**POINTS RATIONNELS ET GROUPES FONDAMENTAUX :
APPLICATIONS DE LA COHOMOLOGIE p -ADIQUE**
[d'après P. Berthelot, T. Ekedahl, H. Esnault, etc.]

par **Antoine CHAMBERT-LOIR**

Dans cet exposé, je présente trois résultats concernant les variétés algébriques en caractéristique positive :

a) *Deux variétés propres et lisses sur $\mathbf{F}_q$ qui sont birationnelles ont même nombre de points rationnels modulo q (cf. T. Ekedahl, [25]).*

b) *Sur un corps fini, une variété propre et lisse qui est de Fano, ou bien géométriquement faiblement unirationnelle, ou plus généralement rationnellement connexe par chaînes, a un point rationnel (H. Esnault, [26]).*

c) *Sur un corps algébriquement clos de caractéristique $p > 0$, le groupe fondamental d'une variété propre et lisse qui est de Fano, ou bien géométriquement faiblement unirationnelle, ou plus généralement rationnellement connexe par chaînes, est un groupe fini d'ordre premier à p (cf. T. Ekedahl, [25]).*

Le point commun des démonstrations est un contrôle des valuations p -adiques des valeurs propres de Frobenius. Elles gagnent donc à être présentées dans le cadre d'une théorie cohomologique p -adique. La cohomologie rigide, développée par P. Berthelot, fournit l'outil idéal pour cela. Elle a connu récemment des progrès importants et je décris le formalisme auquel elle donne lieu. Les énoncés ci-dessus s'obtiennent en contrôlant les *pentés* des F-isocristaux que fournit la cohomologie rigide.

Je voudrais remercier P. Berthelot, J.-L. Colliot-Thélène, O. Debarre, P. Deligne, H. Esnault, B. Kahn, Y. Laszlo, D. Petrequin et J.-P. Serre pour leurs conseils, suggestions ou corrections.

1. AUTOUR DU THÉORÈME DE CHEVALLEY-WARNING

Je commence cet exposé par un énoncé élémentaire et assez ancien, dû à C. Chevalley et E. Warning [69].

THÉORÈME 1.1. — Soit $\mathbf{F}$ un corps fini, notons q son cardinal et p sa caractéristique. Soient $F_1, \dots, F_r$ des polynômes en $x_1, \dots, x_n$, à coefficients dans $\mathbf{F}$ et de degrés $d_1, \dots, d_r$. Si $n > d_1 + \dots + d_r$, le nombre de solutions dans $\mathbf{F}^n$ du système

$$(1.2) \quad F_1(x_1, \dots, x_n) = \dots = F_r(x_1, \dots, x_n) = 0$$

est multiple de p .

La démonstration classique est très simple et repose sur le fait que pour $x \in \mathbf{F}$, x^{q-1} vaut 1 si $x \neq 0$ et 0 sinon. Ainsi, le nombre de solutions du système est congru modulo p à l'expression

$$\sum_{\mathbf{x} \in \mathbf{F}^n} \prod_{i=1}^r (1 - F_i(\mathbf{x})^{q-1}).$$

Le produit

$$\prod_{i=1}^r (1 - F_i(\mathbf{x})^{q-1})$$

est un polynôme de degré $\leq (q-1) \sum d_i$. Soit

$$c_{\mathbf{m}} x_1^{m_1} \dots x_n^{m_n}$$

un de ses monômes non nuls. On a donc $m_1 + \dots + m_n \leq (q-1) \sum d_i < n(q-1)$ si bien que nécessairement, l'un des entiers m_i est strictement inférieur à $q-1$ et

$$\sum_{\mathbf{x} \in \mathbf{F}^n} c_{\mathbf{m}} x_1^{m_1} \dots x_n^{m_n} = c_{\mathbf{m}} \prod_{i=1}^n \sum_{t \in \mathbf{F}} t^{m_i} = 0$$

puisque

$$\sum_{t \in \mathbf{F}} t^m = \begin{cases} -1 & \text{si } (q-1) \text{ divise } m \text{ et } m \geq 1, \\ 0 & \text{sinon.} \end{cases}$$

Ce théorème a été généralisé par J. Ax [1] et N. Katz [40] :

THÉORÈME 1.3. — Si b désigne le plus petit entier tel que

$$b \geq \frac{n - \sum d_i}{\max d_i},$$

le nombre de solutions du système (1.2) est divisible par q^b .

Leurs démonstrations sont assez savantes. Celle qu'a proposée récemment D. Wan dans [68] lorsque $\mathbf{F} = \mathbf{F}_p$ est en revanche élémentaire et tout à fait dans l'esprit de celle du théorème 1.1. Commençons par introduire l'anneau $\mathbf{Z}_p$ des entiers p -adiques. C'est un anneau de valuation discrète complet, de caractéristique 0, de corps résiduel $\mathbf{F}_p$; son idéal maximal est engendré par p ; il contient les p racines de l'équation $x^p - x = 0$ (notons S cet ensemble). L'idée de base est maintenant que, pour $x \in \mathbf{Z}_p$,

$x^{p^n(p-1)}$ est congru modulo p^n à 1 si $x \not\equiv 0 \pmod{p}$, et à 0 si $x \equiv 0 \pmod{p}$. Le nombre de solutions du système (1.2) est ainsi congru modulo p^n à l'expression

$$\sum_{\mathbf{x} \in S^n} \prod_{i=1}^r (1 - F_i(\mathbf{x})^{p^n(p-1)}).$$

Par récurrence sur r , il suffit de montrer que

$$\sum_{\mathbf{x} \in S^n} \prod_{i=1}^r F_i(\mathbf{x})^{p^n(p-1)} \equiv 0 \pmod{p^b},$$

ce que fait Wan en développant $F_i^{p^n(p-1)}$ puis en constatant que la valuation des divers symboles du multinôme et celle de la somme de puissances qui apparaissent s'ajoutent pour dépasser b . (C'est tout de même assez délicat.)

Lorsque $\mathbf{F}$ n'est pas le corps à p éléments, on peut suivant C. Moreno et O. Moreno [59] effectuer une réduction des scalaires (à la Weil) de $\mathbf{F}$ à $\mathbf{F}_p$: si on fixe une base de $\mathbf{F}$ sur $\mathbf{F}_p$, de cardinal a , on se ramène à un système de ar équations en nr variables de degrés $d_1, \dots, d_r$ (a fois). La nouvelle quantité $(n - \sum d_i) / \max(d_i)$ est égale à a fois l'ancienne. À cause de la partie entière, on en déduit une divisibilité un peu plus faible que celle affirmée par le théorème 1.3.

2. FONCTIONS ZÊTA ET COHOMOLOGIES DE WEIL

Soit $\mathbf{F}$ un corps fini, notons q son cardinal. Dans [70], A. Weil avait introduit pour tout système d'équations polynomiales à coefficients dans $\mathbf{F}$, voire tout $\mathbf{F}$ -schéma V de type fini, la série génératrice

$$Z_V(t) = \exp \left(\sum_{a \geq 0} |V(\mathbf{F}^{(a)})| \frac{t^a}{a} \right)$$

où $\mathbf{F}^{(a)}$ désigne l'unique extension de $\mathbf{F}$ de degré a . B. Dwork [24] a démontré que c'est une fraction rationnelle (première conjecture de Weil). Les inverses de ses zéros et ses pôles sont nécessairement des entiers algébriques. En fait, la congruence du théorème 1.3 implique qu'ils sont divisibles par q^b dans l'anneau des entiers algébriques (*cf.* [1], p. 256).

Les deux autres conjectures de Weil ont été démontrées par A. Grothendieck (rationalité et équation fonctionnelle) dans SGA 5 et P. Deligne (analogue de l'hypothèse de Riemann, [23]), grâce à l'introduction de la cohomologie (étale) ℓ -adique, où ℓ est un nombre premier *distinct* de p . L'utilité d'une telle théorie cohomologique avait déjà été pressentie dans l'article de Weil. En effet, V dispose d'un endomorphisme de Frobenius F et l'ensemble $V(\mathbf{F}^{(a)})$ n'est autre que le lieu des points fixes de F^a ; il faudrait pouvoir disposer alors d'une formule des traces de Lefschetz. Les conditions nécessaires sur une telle cohomologie ont été rapidement formalisées sous le nom de

cohomologie de Weil : la théorie cohomologique doit vérifier la formule de Künneth, la dualité de Poincaré, fournie par une classe fondamentale, et les sous-variétés (non nécessairement lisses) doivent posséder une classe de cohomologie, de manière compatible au produit d'intersection et à la classe fondamentale. Tout ceci est exposé en détail dans [48], en lien avec les théorèmes de Lefschetz faible et difficile, les conjectures « standard » et la conjecture de Hodge.

Lorsque $\ell \neq p$, la cohomologie étale ℓ -adique est effectivement une cohomologie de Weil. Lorsque $\ell = p$, ce n'est pas vrai : $H^i(X, \mathbf{Q}_p)$ est nul dès que $i > \dim X$ ce qui viole la dualité de Poincaré.

Finalement, par voie ℓ -adique, on sait que la fonction zêta d'un $\mathbf{F}$ -schéma géométriquement connexe, propre, lisse de dimension d , est de la forme suivante :

$$Z_X(t) = \frac{P_1(t) \cdots P_{2d-1}(t)}{P_0(t) \cdots P_{2d}(t)},$$

où $P_i(t) \in \mathbf{Z}[t]$, avec $P_0(t) = 1 - t$, $P_{2d}(t) = 1 - q^{2d}t$; si $P_i(t) = \prod_{j=1}^{b_i} (1 - a_{ij}t)$, on sait aussi que les a_{ij} sont des entiers algébriques de valeur absolue archimédienne $q^{i/2}$ (hypothèse de Riemann) et, si $\ell \neq p$, de valeur absolue ℓ -adique nulle.

L'interprétation des valuations p -adiques des a_{ij} , et notamment de congruences du type fourni par les théorèmes 1.1 et 1.3 justifie la recherche d'une théorie cohomologique de Weil qui soit p -adique.

Il y a un autre intérêt — sur lequel insiste Kedlaya — des cohomologies p -adiques que je vais décrire maintenant : elles sont par nature plus calculables que ne l'est la cohomologie étale. Il est par exemple remarquable que soient apparus récemment trois *algorithmes* efficaces (Sato [63], Kedlaya [44], Lauder-Wan [51]) pour calculer le nombre de points de certaines variétés algébriques sur un corps fini, et tous trois sont de nature p -adique. Celui de Kedlaya repose sur l'explicitation de la cohomologie de Monsky-Washnitzer, celui de Lauder-Wan est inspiré de la démonstration par Dwork de la rationalité de la fonction zêta. De même, c'est par des techniques p -adiques que Bombieri [12] a étudié le degré des numérateurs et dénominateurs de fonctions rationnelles associées à des sommes d'exponentielles.

3. COHOMOLOGIES p -ADIQUES

Mais avant cela, il faut peut-être dire pourquoi il n'existe pas de cohomologie de Weil sur la catégorie des variétés algébriques projectives lisses sur un corps algébriquement clos de caractéristique positive à valeur dans la catégorie des $\mathbf{Q}$ -espaces vectoriels de dimension finie. Pour toute cohomologie de Weil à valeurs dans les K -vectoriels (K est un corps commutatif), le H^1 d'une courbe elliptique E est de dimension 2. De plus, pour tout endomorphisme non nul α de E , l'endomorphisme $\alpha^* : H^1(E) \rightarrow H^1(E)$ est injectif, d'où une injection de l'anneau (opposé à celui) des endomorphismes de E

dans l'anneau des matrices 2×2 à coefficients dans K . En caractéristique 0, tout irait bien (d'ailleurs, la cohomologie singulière est une cohomologie de Weil), mais en caractéristique finie, il existe des courbes elliptiques *supersingulières* dont l'anneau des endomorphismes est plus gros que prévu : c'est une algèbre de quaternions sur $\mathbf{Q}$. Comme une telle algèbre ne se plonge pas dans $M_2(\mathbf{Q})$, il n'y a pas de cohomologie de Weil à coefficients dans $\mathbf{Q}$. M. Deuring a même montré que l'algèbre de quaternions $\text{End}(E) \otimes \mathbf{Q}$ est ramifiée en p et l'infini, c'est-à-dire que $\text{End}(E) \otimes \mathbf{Q}_p$ et $\text{End}(E) \otimes \mathbf{R}$ sont des corps gauches. Cela empêche aussi $K = \mathbf{Q}_p$ ou $K = \mathbf{R}$. (Cet argument est dû à J.-P. Serre, cf. [32].)

La théorie que nous utiliserons dans cet exposé est la *cohomologie rigide*, construite par P. Berthelot. Elle unifie deux théories disjointes qui sont la cohomologie de Monsky-Washnitzer [58], valable pour les variétés affines et lisses, et la cohomologie cristalline [32, 2], qui a de bonnes propriétés pour les variétés propres et lisses. Cette théorie est encore éparpillée dans la littérature, et un petit guide de lecture ne sera peut-être pas inutile. Il faudrait aussi citer les travaux de Y. André, F. Baldassarri, P. Berthelot, B. Chiarellotto, G. Christol, R. Crew, B. Dwork, Z. Mebkhout, P. Robba, N. Tsuzuki...

Je trouve l'introduction que propose Berthelot dans [3] très agréable à lire ; le gros article [4] fournit des détails importants dans la construction (les fameux « théorèmes de fibrations »). L'article [6] est très important : outre la démonstration du fait que la cohomologie rigide d'une variété lisse est de dimension finie, on y trouve les théorèmes de comparaison avec les théories de Monsky-Washnitzer et cristalline. Concernant ce théorème de finitude, citons aussi l'article [56] de Z. Mebkhout qui propose une démonstration de la finitude de la cohomologie de Monsky-Washnitzer indépendante des théorèmes de de Jong sur l'existence d'altérations. Notons que la finitude de la cohomologie de Monsky-Washnitzer n'était pas connue avant ces deux articles, à l'exception du H^0 et du H^1 par P. Monsky. La finitude de la cohomologie rigide dans le cas général est démontrée (indépendamment) dans l'article [31] de E. Grosse-Klönne et dans celui [67] de N. Tsuzuki dans lequel il établit un théorème de descente cohomologique propre.

La dualité de Poincaré et la formule de Künneth sont établies dans la note [5] de Berthelot. Enfin, l'existence de classes de Chern est démontrée par D. Petrequin [61].

Qu'est-ce que la cohomologie rigide ? Disons tout d'abord que c'est une sorte de cohomologie de de Rham. Fixons quelques notations : soit k un corps de caractéristique $p > 0$, fixons alors un anneau de valuation discrète complet $\mathcal{V}$ de corps résiduel k , dont nous noterons K le corps des fractions, supposé de caractéristique zéro, et π un générateur de l'idéal maximal de $\mathcal{V}$. Nous supposons que $\mathcal{V}$ admet un endomorphisme σ qui se réduit modulo π en l'automorphisme de Frobenius $\sigma: x \mapsto x^p$ de k ; alors, σ s'étend en un endomorphisme de K . Dans tout ce qui va suivre, on peut se