

VERS UNE COMPRÉHENSION DES CONJECTURES DE WEIL

F. JOUVE

Les conjectures de Weil décrivent de manière très précise le nombre de solutions de systèmes d'équations polynômiales à coefficients dans un corps fini donné. Les connaissances antérieures à l'énoncé de ces conjectures ont constitué autant d'indices qui ont amené André Weil à leur formulation en 1949. Cependant, le fait que les objets manipulés sont de caractéristique p a constitué une difficulté centrale et nécessité la mise au point d'objets, et même d'une théorie entièrement nouvelles.

Ces notes sont, pour l'essentiel, un résumé (en français...) de la première partie de [K]. Pour les questions générales de géométrie algébrique (en particulier en ce qui concerne les schémas), on renvoie à [L]. On trouvera dans [M] de nombreux points de cohomologie étale traités en détails.

1. ÉNONCÉ DES CONJECTURES

Soit X_0 une variété algébrique sur $\mathbb{F}_q$: pour l'exposé, on pourra se contenter de la vision intuitive de la variété X_0 comme étant l'ensemble des solutions d'un système d'équations polynômiales à coefficients dans $\mathbb{F}_q$. Dans le cadre rigoureux "naturel" de l'énoncé des conjectures de Weil, X_0 est en fait défini comme étant un schéma sur $\text{Spec}\mathbb{F}_q$. Lorsqu'on considérera X_0 comme une variété sur $\mathbb{F}_{q^n}$ (resp. $\overline{\mathbb{F}_q}$), on notera

$$X_n = X_0 \times \mathbb{F}_{q^n} \text{ (resp. } X = X_0 \times \overline{\mathbb{F}_q} \text{),}$$

où la notation peut être vue comme symbolique tout aussi bien que désignant le produit fibré de X_0 avec $\text{Spec}\mathbb{F}_{q^n}$ (resp. $\text{Spec}\overline{\mathbb{F}_q}$) au dessus de $\text{Spec}\mathbb{F}_q$.

L'objet essentiel d'étude apparaissant dans les conjectures de Weil est la *fonction zeta* de $X_0/\mathbb{F}_q$, c'est une série formelle à coefficients rationnels définie comme suit :

$$Z(X_0/\mathbb{F}_q; T) = \exp\left(\sum_{n \geq 1} |X_0(\mathbb{F}_{q^n})| \frac{T^n}{n}\right),$$

où $|X_0(\mathbb{F}_{q^n})|$ est le nombre de points $\mathbb{F}_{q^n}$ -rationnels de $X_0/\mathbb{F}_q$ (i.e. le nombre de morphismes de $\mathbb{F}_q$ -schémas : $\text{Spec}\mathbb{F}_{q^n} \rightarrow X_0$) correspondant intuitivement au nombre de points à coordonnées dans $\mathbb{F}_{q^n}$ de X_0 . Comme on peut s'y attendre, étant donnée l'appellation "fonction zeta", $Z(X_0/\mathbb{F}_q; T)$ admet un développement en produit eulérien :

Lemme 1. Soit $\overline{X_0}$ l'ensemble des points fermés de X_0 (i.e. l'ensemble des orbites pour l'action de $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ sur l'ensemble des points $\overline{\mathbb{F}_q}$ -rationnels de X_0) et $\deg x$ la cardinalité du corps résiduel associé au point fermé x (i.e. la cardinalité de l'orbite x), alors

$$Z(X_0/\mathbb{F}_q; T) = \prod_{x \in \overline{X_0}} (1 - T^{\deg x})^{-1}.$$

Démonstration. Il s'agit de réinterpréter $X_0(\mathbb{F}_{q^n})$ en termes des points fermés de X_0 :

$$\begin{aligned} |X_0(\mathbb{F}_{q^n})| &= \sum_{d|n} \left(|\{\text{Orbites de points de corps minimal de déf } \mathbb{F}_{q^d}\}| \right. \\ &\quad \times \left. (\text{le cardinal d'une telle orbite}) \right). \end{aligned}$$

Dans la somme précédente, le premier facteur du sommant correspondant à d est, vues les notations introduites dans le lemme, égal à $\sum_{x \in \overline{X_0}, \deg x = d} 1$.

Par ailleurs, l'orbite d'un point $\overline{\mathbb{F}_q}$ -rationnel de X_0 est en bijection avec le quotient de $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ par son stabilisateur : $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^d})$. Ce quotient n'est autre que le groupe cyclique d'ordre d : $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. Finalement :

$$|X_0(\mathbb{F}_{q^n})| = \sum_{d|n} d \sum_{(x \in \overline{X_0}, \deg x = d)} 1.$$

On compare alors les dérivées logarithmiques des séries considérées : d'une part

$$\begin{aligned} T \frac{Z'(X_0/\mathbb{F}_q; T)}{Z(X_0/\mathbb{F}_q; T)} &= \sum_{n \geq 1} |X_0(\mathbb{F}_{q^n})| T^n \\ &= \sum_{n \geq 1} \left(\sum_{d|n} d \sum_{(x \in \overline{X_0}, \deg x = d)} 1 \right) T^n, \end{aligned}$$

d'autre part

$$\begin{aligned} T \frac{d}{dT} \left(\log \prod_{x \in \overline{X_0}} (1 - T^{\deg x})^{-1} \right) &= \sum_{x \in \overline{X_0}} \frac{T^{\deg x}}{1 - T^{\deg x}} \\ &= \sum_{x \in \overline{X_0}} \sum_{k \geq 1} T^{k \deg x} \\ &= \sum_{n \geq 1} \left(\sum_{d|n} d \sum_{(x \in \overline{X_0}, \deg x = d)} 1 \right) T^n. \end{aligned}$$

Les deux séries considérées ont même dérivée logarithmique et un coefficient constant égal à 1, ce qui prouve que ces deux séries sont égales dans $\mathbb{Q}[[T]]$. $\square$

Le calcul de la fonction zeta d'une variété sur $\mathbb{F}_q$ est, en général un problème difficile (donner des informations précises dans un cadre général sur cette fonction zeta est d'ailleurs l'objectif principal des conjectures de Weil). Cependant des calculs peuvent être fait de manière élémentaire dans certains cas simples.

EX : Dans le cas où X_0 est l'espace projectif $\mathbb{P}_{\mathbb{F}_q}^d$ de dimension d sur $\mathbb{F}_q$, on peut donner une formule explicite pour $|X_0(\mathbb{F}_{q^n})|$. En effet, on montre facilement par récurrence que

$$|X_0(\mathbb{F}_{q^n})| = \sum_{k=0}^d q^{nk}.$$

On en déduit

$$\begin{aligned} Z(\mathbb{P}_{\mathbb{F}_q}^d/\mathbb{F}_q; T) &= \exp \left(\sum_{n \geq 1} \sum_{k=0}^d q^{nk} \frac{T^n}{n} \right) \\ &= \exp \left(\sum_{k=0}^d -\log(1 - q^k T) \right) \\ &= \frac{1}{(1-T)(1-qT) \dots (1-q^dT)}. \end{aligned}$$

On remarque que, dans cet exemple, la fonction zeta calculée est rationnelle, à coefficients dans $\mathbb{Z}$ et que le nombre de facteurs à coefficients entiers du dénominateur ne dépend que de la dimension de la variété.

L'exemple précédent, ainsi que d'autres cas où des calculs explicites ont pu être fait, ont conduit André Weil à formuler les conjectures suivantes en 1949.

Si $X_0/\mathbb{F}_q$ est lisse et projective de dimension d , alors

- (1) $Z(X_0/\mathbb{F}_q; T)$ est une fonction rationnelle de T .
- (2) Il existe des entiers χ et $\epsilon = \pm 1$ tels que

$$Z(X_0/\mathbb{F}_q; \frac{1}{q^d T}) = \epsilon q^{d\chi/2} T^\chi Z(X_0/\mathbb{F}_q; T).$$

- (3) La fonction zeta de $X_0/\mathbb{F}_q$ se met sous la forme

$$Z(X_0/\mathbb{F}_q; T) = \frac{P_1 \dots P_{2d-1}}{P_0 \dots P_{2d}},$$

où $P_0 = 1 - T$, $P_{2d} = 1 - q^d T$ et chaque P_i est un polynôme à coefficients entiers dont les zéros sont de module $q^{-i/2}$.

La dernière de ces trois conjectures est connue sous le nom d'*hypothèse de Riemann sur les corps finis*; c'est évidemment l'analogue de l'hypothèse de Riemann pour la fonction ζ de $\mathbb{Q}$. Il est à noter que cette conjecture donne une information plus précise que la simple estimation de $|X_0(\mathbb{F}_{q^n})|$. On a en effet

$$|X_0(\mathbb{F}_{q^n})| = \sum_{0 \leq i \leq 2d} (-1)^i \sum_j \alpha_{i,j}^n,$$

où $P_i = \prod_j (1 - \alpha_{i,j} T)$. Estimer les $\alpha_{i,j}$ donne donc une information "strictement plus forte" que la connaissance de $|X_0(\mathbb{F}_{q^n})|$ sauf dans le cas où tous les $\alpha_{i,j}$ sauf 1 sont connus.

L'ingrédient essentiel ayant conduit à la résolution de ces conjectures est la construction d'une théorie cohomologique des variétés sur les corps finis "adaptée" aux conjectures de Weil : la *cohomologie étale*. Nous allons introduire cette théorie via la cohomologie de Čech.

2. COHOMOLOGIE DE ČECH

L'idée de la cohomologie de Čech est de savoir comment, pour un problème dont on connaît des solutions locales, obtenir des informations "globales". Si l'on se donne une équation différentielle sur $\mathbb{R}^n$, par exemple, on sait qu'on a, sous des hypothèses faibles, existence de solutions locales. Déterminer l'existence de solutions globales est, en revanche, plus délicat : l'idée naturelle est de comparer les solutions locales sur les intersections des ouverts sur lesquels elles sont définies.

Soit alors T un espace topologique (disons une variété différentiable sur $\mathbb{C}$, pour fixer les idées) et $\mathcal{U} = (U_i)_{i \in J}$ un recouvrement ouvert de T . Pour $I = (i_0, \dots, i_n) \in J^{n+1}$, on pose :

$$U_I = U_{i_0} \cap \dots \cap U_{i_n}.$$

Soit C_I l'espace vectoriel des fonctions définies sur les composantes connexes de U_I , ou de manière équivalente, l'espace vectoriel des fonctions continues localement constantes sur U_I . Enfin, pour $n \geq 1$, on pose

$$C^n(\mathcal{U}, \mathbb{C}) = \prod_{I \in J^{n+1}} C_I;$$

ce sont les *n-cochaines*. Pour $f \in C^n(\mathcal{U}, \mathbb{C})$, on notera $f(I)$ sa I -ième composante.

On remarque tout d'abord que, si chaque U_i est connexe ($i \in J$), un élément $f \in C^0(\mathcal{U}, \mathbb{C})$ associe, via $f(i)$, un nombre complexe unique c_i à chaque U_i . C'est donc naturellement à $U_i \cap U_j$ que l'on va associer le nombre complexe $c_i - c_j$. Suivant cette idée, on définit une application linéaire

$$d^0 : C^0(\mathcal{U}, \mathbb{C}) \rightarrow C^1(\mathcal{U}, \mathbb{C}),$$

par $d^0(f)(i, j) = f(i) - f(j)$, où la différence de ces deux fonctions est définie sur $U_{(i, j)} = U_i \cap U_j$. Dans le cas où chaque U_i est connexe et où T est connexe, on en déduit donc $d^0(f) = 0$ si et seulement si f est constante. Un seul nombre complexe "global" est alors associé à T par f . C'est bien le type de conclusion à laquelle on voulait arriver.

Pour $n \geq 1$ on définit $d^n : C^n(\mathcal{U}, \mathbb{C}) \rightarrow C^{n+1}(\mathcal{U}, \mathbb{C})$ par

$$d^n(f)(i_0, \dots, i_{n+1}) = \sum_{0 \leq j \leq n+1} (-1)^j f(i_0, \dots, i_{j-1}, i_{j+1}, \dots, i_{n+1}).$$

Ces applications d^n satisfont à l'équation fondatrice de toute théorie cohomologique : $d^{n+1} \circ d^n = 0$. On le vérifie au rang 0 :

$$\begin{aligned} d^1 \circ d^0(f)(i, j, k) &= d^0(f)(j, k) - d^0(f)(i, k) + d^0(f)(i, j) \\ &= (f(j) - f(k)) - (f(i) - f(k)) + (f(i) - f(j)) \\ &= 0. \end{aligned}$$

Si l'on définit les n -cocycles $Z^n(\mathcal{U}, \mathbb{C}) = \text{Ker } d^n$ et les n -cobords $B^n(\mathcal{U}, \mathbb{C}) = \text{Im } d^{n-1}$, on peut alors, pour $n \geq 1$, définir le n -ième groupe de cohomologie de Čech relatif à $\mathcal{U}$:

$$H^n(\mathcal{U}, \mathbb{C}) = Z^n(\mathcal{U}, \mathbb{C}) / B^n(\mathcal{U}, \mathbb{C}).$$

Avec la convention $C^{-1} = 0$ et $d^{-1} = 0$, cette définition s'étend à tous les indices $n \geq 0$.

Les espaces vectoriels $H^n(\mathcal{U}, \mathbb{C})$ dépendent a priori du choix d'un recouvrement $\mathcal{U}$. On peut cependant remarquer que si $\mathcal{U}$ et $\mathcal{V}$ sont 2 recouvrements ouverts de T , il en existe un raffinant tous les deux (il suffit de prendre les intersections de chaque U_i avec chaque V_j). On obtient un recouvrement $\mathcal{W}$ et des applications :

$$\begin{aligned} H^n(\mathcal{U}, \mathbb{C}) &\rightarrow H^n(\mathcal{W}, \mathbb{C}) \\ H^n(\mathcal{V}, \mathbb{C}) &\rightarrow H^n(\mathcal{W}, \mathbb{C}) \end{aligned}$$

permettant de parler de "réunion" de tous les recouvrements de T (la notion se cachant derrière cette intuition étant celle de limite inductive) puis des groupes de cohomologie de Čech intrinsèques à T (i.e. ne dépendant pas du choix d'un recouvrement). Ces groupes seront notés $H^n(T, \mathbb{C})$.

EX : Supposons T localement connexe et soit $\mathcal{U} = (U_i)_{i \in \pi_0(T)}$ le recouvrement de T par ses composantes connexes. On a bien sûr $U_{(i, j)} = U_i \cap U_j = \emptyset$ dès que $i \neq j$ d'où $d_0 = 0$ et $Z^0(\mathcal{U}, \mathbb{C}) = C^0(\mathcal{U}, \mathbb{C})$. Comme $d^{-1} = 0$, on a même $C^0(\mathcal{U}, \mathbb{C}) = H^0(\mathcal{U}, \mathbb{C})$. Or, se donner un élément $f \in C^0(\mathcal{U}, \mathbb{C})$ c'est se donner pour chaque $i \in \pi_0(T)$ une application $f(i)$ sur l'ensemble des composantes connexes de U_i (i.e. U_i !). Ainsi, pour chaque i , $f(i)$ associe un unique nombre complexe à U_i . En admettant le fait que, dans le cas présent, ce choix de recouvrement suffit (ce n'est pas vrai en général !), on en déduit :

$$H^0(T, \mathbb{C}) = \mathbb{C}^{\pi_0(T)}.$$

A travers cet exemple, on voit que les groupes de cohomologie de Čech sont porteur d'informations topologiques sur l'espace T ($\dim_{\mathbb{C}} H^0(T, \mathbb{C}) = \pi_0(T)$).

Revenant sur ce que l'on vient d'exposer, on voit que le choix de $\mathbb{C}$ comme espace vectoriel "des coefficients" n'a rien de crucial et qu'il pourrait très bien être remplacé par un espace vectoriel plus général. Par exemple, dans le cas où l'on cherche à résoudre une équation différentielle, il paraît naturel de choisir pour C_I l'espace vectoriel des solutions définies sur U_I . Calculer $d^0(f)$ donne alors une information sur le recollement des solutions sur $U_i \cap U_j$.

On va voir que l'on peut définir des espaces de coefficients très généraux via la théorie des faisceaux.

3. FAISCEAUX

Un *faisceau* (d'espaces vectoriels) $\mathcal{F}$ sur un espace topologique T est une règle associant un espace vectoriel $\mathcal{F}(U)$ à tout ouvert $U \subset T$ telle que les axiomes suivants soient vérifiés :

$$(1) \mathcal{F}(\emptyset) = 0.$$

(2) Si $V \subset U$ sont 2 ouverts, on a un morphisme (restriction) :

$$\rho_{U,V} : \mathcal{F}(U) \rightarrow \mathcal{F}(V).$$

(3) Si on a les inclusions d'ouverts : $W \subset V \subset U$ alors $\rho_{U,W} = \rho_{V,W} \circ \rho_{U,V}$.

(4) (*unicité*) Si U est un ouvert de T et $(U_i)_i$ un recouvrement ouvert de U , alors, si $s \in \mathcal{F}(U)$ vérifie $\rho_{U,U_i}(s) = 0$ pour tout i , on a $s = 0$.

(5) (*recollement*) Avec les mêmes notations, s'il est donné, pour chaque i , un élément $s_i \in \mathcal{F}(U_i)$ tel que $\rho_{U_i, U_i \cap U_j}(s_i) = \rho_{U_j, U_i \cap U_j}(s_j)$ (pour tout couple (i, j)) alors il existe une section $s \in \mathcal{F}(U)$ telle que, pour tout i , $s_i = \rho_{U, U_i}(s)$.

EX : -Les fonctions continues sur un ouvert d'un espace topologique forment un faisceau d'espaces vectoriels.

- Si f est un polynôme de $k[X_1, \dots, X_n]$ (où k est un corps) qui engendre un idéal premier alors, pour l'hypersurface X définie par $f = 0$, l'anneau $k[X] = k[X_1, \dots, X_n]/(f)$ est appelé anneau des fonctions régulières sur X . Le faisceau (d'anneaux) qui à chaque ouvert (de Zariski) de X associe les restrictions à U des fonctions régulières sur X est appelé *faisceau de structure* de X .

Soit alors $\mathcal{F}$ un faisceau (d'espaces vectoriels) sur T , on peut reprendre les définitions de la section précédente pour définir les groupes de cohomologie de Čech à coefficients dans $\mathcal{F}$: pour un recouvrement ouvert $\mathcal{U} = (U_i)_{i \in I}$, on pose $C_I = \mathcal{F}(U_I)$ avec $I \in J^{n+1}$.

On peut alors définir, en suivant la construction précédente, les espaces $Z^n(T, \mathcal{F})$, $B^n(T, \mathcal{F})$ et $H^n(T, \mathcal{F})$. Puisque $d^{-1} = 0$, on a toujours $H^0(T, \mathcal{F}) = Z^0(T, \mathcal{F})$, par ailleurs, se donner $f \in Z^0(T, \mathcal{F})$, c'est se donner, pour chaque i , un élément $s_i = f(i) \in \mathcal{F}(U_i)$ tel que $f(i) = f(j)$ sur $U_i \cap U_j$ (i.e. $\rho_{U_i, U_i \cap U_j}(s_i) = \rho_{U_j, U_i \cap U_j}(s_j)$).

D'après l'axiome de recollement on en conclut que la donnée de $f \in Z^0(T, \mathcal{F})$ équivaut à la donnée d'un élément $s \in \mathcal{F}(T)$. Ainsi

$$H^0(T, \mathcal{F}) = Z^0(T, \mathcal{F}) = \mathcal{F}(T).$$

C'est essentiellement la connaissance de la cohomologie des variétés complexes qui incita Weil à formuler ses conjectures.

4. MOTIVATION DES CONJECTURES DE WEIL

De nombreux résultats sur la cohomologie des variétés complexes dont on peut considérer une réduction modulo p premier, étaient connus antérieurement à l'énoncé des conjectures de Weil :

EX : Pour l'espace projectif de dimension n sur $\mathbb{C}$,

- $H^k(\mathbb{P}_{\mathbb{C}}^n, \mathbb{C}) = 0$ si $k > 2n$,
- $H^{2k}(\mathbb{P}_{\mathbb{C}}^n, \mathbb{C}) = \mathbb{C}$ si $0 \leq k \leq n$,
- $H^{2k+1}(\mathbb{P}_{\mathbb{C}}^n, \mathbb{C}) = 0$ si $0 \leq k < n$.

Par ailleurs, on a vu que

$$Z(\mathbb{P}_{\mathbb{F}_q}^n/\mathbb{F}_q; T) = \frac{1}{(1-T)(1-qT)\dots(1-q^nT)}.$$

Le cas des courbes lisses et projectives sur $\mathbb{F}_q$ (résolu par Weil) constitue un autre indice fort qu'il doit exister une interprétation cohomologique de la fonction zeta. On a en effet

$$Z(C_0/\mathbb{F}_q; T) = \frac{P_{2g}(T)}{(1-T)(1-qT)},$$

où $C_0/\mathbb{F}_q$ est une courbe lisse et projective de genre g et $P_{2g} \in \mathbb{Z}[T]$ est de degré $2g$. Par ailleurs pour toute surface de Riemann C de genre g :

$$H^0(C, \mathbb{C}) = \mathbb{C}, \quad H^1(C, \mathbb{C}) = \mathbb{C}^{2g}, \quad H^2(C, \mathbb{C}) = \mathbb{C},$$

et les autres groupes de cohomologie sont nuls.

On cite enfin quelques uns des résultats fondamentaux concernant la cohomologie des variétés complexes :

- (1) (*Dimension*) $H^i(X, \mathbb{C}) = 0$ pour $i > 2d$ où $d = \dim X$.
- (2) (*Finitude*) Pour $i \geq 0$, $H^i(X, \mathbb{C})$ est un $\mathbb{C}$ -espace vectoriel de dimension finie.
- (3) (*Fonctorialité*) $f: X \rightarrow Y$ donne lieu à $f^*: H^i(Y, \mathbb{C}) \rightarrow H^i(X, \mathbb{C})$.
- (4) (*Dualité de Poincaré*) $H^{2d-i}(X, \mathbb{C}) \simeq H^i(X, \mathbb{C})$ pour $0 \leq i \leq d$.
- (5) (*Formule des traces de Lefschetz*) Si $f: X \rightarrow X$ est différentiable à points fixes isolés et si $L(f)$ désigne le nombre de ces points fixes comptés avec multiplicité (algébrique), alors :

$$L(f) = \sum_{i=0}^{2d} (-1)^i \text{Tr}(f^* | H^i(X, \mathbb{C})).$$

Cette dernière formule semble pouvoir être reliée au comptage de points sur une variété $X_0/\mathbb{F}_q$ de dimension d dans l'hypothèse où elle peut être appliquée au morphisme de Frobenius. En effet, on aurait alors $|X_0(\mathbb{F}_{q^n})| = L(f^n)$, pour $n \geq 1$. On exploite alors le lemme élémentaire suivant (dont on fera la preuve à la fin de cette section) :

Lemme 2. *Soit f un endomorphisme d'un espace vectoriel V de dimension finie, on a l'égalité de séries formelles :*

$$-\log(\det(1 - fT)) = \sum_{k \geq 1} \text{Tr}(f^k) \frac{T^k}{k}.$$

Combinant le lemme 2 et la formule de Lefschetz pour le morphisme de Frobenius Fr^* , on obtient :

$$\begin{aligned} \sum_{n \geq 1} |X_0(\mathbb{F}_{q^n})| \frac{T^n}{n} &= \sum_{i=0}^{2d} (-1)^i \sum_{n \geq 1} \text{Tr}((\text{Fr}^*)^n | H^i(X_0)) \frac{T^n}{n} \\ &= \sum_{i=0}^{2d} (-1)^{i+1} \log(\det(1 - \text{Fr}^* T | H^i(X_0))) \\ &= \log \prod_{i=0}^{2d} \det(1 - \text{Fr}^* T | H^i(X_0))^{(-1)^{i+1}}, \end{aligned}$$

d'où l'on conclut

$$Z(X_0/\mathbb{F}_q; T) = \prod_{i=0}^{2d} \det(1 - \text{Fr}^* T | H^i(X_0))^{(-1)^{i+1}}.$$

Bien qu'on ait l'illusion que cette dernière formule prouve la rationalité de la fonction zeta de $X_0/\mathbb{F}_q$, l'essentiel du calcul nécessite une justification cruciale. Le faisceau des coefficients dans les calculs sur les groupes de cohomologie a été sciemment omis ci-dessus. Bien entendu, $X_0/\mathbb{F}_q$ n'est pas une variété complexe sur laquelle le Frobenius serait une fonction différentiable vérifiant les conditions nécessaires à l'application de la formule des traces de Lefschetz. Trouver le cadre cohomologique dans lequel les calculs ci-dessus puissent être justifiés constitue l'essentiel de la difficulté. La section suivante présente une introduction à cette théorie : la *cohomologie étale*.

Preuve du lemme 2.

Notons r la dimension de V et $\alpha_1, \dots, \alpha_r$ les valeurs propres de f . On a alors

$$\begin{aligned} -\log(1 - fT) &= -\sum_{i=1}^r \log(1 - \alpha_i T) \\ &= \sum_{i=1}^r \sum_{k \geq 1} \frac{\alpha_i^k T^k}{k} \\ &= \sum_{k \geq 1} \left(\sum_{i=1}^r \alpha_i^k \right) \frac{T^k}{k} \\ &= \sum_{k \geq 1} \text{Tr}(f^k) \frac{T^k}{k}. \end{aligned}$$

5. COHOMOLOGIE ÉTALE

5.1. Topologie étale. On peut dans un premier temps penser à utiliser la topologie de Zariski pour définir la cohomologie souhaitée. Mais celle-ci est mal adaptée au cadre que l'on s'est fixé (entre autres tares, tous les groupes de cohomologie correspondants sont nuls).

Il est également vain de vouloir utiliser le faisceau de structure de la variété X_0 , puisqu'on ne produira ainsi que des "objets de caractéristique p " qui ne seront d'aucune aide pour le comptage de points en terme de trace d'un morphisme.

L'idée est le prolongement de celle à la base de la cohomologie de Čech : ayant suffisamment d'informations de structure sur les variétés complexes, on suppose que l'on peut résoudre les problèmes attachés à ces variétés en les restreignant aux ouverts d'un certain recouvrement puis en comparant les solutions, via les groupes de cohomologie de Čech, sur l'intersection de ces ouverts, pour finalement en déduire des informations globales.

On cherche un processus analogue pour une variété algébrique X/k (k est un corps) rendant la variété X "arithmétiquement" plus simple et pouvant être vue comme une localisation de X .

Grothendieck montra que regarder X comme variété sur les extensions séparables k'/k répond à cette question. Ce processus permet d'obtenir des points sur X et de nombreux problèmes sont plus simples à résoudre (sur la clôture séparable k^{sep}/k , les formes quadratiques sont classifiées par le rang, les polynômes sont scindés...).

La notion d'ouvert d'un espace topologique doit donc être changée en quelque chose de plus général, tout en gardant à l'esprit la structure nécessaire à la construction de la cohomologie de Čech correspondant. Les objets généralisant de la manière souhaitée la notion usuelle de topologie forment une *topologie de Grothendieck*.

C'est tout d'abord la notion de *morphisme étale* qui doit être définie (on n'en donne pas ici la définition rigoureuse, mais simplement la propriété essentielle qui nous servira) :

si X et Y sont 2 variétés définies sur k , un morphisme étale $f : X \rightarrow Y$ est un morphisme d'image ouverte U telle que X soit un revêtement non ramifié fini de U .

Ex : Si X/k est une variété et k'/k une extension séparable de corps, alors l'extension des scalaires

$$X \times k' \rightarrow X,$$

est un morphisme étale (on rajoute des points rationnels à coefficients dans le corps de base à la variété X).

Un autre type de morphisme étale est obtenu en considérant les équations polynômiales à coefficients dans l'anneau des fonction régulière sur un ouvert U d'une variété X :

$$Y = \{(x, y) \in U \times k \mid y^d + a_1(x)y^{d-1} + \dots + a_d(x) = 0\},$$

avec $Y \rightarrow X$ la projection. Si les a_i sont des fonctions régulières sur U et l'équation définissant Y est séparable, alors Y est un revêtement étale de U . Les fibres d'un tel revêtement sont finies d'où $\dim X = \dim Y$.

Les morphismes étales sont les analogues des ouverts pour une topologie de Grothendieck. On définit alors les opérations suivantes sur ces "ouverts" :

- *Intersection* : si $f_1 : X_1 \rightarrow X$ et $f_2 : X_2 \rightarrow X$ sont étales, on considère

$$Z = \{(x_1, x_2) \in X_1 \times X_2 \mid f_1(x_1) = f_2(x_2)\} \quad (\text{produit fibré}),$$

alors "l'intersection" des morphismes étales f_1 et f_2 est $f : Z \rightarrow X$ définie par $f(x_1, x_2) = f_1(x_1) = f_2(x_2)$.

- *Restriction* : si $Z \rightarrow Y$ et $Y \rightarrow X$ sont étales alors la composée

$$Z \rightarrow Y \rightarrow X,$$

est étale. Ce morphisme est appelé restriction à Z de $Y \rightarrow X$.

- *Recouvrement* : Un recouvrement étale de X est une famille de morphismes étales $(f_i : X_i \rightarrow X)_i$ telle que $X = \cup_i f_i(X_i)$.

5.2. Faisceaux pour la topologie étale. La topologie étale est "suffisamment semblable" à la notion classique de topologie pour que l'on puisse définir un faisceau $\mathcal{F}$ pour la topologie étale de X . On notera par exemple qu'à toute restriction $Z \rightarrow Y \rightarrow X$, le faisceau $\mathcal{F}$ associe

$$\rho_{YZ} : \mathcal{F}(Y) \rightarrow \mathcal{F}(Z);$$

les autres propriétés se transposant de manière analogue.

Si $\mathcal{F}$ est un faisceau sur X pour la topologie étale, on peut construire, pour un recouvrement étale $\mathcal{U}$ de X fixé, les groupes de cohomologie de Čech de X relatifs à $\mathcal{U}$ à coefficients dans $\mathcal{F}$ (voir les sections 2 et 3). On montre comme précédemment que

$$H^0(\mathcal{U}, \mathcal{F}) = \mathcal{F}(X).$$

Par ailleurs, passant une nouvelle fois à la limite inductive sur les recouvrements (étales) de X , on montre que l'on peut définir des groupes de cohomologie indépendant du choix d'un recouvrement et, par conséquent, intrinsèques à la variété X/k . Ces groupes sont notés

$$H_{\text{ét}}^i(X, \mathcal{F}).$$

Exemples de faisceaux étales :

- (1) Soit M un groupe abélien. Le *faisceau constant* sur X est défini pour $Y \rightarrow X$ étale par

$$\underline{M}(Y) = \text{Map}(Y, M),$$

groupe des applications continues $Y \rightarrow M$, où M est muni de la topologie discrète. Ainsi $f \in \underline{M}(Y)$ est constant sur les composantes connexes de Y (en toute logique $\underline{M}$ devrait donc s'appeler faisceau *localement* constant. $\underline{M}$ est en

fait la *faisceautisation* du pré-faisceau constant). Les groupes de cohomologie étale correspondant sont notés $H_{\text{ét}}^i(X, M)$ (on verra que le faisceau constant (de torsion) $\underline{\mathbb{Z}/n\mathbb{Z}}$ joue un rôle essentiel).

- (2) Le “groupe multiplicatif” $\mathbb{G}_m$ associe à tout morphisme étale $Y \rightarrow X$ le groupe $\mathbb{G}_m(Y)$ des inversibles de l’anneau des fonctions régulières sur Y . Le sous groupe de $\mathbb{G}_m(Y)$ consistant en les racines n -ièmes de 1 est noté $\mu_n(Y)$. On note μ_n le faisceau associé.

Sur la restriction $X \times k[\zeta_n] \rightarrow X$, (où il faut supposer n premier à $p = \text{car } k$ pour que ce morphisme soit étale et où ζ_n désigne une racine primitive n -ième de 1 dans $\bar{k}$), μ_n est le faisceau constant $\underline{\mathbb{Z}/n\mathbb{Z}}$.

REMARQUE : Dans le cas où la variété X/k est réduite à un point (X est le spectre d’un corps L extension de k), on a, pour chaque extension finie séparable k'/L , un morphisme étale $Y \rightarrow X$ (alors $Y = \text{Spec } k'$). Une telle application donne un recouvrement de X (consistant en un unique morphisme étale) puisque Y et X sont réduites à un point. Cependant, même dans ce cas, l’étude de l’intersection (étale) de Y avec lui-même présente un intérêt (en particulier, la variété obtenue n’est pas Y en général). Cela provient de l’existence de L -automorphismes non-triviaux pour k' , c’est à dire du groupe de Galois $\text{Gal}(k'/L)$, dans le cas où cette extension est galoisienne.

Par ailleurs, l’étude des faisceaux étales sur une variété réduite à un point est équivalente à celle des $\text{Gal}(k^{\text{sep}}/k)$ -modules M et les groupes de cohomologie correspondants sont isomorphes aux groupes de cohomologie galoisienne $H^i(k, M)$.

5.3. Résultats fondamentaux pour la cohomologie étale. On se place dans le cadre où X/k est une variété lisse et projective, avec $\text{car } k = p$ et $k = \bar{k}$. On montre que seuls les faisceaux de torsion de caractéristique première à p se comportent comme attendu (du point de vue de la comparaison avec la cohomologie classique des variétés complexes par exemple). Considérons alors le faisceau constant $\underline{\mathbb{Z}/\ell^n\mathbb{Z}}$ où $\ell \neq p$ est premier. Les groupes $H_{\text{ét}}^i(X, \underline{\mathbb{Z}/\ell^n\mathbb{Z}})$ possèdent les propriétés qui en font les objets que l’on souhaitait construire : on en dérive tout d’abord des “objets” de caractéristique 0 :

$$H_{\text{ét}}^i(X, \mathbb{Z}_{\ell}) = \varprojlim H_{\text{ét}}^i(X, \underline{\mathbb{Z}/\ell^n\mathbb{Z}}),$$

$$H_{\text{ét}}^i(X, \mathbb{Q}_{\ell}) = H_{\text{ét}}^i(X, \mathbb{Z}_{\ell}) \otimes \mathbb{Q}_{\ell}.$$

Les groupes de cohomologie ainsi construits possèdent les propriétés suivantes (analogues à celles énoncées plus haut pour la cohomologie des variétés complexes) ayant conduit à la résolution des deux premières conjectures de Weil :

- (1) $H_{\text{ét}}^i(X, \mathbb{Q}_{\ell}) = 0$ pour $i \geq 2 \dim X + 1$.
- (2) Pour $i \geq 0$, le $\mathbb{Q}_{\ell}$ -espace vectoriel $H_{\text{ét}}^i(X, \mathbb{Q}_{\ell})$ est de dimension finie.
- (3) Tout morphisme $f : X \rightarrow Y$ donne lieu à un morphisme sur les groupes de cohomologie

$$f^* : H_{\text{ét}}^i(Y, \mathbb{Q}_{\ell}) \rightarrow H_{\text{ét}}^i(X, \mathbb{Q}_{\ell}).$$

- (4) (*Dualité de Poincaré*) Pour $0 \leq i \leq 2 \dim X$, la forme bilinéaire naturelle

$$H_{\text{ét}}^i(X, \mathbb{Q}_{\ell}) \times H_{\text{ét}}^{2 \dim X - i}(X, \mathbb{Q}_{\ell}) \rightarrow H_{\text{ét}}^{2 \dim X}(X, \mathbb{Q}_{\ell}) \simeq \mathbb{Q}_{\ell}$$

est un accouplement parfait. En particulier, les espaces vectoriels $H_{\text{ét}}^i$ et $H_{\text{ét}}^{2 \dim X - i}$ sont duaux.

- (5) (*Formule des traces de Lefschetz*) Si $f : X \rightarrow X$ est un morphisme dont les points fixes sont isolés (avec une condition de séparabilité sur $1 - df$ agissant

sur l'espace tangent en les points fixes) et si $L(f)$ désigne le nombre de tels points fixes, alors

$$L(f) = \sum_{i=0}^{2 \dim X} (-1)^i \operatorname{Tr}(f^* | H_{\text{ét}}^i(X, \mathbb{Q}_\ell)).$$

(6) (*Comparaison*) Si X est lisse et projective sur $\mathbb{C}$, alors

$$H_{\text{ét}}^i(X, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \simeq H^i(X_{\mathbb{C}}, \mathbb{C}).$$

Le calcul fait à la fin de la section 4 trouve donc maintenant sa justification.

Malgré le travail énorme réalisé pour obtenir les théorèmes énoncés ci-dessus, des ingrédients manquaient encore en 1970 pour démontrer l'hypothèse de Riemann sur les corps finis. Utilisant l'intégralité des outils mis au point jusque là et bien plus encore (...), Deligne arriva finalement à bout de cette dernière conjecture en 1973.

RÉFÉRENCES

- [K] Kowalski, E. : *Trying to understand Deligne's proof of the Weil conjectures*, [http ://www.math.u-bordeaux1.fr/%7Ekowalski/deligne.pdf](http://www.math.u-bordeaux1.fr/%7Ekowalski/deligne.pdf).
- [L] Liu, Q. : *Algebraic geometry and arithmetic curves*, Oxford Grad. Texts in Math., 6, Oxford Univ. Press, 2002.
- [M] Milne, J. : *Lectures on étale cohomology*, [http ://www.jmilne.org/math/](http://www.jmilne.org/math/).