Groupe de travail
d'analyse ultramétrique

Jan Stienstra

Les groupes formels d'Artin-Mazur et les congruences d'Atkin-Swinnerton-Dyer

Groupe de travail d'analyse ultramétrique, tome 12, n° 2 (1984-1985), exp. n° 18, p. 1-13

<http://www.numdam.org/item?id=GAU_1984-1985__12_2_A1_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
12e année, 1984/85, n° 18, 13 p.

15 avril 1985

LES GROUPES FORMELS D'ARTIN — MAZUR ET LES CONGRUENCES D'ATKIN - SWINNERTON-DYER

par Jan STIENSTRA (*)

Les congruences d'Atkin - Swinnerton-Dyer, pour un modèle E sur $\underset{\sim}{Z}$ (ou $\underset{\sim}{Z}_p$) d'une courbe elliptique, relient la fonction zêta de E et la forme différentielle canonique sur E (voir [2], [6], [8], [9]). De telles congruences existent aussi pour d'autres classes de variétés à modèles entiers et de genre $p_g = 1$; par exemple pour certaines surfaces $K3$ (cf. [16]). Dans cette note, on donne une démonstration de ces congruences. La méthode est fondée sur une analyse des foncteurs d'Artin-Mazur, qui dans les cas considérés sont des groupes formels (cf. [1]). Le lien entre ces groupes formels et les facteurs de la fonction zêta de la variété est fourni par la théorie de Cartier-Dieudonné et la cohomologie cristalline, en particulier la suite spectrale des pentes ([19], [10]). Le lien entre ces groupes formels et les formes différentielles est établi, dans les cas considérés, par un calcul direct en cohomologie de Čech de l'espace projectif [17]. Les congruences sont alors une traduction précise du rapport entre les deux descriptions.

Voici le plan de cette note. Au paragraphe 1, on rappelle la définition et quelques propriétés élémentaires des groupes formels. Au paragraphe 2, on montre comment la théorie de Cartier implique des congruences. Au paragraphe 3, on donne la définition des foncteurs d'Artin-Mazur et leur lien avec la cohomologie du faisceau des vecteurs de Witt. Au paragraphe 4, on rappelle quelques résultats de la théorie de la cohomologie cristalline, du complexe de De Rham-Witt et des fonctions zêta. Au paragraphe 5, on décrit une classe de variétés pour lesquelles on peut calculer les groupes formels d'Artin-Mazur très explicitement. Au paragraphe 6, on fait la synthèse et on décrit un exemple.

1. Rappels sur les groupes formels.

Pour la théorie générale voir [8], [9], [15], [19].

1.1. Soit K un anneau, commutatif avec unité. Soit $\mathbf{Nilalgs}_K$ la catégorie des K-algèbres commutatives associatives sans unité, dont les éléments sont nilpotents. L'espace affine formel à n dimensions sur K est le foncteur

$$\underset{\sim}{A}^n_K : \mathbf{Nilalgs}_K \longrightarrow \text{Ensembles}$$

qui à un objet A (resp. un morphisme f) de $\mathbf{Nilalgs}_K$ associe l'ensemble $A \times \ldots \times A$ (resp. l'application $f \times \ldots \times f$), produit cartésien à n facteurs.

(*) Jan STIENSTRA, Mathematisch Instituut, Rijksuniversiteit Utrecht, 6 Budapestlaan, NL-3508 TA UTRECHT (Pays-Bas).

Un groupe formel de dimension n sur K (sauf mention du contraire les groupes formels, que nous considérons, sont lisses et commutatifs) est un foncteur covariant

$$G \ ; \ \mathbf{Nilalgs}_K \longrightarrow \text{Groupes abéliens}$$

tel que le foncteur "ensembliste" sous-jacent admette une bijection fonctorielle vers $\underset{\sim}{A}^n_K$. Une telle bijection fonctorielle, $c : G \xrightarrow{\sim} \underset{\sim}{A}^n_K$ s'appelle une paramétrisation de G .

1.2. Le choix d'une paramétrisation $c : G \xrightarrow{\sim} \underset{\sim}{A}^n_K$ fournit une loi de groupe formel $L(\xi , \eta)$ de dimension n sur K ; i. e. un n-uple $L = (L_1 , \dots , L_n)$ de séries formelles à coefficients dans K en deux n-uples de variables $\xi = (\xi_1 , \dots , \xi_n)$ et $\eta = (\eta_1 , \dots , \eta_n)$, tel que, pour tout $A \in \mathrm{Nilalgs}_K$ et tous $\alpha , \beta \in G(A)$

$$c(\alpha \oplus \beta) = L(c(\alpha) , c(\beta)) ,$$

où $\oplus$ est l'addition dans le groupe $G(A)$. Les axiomes de groupe commutatif pour G sont alors équivalents aux identités suivantes, pour $L(\xi , \eta)$,

$$L(L(\xi , \eta) , \zeta) = L(\xi , L(\eta , \zeta)) , \quad L(\xi , 0) = \xi , \quad L(\xi , \eta) = L(\eta , \xi) ,$$

où ζ est un autre n-uple d'indéterminées et $0 = (0 , \dots , 0)$. Aussi

$$L(\xi , \eta) \equiv \xi + \eta \mod \deg \geq 2 .$$

1.3. Si l'homomorphisme $K \longrightarrow K \otimes \mathbb{Q}$ est injectif, à toute loi de groupe formel de dimension n sur K , $L(\xi , \eta)$, correspond un n-uple $\lambda(\tau)$ de séries formelles à coefficients dans $K \otimes \mathbb{Q}$ en n indéterminées $\tau = (\tau_1 , \dots , \tau_n)$, tel que

$$\lambda(\tau) \equiv \tau \mod \deg \geq 2$$

$$L(\xi , \eta) = \lambda^{-1}(\lambda(\xi) + \lambda(\eta)) .$$

On appelle $\lambda(\tau)$ le logarithme de la loi de groupe formel $L(\xi , \eta)$.

1.4. Les exemples les plus simples sont le groupe formel additif $\underset{\sim}{G}_a^{\wedge}$ et le groupe formel multiplicatif $\underset{\sim}{G}_m^{\wedge}$; ces groupes sont de dimension 1 et définis sur $\underset{\sim}{Z}$. $\underset{\sim}{G}_a^{\wedge}$ admet une paramétrisation pour laquelle la loi de groupe formel est $L(\xi , \eta) = \xi + \eta$ et le logarithme est $\lambda(\tau) = \tau$. $\underset{\sim}{G}_m^{\wedge}$ admet une paramétrisation pour laquelle la loi de groupe formel est $L(\xi , \eta) = \xi + \eta - \xi\eta$, et le logarithme est

$$\lambda(\tau) = \sum_n n^{-1} \tau^n = - \log(1 - \tau) .$$

2. Module des courbes et congruences.

Pour la théorie générale de Cartier voir ([5], [19], [15], [8]).

2.1. La théorie de Cartier associe à un groupe formel G de dimension n sur un anneau K son module des courbes, défini par

$$CG = \lim_{\leftarrow m} G(tK[t]/(t^m)) .$$

Ayant choisi une paramétrisation de G, on peut identifier CG avec l'ensemble $(tK[[t]])^n$ des n-uples de séries formelles, en une variable, sans termes constants, muni de l'addition donnée par la loi de groupe formel associée avec la paramétrisation de G.

2.2. CG est un module sur l'anneau de Cartier de K. On dispose, en particulier, d'éléments V_k (Verschiebung = décalage) et F_k (Frobenius), pour tout entier $k \geqslant 1$, qui opèrent comme suit :

V_k correspond à l'application induite par la substitution $t \mapsto t^k$;

F_k se définit par la formule

$$F_k(\gamma(t)) = \gamma(\zeta t^{1/k}) \oplus \gamma(\zeta^2 t^{1/k}) \oplus \dots \oplus \gamma(\zeta^k t^{1/k})$$

pour $\gamma(t) \in CG$, et ζ une racine k-ième primitive de l'unité.

2.3. THÉORÈME. - *Soit K un anneau tel que $K \to K \otimes \mathbb{Q}$ soit injectif. Soit p un nombre premier. Soit G un groupe formel de dimension 1 sur K, et $\bar{G}$ sa réduction sur K/pK (i. e. la restriction du foncteur G à la sous-catégorie $\mathrm{Nilalgs}_{K/pK}$ de $\mathrm{Nilalgs}_K$). Etant donnée une paramétrisation de G, soit*

$$\lambda(\tau) = \sum_{n \geqslant 1} n^{-1} \beta_n \tau^n$$

le logarithme de la loi de groupe formel correspondante. Les β_n sont automatiquement dans K. Supposons qu'il existe des nombres entiers $a_1, \dots, a_k$ tels que l'opérateur

$$F_p + a_1 I + a_2 V_p + a_3 V_p^2 + \dots + a_k V_p^{k-1}$$

s'annule sur $C\bar{G}$ (I = identité).

Alors on a les congruences : pour tout $n \geqslant 1$,

$$\beta_n + a_1 \beta_{n/p} + p a_2 \beta_{n/p^2} + \dots + p^{k-1} a_k \beta_{n/p^k} \equiv 0 \mod p^s \quad \text{si} \quad p^s | n$$

(avec la convention $\beta_m = 0$ si $m \notin \mathbb{Z}$).

Démonstration. - En utilisant la paramétrisation de G, on identifie CG avec $tK[[t]]$. Par restriction de $\mathrm{Nilalgs}_K$ à $\mathrm{Nilalgs}_{K/pK}$, on obtient une paramétrisation de $\bar{G}$ et donc une identification de $C\bar{G}$ avec $t(K/pK)[[t]]$. L'hypothèse que $F_p + a_1 V_p^0 + \dots + a_k V_p^{k-1}$ s'annule sur $C\bar{G}$ implique que cet opérateur opérant sur CG a son image dans le noyau de $CG \to C\bar{G}$; i. e., avec les identifications données, dans $tpK[[t]]$. En particulier, on a

$$(F_p + a_1 V_p^0 + \dots + a_k V_p^{k-1})(t) = tpf(t)$$

avec $f(t) \in K[[t]]$. D'après les définitions de F_p, V_p et λ, le membre de gauche s'écrit

$$\lambda^{-1}(\lambda(\zeta t^{1/p}) + \dots + \lambda(\zeta^p t^{1/p}) + a_1 \lambda(t) + a_2 \lambda(t^p) + \dots + a_k \lambda(t^{p^{k-1}})),$$

où ζ est une racine p-ième primitive de 1, et $+$ désigne l'addition ordinaire des séries. Un calcul simple montre que cette expression est égale à

$$\mathcal{L}^{-1}\left(\sum_{n\geq 1}\left(\beta_{np} + a_1\,\beta_n + pa_2\,\beta_{n/p} + \cdots + p^{k-1}\,a_k\,\beta_{n/p^{k-1}}\right)\frac{t^n}{n}\right).$$

Par conséquent,

$$\begin{aligned}\sum_{n\geq 1}\left(\beta_{np} + a_1\,\beta_n + pa_2\,\beta_{n/p} + \cdots + p^{k-1}\,a_k\,\beta_{n/p^{k-1}}\right)\frac{t^n}{n}&\\ = \mathcal{L}(pt(t))&\\ = \sum_{n\geq 1} n^{-1}\,p^n\,\beta_n\,t^n\,f(t)^n&\\ = \text{une série formelle en } t \text{ à coefficients dans } pK\otimes \mathbb{Z}_{(p)}&,\end{aligned}$$

où $\mathbb{Z}_{(p)} = \{\, n/m \in \mathbb{Q} \;;\; (n\,,\,m) = (p\,,\,m) = 1\,\}$. En comparant les coefficients de ces séries on trouve les congruences annoncées.

Remarque. - On trouve des résultats analogues plus généraux, sans référence à la théorie de Cartier, dans la théorie de Honda [9] et le "functional equation lemma" de Hazewinkel [8].

3. Les foncteurs d'Artin-Mazur. [1].

3.1. Soit X un schéma sur un anneau K. On lui associe les foncteurs d'Artin-Mazur (pour $i = 0\,,\,1\,,\,2\,,\,\ldots$)

$$H^i(X\,,\,\hat{\mathbb{G}}_{m,X}) : \text{Nilalgs}_K \longrightarrow \text{Groupes abéliens}$$

(dans [1] ce foncteur est noté $\mathfrak{X}^i$), définis comme suit. Soit $\mathcal{O}_X$ le faisceau d'anneaux structural sur X. Si A est une nil-K-algèbre, notons $\mathcal{O}_X \otimes_K A$ le faisceau pour la topologie de Zariski sur X associé au pré-faisceau

$$(U \subset X \text{ ouvert}) \longmapsto \Gamma(U\,,\,\mathcal{O}_X)\otimes_K A\,,$$

et $\hat{\mathbb{G}}_{m,X}(A)$ le faisceau de groupes abéliens, tel que

$$\Gamma(U\,,\,\hat{\mathbb{G}}_{m,X}(A)) = \hat{\mathbb{G}}_m(\Gamma(U\,,\,\mathcal{O}_X\otimes_K A))\,.$$

Alors le foncteur $H^i(X\,,\,\hat{\mathbb{G}}_{m,X})$ associe à la nil-K-algèbre A le i-ième groupe de cohomologie, $H^i(X\,,\,\hat{\mathbb{G}}_{m,X}(A))$, du faisceau $\hat{\mathbb{G}}_{m,X}(A)$.

3.2. Supposons X/K propre. Alors, si $H^i(X\,,\,\hat{\mathbb{G}}_{m,X})$ est un groupe formel, son module des courbes est donné par

$$\begin{aligned}C(H^i(X\,,\,\hat{\mathbb{G}}_{m,X})) &= \lim_{\leftarrow n} H^i(X\,,\,\hat{\mathbb{G}}_{m,X}(tK[t]/(t^n))\\ &= H^i(X\,,\,\lim_{\leftarrow n}\hat{\mathbb{G}}_{m,X}(tK[t]/(t^n))\\ &= H^i(X\,,\,C\hat{\mathbb{G}}_{m,X})\,.\end{aligned}$$

Le faisceau $C\underset{\sim}{G}_{m,X}^{\wedge}$, par définition égal à $\varprojlim \underset{\sim}{G}_{m,X}^{\wedge}(tK[t]/(t^n))$, s'identifie, par une paramétrisation de $\underset{\sim}{G}_{m}^{\wedge}$, au faisceau $t\mathcal{O}_X[[t]]$ muni de l'addition $f \oplus g = f + g - fg$.

Ce faisceau $C\underset{\sim}{G}_{m,X}^{\wedge}$ est le faisceau des groupes additifs sousjacents au faisceau des anneaux des vecteurs de Witt généralisés (cf. [5], [4], [10]).

3.3. Soit p un nombre premier. Supposons que tous les nombres premiers $\neq p$ soient inversibles dans l'anneau K. L'opérateur

$$E = \sum_{n \in \underset{\sim}{N} \setminus p\underset{\sim}{N}} n^{-1}\, \mu(n)\, V_n F_n : C\underset{\sim}{G}_{m,X}^{\wedge} \longrightarrow C\underset{\sim}{G}_{m,X}^{\wedge},$$

où μ désigne la fonction de Möbius, est un projecteur. Son image, $EC\underset{\sim}{G}_{m,X}^{\wedge}$, s'identifie au faisceau $\mathbb{W}\mathcal{O}_X$ des vecteurs de Witt p-typiques sur X (voir [4], [5], [10], [11], [12]), et l'on a un isomorphisme

$$C\underset{\sim}{G}_{m,X}^{\wedge} \underset{\sum n^{-1} V_n}{\overset{(E F_n)_n}{\rightleftarrows}} \prod_n \mathbb{W}\mathcal{O}_X,$$

où n parcourt les entiers positifs non divisibles par p (voir [4], [5], [10]). Les opérateurs V_n et F_n, pour $(n, p) = 1$, commutent avec V_p et F_p. Par conséquent, E aussi commute avec V_p et F_p. Donc, V_p et F_p opèrent sur $\mathbb{W}\mathcal{O}_X$, et cette action commute avec la décomposition $C\underset{\sim}{G}_{m,X}^{\wedge} \xrightarrow{\sim} \prod_{p \nmid n} \mathbb{W}\mathcal{O}_X$.

3.4. Soient maintenant p un nombre premier, K un anneau tel que les nombres premiers $\neq p$ soient inversibles dans K, et X un schéma propre sur K. Si $H^i(X, \underset{\sim}{G}_{m,X}^{\wedge})$ est un groupe formel, on a, d'après ce qui précède, une décomposition

$$C(H^i(X, \underset{\sim}{G}_{m,X}^{\wedge})) \xrightarrow{\sim} \prod_{p \nmid n} H^i(X, \mathbb{W}\mathcal{O}_X),$$

commutante avec l'action des opérateurs V_p et F_p. En particulier, pour qu'un opérateur $F_p + a_1 I + a_2 V_p + \ldots + a_k V_p^{k-1}$, avec $a_j \in \underset{\sim}{Z}$, s'annule sur $C(H^i(X, \underset{\sim}{G}_{m,X}^{\wedge}))$, il faut et il suffit qu'il s'annule sur $H^i(X, \mathbb{W}\mathcal{O}_X)$.

4. Cohomologie cristalline.

Pour la théorie générale, voir [4], [10], [11], [12], [3].

4.1. Dans ce paragraphe, K désigne un corps parfait de caractéristique $p > 0$, et X est un schéma projectif lisse sur K. D'après BLOCH [4], DELIGNE et ILLUSIE ([10], [11], [12]), la cohomologie cristalline $H^*_{cris}(X)$ de X s'écrit comme (limite de) l'hypercohomologie d'un (pro -) complexe de faisceaux pour la topologie de Zariski sur X

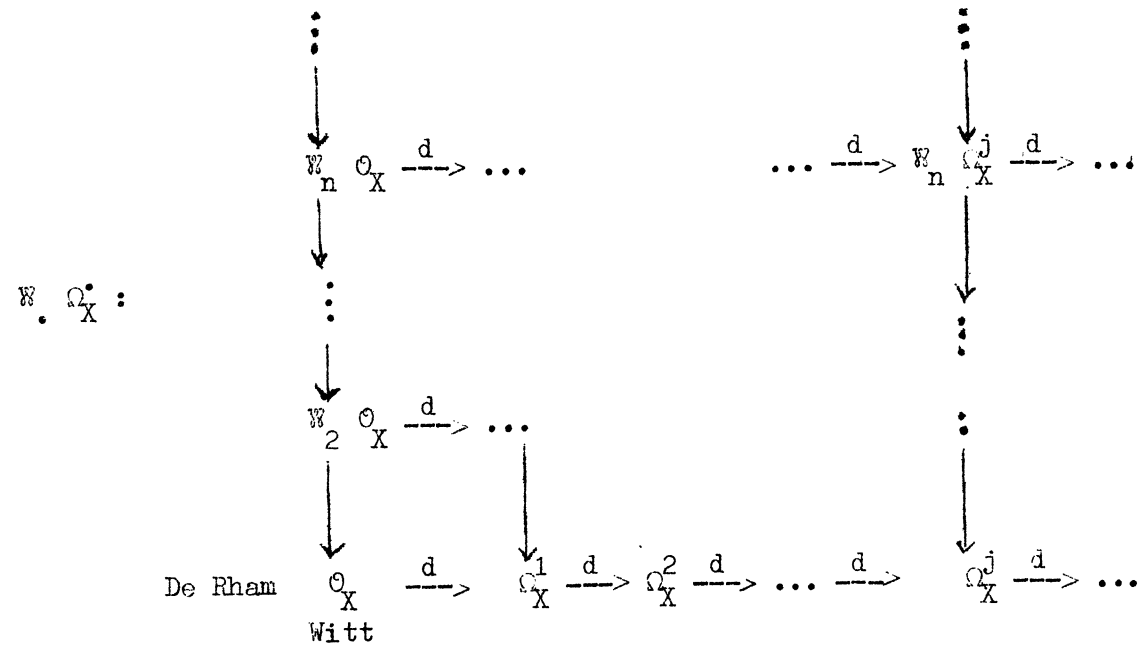
$$(*) \qquad H^i_{cris}(X) = \varprojlim_n \underset{\sim}{H}^i(X, W_n \Omega_X^\cdot) = \underset{\sim}{H}^i(X, \mathbb{W}\Omega_X^\cdot).$$

Le pro-complexe $\mathbb{W}\Omega_X^\cdot$, qu'on appelle le pro-complexe de De Rham — Witt sur X,

combine le complexe de De Rham $\Omega_X^\cdot$ d'une part avec le système

$$W_\cdot \mathcal{O}_X = \{W_n \mathcal{O}_X\}_{n\geq 1} = \{W\mathcal{O}_X/V_p^n W\mathcal{O}_X\}_{n\geq 1}$$

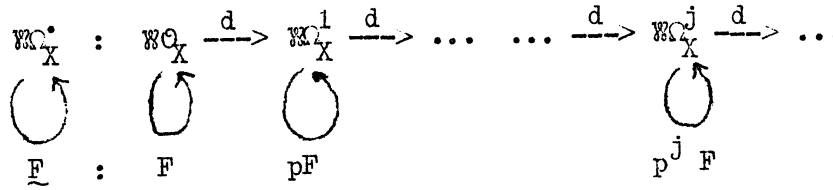
des vecteurs de Witt tronqués sur X, d'autre part



Dans ce diagramme, chaque ligne représente une algèbre différentielle graduée, et les flèches verticales donnent des homomorphismes d'ADG's. Chaque colonne est munie d'opérateurs $V : W_n \Omega_X^j \longrightarrow W_{n+1} \Omega_X^j$ et $F : W_{n+1} \Omega_X^j \longrightarrow W_n \Omega_X^j$, qui pour $j = 0$ (i. e. $W\mathcal{O}_X$), sont les $V(= V_p)$ et $F(= F_p)$ usuels. On a les relations

$$FV = VF = p \ , \quad FdV = d \ , \quad pFd = dF \ , \quad pdV = Vd \ .$$

Le <u>complexe de De Rham - Witt</u> $W\Omega_X^\cdot$ est la limite du pro-complexe $W_\cdot \Omega_X^\cdot$. Les opérateurs V et F passent à la limite et satisfont encore aux relations précédentes. On construit un endomorphisme $\underset{\sim}{F}$ du complexe $\Omega_X^\cdot$ en prenant $p^j F$ en degré j



L'endomorphisme $\underset{\sim}{F}$ de $W\Omega_X^\cdot$ induit un endomorphisme en hypercohomologie

$$F : \underset{\sim}{H}^i(X , W\Omega_X^\cdot) \longrightarrow \underset{\sim}{H}^i(X , W\Omega_X^\cdot)$$

pour chaque i. Via (*), cette opération correspond à l'action par fonctorialité de l'endomorphisme de Frobenius absolu sur X.

4.2. Par projection sur la partie de degré 0, on obtient un homomorphisme du complexe de De Rham - Witt sur le faisceau des vecteurs de Witt :

$$\begin{array}{ccccccccccc} W\Omega_X^\cdot & : & W\mathcal{O}_X & \longrightarrow & W\Omega_X^1 & \longrightarrow & \cdots & \cdots & \longrightarrow & W\Omega_X^j & \longrightarrow \cdots \\ \downarrow & & \| & & \downarrow & & & & & \downarrow & \\ W\mathcal{O}_X & : & W\mathcal{O}_X & \longrightarrow & 0 & \longrightarrow & \cdots & \cdots & \longrightarrow & 0 & \longrightarrow \cdots \end{array}$$

Cet homomorphisme commute avec $\underset{\sim}{F}$ sur $W\Omega_X^\cdot$ et F sur $W\mathcal{O}_X$. Il induit, pour tout i, un homomorphisme

$$\pi : \underset{\sim}{H}^i(X , W\Omega_X^\cdot) \longrightarrow H^i(X , W\mathcal{O}_X) ,$$

commutant avec les endomorphismes F.

L'homomorphisme π s'identifie au composé

$$\underset{\sim}{H}^i(X , W\Omega_X^\cdot) \longrightarrow E^{0i} \longrightarrow E_1^{0i} = H^i(X , W\mathcal{O}_X)$$

déduit de la suite spectrale (dite suite spectrale des pentes)

$$E_1^{ji} = H^i(X , W\Omega_X^j) \Longrightarrow \underset{\sim}{H}^*(X , W\Omega_X^\cdot)$$

(voir [10], [4]). Cette suite spectrale dégénère modulo torsion (loc. cit.) ; i. e. les différentielles de la suite spectrale

$$E_1^{ji} \otimes \underset{\sim}{Q} = H^i(X , W\Omega_X^j) \otimes \underset{\sim}{Q} \Longrightarrow \underset{\sim}{H}^*(X , W\Omega_X^\cdot) \otimes \underset{\sim}{Q}$$

sont nulles. Par conséquent, l'application

$$\pi \otimes \underset{\sim}{Q} : \underset{\sim}{H}^i(X , W\Omega_X^\cdot) \otimes \underset{\sim}{Q} \longrightarrow H^i(X , W\mathcal{O}_X) \otimes \underset{\sim}{Q}$$

est surjective pour tout i. Comme $\pi \otimes \underset{\sim}{Q}$ commute avec F, un endomorphisme $F^k + b_1 F^{k-1} + \ldots + b_{k-1} F + b_k I$, avec $b_i , \ldots , b_k \in \underset{\sim}{Z}$, qui s'annule sur $H^i_{cris}(X) \otimes \underset{\sim}{Q}$, s'annule aussi sur $H^i(X , W\mathcal{O}_X) \otimes \underset{\sim}{Q}$.

4.3. On suppose désormais $K = \underset{\sim}{F}_p$. La fonction zêta de $X/\underset{\sim}{F}_p$ est définie par

$$Z(X/\underset{\sim}{F}_p ; T) = \exp\Big(\sum_{n\geq 1} n^{-1} \, \# X(\underset{\sim}{F}_{p^n}) \, T^n\Big) ,$$

où $\# X(\underset{\sim}{F}_{p^n})$ est le nombre des points de X définis sur $\underset{\sim}{F}_{p^n}$.

D'après DELIGNE [7] et KATZ-MESSING [13], on a

$$Z(X/\underset{\sim}{F}_p ; T) = \frac{P_1(T).P_3(T) \ldots P_{2N-1}(T)}{P_0(T).P_2(T) \ldots P_{2N}(T)}$$

avec $N = \dim X$, $P_i(T) = \det(1 - TF | H^i_{cris}(X) \otimes \underset{\sim}{Q})$, $P_i(T) \in \underset{\sim}{Z}[T]$ pour $i = 0, \cdots, 2N$; F est l'endomorphisme de Frobenius.

4.4. THÉORÈME. - *Soit X une variété projective et lisse sur $\underset{\sim}{F}_p$. Soit i un nombre entier positif $\leq 2 \dim X$. Soit $P_i(T) = \det(1 - TF | H^i_{cris}(X) \otimes \underset{\sim}{Q})$. On fait l'hypothèse que $H^i(X , \hat{G}_{m,X})$ est un groupe formel de dimension 1 sur $\underset{\sim}{F}_p$. Alors le polynôme $P_i(T)$ s'écrit comme*

$$P_i(T) = 1 + a_1 T + p a_2 T^2 + \ldots + p^{k-1} a_k T^k$$

avec $a_1, \ldots, a_k \in \underset{\sim}{Z}$, et l'opérateur

$$F + a_1 I + a_2 V + a_3 V^2 + \ldots + a_k V^{k-1}$$

sur le module des courbes $C(H^i(X, \hat{G}_{m,X}))$ est nul.

Démonstration. - Le corps de base étant $\underset{\sim}{F}_p$, le polygone de Newton pour l'action de F sur $H^i_{cris}(X) \otimes \underset{\sim}{Q}$ coïncide avec le polygone de Newton du polynôme $P_i(T)$ (cf. [14]). Si $P_i(T) = 1 + b_1 T + \ldots + b_k T^k$, ce polygone est la plus haute courbe polygonale convexe dans $\underset{\sim}{R}^2$ entre $(0, 0)$ et $(k, \mathrm{ord}_p b_k)$ qui passe par (ou dessous) des points $(j, \mathrm{ord}_p b_j)$ pour $j = 1, \ldots, k$. D'autre part, on a le polygone de Hodge pour H^i de X : c'est le polygone de sommets $(0, 0)$ et $(\sum_{0 \leqslant r \leqslant j} h^{r,i-r}, \sum_{0 \leqslant r \leqslant j} r\, h^{r,i-r})$ pour $j = 1, 2, \ldots, i$; les $h^{r,i-r}$ sont les nombres de Hodge $h^{r,i-r} = \dim H^{i-r}(X, \Omega^r_X)$. D'après la conjecture de Katz, démontrée par MAZUR, OGUS et NIGAARD ([3], [10], [11], [12]), le polygone de Newton est situé sur (ou au-dessus) du polygone de Hodge. Par conséquent, si $h^{0i} = 1$, le nombre b_j est divisible par p^{j-1} pour $j = 1, \ldots, k$.

L'espace tangent de $H^i(X, \hat{G}_{m,X})$, par définition égal à

$$H^i(X, \hat{G}_{m,X}(t \underset{\sim}{F}_p[t]/(t^2))),$$

est isomorphe à $H^i(X, \mathcal{O}_X)$. Donc $H^i(X, \mathcal{O}_X)$ est de dimension 1 sur $\underset{\sim}{F}_p$, i. e. $h^{0i} = 1$, et d'après ce qui précède, le polynôme $P_i(T)$ peut s'écrire

$$P_i(T) = 1 + a_1 T + p a_2 T^2 + \ldots + p^{k-1} a_k T^k$$

avec $a_1, \ldots, a_k \in \underset{\sim}{Z}$. D'après Cayley-Hamilton, l'opérateur

$$F^k + a_1 F^{k-1} + p a_2 F^{k-2} + \ldots + p^{k-1} a_k I$$

s'annule sur $H^i_{cris}(X) \otimes \underset{\sim}{Q}$, et donc aussi sur $H^i(X, W\mathcal{O}_X) \otimes \underset{\sim}{Q}$ (cf. (4.2)). Sur $H^i(X, W\mathcal{O}_X)$, on dispose de l'endomorphisme V, vérifiant $FV = VF = p$, et l'opérateur ci-dessus peut s'écrire aussi

$$(F + a_1 I + a_2 V + a_3 V^2 + \ldots + a_k V^{k-1}) F^{k-1}.$$

Comme $H^i(X, \hat{G}_{m,X})$ est un groupe formel de dimension 1, ou bien F est nul sur son module des courbes, et donc aussi sur $H^i(X, W\mathcal{O}_X)$, ou bien F est injectif sur le module des courbes et sur $H^i(X, W\mathcal{O}_X)$.

Considérons d'abord le cas où F est injectif sur $H^i(X, W\mathcal{O}_X)$. Alors $F + a_1 I + a_2 V + \ldots + a_k V^{k-1}$ est nul sur $H^i(X, W\mathcal{O}_X) \otimes \underset{\sim}{Q}$. Par ailleurs, comme $H^i(X, \hat{G}_{m,X})$ est un groupe formel, l'endomorphisme V de $H^i(X, W\mathcal{O}_X)$ est injectif [5]. Comme $FV = p$, il s'ensuit que $H^i(X, W\mathcal{O}_X)$ est sans p-torsion et que l'application $H^i(X, W\mathcal{O}_X) \longrightarrow H^i(X, W\mathcal{O}_X) \otimes \underset{\sim}{Q}$ est injective. Par conséquent,

$F + a_1 I + a_2 V + \ldots + a_k V^{k-1}$ s'annule sur $H^i(X , \mathbb{W}\mathcal{O}_X)$, et donc aussi sur le module des courbes $C(H^i(X , \underset{\sim}{G}_{m,X}^{\wedge}))$.

Considérons maintenant le cas où $F = 0$ sur $H^i(X , \mathbb{W}\mathcal{O}_X)$. Alors $p = VF = 0$ sur $H^i(X , \mathbb{W}\mathcal{O}_X)$ et donc $H^i(X , \mathbb{W}\mathcal{O}_X) \otimes \underset{\sim}{Q} = 0$. Par la théorie générale de la suite spectrale des pentes ([4], [10], [11], [12]), toutes les pentes de $H^i_{cris}(X)$ sont alors $\geqslant 1$. Pour le polynôme $P_i(T) = 1 + a_1 T + p\, a_2 T^2 + \ldots + p^{k-1} a_k T^k$, ceci implique que chaque a_j est divisible par p . Par conséquent, l'opérateur $F + a_1 I + a_2 V + \ldots + a_k V^{k-1}$ sur $H^i(X , \mathbb{W}\mathcal{O}_X)$, et sur $C(H^i(X , \underset{\sim}{G}_{m,X}^{\wedge}))$, est nul.

5. Revêtements doubles de $\underset{\sim}{P}^N$ et logarithmes.

5.1. Soit N un entier $\geqslant 1$. Soit $G(T_0 , \ldots , T_N) \in \underset{\sim}{Z}[T_0 , \ldots , T_N]$ une forme homogène de degré $2N + 2$. Soit X le revêtement double de $\underset{\sim}{P}^N_{\underset{\sim}{Z}}$ donné par l'équation

$$S^2 = G(T_0 , \ldots , T_N) .$$

On sait [17] que $H^N(X , \underset{\sim}{G}_{m,X}^{\wedge})$ est un groupe formel de dimension 1 sur $\underset{\sim}{Z}$. De plus, on dispose d'une paramétrisation pour laquelle le logarithme est

$$\mathcal{L}(\tau) = \sum_{n \geqslant 1} n^{-1} \beta_n \tau^n$$

avec

$$\beta_n = \begin{cases} \text{coefficient de } (T_0 \ldots T_N)^{n-1} \text{ dans } (G(T_0 , \ldots , T_N))^{(n-1)/2} & \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{si } n \text{ est impair} & \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{si } n \text{ est pair .} & \end{cases}$$

5.2. La série $\mathcal{L}(\tau)$ admet aussi (loc. cit.) la représentation intégrale suivante

$$\mathcal{L}(\tau) = (2\pi \sqrt{-1})^{1-N} \int_{X(\underset{\sim}{\varepsilon} , \tau)} \frac{dt_1 \wedge \ldots \wedge dt_N}{2\sqrt{G(1 , t_1 , \ldots , t_N)}}$$

où le domaine d'intégration, $X(\underset{\sim}{\varepsilon} , \tau)$, est donné (si $G(T_0 , \ldots , T_N)$ n'est pas divisible par τ_1^2) par

$$X(\underset{\sim}{\varepsilon} , \tau) = \begin{cases} (s , t_1 , \ldots , t_N) \in \underset{\sim}{C}^{N+1} \text{ t. q. } s^2 = G(1 , t_1 , \ldots , t_N) , \ |t_1| \leqslant \varepsilon_1 & \\ |t_j| = \varepsilon_j \text{ pour } 2 \leqslant j \leqslant N , \ |t_1 \cdot \ldots \cdot t_N . s^{-1}| \leqslant |\tau| , & \\ \arg(t_1 \cdot \ldots \cdot t_N . s^{-1}) = \arg \tau & \end{cases}$$

$\underset{\sim}{\varepsilon} = (\varepsilon_1 , \ldots , \varepsilon_N)$ est un n-uple de nombres réels positifs convenablement choisis et τ appartient à un disque ouvert suffisament petit de centre 0 dans $\underset{\sim}{C}$

5.3. Prenons $N = 1$ et $G(T_0 , T_1) = T_0(T_1^3 + b\, T_1 T_0^2 + c\, T_0^3)$ avec $4b^3 + 27c^2 \neq 0$,

i. e. considérons la courbe elliptique E donnée par l'équation de Weierstrass $y^2 = x^3 + bx + c$, alors le résultat de (5.1) fournit la description habituelle, en termes du paramètre $\tau = x/y$ à l'infini, de la loi de groupe formel de E (voir [18]), et (5.2) n'est autre que l'intégrale elliptique classique.

6. Synthèse.

Soit N un entier $\geqslant 1$. Soit $G(T_0 , \dots , T_N) \in \underset{\sim}{Z}[T_0 , \dots , T_N]$ un polynôme homogène de degré $2N + 2$.

6.1. Soit X le schéma donné comme revêtement double de $\underset{\sim}{P}^N_{\underset{\sim}{Z}}$ par l'équation $S^2 = G(T_0 , \dots , T_N)$. D'après (5.1), on sait que $H^N(X , \underset{\sim}{G}^{\wedge}_{m,X})$ est un groupe formel de dimension 1 sur $\underset{\sim}{Z}$, et on a un logarithme $\lambda(\tau)$ pour ce groupe formel. Le lien entre ce logarithme et la forme différentielle de degré N , régulière et sans zéros, sur la partie lisse de la variété (algébrique ou analytique) $X_{\underset{\sim}{C}}$, est donné par l'intégrale dans (5.2).

6.2. Soit p un nombre premier. Soit $X_p/\underset{\sim}{F}_p$ la réduction mod p de $X/\underset{\sim}{Z}$; i. e. le revêtement double de $\underset{\sim}{P}^N_{\underset{\sim}{F}_p}$, donné par l'équation $S^2 = G(T_0 , \dots , T_N)$ mod p . On montre, dans [17], que $H^N(X_p , \underset{\sim}{G}^{\wedge}_{m,X_p})$ est la restriction de $H^N(X , \underset{\sim}{G}^{\wedge}_{m,X})$ à la sous-catégorie $\mathrm{Nilalgs}_{\underset{\sim}{F}_p}$ de $\mathrm{Nilalgs}_{\underset{\sim}{Z}}$.

6.3. Il peut arriver dans (6.2) que X_p ne soit pas lisse sur $\underset{\sim}{F}_p$. Parce que la théorie de la cohomologie cristalline, du complexe de De Rham-Witt et des fonctions zêta n'a été développée qu'au cas lisse et projectif, nous ferons l'hypothèse supplémentaire suivante.

Hypothèse. - Il existe un schéma lisse et projectif sur $\underset{\sim}{F}_p$, $\tilde{X}_p$, et un morphisme $f : \tilde{X}_p \longrightarrow X_p$ tel que $R^i f_* \mathcal{O}_{\tilde{X}} = 0$ pour tout $i \geqslant 1$ et $f_* \mathcal{O}_{\tilde{X}} = \mathcal{O}_X$.

Cette hypothèse implique, d'après [17], que f induit un isomorphisme fonctoriel

$$H^N(\tilde{X}_p , \underset{\sim}{G}^{\wedge}_{m,\tilde{X}_p}) \simeq H^N(X_p , \underset{\sim}{G}^{\wedge}_{m,X_p}) .$$

6.4. La théorie du paragraphe 4 s'applique à $H^N(\tilde{X}_p , \underset{\sim}{G}^{\wedge}_{m,\tilde{X}_p})$. Soit $P_N(T)$ le facteur de la fonction zêta de $\tilde{X}_p/\underset{\sim}{F}_p$ qui correspond à H^N

$$P_N(T) = \det(1 - TF | H^N_{\mathrm{cris}}(\tilde{X}_p) \otimes \underset{\sim}{Q}) = 1 + a_1 T + pa_2 T^2 + \dots + p^{k-1} a_k T^k ,$$

avec $a_1 , \dots , a_k \in \underset{\sim}{Z}$. Alors l'opérateur $F + a_1 I + a_2 V + \dots + a_k V^{k-1}$ s'annule sur le module des courbes de $H^N(\tilde{X}_p , \underset{\sim}{G}^{\wedge}_{m,\tilde{X}_p})$ (n. b. $F = F_p$ et $V = V_p$). Ce module est isomorphe au module des courbes du groupe formel $H^N(X_p , \underset{\sim}{G}^{\wedge}_{m,X_p})$, et ce groupe formel sur $\underset{\sim}{F}_p$ est la réduction mod p du groupe formel $H^N(X , \underset{\sim}{G}^{\wedge}_{m,X})$ sur $\underset{\sim}{Z}$. Pour $H^N(X , \underset{\sim}{G}^{\wedge}_{m,X})$, on a une paramétrisation qui lui associe le logarithme $\lambda(\tau) = \sum n^{-1} \beta_n \tau^n$ avec

$$\beta_n = \begin{cases} \text{coefficient de } (T_0 \cdot \ldots \cdot T_N)^{n-1} \text{ dans } (G(T_0, \ldots, T_n))^{(n-1)/2} & \\ & \text{si } n \text{ est impair} \\ 0 & \text{si } n \text{ est pair .} \end{cases}$$

D'après (2.3), on a donc les congruences :

$$\beta_n + a_1 \beta_{n/p} + p\, a_2 \beta_{n/p^2} + \ldots + p^{k-1} a_k \beta_{n/p^k} \equiv 0 \bmod p^s \quad \text{si} \quad p^s | n .$$

Dans le cas d'une courbe elliptique, on retrouve les congruences d'Atkin-Swinnerton-Dyer [2].

6.5. Exemple (cf. [16]).

Prenons $N = 2$ et $G(T_0, T_1, T_2) = T_0 T_1 T_2 (T_0 + T_1)(T_1 + T_2)(T_2 + T_0)$. Les singularités de la surface X d'équation $S^2 = G(T_0, T_1, T_2)$ sont des singularités, $\tilde{X}$ est un surface K 3 . Pour chaque nombre premier $p \neq 2$ la réduction $f_p : \tilde{X}_p \to X_p \bmod p$ est encore une résolution des singularités de X_p , et l'hypothèse de (6.3) est satisfaite.

Le logarithme pour $H^2(X, \underset{\sim}{G}_{m,X}^{\wedge})$, fourni par le paragraphe 5, est

$$\lambda(\tau) = \sum n^{-1} \beta_n \tau^n$$

avec $\beta_n = 0$ si n est pair et

$$\beta_{2m+1} = (-1)^m \sum_k \binom{m}{k}^3 .$$

Dans [16], on a déterminé la fonction zêta de $\tilde{X}_p / \underset{\sim}{F}_p$: le facteur correspondant à H^2 est

$$P_2(T) = \begin{cases} (1 - pT)^{20} (1 - p^2 T^2) & \text{si } p \equiv 5, 7 \bmod 8 \\ (1 - pT)^{20} (1 + (2p - 4u_p^2) T + p^2 T^2) & \text{si } p \equiv 1, 3 \bmod 8 \end{cases}$$

avec u_p^2 donné par $p = u_p^2 + 2v_p^2$, $u_p, v_p \in \underset{\sim}{Z}$.

Les congruences qu'on déduit de la formule générale, se simplifient ici. On peut omettre le facteur $(1 - pT)^{20}$, et l'on obtient les congruences équivalentes suivantes : si $n \equiv 0 \bmod p^r$, on a

$$(**) \begin{cases} \beta_n + (2p - 4u_p^2) \beta_{n/p} + p^2 \beta_{n/p^2} \equiv 0 \bmod p^r & \text{si } p \equiv 1 \text{ ou } 3 \bmod 8 \\ \beta_n - p^2 \beta_{n/p^2} \equiv 0 \bmod p^r & \text{si } p \equiv 5 \text{ ou } 7 \bmod 8 . \end{cases}$$

(Cette dernière congruence équivaut à $\beta_n \equiv 0 \bmod p^r$ si $n \equiv 0 \bmod p^r$ et $p \equiv 5$ ou $7 \bmod 8$.)

Considérons la série de Dirichlet $L(s)$, donnée par le produit Eulérien

$$L(s) = \prod_{p \neq 2} (1 + \alpha_p\, p^{-s} + \varepsilon_p\, p^{2-2s})^{-1}$$

avec

$$\alpha_p = 0 \quad \text{et} \quad \varepsilon_p = -1 \qquad \text{si} \quad p \equiv 5 \text{ ou } 7 \bmod 8$$

$$\alpha_p = 2p - 4u_p^2 \quad \text{et} \quad \varepsilon_p = +1 \quad \text{si} \quad p \equiv 1 \text{ ou } 3 \bmod 8 \ .$$

Alors les congruences (**), **pour tous** n et tous p simultanément, sont équivalentes à

$$\sum_{n \geq 1} \beta_n\, n^{-s} \equiv L(s)$$

où $\equiv$ s'interprète comme congruence dans le groupe multiplicatif des séries de Dirichlet formelles $\{\sum_{n \geq 1} c_n\, n^{-s} \ ; \ c_n \in \mathbb{Z} \ , \ c_1 = 1\}$ modulo le sous-groupe $(\sum c_n\, n^{-s} \ ; \ c_n \in n\mathbb{Z}$ pour tout n , $c_1 = 1\}$.

Grâce au choix ci-dessus des facteurs Eulériens pour les nombres premiers congrus à 5 ou 7 mod 8 , $L(s)$ n'est autre que la fonction L de Hecke

$$L(s) = L(s \ , \ \chi) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s})^{-1}$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de $\mathbb{Z}[\sqrt{-2}]$ et le caractère χ est donné par $\chi((\sqrt{-2})) = 0$ et $\chi(\mathfrak{p}) = \pi^2$ avec π un générateur de $\mathfrak{p}$ si $\mathfrak{p} \neq (\sqrt{-2})$.

BIBLIOGRAPHIE

[1] ARTIN (M.) and MAZUR (B.). - Formal groups arising from algebraic varieties, Ann. scient. Ec. Norm. Sup., 4e série, t. 10, 1977, p. 87-132.

[2] ATKIN (A.) and SWINNERTON-DYER (H.). - Modular forms on non congruence subgroups, "Combinatorics", p. 1-25. - Providence, American mathematical Society, 1971 (Proceedings of Symposia in pure Mathematics, 29).

[3] BERTHELOT (P.) and OGUS (A.). - Notes on cristalline cohomology. - Princeton, Princeton University Press and University of Tokyo Press, 1978 (Mathematical Notes, 21).

[4] BLOCH (S.). - Algebraic K-theory and crystalline cohomology. - Paris, Presses universitaires de France, 1977 (Institut des hautes Etudes scientifiques, Publications mathématiques, 47, p. 187-268).

[5] CARTIER (P.). - Groupes formels associés aux anneaux de Witt généralisés, C. R. Acad. Sc. Paris, t. 265, 1967, série A, p. 49-52 ; Modules associés à un groupe formel commutatif. Courbes typiques, C. R. Acad. Sc. Paris, t. 265, 1967, série A, p. 129-132.

[6] CARTIER (P.). - Groupes formels, fonctions automorphes et fonctions zêta des courbes elliptiques, "Actes du Congrès International des Mathématiciens [1970. Nice]", vol. 2, p. 291-299. - Paris, Gauthier-Villars, 1971.

[7] DELIGNE (P.). - La conjecture de Weil,I. - Paris, Presses universitaires de France, 1973 (Institut des hautes Etudes scientifiques, Publications mathématiques, 43, p. 273-307).

[8] HAZEWINKEL (M.). - Formal groups and applications. - New York, San Francisco, London, Academic Press, 1978 (Pure and applied Mathematics. Academic Press, 78).

[9] HONDA (T.). - On the theory of commutative formal groups, J. of math. Soc. of Japan, t. 22, 1970, p. 213-246.

[10] ILLUSIE (L.). - Complexe de De Rham-Witt et cohomologie cristalline, Ann. scient. Ec. Norm. Sup., 4e série, t. 12, 1979, p. 501-661.

[11] ILLUSIE (L.). - Complexe de De Rham-Witt, "Journées de géométrie algébrique [1978. Rennes]", Astérisque, t. 63, 1979, p. 83-112.

[12] ILLUSIE (L.). - Finiteness, duality and Künneth theorems in the cohomology of the De Rham-Witt complex, "Algebraic geometry [1982. Tokyo/Kyoto]", p. 20-72. - Berlin, Heidelberg, New York, Springer-Verlag, 1983 (Lecture Notes in Mathematics, 1016).

[13] KATZ (N.) and MESSING (W.). - Some consequences of the Riemann hypothesis for varieties over finite fields, Invent. Math., t. 23, 1974, p. 73-77.

[14] KATZ (N.). - Slope filtration of F-crystals, "Journées de géométrie algébrique [1978. Rennes]", Astérisque, t. 63, 1979, p. 113-163.

[15] LAZARD (M.). - Commutative formal groups. - Berlin, Heidelberg, New York, Springer-Verlag, 1975 (Lecture Notes in Mathematics, 443).

[16] STIENSTRA (J.) and BEUKERS (F.). - On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces, Math. Annalen, t. 271, 1985, p. 269-304.

[17] STIENSTRA (J.). - Formal group laws arising from algebraic varieties (en préparation).

[18] TATE (J.). - The arithmetic of elliptic curves, Invent. Math., t. 23, 1974, p. 179-206.

[19] ZINK (T.). - Cartiertheorie kommutativer formaler Gruppen. - Leipzig, Teubner Verlagsgesellschaft, 1984 (Teubner Texte zur Mathematik, 68).