

La conjecture de Weil pour les surfaces $K3$

Pierre Deligne* (Bures-sur-Yvette)

1. Énoncé du théorème

Soient $\mathbb{F}_q$ un corps à q éléments, $\overline{\mathbb{F}}_q$ une clôture algébrique de $\mathbb{F}_q$, $\varphi \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ la substitution de Frobenius $x \mapsto x^q$, et $F = \varphi^{-1}$ le «Frobenius géométrique».

Soit X un schéma (séparé de type fini) sur $\mathbb{F}_q$, et soit $\overline{X}$ le schéma sur $\overline{\mathbb{F}}_q$ qui s'en déduit par extension des scalaires. Pour tout point fermé x de X , soit $\deg(x) = [k(x) : \mathbb{F}_q]$ le degré sur $\mathbb{F}_q$ de l'extension résiduelle. La fonction zêta $Z(X, t) \in \mathbb{Z}[[t]]$ est définie par

$$Z(X, t) = \prod_{x \in X} (1 - t^{\deg(x)})^{-1} \quad (x \text{ point fermé de } X),$$

$$\log Z(X, t) = \sum_{n>0} \#X(\mathbb{F}_{q^n}) \frac{t^n}{n}.$$

Pour tout nombre premier ℓ premier à q , la cohomologie ℓ -adique à supports propres $H_c^i(\overline{X}, \mathbb{Q}_\ell)$ de $\overline{X}$ est un espace vectoriel de dimension finie sur $\mathbb{Q}_\ell$, sur lequel $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ agit par transport de structures. D'après Grothendieck, on a

$$Z(X, t) = \prod_i \det(1 - Ft, H_c^i(\overline{X}, \mathbb{Q}_\ell))^{(-1)^{i+1}}.$$

Prenons pour X une surface projective non singulière. On sait dans ce cas que les facteurs

$$P_i(t) = \det(1 - Ft, H^i(\overline{X}, \mathbb{Q}_\ell))$$

de $Z(X, t)$ sont des polynômes à coefficients entiers rationnels indépendants de ℓ . La conjecture de Weil affirme ici que les racines du polynôme $P_i(t)$ sont de valeur absolue complexe $q^{-i/2}$. Cette conjecture est invariante par extension finie du corps fini de base. Pour X comme plus haut, et $i \neq 2$, elle résulte de Weil [9]. Si, pour simplifier, on suppose X géométriquement connexe, on a en effet

$$P_0(t) = 1 - t, \quad P_4(t) = 1 - q^2 t,$$

$$P_1(t) = \det(1 - \varphi t; T_\ell(\text{Pic}^0(X)_{\text{red}})), \quad P_3(t) = P_1(qt).$$

*Cet article a été rédigé pendant un séjour à l'Université de Warwick, que je remercie de son hospitalité.

Soient k un corps de caractéristique 0 et X une surface projective non singulière géométriquement connexe sur k . On dit que X est une surface $K3$ si X est régulière et de diviseur canonique trivial, c'est-à-dire si $H^1(X, \mathcal{O}) = 0$ et que Ω_X^2 est isomorphe à $\mathcal{O}_X$. Pour les mirifiques propriétés de ces surfaces, on renvoie à [8]. Nous utiliserons surtout les faits suivants.

1.1. Lemme. (i) On a $h^{2,0} = h^{0,2} = 1$.

(i) On a $H^2(X, T_X^1) = 0$ (les déformations infinitésimales ne sont pas obstruées), l'application déduite du produit intérieur

$$H^1(X, T_X^1) \otimes H^0(X, \Omega_X^2) \xrightarrow{\sim} H^1(X, \Omega_X^1) \quad (1.1.1)$$

est bijective, et $H^0(X, T_X^1) = 0$ (X n'a pas d'automorphismes infinitésimaux).

On a

$$h^{2,0} =_{\text{dfn}} \dim H^0(X, \Omega_X^2) = \dim H^0(X, \mathcal{O}_X) = 1,$$

et (i) s'en déduit par symétrie de Hodge. Puisque $H^1(X, \mathcal{O}_X) = 0$, on a par symétrie de Hodge et dualité de Serre

$$h^{0,1} = h^{1,0} = h^{2,1} = h^{1,2} = 0.$$

Puisque $\Omega_X^2 = \mathcal{O}_X$, l'isomorphisme «produit intérieur»

$$T_X^1 \otimes \Omega_X^2 \xrightarrow{\sim} \Omega_X^1$$

induit des isomorphismes $T_X^1 \simeq \Omega_X^1$. La nullité de $H^2(X, T_X^1)$ se déduit donc de celle de $h^{1,2}$, et il est clair que (1.1.1) est bijectif. Le même argument donne $H^0(X, T_X^1) = 0$.

1.2. Lemme. Soit Y_0 une surface projective non singulière sur un corps fini $\mathbb{F}_q$. Les conditions suivantes sont équivalentes.

- (i) Il existe un anneau de valuation discrète complet d'inégale caractéristique V de corps résiduel fini k , un morphisme propre et lisse $f_V : Y \rightarrow \text{Spec}(V)$ de fibre générale une surface $K3$ et $i : \mathbb{F}_q \rightarrow k$ tel que $Y_0 \otimes_{\mathbb{F}_q} k \simeq Y \otimes_V k$.
- (ii) Il existe un schéma intègre S de corps des fractions de caractéristique 0, un point $s \in S$, un morphisme propre et lisse $f : Y \rightarrow S$ de fibre générale une surface $K3$ et $i : \mathbb{F}_q \rightarrow k(s)$ tel que $Y_0 \otimes_{\mathbb{F}_q} k(s) \simeq Y_s$.

La démonstration utilise un passage à la limite standard. Si les conditions équivalentes de 1.2 sont remplies, on dit que Y_0 se relève en une surface $K3$.

1.3. Théorème. Une surface projective non singulière sur un corps fini $\mathbb{F}_q$ qui se relève en une surface $K3$ vérifie la conjecture de Weil.

Ce théorème a été obtenu indépendamment par Pjateckii-Shapiro et Šafarevitch.

Il s'applique par exemple aux surfaces de degré 4 dans $\mathbb{P}^3$. Les nombres de Betti d'une surface $K3$ sont $(1, 0, 22, 0, 1)$; le théorème implique

donc que

$$|\#X(\mathbb{F}_q) - \#\mathbb{P}^2(\mathbb{F}_q)| \leq 21q.$$

La théorie conjecturale des motifs de Grothendieck (en particulier sa théorie du «groupe de Galois motivique») m'a été très utile pour construire la démonstration. Dans ce langage (qui ne sera pas utilisé par la suite), l'idée est, en gros, de construire par réduction de $\mathbb{C}$ à $\mathbb{F}_q$ une variété abélienne A et un «morphisme» injectif de motifs

$$H^2(X) \hookrightarrow H^1(A) \otimes H^1(A),$$

pour déduire la conjecture de Weil pour X du théorème de Weil pour A . Toutefois, nous ne définissons pas ce «morphisme» par un cycle algébrique; ce n'est donc pas un morphisme au sens de [5]. En théorie de Hodge, son mode de définition a l'analogue suivant (qui ne sera pas utilisé par la suite).

1.4. Lemme. *Soit H une variation de structures de Hodge de poids n sur un schéma S . Si le système local $H_{\mathbb{Z}}$ n'a pour sections globales que la section s et ses multiples, alors s est en tout point de S de type $(n/2, n/2)$.*

1.5. Notations. 1.5.1. On notera en indice les extensions de scalaires: si M_A est un module sur un anneau (commutatif à unité) A (ou un schéma sur A , par exemple un groupe algébrique sur A), on désignera par M_B le module sur la A -algèbre B (ou le schéma sur B) qui s'en déduit par extension des scalaires.

1.5.2. Si un groupe G agit sur un ensemble X , on notera $g * x$ le transformé de x par g .

1.5.3. Quand une égalité est la définition de l'un des membres, on la note $=_{\text{dfn}}$.

2. Structures de Hodge polarisées

Pour manier les structures de Hodge, nous utiliserons le formalisme exposé dans [4] et brièvement rappelé ci-dessous.

2.1. Soient $\underline{S}$ le groupe algébrique réel des éléments inversibles de la $\mathbb{R}$ -algèbre $\mathbb{C}$, $w : \mathbb{G}_{m_{\mathbb{R}}} \rightarrow \underline{S}$ l'inclusion de $\mathbb{R}^*$ dans $\mathbb{C}^*$ et $t : \underline{S} \rightarrow \mathbb{G}_{m_{\mathbb{R}}}$ l'inverse de la norme; on a $tw(x) = x^{-2}$. Soit V un vectoriel réel de dimension finie. Il revient au même de se donner

a) $\rho : \underline{S} \rightarrow \text{GL}(V)$ de poids n : $\rho w(x) * v = x^n \cdot v$;

b) une bigraduation de Hodge de poids n de $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$:

$$V_{\mathbb{C}} = \bigoplus_{p+q=n} V^{p,q} \quad \text{avec} \quad \overline{V^{p,q}} = V^{q,p};$$

c) une filtration de Hodge de poids n de $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$: c'est une filtration décroissante avec

$$F^p(V_{\mathbb{C}}) \oplus \overline{F^{n-p+1}(V_{\mathbb{C}})} \xrightarrow{\sim} V_{\mathbb{C}}.$$

On a

$$F^p(V_{\mathbb{C}}) = \bigoplus_{p' \geq p} V^{p', q'};$$

pour $z \in \underline{S}(\mathbb{R}) = \mathbb{C}^*$ et $v^{p,q} \in V^{p,q}$, on a

$$z * v^{p,q} = z^p \bar{z}^q v^{p,q}.$$

On pose $C = \rho(i)$; c'est l'opérateur C de Weil. On a $Cv^{p,q} = i^{p-q}v^{p,q}$. Pour $\mathcal{E}$ une partie de $\mathbb{Z} \times \mathbb{Z}$, une bigraduation de Hodge est dite de type $\mathcal{E}$ si les nombres de Hodge $h^{p,q} = \dim V^{p,q}$ sont nuls pour $(p,q) \notin \mathcal{E}$.

2.2. On appellera ici *structure de Hodge de poids n* H la donnée d'un $\mathbb{Z}$ -module libre de type fini $H_{\mathbb{Z}}$ et d'une bigraduation de Hodge de poids n de $H_{\mathbb{C}} = H_{\mathbb{Z}} \otimes \mathbb{C}$. La *structure de Hodge de Tate* $\mathbb{Z}(n)$ est la structure de Hodge de type $\{(-n, -n)\}$ donnée par

$$\mathbb{Z}(n)_{\mathbb{C}} = \mathbb{C} \quad \text{et} \quad \mathbb{Z}(n)_{\mathbb{Z}} = (2\pi i)^n \mathbb{Z} \subset \mathbb{C}.$$

Une polarisation d'une structure de Hodge de poids n H est un morphisme de structures de Hodge

$$\psi : H \otimes H \longrightarrow \mathbb{Z}(-n)$$

telle que, sur $H_{\mathbb{R}} = H_{\mathbb{Z}} \otimes \mathbb{R}$, la forme bilinéaire réelle

$$(2\pi i)^n \psi(x, Cy)$$

soit symétrique et définie positive. La forme ψ est alors $(-1)^n$ -symétrique.

Une *structure de Hodge de poids n rationnelle* consiste en un $\mathbb{Q}$ -vectoriel $H_{\mathbb{Q}}$ et une bigraduation de Hodge de poids n de $H_{\mathbb{C}} = H_{\mathbb{Q}} \otimes \mathbb{C}$. On désigne par $\mathbb{Q}(n)$ la structure de Hodge rationnelle sous-jacente à $\mathbb{Z}(n)$. La définition des polarisations est laissée au lecteur.

L'énoncé suivant reformule un théorème de Riemann.

2.3. Scholie. *Le foncteur $A \mapsto H^1(A, \mathbb{Z})$ identifie les variétés abéliennes polarisées aux structures de Hodge polarisées de type $\{(0, 1), (1, 0)\}$.*

De la fin de ce n^o, nous n'utiliserons que 2.11(iii') $\Rightarrow$ (ii). Pour prouver cette implication, on peut se limiter à ne considérer que des groupes connexes, ce qui rend 2.5 inutile ou évident.

2.4. Soit G un groupe algébrique linéaire réel. On dit que G est *compact* si $G(\mathbb{R})$ est compact et que toute composante connexe de $G(\mathbb{C})$ a un point réel. Le foncteur évident est alors une équivalence de la catégorie des représentations linéaires algébriques de G avec la catégorie des représentations linéaires du groupe compact $G(\mathbb{R})$.

2.5. Lemme. *Tout sous-groupe algébrique réel H d'un groupe algébrique réel compact G est compact.*

On sait que l'application

$$(g, \ell) \longmapsto g \cdot \exp(i\ell) : G(\mathbb{R}) \times \text{Lie}(G) \longrightarrow G(\mathbb{C})$$

est bijective. Il suffit de prouver que, pour tout sous-groupe réel H de G et tout $h = g \cdot \exp(i\ell) \in H(\mathbb{C})$, on a $\ell \in \text{Lie}(H)$. Puisque $\bar{h} \in H(\mathbb{C})$, on a

$$\exp(2i\ell) = \bar{h}^{-1}h \in H(\mathbb{C}).$$

Regardons $G(\mathbb{C})$ comme l'ensemble des points réels d'un groupe algébrique réel. Soit $\bar{J} \subset H(\mathbb{C})$ l'adhérence de Zariski, dans ce groupe, de $J = \{\exp(ni\ell) \mid n \in 2\mathbb{Z}\}$. Les $g \in J$, donc les $g \in \bar{J}$, vérifient $g^{-1} = \bar{g}$, d'où $\text{Lie}(\bar{J}) \subset i \text{Lie}(G)$. L'algèbre de Lie $\text{Lie}(\bar{J})$ est abélienne, et $\exp(\text{Lie}(\bar{J}))$ est un groupe, nécessairement d'indice fini dans $\bar{J}$. Il existe donc n et $\ell' \in \text{Lie}(\bar{J})$ tel que

$$\exp(ni\ell) = \exp(\ell').$$

On a alors $i\ell \in \text{Lie}(\bar{J}) \subset \text{Lie}(H)$ et $\ell \in \text{Lie}(H)$, ce qui achève la démonstration.

2.6. Lemme. *Soit G un groupe algébrique réel. Les conditions suivantes sont équivalentes:*

- (i) G est compact;
- (ii) pour toute représentation linéaire réelle (resp. complexe) de G , il existe une forme bilinéaire (resp. sesquilineaire) symétrique (resp. hermitienne) définie positive et G -invariante;
- (iii) pour une représentation fidèle de G , il existe une forme comme en (ii).

Pour G connexe, ces conditions équivalent encore à

- (iii') pour une représentation de G , de noyau fini, il existe une forme comme en (ii).

Pour G compact, la G -invariance équivaut à la $G(\mathbb{R})$ -invariance et (ii) est classique. Si (iii) est vérifié, G est sous-groupe d'un groupe orthogonal ou unitaire, et on applique 2.5. La condition (iii') implique que $G(\mathbb{R})$ est compact (comme revêtement fini d'un groupe compact); si G est connexe, G est donc compact.

2.7. Soit G un groupe algébrique linéaire réel. Pour tout automorphisme involutif σ de G , soit $G^{(\sigma)}$ la forme réelle de $G_{\mathbb{C}}$ définie par l'involution antilinéaire $g \mapsto \sigma(\bar{g})$. On dit que σ est une *involution de Cartan* si $G^{(\sigma)}$ est compact.

Soit C un élément de $G(\mathbb{R})$ de carré central. Une représentation réelle (resp. complexe) de G sera dite C -polarisable s'il existe sur V une forme bilinéaire (resp. sesquilineaire) G -invariante ψ telle que la forme $\psi(x, Cy)$ soit symétrique (resp. hermitienne) et définie positive. On dit alors que ψ est une C -polarisation de V . Un cas particulier du lemme suivant est énoncé sans démonstration dans [4].

2.8. Lemme. *a) Que ψ soit une C -polarisation de V ne dépend que de la classe de $G(\mathbb{R})$ -conjugaison de C .*

b) Les conditions suivantes sont équivalentes:

- (i) $\text{ad } C$ est une involution de Cartan de G ;
- (ii) toute représentation réelle (resp. complexe) de G est C -polarisable;
- (iii) G admet une représentation réelle (resp. complexe) C -polarisable fidèle.

Si G est connexe, ces conditions équivalent encore à

- (iii') G admet une représentation réelle (resp. complexe) C -polarisable de noyau fini.

Pour prouver a), on note que $\psi(x, gCg^{-1}y) = \psi(g^{-1}x, Cg^{-1}y)$. Une forme sesquilinéaire ψ sur une représentation complexe de G est G -invariante si et seulement si

$$\psi(gx, \bar{g}y) = \psi(x, y) \quad \text{pour } g \in G(\mathbb{C}).$$

Cette condition équivaut à

$$\psi(gx, CC^{-1}\bar{g}Cy) = \psi(x, Cy) \quad \text{pour } g \in G(\mathbb{C})$$

(remplacer y par Cy), i.e. à la $G^{(\text{ad } C)}$ -invariance de $\psi(x, Cy)$. La forme $\text{resp}^{\text{ée}}$ de 2.8 résulte donc de 2.6. La forme non $\text{resp}^{\text{ée}}$ s'en déduit:

- a) la complexifiée (resp. réellifiée) d'une représentation réelle (resp. complexe) C -polarisable est C -polarisable;
- b) une polarisation de V induit une polarisation de toute sous-représentation de V ;
- c) pour V réel (resp. complexe), on a $V \hookrightarrow V \otimes_{\mathbb{R}} \mathbb{C}$.

2.9. Soient G un groupe réductif sur $\mathbb{Q}$, et t et w des morphismes définis sur $\mathbb{Q}$

$$\mathbb{G}_m \xrightarrow{w} G \xrightarrow{t} \mathbb{G}_m,$$

avec $tw(x) = x^{-2}$ et w central. Soit de plus un diagramme commutatif

$$\begin{array}{ccccc} \mathbb{G}_{m,\mathbb{R}} & \xrightarrow{w} & \underline{S} & \xrightarrow{t} & \mathbb{G}_{m,\mathbb{R}} \\ \parallel & & \downarrow h & & \parallel \\ \mathbb{G}_{m,\mathbb{R}} & \xrightarrow{w} & G_{\mathbb{R}} & \xrightarrow{t} & \mathbb{G}_{m,\mathbb{R}}. \end{array}$$

Une représentation définie sur $\mathbb{Q}$ $V_{\mathbb{Q}}$ de G est dite *homogène de poids n* si $w(x) * v = x^n \cdot v$ ($v \in V$). Toute représentation est somme de représentations homogènes. Soit $V_{\mathbb{Q}}$ une représentation de poids n . Alors, h munit $V_{\mathbb{Q}}$ d'une structure de Hodge rationnelle de poids n .

On regardera $\mathbb{Q}(n)_{\mathbb{Q}}$ comme une représentation de G , par la règle

$$g * x = t(g)^n \cdot x.$$

Cette convention est raisonnable, car $\underline{S}$ agit sur $\mathbb{Q}(n)_{\mathbb{R}}$ par la même formule. Une *polarisation* d'une représentation de poids n $V_{\mathbb{Q}}$ de G est une forme G -invariante

$$\psi : V_{\mathbb{Q}} \otimes V_{\mathbb{Q}} \longrightarrow \mathbb{Q}(n)$$

telle que $\psi(x, h(i)y)$ soit une forme symétrique et définie positive sur $V_{\mathbb{R}}$. Une polarisation ψ , étant G -invariante, est aussi $\underline{S}$ -invariante, donc une polarisation de la structure de Hodge rationnelle $V_{\mathbb{Q}}$.

2.10. Lemme. *Pour que la représentation $V_{\mathbb{Q}}$ soit polarisable, il faut et il suffit que la représentation $V_{\mathbb{R}}$ soit $h(i)$ -polarisable.*

Soit $P_{\mathbb{Q}}$ (resp. $P_{\mathbb{R}}$) l'espace des formes bilinéaires $(-1)^n$ -symétriques G -invariantes sur $V_{\mathbb{Q}}$ (resp. $V_{\mathbb{R}}$). On a $P_{\mathbb{R}} = \mathbb{R} \otimes P_{\mathbb{Q}}$. Les $h(i)$ -polarisations forment un ouvert de $P_{\mathbb{R}}$, et les polarisations de $V_{\mathbb{Q}}$ forment la trace de cet ouvert sur $P_{\mathbb{Q}}$. Le lemme en résulte.

2.11. Proposition. *a) Que ψ soit une polarisation de V ne dépend que de la classe de $G(\mathbb{R})$ -conjugaison de h .*

b) Les conditions suivantes sont équivalentes:

- (i) *$\text{ad } h(i)$ est une involution de Cartan de $\text{Ker}(t)_{\mathbb{R}}$;*
- (ii) *toute représentation homogène de G est polarisable;*
- (iii) *G admet une famille fidèle de représentations homogènes polarisables.*

Si G est connexe, ces conditions équivalent à

- (iii') *G admet une représentation polarisable ρ telle que $\text{Ker}(\rho) \cap \text{Ker}(t)$ soit fini.*

L'assertion a) résulte de 2.8.a). Si G est connexe, alors $\text{Ker}(t)$ est connexe: sinon t serait de la forme t_0^n , avec $n > 1$. Puisque $twx = x^{-2}$, on aurait $n = 2$, et $w(-1) \notin \text{Ker}(t)^0$. Ceci est absurde, car

$$w(-1) \in h(\text{Ker}(t : \underline{S} \longrightarrow \mathbb{G}_{m, \mathbb{R}})),$$

qui est connexe. Ceci dit, b) résulte de 2.10 et 2.8.b).

3. Rappels sur le groupe spinoriel

Pour les rappels contenus dans ce n^o, on pourra consulter [3].

3.1. Soit V un module libre sur un anneau A , muni d'une forme quadratique Q . Le module V s'identifie à un sous-module de l'algèbre de Clifford $C(V)$; dans $C(V)$, on a

$$v \cdot v = Q(v).$$

On désignera par $C^+(V)$ la partie paire de $C(V)$.

Si V est un module libre sur A , muni d'une forme bilinéaire symétrique ψ , on désignera par $C(V)$ (ou par $C(V, \psi)$) l'algèbre de Clifford de V muni de la forme quadratique $\psi(x, x)$.

3.2. Supposons que A soit un corps de caractéristique 0, et que Q soit non dégénérée. On note $\text{CSpin}(V)$ le *groupe de Clifford*. C'est le groupe algébrique des éléments inversibles g de $C^+(V)$ tels que $gVg^{-1} = V$. On définit un morphisme de $\text{CSpin}(V)$ dans $\text{SO}(V)$ par

$$g \longmapsto (v \longmapsto gvg^{-1}).$$

Le noyau de ce morphisme est réduit aux scalaires: on dispose d'une suite exacte de groupes algébriques

$$0 \longrightarrow \mathbb{G}_m \xrightarrow{w} \text{CSpin}(V) \longrightarrow \text{SO}(V) \longrightarrow 0.$$

Le groupe spinoriel $\text{Spin}(V)$ est le sous-groupe algébrique de $\text{CSpin}(V)$ noyau de la norme spinorielle

$$N : \text{CSpin}(V) \longrightarrow \mathbb{G}_m.$$

Désignons par t l'inverse de N ; on dispose d'un diagramme commutatif

$$\begin{array}{ccccccc}
 & & 0 & & & & \\
 & & \downarrow & & & & \\
 & & \text{Spin}(V) & & & & \\
 & & \downarrow & \searrow & & & \\
 0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{w} & \text{CSpin}(V) & \longrightarrow & \text{SO}(V) \longrightarrow 0 \\
 & & \searrow & & \downarrow & & \\
 & & & & \mathbb{G}_m & & \\
 & & & & \downarrow & & \\
 & & & & 0 & &
 \end{array} \tag{3.2.1}$$

$x \mapsto x^{-2}$

Par définition, on dispose aussi de

$$\alpha : \text{CSpin}(V) \hookrightarrow C^+(V)^*. \tag{3.2.2}$$

3.3. On note $(C^+(V))_s$ la représentation de $\text{CSpin}(V)$ sur $C^+(V)$ donnée par

$$g * x = \alpha(g) \cdot x. \tag{3.3.1}$$