

The Weil Conjecture for K3 Surfaces

Pierre Deligne* (Bures-sur-Yvette)

1. Statement of the Theorem

Let $\mathbb{F}_q$ be a field with q elements, let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$, let $\varphi \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ be the Frobenius substitution $x \mapsto x^q$, and let $F = \varphi^{-1}$ be the “geometric Frobenius.”

Let X be a scheme (separated and of finite type) over $\mathbb{F}_q$, and let $\overline{X}$ be the scheme over $\overline{\mathbb{F}}_q$ obtained from it by extension of scalars. For every closed point x of X , let $\deg(x) = [k(x) : \mathbb{F}_q]$ be the degree of the residue-field extension over $\mathbb{F}_q$. The zeta function $Z(X, t) \in \mathbb{Z}[[t]]$ is defined by

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

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

For every prime number ℓ prime to q , the ℓ -adic cohomology with proper supports $H_c^i(\overline{X}, \mathbb{Q}_\ell)$ of $\overline{X}$ is a finite-dimensional vector space over $\mathbb{Q}_\ell$, on which $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts by transport of structure. By Grothendieck, one has

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

Take X to be a nonsingular projective surface. In this case it is known that the factors

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

of $Z(X, t)$ are polynomials with integer coefficients independent of ℓ . The Weil conjecture asserts here that the roots of $P_i(t)$ have complex absolute value $q^{-i/2}$. This conjecture is invariant under finite extension of the finite base field. For X as above, and $i \neq 2$, it follows from Weil [9]. If, for simplicity, X is assumed geometrically connected, one indeed has

$$\begin{aligned} P_0(t) &= 1 - t, & P_4(t) &= 1 - q^2 t, \\ P_1(t) &= \det(1 - \varphi t; T_\ell(\text{Pic}^0(X)_{\text{red}})), & P_3(t) &= P_1(qt). \end{aligned}$$

*This article was written during a stay at the University of Warwick, which I thank for its hospitality.

Let k be a field of characteristic 0, and let X be a nonsingular projective geometrically connected surface over k . We say that X is a K3 surface if X is regular and has trivial canonical divisor, that is, if $H^1(X, \mathcal{O}) = 0$ and Ω_X^2 is isomorphic to $\mathcal{O}_X$. For the remarkable properties of these surfaces, we refer to [8]. We shall mainly use the following facts.

1.1. Lemma. (i) One has $h^{2,0} = h^{0,2} = 1$.

(i) One has $H^2(X, T_X^1) = 0$ (infinitesimal deformations are unobstructed), and the map induced by interior product

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

is bijective, while $H^0(X, T_X^1) = 0$ (X has no infinitesimal automorphisms).

One has

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

and (i) follows by Hodge symmetry. Since $H^1(X, \mathcal{O}_X) = 0$, Hodge symmetry and Serre duality give

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

Since $\Omega_X^2 = \mathcal{O}_X$, the “interior product” isomorphism

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

induces isomorphisms $T_X^1 \simeq \Omega_X^1$. The vanishing of $H^2(X, T_X^1)$ therefore follows from that of $h^{1,2}$, and it is clear that (1.1.1) is bijective. The same argument gives $H^0(X, T_X^1) = 0$.

1.2. Lemma. Let Y_0 be a nonsingular projective surface over a finite field $\mathbb{F}_q$. The following conditions are equivalent.

- (i) There exists a complete discrete valuation ring V of unequal characteristic with finite residue field k , a proper smooth morphism $f_V : Y \rightarrow \text{Spec}(V)$ whose generic fiber is a K3 surface, and $i : \mathbb{F}_q \rightarrow k$ such that $Y_0 \otimes_{\mathbb{F}_q} k \simeq Y \otimes_V k$.
- (ii) There exists an integral scheme S whose fraction field has characteristic 0, a point $s \in S$, a proper smooth morphism $f : Y \rightarrow S$ whose generic fiber is a K3 surface, and $i : \mathbb{F}_q \rightarrow k(s)$ such that $Y_0 \otimes_{\mathbb{F}_q} k(s) \simeq Y_s$.

The proof uses a standard passage to the limit. If the equivalent conditions of 1.2 are satisfied, we say that Y_0 lifts to a K3 surface.

1.3. Theorem. A nonsingular projective surface over a finite field $\mathbb{F}_q$ which lifts to a K3 surface satisfies the Weil conjecture.

This theorem was obtained independently by Pjateckii-Shapiro and Šafarevitch.

It applies, for example, to surfaces of degree 4 in $\mathbb{P}^3$. The Betti numbers of a K3 surface are $(1, 0, 22, 0, 1)$; the theorem therefore implies

that

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

Grothendieck's conjectural theory of motives (in particular his theory of the “motivic Galois group”) was very useful to me in constructing the proof. In this language (which will not be used below), the idea is, roughly speaking, to construct, by reduction from $\mathbb{C}$ to $\mathbb{F}_q$, an abelian variety A and an injective “morphism” of motives

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

in order to deduce the Weil conjecture for X from Weil's theorem for A . However, we do not define this “morphism” by an algebraic cycle; it is therefore not a morphism in the sense of [5]. In Hodge theory, its mode of definition has the following analogue (which will not be used below).

1.4. Lemma. *Let H be a variation of Hodge structures of weight n on a scheme S . If the local system $H_{\mathbb{Z}}$ has no global sections other than the section s and its multiples, then at every point of S the section s is of type $(n/2, n/2)$.*

1.5. Notations. 1.5.1. Scalar extensions will be denoted by subscripts: if M_A is a module over a ring (commutative with identity) A (or a scheme over A , for example an algebraic group over A), then M_B denotes the module over the A -algebra B (or the scheme over B) obtained from it by extension of scalars.

1.5.2. If a group G acts on a set X , we write $g * x$ for the transform of x by g .

1.5.3. When an equality is the definition of one of its sides, we write it $=_{\text{def}}$.

2. Polarized Hodge Structures

To work with Hodge structures, we shall use the formalism set out in [4] and briefly recalled below.

2.1. Let $\underline{S}$ be the real algebraic group of invertible elements of the $\mathbb{R}$ -algebra $\mathbb{C}$, let $w : \mathbb{G}_{m_{\mathbb{R}}} \rightarrow \underline{S}$ be the inclusion of $\mathbb{R}^*$ into $\mathbb{C}^*$, and let $t : \underline{S} \rightarrow \mathbb{G}_{m_{\mathbb{R}}}$ be the inverse of the norm; then $tw(x) = x^{-2}$. Let V be a finite-dimensional real vector space. It amounts to the same thing to give:

- a) $\rho : \underline{S} \rightarrow \text{GL}(V)$ of weight n : $\rho w(x) * v = x^n \cdot v$;
- b) a Hodge bigrading of weight n of $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$:

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

- c) a Hodge filtration of weight n of $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$: this is a decreasing filtration such that

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

One has

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

for $z \in \underline{S}(\mathbb{R}) = \mathbb{C}^*$ and $v^{p,q} \in V^{p,q}$, one has

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

Put $C = \rho(i)$; this is the *Weil operator* C . One has $Cv^{p,q} = i^{p-q}v^{p,q}$. For $\mathcal{E}$ a subset of $\mathbb{Z} \times \mathbb{Z}$, a Hodge bigrading is said to be of *type* $\mathcal{E}$ if the *Hodge numbers* $h^{p,q} = \dim V^{p,q}$ vanish for $(p,q) \notin \mathcal{E}$.

2.2. Here a *Hodge structure of weight* n H will mean a free finite-type $\mathbb{Z}$ -module $H_{\mathbb{Z}}$ together with a Hodge bigrading of weight n of $H_{\mathbb{C}} = H_{\mathbb{Z}} \otimes \mathbb{C}$. The *Tate Hodge structure* $\mathbb{Z}(n)$ is the Hodge structure of type $\{(-n, -n)\}$ given by

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

A polarization of a Hodge structure H of weight n is a morphism of Hodge structures

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

such that, on $H_{\mathbb{R}} = H_{\mathbb{Z}} \otimes \mathbb{R}$, the real bilinear form

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

is symmetric and positive definite. The form ψ is then $(-1)^n$ -symmetric.

A *rational Hodge structure of weight* n consists of a $\mathbb{Q}$ -vector space $H_{\mathbb{Q}}$ and a Hodge bigrading of weight n of $H_{\mathbb{C}} = H_{\mathbb{Q}} \otimes \mathbb{C}$. We denote by $\mathbb{Q}(n)$ the rational Hodge structure underlying $\mathbb{Z}(n)$. The definition of polarizations is left to the reader.

The following statement reformulates a theorem of Riemann.

2.3. Scholium. *The functor $A \mapsto H^1(A, \mathbb{Z})$ identifies polarized abelian varieties with polarized Hodge structures of type $\{(0, 1), (1, 0)\}$.*

From the remainder of this subsection, we shall use only 2.11(iii') $\Rightarrow$ (ii). To prove this implication, one may restrict to connected groups, which makes 2.5 unnecessary or obvious.

2.4. Let G be a real linear algebraic group. We say that G is *compact* if $G(\mathbb{R})$ is compact and every connected component of $G(\mathbb{C})$ has a real point. The obvious functor is then an equivalence from the category of algebraic linear representations of G to the category of linear representations of the compact group $G(\mathbb{R})$.

2.5. Lemma. *Every real algebraic subgroup H of a compact real algebraic group G is compact.*

It is known that the map

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

is bijective. It is enough to prove that, for every real subgroup H of G and every $h = g \cdot \exp(i\ell) \in H(\mathbb{C})$, one has $\ell \in \text{Lie}(H)$. Since $\bar{h} \in H(\mathbb{C})$, one has

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

Regard $G(\mathbb{C})$ as the set of real points of a real algebraic group. Let $\bar{J} \subset H(\mathbb{C})$ be, within this group, the Zariski closure of $J = \{\exp(ni\ell) \mid n \in 2\mathbb{Z}\}$. The elements $g \in J$, and hence the elements $g \in \bar{J}$, satisfy $g^{-1} = \bar{g}$, whence $\text{Lie}(\bar{J}) \subset i\text{Lie}(G)$. The Lie algebra $\text{Lie}(\bar{J})$ is abelian, and $\exp(\text{Lie}(\bar{J}))$ is a group, necessarily of finite index in $\bar{J}$. There are therefore n and $\ell' \in \text{Lie}(\bar{J})$ such that

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

Thus $i\ell \in \text{Lie}(\bar{J}) \subset \text{Lie}(H)$ and $\ell \in \text{Lie}(H)$, completing the proof.

2.6. Lemma. *Let G be a real algebraic group. The following conditions are equivalent:*

- (i) *G is compact;*
- (ii) *for every real (respectively complex) linear representation of G , there exists a positive-definite G -invariant symmetric bilinear (respectively hermitian sesquilinear) form;*
- (iii) *for a faithful representation of G , there exists a form as in (ii).*

For G connected, these conditions are further equivalent to

- (iii') *for a representation of G with finite kernel, there exists a form as in (ii).*

For G compact, G -invariance is equivalent to $G(\mathbb{R})$ -invariance, and (ii) is classical. If (iii) holds, G is a subgroup of an orthogonal or unitary group, and 2.5 applies. Condition (iii') implies that $G(\mathbb{R})$ is compact (as a finite covering of a compact group); if G is connected, G is therefore compact.

2.7. Let G be a real linear algebraic group. For every involutive automorphism σ of G , let $G^{(\sigma)}$ be the real form of $G_{\mathbb{C}}$ defined by the antilinear involution $g \mapsto \sigma(\bar{g})$. We say that σ is a *Cartan involution* if $G^{(\sigma)}$ is compact.

Let C be an element of $G(\mathbb{R})$ whose square is central. A real (respectively complex) representation of G will be called C -polarizable if there exists on V a G -invariant bilinear (respectively sesquilinear) form ψ such that $\psi(x, Cy)$ is symmetric (respectively hermitian) and positive definite. We then say that ψ is a C -polarization of V . A special case of the following lemma is stated without proof in [4].

2.8. Lemma. *a) Whether ψ is a C -polarization of V depends only on the $G(\mathbb{R})$ -conjugacy class of C .
b) The following conditions are equivalent:*

- (i) $\text{ad } C$ is a Cartan involution of G ;
- (ii) every real (respectively complex) representation of G is C -polarizable;
- (iii) G has a faithful real (respectively complex) C -polarizable representation.

If G is connected, these conditions are also equivalent to

- (iii') G has a real (respectively complex) C -polarizable representation with finite kernel.

To prove a), note that $\psi(x, gCg^{-1}y) = \psi(g^{-1}x, Cg^{-1}y)$. A sesquilinear form ψ on a complex representation of G is G -invariant if and only if

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

This condition is equivalent to

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

(replace y by Cy), i.e. to the $G^{(\text{ad } C)}$ -invariance of $\psi(x, Cy)$. The “respectively” version of 2.8 therefore follows from 2.6. The non-“respectively” version follows from it:

- a) the complexification (respectively realification) of a real (respectively complex) C -polarizable representation is C -polarizable;
- b) a polarization of V induces a polarization of every subrepresentation of V ;
- c) for V real (respectively complex), one has $V \hookrightarrow V \otimes_{\mathbb{R}} \mathbb{C}$.

2.9. Let G be a reductive group over $\mathbb{Q}$, and let t and w be morphisms defined over $\mathbb{Q}$

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

with $tw(x) = x^{-2}$ and w central. Suppose also given a commutative diagram

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

A representation defined over $\mathbb{Q}$, $V_{\mathbb{Q}}$, of G is called *homogeneous of weight n* if $w(x) * v = x^n \cdot v$ ($v \in V$). Every representation is a sum of homogeneous representations. Let $V_{\mathbb{Q}}$ be a representation of weight n . Then h endows $V_{\mathbb{Q}}$ with a rational Hodge structure of weight n .

We shall regard $\mathbb{Q}(n)_{\mathbb{Q}}$ as a representation of G by the rule

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

This convention is reasonable, since $\underline{S}$ acts on $\mathbb{Q}(n)_{\mathbb{R}}$ by the same formula. A *polarization* of a weight- n representation $V_{\mathbb{Q}}$ of G is a G -invariant form

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

such that $\psi(x, h(i)y)$ is a symmetric positive-definite form on $V_{\mathbb{R}}$. Being G -invariant, a polarization ψ is also $\underline{S}$ -invariant and hence a polarization of the rational Hodge structure $V_{\mathbb{Q}}$.

2.10. Lemma. *A representation $V_{\mathbb{Q}}$ is polarizable if and only if the representation $V_{\mathbb{R}}$ is $h(i)$ -polarizable.*

Let $P_{\mathbb{Q}}$ (resp. $P_{\mathbb{R}}$) be the space of G -invariant $(-1)^n$ -symmetric bilinear forms on $V_{\mathbb{Q}}$ (resp. $V_{\mathbb{R}}$). One has $P_{\mathbb{R}} = \mathbb{R} \otimes P_{\mathbb{Q}}$. The $h(i)$ -polarizations form an open subset of $P_{\mathbb{R}}$, and the polarizations of $V_{\mathbb{Q}}$ are the intersection of this open subset with $P_{\mathbb{Q}}$. The lemma follows.

2.11. Proposition. *a) Whether ψ is a polarization of V depends only on the $G(\mathbb{R})$ -conjugacy class of h .*

b) The following conditions are equivalent:

- (i) *$\text{ad } h(i)$ is a Cartan involution of $\text{Ker}(t)_{\mathbb{R}}$;*
- (ii) *every homogeneous representation of G is polarizable;*
- (iii) *G has a faithful family of polarizable homogeneous representations.*

If G is connected, these conditions are equivalent to

- (iii') *G has a polarizable representation ρ such that $\text{Ker}(\rho) \cap \text{Ker}(t)$ is finite.*

Assertion a) follows from 2.8.a). If G is connected, then $\text{Ker}(t)$ is connected: otherwise t would be of the form t_0^n , with $n > 1$. Since $twx = x^{-2}$, one would have $n = 2$ and $w(-1) \notin \text{Ker}(t)^0$. This is absurd, since

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

which is connected. With this established, b) follows from 2.10 and 2.8.b).

3. Review of the Spinor Group

For the material recalled in this section, see [3].

3.1. Let V be a free module over a ring A , equipped with a quadratic form Q . The module V is identified with a submodule of the Clifford algebra $C(V)$; in $C(V)$ one has

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

We denote by $C^+(V)$ the even part of $C(V)$.

If V is a free module over A , equipped with a symmetric bilinear form ψ , we denote by $C(V)$ (or by $C(V, \psi)$) the Clifford algebra of V equipped with the quadratic form $\psi(x, x)$.

3.2. Suppose that A is a field of characteristic 0, and that Q is nondegenerate. We denote by $\text{CSpin}(V)$ the *Clifford group*. It is the algebraic group of invertible elements g of $C^+(V)$ such that $gVg^{-1} = V$. We define a morphism from $\text{CSpin}(V)$ to $\text{SO}(V)$ by

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

The kernel of this morphism consists only of the scalars: there is an exact sequence of algebraic groups

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

The spin group $\text{Spin}(V)$ is the algebraic subgroup of $\text{CSpin}(V)$ that is the kernel of the spinor norm

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

Let t denote the inverse of N ; there is a commutative diagram

$$\begin{array}{ccccccc}
& & & 0 & & & \\
& & & \downarrow & & & \\
& & & \text{Spin}(V) & & & \\
& & & \downarrow & \searrow & & \\
0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{w} & \text{CSpin}(V) & \longrightarrow & \text{SO}(V) \longrightarrow 0 \\
& & \searrow & & \downarrow & & \\
& & x \mapsto x^{-2} & & t & & \\
& & & & \mathbb{G}_m & & \\
& & & & \downarrow & & \\
& & & & 0 & &
\end{array} \tag{3.2.1}$$

By definition, one also has

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

3.3. We denote by $(C^+(V))_s$ the representation of $\text{CSpin}(V)$ on $C^+(V)$ given by

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