversible et le produit

$$\zeta(X, s) := \prod_{x \in |X|} \frac{1}{1 - N(x)^{-s}}$$

converge (dans l'anneau des séries de Dirichlet). C'est la *fonction zêta arithmétique* de X. Dans le cas particulier ou $X = \operatorname{Spec} \mathbf{Z}$, on retrouve la fonction zêta de Riemann

$$\zeta(s) = \sum n^{-s}.$$

Fonctions zêta géométriques

Lorsque X est une variété algébrique sur $\mathbf{F}_q$, si on pose

$$\deg x := [k(x) : \mathbf{F}_q]$$

pour $x \in |X|$, on aura $N(x) = q^{\deg x}$ et donc

$$\zeta(X, s) := \prod_{x \in |X|} \frac{1}{1 - (q^{-s})^{\deg x}}.$$

En fait, le produit

$$Z(X, t) := \prod_{x \in |X|} \frac{1}{1 - t^{\deg x}}$$

converge dans $\mathbf{Z}[[t]]$. C'est la *fonction zêta géométrique* de X et on a

$$\zeta(X, s) = Z(X, q^{-s}).$$

Réciproquement, si X est un schéma de type fini sur $\mathbf{Z}$, on aura

$$\zeta(X,s) = \prod_{p \in P} Z(X_p, p^{-s})$$

où P désigne l'ensemble des nombres premiers et $X_p := X \otimes_{\mathbf{Z}} \mathbf{F}_p$.

Supposons de nouveau que X soit une variété sur $\mathbf{F}_q$. On a alors

$$Z(X,t) = \exp\left(\sum_{r=1}^{\infty} N_r(X)\frac{t^r}{r}\right).$$

Exemple

Pour la courbe $\overline{X}$ d'équation $y^2z = x^3 + xz^2$, on peut montrer que

$$Z(\overline{X},t) = \frac{1 - at + qt^2}{(1-t)(1-qt)}$$

avec $a = 1 + q - N(\overline{X})$.

Théorème (Conjectures de Weil, rationalité, version multiplicative)

On a $Z(X,t) \in \mathbf{Q}(t)$.

Théorème (Conjectures de Weil, equation fonctionnelle, version multiplicative)

Si X *est propre et lisse de pure dimension* d, *alors*

$$Z(X, \frac{1}{q^d t}) = \pm q^{\frac{dE}{2}} t^E Z(X,t) \quad \text{avec} \quad E \in \mathbf{Z}.$$

Théorème (Conjectures de Weil, pureté, version multiplicative)

Si X *est de dimension* d, *les zéros et les pôles de* $Z(X,t)$ *sont des nombres de Weil de poids* $\in [0, 2d]$. *Si* X *est propre et lisse, les poids des zéros sont pairs ceux des pôles sont impairs.*

Un *polynôme de Weil (pur de poids m)* est un polynôme

$$P := \prod_{i=1}^{B} (1 - \gamma_i t) \in \mathbf{Z}[t]$$

ou les γ_i sont des nombres de Weil (de même poids m).

Théorème (Conjectures de Weil, version raffinée)

On peut écrire

$$Z(X,t) = \prod_{i=0}^{2d} P_i(t)^{(-1)^{i+1}}$$

ou les P_i sont des polynômes de Weil. Si X est propre et lisse de pure dimension d, les P_i sont purs de poids i et on a

$$P_{2d-i}(t) = C_i t^{B_i} P_i(\frac{1}{q^d t}) \quad \text{avec} \quad C_i \in \mathbf{Z}, B_i \in \mathbf{N}.$$

De plus, $B_i = \mathrm{rang} H_i(V)$ si X provient par réduction d'une variété V.

Théorème du point fixe

Si X est une variété algébrique sur $\mathbf{F}_q$, l'ensemble des points fixes du Frobenius $F : x \mapsto x^q$ agissant sur X est exactement $X(\mathbf{F}_q)$. Or on a :

Théorème (Lefschetz)

Si X est un espace topologique compact triangulable et $F : X \to X$ une application continue sans point fixe, alors

$$\sum (-1)^i \mathrm{Tr} F_{*|H_i(X)} = 0.$$

Supposons que l'on dispose de « foncteurs »

$$X \mapsto H_i(X), \quad i = 0, \ldots, 2d \quad (d = \dim X)$$

définis sur les variété algébriques sur $\mathbf{F}_q$, à valeur dans les espaces vectoriels de dimension finie sur un corps de caractéristique nulle, qui soit contravariant en les immersions ouvertes et covariant en les morphismes propres (avec compatibilité).

Supposons que l'on ait en plus

1. $\sum_{i=0}^{2d}(-1)^i \mathrm{Tr} F_{*|H_i(X)} = 0$ si $X(\mathrm{F}_q) = \emptyset$ (Lefschetz),
2. $\dim H_0(\mathrm{Spec}(F_q)) = 1$ (normalisation),
3. et une suite exacte longue (fonctorielle) chaque fois que Y est un fermé de X de complémentaire U :

$$\cdots \to H_i(Y) \to H_i(X) \to H_i(U) \to H_{i-1}(Y) \to \cdots \quad \text{(Gysin)}.$$

On aura alors automatiquement pour toute variété algébrique X sur $\mathbf{F}_q$:

$$\sum_{i=0}^{2d}(-1)^i \mathrm{Tr} F_{*|H_i(X)} = N(X) \quad (\mathit{Lefschetz - Hopf}).$$

En pratique, on prendra pour $H_i(X)$ le dual de $H_c^i(\overline{\mathbf{F}}_q \otimes X, \mathbf{Q}_l)$ pour $l \neq p$ ou le dual de $H^i_{\mathrm{rig},c}(X)$ (petit camarade cristallin).

Pour passer aux points à valeur dans des extensions de $\mathbf{F}_q$, on a besoin de

1. $\sum (-1)^i \mathrm{Tr} F^r_{*|H_i(X)} = 0$ si $X(\mathrm{F}_{q^r}) = \emptyset$,
2. $\dim H_0(\mathrm{Spec}(F_{q^r})) = r$

(compatibilité à l'extension des scalaires).

En utilisant $\det(1 - tF_*) = \exp\left(-\sum_{r=1}^{\infty} \mathrm{Tr} F_*^r \frac{t^r}{r}\right)$, on aura alors

$$Z(X,t) = \prod_{i=0}^{2d} \det(1 - tF_{*|H_i(X)})^{(-1)^{i+1}}.$$

D'où la rationalité (et une formule pour les P_i). Et l'équation fonctionnelle résultera de la *dualité de Poincaré* : pour X propre et lisse, on demande des accouplements parfaits

$$H_{2d-i}(X) \times H_i(X) \to K$$

compatibles aux Frobenius à multiplication prés par q^{2d} sur K. Il restera uniquement la pureté à démontrer.

Pour résumer :

Supposons qu'on dispose d'une théorie homologique qui

1. prend ses valeurs dans la catégorie des espaces vectoriels de dimension finie sur un corps de caractéristique nulle
2. est contravariante en les immersions ouvertes et covariante en les morphismes propres (avec compatibilité)
3. commute aux extensions finies du corps de base
4. est compatible avec l'homologie singulière dans le cas propre et lisse
5. fournit des suites exactes longues de Gysin
6. fournit une dualité de Poincaré dans le cas propre et lisse
7. fournit une formule du point fixe de Lefschetz

On aura alors la rationalité et l'équation fonctionnelle pour la fonction zêta. Et la pureté est équivalente au fait que les valeurs propres du Frobenius sont des nombres de Weil (du bon poids si X est propre et lisse).

Intersection de cycles

On peut montrer la formule de Lefschetz-Hopf directement. La stratégie standard passe par les classes de cycles. Il faut construire une application fonctorielle

$$A_i(X) \to H_{2i}(X), \quad \Gamma \to \mathrm{cl}(\Gamma)$$

ou $A_i(X)$ désigne l'homologie (gradué par la dimension) de Chow (cycles modulo équivalence rationnelle). Lorsque X n'est pas lisse, on a aussi besoin d'une version cohomologique (graduée par la codimension)

$$A^i(X) \to H^{2i}(X), \quad \Gamma \to \mathrm{cl}(\Gamma).$$

On dispose d'une théorie de l'intersection

$$\cap : A_i(X) \otimes A^j(X) \to A_{i-j}(X),$$

et on aura besoin d'un cap-produit compatible

$$\cap : H_i(X) \otimes H^j(X) \to H_{i-j}(X).$$

Poincaré et Künneth

La cohomologie doit être fonctorielle et à valeurs dans les espaces de dimension finie. Pour X lisse, on veut un isomorphisme (fonctoriel)

$$\mathrm{cl}(X) \cap - : H^j(X) \simeq H_{2d-j}(X).$$

Pour X propre, on veut un accouplement parfait (fonctoriel)

$$< \, , \, > : H_i(X) \otimes H^i(X) \to K$$

Dans le cas propre et lisse, ça redonne la dualité de Poincaré.

On aura aussi besoin d'une *formule de Künneth* naturelle

$$H_k(X \times Y) \simeq \bigoplus_{i=0}^{k} H_i(X) \otimes H_{k-i}(Y)$$

si X et Y sont des variétés quelconques.

Supposons que X est lisse de pure dimension d. Soit Γ une *correspondance propre* sur X (Γ est une sous-variété de pure dimension d de $X \times X$ et la seconde projection est propre – penser au graphe d'un morphisme propre). On peut alors considérer

$$\Gamma_{*,i} : \; H_i(X) \xrightarrow{p_1^*} H_i(\Gamma) \xrightarrow{p_{2*}} H_i(X) \; .$$

(c'est $\varphi_{*|H_i(X)}$ lorsque Γ est le graphe de φ). Comme X est lisse, on peut interpréter $\Gamma_{*,i}$ comme un morphisme

$$\Gamma_{*,i} : H^{2d-i}(X) \to H_i(X).$$

Si de plus, X est propre, on peut même le voir comme un élément

$$\Gamma_{*,i} : H_i(X) \otimes H_{2d-i}(X).$$

Par fonctorialité, ça correspond en fait la i-ème composante de

$$\mathrm{cl}(\Gamma) \in H_{2d}(X \times X) \simeq \bigoplus_{i=0}^{k} H_i(X) \otimes H_{2d-i}(X).$$

Théorème

Si X est propre est lisse, on a

$$\mathrm{cl}(\Gamma \cap \Delta) = \mathrm{cl}(\Gamma) \cap \mathrm{cl}(\Delta) = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}\ \Gamma_{i,*}$$

(La première partie résulte de la théorie des classes de cycles et la seconde est purement formelle).

Comme corollaire, on obtient directement le théorème de Lefschetz-Hopf pour X propre et lisse. Pour traiter le cas d'une variété quelconque, il y a plusieurs solutions :

- Introduire les coefficients constructibles et passer par les fibrations en courbes
- Utiliser les altération de de Jong (et la cohomologie logarithmique)
- Passer par la théorie des motifs
- ...

Méthode rigide

Lefschetz-Hopf résulte formellement de Lefschetz dans le cas affine et lisse de pure dimension d. Les espaces rigides $H^i_c(X)$ sont alors les espaces de cohomologie d'un complexe de de Rham démarrant en degré d

$$A_c \to A_c \otimes_A \Omega^1_A \to \cdots$$

Ici, A est un relèvement lisse de l'algèbre des fonctions de X et on a

$$A_c = H^d_{\mathrm{Spf}\hat{A}_K}\left(\mathrm{Spec} A_K^{\mathrm{an}}, \mathcal{O}\right).$$

Ce complexe est naturellement muni d'un Frobenius. Il suffit donc de montrer que (ce Frobenius est complètement continu et que) l'on a

$$\mathrm{Tr} F^*_{|A_c \otimes_A \Omega^i_A} = 0 \quad \text{lorsque} \quad X(\mathbf{F}_q) = 0.$$

L'hypothèse implique que l'on peut écrire $1 = \sum_{k=1}^m (F^*(f_k) - f_k) g_k$. D'autre part, on a toujours $\mathrm{Tr}(F^*(f) g F^*) = \mathrm{Tr}(f g F^*)$ (c'est formel), et alors $\mathrm{Tr}(F^*) = \sum_{k=1}^m \mathrm{Tr}(F^*(f_k) - f_k) g_k F^* = 0$.

Pierre Deligne.
La conjecture de Weil. I.
Inst. Hautes Études Sci. Publ. Math., (43) :273–307, 1974.

Bernard Dwork.
On the rationality of the zeta function of an algebraic variety.
Amer. J. Math., 82 :631–648, 1960.

Alexander Grothendieck.
Formule de Lefschetz et rationalité des fonctions L.
In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 279, 41–55.
Soc. Math. France, Paris, 1995.

André Weil.
Numbers of solutions of equations in finite fields.
Bull. Amer. Math. Soc., 55 :497–508, 1949.