Pure and Applied Mathematics Quarterly
Volume 5, Number 1
(*Special Issue : In honor of
Jean-Pierre Serre, Part 2 of 2*)
495—506, 2009

Equivalence numérique, équivalence cohomologique, et théorie de Lefschetz des variétés abéliennes sur les corps finis

P. Deligne (rédigé par L. Clozel)*

A Jean-Pierre Serre, en témoignage de notre admiration

Abstract : We determine the group of automorphisms generated, in the endomorphisms of the cohomology of an Abelian variety on a finite field, by the Lefschetz operators and the complex multiplications.
Keywords : Algebraic geometry (Abelian varieties, tale cohomology) ; 14 F 20, 14 K 22

1. Soit k une clôture algébrique du corps $\mathbb{F}_p$ à p éléments. On désignera par ℓ un nombre premier différent de p. On fixe, sur k, un isomorphisme $\mathbb{Q}_\ell \cong \mathbb{Q}_\ell(1)$.

Soit A une variété abélienne sur k. On note Z, ou $Z(A)$, le groupe des cycles à coefficients rationnels sur A, gradué par la codimension :

$$Z = \bigoplus_i Z^i \,.$$

On dispose sur Z^i des relations d'équivalence numérique et d'équivalence cohomologique, pour la cohomologie étale à coefficients dans $\mathbb{Q}_\ell$. Deux cycles cohomologiquement équivalents sont numériquement équivalents.

Received January 8, 2008.
*Rédaction basée sur une note de Deligne et une lettre du 12 juillet 1997.

Soient A_j les facteurs simples de A, E_j le centre de $\mathrm{End}(A_j) \otimes \mathbb{Q}$ et F le composé, dans une clôture algébrique de $\mathbb{Q}$, des clôtures galoisiennes des E_j ; F est donc un corps totalement réel ou un corps CM. Si ℓ est un nombre premier, soit $D_\ell \subset \mathrm{Gal}(F/\mathbb{Q})$ un groupe de décomposition en ℓ ; soit $c \in \mathrm{Gal}(F/\mathbb{Q})$ la conjugaison complexe.

Théorème 1.— *Si $c \in D_\ell$, l'équivalence numérique et l'équivalence cohomologique, pour la cohomologie étale ℓ–adique, coïncident pour A.*

Un théorème moins précis, où la condition sur ℓ dépendait, pour une variété simple, du choix d'un corps maximal de multiplication complexe, était démontré dans [2].

Les remarques suivantes sont évidentes :

(a) A étant donnée, la condition du Théorème 1 est vérifiée, d'après le théorème de Cebotarev, pour un ensemble $\mathcal{L}$ de nombres premiers ℓ de densité (analytique ou naïve) non nulle.

(b) Si la condition du Théorème 1 est vérifiée pour A, elle l'est aussi pour les puissances A^n de A. Il existe donc un ensemble $\mathcal{L}$, de densité > 0, tel que la conclusion soit vraie pour toute puissance A^n. Ceci avait été remarqué par Milne [5].

Soit $H = \bigoplus_{i=0}^{2g} H^i(A, \mathbb{Q}_\ell) = \bigoplus_{i=0}^{2g} H^i$, où $g = \dim(A)$. Soit $D = \mathrm{End}(A) \otimes \mathbb{Q}$.

Le groupe $D^\times$ opère sur H_ℓ, ainsi que le groupe, isomorphe à $SL(2, \mathbb{Q})$, donné par la théorie de Lefschetz. Tous deux préservent les classes de cohomologie algébriques. Soit $G \subset GL(H)$ l'adhérence de Zariski du groupe engendré par $D^\times$ et $SL(2)$. Le point–clé de notre démonstration du Théorème 1 est une description de G, ou plutôt du groupe $G_{\overline{\mathbb{Q}}_\ell}$ sur $\overline{\mathbb{Q}_\ell}$ qui s'en déduit par extension des scalaires. Nous montrerons au § 4 comment cette description se ramène aux deux cas suivants.

Soient d'abord $\mathcal{E}$ une courbe elliptique supersingulière et $A = \mathcal{E}^n$. Le groupe $\mathrm{End}(A)^\times$ agissant sur $H \otimes \overline{\mathbb{Q}}_\ell = \Lambda^\bullet(H^1 \otimes \overline{\mathbb{Q}}_\ell)$ a pour adhérence de Zariski le groupe $GL(H^1 \otimes \overline{\mathbb{Q}}_\ell)$. Soit $V = H^1 \otimes \overline{\mathbb{Q}}_\ell$ et V^* son dual.

Théorème 2.— *Le groupe $G_{\overline{\mathbb{Q}}_\ell}$ est isomorphe au groupe $CSpin(V \oplus V^*)$ des similitudes spinorielles, $V \oplus V^*$ étant muni de la forme quadratique naturelle. Il opère sur $H \otimes \overline{\mathbb{Q}}_\ell = \bigoplus H^i(A, \overline{\mathbb{Q}}_\ell)$ par la somme de ses deux représentations demi–spinorielles. En particulier, la représentation sur les classes de degré pair (resp. impair) est irréductible.*

A l'opposé, soit A une variété irréductible telle que $\mathrm{End}(A) \otimes \mathbb{Q} = D$ soit une algèbre à division, de degré réduit n, sur un corps quadratique imaginaire E ; A est de dimension n.

Soit $c \in \mathrm{Gal}(E/\mathbb{Q})$ la conjugaison complexe, et choisissons un plongement j de E dans $\overline{\mathbb{Q}}_\ell$. La structure de E–module de $H_1(A, \overline{\mathbb{Q}}_\ell)$ fournit une décomposition $H_1 = H_1' \oplus H_1''$, où $\lambda \in E$ agit sur H_1' (resp. H_1'') par multiplication par $j(\lambda)$ (resp. $j(c\ \lambda)$). Soit $V = V_1 \oplus V_2$ la décomposition duale de $H^1(A, \overline{\mathbb{Q}}_\ell)$. L'adhérence de Zariski de $D^\times$ devient, sur $\overline{\mathbb{Q}}_\ell$, le groupe $GL(V_1) \times GL(V_2)$.

Munissons

$$H^\bullet(A, \overline{\mathbb{Q}}_\ell) = \bigoplus_{p,q} \Lambda^p\ V_1 \otimes \Lambda^q\ V_2$$

de la graduation donnée par $k := p - q$:

$$gr^k = \bigoplus_{p-q=k} \Lambda^p\ V_1 \otimes \Lambda^q\ V_2\,. \tag{1.1}$$

La partie de degré $(-n)$ est donc $\Lambda^0\, V_1 \otimes \Lambda^n\, V_2$, de dimension 1, et celle de degré $(-n+1)$ est $V_1 \otimes \Lambda^n\, V_2 \oplus \Lambda^0\, V_1 \otimes V^{n-1}\, V_2$, de dimension $2n$.

Théorème 3.—(i) *Pour un isomorphisme de $\bigoplus \Lambda^p\, V_1 \otimes \Lambda^q\, V_2$ avec $\Lambda^\bullet(gr^{-n+1})$, transformant gr^k en $\Lambda^{n+k} gr^{-n+1}$, $G_{\overline{\mathbb{Q}}_\ell}$ s'identifie au groupe engendré par $GL(gr^{-n+1})$ agissant sur $\Lambda^\bullet gr^{-n+1}$, et par les homothéties $x \longmapsto \lambda x$.*

(ii) *Les gr^k $(-n \leq k \leq n)$ sont donc des représentations irréductibles non isomorphes de G. Les sous–espaces gr^k et gr^ℓ sont orthogonaux pour le cup–produit si $k + \ell \neq 0$, et en dualité parfaite si $k + \ell = 0$.*

2. Montrons comment réduire le Théorème 1 (et même une variante un plus plus forte, cf. § 5) à l'analyse du groupe G.

(a) Soient Z_0 le $\mathbb{Q}$–sous–espace vectoriel de $H^\bullet(A, \mathbb{Q}_\ell)$ image de Z, et Z_1 le $\mathbb{Q}_\ell$–sous–espace vectoriel engendré par Z_0. Nous montrerons que la forme d'intersection est non dégénérée sur Z_1. Sa restriction (qui est rationnelle) à Z_0 a donc un noyau nul : elle est non dégénérée et induit une surjection de Z_1 dans $\mathrm{Hom}(Z_0, \mathbb{Q}_\ell)$. On a donc $\dim_{\mathbb{Q}_\ell}(Z_1) \geq \dim_{\mathbb{Q}}(Z_0)$, les éléments d'une base de Z_0 sont linéairement indépendants sur $\mathbb{Q}_\ell$, et $Z_0 \otimes \mathbb{Q}_\ell \cong Z_1$.

(b) On notera $\mathbb{Q}_\lambda$ une extension galoisienne finie assez grande de $\mathbb{Q}_\ell$. Il suffit alors de vérifier la non–dégénérescence de la forme d'intersection sur $Z_\lambda := Z_1 \underset{\mathbb{Q}_\ell}{\otimes} \mathbb{Q}_\lambda \subset H_\lambda := H^\bullet(A, \mathbb{Q}_\lambda)$.

(c) Soit L l'opérateur de Lefschetz, opérant sur H, déduit d'une polarisation sur A, et soit $\Lambda : H^i \longrightarrow H^{i-2}$ l'opérateur associé [4]. Les exponentielles des endomorphismes nilpotents L et Λ de H engendrent un sous–groupe S, isomorphe à $SL(2, \mathbb{Q})$. Soit G l'adhérence de Zariski, dans $GL(H)$, du sous–groupe engendré par S et par $(\mathrm{End}(A) \otimes \mathbb{Q})^\times$. Il préserve Z_1, donc Z_λ (le fait que Λ préserve les cycles algébriques est dû à Lieberman ; cf. [4]). Puisque G contient le groupe $\mathbb{G}_m$ correspondant à la graduation de $H^\bullet(A)$ (action de $(\mathbb{Q} \cdot 1)^\times \subset \mathrm{End}(A) \otimes \mathbb{Q}$), ainsi que celui qui correspond à la même graduation, décalée de $\dim(A)$ (matrices diagonales dans S), il contient les homothéties $x \longmapsto \lambda x$.

(d) Supposons que $\mathbb{Q}_\lambda$ est une extension galoisienne assez grande de $\mathbb{Q}_\ell$. On vérifiera que H_λ est une somme de représentations absolument irréductibles non isomorphes W de G, et que la forme d'intersection définit des accouplements non dégénérés sur $W \times W'$, $W \longmapsto W'$ étant une involution des facteurs. Supposons qu'il existe $\sigma \in \mathrm{Gal}(\mathbb{Q}_\lambda/\mathbb{Q}_\ell)$ échangeant les facteurs en dualité. Puisque Z_λ est stable par le groupe de Galois, la forme d'intersection est alors non dégénérée : ceci terminera la démonstration.

Soit E le centre de $\mathrm{End}(A) \otimes \mathbb{Q}$: E est un produit de corps CM E_i (on convient qu'un corps totalement réel est CM ...). Supposons que E a la propriété suivante, équivalente à l'hypothèse "$c \in D_\ell$" du Théorème 1 :

(2.1) **Il existe une extension galoisienne $\mathbb{Q}_\lambda$ de $\mathbb{Q}_\ell$ et $\sigma \in \mathrm{Gal}(\mathbb{Q}_\lambda/\mathbb{Q}_\ell)$ tels que, pour tout i et pour tout plongement $\tau : E_i \longrightarrow \mathbb{Q}_\ell$, on ait $\sigma\tau = \tau \circ c$, c étant la conjugaison complexe sur E_i.**

On vérifiera alors ci–dessous l'existence de σ échangeant W et W'. Sous cette hypothèse, donc, le Théorème 1 s'ensuit.

3. Voici quelques rappels d'algèbre linéaire, pour lesquels nous renvoyons à [3], basé sur [1]. Soit V un espace vectoriel sur un corps K (ici $\mathbb{Q}_\ell$, $\mathbb{Q}_\lambda$ ou $\overline{\mathbb{Q}}_\ell$), V^* son dual, et munissons $W = V \oplus V^*$ de la forme quadratique non dégénérée

$$Q(v+\lambda) = <\lambda, v> \qquad (v \in V,\ \lambda \in V^*)\,.$$

Soit C l'algèbre de Clifford associée, quotient de l'algèbre tensorielle $T(V \oplus V^*)$ par l'idéal engendré par les $x \cdot x - Q(x)$ ($x \in V \oplus V^*$). C'est une algèbre graduée par $\mathbb{Z}/2\mathbb{Z}$ [3] ; soit $C = C^+ \oplus C^-$ cette graduation. Faisons agir W sur l'algèbre extérieure $\Lambda^\bullet V$ de V par

$$\begin{aligned} &v \cdot x = v \wedge x \ (v \in V,\ x \in \Lambda^\bullet V) \\ &\lambda \cdot x = \lambda \perp x \ \ (\lambda \in V^*,\ x \in \Lambda^\bullet V) \end{aligned} \tag{3.1}$$

où $\lambda \perp x = i(\lambda)x$. La relation qui définit C est vérifiée, et (3.1) se prolonge donc en une structure de C–module

$$C \longrightarrow \mathrm{End}(\Lambda^\bullet V)\,. \tag{3.2}$$

Le morphisme (3.2) est un isomorphisme : voir [1], Thm. 2 ; ou remarquer que si $V = V' \oplus V''$, C est le produit tensoriel (au sens $\mathbb{Z}/2$–gradué) des algèbres analogues C' et C'' : on est donc ramené au cas, facile, où V est de rang 1. L'image de C^+ par (3.2) est l'algèbre des endomorphismes de $\Lambda^\bullet V$ respectant la $\mathbb{Z}/2$–graduation de $\Lambda^\bullet V$.

Le groupe $C^\times$ agit sur l'algèbre C par conjugaison. Le sous–groupe H qui normalise $W \subset C$ respecte la $\mathbb{Z}/2$–graduation de C, donc est formé d'éléments pairs ou impairs. Son action sur W définit $H \longrightarrow O(W)$, de noyau le centre de $C^\times$. Le sous–groupe $(C^+)^\times \cap H$ de $(C^+)^\times$ qui normalise W est le groupe des similitudes spinorielles $C\,\mathrm{Spin}(W)$. Il s'envoie sur $SO(W)$:

$$1 \longrightarrow \mathbb{G}_m \longrightarrow C\,\mathrm{Spin}(W) \longrightarrow SO(W) \longrightarrow 1\,.$$

Le groupe $C\,\mathrm{Spin}(W)$ est donc le groupe des automorphismes de $\Lambda^\bullet V$, respectant la $\mathbb{Z}/2$–graduation et le sous–espace W de $\mathrm{End}(\Lambda^\bullet V)$. Son algèbre de Lie est celle des endomorphismes pairs T de $\Lambda^\bullet V$ tels que, pour W identifié à un sous–espace de $\mathrm{End}(\Lambda^\bullet V)$, on ait $[T,W]\subset W$. La représentation $\Lambda^\bullet V$ de $C\,\mathrm{Spin}(W)$ est la somme des deux représentations semi–spinorielles.

Il est clair que $GL(V)$, agissant sur $\Lambda^\bullet V$, est un sous–groupe de $C\,\mathrm{Spin}(W)$. Il relève dans $C\,\mathrm{Spin}$ le sous–groupe de Levi de $SO(W)$, intersection des sous–groupes paraboliques opposés respectant les sous–espaces isotropes maximaux V et V^* de W.

Le sous–espace isotrope maximal $V^*\subset W\subset C$ et la droite $K\cdot 1$ de $\Lambda^\bullet V$ se déterminent mutuellement : V^* est le sous–espace de W annulant 1 et $K\cdot 1$ est le sous–espace de $\Lambda^\bullet V$ annulé par V^*. Par la même règle, V correspond à la droite $\Lambda^{\max}V$.

La même histoire se répète pour tout sous–espace isotrope maximal de W. Le cas qui nous intéresse est celui où $V=V_1\oplus V_2$, et où W est décomposé en la somme de deux sous–espaces isotropes maximaux par

$$W=(V_1\oplus V_2^*)\oplus(V_1^*\oplus V_2)\,.$$

L'annulateur de $V_1^*\oplus V_2$ est la droite $\Lambda^{\max}V_2\subset\Lambda^\bullet V$. Fixons–en un générateur Ω. L'inclusion dans W du sous–espace isotrope complémentaire $V_1\oplus V_2^*$ se prolonge en un morphisme d'algèbres

$$\Lambda^\bullet(V_1\oplus V_2^*)\longrightarrow C\,,$$

et

$$I:\Lambda^\bullet(V_1\oplus V_2^*)\longrightarrow\Lambda^\bullet V\,,\qquad \lambda\longmapsto\lambda\Omega \tag{3.3}$$

est un isomorphisme. Le super–crochet avec $x\in W$ stabilise $\Lambda^\bullet(V_1\oplus V_2^*)\subset C$ et induit une super–dérivation. Pour $x\in V_1^*\oplus V_2$, identifié au dual de $V_1\oplus V_2^*$, cette dérivation est le produit intérieur $x\perp$. Via l'isomorphisme I, l'action de $v\in V_1\oplus V_2^*\subset W$ devient donc un produit extérieur, et celle de $x\in V_1^*\oplus V_2\subset W$, qui annule Ω, devient un produit intérieur.

Le produit extérieur dans $\Lambda^\bullet(V_1\oplus V_2^*)$, transporté par I, définit un nouveau produit, noté $*$, sur $\Lambda^\bullet V$. Si on munit $\Lambda^\bullet(V_1\oplus V_2^*)$ de la graduation pour laquelle V_1 (resp.V_2^*) est de degré 1 (resp. -1), le produit est compatible avec la graduation. L'isomorphisme I la transporte en la graduation évidente de $\Lambda^\bullet V$, translatée par $\dim(V_2)$ pour placer Ω en degré 0. Le produit $*$ est donc compatible avec la graduation évidente translatée. La graduation naturelle de $\Lambda^\bullet(V_1 \oplus V_2^*)$ (pour laquelle V_2^* est de degré 1) est aussi compatible au produit. On obtient alors sur $\Lambda^\bullet V$ la graduation gr^k de (1.1), décalée de $\dim(V_2)$ ($1 \in \Lambda^\bullet V_2$, de degré 0 pour gr^k, est de degré $\dim(V_2)$).

Pour $v_1 \in V_1$, $v_2 \in V_2$, calculons $(v_1 \wedge v_2)\wedge : \Lambda^\bullet V \longrightarrow \Lambda^\bullet V$ à l'aide de l'isomorphisme (3.3) : on a le diagramme

$$\begin{array}{ccc} \Lambda^\bullet(V_1 \oplus V_2^*) & \xrightarrow[I]{} & \Lambda^\bullet V \\ \| & & \| \\ \Lambda^\bullet V_1 \otimes \Lambda^\bullet V_2^* & \longrightarrow & \Lambda^\bullet V_1 \otimes \Lambda^\bullet V_2 \end{array}$$

et l'application du bas est un produit tensoriel d'applications. Si $a \in \Lambda^\bullet V_1$, $b \in \Lambda^\bullet V_2$,

$$(v_1 \wedge v_2)(a \wedge b) = (-1)^{\deg a}(v_1 \wedge a) \wedge (v_2 \wedge b)\,.$$

Pour l'isomorphisme $\Lambda^\bullet V_2^* \longrightarrow \Lambda^\bullet V_2$ définissant I, $b \longmapsto v_2 \wedge b$ se transporte en $b^* \longmapsto v_2 \perp b^*$. On en déduit que $(v_1 \wedge v_2)\wedge$ se transporte en l'endomorphisme $v_1 \wedge v_2 \perp$ de $\Lambda^\bullet(V_1 \oplus V_2^*)$ dont on vérifie aussitôt que c'est une dérivation. Celle–ci respecte $V_1 \oplus V_2^*$.

4. Calculer le groupe G (du §1, et sur une extension assez grande de $\mathbb{Q}_\ell$) est amusant. Voici l'histoire.

(a) Soit E le centre de $D = \mathrm{End}(A) \otimes \mathbb{Q}$, produit de corps CM E_i ; D est centrale simple sur E.

(b) Après extension des scalaires de $\mathbb{Q}$ à $\mathbb{Q}_\lambda$ (assez grand), E devient une somme de copies de $\mathbb{Q}_\lambda$, indexée par l'ensemble Σ des morphismes de $\mathbb{Q}$–algèbres $E \longrightarrow \mathbb{Q}_\lambda$. Après extension des scalaires de $\mathbb{Q}_\ell$ à $\mathbb{Q}_\lambda$, $H^1(A)$ devient $\bigoplus H_\sigma$ ($\sigma \in \Sigma$), où

$$H_\sigma = \{\alpha \in H^1(A, \mathbb{Q}_\lambda) : [z]\alpha = \sigma(z)\alpha \ (z \in E)\}\,,$$

$[z]$ désignant l'action de E sur $H^1(A)$ déduite de son action sur A. L'algèbre $D \otimes \mathbb{Q}_\lambda$ est $\prod\limits_\sigma \mathrm{End}(H_\sigma)$.

Le groupe G, qui agit sur $\Lambda^\bullet\big(\bigoplus\limits_\sigma H_\sigma\big)$, est engendré par le produit des $GL(H_\sigma)$ et par un $SL(2)$ “diagonal”. Soit $L : H^i(A, \mathbb{Q}_\lambda) \longrightarrow H^{i+2}(A, \mathbb{Q}_\lambda)$ l'opérateur de Lefschetz, que l'on identifie à une classe de cohomologie dans $H^2(A, \mathbb{Q}_\lambda) =$

$\Lambda^2(\bigoplus H_\sigma)$; le Lemme 2.1 de [2] implique que

$$L = \sum_v L_v$$

où v parcourt l'ensemble quotient $\Sigma/\{1, c\}$, la conjugaison complexe opérant sur Σ par son action sur E, et où

$$L_v \in \Lambda^2(H_\sigma \oplus H_{c\sigma})$$

pour $v = \{\sigma, c\sigma\}$. (σ peut être fixé par c, auquel cas $L_v \in \Lambda^2 H_\sigma$). Chaque L_v est dans l'adhérence de l'orbite de L sous $\Pi GL(H_\sigma)$ et donc dans l'algèbre de Lie de G.

Les mêmes arguments donnent une décomposition analogue de l'opérateur Λ ; les relations de commutation sont préservées par les composantes L_v et Λ_v. Par conséquent, G est aussi engendré par le produit des $GL(H_\sigma)$ et d'une copie de $SL(2)$ définie sur $\mathbb{Q}_\lambda$ pour chaque orbite de c dans Σ. Ainsi G est un produit agissant sur un produit tensoriel.

(c) Histoire pour $\{\sigma\}$, $\sigma = c\sigma$.

Ceci correspond à un éventuel facteur $\mathbb{Q}$ de E, donc à un facteur isogène à $B = \mathcal{E}^n$ de A, où $\mathcal{E}$ est une courbe elliptique supersingulière sur k.

Soit $V = H_\sigma = H^1(B, \mathbb{Q}_\lambda)$, espace de dimension paire. Soit $W = V \oplus V^*$. La classe de Lefschetz $L \in \Lambda^2 V$ est un isomorphisme de V vers V^*. On va montrer que le groupe engendré par $GL(V)$ et le sous–groupe $SL(2)$ associé à L est $C\,\mathrm{Spin}(W)$ dans sa représentation spinorielle sur $H^\bullet(B) = \Lambda^\bullet V$.

On vérifie aussitôt que, pour son action sur $\Lambda^2 V$ par multiplication à gauche, L vérifie

$$[L, W] \subset W\,.$$

Par conséquent, L est un élément de Lie $(C\,\mathrm{Spin}(W))$; celui–ci appartient à l'algèbre de Lie du radical unipotent N du sous–groupe de Levi défini par $W = V \oplus V^*$ (§ 3) et en est un élément non–singulier. Les conjugués par $GL(V)$ de l'exponentielle de L engendrent donc N. De même, Λ et ses conjugués engendrent l'algèbre de Lie du sous–groupe unipotent opposé. Par conséquent, le groupe engendré par $GL(V)$ et $SL(2)$ contient le groupe de Spin ; on a déjà vu qu'il contenait les homothéties (§ 2, (c)). Son adhérence de Zariski, sur $\overline{\mathbb{Q}}_\ell$, est donc $\mathrm{CSpin}(V \oplus V^*)$, ce qui démontre le Théorème 2.

(d) Histoire pour $\{\sigma, c\sigma\}$, $\sigma \neq c\sigma$.

Dans ce cas $H_v = H_\sigma \oplus H_{c\sigma} = V_1 \oplus V_2$ et $(\mathrm{End}(A) \otimes \mathbb{Q}_\lambda)^\times$ opère sur H_v par $GL(V_1) \times GL(V_2)$.

Ecrivons, selon le §3 :

$$\Lambda^\bullet(V_1 \oplus V_2) \xrightarrow[I^{-1}]{\approx} \Lambda^\bullet(V_1 \oplus V_2^*)\,.$$

On munit $\Lambda^\bullet(V_1 \oplus V_2)$ du produit $*$, qui devient par I^{-1} le produit extérieur à droite. On peut écrire ([2, Lemme 2.1]) :

$$L = \sum\ e_i \wedge f_i \in \Lambda^2(V_1 \oplus V_2)$$

avec $e_i \in V_1,\ f_i \in V_2$. L'isomorphisme I^{-1} échange l'action de L sur $\Lambda^\bullet(V_1 \oplus V_2)$ et l'action sur le membre de droite donnée par

$$\sum e_i \wedge f_i \perp .$$

Celle–ci est une dérivation (§3) ; en fait, dans les bases de V_1 et V_2^* données par (e_i, f_i^*), c'est la somme des endomorphismes

$$x = \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix} \in \mathfrak{sl}(2)$$

de k^2, donc l'endomorphisme de k^{2n} correspondant étendu (comme action d'algèbre de Lie) à $\Lambda^\bullet(V_1 \oplus V_2^*) = \Lambda^\bullet(k^{2n})$. L'action de L sur $\Lambda^\bullet(V_1 \oplus V_2)$ laisse donc invariant (au sens des algèbres de Lie) le produit $*$, c'est donc une dérivation.

Par ailleurs l'élément $h = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ de $\mathfrak{sl}(2)$ opère sur $\Lambda^i V$ par $i - n = gr_1(\Lambda^i V)$ où gr_1 est la graduation naturelle translatée (§ 3). Celle–ci étant compatible au produit $*$, celui–ci est invariant par la sous–algèbre de Borel de $\mathfrak{sl}(2)$. Or dans une représentation de $\mathfrak{sl}(2)$, un vecteur annulé par une sous–algèbre de Borel l'est par $\mathfrak{sl}(2)$. On en déduit que $*$ est invariant par $SL(2)$.

Considérons la décomposition de $\Lambda^\bullet V$ donnée par (1.1) :

$$gr^k \Lambda^\bullet V = \bigoplus_{p-q=k} \Lambda^p V_1 \otimes \Lambda^q V_2\,.$$

Noter que cette décomposition est invariante par L et Λ. En effet, E (par son plongement dans $\mathbb{Q}_\lambda$) opère sur $\Lambda^\bullet V$. Soit $U(1)$ le groupe $\{\lambda \in E : N_{E/F}\lambda = 1\}$ où F est la sous-algèbre de E formée des points fixes de c. Si $\lambda \in U(1)$, λ opère sur

gr^k par le scalaire $\lambda^{p-q}(\in \mathbb{Q}_\lambda)$; il comute à L et Λ, et les λ^{p-q} sont des caractères distincts de $U(1)$. Résumons :

LEMME 4.1.— *On munit $\Lambda^\bullet V$ du produit $*$, et de la graduation* (1.1).

(i) *$\Lambda^\bullet V$ est engendré par*

$$gr^{1-n} = V_1 \otimes \Lambda^n V_2 \oplus \Lambda^0 V_1 \otimes \Lambda^{n-1} V_2 \,.$$

(ii) *Le produit $* : gr^i \times gr^j \longrightarrow gr^{i+j}$ est invariant par $SL(2)$, $SL(V_1)$ et $SL(V_2)$.*

(iii) *La graduation de $\Lambda^\bullet V$ est préservée par G.*

L'image de G dans $GL(gr^{n-1})$ contient $GL(V_1)$, $GL(V_2) \cong GL(\Lambda^{n-1}V_2)$ ainsi qu'un isomorphisme $\Lambda^0 V_1 \otimes \Lambda^n V_2 \longrightarrow V_1 \otimes \Lambda^n V_2$ (donné par L) et un isomorphisme inverse (donné par Λ). C'est donc $GL(gr^{n-1})$. La propriété (i) identifie $\Lambda^\bullet V$ à $\Lambda^\bullet(gr^{n-1})$, de façon compatible à l'action de $SL(2) \times SL(V_1) \times SL(V_2)$. Le groupe engendré par $\{zs_1, z^{-1}s_2\}$, où z est un scalaire et $s_i \in SL(V_i)$, dans $GL(V_1) \times GL(V_2)$ opère sur $\Lambda^\bullet V$ par l'action de $GL(gr^{1-n})$ décrite par le Théorème 3. Le groupe G est donc engendré par $GL(gr^{1-n})$, isomorphe à $GL(2n)$, et par un tore de dimension 1, qui opère par homothéties globales sur $\Lambda^\bullet V$, d'où le Théorème 3 (i). Il est clair que, déjà pour l'action de $GL(gr^{1-n})$, les représentations obtenues sont absolument irréductibles et non isomorphes ; enfin, si $k + \ell \neq 0$, les espaces gr^k et gr^ℓ ne sont pas des représentations duales, même pour l'action de $GL(2n) \subset G$. Le cup–produit étant non dégénéré, gr^k et gr^ℓ sont donc en dualité parfaite.

5. Une fois acquise la description de G, voici la démonstration du Théorème 1. Ecrivons

$$H_\lambda = H^\bullet(A, \mathbb{Q}_\lambda) = \bigotimes_{v \in \Sigma/c} H_v^\bullet$$

où $H_v^\bullet$ est comme dans le § 4. On suppose $\mathbb{Q}_\lambda$ assez grand, et galoisien sur $\mathbb{Q}_\ell$. Sous l'action du produit (désormais noté G) des groupes décrits dans le § 4, H_λ se décompose comme somme directe indexée par les fonctions $\sigma \longmapsto k(\sigma)$ $(\sigma \in \Sigma)$ où

(5.1) $$k(\sigma) \in \mathbb{Z} \quad \text{si} \quad \sigma \neq \sigma c\,; \ \text{alors } k(\sigma c) = -k(\sigma)$$

(5.2) $$k(\sigma) \in \mathbb{Z}/2\mathbb{Z} \quad \text{si} \quad \sigma = \sigma c \ \ (\text{facteur supersingulier éventuel})\,.$$

Dans (5.1), $k(\sigma)$ est donné par le Théorème 3, étendu, comme dans le § 4, au cas où E est CM plutôt que quadratique imaginaire. On remarquera que si on change σ en σc, les espaces V_1 et V_2 du § 4 sont échangés, d'où la relation (5.1).

Soit $\mathcal{K}$ le groupe des fonctions vérifiant (5.1) et (5.2). Puisque l'espace vectoriel sur $\mathbb{Q}_\lambda$ engendré par les cycles algébriques est stable par G ainsi que par cup–produit, il correspond à un sous–monoïde $\mathcal{A}lg$ de $\mathcal{K}$. De plus,

$$\mathcal{A}lg \subset \mathcal{K}_0 = \{k : \sum_{\sigma \mod c} k(\sigma) \text{ pair}\} \tag{5.3}$$

$$\begin{aligned} &H_\lambda(k) \text{ est orthogonal à } H_\lambda(\ell) \text{ si } k + \ell \neq 0\,; \\ &H_\lambda(k) \text{ et } H_\lambda(-k) \text{ sont en dualité} \end{aligned} \tag{5.4}$$

$$\mathcal{A}lg \text{ est stable par } \mathrm{Gal}(\mathbb{Q}_\lambda/\mathbb{Q}_\ell)\,. \tag{5.5}$$

Supposons que le groupe de Galois contient un élément agissant comme (-1) sur $\mathcal{K}$. Alors, sur tout sous–espace $\mathbb{Q}_\ell$–rationnel de H_λ, invariant par G, la dualité donnée par la forme d'intersection est non dégénérée. C'est en particulier le cas si (avec les notations du § 1) la conjugaison complexe $c \in \mathrm{Gal}(E/\mathbb{Q})$ appartient au groupe de décomposition de ℓ, d'où le Théorème 1.

Un peu moins suffit : pour que tout sous–monoïde stable soit un sous–groupe de $\mathcal{K}$ (donc que l'espace des cycles algébriques contienne, avec l'espace associé à k, son dual associé à $-k$), il suffit que $\mathcal{K} \otimes \mathbb{Q}$ n'admette pas de droite fixe sous l'action de $\mathrm{Gal}(\mathbb{Q}_\lambda/\mathbb{Q}_\ell)$. En d'autres termes, si ℓ est non ramifié dans les facteurs de E, il suffit que Frob_ℓ agissant sur Σ vérifie :

Pour tout $\sigma \in \Sigma$, il existe $a \in \mathbb{Z} : \mathbf{Frob}_\ell^a(\sigma) = \sigma c$.

Références

[1] N. Bourbaki, *Algèbres de Clifford,* in *Algèbre*, livre II, Ch. IX, § 9, Hermann, Paris 1959.

[2] L. Clozel, *Equivalence numérique et équivalence cohomologique pour les variétés abéliennes sur les corps finis,* **Ann. Math. 150** (1999), 151–163.

[3] P. Deligne, *Clifford modules,* in *Quantum Fields and Strings, A course for Mathematicians,* Deligne et al. eds., vol. I, AMS/IAS 1999, 107–112.

[4] S.L. Kleiman, *Algebraic cycles and the Weil conjectures,* in *Dix exposés sur la cohomologie des schémas*, North–Holland, Amsterdam, Paris, 1968, 359–386.

[5] J.S. Milne, *The Tate conjecture for certain Abelian varieties over finite fields,* **Acta Arith. 100** (2001), 135–166.

Pierre Deligne
School of Mathematics, Institute for Advanced Study
Princeton NJ 08540 (USA)
E-mail : deligne@math.ias.edu

Laurent Clozel
Mathématiques, Bat. 425, Université Paris-Sud, 91405 Orsay Cedex, France
E-mail : Laurent.Clozel@math.u-psud.fr