# The Riemann Hypothesis over Finite Fields: From Weil to the Present Day*

**by James S. Milne**†

**Abstract.** The statement of the Riemann hypothesis makes sense for all global fields, not just the rational numbers. For function fields, it has a natural restatement in terms of the associated curve. Weil's work on the Riemann hypothesis for curves over finite fields led him to state his famous "Weil conjectures", which drove much of the progress in algebraic and arithmetic geometry in the following decades.

MSC 2010 subject classifications: 01A60, 11-03, 14-03.

## Contents



A global field $K$ of characteristic $p$ is a field finitely generated and of transcendence degree 1 over $\mathbb{F}_p$. The field of constants $k$ of $K$ is the algebraic closure of $\mathbb{F}_p$ in $K$. Let $x$ be an element of $K$ transcendental over $k$. Then

$$\zeta(K,s) \stackrel{\text{def}}{=} \prod_{\mathfrak{p}} \frac{1}{1-N\mathfrak{p}^{-s}}$$

where $\mathfrak{p}$ runs over the prime ideals of the integral closure $\mathscr{O}_K$ of $k[x]$ in $K$ and $N\mathfrak{p} = |\mathscr{O}_K/\mathfrak{p}|$; we also include factors for each of the finitely many prime ideals $\mathfrak{p}$ in the integral closure of $k[x^{-1}]$ not corresponding to an ideal of $\mathscr{O}_K$. The Riemann hypothesis for $K$ states that the zeros of $\zeta(K,s)$ lie on the line $\Re(s) = 1/2$.

Let $C$ be the (unique) nonsingular projective over $k$ with function field is $K$. Let $k_n$ denote the finite field of degree $n$ over $k$, and let $N_n$ denote the number of points of $C$ rational over $k_n$:

$$N_n \stackrel{\text{def}}{=} |C(k_n)|.$$

The zeta function of $C$ is the power series $Z(C,T) \in \mathbb{Q}[[T]]$ such that

$$\frac{d\log Z(C,T)}{dT} = \sum_{n=1}^{\infty} N_n T^{n-1}.$$

This can also be expressed as a product

$$Z(C,T) = \prod_{P} \frac{1}{1-T^{\deg(P)}}$$

where $P$ runs over the closed points of $C$ (as a scheme). Each $P$ corresponds to a prime ideal $\mathfrak{p}$ in the preceding paragraph, and $N\mathfrak{p} = q^{\deg(P)}$ where $q = |k|$. Therefore

$$\zeta(K,s) = Z(C,q^{-s}).$$

Let $g$ be the genus of $C$. Using the Riemann-Roch theorem, one finds that

$$Z(C,T) = \frac{P(C,T)}{(1-T)(1-qT)}$$

* Reprinted with permission from "The legacy of Bernhard Riemann after one hundred and fifty years", edited by Lizhen Ji, Frans Oort and Shing-Tung Yau, International Press, 2016.
† Professor Emeritus, Department of Mathematics, University of Michigan, Ann Arbor, Mich., U.S.A.
E-mail: jmilne@umich.edu

where

$$P(C,T) = 1 + c_1 T + \cdots + c_{2g} T^{2g} \in \mathbb{Z}[T];$$

moreover $Z(C,T)$ satisfies the functional equation

$$Z(C,1/qT) = q^{1-g} \cdot T^{2-2g} \cdot Z(C,T).$$

Thus $\zeta(K,s)$ is a rational function in $q^{-s}$ with simple poles at $s=0$, $1$ and zeros at $a_1,\ldots,a_{2g}$ where the $a_i$ are the inverse roots of $P(C,T)$, i.e.,

$$P(C,T) = \prod_{i=1}^{2g}(1-a_i T),$$

and it satisfies a functional equation relating $\zeta(K,s)$ and $\zeta(K,1-s)$. The Riemann hypothesis now asserts that

$$|a_i| = q^{\frac{1}{2}}, \quad i = 1,\ldots,2g.$$

Note that

$$\log Z(C,T) = \begin{cases} \sum_1^\infty N_n \frac{T^n}{n} \\ \log \frac{(1-a_1T)\cdots(1-a_{2g}T)}{(1-T)(1-qT)}, \end{cases}$$

and so

$$N_n = 1 + q^n - (a_1^n + \cdots + a_{2g}^n).$$

Therefore, the Riemann hypothesis implies that

$$|N_n - q^n - 1| \le 2g \cdot (q^n)^{1/2};$$

conversely, if this inequality holds for all $n$, then the Riemann hypothesis holds for $C$.[1]

The above is a brief summary of the results obtained by the German school of number theorists (Artin, F. K. Schmidt, Deuring, Hasse, ....) by the mid-1930s. In the 1930s Hasse gave two proofs of the Riemann hypothesis for curves of genus 1, the second of which uses the endomorphism ring of the elliptic curve[2] in an essential way (see the sketch below). Deuring recognized that for curves of higher genus it was necessary to replace the endomorphism ring of the curve with its ring of correspondences in the sense of Severi 1903, and he wrote two articles reformulating part of Severi's theory in terms of "double-fields" (in particular, extending it to all characteristics). Weil was fully aware of these ideas of Deuring and Hasse. For an account of this early work, see Schappacher 2006 and Oort and Schappacher 2016.

[1] The condition implies that the power series

$$\sum_{i=1}^{2g} \frac{1}{1-a_i z} = \sum_{n=0}^{\infty}\left(\sum_{i=1}^{2g} a_i^n\right) z^n$$

converges for $|z| \le q^{-1/2}$, and so $|a_i| \le q^{1/2}$ for all $i$. The functional equation shows that $q/a_i$ is also a root of $P(C,T)$, and so $|a_i| = q^{1/2}$.

[2] F. K. Schmidt (1931) showed that every curve over a finite field has a rational point. The choice of such a point on a curve of genus 1 makes it an elliptic curve.



For future reference, we sketch the proof of the Riemann hypothesis for elliptic curves. Let $E$ be such a curve over a field $k$, and let $\alpha$ be an endomorphism of $E$. For $\ell \neq \operatorname{char}(k)$, the $\mathbb{Z}_\ell$-module $T_\ell E \stackrel{\text{def}}{=} \varprojlim_n E_{\ell^n}(k^{\text{al}})$ is free of rank 2 and $\alpha$ acts on it with determinant $\deg\alpha$. Over $\mathbb{C}$ this statement can be proved by writing $E = \mathbb{C}/\Lambda$ and noting that $T_\ell E \simeq \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \Lambda$. Over a field of nonzero characteristic the proof is more difficult—it will be proved in a more general setting later (1.21, 1.26).

Now let $\alpha$ be an endomorphism of $E$, and let $T^2 + cT + d$ be its characteristic polynomial on $T_\ell E$:

$$T^2 + cT + d \stackrel{\text{def}}{=} \det(T - \alpha | T_\ell E).$$

Then,

$$d = \det(-\alpha|T_\ell E) = \deg(\alpha)$$
$$1 + c + d = \det(\mathrm{id}_E - \alpha|T_\ell E) = \deg(\mathrm{id}_E - \alpha),$$

and so $c$ and $d$ are integers independent of $\ell$.

For an integer $n$, let

$$T^2 + c'T + d' = \det(T - n\alpha|T_\ell E). \tag{1}$$

Then $c' = nc$ and $d' = n^2 d$. On substituting $m$ for $T$ in (1), we find that

$$m^2 + cmn + dn^2 = \det(m - n\alpha|T_\ell E).$$

The right hand side is the degree of the map $m - n\alpha$, which is always nonnegative, and so the discriminant $c^2 - 4d \le 0$, i.e., $c^2 \le 4d$.

We apply these statements to the Frobenius map $\pi\colon (x_0 \colon x_1 \colon \ldots) \mapsto (x_0^q \colon x_1^q \colon \ldots)$. The homomorphism $\mathrm{id}_E - \pi\colon E \to E$ is étale and its kernel on $E(k^{\text{al}})$ is $E(k)$, and so its degree is $|E(k)|$. Let $f = T^2 + cT + d$ be the characteristic polynomial of $\pi$. Then $d = \deg(\pi) = q$, and $c^2 \le 4d = 4q$. From

$$|E(k)| = \deg(\mathrm{id}_E - \pi) = \det(\mathrm{id}_E - \pi|T_\ell E) = f(1) = 1 + c + q,$$

we see that

$$||E(k)| - q - 1| = |c| \le 2q^{1/2},$$

as required.

## 1. Weil's Work in the 1940s and 1950s

### The 1940 and 1941 Announcements

Weil announced the proof of the Riemann hypothesis for curves over finite fields in a brief three-page note (Weil 1940), which begins with the following paragraph:

I shall summarize in this Note the solution of the main problems in the theory of algebraic functions with a finite field of constants; we know that this theory has been the subject of numerous works, especially, in recent years, by Hasse and his students; as they have caught a glimpse of, the key to these problems is the theory of correspondences; but the algebraic theory of correspondences, due to Severi, is not sufficient, and it is necessary to extend Hurwitz's transcendental theory to these functions.[3]

The "main problems" were the Riemann hypothesis for curves of arbitrary genus, and Artin's conjecture that the (Artin) $L$-function attached to a nontrivial simple Galois representation is entire.

"Hurwitz's transcendental theory" refers to the memoir Hurwitz 1887, which Weil had studied already as a student at the Ecole Normale Supérieure. There Hurwitz gave the first proof[4] of the formula expressing the number of coincident points of a correspondence $X$ on a complex algebraic curve $C$ in terms of traces. In modern terms,

$$\begin{aligned}&(\text{number of coincidences})\\&\quad=\mathrm{Tr}(X|H_0(C,\mathbb{Q}))-\mathrm{Tr}(X|H_1(C,\mathbb{Q}))+\mathrm{Tr}(X|H_2(C,\mathbb{Q})).\end{aligned}$$

This can be rewritten

$$(X\cdot\Delta)=d_2(X)-\mathrm{Tr}(X|H_1(C))+d_1(X) \tag{2}$$

where $d_1(X)=(X\cdot C\times\mathrm{pt})$ and $d_2(X)=(X\cdot\mathrm{pt}\times C)$.

Now consider a nonsingular projective curve $C_0$ over a field $k_0$ with $q$ elements, and let $C$ be the curve over the algebraic closure $k$ of $k_0$ obtained from $C$ by extension of scalars. For the graph of the Frobenius endomorphism $\pi$ of $C$, the equality (2) becomes

$$(\Gamma_\pi\cdot\Delta)=1-\text{“}\mathrm{Tr}(\pi|H_1(C))\text{”}+q.$$

As $(\Gamma_\pi\cdot\Delta)=|C_0(k_0)|$, we see that everything comes down to understanding algebraically (and in nonzero characteristic!), the "trace of a correspondence on the first homology group of the curve".

Let $g$ be the genus of $C_0$. In his 1940 note,[5] Weil considers the group $G$ of divisor classes on $C$ of degree 0 and order prime to $p$, and assumes that $G$ is isomorphic to $(\mathbb{Q}/\mathbb{Z}(\text{non}-p))^{2g}$. A correspondence[6] $X$ on $C$ defines an endomorphism of $G$ whose trace Weil calls the trace $\mathrm{Tr}(X)$ of $X$. This is an element of $\prod_{l\neq p}\mathbb{Z}_l$, which nowadays we prefer to define as the trace of $X$ on $TG\overset{\text{def}}{=}\varprojlim_{(n,p)=1}G_n$.[7]

After some preliminaries, including the definition in this special case of what is now called the Weil pairing, Weil announces his "important lemma": let $X$ be an $(m_1,m_2)$ correspondence on $C$, and let $X'$ be the $(m_2,m_1)$-correspondence obtained by reversing the factors;

> if $m_1=g$, we have in general (i.e., under conditions which it is unnecessary to make precise here) $2m_2=\mathrm{Tr}(X\circ X')$.[8]

From this he deduces that, for all correspondences $X$, the trace $\mathrm{Tr}(X\circ X')$ is a rational integer $\geq 0$ and that the number of coincident points of $X$ is $m_1+m_2-\mathrm{Tr}(X)$. On applying these statements to the graph of the Frobenius map, he obtains his main results.

At the time Weil wrote his note, he had little access to the mathematical literature. His confidence in the statements in his note was based on his own rather ad hoc heuristic calculations (Œuvres, I, pp. 548–550). As he later wrote:

> In other circumstances, publication would have seemed very premature. But in April 1940, who could be sure of a tomorrow? It seemed to me that my ideas contained enough substance to merit not being in danger of being lost.[9] (Œuvres I, p. 550.)

In his note, Weil had replaced the jacobian variety with its points of finite order. But he soon realized that proving his "important lemma" depended above all on intersection theory on the jacobian variety.

> In 1940 I had seen fit to replace the jacobian with its group of points of finite order. But I began to realize that a considerable part of Italian geometry was based entirely on intersection theory… In particular, my "important lemma" of 1940 seemed to depend primarily on intersection theory on the jacobian; so this is what I needed.[10] (Œuvres I, p. 556.)

[3] Je vais résumer dans cette Note la solution des principaux problèmes de la théorie des fonctions algébriques à corps de constantes fini; on sait que celle-ci a fait l'objet de nombreux travaux, et plus particulièrement, dans les derniéres années, de ceux de Hasse et de ses élèves; comme ils l'ont entrevu, la théorie des correspondances donne la clef de ces problèmes; mais la théorie algébrique des correspondances, qui est due à Severi, n'y suffit point, et il faut étendre à ces fonctions la théorie transcendante de Hurwitz.

[4] As Oort pointed out to me, Chasles-Cayley-Brill 1864, 1866, 1873, 1874 discussed this topic before Hurwitz did, but perhaps not "in terms of traces".

[5] In fact, following the German tradition (Artin, Hasse, Deuring, …), Weil expressed himself in this note in terms of functions fields instead of curves. Later, he insisted on geometric language.

[6] See p. 19.

[7] In terms of the jacobian variety $J$ of $C$, which wasn't available to Weil at the time, $TG=\prod_{l\neq p}T_lJ$, and the positivity of $\mathrm{Tr}(X\circ X')$ expresses the positivity of the Rosati involution on the endomorphism algebra of $J$.

[8] Si $m_1=g$, on a en général (c'est-à-dire à des conditions qu'il est inutile de préciser ici) $2m_2=\mathrm{Tr}(X\circ X')$.

[9] "En d'autres circonstances, une publication m'aurait paru bien prématurée. Mais, en avril 1940, pouvait-on se croire assuré du lendemain? Il me sembla que mes idées contenaient assez de substance pour ne pas mériter d'être en danger de se perdre." This was seven months after Germany had invaded Poland, precipitating the Second World War. At the time, Weil was confined to a French military prison as a result of his failure to report for duty. His five-year prison sentence was suspended when he joined a combat unit. During the collapse of France, his unit was evacuated to Britain. Later he was repatriated to Vichy France, from where in January 1941 he managed to exit to the United States. Because of his family background, he was in particular danger during this period.

[10] En 1940 j'avais jugé opportun de substituer à la jacobienne le groupe de ses points d'ordre fini. Mais je com-

In expanding the ideas in his note, he would construct the jacobian variety of a curve and develop a comprehensive theory of abelian varieties over arbitrary fields parallel to the transcendental theory over $\mathbb{C}$. But first he had to rewrite the foundations of algebraic geometry.

In the meantime, he had found a more elementary proof of the Riemann hypothesis, which involved only geometry on the product of two curves. First he realized that if he used the fixed point formula (2) to *define* the trace $\sigma(X)$ of a correspondence $X$ on $C$, i.e.,

$$\sigma(X) \stackrel{\text{def}}{=} d_1(X) + d_2(X) - (X \cdot \Delta),$$

then it was possible to prove directly that $\sigma$ had many of the properties expected of a trace on the ring of correspondence classes. Then, as he writes (Œuvres I, p. 557):

> At the same time I returned seriously to the study of the *Trattato* [Severi 1926]. The trace $\sigma$ does not appear as such; but there is much talk of a "difetto di equivalenza" whose positivity is shown on page 254. I soon recognized it as my integer $\sigma(X \circ X')$ ... I could see that, to ensure the validity of the Italian methods in characteristic $p$, all the foundations would have to be redone, but the work of van der Waerden, together with that of the topologists, allowed me to believe that it would not be beyond my strength.[11]

Weil announced this proof in (Weil 1941). Before describing it, I present a simplified modern version of the proof.

**Notes.** Whereas the 1940 proof (implicitly) uses the jacobian $J$ of the curve $C$, the 1941 proof involves only geometry on $C \times C$. Both use the positivity of "$\sigma(X \circ X')$" but the first proof realizes this integer as a trace on the torsion group $\mathrm{Jac}(C)$(non-$p$) whereas the second expresses it in terms of intersection theory on $C \times C$.

## The Geometric Proof of the Riemann Hypothesis for Curves

Let $V$ be a nonsingular projective surface over an algebraically closed field $k$.

#### Divisors

A divisor on $V$ is a formal sum $D = \sum n_i C_i$ with $n_i \in \mathbb{Z}$ and $C_i$ an irreducible curve on $V$. We say that $D$ is positive, denoted $D \geq 0$, if all the $n_i \geq 0$. Every $f \in k(V)^\times$ has an associated divisor $(f)$ of zeros and poles—these are the principal divisors. Two divisors $D$ and $D'$ are said to be linearly equivalent if

$$D' = D + (f) \text{ some } f \in k(V)^\times.$$

For a divisor $D$, let

$$L(D) = \{f \in k(V) \mid (f) + D \geq 0\}.$$

Then $L(C)$ is a finite-dimensional vector space over $k$, whose dimension we denote by $l(D)$. The map $g \mapsto gf$ is an isomorphism $L(D) \to L(D - (f))$, and so $l(D)$ depends only on the linear equivalence class of $D$.

#### Elementary Intersection Theory

Because $V$ is nonsingular, a curve $C$ on $V$ has a local equation at every closed point $P$ of $V$, i.e., there exists an $f$ such that

$$C = (f) + \text{components not passing through } P.$$

If $C$ and $C'$ are distinct irreducible curves on $V$, then their intersection number at $P \in C \cap C'$ is

$$(C \cdot C')_P \stackrel{\text{def}}{=} \dim_k(\mathscr{O}_{V,P}/(f, f'))$$

where $f$ and $f'$ are local equations for $C$ and $C'$ at $P$, and their (global) intersection number is

$$(C \cdot C') = \sum_{P \in C \cap C'} (C \cdot C')_P.$$

This definition extends by linearity to pairs of divisors $D, D'$ without common components. Now observe that $((f) \cdot C) = 0$, because it equals the degree of the divisor of $f|C$ on $C$, and so $(D \cdot D')$ depends only on the linear equivalence classes of $D$ and $D'$. This allows us to define $(D \cdot D')$ for all pairs $D, D'$ by replacing $D$ with a linearly equivalent divisor that intersects $D'$ properly. In particular, $(D^2) \stackrel{\text{def}}{=} (D \cdot D)$ is defined. See Shafarevich 1994, IV, §1, for more details.

#### The Riemann-Roch Theorem

Recall that the Riemann-Roch theorem for a curve $C$ states that, for all divisors $D$ on $C$,

$$l(D) - l(K_C - D) = \deg(D) + 1 - g$$

where $g$ is the genus of $C$ and $K_C$ is a canonical divisor (so $\deg K_C = 2g - 2$ and $l(K_C) = g$). Better, in terms of cohomology,

$$\chi(\mathscr{O}(D)) = \deg(D) + \chi(\mathscr{O})$$
$$h^1(D) = h^0(K_C - D).$$

---

mençais à apercevoir qu'une notable partie de la géométrie italienne reposait exclusivement sur la théorie des intersections. Les travaux de van der Waerden, bien qu'ils fussent restés bien en deçà des besoins, donnaient lieu d'espérer que le tout pourrait un jour se transposer en caractéristique $p$ sans modification substantielle. En particulier, mon "lemme important" de 1940 semblait dépendre avant tout de la théorie des intersections sur la jacobienne; c'est donc celle-ci qu'il me fallait.

[11] En même temps je m'étais remis sérieusement à l'étude du *Trattato*. La trace $\sigma$ a n'y apparaît pas en tant que telle; mais il y est fort question d'un "difetto di equivalenza" dont la positivité est démontrée à la page 254. J'y reconnus bientôt mon entier $\sigma(yy')$... Je voyais bien que, pour s'assurer de la validité des méthodes italiennes en caractéristique $p$, toutes les fondations seraient à reprendre, mais les travaux de van der Waerden, joints à ceux des topologues, donnaient à croire que ce ne serait pas au dessus de mes forces.

The Riemann-Roch theorem for a surface $V$ states that, for all divisors $D$ on $V$,

$$l(D) - \sup(D) + l(K_V - D) = p_a + 1 + \frac{1}{2}(D \cdot D - K_V)$$

where $K_V$ is a canonical divisor and

$$p_a = \chi(\mathscr{O}) - 1 \quad \text{(arithmetic genus)},$$
$$\sup(D) = \text{superabundance of } D (\geq 0, \text{and} = 0 \text{ for some divisors}).$$

Better, in terms of cohomology,

$$\chi(\mathscr{O}(D)) = \chi(\mathscr{O}_V) + \frac{1}{2}(D \cdot D - K)$$
$$h^2(D) = h^0(K - D),$$

and so

$$\sup(D) = h^1(D).$$

We shall also need the adjunction formula: let $C$ be a curve on $V$; then

$$K_C = (K_V + C) \cdot C.$$

### The Hodge Index Theorem

Embed $V$ in $\mathbb{P}^n$. A hyperplane section of $V$ is a divisor of the form $H = V \cap H'$ with $H'$ a hyperplane in $\mathbb{P}^n$ not containing $V$. Any two hyperplane sections are linearly equivalent (obviously).

**Lemma 1.1.** *For a divisor* $D$ *and hyperplane section* $H$*,*

$$(3) \qquad l(D) > 1 \implies (D \cdot H) > 0.$$

*Proof.* The hypothesis implies that there exists a $D_1 > 0$ linearly equivalent to $D$. If the hyperplane $H'$ is chosen not to contain a component of $D_1$, then the hyperplane section $H = V \cap H'$ intersects $D_1$ properly. Now $D_1 \cap H = D_1 \cap H'$, which is nonempty by dimension theory, and so $(D_1 \cdot H) > 0$. □

**Theorem 1.2 (Hodge Index Theorem).** *For a divisor* $D$ *and hyperplane section* $H$*,*

$$(D \cdot H) = 0 \implies (D \cdot D) \leq 0.$$

*Proof.* We begin with a remark: suppose that $l(D) > 0$, i.e., there exists an $f \neq 0$ such that $(f) + D \geq 0$; then, for a divisor $D'$,

$$(4) \qquad l(D + D') = l((D + (f)) + D') \geq l(D').$$

We now prove the theorem. To prove the contrapositive, it suffices to show that

$$(D \cdot D) > 0 \implies l(mD) > 1 \text{ for some integer } m,$$

because then

$$(D \cdot H) = \frac{1}{m}(mD \cdot H) \neq 0$$

by (3) above. Hence, suppose that $(D \cdot D) > 0$. By the Riemann-Roch theorem

$$l(mD) + l(K_V - mD) \geq \frac{(D \cdot D)}{2} m^2 + \text{ lower powers of } m.$$

Therefore, for a fixed $m_0 \geq 1$, we can find an $m > 0$ such that

$$l(mD) + l(K_V - mD) \geq m_0 + 1$$
$$l(-mD) + l(K_V + mD) \geq m_0 + 1.$$

If both $l(mD) \leq 1$ and $l(-mD) \leq 1$, then both $l(K_V - mD) \geq m_0$ and $l(K_V + mD) \geq m_0$, and so

$$l(2K_V) = l(K_V - mD + K_V + mD) \overset{(4)}{\geq} l(K_V + mD) \geq m_0.$$

As $m_0$ was arbitrary, this is impossible. □

Let $Q$ be a symmetric bilinear form on a finite-dimensional vector space $W$ over $\mathbb{Q}$ (or $\mathbb{R}$). There exists a basis for $W$ such that $Q(x,x) = a_1 x_1^2 + \cdots + a_n x_n^2$. The number of $a_i > 0$ is called the *index* (of positivity) of $Q$—it is independent of the basis. There is the following (obvious) criterion: $Q$ has index 1 if and only if there exists an $x \in V$ such that $Q(x,x) > 0$ and $Q(y,y) \leq 0$ for all $y \in \langle x \rangle^{\perp}$.

Now consider a surface $V$ as before, and let $\mathrm{Pic}(V)$ denote the group of divisors on $V$ modulo linear equivalence. We have a symmetric bi-additive intersection form

$$\mathrm{Pic}(V) \times \mathrm{Pic}(V) \to \mathbb{Z}.$$

On tensoring with $\mathbb{Q}$ and quotienting by the kernels, we get a nondegenerate intersection form

$$N(V) \times N(V) \to \mathbb{Q}.$$

**Corollary 1.3.** *The intersection form on* $N(V)$ *has index* 1*.*

*Proof.* Apply the theorem and the criterion just stated. □

**Corollary 1.4.** *Let* $D$ *be a divisor on* $V$ *such that* $(D^2) > 0$*. If* $(D \cdot D') = 0$*, then* $(D'^2) \leq 0$*.*

*Proof.* The form is negative definite on $\langle D \rangle^{\perp}$. □

### The Inequality of Castelnuovo-Severi

Now take $V$ to be the product of two curves, $V = C_1 \times C_2$. Identify $C_1$ and $C_2$ with the curves $C_1 \times \mathrm{pt}$ and $\mathrm{pt} \times C_2$ on $V$, and note that

$$C_1 \cdot C_1 = 0 = C_2 \cdot C_2$$
$$C_1 \cdot C_2 = 1 = C_2 \cdot C_1.$$

Let $D$ be a divisor on $C_1 \times C_2$ and set $d_1 = D \cdot C_1$ and $d_2 = D \cdot C_2$.

**Theorem 1.5 (Castelnuovo-Severi Inequality).** *Let $D$ be a divisor on $V$; then*

$$(D^2) \le 2d_1 d_2. \tag{5}$$

*Proof.* We have

$$(C_1 + C_2)^2 = 2 > 0$$
$$(D - d_2 C_1 - d_1 C_2) \cdot (C_1 + C_2) = 0.$$

Therefore, by the Hodge index theorem,

$$(D - d_2 C_1 - d_1 C_2)^2 \le 0.$$

On expanding this out, we find that $D^2 \le 2d_1 d_2$. □

Define the equivalence defect (*difetto di equivalenza*) of a divisor $D$ by

$$\mathrm{def}(D) = 2d_1 d_2 - (D^2) \ge 0.$$

**Corollary 1.6.** *Let $D$, $D'$ be divisors on $V$; then*

$$\left|(D \cdot D') - d_1 d_2' - d_2 d_1'\right| \le \left(\mathrm{def}(D)\mathrm{def}(D')\right)^{1/2}. \tag{6}$$

*Proof.* Let $m, n \in \mathbb{Z}$. On expanding out

$$\mathrm{def}(mD + nD') \ge 0,$$

we find that

$$m^2 \mathrm{def}(D) - 2mn\left((D \cdot D') - d_1 d_2' - d_2 d_1'\right) + n^2 \mathrm{def}(D') \ge 0.$$

As this holds for all $m, n$, it implies (6). □

**Example 1.7.** Let $f$ be a nonconstant morphism $C_1 \to C_2$, and let $g_i$ denote the genus of $C_i$. The graph of $f$ is a divisor $\Gamma_f$ on $C_1 \times C_2$ with $d_2 = 1$ and $d_1$ equal to the degree of $f$. Now

$$K_{\Gamma_f} = (K_V + \Gamma_f) \cdot \Gamma_f \qquad \text{(adjunction formula)}.$$

On using that $K_V = K_{C_1} \times C_2 + C_1 \times K_{C_2}$, and taking degrees, we find that

$$2g_1 - 2 = (\Gamma_f)^2 + (2g_1 - 2) \cdot 1 + (2g_2 - 2)\deg(f).$$

Hence

$$\mathrm{def}(\Gamma_f) = 2g_2 \deg(f). \tag{7}$$

### Proof of the Riemann Hypothesis for Curves

Let $C_0$ be a projective nonsingular curve over a finite field $k_0$, and let $C$ be the curve obtained by extension of scalars to the algebraic closure $k$ of $k_0$. Let $\pi$ be the Frobenius endomorphism of $C$. Then (see (7)), $\mathrm{def}(\Delta) = 2g$ and $\mathrm{def}(\Gamma_\pi) = 2gq$, and so (see (6)),

$$|(\Delta \cdot \Gamma_\pi) - q - 1| \le 2gq^{1/2}.$$

As

$$(\Delta \cdot \Gamma_\pi) = \text{ number of points on } C \text{ rational over } k_0,$$

we obtain Riemann hypothesis for $C_0$.

**Aside 1.8.** Note that, except for the last few lines, the proof is purely geometric and takes place over an algebraically closed field.[12] This is typical: study of the Riemann hypothesis over finite fields suggests questions in algebraic geometry whose resolution proves the hypothesis.

### Correspondences

A divisor $D$ on a product $C_1 \times C_2$ of curves is said to have *valence zero* if it is linearly equivalent to a sum of divisors of the form $C_1 \times \mathrm{pt}$ and $\mathrm{pt} \times C_2$. The group of correspondences $\mathscr{C}(C_1, C_2)$ is the quotient of the group of divisors on $C_1 \times C_2$ by those of valence zero. When $C_1 = C_2 = C$, the composite of two divisors $D_1$ and $D_2$ is

$$D_1 \circ D_2 \stackrel{\text{def}}{=} p_{13*}(p_{12}^* D_1 \cdot p_{23}^* D_2)$$

where the $p_{ij}$ are the projections $C \times C \times C \to C \times C$; in general, it is only defined up to linear equivalence. When $D \circ E$ is defined, we have

$$\begin{aligned} &d_1(D \circ E) = d_1(D) d_1(E), \quad d_2(D \circ E) = d_2(D) d_2(E), \\ &(D \cdot E) = (D \circ E', \Delta) \end{aligned} \tag{8}$$

where, as usual, $E'$ is obtained from $E$ by reversing the factors. Composition makes the group $\mathscr{C}(C, C)$ of correspondences on $C$ into a ring $\mathscr{R}(C)$.

Following Weil (cf. (2), p. 16), we define the "trace" of a correspondence $D$ on $C$ by

$$\sigma(D) = d_1(D) + d_2(D) - (D \cdot \Delta).$$

Applying (8), we find that

$$\begin{aligned} \sigma(D \circ D') &\stackrel{\text{def}}{=} d_1(D \circ D') + d_2(D \circ D') - ((D \circ D') \cdot \Delta) \\ &= d_1(D) d_2(D) + d_2(D) d_1(D) - (D^2) \\ &= \mathrm{def}(D). \end{aligned}$$

Thus Weil's inequality $\sigma(D \circ D') \ge 0$ is a restatement of (5).

### Sur les Courbes... (Weil 1948a)

In this short book, Weil provides the details for his 1941 proof. He does not use the Riemann-Roch theorem for a surface, which was not available in nonzero characteristic at the time.

Let $C$ be a nonsingular projective curve of genus $g$ over an algebraically closed field $k$. We assume a theory of intersections on $C \times C$, for example, that in Weil 1946 or, more simply, that sketched above (p.17). We briefly sketch Weil's proof that $\sigma(D \circ D') \ge 0$. As we

[12] I once presented this proof in a lecture. At the end, a listener at the back triumphantly announced that I couldn't have proved the Riemann hypothesis because I had only ever worked over an algebraically closed field.

have just seen, this suffices to prove the Riemann hypothesis.

Assume initially that $D$ is positive, that $d_2(D) = g \geq 2$, and that

$$D = D_1 + \cdots + D_g$$

with the $D_i$ distinct. We can regard $D$ as a multivalued map $P \mapsto D(P) = \{D_1(P), \ldots, D_g(P)\}$ from $C$ to $C$. Then

$$\begin{aligned} D(k) &= \{(P, D_i(P)) \mid P \in C(k), \quad 1 \leq i \leq g\} \\ D'(k) &= \{(D_i(P), P) \mid P \in C(k), \quad 1 \leq i \leq g\} \\ \left(D \circ D'\right)(k) &= \{(D_i(P), D_j(P)) \mid P \in C(k), \quad 1 \leq i, j \leq g\}. \end{aligned}$$

The points with $i = j$ contribute a component $Y_1 = d_1(D)\Delta$ to $D \circ D'$, and

$$(Y_1 \cdot \Delta) = d_1(D)(\Delta \cdot \Delta) = d_1(D)(2 - 2g).$$

It remains to estimate $(Y_2 \cdot \Delta)$ where $Y_2 = D - Y_1$. Let $K_C$ denote a positive canonical divisor on $C$, and let $\{\varphi_1, \ldots, \varphi_g\}$ denote a basis for $L(K_C)$. For $P \in C(k)$, let

$$\Phi(P) = \det(\varphi_i(D_j(P))$$

(Weil 1948a, II, n°13, p. 52). Then $\Phi$ is a rational function on $C$, whose divisor we denote $(\Phi) = (\Phi)_0 - (\Phi)_\infty$. The zeros of $\Phi$ correspond to the points $(D_i(P), D_j(P))$ with $D_i(P) = D_j(P)$, $i \neq j$, and so

$$\deg(\Phi)_0 = (Y_2 \cdot \Delta).$$

On the other hand the poles of $\Phi$ are at the points $P$ for which $D_j(P)$ lies in the support of $K_C$, and so

$$\deg(\Phi)_\infty \leq \deg(K_C) d_1(D) = (2g - 2) d_1(D).$$

Therefore,

$$(D \circ D', \Delta) \leq d_1(D)(2 - 2g) + (2g - 2) d_1(D) = 0$$

and so

$$\sigma(D \circ D') \stackrel{\text{def}}{=} d_1(D \circ D') + d_2(D \circ D') - (D \circ D', \Delta) \geq 2g d_1(D) \geq 0.$$

Let $D$ be a divisor on $C \times C$. Then $D$ becomes equivalent to a divisor of the form considered in the last paragraph after we pass to a finite generically Galois covering $V \to C \times C$ (this follows from Weil 1948a, Proposition 3, p. 43). Elements of the Galois group of $k(V)$ over $k(C \times C)$ act on the matrix $(\varphi_i(D_j(P))$ by permuting the columns, and so they leave its determinant unchanged except possibly for a sign. On replacing $\Phi$ with its square, we obtain a rational function on $C \times C$, to which we can apply the above argument. This completes the sketch.

Weil gives a rigorous presentation of the argument just sketched in II, pp. 42–54, of his book 1948a. In fact, he proves the stronger result: $\sigma(\xi \circ \xi') > 0$ for all nonzero $\xi \in \mathscr{R}(C)$ (ibid. Thm 10, p. 54). In the earlier part of the book, Weil (re)proves the Riemann-Roch theorem for curves and develops the theory of correspondences on a curve based on the intersection theory developed in his *Foundations*. In the later part he applies the inequality to obtain his results on the zeta function of $C$, but he defers the proof of his results on Artin $L$-series to his second book.[13]

### Some History

Let $C_1$ and $C_2$ be two nonsingular projective curves over an algebraically closed field $k$. Severi, in his fundamental paper (1903), defined a bi-additive form

$$\sigma(D, E) = d_1(D) d_2(E) + d_2(D) d_1(E) - (D \cdot E)$$

on $\mathscr{C}(C_1, C_2)$ and conjectured that it is non-degenerate. Note that

$$\sigma(D, D) = 2 d_1(D) d_2(D) - (D^2) = \operatorname{def}(D).$$

Castelnuovo (1906) proved the following theorem,

> let $D$ be a divisor on $C_1 \times C_2$; then $\sigma(D, D) \geq 0$, with equality if and only if $D$ has valence zero.[14]

from which he was able to deduce Severi's conjecture. Of course, this all takes place in characteristic zero.

As noted earlier, the Riemann-Roch theorem for surfaces in characteristic $p$ was not available to Weil. The Italian proof of the complex Riemann-Roch theorem rests on a certain lemma of Enriques and Severi. Zariski (1952) extended this lemma to normal varieties of all dimensions in all characteristics; in particular, he obtained a proof of the Riemann-Roch theorem for normal surfaces in characteristic $p$.

Mattuck and Tate (1958) used the Riemann-Roch theorem in the case of a product of two curves to obtain a simple proof of the Castelnuovo-Severi inequality.[15]

---

[13] Serre writes (email July 2015):

> Weil always insisted that Artin's conjecture on the holomorphy of non-abelian $L$-functions is on the same level of difficulty as the Riemann hypothesis. In his book "Courbes algébriques ..." he mentions (on p. 83) that the $L$-functions are polynomials, but he relies on the second volume for the proof (based on the $\ell$-adic representations: the positivity result alone is not enough). I find interesting that, while there are several "elementary" proofs of the Riemann hypothesis for curves, none of them gives that Artin's $L$-functions are polynomial. The only way to prove it is via $\ell$-adic cohomology, or equivalently, $\ell$-adic representations. Curiously, the situation is different over number fields, since we know several non-trivial cases where Artin's conjecture is true (thanks to Langlands theory), and no case where the Riemann hypothesis is!

[14] In fact, Castelnuovo proved a more precise result, which Kani (1984) extended to characteristic $p$, thereby obtaining another proof of the defect inequality in characteristic $p$.

[15] In their introduction, they refer to Weil's 1940 note and write: "the [Castelnuovo-Severi] inequality is really a state-

In trying to understand the exact scope of the method of Mattuck and Tate, Grothendieck (1958a) stumbled on the Hodge index theorem.[16] In particular, he showed that the Castenuovo-Severi-Weil inequality follows from a general statement, valid for all surfaces, which itself is a simple consequence of the Riemann-Roch theorem for surfaces.

The proof presented in the preceding subsection incorporates these simplifications.

#### Variants

Igusa (1949) gave another elaboration of the proof of the Riemann hypothesis for curves sketched in Weil 1941. Following Castelnuovo, he first proves a formula of Schubert, thereby giving the first rigorous proof of this formula valid over an arbitrary field. His proof makes use of the general theory of intersection multiplicities in Weil's *Foundations*.

Intersection multiplicities in which one of the factors is a hypersurface can be developed in an elementary fashion, using little more that the theory of discrete valuations (cf. p. 17). In his 1953 thesis, Weil's student Frank Quigley "arranged" Weil's 1941 proof so that it depends only on this elementary intersection theory (Quigley 1953). As did Igusa, he first proved Schubert's formula.

Finally, in his thesis (Hamburg 1951), Hasse's student Roquette gave a proof of the Riemann hypothesis for curves based on Deuring's theory of correspondences for double-fields (published as Roquette 1953).

#### Applications to Exponential Sums

Davenport and Hasse (1935) showed that certain arithmetic functions can be realized as the traces of Frobenius maps. Weil (1948c) went much further, and showed that all exponential sums in one variable can be realized in this way. From his results on the zeta functions of curves, he obtained new estimates for these sums. Later developments, especially the construction of $\ell$-adic and $p$-adic cohomologies, and Deligne's work on the zeta functions of varieties over finite fields, have made this a fundamental tool in analytic number theory.

ment about the geometry on a very special type of surface—the product of two curves—and it is natural to ask whether it does not follow from the general theory of surfaces." Apparently they had forgotten that Weil had answered this question in 1941!

[16] "En essayant de comprendre la portée exacte de leur méthode, je suis tombé sur l'énoncé suivant, connu en fait depuis 1937 (comme me l'a signalé J. P. Serre), mais apparemment peu connu et utilisé." The Hodge index theorem was first proved by analytic methods in Hodge 1937, and by algebraic methods in Segre 1937 and in Bronowski 1938.

### Foundations of Algebraic Geometry (Weil 1946)

When Weil began the task of constructing foundations for his announcements he was, by his own account, not an expert in algebraic geometry. During a six-month stay in Rome, 1925–1926, he had learnt something of the Italian school of algebraic geometry, but mainly during this period he had studied linear functionals with Vito Volterra.

In writing his Foundations, Weil's main inspiration was the work of van der Waerden,[17] which gives a rigorous algebraic treatment of projective varieties over fields of arbitrary characteristic and develops intersection theory by global methods. However, Weil was unable to construct the jacobian variety of a curve as a projective variety. This forced him to introduce the notion of an abstract variety, defined by an atlas of charts, and to develop his intersection theory by local methods. Without the Zariski topology, his approach was clumsy. However, his "abstract varieties" liberated algebraic geometry from the study of varieties embedding in an affine or projective space. In this respect, his work represents a break with the past.

Weil completed his book in 1944. As Zariski wrote in a review (BAMS 1948):

> In the words of the author the main purpose of this book is "to present a detailed and connected treatment of the properties of intersection multiplicities, which is to include all that is necessary and sufficient to legitimize the use made of these multiplicities in classical algebraic geometry, especially of the Italian school". There can be no doubt whatsoever that this purpose has been fully achieved by Weil. After a long and careful preparation (Chaps. I–IV) he develops in two central chapters (V and VI) an intersection theory which for completeness and generality leaves little to be desired. It goes far beyond the previous treatments of this foundational topic by Severi and van der Waerden and is presented with that absolute rigor to which we are becoming accustomed in algebraic geometry. In harmony with its title the book is entirely self-contained and the subject matter is developed *ab initio*.
>
> It is a remarkable feature of the book that—with one exception (Chap. III)—no use is made of the higher methods of modern algebra. The author has made up his mind not to assume or use modern algebra "beyond the simplest facts about abstract fields and their extensions and the bare rudiments of the theory of ideals." …The author justifies his procedure by an argument of historical continuity, urging a return "to the palaces which are ours by birthright." But it is very unlikely that our predecessors will recognize in Weil's book their own familiar edifice, however improved and completed. If the traditional geometer were invited to choose between "makeshift constructions full of rings, ideals and val-

[17] In the introduction, Weil writes that he "greatly profited from van der Waerden's well-known series of papers (published in Math. Ann. between 1927 and 1938)…; from Severi's sketchy but suggestive treatment of the same subject, in his answer to van der Waerden's criticism of the work of the Italian school; and from the topological theory of intersections, as developed by Lefschetz and other contemporary mathematicians."

uations"[18] on one hand, and constructions full of fields, linearly disjoint fields, regular extensions, independent extensions, generic specializations, finite specializations and specializations of specializations on the other, he most probably would decline the choice and say: "A plague on both your houses!"

For fifteen years, Weil's book provided a secure foundation for work in algebraic geometry, but then was swept away by commutative algebra, sheaves, cohomology, and schemes, and was largely forgotten.[19] For example, his intersection theory plays little role in Fulton 1984. It seems that the approach of van der Waerden and Weil stayed too close to the Italian original with its generic points, specializations, and so on; what algebraic geometry needed was a complete renovation.

### Variétés Abéliennes et ... (Weil 1948b)

In this book and later work, Weil constructs the jacobian variety of a curve, and develops a comprehensive theory of abelian varieties over arbitrary fields, parallel to the transcendental theory over $\mathbb{C}$. Although inspired by his work on the Riemann hypothesis, this work goes far beyond what is needed to justify his 1940 note. Weil's book opened the door to the arithmetic study of abelian varieties. In the twenty years following its publication, almost all of the important results on elliptic curves were generalized to abelian varieties. Before describing two of Weil's most important accomplishments in his book, I list some of these developments.

1.9. There were improvements to the theory of abelian varieties by Weil and others; see (1.19) below.

1.10. Deuring's theory of complex multiplication for elliptic curves was extended to abelian varieties of arbitrary dimension by Shimura, Taniyama, and Weil (see their talks at the Symposium on Algebraic Number Theory, Tokyo & Nikko, 1955).

1.11. For a projective variety $V$, one obtains a height function by choosing a projective embedding of $V$. In 1958 Néron conjectured that for an abelian variety there is a *canonical* height function characterized by having a certain quadratic property. The existence of such a height function was proved independently by Néron and Tate in the early 1960s.

1.12. Tate studied the Galois cohomology of abelian varieties, extending earlier results of Cassels for elliptic curves. This made it possible, for example, to give a simple natural proof of the Mordell-Weil theorem for abelian varieties over global fields.

1.13. Néron (1964) developed a theory of minimal models of abelian varieties over local and global fields, extending Kodaira's theory for elliptic curves over function fields in one variable over $\mathbb{C}$.

1.14. These developments made it possible to state the conjecture of Birch and Swinnerton-Dyer for abelian varieties over global fields (Tate 1966a). The case of a jacobian variety over a global function field inspired the conjecture of Artin-Tate concerning the special values of the zeta function of a surface over a finite field (ibid. Conjecture C).

1.15. Tate (1964) conjectured that, for abelian varieties $A$, $B$ over a field $k$ finitely generated over the prime field, the map

$$\mathbb{Z}_\ell \otimes \operatorname{Hom}(A,B) \to \operatorname{Hom}(T_\ell A, T_\ell B)^{\operatorname{Gal}(k^{\mathrm{sep}}/k)}$$

is an isomorphism. Mumford explained to Tate that, for elliptic curves over a finite field, this follows from the results of Deuring (1941). In one of his most beautiful results, Tate proved the statement for all abelian varieties over finite fields (Tate 1966b). At a key point in the proof, he needed to divide a polarization by $l^n$; for this he was able to appeal to "the proposition on the last page of Weil 1948b".

1.16. (Weil-Tate-Honda theory) Fix a power $q$ of a prime $p$. An element $\pi$ algebraic over $\mathbb{Q}$ is called a *Weil number* if it is integral and $|\rho(\pi)| = q^{1/2}$ for all embeddings $\rho\colon \mathbb{Q}[\pi] \to \mathbb{C}$. Two Weil numbers $\pi$ and $\pi'$ are conjugate if there exists an isomorphism $\mathbb{Q}[\pi] \to \mathbb{Q}[\pi']$ sending $\pi$ to $\pi'$. Weil attached a Weil number to each simple abelian variety over $\mathbb{F}_q$, whose conjugacy class depends only on the isogeny class of the variety, and Tate showed that the map from isogeny classes of simple abelian varieties over $\mathbb{F}_q$ to conjugacy classes of Weil numbers is injective. Using the theory of complex multiplication, Honda (1968) shows that the map is also surjective. In this way, one obtains a classification of the isogeny classes of simple abelian varieties over $\mathbb{F}_q$. Tate determined the endomorphism algebra of simple abelian variety $A$ over $\mathbb{F}_q$ in terms of its Weil number $\pi$: it is a central division algebra over $\mathbb{Q}[\pi]$ which splits at no real prime of $\mathbb{Q}[\pi]$, splits at every finite prime not lying over $p$, and at a prime $v$ above $p$ has invariant

$$\text{(9)} \qquad \operatorname{inv}_v(\operatorname{End}^0(A)) \equiv \frac{\operatorname{ord}_v(\pi)}{\operatorname{ord}_v(q)}[\mathbb{Q}[\pi]_v : \mathbb{Q}_p] \pmod 1;$$

moreover,

$$2\dim(A) = [\operatorname{End}^0(A) : \mathbb{Q}[\pi]]^{1/2} \cdot [\mathbb{Q}[\pi] : \mathbb{Q}].$$

Here $\operatorname{End}^0(A) = \operatorname{End}(A) \otimes \mathbb{Q}$. See Tate 1968.

#### Iwasawa Theory Foretold

Weil was very interested in the analogy between number fields and function fields and, in particular, in "extending" results from function fields to number fields. In 1942 he wrote:

[18] Weil's description of Zariski's approach to the foundations.

[19] When Langlands decided to learn algebraic geometry in Berkeley in 1964–1965, he read Weil's *Foundations*... and Conforto's *Abelsche Funktionen*... A year later, as a student at Harvard, I was able to attend Mumford's course on algebraic geometry which used commutative algebra, sheaves, and schemes.

Our proof for the Riemann hypothesis depended upon the extension of the function-fields by roots of unity, i.e., by constants; the way in which the Galois group of such extensions operates on the classes of divisors in the original field and its extensions gives a linear operator, the characteristic roots (i.e., the eigenvalues) of which are the roots of the zeta-function. On a number field, the nearest we can get to this is by the adjunction of $l^n$-th roots of unity, $l$ being fixed; the Galois group of this infinite extension is cyclic, and defines a linear operator on the projective limit of the (absolute) class groups of those successive finite extensions; this should have something to do with the roots of the zeta-function of the field. (Letter to Artin, Œuvres I, p. 298, 1942.)

## Construction of the Jacobian Variety of a Curve

Let $C$ be a nonsingular projective curve over a field $k$, which for simplicity we take to be algebraically closed. The jacobian variety $J$ of $C$ should be such that $J(k)$ is the group $\mathrm{Jac}(C)$ of linear equivalence classes of divisors on $C$ of degree zero. Thus, the problem Weil faced was that of realizing the abstract group $\mathrm{Jac}(C)$ as a projective variety in some natural way—over $\mathbb{C}$ the theta functions provide a projective embedding of $\mathrm{Jac}(C)$. He was not able to do this, but as he writes (Œuvres I, p. 556):

In the spring of 1941, I was living in Princeton… I often worked in Chevalley's office in Fine Hall; of course he was aware of my attempts to "define" the jacobian, i.e., to construct algebraically a projective embedding. One day, coming into his office, I surprised him by telling him that there was no need; for the jacobian everything comes down to its local properties, and a piece of the jacobian, joined to the group property (the addition of divisor classes) suffices amply for that. The idea came to me on the way to Fine Hall. It was both the concept of an "abstract variety" which had just taken shape, and the construction of the jacobian as an algebraic group.[20]

In order to explain Weil's idea, we need the notion of a *birational group* over $k$. This is a nonsingular variety $V$ together with a rational map $m\colon V\times V \dashrightarrow V$ such that

(a) $m$ is associative (that is, $(ab)c = a(bc)$ whenever both terms are defined);
(b) the rational maps $(a,b)\mapsto(a,ab)$ and $(a,b)\mapsto(b,ab)$ from $V\times V$ to $V\times V$ are both birational.

**Theorem 1.17.** *Let $(V,m)$ be a birational group $V$ over $k$. Then there exists a group variety $G$ over $k$ and a birational map $f\colon V \dashrightarrow G$ such that $f(ab)=f(a)f(b)$ whenever $ab$ is defined; the pair $(G,f)$ is unique up to a unique isomorphism. (Weil 1948b, n° 33, Thm 15; Weil 1955.)*

Let $C^{(g)}$ denote the symmetric product of $g$ copies of $C$, i.e., the quotient of $C^g$ by the action of the symmetric group $S_g$. It is a smooth variety of dimension $g$ over $k$. The set $C^{(g)}(k)$ consists of the unordered $g$-tuples of closed points on $C$, which we can regard as positive divisors of degree $g$ on $C$.

Fix a $P\in C(k)$. Let $D$ be a positive divisor of degree $g$ on $C$. According to the Riemann-Roch theorem

$$l(D)=1+l(K_C-D)\geq 1,$$

and one can show that equality holds on a dense open subset of $C^{(g)}$. Similarly, if $D$ is a positive divisor of degree $2g$ on $C$, then $l(D-gP)\geq 1$ and equality holds on a nonempty open subset $U'$ of $C^{(2g)}$. Let $U$ be the inverse image of $U'$ under the obvious map $C^{(g)}\times C^{(g)}\to C^{(2g)}$. Then $U$ is a dense open subset of $C^{(g)}\times C^{(g)}$ with the property that $l(D+D'-gP)=1$ for all $(D,D')\in U(k)$.

Now let $(D,D')\in U(k)$. Because $l(D+D'-gP)>0$, there exists a positive divisor $D''$ on $C$ linearly equivalent to $D+D'-gP$, and because $l(D+D'-gP)=1$, the divisor $D''$ is unique. Therefore, there is a well-defined law of composition

$$(D,D')\mapsto D''\colon U\times U\to C^{(g)}(k).$$

**Theorem 1.18.** *There exists a unique rational map*

$$m\colon C^{(g)}\times C^{(g)} \dashrightarrow C^{(g)}$$

*whose domain of definition contains the subset $U$ and which is such that, for all fields $K$ containing $k$ and all $(D,D')$ in $U(K)$, $m(D,D')\sim D+D'-gP$; moreover $m$ makes $C^{(g)}$ into a birational group.*

This can be proved, according to taste, by using generic points (Weil 1948b) or functors (Milne 1986). On combining the two theorems, we obtain a group variety $J$ over $k$ birationally equivalent to $C^{(g)}$ with its partial group structure. This is the jacobian variety.

### Notes

1.19. Weil (1948b Thm 16, et seqq.) proved that the jacobian variety is complete, a notion that he himself had introduced. Chow (1954) gave a direct construction of the jacobian variety as a projective variety over the same base field as the curve. Weil (1950) announced the existence of two abelian varieties attached to a complete normal algebraic variety, namely, a Picard variety and an Albanese variety. For a curve, both varieties equal the jacobian variety, but in general they are distinct dual abelian varieties. This led to a series of papers on these topics (Matsusaka, Chow, Chevalley, Nishi, Cartier, …) culminating in Grothendieck's general construction of the Picard scheme (see Kleiman 2005).

[20] En ce printemps de 1941, je vivais à Princeton… Je travaillais souvent dans le bureau de Chevalley à Fine Hall; bien entendu il était au courant de mes tentatives pour "définir" la jacobienne, c'est-à-dire pour en construire algébriquement un plongement projectif. Un jour, entrant chez lui, je le surpris en lui disant qu'il n'en était nul besoin; sur la jacobienne tout se ramène à des propriétés locales, et un morceau de jacobienne, joint à la propriété de groupe (l'addition des classes de diviseurs) y suffit amplement. L'idée m'en était venue sur le chemin de Fine Hall. C'était à la fois la notion de "variété abstraite" qui venait de prendre forme, et la construction de la jacobienne en tant que groupe algébrique, telle qu'elle figure dans [1948b].

1.20. Weil's construction of an algebraic group from a birational group has proved useful in other contexts, for example, in the construction of the Néron model of abelian variety (Néron 1964; Artin 1964, 1986; Bosch et al. 1990, Chapter 5).

## The Endomorphism Algebra of an Abelian Variety

The exposition in this subsection includes improvements explained by Weil in his course at the University of Chicago, 1954–1955, and other articles, which were incorporated in Lang 1959. In particular, we use that an abelian variety admits a projective embedding, and we use the following consequence of the theorem of the cube: Let $f,g,h$ be regular maps from a variety $V$ to an abelian variety $A$, and let $D$ be a divisor on $A$; then

$$(10)\quad (f+g+h)^*D-(f+g)^*D-(g+h)^*D-(f+h)^*D \\ +f^*D+g^*D+h^*D\sim 0.$$

We shall also need to use the intersection theory for divisors on smooth projective varieties. As noted earlier, this is quite elementary.

### Review of the Theory Over $\mathbb{C}$

Let $A$ be an abelian variety of dimension $g$ over $\mathbb{C}$. Then $A(\mathbb{C})\simeq T/\Lambda$ where $T$ is the tangent space to $A$ at $0$, and $\Lambda=H_1(A,\mathbb{Z})$. The endomorphism ring $\mathrm{End}(A)$ of $A$ acts faithfully on $\Lambda$, and so it is a free $\mathbb{Z}$-module of rank $\leq 4g$. We define the characteristic polynomial $P_\alpha(T)$ of an endomorphism $\alpha$ of $A$ to be its characteristic polynomial $\det(T-\alpha\mid\Lambda)$ on $\Lambda$. It is the unique polynomial in $\mathbb{Z}[T]$ such that

$$P_\alpha(m)=\deg(m-\alpha)$$

for all $m\in\mathbb{Z}$. It can also be described as the characteristic polynomial of $\alpha$ acting on $A(\mathbb{C})_{\mathrm{tors}}\simeq(\mathbb{Q}\otimes\Lambda)/\Lambda$.[21]

Choose a Riemann form for $A$. Let $H$ be the associated positive-definite hermitian form on the complex vector space $T$ and let $\alpha\mapsto\alpha^\dagger$ be the associated Rosati involution on $\mathrm{End}^0(A)\overset{\mathrm{def}}{=}\mathrm{End}(A)\otimes\mathbb{Q}$. Then

$$H(\alpha x,y)=H(x,\alpha^\dagger y),\quad \text{all } x,y\in T,\ \alpha\in\mathrm{End}^0(A),$$

and so $^\dagger$ is a positive involution on $\mathrm{End}^0(A)$, i.e., the trace pairing

$$(\alpha,\beta)\mapsto\mathrm{Tr}(\alpha\circ\beta^\dagger)\colon\ \mathrm{End}^0(A)\times\mathrm{End}^0(A)\to\mathbb{Q}$$

is positive definite (see, for example, Rosen 1986).

Remarkably, Weil was able to extend these statements to abelian varieties over arbitrary base fields.

21 Choose an isomorphism $(\mathbb{Q}\otimes\Lambda/\Lambda)\to(\mathbb{Q}/\mathbb{Z})^{2g}$, and note that $\mathrm{End}(\mathbb{Q}/\mathbb{Z})\simeq\hat{\mathbb{Z}}$. The action of $\alpha$ on $\mathbb{Q}\otimes\Lambda/\Lambda$ defines an element of $M_{2g}(\hat{\mathbb{Z}})$, whose characteristic polynomial is $P_\alpha(T)$.

### The Characteristic Polynomial of an Endomorphism

**Proposition 1.21.** *For all integers $n\geq 1$, the map $n_A\colon A\to A$ has degree $n^{2g}$. Therefore, for $\ell\neq\mathrm{char}(k)$, the $\mathbb{Z}_\ell$-module $T_\ell A\overset{\mathrm{def}}{=}\varprojlim_n A_{\ell^n}(k^{\mathrm{al}})$ is free of rank $2g$.*

*Proof.* Let $D$ be an ample divisor on $A$ (e.g., a hyperplane section under some projective embedding); then $D^g$ is a positive zero-cycle, and $(D^g)\neq 0$. After possibly replacing $D$ with $D+(-1)_A^*D$, we may suppose that $D$ is symmetric, i.e., $D\sim(-1)_A^*D$. An induction argument using (10) shows that $n_A^*D\sim n^2D$, and so

$$(n_A^*D^g)=(n_A^*D\cdot\ldots\cdot n_A^*D)\sim(n^2D\cdot\ldots\cdot n^2D)\sim n^{2g}(D^g).$$

Therefore $n_A^*$ has degree $n^{2g}$. □

A map $f\colon W\to Q$ on a vector space $W$ over a field $Q$ is said to be *polynomial (of degree $d$)* if, for every finite linearly independent set $\{e_1,\ldots,e_n\}$ of elements of $V$,

$$f(a_1e_1+\cdots+a_ne_n)=P(a_1,\ldots,a_n),\quad x_i\in Q,$$

for some $P\in Q[X_1,\ldots,X_n]$ (of degree $d$). To show that a map $f$ is polynomial, it suffices to check that, for all $v,w\in W$, the map $x\mapsto f(xv+w)\colon Q\to Q$ is a polynomial in $x$.

**Lemma 1.22.** *Let $A$ be an abelian variety of dimension $g$. The map $\alpha\mapsto\deg(\alpha)\colon\ \mathrm{End}^0(A)\to\mathbb{Q}$ is a polynomial function of degree $2g$ on $\mathrm{End}^0(A)$.*

*Proof.* Note that $\deg(n\beta)=\deg(n_A)\deg(\beta)=n^{2g}\deg(\beta)$, and so it suffices to prove that $\deg(n\beta+\alpha)$ (for $n\in\mathbb{Z}$ and $\beta,\alpha\in\mathrm{End}(A)$) is polynomial in $n$ of degree $\leq 2g$. Let $D$ be a symmetric ample divisor on $A$. A direct calculation using (10) shows shows that

$$(11)\quad \deg(n\beta+\alpha)(D^g) \\ =(n(n-1))^g(D^g)+\text{terms of lower degree in } n.$$

As $(D^g)\neq 0$ this completes the proof. □

**Theorem 1.23.** *Let $\alpha\in\mathrm{End}(A)$. There is a unique monic polynomial $P_\alpha(T)\in\mathbb{Z}[T]$ of degree $2g$ such that $P_\alpha(n)=\deg(n_A-\alpha)$ for all integers $n$.*

*Proof.* If $P_1$ and $P_2$ both have this property, then $P_1-P_2$ has infinitely many roots, and so is zero. For the existence, take $\beta=1_A$ in (11). □

We call $P_\alpha$ the *characteristic polynomial* of $\alpha$ and we define the *trace* $\mathrm{Tr}(\alpha)$ of $\alpha$ by the equation

$$P_\alpha(T)=T^{2g}-\mathrm{Tr}(\alpha)T^{2g-1}+\cdots+\deg(\alpha).$$

### The Endomorphism Ring of an Abelian Variety

Let $A$ and $B$ be abelian varieties over $k$, and let $\ell$ be a prime $\neq\mathrm{char}(k)$. The family of $\ell$-power torsion points in $A(k^{\mathrm{al}})$ is dense, and so the map

$$\mathrm{Hom}(A,B) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$$

is injective. Unfortunately, this doesn't show that $\mathrm{Hom}(A,B)$ is finitely generated over $\mathbb{Z}$.

**Lemma 1.24.** *Let $\alpha \in \mathrm{Hom}(A,B)$; if $\alpha$ is divisible by $\ell^n$ in $\mathrm{Hom}(T_\ell A, T_\ell B)$, then it is divisible by $\ell^n$ in $\mathrm{Hom}(A,B)$.*

*Proof.* For each $n$, there is an exact sequence

$$0 \to A_{\ell^n} \to A \xrightarrow{\ell^n} A \to 0.$$

The hypothesis implies that $\alpha$ is zero on $A_{\ell^n}$, and so it factors through the quotient map $A \xrightarrow{\ell^n} A$. □

**Theorem 1.25.** *The natural map*

$$\mathbb{Z}_\ell \otimes \mathrm{Hom}(A,B) \to \mathrm{Hom}(T_\ell A, T_\ell B) \tag{12}$$

*is injective (with torsion-free cokernel). Hence $\mathrm{Hom}(A,B)$ is a free $\mathbb{Z}$-module of finite rank $\leq 4\dim(A)\dim(B)$.*

*Proof.* The essential case is that with $A = B$ and $A$ simple. Let $e_1,\ldots,e_m$ be elements of $\mathrm{End}(A)$ linearly independent over $\mathbb{Z}$; we have to show that $T_\ell(e_1),\ldots,T_\ell(e_m)$ are linearly independent over $\mathbb{Z}_\ell$.

Let $M$ (resp. $\mathbb{Q}M$) denote the $\mathbb{Z}$-module (resp. $\mathbb{Q}$-vector space) generated in $\mathrm{End}^0(A)$ by the $e_i$. Because $A$ is simple, every nonzero endomorphism $\alpha$ of $A$ is an isogeny, and so $\deg(\alpha)$ is an integer $> 0$. The map $\deg\colon \mathbb{Q}M \to \mathbb{Q}$ is continuous for the real topology because it is a polynomial function (1.22), and so $U \stackrel{\text{def}}{=} \{\alpha \in \mathbb{Q}M \mid \deg(\alpha) < 1\}$ is an open neighbourhood of 0. As

$$(\mathbb{Q}M \cap \mathrm{End}(A)) \cap U \subset \mathrm{End}(A) \cap U = 0,$$

we see that $\mathbb{Q}M \cap \mathrm{End}(A)$ is discrete in $\mathbb{Q}M$, which implies that it is finitely generated as a $\mathbb{Z}$-module. Hence there exists an integer $N > 0$ such that

$$N(\mathbb{Q}M \cap \mathrm{End}(A)) \subset M. \tag{13}$$

Suppose that there exist $a_i \in \mathbb{Z}_\ell$, not all zero, such that $\sum a_i T_\ell(e_i) = 0$. For a fixed $m \in \mathbb{N}$, we can find integers $n_i$ sufficiently close to the $a_i$ that the sum $\sum n_i e_i$ is divisible by $\ell^m$ in $\mathrm{End}(T_\ell A)$, and hence in $\mathrm{End}(A)$. Therefore

$$\sum (n_i/\ell^m) e_i \in \mathbb{Q}M \cap \mathrm{End}(A),$$

and so $N\sum(n_i/\ell^m)e_i \in M$, i.e., $n_i N/\ell^m \in \mathbb{Z}$ and $\mathrm{ord}_\ell(n_i) + \mathrm{ord}_\ell(N) \geq m$ for all $i$. But if $n_i$ is close to $a_i$, then $\mathrm{ord}_\ell(n_i) = \mathrm{ord}_\ell(a_i)$, and so $\mathrm{ord}_\ell(a_i) + \mathrm{ord}_\ell(N) \geq m$. As $m$ was arbitrary, we have a contradiction. □

### The $\ell$-Adic Representation

**Proposition 1.26.** *For all $\ell \neq \mathrm{char}(k)$, $P_\alpha(T)$ is the characteristic polynomial of $\alpha$ acting on $T_\ell A$; in particular, $\det(\alpha \mid T_\ell A) = \deg(\alpha)$.*

*Proof.* For an endomorphism $\alpha$ of $A$,

$$|\det(T_\ell \alpha)|_\ell = |\deg(\alpha)|_\ell. \tag{14}$$

To continue, we shall need an elementary lemma (Weil 1948b, n°68, Lemme 12):

> A polynomial $P(T) \in \mathbb{Q}_\ell[T]$, with roots $a_1,\ldots,a_d$ in $\mathbb{Q}_\ell^{\mathrm{al}}$, is uniquely determined by the numbers $\left|\prod_{i=1}^d F(a_i)\right|_\ell$ as $F$ runs through the elements of $\mathbb{Z}[T]$.

For the polynomial $P_\alpha(T)$,

$$\prod_{i=1}^d F(a_i) = \pm\deg(F(\alpha)),$$

and for the characteristic polynomial $P_{\alpha,\ell}(T)$ of $\alpha$ on $T_\ell A$,

$$\left|\prod_{i=1}^d F(a_i)\right|_\ell = |\det(F(T_\ell \alpha))|_\ell.$$

Therefore, (14) shows that $P_\alpha(T)$ and $P_{\alpha,\ell}(T)$ coincide as elements of $\mathbb{Q}_\ell[T]$. □

### Positivity

An ample divisor $D$ on $A$ defines an isogeny $\varphi_D\colon A \to A^\vee$ from $A$ to the dual abelian variety $A^\vee \stackrel{\text{def}}{=} \mathrm{Pic}^0(A)$, namely, $a \mapsto [D_a - D]$ where $D_a$ is the translate of $D$ by $a$. A polarization of $A$ is an isogeny $\lambda\colon A \to A^\vee$ that becomes of the form $\varphi_D$ over $k^{\mathrm{al}}$. As $\lambda$ is an isogeny, it has an inverse in $\mathrm{Hom}^0(A^\vee, A)$. The Rosati involution on $\mathrm{End}^0(A)$ corresponding to $\lambda$ is

$$\alpha \mapsto \alpha^\dagger \stackrel{\text{def}}{=} \lambda^{-1} \circ \alpha^\vee \circ \lambda.$$

It has the following properties:

$$(\alpha+\beta)^\dagger = \alpha^\dagger + \beta^\dagger, \quad (\alpha\beta)^\dagger = \beta^\dagger\alpha^\dagger, \quad a^\dagger = a \text{ for all } a \in \mathbb{Q}.$$

**Theorem 1.27.** *The Rosati involution on $E \stackrel{\text{def}}{=} \mathrm{End}^0(A)$ is positive, i.e., the pairing*

$$\alpha,\beta \mapsto \mathrm{Tr}_{E/\mathbb{Q}}(\alpha \circ \beta^\dagger)\colon E \times E \to \mathbb{Q}$$

*is positive definite.*

*Proof.* We have to show that $\mathrm{Tr}(\alpha \circ \alpha^\dagger) > 0$ for all $\alpha \neq 0$. Let $D$ be the ample divisor corresponding to the polarization used in the definition of †. A direct calculation shows that

$$\mathrm{Tr}(\alpha \circ \alpha^\dagger) = \frac{2g}{(D^g)}(D^{g-1} \cdot \alpha^{-1}(D))$$

(Lang 1959, V, §3, Thm 1). I claim that $(D^{g-1} \cdot \alpha^{-1}(D)) > 0$. We may suppose that $D$ is a hyperplane section of $A$ relative to some projective embedding. There exist hyperplane sections $H_1,\ldots,H_{g-1}$ such that $H_1 \cap \ldots \cap H_{g-1} \cap \alpha^{-1}D$ has dimension zero. By dimension theory, the intersection is nonempty, and so

$$(H_1 \cdot \ldots \cdot H_{g-1} \cdot \alpha^{-1}D) > 0.$$

As $D \sim H_i$ for all $i$, we have $(D^{g-1} \cdot \alpha^{-1} D) = (H_1 \cdot \ldots \cdot H_{g-1} \cdot \alpha^{-1} D) > 0$. □

Recall that the *radical* $\mathrm{rad}(R)$ of a ring $R$ is the intersection of the maximal left ideals in $R$. It is a two-sided ideal, and it is nilpotent if $R$ is artinian. An algebra $R$ of finite dimension over a field $Q$ is semisimple if and only if $\mathrm{rad}(R) = 0$.

**Corollary 1.28.** *The $\mathbb{Q}$-algebra $\mathrm{End}^0(A)$ is semisimple.*

*Proof.* If not, the radical of $\mathrm{End}^0(A)$ contains a nonzero element $\alpha$. As $\beta \overset{\text{def}}{=} \alpha\alpha^\dagger$ has nonzero trace, it is a nonzero element of the radical. It is symmetric, and so $\beta^2 = \beta\beta^\dagger \neq 0$, $\beta^4 = (\beta^2)^2 \neq 0$, .... Therefore $\beta$ is not nilpotent, which is a contradiction. □

**Corollary 1.29.** *Let $\alpha$ be an endomorphism of $A$ such that $\alpha \circ \alpha^\dagger = q_A$, $q \in \mathbb{Z}$. For every homomorphism $\rho\colon \mathbb{Q}[\alpha] \to \mathbb{C}$,*

$$\rho(\alpha^\dagger) = \overline{\rho(\alpha)} \text{ and } |\rho\alpha| = q^{1/2}.$$

*Proof.* As $\mathbb{Q}[\alpha]$ is stable under $^\dagger$, it is semisimple, and hence a product of fields. Therefore $\mathbb{R} \otimes \mathbb{Q}[\alpha]$ is a product of copies of $\mathbb{R}$ and $\mathbb{C}$. The involution $^\dagger$ on $\mathbb{Q}[\alpha]$ extends by continuity to an involution of $\mathbb{R} \otimes \mathbb{Q}[\alpha]$ having the property that $\mathrm{Tr}(\beta \circ \beta^\dagger) \geq 0$ for all $\beta \in \mathbb{R} \otimes \mathbb{Q}[\alpha]$ with inequality holding on a dense subset. The only such involution preserves the each factor and acts as the identity on the real factors and as complex conjugation on the complex factors. This proves the first statement, and the second follows:

$$q = \rho(q_A) = \rho(\alpha \circ \alpha^\dagger) = \rho(\alpha) \cdot \overline{\rho(\alpha)} = \left|\rho(\alpha)^2\right|. \qquad \square$$

**Theorem 1.30.** *Let $A$ be an abelian variety over $k = \mathbb{F}_q$, and let $\pi \in \mathrm{End}(A)$ be the Frobenius endomorphism. Let $^\dagger$ be a Rosati involution on $\mathrm{End}^0(A)$. For every homomorphism $\rho\colon \mathbb{Q}[\pi] \to \mathbb{C}$,*

$$\rho(\alpha^\dagger) = \overline{\rho(\pi)} \text{ and } |\rho\pi| = q^{1/2}.$$

*Proof.* This will follow from (1.29) once we show that $\pi \circ \pi^\dagger = q_A$. This can be proved by a direct calculation, but it is more instructive to use the Weil pairing. Let $\lambda$ be the polarization defining $^\dagger$. The Weil pairing is a nondegenerate skew-symmetric pairing

$$e^\lambda\colon T_l A \times T_l A \to T_l \mathbb{G}_m$$

with the property that

$$e^\lambda(\alpha x, y) = e^\lambda(x, \alpha^\dagger y) \qquad (x, y \in T_l A, \quad \alpha \in \mathrm{End}(A)).$$

Now

$$\begin{aligned} &e^\lambda(x, (\pi^\dagger \circ \pi) y) \\ &\quad = e^\lambda(\pi x, \pi y) = \pi e^\lambda(x, y) = q e^\lambda(x, y) = e^\lambda(x, q_A y). \end{aligned}$$

Therefore $\pi^\dagger \circ \pi$ and $q_A$ agree as endomorphisms of $T_l A$, and hence as endomorphisms of $A$. □

The Riemann hypothesis for a curve follows from applying (1.30) to the jacobian variety of $C$.

**Summary 1.31.** Let $A$ be an abelian variety of dimension $g$ over $k = \mathbb{F}_q$, and let $P(T)$ be the characteristic polynomial of the Frobenius endomorphism $\pi$. Then $P(T)$ is a monic polynomial of degree $2g$ with integer coefficients, and its roots $a_1, \ldots, a_{2g}$ have absolute value $q^{1/2}$. For all $\ell \neq p$,

$$P(T) = \det(T - \pi \mid V_\ell A), \quad V_\ell A \overset{\text{def}}{=} T_\ell A \otimes \mathbb{Q}_\ell.$$

For all $n \geq 1$,

$$\prod_{i=1}^{2g} (1 - a_i^n) = |A(k_n)| \quad \text{where } [k_n\colon k] = n, \tag{15}$$

and this condition determines $P$. We have

$$P(T) = q^g \cdot T^{2g} \cdot P(1/qT).$$

**Notes.** Essentially everything in this subsection is in Weil 1948b, but, as noted at the start, some of the proofs have been simplified by using Weil's later work. In 1948 Weil didn't know that abelian varieties are projective, and he proved (1.27) first for jacobians, where the Rosati involution is obvious. The more direct proof of (1.27) given above is from Lang 1957.

### The Weil Conjectures (Weil 1949)

Weil studied equations of the form

$$a_0 X_0^{m_0} + \cdots + a_r X_r^{m_r} = b \tag{16}$$

over a finite field $k$, and obtained an expression in terms of Gauss sums for the number of solutions in $k$. Using a relation, due to Davenport and Hasse (1935), between Gauss sums in a finite field and in its extensions, he was able to obtain a simple expression for the formal power series ("generating function")

$$\sum_1^\infty (\#\text{ solutions of (16) in } k_n)\, T^n.$$

In the homogeneous case

$$a_0 X_0^m + \cdots + a_r X_r^m = 0, \tag{17}$$

he found that

$$\begin{aligned} \sum_1^\infty N_n T^{n-1} &= \frac{d}{dT} \log\left(\frac{1}{(1-T)\cdots(1-q^{r-1}T)}\right) \\ &\quad + (-1)^r \frac{d}{dT} \log P(T) \end{aligned}$$

where $P(T)$ is a polynomial of degree $A$ equal to the number of solutions in rational numbers $\alpha_i$ of the system $n\alpha_i \equiv 1$, $\sum \alpha_i \equiv 0 \pmod 1$, $0 < \alpha_i < 1$. Dolbeault was able to tell Weil that the Betti numbers of a hypersurface defined by an equation of the form (17) over $\mathbb{C}$ are the coefficients of the polynomial

$$1+T^2+\cdots+T^{2r-2}+AT^r.$$

As he wrote (1949, p. 409):

> This, and other examples which we cannot discuss here, seems to lend some support to the following conjectural statements, which are known to be true for curves, but which I have not so far been able to prove for varieties of higher dimension.[22]

**Weil Conjectures.** Let $V$ be a nonsingular projective variety of dimension $d$ defined over a finite field $k$ with $q$ elements. Let $N_n$ denote the number points of $V$ rational over the extension of $k$ of degree $n$. Define the zeta function of $C$ to be the power series $Z(V,T)\in\mathbb{Q}[[T]]$ such that

$$\frac{d\log Z(V,T)}{dT}=\sum_1^\infty N_nT^{n-1}. \tag{18}$$

Then:

(W1) (rationality) $Z(V,T)$ is a rational function in $T$;

(W2) (functional equation) $Z(V,T)$ satisfies the functional equation

$$Z(V,1/q^dT)=\pm q^{d\chi/2}\cdot T^\chi\cdot Z(V,T) \tag{19}$$

with $\chi$ equal to the Euler-Poincaré characteristic of $V$ (intersection number of the diagonal with itself);

(W3) (integrality) we have

$$Z(V,T)=\frac{P_1(T)\cdots P_{2d-1}(T)}{(1-T)P_3(T)\cdots(1-q^dT)} \tag{20}$$

with $P_r(T)\in\mathbb{Z}[T]$ for all $r$;

(W4) (Riemann hypothesis) write $P_r(T)=\prod_1^{B_r}(1-\alpha_{ri}T)$; then

$$|\alpha_{ri}|=q^{r/2}$$

for all $r$, $i$;

(W5) (Betti numbers) call the degrees $B_r$ of the polynomials $P_r$ the *Betti numbers* of $V$; if $V$ is obtained by reduction modulo a prime ideal $\mathfrak{p}$ in a number field $K$ from a nonsingular projective variety $\tilde{V}$ over $K$, then the Betti numbers of $V$ are equal to the Betti numbers of $\tilde{V}$ (i.e., of the complex manifold $\tilde{V}(\mathbb{C})$).

Weil's considerations led him to the conclusion, startling at the time, that the "Betti numbers" of an algebraic variety have a purely algebraic meaning. For a curve $C$, the Betti numbers are $1$, $2g$, $1$ where $g$ is the smallest natural number for which the Riemann inequality

$$l(D)\geq\deg(D)-g+1$$

holds, but for dimension $>1$?

No cohomology groups appear in Weil's article and no cohomology theory is conjectured to exist,[23] but Weil was certainly aware that cohomology provides a heuristic explanation of (W1–W3). For example, let $\varphi$ be a finite map of degree $\delta$ from a nonsingular complete variety $V$ to itself over $\mathbb{C}$. For each $n$, let $N_n$ be the number of solutions, supposed finite, of the equation $P=\varphi^n(P)$ or, better, the intersection number $(\Delta\cdot\Gamma_{\varphi^n})$. Then standard arguments show that the power series $Z(T)$ defined by (18) satisfies the functional equation

$$Z(1/\delta T)=\pm(\delta^{1/2}T)^\chi\cdot Z(T) \tag{21}$$

where $\chi$ is the Euler-Poincaré characteristic of $V$ (Weil, Œuvres I, p. 568). For a variety $V$ of dimension $d$, the Frobenius map has degree $q^d$, and so (21) suggests (19).

**Example 1.32.** Let $A$ be an abelian variety of dimension $g$ over a field $k$ with $q$ elements, and let $a_1,\ldots,a_{2g}$ be the roots of the characteristic polynomial of the Frobenius map. Let $P_r(T)=\prod(1-a_{i,r}T)$ where the $a_{i,r}$ run through the products

$$a_{i_1}\cdots a_{i_r},\quad 0<i_1<\cdots<i_r\leq 2g.$$

It follows from (15) that

$$Z(A,T)=\frac{P_1(T)\cdots P_{2g-1}(T)}{(1-T)P_3(T)\cdots(1-q^gT)}.$$

The $r$th Betti number of an abelian variety of dimension $g$ over $\mathbb{C}$ is $\binom{g}{r}$, which equals $\deg(P_r)$, and so the Weil conjectures hold for $A$.

**Aside 1.33.** To say that $Z(V,T)$ is rational means that there exist elements $c_1,\ldots,c_m\in\mathbb{Q}$, not all zero, and an integer $n_0$ such that, for all $n\geq n_0$,

$$c_1N_n+c_2N_{n+1}+\cdots+c_mN_{n+m-1}=0.$$

In particular, the set of $N_n$ can be computed inductively from a finite subset.

## 2. Weil Cohomology

After Weil stated his conjectures, the conventional wisdom eventually became that, in order to

[22] Weil's offhand announcement of the conjectures misled one reviewer into stating that "the purpose of this paper is to give an exposition of known results concerning the equation $a_0X_0^{m_0}+\cdots+a_rX_r^{m_r}=b$" (MR 29393).

[23] Weil may have been aware that there cannot exist a good cohomology theory with $\mathbb{Q}$-coefficients; see (2.2). Recall also that Weil was careful to distinguish conjecture from speculation.

prove the rationality of the zeta functions, it was necessary to define a good "Weil cohomology theory" for algebraic varieties. In 1959, Dwork surprised everyone by finding an elementary proof, depending only on $p$-adic analysis, of the rationality of the zeta function of an arbitrary variety over a finite field (Dwork 1960).[24] Nevertheless, a complete understanding of the zeta function requires a cohomology theory, whose interest anyway transcends zeta functions, and so the search continued.

After listing the axioms for a Weil cohomology theory, we explain how the existence of such a theory implies the first three Weil conjectures. Then we describe the standard Weil cohomologies.

For a smooth projective variety $V$, we write $C^r_{\mathrm{rat}}(V)$ for the $\mathbb{Q}$-vector space of algebraic cycles of codimension $r$ (with $\mathbb{Q}$-coefficients) modulo rational equivalence.

## The Axioms for a Weil Cohomology Theory

We fix an algebraically closed "base" field $k$ and a "coefficient" field $Q$ of characteristic zero. A *Weil cohomology theory* is a contravariant functor $V \rightsquigarrow H^*(V)$ from the category of nonsingular projective varieties over $k$ to the category of finite-dimensional, graded, anti-commutative $Q$-algebras carrying disjoint unions to direct sums and admitting a Poincaré duality, a Künneth formula, and a cycle map in the following sense.

**Poincaré duality.** Let $V$ be connected of dimension $d$.

(a) The $Q$-vector spaces $H^r(V)$ are zero except for $0 \le r \le 2d$, and $H^{2d}(V)$ has dimension 1.

(b) Let $Q(-1) = H^2(\mathbb{P}^1)$, and let $Q(1)$ denote its dual. For a $Q$-vector space $V$ and integer $m$, we let $V(m)$ equal $V \otimes_Q Q(1)^{\otimes m}$ or $V \otimes_Q Q(-1)^{\otimes -m}$ according as $m$ is positive or negative. For each $V$, there is given a natural isomorphism $\eta_V : H^{2d}(V)(d) \to Q$.

(c) The pairings

$$H^r(V) \times H^{2d-r}(V)(d) \to H^{2d}(V)(d) \simeq Q \tag{22}$$

induced by the product structure on $H^*(V)$ are non-degenerate.

[24] "His method consists in assuming that the variety is a hypersurface in affine space (every variety is birationally isomorphic to such a hypersurface, and an easy unscrewing lets us pass from there to the general case); in this case he does a computation with "Gauss sums" analogous to that of Weil for an equation $\sum a_i x_i^{n_i} = b$. Of course, Weil himself had tried to extend his method and had got nowhere…" Serre, *Grothendieck-Serre Correspondence* p. 102. Dwork expressed $Z(V,T)$ as a quotient of two $p$-adically entire functions, and showed that every such function with nonzero radius of convergence is rational.

**Künneth formula.** Let $p,q\colon V \times W \rightrightarrows V,W$ be the projection maps. Then the map

$$x \otimes y \mapsto p^*x \cdot q^*y : H^*(V) \otimes H^*(W) \to H^*(V \times W)$$

is an isomorphism of graded $Q$-algebras.

**Cycle map.** There are given group homomorphisms

$$cl_V : C^r_{\mathrm{rat}}(V) \to H^{2r}(V)(r)$$

satisfying the following conditions:

(a) (functoriality) for every regular map $\phi\colon V \to W$,

$$\begin{cases} \phi^* \circ cl_W = cl_V \circ \phi^* \\ \phi_* \circ cl_V = cl_W \circ \phi_* \end{cases} \tag{23}$$

(b) (multiplicativity) for every $Y \in C^r_{\mathrm{rat}}(V)$ and $Z \in C^s_{\mathrm{rat}}(W)$,

$$cl_{V\times W}(Y \times Z) = cl_V(Y) \otimes cl_W(Z).$$

(c) (normalization) If $P$ is a point, so that $C^*_{\mathrm{rat}}(P) \simeq \mathbb{Q}$ and $H^*(P) \simeq Q$, then $cl_P$ is the natural inclusion map.

Let $\phi\colon V \to W$ be a regular map of nonsingular projective varieties over $k$, and let $\phi^*$ be the map $H^*(\phi)\colon H^*(W) \to H^*(V)$. Because the pairing (22) is non-degenerate, there is a unique linear map

$$\phi_*\colon H^*(V) \to H^{*-2c}(W)(-c), \quad c = \dim V - \dim W$$

such that the projection formula

$$\eta_W(\phi_*(x) \cdot y) = \eta_V(x \cdot \phi^* y)$$

holds for all $x \in H^r(V)$, $y \in H^{2\dim V - r}(W)(\dim V)$. This explains the maps on the left of the equals signs in (23), and the maps on the right refer to the standard operations on the groups of algebraic cycles modulo rational equivalence (Fulton 1984, Chapter I).

### The Lefschetz Trace Formula

Let $H^*$ be a Weil cohomology over the base field $k$, and let $V$ be nonsingular projective variety over $k$. We use the Künneth formula to identify $H^*(V \times V)$ with $H^*(V) \otimes H^*(V)$.

Let $\phi\colon V \to V$ be a regular map. We shall need an expression for the class of the graph $\Gamma_\phi$ of $\phi$ in

$$H^{2d}(V \times V)(d) \simeq \bigoplus_{r=0}^{2d} H^r(V) \otimes H^{2d-r}(V)(d).$$

Let $(e^r_i)_i$ be a basis for $H^r(V)$ and let $(f^{2d-r}_i)_i$ be the dual basis in $H^{2d-r}(V)(d)$; we choose $e^0 = 1$, so that $\eta_V(f^{2d}) = 1$. Then

$$cl_{V\times V}(\Gamma_\phi) = \sum_{r,i} \phi^*(e^r_i) \otimes f^{2d-r}_i.$$

**Theorem 2.1 (Lefschetz trace formula).** *Let $\phi\colon V \to V$ be a regular map such that $\Gamma_\phi \cdot \Delta$ is defined. Then*

$$(\Gamma_\phi \cdot \Delta) = \sum_{r=0}^{2d} (-1)^r \operatorname{Tr}(\phi \mid H^r(V))$$

*Proof.* We the above notations, we have

$$\begin{aligned} cl_{V\times V}(\Gamma_\phi) &= \sum_{r,i} \phi^*(e_i^r) \otimes f_i^{2d-r} \quad \text{and} \\ cl_{V\times V}(\Delta) &= \sum_{r,i} e_i^r \otimes f_i^{2d-r} \\ &= \sum_{r,i} (-1)^{r(2d-r)} f_i^{2d-r} \otimes e_i^r \\ &= \sum_{r,i} (-1)^r f_i^{2d-r} \otimes e_i^r. \end{aligned}$$

Thus

$$\begin{aligned} cl_{V\times V}(\Gamma_\phi \cdot \Delta) &= \sum_{r,i} (-1)^r \phi^*(e_i^r) f_i^{2d-r} \otimes f^{2d} \\ &= \sum_{r=0}^{2d} (-1)^r \operatorname{Tr}(\phi^*)(f^{2d} \otimes f^{2d}) \end{aligned}$$

because $\phi^*(e_i^r) f_j^{2d-r}$ is the coefficient of $e_j^r$ when $\phi^*(e_i^r)$ is expressed in terms of the basis $(e_j^r)$. On applying $\eta_{V\times V}$ to both sides, we obtain the required formula. □

This is Lefschetz's original 1924 proof (see Steenrod 1957, p. 27).

### There Is no Weil Cohomology Theory with Coefficients in $\mathbb{Q}_p$ or $\mathbb{R}$.

2.2. Recall (1.16) that for a simple abelian variety $A$ over a finite field $k$, $E \overset{\text{def}}{=} \operatorname{End}^0(A)$ is a division algebra with centre $F \overset{\text{def}}{=} \mathbb{Q}[\pi]$, and $2\dim(A) = [E\colon F]^{1/2} \cdot [F\colon \mathbb{Q}]$. Let $Q$ be a field of characteristic zero. In order for $E$ to act on a $Q$-vector space of dimension $2\dim(A)$, the field $Q$ must split $E$, i.e., $Q \otimes_{\mathbb{Q}} E$ must be a matrix algebra over $Q \otimes_{\mathbb{Q}} F$. The endomorphism algebra of a supersingular elliptic curve over a finite field containing $\mathbb{F}_{p^2}$ is a division quaternion algebra over $\mathbb{Q}$ that is nonsplit exactly at $p$ and the real prime (Hasse 1936). Therefore, there cannot be a Weil cohomology with coefficients in $\mathbb{Q}_p$ or $\mathbb{R}$ (hence not in $\mathbb{Q}$ either).[25] Tate's formula (9) doesn't forbid there being a Weil cohomology with coeffients in $\mathbb{Q}_\ell$, $\ell \neq p$, or in the field of fractions of the Witt vectors over $k$. That Weil cohomology theories exist over these fields (see below) is an example of Yhprum's law in mathematics: everything that can work, will work.

### Proof of the Weil Conjectures W1–W3

Let $V_0$ be a nonsingular projective variety of dimension $d$ over $k_0 = \mathbb{F}_q$, and let $V$ be the variety obtained by extension of scalars to the algebraic closure $k$ of $k_0$. Let $\pi\colon V \to V$ be the Frobenius map (relative to $V_0/k_0$). We assume that there exists a Weil cohomology theory over $k$ with coefficients in $Q$.

**Proposition 2.3.** *The zeta function*

$$Z(V,T) = \frac{P_1(T)\cdots P_{2d-1}(T)}{(1-T)P_2(T)\cdots(1-q^dT)} \tag{24}$$

*with $P_r(V,T) = \det(1 - \pi T \mid H^r(V,Q))$.*

*Proof.* Recall that

$$\log Z(V,T) \overset{\text{def}}{=} \sum_{n>0} N_n \frac{T^n}{n}.$$

The fixed points of $\pi^n$ have multiplicity 1, and so

$$N_n = (\Gamma_{\pi^n} \cdot \Delta) \overset{(2.1)}{=} \sum_{r=0}^{2d} (-1)^r \operatorname{Tr}(\pi^n \mid H^r(V,Q)).$$

The following elementary statement completes the proof: Let $\alpha$ be an endomorphism of a finite-dimensional vector space $V$; then

$$\log\left(\det(1 - \alpha T \mid V)\right) = -\sum_{n\geq 1} \operatorname{Tr}(\alpha^n \mid V)\frac{T^n}{n}. \tag{25}$$

□

**Proposition 2.4.** *The zeta function $Z(V,T) \in \mathbb{Q}[T]$.*

*Proof.* We know that $Z(V,T) \in Q[T]$. To proceed, we shall need the following elementary criterion:

Let $f(T) = \sum_{i\geq 0} a_i T^i \in Q[[T]]$; then $f(T) \in Q[T]$ if and only if there exist integers $m$ and $n_0$ such that the Hankel determinant

$$\begin{vmatrix} a_n & a_{n+1} & \cdots & a_{n+m-1} \\ a_{n+1} & a_{n+2} & \cdots & a_{n+m} \\ a_{n+2} & a_{n+3} & \cdots & a_{n+m+1} \\ \vdots & \vdots & & \vdots \\ a_{n+m-1} & a_{n+m} & \cdots & a_{n+2m-2} \end{vmatrix}$$

is 0 for all $n \geq n_0$ (this is a restatement of (1.33); it is an exercise in Chap. 4 of Bourbaki's *Algèbre*).

The power series $Z(V,T)$ satisfies this criterion in $Q[[T]]$, and hence also in $\mathbb{Q}[[T]]$. □

As in the case of curves, the zeta function can be written

$$Z(V,T) = \prod_{v\in|V|} \frac{1}{1 - T^{\deg(v)}}$$

where $v$ runs over the set $|V|$ of closed points of $V$ (as a scheme). Hence

$$Z(V,T) = 1 + a_1 T + a_2 T^2 + \cdots$$

with the $a_i \in \mathbb{Z}$. When we write

$$Z(V,T) = \frac{P(T)}{R(T)}, \quad P,R \in \mathbb{Q}[T], \quad \gcd(P,R) = 1,$$

we can normalize $P$ and $R$ so that

$$\begin{aligned} P(T) &= 1 + b_1 T + \cdots \quad &\in \mathbb{Q}[T] \\ R(T) &= 1 + c_1 T + \cdots \quad &\in \mathbb{Q}[T]. \end{aligned}$$

[25] It was Serre who explained this to Grothendieck, sometime in the 1950s.

**Proposition 2.5.** *Let $P,R$ be as above. Then $P$ and $R$ are uniquely determined by $V$, and they have coefficients in $\mathbb{Z}$.*

*Proof.* The uniqueness follows from unique factorization in $\mathbb{Q}[T]$. If some coefficient of $R$ is not an integer, then $\beta^{-1}$ is not an algebraic integer for some root $\beta$ of $R$. Hence $\mathrm{ord}_l(\beta) > 0$ for some prime $l$, and $Z(V,\beta) = 1 + a_1\beta + a_2\beta^2 + \cdots$ converges $l$-adically. This contradicts the fact that $\beta$ is a pole of $Z(V,T)$. We have shown that $R(T)$ has coefficients in $\mathbb{Z}$. As $Z(V,T)^{-1} \in \mathbb{Z}[[T]]$, the same argument applies to $P(T)$. □

**Proposition 2.6.** *We have*

$$Z(V,1/q^dT) = \pm q^{d\chi/2} \cdot T^\chi \cdot Z(V,T)$$

*where $\chi = (\Delta \cdot \Delta)$.*

*Proof.* The Frobenius map $\pi$ has degree $q^d$. Therefore, for any closed point $P$ of $V$, $\pi^*P = q^dP$, and

$$\pi^* cl_V(P) = cl_V(\pi^*P) = cl_V(q^dP) = q^d cl_V(P). \tag{26}$$

Thus $\pi$ acts as multiplication by $q^d$ on $H^{2d}(V)(d)$. From this, and Poincaré duality, it follows that if $\alpha_1,\ldots,\alpha_s$ are the eigenvalues of $\pi$ acting on $H^r(V)$, then $q^d/\alpha_1,\ldots,q^d/\alpha_s$ are the eigenvalues of $\pi$ acting on $H^{2d-r}(V)$. An easy calculation now shows that the required formula holds with $\chi$ replaced by

$$\sum(-1)^r \dim H^r(V),$$

but the Lefschetz trace formula (2.1) with $\phi = \mathrm{id}$ shows that this sum equals $(\Delta \cdot \Delta)$. □

2.7. In the expression (24) for $Z(V,T)$, we have not shown that the polynomials $P_r$ have coefficients in $\mathbb{Q}$ nor that they are independent of the Weil cohomology theory. However, (2.5) shows that this is true for the numerator and denominator after we have removed any common factors. If the $P_r(T)$ are relatively prime in pairs, then there can be no cancellation, and $P_r(T) = 1 + \sum_i a_{r,i}T^i$ has coefficients in $\mathbb{Z}$ and is independent of the Weil cohomology (because this is true of the irreducible factors of the numerator and denominator). If $|\iota(\alpha)| = q^{r/2}$ for every eigenvalue $\alpha$ of $\pi$ acting on $H^r(V,Q)$ and embedding $\iota$ of $Q(\alpha)$ into $\mathbb{C}$, then the $P_r(T)$ are relatively prime in pairs, and so the Weil conjectures W1–W4 are true for $V$.

### Application to Rings of Correspondences

We show that the (mere) existence of a Weil cohomology theory implies that the $\mathbb{Q}$-algebra of correspondences for numerical equivalence on an algebraic variety is a semisimple $\mathbb{Q}$-algebra of finite dimension.

2.8. Let $V$ be a connected nonsingular projective variety of dimension $d$. An *algebraic $r$-cycle* on $V$ is a formal sum $Z = \sum n_iZ_i$ with $n_i \in \mathbb{Z}$ and $Z_i$ an irreducible closed subvariety of codimension $r$; such cycles form a group $C^r(V)$.

2.9. Let $\sim$ be an adequate equivalence relation on the family of groups $C^r(V)$. Then $C^*_\sim(V) \stackrel{\text{def}}{=} \bigoplus_{r\geq 0} C^r/\sim$ becomes a graded ring under intersection product; moreover, push-forwards and pull-backs of algebraic cycles with respect to regular maps are well-defined. Let $A^r_\sim(V) = C^r_\sim(V) \otimes \mathbb{Q}$. There is a bilinear map

$$A^{\dim(V_1)+r}_\sim(V_1\times V_2)\times A^{\dim(V_2)+s}_\sim(V_2\times V_3) \to A^{\dim(V_1)+r+s}_\sim(V_1\times V_3)$$

sending $(f,g)$ to

$$g \circ f \stackrel{\text{def}}{=} (p_{13})_*(p_{12}^*f \cdot p_{23}^*g)$$

where $p_{ij}$ is the projection $V_1 \times V_2 \times V_3 \to V_i \times V_j$. This is associative in an obvious sense. In particular, $A^{\dim(V)}_\sim(V \times V)$ is a $\mathbb{Q}$-algebra.

2.10. Two algebraic $r$-cycles $f,g$ are *numerically equivalent* if $(f \cdot h) = (g \cdot h)$ for all $(d-r)$-cycles $h$ for which the intersection products are defined. This is an adequate equivalence relation, and so we get a $\mathbb{Q}$-algebra $A^d_{\mathrm{num}}(V \times V)$.

Let $H$ be a Weil cohomology theory with coefficient field $Q$, and let $A^r_H(V)$ (resp. $A^r_H(V,Q)$) denote the $\mathbb{Q}$-subspace (resp. $Q$-subspace) of $H^{2r}(V)(r)$ spanned by the algebraic classes.

2.11. The $\mathbb{Q}$-vector space $A^r_{\mathrm{num}}(V)$ is finite-dimensional. To see this, let $f_1,\ldots,f_s$ be elements of $A^{d-r}_{\mathrm{H}}(V)$ spanning the $Q$-subspace $A^{d-r}_H(V,Q)$ of $H^{2d-2r}(V)(d-r)$; then the kernel of the map

$$x \mapsto (x\cdot f_1,\ldots,x\cdot f_s)\colon A^r_H(V) \to \mathbb{Q}^s$$

consists of the elements of $A^r_H(V)$ numerically equivalent to zero, and so its image is $A^r_{\mathrm{num}}(V)$.

2.12. Let $A^r_{\mathrm{num}}(V,Q)$ denote the quotient of $A^r_H(V,Q)$ by the left kernel of the pairing

$$A^r_H(V,Q) \times A^{d-r}_H(V,Q) \to A^d_H(V,Q) \simeq Q.$$

Then $A^r_H(V) \to A^r_{\mathrm{num}}(V,Q)$ factors through $A^r_{\mathrm{num}}(V)$, and I claim that the map

$$a \otimes f \mapsto af\colon Q \otimes A^r_{\mathrm{num}}(V) \to A^r_{\mathrm{num}}(V,Q)$$

is an isomorphism. As $A^r_{\mathrm{num}}(V,Q)$ is spanned by the image of $A^r_{\mathrm{num}}(V)$, the map is obviously surjective. Let $e_1,\ldots,e_m$ be a $\mathbb{Q}$-basis for $A^r_{\mathrm{num}}(V)$, and let $f_1,\ldots,f_m$ be the dual basis in $A^{d-r}_{\mathrm{num}}(V)$. If $\sum_{i=1}^m a_i \otimes e_i$ ($a_i \in Q$) becomes zero in $A^r_{\mathrm{num}}(V,Q)$, then $a_j = (\sum a_ie_i)\cdot f_j = 0$ for all $j$. Thus the map is injective.

**Theorem 2.13.** *The $\mathbb{Q}$-algebra $A^{\dim(V)}_{\mathrm{num}}(V \times V)$ is finite-dimensional and semisimple.*

*Proof.* Let $d = \dim(V)$ and $B = A^d_{\mathrm{num}}(V \times V)$. Then $B$ is a finite-dimensional $\mathbb{Q}$-algebra (2.11), and the pairing

$$f,g \mapsto (f\cdot g)\colon B \times B \to \mathbb{Q}$$

is nondegenerate. Let $f$ be an element of the radical $\mathrm{rad}(B)$ of $B$. We have to show that $(f \cdot g) = 0$ for all $g \in B$.

Let $A = A_H^d(V \times V, Q)$. Then $A$ is a finite-dimensional $Q$-algebra, and there is a surjective homomorphism

$$A \overset{\text{def}}{=} A_H^d(V \times V, Q) \xrightarrow{S} A_{\text{num}}^d(V \times V, Q) \overset{2.12}{\simeq} Q \otimes B.$$

As the ring $A/\mathrm{rad}(A)$ is semisimple, so also is its quotient $(Q \otimes B)/S(\mathrm{rad}(A))$. Therefore $S(\mathrm{rad}(A)) \supset \mathrm{rad}(Q \otimes B)$, and so there exists an $f' \in \mathrm{rad}(A)$ mapping to $1 \otimes f$. For all $g \in A$,

$$(f' \cdot g^t) = \sum_i (-1)^i \operatorname{Tr}(f' \circ g \mid H^i(V)) \tag{27}$$

—this can be proved exactly as (2.1). But $f' \circ g^t \in \mathrm{rad}(A)$; therefore it is nilpotent, and so its trace on $H^i(V)$ is zero. Hence $(f' \cdot g^t) = 0$, and so $(1 \otimes f \cdot S(g^t)) = 0$ for all $g \in A$. It follows that $f = 0$. □

Theorem 2.13 was extracted from Jannsen 1992.

### Etale Cohomology

> *From all the work of Grothendieck, it is without doubt étale cohomology which has exercised the most profound influence on the development of arithmetic geometry in the last fifty years.*
>
> Illusie 2014.[26]

With his definition of fibre spaces on algebraic varieties, Weil began the process of introducing into abstract algebraic geometry the powerful topological methods used in the study of complex algebraic varieties. He introduced fibre spaces in a 1949 conference talk, and then, in more detail, in a course at the University of Chicago (Weil 1952). For the first time, he made use of the Zariski topology in his definition of an abstract variety, and he equipped his varieties with this topology. He required a fibre space to be locally trival for the Zariski topology on the base variety. Weil's theory works much as expected, but some fibre spaces that one expects (from topology) to be locally trivial are not, because the Zariski topology has too few open sets.

In a seminar in April 1958, Serre enlarged the scope of Weil's theory by admitting also fibre spaces that are only "locally isotrivial" in the following sense: there exists a covering $V = \bigcup_i U_i$ of the base variety $V$ by open subvarieties $U_i$ and finite étale maps $U_i' \to U_i$ such that the fibre space becomes trivial when pulled back to each $U_i'$. For an algebraic group $G$ over $k$, Serre defined $H^1(V, G)$ to be the set of isomorphism classes of principal fibre spaces on $V$ under $G$, which he considered to be the "good $H^1$". At the end of the seminar, Grothendieck said to Serre that this will give the Weil cohomology in all dimensions![27] (Serre 2001, p. 125, p. 255.) By the time Serre wrote up his seminar in September 1958, he was able to include a reference to Grothendieck's announcement (1958b) of a "Weil cohomology".

Grothendieck's claim raised two questions:

(A) when $G$ is commutative, is it possible to define higher cohomology groups?
(B) assuming (A) are they the "true" cohomology groups when $G$ is finite?

To answer (A), Grothendieck observed that to define a sheaf theory and a sheaf-cohomology, much less is needed than a topological space. In particular the "open subsets" need not be subsets.

Specifically, let $\mathsf{C}$ be an essentially small category admitting finite fibred products and a final object $V$, and suppose that for each object $U$ of $\mathsf{C}$ there is given a family of "coverings" $(U_i \to U)_i$. The system of coverings is said to be a *Grothendieck topology* on $\mathsf{C}$ if it satisfies the following conditions:

(a) (base change) if $(U_i \to U)$ is a covering and $U' \to U$ is a morphism in $\mathsf{C}$, then $(U_i \times_U U' \to U')$ is a covering;
(b) (local nature) if $(U_i \to U)_i$ is a covering, and, for each $i$, $(U_{i,j} \to U_i)_j$ is a covering, then the family of composites $(U_{i,j} \to U)_{i,j}$ is a covering;
(c) a family consisting of a single isomorphism $\varphi \colon U' \to U$ is a covering.

For example, let $V$ be a topological space, and consider the category $\mathsf{C}$ whose objects are the open subsets of $V$ with the inclusions as morphisms; then the coverings of open subsets in the usual sense define a Grothendieck topology on $\mathsf{C}$.

Consider a category $\mathsf{C}$ equipped with a Grothendieck topology. A *presheaf* is simply a contravariant functor from $\mathsf{C}$ to the category of abelian groups. A presheaf $P$ is a *sheaf* if, for every covering $(U_i \to U)_i$, the sequence

$$P(U) \to \prod_i P(U_i) \rightrightarrows \prod_{i,j} P(U_i \times_U U_j)$$

is exact. With these definitions, the sheaf theory in Grothendieck 1957 carries over almost word-for-word. The category of sheaves is abelian, satisfies Grothendieck's conditions (AB5) and (AB3*), and admits a family of generators. Therefore, it has enough injectives, and the cohomology groups can be defined to be the right derived functors of $F \rightsquigarrow F(V)$.

When Grothendieck defined the étale topology on a variety (or scheme) $V$, he took as coverings those in Serre's definition of "locally isotrivial", but Mike

[26] De toute l'oeuvre de Grothendieck, c'est sans doute la cohomologie étale qui aura exercé l'influence la plus profonde sur l'évolution de la géométrie arithmétique dans les cinquante dernières années.

[27] Dès la fin de l'exposé oral, Grothendieck m'a dit: cela va donner la cohomologie de Weil en toute dimension!

Artin realized that it was better to allow as coverings all surjective families of étale morphisms. With his definition the local rings satisfy Hensel's lemma.

A test for (B) is:

> (C) let $V$ be a nonsingular algebraic variety over $\mathbb{C}$, and let $\Lambda$ be a finite abelian group; do the étale cohomology groups $H^r(V_{\text{et}},\Lambda)$ coincide with the singular cohomology groups $H^r(V^{\text{an}},\Lambda)$?

For $r=0$, this just says that an algebraic variety over $\mathbb{C}$ is connected for the complex topology if it is connected for the Zariski topology. For $r=1$, it is the Riemann existence theorem,[28] which says that every finite covering of $V^{\text{an}}$ is algebraic. In particular, (C) is true for curves. It was probably this that made Grothendieck optimistic that (C) is true in all degrees.

> Grothendieck thought always in relative terms: one space over another. Once the cohomology of curves (over an algebraically closed field) was understood, we could expect similar results for the direct images for a *relative* curve ..., and, "by unscrewing [dévissage]"... for the higher $H^r$.[29] (Illusie 2014, p. 177.)

Initially (in 1958), Serre was less sure:

> Of course, the Zariski topology gives a $\pi_1$ and $H^1$ that are too small, and I had fixed that defect. But was that enough? My reflexes as a topologist told me that we must also deal with the higher homotopy groups: $\pi_2$, $\pi_3$, etc.[30] (Serre 2001, p. 255.)

Artin proved (C) by showing that, in the relative dimension one case, the Zariski topology is sufficiently fine to give coverings by $K(\pi,1)$'s (SGA 4, XI).[31]

Although Grothendieck had the idea for étale cohomology in 1958,

> a few years passed before this idea really took shape: Grothendieck did not see how to start. He also had other occupations.[32] (Illusie 2014, p. 175.)

When Grothendieck came to Harvard in 1961, Mike Artin asked him:

> if it was all right if I thought about it, and so that was the beginning... [Grothendieck] didn't work on it until I proved the first theorem. ... I thought about it that fall ... And then I gave a seminar... (Segel 2009, p. 358.)

Serre writes (email July 2015):

> Grothendieck, after the seminar lecture where I defined "the good $H^1$", had the idea that the higher cohomology groups would also be the good ones. But, as far as I know, he could not prove their expected properties... It was Mike Artin, in his Harvard seminar notes of 1962, who really started the game, by going beyond $H^1$. For instance, he proved that a smooth space of dimension 2 minus a point has (locally) the same cohomology as a 3-sphere (Artin 1962, p. 110). After that, he and Grothendieck took up, with SGA 4: la locomotive de Bures était lancée.

In 1963–1964, Artin and Grothendieck organized their famous SGA 4 seminar.

The étale topology gives good cohomology groups only for torsion groups. To obtain a Weil cohomology theory, it is necessary to define

$$H^r(V_{\text{et}},\mathbb{Z}_\ell)=\varprojlim_n H^r(V_{\text{et}},\mathbb{Z}/\ell^n\mathbb{Z}),$$

and then tensor with $\mathbb{Q}_\ell$ to get $H^r(V_{\text{et}},\mathbb{Q}_\ell)$. This does give a Weil cohomology theory, and so the Weil conjectures (W1–W3) hold with

$$P_r(V,T)=\det(1-\pi T\mid H^r(V_{\text{et}},\mathbb{Q}_\ell)).$$

More generally, Grothendieck (1964) proved that, for every algebraic variety $V_0$ over a finite field $k_0$,

$$Z(V_0,T)=\prod_r \det(1-\pi T\mid H^r_c(V_{\text{et}},\mathbb{Q}_\ell))^{(-1)^{r+1}} \tag{28}$$

where $H_c$ denotes cohomology with compact support. In the situation of (W5),

$$H^r(V_{\text{et}},\mathbb{Q}_\ell)\simeq H^r(\tilde{V}(\mathbb{C}),\mathbb{Q})\otimes\mathbb{Q}_\ell$$

(proper and smooth base change theorem), and so the $\ell$-adic Betti numbers of $V$ are independent of $\ell$. If the Riemann hypothesis holds, then they equal Weil's Betti numbers.

In the years since it was defined, étale cohomology has become such a fundamental tool that today's arithmetic geometers have trouble imagining an age in which it didn't exist.

[28] Riemann used the Dirichlet principle (unproven at the time) to show that on every compact Riemann surface $S$ there are enough meromorphic functions to realize $S$ as a projective algebraic curve; this proves the Riemann existence theorem for nonsingular projective curves.

[29] Grothendieck pensait toujours en termes relatifs: un espace au-dessus d'un autre. Une fois la cohomologie des courbes (sur un corps algébriquement clos) tirée au clair, on pouvait espérer des résultats similaires pour les images directes pour une courbe *relative* (les théorèmes de spécialisation du $\pi_1$ devaient le lui suggérer), et, "par dévissage" (fibrations en courbes, suites spectrales de Leray), atteindre les $H^i$ supérieurs.

[30] Bien sûr, la topologie de Zariski donne un $\pi_1$ et un $H^1$ trop petits, et j'avais remédié à ce défaut. Mais était-ce suffisant? Mes réflexes de topologue me disaient qu'il fallait aussi s'occuper des groupes d'homotopie supérieurs: $\pi_2$, $\pi_3$, etc.

[31] This is rather Serre's way of viewing Artin's proof. As Serre wrote (email July 2015):

> [This] was the way I saw it, and I liked it for two reasons: a) it is a kind of explanation why higher homotopy groups don't matter: they don't occur in these nice Artin neighbourhoods; b) the fundamental group of such a neighbourhood has roughly the same structure (iterated extension of free groups) as the braid groups which were so dear to Emil Artin; in particular, it is what I called a "good group": its cohomology is the same when it is viewed as a discrete group or as a profinite group.

[32] Quelques années s'écoulèrent avant que cette idée ne prenne réellement forme: Grothendieck ne voyait pas comment démarrer. Il avait aussi d'autres occupations.

## de Rham Cohomology (Characteristic Zero)

Let $V$ be a nonsingular algebraic variety over a field $k$. Define $H^*_{\mathrm{dR}}(V)$ to be the (hyper)cohomology of the complex

$$\Omega^\bullet_{V/k} = \quad \mathscr{O}_X \xrightarrow{d} \Omega^1_{V/k} \xrightarrow{d} \cdots \xrightarrow{d} \Omega^r_{V/k} \xrightarrow{d} \cdots$$

of sheaves for the Zariski topology on $V$. When $k = \mathbb{C}$, we can also define $H^*_{\mathrm{dR}}(V^{\mathrm{an}})$ by replacing $\Omega^\bullet_{V/k}$ with the complex of sheaves of holomorphic differentials on $V^{\mathrm{an}}$ for the complex topology. Then

$$H^r(V^{\mathrm{an}}, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \simeq H^r_{\mathrm{dR}}(V^{\mathrm{an}})$$

for all $r$.

When $k = \mathbb{C}$, there is a canonical homomorphism

$$H^*_{\mathrm{dR}}(V) \to H^*_{\mathrm{dR}}(V^{\mathrm{an}}).$$

In a letter to Atiyah in 1963, Grothendieck proved that this is an isomorphism (Grothendieck 1966). Thus, for a nonsingular algebraic variety over a field $k$ of characteristic zero, there are algebraically defined cohomology groups $H^*_{\mathrm{dR}}(V)$ such that, for every embedding $\rho\colon k \to \mathbb{C}$,

$$H^*_{\mathrm{dR}}(V) \otimes_{k,\rho} \mathbb{C} \simeq H^*_{\mathrm{dR}}(\rho V) \simeq H^*_{\mathrm{dR}}((\rho V)^{\mathrm{an}}).$$

This gives a Weil cohomology theory with coefficients in $k$.

## $p$-Adic Cohomology

The étale topology gives Weil cohomologies with coefficients in $\mathbb{Q}_\ell$ for all primes $\ell$ different from the characteristic of $k$. Dwork's early result (see p. 28) suggested that there should also be $p$-adic Weil cohomology theories, i.e., a cohomology theories with coefficients in a field containing $\mathbb{Q}_p$.

Let $V$ be an algebraic variety over a field $k$ of characteristic $p \neq 0$. When Serre defined the cohomology groups of coherent sheaves on algebraic varieties, he asked whether the formula

$$\beta_r(V) \stackrel{?}{=} \sum_{i+j=r} \dim_k H^j(V, \Omega^i_{V/k})$$

gives the "true" Betti numbers, namely, those intervening in the Weil conjectures (Serre 1954, p. 520). An example of Igusa (1955) showed that this formula gives (at best) an upper bound for Weil's Betti numbers. Of course, the groups $\bigoplus_{i+j=r} H^j(V, \Omega^i_{V/k})$ wouldn't give a Weil cohomology theory because the coefficient field has characteristic $p$. Serre (1958) next considered the Zariski cohomology groups $H^r(V, W\mathscr{O}_V)$ where $W\mathscr{O}_V$ is the sheaf of Witt vectors over $\mathscr{O}_V$ (a ring of characteristic zero), but found that they did not have good properties (they would have given only the $H^{0,r}$ part of the cohomology).

In 1966, Grothendieck discovered how to obtain the de Rham cohomology groups in characteristic zero without using differentials, and suggested that his method could be modified to give a good $p$-adic cohomology theory in characteristic $p$.

Let $V$ be a nonsingular variety over a field $k$ of characteristic zero. Define $\mathrm{inf}(V/k)$ to be the category whose objects are open subsets $U$ of $V$ together with thickening of $U$, i.e., an immersion $U \hookrightarrow T$ defined by a nilpotent ideal in $\mathscr{O}_T$. Define a covering family of an object $(U, U \hookrightarrow T)$ of $\mathrm{inf}(V/k)$ to be a family $(U_i, U_i \hookrightarrow T_i)_i$ with $(T_i)_i$ a Zariski open covering of $T$ and $U_i = U \times_T T_i$. These coverings define the "infinitesimal" Grothendieck topology on $\mathrm{inf}(V/k)$. There is a structure sheaf $\mathscr{O}_{V_{\mathrm{inf}}}$ on $V_{\mathrm{inf}}$, and Grothendieck proves that

$$H^*(V_{\mathrm{inf}}, \mathscr{O}_{V_{\mathrm{inf}}}) \simeq H^*_{\mathrm{dR}}(V)$$

(Grothendieck 1968, 4.1).

This doesn't work in characteristic $p$, but Grothendieck suggested that by adding divided powers to the thickenings, one should obtain a good cohomology in characteristic $p$. There were technical problems at the prime 2, but Berthelot resolved these in this thesis to give a good definition of the "crystalline" site, and he developed a comprehensive treatment of crystalline cohomology (Berthelot 1974). This is a cohomology theory with coefficients in the ring of Witt vectors over the base field $k$. On tensoring it with the field of fractions, we obtain a Weil cohomology.

About 1975, Bloch extended Serre's sheaf $W\mathscr{O}_V$ to a "de Rham-Witt complex"

$$W\Omega^\bullet_{V/k}: \quad W\mathscr{O}_V \xrightarrow{d} W\Omega^1_{V/k} \xrightarrow{d} \cdots$$

and showed that (except for some small $p$) the Zariski cohomology of this complex is canonically isomorphic to crystalline cohomology (Bloch 1977). Bloch used $K$-theory to define $W\Omega^\bullet_{V/k}$ (he was interested in relating $K$-theory to crystalline cohomology among other things). Deligne suggested a simpler, more direct, definition of the de Rham-Witt complex and this approach was developed in detail by Illusie and Raynaud (Illusie 1983).

Although $p$-adic cohomology is more difficult to define than $\ell$-adic cohomology, it is often easier to compute with it. It is essential for understanding $p$-phenomena, for example, $p$-torsion, in characteristic $p$.

**Notes.** The above account of the origins of $p$-adic cohomology is too brief—there were other approaches and other contributors.

## 3. The Standard Conjectures

*Alongside the problem of resolution of singularities, the proof of the standard conjectures seems to me to be the most urgent task in algebraic geometry.*

Grothendieck 1969.

We have seen how to deduce the first three of the Weil conjectures from the existence of a Weil cohomology. What more is needed to deduce the Riemann hypothesis? About 1964, Bombieri and Grothendieck independently found the answer: we need a Künneth formula and a Hodge index theorem for algebraic classes. Before explaining this, we look at the analogous question over $\mathbb{C}$.

### A Kählerian Analogue

In his 1954 ICM talk, Weil sketched a transcendental proof of the inequality $\sigma(\xi \circ \xi') > 0$ for correspondences on a complex curve, and wrote:

> ... this is precisely how I first persuaded myself of the truth of the abstract theorem even before I had perceived the connection between the trace $\sigma$ and Castelnuovo's equivalence defect.

In a letter to Weil in 1959, Serre wrote:

> In fact, a similar process, based on Hodge theory, applies to varieties of any dimension, and one obtains both the positivity of certain traces, and the determination of the absolute values of certain eigenvalues in perfect analogy with your beloved conjectures on the zeta functions.[33]

We now explain this. More concretely, we consider the following problem: Let $V$ be a connected nonsingular projective variety of dimension $d$ over $\mathbb{C}$, and let $f\colon V \to V$ be an endomorphism of degree $q^d$; find conditions on $f$ ensuring that the eigenvalues of $f$ acting on $H^r(V,\mathbb{Q})$ have absolute value $q^{r/2}$ for all $r$.

For a curve $V$, no conditions are needed. The action of $f$ on the cohomology of $V$ preserves the Hodge decomposition

$$H^1(V,\mathbb{C}) \simeq H^{1,0}(V) \oplus H^{0,1}(V), \quad H^{i,j}(V) \stackrel{\text{def}}{=} H^j(V,\Omega^i),$$

and the projection $H^1(V,\mathbb{C}) \to H^{1,0}(V)$ realizes $H^1(V,\mathbb{Z}) \subset H^1(V,\mathbb{C})$ as a lattice in $H^{1,0}(V)$, stable under the action of $f$. Define a hermitian form on $H^{1,0}(V)$ by

$$\langle \omega, \omega' \rangle = \frac{1}{2\pi i}\int_V \omega \wedge \bar{\omega}'.$$

This is positive definite. As $f^*$ acts on $H^2_{\mathrm{dR}}(V)$ as multiplication by $\deg(f) = q$,

$$\langle f^*\omega, f^*\omega' \rangle \stackrel{\text{def}}{=} \frac{1}{2\pi i}\int_V f^*(\omega \wedge \bar{\omega}') = \frac{q}{2\pi i}\int_V \omega \wedge \bar{\omega}' \stackrel{\text{def}}{=} q\langle \omega, \omega' \rangle.$$

[33] "En fait, un procédé analogue, basé sur la théorie de Hodge, s'applique aux variétés de dimension quelconque, et l'on obtient à la fois la positivité de certaines traces, et la détermination des valeurs absolues de certaines valeurs propres, en parfaite analogie avec tes chères conjectures sur les fonctions zêta."

Hence, $q^{-1/2}f$ is a unitary operator on $H^{1,0}(V)$, and so its eigenvalues $a_1,\dots,a_g$ have absolute value 1. The eigenvalues of $f^*$ on $H^1(V,\mathbb{Q})$ are $q^{1/2}a_1,\dots,q^{1/2}a_g$, $q^{1/2}\bar{a}_1,\dots,q^{1/2}\bar{a}_g$, and so they have absolute value $q^{1/2}$.

In higher dimensions, an extra condition is certainly needed (consider a product). Serre realized that it was necessary to introduce a polarization.

**Theorem 3.1 (Serre 1960, Thm 1).** *Let $V$ be a connected nonsingular projective variety of dimension $d$ over $\mathbb{C}$, and let $f$ be an endomorphism $V$. Suppose that there exists an integer $q > 0$ and a hyperplane section $E$ of $V$ such that $f^{-1}(E)$ is algebraically equivalent to $qE$. Then, for all $r \geq 0$, the eigenvalues of $f$ acting on $H^r(V,\mathbb{Q})$ have absolute value $q^{r/2}$.*

For a variety over a finite field and $f$ the Frobenius map, $f^{-1}(E)$ is equivalent to $qE$, and so this is truly a kählerian analogue of the Riemann hypothesis over finite fields. Note that the condition $f^{-1}(E) \sim qE$ implies that $(f^{-1}E^d) = q^d(E^d)$, and hence that $f$ has degree $q^d$.

The proof is an application of two famous theorems. Throughout, $V$ is as in the statement of the theorem. Let $E$ be an ample divisor on $V$, let $u$ be its class in $H^2(V,\mathbb{Q})$, and let $L$ be the "Lefschetz operator"

$$x \mapsto u \cup x\colon H^*(V,\mathbb{Q}) \to H^{*+2}(V,\mathbb{Q})(1).$$

**Theorem 3.2 (Hard Lefschetz).** *For $r \leq d$, the map*

$$L^{d-r}\colon H^r(V,\mathbb{Q}) \to H^{2d-r}(V,\mathbb{Q})(d-r)$$

*is an isomorphism.*

*Proof.* It suffices to prove this after tensoring with $\mathbb{C}$. Lefschetz's original "topological proof" (1924) is inadequate, but there are analytic proofs (e.g., Weil 1958, IV, n°6, Cor. to Thm 5). □

Now let $H^r(V) = H^r(V,\mathbb{C})$, and omit the Tate twists. Suppose that $r \leq d$, and consider

$$H^{r-2}(V) \xrightarrow{L} H^r(V) \xrightarrow[\simeq]{L^{d-r}} H^{2d-r}(V) \xrightarrow{L} H^{2d-r+2}(V).$$

The composite of the maps is an isomorphism (3.2), and so

$$H^r(V) = P^r(V) \oplus LH^{r-2}(V)$$

with $P^r(V) = \mathrm{Ker}(H^r(V) \xrightarrow{L^{d-r+1}} H^{2d-r+2}(V))$. On repeating this argument, we obtain the first of the following decompositions, and the second is proved similarly:

$$H^r(V) = \begin{cases} \bigoplus_{j\geq 0} L^j P^{r-2j} & \text{if } r \leq d \\ \bigoplus_{j \geq r-d} L^j P^{r-2j} & \text{if } r \geq d. \end{cases}$$

In other words, every element $x$ of $H^r(V)$ has a unique expression as a sum

$$x = \sum_{j \geq \max(r-d,0)} L^j x_j, \quad x_j \in P^{r-2j}(V). \tag{29}$$

The cohomology classes in $P^r(V)$, $r \leq d$, are said to be *primitive*.

The *Weil operator* $C\colon H^*(V) \to H^*(V)$ is the linear map such that $Cx = i^{a-b}x$ if $x$ is of type $(a,b)$. It is an automorphism of $H^*(V)$ as a $\mathbb{C}$-algebra, and $C^2$ acts on $H^r(V)$ as multiplication by $(-1)^r$ (Weil 1958, n°5, p. 74).

Using the decomposition (29), we define an operator $*\colon H^r(V) \to H^{2d-r}(V)$ by

$$*x = \sum_{j \geq \max(r-d,0)} (-1)^{\frac{r(r+1)}{2}} \cdot \tfrac{j!}{(d-r-j)!} \cdot C(L^{d-r-j}x_j).$$

For $\omega \in H^r(V)$, let

$$I(\omega) = \begin{cases} \int_V \omega & \text{if } r = 2d \\ 0 & \text{if } r < 2d, \end{cases}$$

and let

$$I(x,y) = I(x \cdot y).$$

**Lemma 3.3.** *For* $x,y \in H^*(V)$,

$$I(x,*y) = I(y,*x) \text{ and } I(x,*x) > 0 \text{ if } x \neq 0.$$

*Proof.* Weil 1958, IV, n°7, Thm 7. □

For $x = \sum L^j x_j$ and $y = \sum L^j y_j$ with $x_j$, $y_j$ primitive of degree $r-2j$, put

$$A(x,y) = \sum_{j \geq \max(r-d,0)} (-1)^{\frac{r(r+1)}{2}} \cdot \tfrac{j!}{(d-r-j)!} \cdot (-1)^j \cdot I(u^{d-r+2j} \cdot x_j \cdot y_j).$$

**Theorem 3.4.** *The map $A$ is a bilinear form on $H^r(V)$, and*

$$A(y,x) = (-1)^r A(x,y), \qquad A(Cx,Cy) = A(x,y)$$
$$A(x,Cy) = A(y,Cx), \qquad A(x,C\bar{x}) > 0 \text{ if } x \neq 0.$$

*Proof.* The first two statements are obvious, and the second two follow from (3.3) because

$$A(x,Cy) = \sum_{j \geq \max(r-d,0)} I(L^j x_j, *L^j y_j).$$

See Weil 1958, IV, n°7, p. 78. □

Note that the intersection form $I$ on $H^d(V)$ is symmetric or skew-symmetric according as $d$ is even or odd.

**Theorem 3.5 (Hodge Index).** *Assume that the dimension $d$ of $V$ is even. Then the signature of the intersection form on $H^d(V)$ is $\sum_{a,b}(-1)^a h^{a,b}(V)$.*

*Proof.* Exercise, using (3.4). See Weil 1958, IV, n°7, Thm 8. □

To deduce (1.2) from the theorem, it is necessary to show that the nonalgebraic cycles contribute only positive terms. This is what Hodge did in his 1937 paper.

We now prove Theorem 3.1. It follows from (3.4) that the sesquilinear form

$$(x,y) \mapsto A(x,C\bar{y})\colon H^r(V) \times H^r(V) \to \mathbb{C} \tag{30}$$

is hermitian and positive definite. Let $g_r = q^{-r/2}H^r(f)$. Then $g_r$ respects the structure of $H^*(V)$ as a bigraded $\mathbb{C}$-algebra, the form $I$, and the operators $a \mapsto \bar{a}$ and $a \mapsto La$. Therefore, it respects the form (30), i.e., it is a unitary operator, and so its eigenvalues have absolute value 1. This completes the proof of the theorem.

This proof extends to correspondences. For curves, it then becomes the argument in Weil's ICM talk; for higher dimensions, it becomes the proof of Theorem 2 of Serre 1960.

## Weil Forms

As there is no Weil cohomology theory in nonzero characteristic with coefficients in a real field, it is not possible to realize the Frobenius map as a unitary operator. Instead, we go back to Weil's original idea.

Let $H$ be a Weil cohomology theory over $k$ with coefficient field $Q$. From the Künneth formula and Poincaré duality, we obtain isomorphisms

$$\begin{aligned} H^{2d}(V \times V)(d) &\simeq \bigoplus_{r=0}^{2d} \left(H^r(V) \otimes H^{2d-r}(V)(d)\right) \\ &\simeq \bigoplus_{r=0}^{2d} \mathrm{End}_{Q\text{-linear}}(H^r(V)). \end{aligned}$$

Let $\pi_r$ be the $r$th Künneth projector. Under the isomorphism, the subring

$$H^{2d}(V \times V)_r \overset{\text{def}}{=} \pi_r \circ H^{2d}(V \times V) \circ \pi_r$$

of $H^{2d}(V \times V)(d)$ corresponds to $\mathrm{End}_{Q\text{-linear}}(H^r(V))$.

Let $A^r_H(-)$ denote the $\mathbb{Q}$-subspace of $H^{2r}(-)(r)$ generated by the algebraic classes. Then $A^d_H(V \times V)$ is the $\mathbb{Q}$-algebra of correspondences on $V$ for homological equivalence (see 2.9). Assume that the Künneth projectors $\pi_r$ are algebraic, and let

$$A^d_H(V \times V)_r = A^d_H(V \times V) \cap H^{2d}(V \times V)_r = \pi_r \circ A^d_H(V \times V) \circ \pi_r.$$

Then

$$A^d_H(V \times V) = \bigoplus_{r=0}^{2d} A^d_H(V \times V)_r.$$

Let

$$\phi\colon H^r(V) \times H^r(V) \to Q(-r)$$

be a nondegenerate bilinear form. For $\alpha \in \mathrm{End}(H^r(V))$, we let $\alpha'$ denote the adjoint of $\alpha$ with respect to $\phi$:

$$\phi(\alpha x, y) = \phi(x, \alpha' y).$$

**Definition 3.6.** We call $\phi$ a *Weil form* if it satisfies the following conditions:

(a) $\phi$ is symmetric or skew-symmetric according as $r$ is even or odd;
(b) for all $\alpha \in A_H^d(V \times V)_r$, the adjoint $\alpha' \in A_H^d(V \times V)_r$; moreover, $\mathrm{Tr}(\alpha \circ \alpha') \in \mathbb{Q}$, and $\mathrm{Tr}(\alpha \circ \alpha') > 0$ if $\alpha \neq 0$.

**Example 3.7.** Let $V$ be a nonsingular projective variety over $\mathbb{C}$. For all $r \geq 0$, the pairing

$$H^r(V) \times H^r(V) \to \mathbb{C}, \quad x, y \mapsto (x \cdot *y)$$

is a Weil form (Serre 1960, Thm 2).

**Example 3.8.** Let $C$ be a curve over $k$, and let $J$ be its jacobian. The Weil pairing $\phi\colon T_\ell J \times T_\ell J \to T_\ell \mathbb{G}_m$ extends by linearity to a $\mathbb{Q}_\ell$-bilinear form

$$H_1(C_{\mathrm{et}}, \mathbb{Q}_\ell) \times H_1(C_{\mathrm{et}}, \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(1)$$

on $H_1(C_{\mathrm{et}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell \otimes T_\ell J$. This is Weil form (Weil 1948b, VI, n°48, Thm 25).

**Proposition 3.9.** *If there exists a Weil form on $H^r(V)$, then the $\mathbb{Q}$-algebra $A_H^d(V \times V)_r$ is semisimple.*

*Proof.* It admits a positive involution $\alpha \mapsto \alpha'$, and so we can argue as in the proof of (1.28). □

**Proposition 3.10.** *Let $\phi$ be a Weil form on $H^r(V)$, and let $\alpha$ be an element of $A^d(V \times V)_r$ such that $\alpha \circ \alpha'$ is an integer $q$. For every homomorphism $\rho\colon \mathbb{Q}[\alpha] \to \mathbb{C}$,*

$$\rho(\alpha') = \overline{\rho(\alpha)} \text{ and } |\rho\alpha| = q^{1/2}.$$

*Proof.* The proof is the same as that of (1.29). □

### The Standard Conjectures

Roughly speaking, the standard conjectures state that the groups of algebraic cycles modulo homological equivalence behave like the cohomology groups of a Kähler manifold. Our exposition in this subsection follows Grothendieck 1969 and Kleiman 1968.[34]

Let $H$ be a Weil cohomology theory over $k$ with coefficient field $Q$. We assume that the hard Lefschetz theorem holds for $H$.[35] This means the following: let $L$ be the Lefschetz operator $x \mapsto u \cdot x$ defined by the class $u$ of an ample divisor in $H^2(V)(1)$; then, for all $r \leq d$, the map

$$L^{d-r}\colon H^r(V) \to H^{2d-r}(V)(d-r)$$

is an isomorphism. As before, this gives decompositions

$$H^r(V) = \bigoplus_{j \geq \max(r-d,0)} L^j P^{r-2j}(V)$$

with $P^r(V)$ equal to the kernel of $L^{d-r+1}\colon H^r(V) \to H^{2d-r+2}(V)$. Hence $x \in H^r(V)$ has a unique expression as a sum

$$x = \sum_{j \geq \max(r-d,0)} L^j x_j, \quad x_j \in P^{r-2j}(V). \tag{31}$$

Define an operator $\Lambda\colon H^r(V) \to H^{r-2}(V)$ by

$$\Lambda x = \sum_{j \geq \max(r-d,0)} L^{j-1} x_j.$$

The Standard Conjectures of Lefschetz Type

**A($V,L$):** For all $2r \leq d$, the isomorphism $L^{d-2r}\colon H^{2r}(V)(r) \to H^{2d-2r}(V)(d-r)$ restricts to an isomorphism

$$A_H^r(V) \to A_H^{d-r}(V).$$

Equivalently, $x \in H^{2r}(V)(r)$ is algebraic if $L^{d-2r}x$ is algebraic.

**B($V$):** The operator $\Lambda$ is algebraic, i.e., it lies in the image of

$$A_H^{d-1}(V \times V) \to H^{2d-2}(V \times V)(d-1) \simeq \bigoplus_{r \geq 0} \mathrm{Hom}(H^{r+2}(V), H^r(V)).$$

**C($V$):** The Künneth projectors $\pi_r$ are algebraic. Equivalently, the Künneth isomorphism

$$H^*(V \times V) \simeq H^*(V) \otimes H^*(V)$$

induces an isomorphism

$$A_H^*(V \times V) \simeq A_H^*(V) \otimes A_H^*(V).$$

**Proposition 3.11.** *There are the following relations among the conjectures.*

*(a) Conjecture $A(V \times V, L \otimes 1 + 1 \otimes L)$ implies $B(V)$.*
*(b) If $B(V)$ holds for one choice of $L$, then it holds for all.*
*(c) Conjecture $B(V)$ implies $A(V,L)$ (all $L$) and $C(V)$.*

*Proof.* Kleiman 1994, Theorem 4-1. □

Thus $A(V,L)$ holds for all $V$ and $L$ if and only if $B(V)$ holds for all $V$; moreover, each conjecture implies Conjecture $C$.

[34] According to Illusie (2010): Grothendieck gave a series of lectures on motives at the IHÉS. One part was about the standard conjectures. He asked John Coates to write down notes. Coates did it, but the same thing happened: they were returned to him with many corrections. Coates was discouraged and quit. Eventually, it was Kleiman who wrote down the notes in *Dix exposés sur la cohomologie des schémas*.

[35] For $\ell$-adic étale cohomology, this was proved by Deligne as a consequence of his proof of the Weil conjectures, and it follows for the other standard Weil cohomology theories.

**Example 3.12.** Let $k = \mathbb{F}$. A smooth projective variety $V$ over $k$ arises from a variety $V_0$ defined over a finite subfield $k_0$ of $k$. Let $\pi$ be the corresponding Frobenius endomorphism of $V$, and let $P_r(T) = \det(1 - \pi T \mid H^r(V))$. According to the Cayley-Hamilton theorem, $P_r(\pi)$ acts as zero on $H^r(V)$. Assume that the $P_r$ are relatively prime (this is true, for example, if the Riemann hypothesis holds). According to the Chinese remainder theorem, there are polynomials $P^r(T) \in Q[T]$ such that

$$P^r(T) = \begin{cases} 1 & \mod P_r(T) \\ 0 & \mod P_s(T) \text{ for } s \neq r. \end{cases}$$

Now $P^r(\pi)$ projects $H^*(V)$ onto $H^r(V)$, and so Conjecture $C(V)$ is true.

**Example 3.13.** Conjecture $B(V)$ holds if $V$ is an abelian variety or a surface with $\dim H^1(V)$ equal to twice the dimension of the Picard variety of $V$ (Kleiman 1968, 2. Appendix).

These are essentially the only cases where the standard conjectures of Lefschetz type are known (see Kleiman 1994).

### The Standard Conjecture of Hodge Type

For $r \leq d$, let $A_H^r(V)_{pr}$ denote the "primitive" part $A_H^r(V) \cap P^{2r}(V)$ of $A_H^r(V)$. Conjecture $A(V,L)$ implies that

$$A_H^r(V) = \bigoplus_{j \geq \max(2r-d,0)} L^j A^{r-j}(V)_{pr}.$$

**I($V,L$):** For $r \leq d$, the symmetric bilinear form

$$x, y \mapsto (-1)^r (x \cdot y \cdot u^{d-2r}) \colon A_H^r(V)_{pr} \times A_H^r(V)_{pr} \to \mathbb{Q}$$

is positive definite.

In characteristic zero, the standard conjecture of Hodge type follows from Hodge theory (see 3.3). In nonzero characteristic, almost nothing is known except for surfaces where it becomes Theorem 1.2.

### Consequences of the Standard Conjectures

**Proposition 3.14.** *Assume the standard conjectures. For every $x \in A_H^r(V)$, there exists a $y \in A_H^{d-r}(V)$ such that $x \cdot y \neq 0$.*

*Proof.* We may suppose that $x = L^j x_j$ with $x_j \in A_H^{r-j}(V)_{pr}$. Now

$$(L^j x_j \cdot L^j x_j \cdot u^{d-2r}) = (x_j \cdot x_j \cdot u^{d-2r+2j}) > 0. \qquad \square$$

Using the decomposition (31), we define an operator $*\colon H^r(V) \to H^{2d-r}(V)$ by[36]

$$*x = \sum_{j \geq \max(r-d,0)} (-1)^{\frac{(r-2j)(r-2j+1)}{2}} L^{d-r+j}(x_j).$$

[36] This differs from the definition in kählerian geometry by some scalar factors. Over $\mathbb{C}$, our form $x, y \mapsto (x \cdot *y)$ is positive definite on some direct summands of $H^r(V)$ and negative definite on others, but this suffices to imply that the involution $\alpha \mapsto \alpha'$ is positive.

**Theorem 3.15.** *Assume the standard conjectures. Then*

$$H^r(V) \times H^r(V) \to Q, \quad x, y \mapsto (x \cdot *y),$$

*is a Weil form.*

*Proof.* Kleiman 1968, 3.11. $\square$

**Corollary 3.16.** *The $\mathbb{Q}$-algebra $A_H^d(V \times V)_r$ is semisimple.*

*Proof.* It admits a positive involution; see (2.4). $\square$

**Theorem 3.17.** *Assume the standard conjectures. Let $V$ be a connected nonsingular projective variety of dimension $d$ over $k$, and let $f$ be an endomorphism $V$. Suppose that there exists an integer $q > 0$ and a hyperplane section $E$ of $V$ such that $f^{-1}(E)$ is algebraically equivalent to $qE$. Then, for all $r \geq 0$, the eigenvalues of $f$ acting on $H^r(V, \mathbb{Q})$ have absolute value $q^{r/2}$.*

*Proof.* Use $E$ to define the Lefschetz operator. Then $\alpha \circ \alpha' = q$, and we can apply (3.10). $\square$

**Aside 3.18.** In particular, the standard conjectures imply that the Frobenius endomorphism acts semisimply on étale cohomology over $\mathbb{F}$. For abelian varieties, this was proved by Weil in the 1940s, but there has been almost no progress since then.

## The Standard Conjectures and Equivalences on Algebraic Cycles

Our statement of the standard conjectures is relative to a choice of a Weil cohomology theory. Grothendieck initially stated the standard conjectures in a letter to Serre[37] for algebraic cycles modulo algebraic equivalence, but an example of Griffiths shows that they are false in that context.

Recall that two algebraic cycles $Z$ and $Z'$ on a variety $V$ are *rationally equivalent* if there exists an algebraic cycle $\mathscr{Z}$ on $V \times \mathbb{P}^1$ such that $\mathscr{Z}_0 = Z$ and $\mathscr{Z}_1 = Z'$; that they are *algebraically equivalent* if there exists a curve $T$ and an algebraic cycle $\mathscr{Z}$ on $V \times T$ such that $\mathscr{Z}_{t_0} = Z$ and $\mathscr{Z}_{t_1} = Z'$ for two points $t_0, t_1 \in T(k)$; that they are *homologically equivalent* relative to some fixed Weil cohomology $H$ if they have the same class in $H^{2*}(V)(*)$; and that they are *numerically equivalent* if $(Z \cdot Y) = (Z' \cdot Y)$ for all algebraic cycles $Y$ of complementary dimension. We have

$$\text{rat} \implies \text{alg} \implies \text{hom} \implies \text{num}.$$

For divisors, rational equivalence coincides with linear equivalence. Rational equivalence certainly differs from algebraic equivalence, except over the algebraic closure of a finite fields, where all four equivalence relations are conjectured to coincide (folklore).

[37] *Grothendieck-Serre Correspondence*, p. 232, 1965.

For divisors, algebraic equivalence coincides with numerical equivalence (Matsusaka 1957). For many decades, it was believed that algebraic equivalence and numerical equivalence coincide—one of Severi's "self-evident" postulates even has this as a consequence (Brigaglia et al. 2004, p. 327).

Griffiths (1969) surprised everyone by showing that, even in the classical situation, algebraic equivalence differs from homological equivalence.[38] However, there being no counterexample, it remains a folklore conjecture that numerical equivalence coincides with homological equivalence for the standard Weil cohomologies. For $\ell$-adic étale cohomology, this conjecture is stated in Tate 1964.

The standard conjectures for a Weil cohomology theory $H$ imply that numerical equivalence coincides with homological equivalence for $H$ (see 3.14). It would be useful to have a statement of the standard conjectures independent of any Weil cohomology theory. One possibility is to state them for the $\mathbb{Q}$-vector spaces of algebraic cycles modulo smash-nilpotent equivalence in the sense of Voevodsky 1995 (which implies homological equivalence, and is conjectured to equal numerical equivalence).

### The Standard Conjectures and the Conjectures of Hodge and Tate

Grothendieck hoped that his standard conjectures would be more accessible than the conjectures of Hodge and Tate, but these conjectures appear to be closely intertwined. Before explaining this, I recall the statements of the Hodge and Tate conjectures.

**Conjecture 3.19 (Hodge).** *Let $V$ be a smooth projective variety over $\mathbb{C}$. For all $r \geq 0$, the $\mathbb{Q}$-subspace of $H^{2r}(V,\mathbb{Q})$ spanned by the algebraic classes is $H^{2r}(V,\mathbb{Q}) \cap H^{r,r}(V)$.*

**Conjecture 3.20 (Tate).** *Let $V_0$ be a smooth projective variety over a field $k_0$ finitely generated over its prime field, and let $\ell$ be a prime $\neq \mathrm{char}(k)$. For all $r \geq 0$, the $\mathbb{Q}_\ell$-subspace of $H^{2r}(V_{\mathrm{et}},\mathbb{Q}_\ell(r))$ spanned by the algebraic classes consists exactly of those fixed by the action of $\mathrm{Gal}(k/k_0)$. Here $k$ is a separable algebraic closure of $k_0$ and $V = (V_0)_k$.*

By the full Tate conjecture, I mean the Tate conjecture plus $\mathrm{num} = \mathrm{hom}(\ell)$ (cf. Tate 1994, 2.9).

3.21. *The Hodge conjecture implies the standard conjecture of Lefschetz type over $\mathbb{C}$ (obviously). Conversely, the standard conjecture of Lefschetz type over $\mathbb{C}$ implies the Hodge conjecture for abelian varieties (Abdulali 1994, André 1996), and hence the standard conjecture of Hodge type for abelian varieties in all characteristics (Milne 2002).*

3.22. *Tate's conjecture implies the standard conjecture of Lefschetz type (obviously). If the full Tate conjecture is true over finite fields of characteristic $p$, then the standard conjecture of Hodge type holds in characteristic $p$.*

Here is a sketch of the proof of the last statement. Let $k$ denote an algebraic closure of $\mathbb{F}_p$. The author showed that the Hodge conjecture for CM abelian varieties over $\mathbb{C}$ implies the standard conjecture of Hodge type for abelian varieties over $k$. The proof uses only that Hodge classes on CM abelian varieties are *almost*-algebraic at $p$ (see (4.5) below for this notion). The Tate conjecture for finite subfields of $k$ implies the standard conjecture of Lefschetz type over $k$ (obviously), and, using ideas of Abdulali and André, one can deduce that Hodge classes on CM abelian varieties are almost-algebraic at $p$; therefore the standard conjecture of Hodge type holds for abelian varieties over $k$. The full Tate conjecture implies that the category of motives over $k$ is generated by the motives of abelian varieties, and so the Hodge standard conjecture holds for all nonsingular projective varieties over $k$. A specialization argument now proves it for all varieties in characteristic $p$.

## 4. Motives

For Grothendieck, the theory of "motifs" took on an almost mystical meaning as the reality that lay beneath the "shimmering ambiguous surface of things". But in their simplest form, as a universal Weil cohomology theory, the idea is easy to explain. Having already written a "popular" article on motives (Milne 2009b), I shall be brief.

Let $\sim$ be an adequate equivalence relation on algebraic cycles, for example, one of those listed on p. 37. We want to define a Weil cohomology theory that is universal among those for which $\sim \Rightarrow \mathrm{hom}$. We also want to have $\mathbb{Q}$ as the field of coefficients, but we know that this is impossible if we require the target category to be that of $\mathbb{Q}$-vector spaces, and so we only ask that the target category be $\mathbb{Q}$-linear and have certain other good properties.

Fix a field $k$ and an adequate equivalence relation $\sim$. The category $\mathrm{Corr}_\sim(k)$ of correspondences over $k$ has one object $hV$ for each nonsingular projective variety over $k$; its morphisms are defined by

$$\mathrm{Hom}(hV,hW) = \bigoplus_r \mathrm{Hom}^r(hV,hW) = \bigoplus_r A_\sim^{\dim(V)+r}(V \times W).$$

[38] In fact, they aren't even close. The first possible counterexample is for 1-cycles on a 3-fold, and, indeed, for a complex algebraic variety $V$ of dimension 3, the vector space

$$\frac{\{\text{ one} - \text{cycles homologically equivalent to zero }\}}{\{\text{ one} - \text{cycles algebraically equivalent to zero }\}} \otimes \mathbb{Q}$$

may be infinite dimensional (Clemens 1983).

The bilinear map in (2.9) can now be written

$$\mathrm{Hom}^r(V_1,V_2)\times\mathrm{Hom}^s(V_2,V_3)\to\mathrm{Hom}^{r+s}(V_1,V_3),$$

and its associativity means that $\mathrm{Corr}_\sim(k)$ is a category. Let $H$ be a Weil cohomology theory. An element of $\mathrm{Hom}^r(hV,hW)$ defines a homomorphism $H^*(V)\to H^{*+r}(W)$ of degree $r$. In order to have the gradations preserved, we consider the category $\mathrm{Corr}^0_\sim(k)$ of correspondences of degree 0, i.e., now

$$\mathrm{Hom}(hV,hW)=\mathrm{Hom}^0(hV,hW)=A_\sim^{\dim V}(V\times W).$$

Every Weil cohomology theory such that $\sim\Rightarrow\mathrm{hom}$ factors uniquely through $\mathrm{Corr}^0_\sim(k)$ as a *functor to graded vector spaces.*

However, $\mathrm{Corr}^0_\sim(k)$ is not an abelian category. There being no good notion of an abelian envelope of a category, we define $\mathscr{M}^{\mathrm{eff}}_\sim(k)$ to be the pseudo-abelian envelope of $\mathrm{Corr}^0_\sim(k)$. This has objects $h(V,e)$ with $V$ as before and $e$ an idempotent in the ring $A_\sim^{\dim(V)}(V\times V)$; its morphisms are defined by

$$\mathrm{Hom}(h(V,e),h(W,f))=f\circ\mathrm{Hom}(hV,hW)\circ e.$$

This is a pseudo-abelian category, i.e., idempotent endomorphisms have kernels and cokernels. The functor

$$hV\rightsquigarrow h(V,\mathrm{id})\colon\ \mathrm{Corr}^0_\sim(k)\to\mathscr{M}^{\mathrm{eff}}_\sim(k)$$

fully faithful and universal among functors from $\mathrm{Corr}^0_\sim(k)$ to pseudo-abelian categories. Therefore, every Weil cohomology theory such that $\sim\Rightarrow\mathrm{hom}$ factors uniquely through $\mathscr{M}^{\mathrm{eff}}_\sim(k)$.

The category $\mathscr{M}^{\mathrm{eff}}_\sim(k)$ is the *category of effective motives* over $k$. It is a useful category, but we need to enlarge it in order to have duals. One of the axioms for a Weil cohomology theory requires $H^2(\mathbb{P}^1)$ to have dimension 1. This means that the object $H^2(\mathbb{P}^1)$ is invertible in the category of vector spaces, i.e., the functor $W\rightsquigarrow H^2(\mathbb{P}^1)\otimes_Q W$ is an equivalence of categories. In $\mathscr{M}^{\mathrm{eff}}_\sim(k)$, the object $h\mathbb{P}^1$ decomposes into a direct sum

$$h\mathbb{P}^1=h^0\mathbb{P}^1\oplus h^2\mathbb{P}^1,$$

and we formally invert $h^2\mathbb{P}^1$. When we do this, we obtain a category $\mathscr{M}_\sim(k)$ whose objects are triples $h(V,e,m)$ with $h(V,e)$ as before and $m\in\mathbb{Z}$. Morphisms are defined by

$$\mathrm{Hom}(h(V,e,m),h(W,f,n))=f\circ A_\sim^{\dim(V)+n-m}(V,W)\circ e.$$

This is the category of *motives over* $k$. It contains the category of effective motives as a full subcategory.

The category $\mathrm{Corr}^0_\sim(k)$ has direct sums and tensor products:

$$hV\oplus hW=h(V\sqcup W)$$

$$hV\otimes hW=h(V\times W).$$

Both of these structures extend to the category of motives. The functor $-\otimes h^2(\mathbb{P}^1)$ is $h(V,e,m)\mapsto h(V,e,m+1)$, which is an equivalence of categories (because we allow negative $m$).

**Properties of the Category of Motives**

For the language of tensor categories, we refer the reader to Deligne and Milne 1982.

4.1. *The category of motives is a $\mathbb{Q}$-linear pseudo-abelian category. If $\sim=\mathrm{num}$, it is semisimple abelian. If $\sim=\mathrm{rat}$ and $k$ is not algebraic over a finite field, then it is not abelian.*

To say that $\mathscr{M}_\sim(k)$ is $\mathbb{Q}$-linear just means that the Hom sets are $\mathbb{Q}$-vector spaces and composition is $\mathbb{Q}$-bilinear. Thus $\mathscr{M}_\sim(k)$ is $\mathbb{Q}$-linear and pseudo-abelian by definition. If $\sim=\mathrm{num}$, the Hom sets are finite-dimensional $\mathbb{Q}$-vector spaces, and the $\mathbb{Q}$-algebras $\mathrm{End}(M)$ are semisimple (2.13). A pseudo-abelian category with these properties is a semisimple abelian category (i.e., an abelian category such that every object is a direct sum of simple objects). For the last statement, see Scholl 1994, 3.1.

4.2. *The category of motives is a rigid tensor category. If $V$ is nonsingular projective variety of dimension $d$, then there is a (Poincaré) duality*

$$h(V)^\vee\simeq h(V)(d).$$

A tensor category is a symmetric monoidal category. This means that every finite (unordered) family of objects has a tensor product, well defined up to a given isomorphism. It is rigid if every object $X$ admits a dual object $X^\vee$. The proof of (4.2) can be found in Saavedra Rivano 1972, VI, 4.1.3.5.

4.3. *Assume that the standard conjecture $C$ holds for some Weil cohomology theory.*

(a) *The category $\mathscr{M}_\sim(k)$ is abelian if and only if $\sim=\mathrm{num}$.*

(b) *The category $\mathscr{M}_{\mathrm{num}}(k)$ is a graded tannakian category.*

(c) *The Weil cohomology theories such that hom= num correspond to fibre functors on the Tannakian category $\mathscr{M}_{\mathrm{num}}(k)$.*

(a) We have seen (2.13) that $\mathscr{M}_\sim(k)$ is abelian if $\sim=\mathrm{num}$; the converse is proved in André 1996, Appendice.

(b) Let $V$ be a nonsingular projective variety over $k$. Let $\pi_0,\ldots,\pi_{2d}$ be the images of the Künneth projectors in $A^d_{\mathrm{num}}(V\times V)$. We define a gradation on $\mathscr{M}_{\mathrm{num}}(k)$ by setting

$$h(V,e,m)^r=h(V,e\pi_{r+2m},m).$$

Now the commutativity constraint can be modified so that

$$\dim(h(V,e,m)) = \sum_{r\geq 0} \dim_Q(eH^r(V)).$$

(rather than the alternating sum). Thus $\dim(M) \geq 0$ for all motives $M$, which implies that $\mathscr{M}_{\text{num}}(k)$ is tannakian (Deligne 1990, 7.1).

(c) Let $\omega$ be a fibre functor on $\mathscr{M}_{\text{num}}(k)$. Then $V \rightsquigarrow \omega(hV)$ is a Weil cohomology theory such that hom=num, and every such cohomology theory arises in this way.

4.4. *The standard conjectures imply that $\mathscr{M}_{\text{num}}(k)$ has a canonical polarization.*

The notion of a Weil form can be defined in any tannakian category over $\mathbb{Q}$. For example, a Weil form on a motive $M$ of weight $r$ is a map

$$\phi\colon M\otimes M \to 1(-r)$$

with the correct parity such that the map sending an endomorphism of $M$ to its adjoint is a positive involution on the $\mathbb{Q}$-algebra $\mathrm{End}(M)$. To give a *polarization* on $\mathscr{M}_{\text{num}}(k)$ is to give a set of Weil forms (said to be *positive* for the polarization) for each motive satisfying certain compatibility conditions; for example, if $\phi$ and $\phi'$ are positive, then so also are $\phi\oplus\phi'$ and $\phi\otimes\phi'$. The standard conjectures (especially of Hodge type) imply that $\mathscr{M}_{\text{num}}(k)$ admits a polarization for which the Weil forms defined by ample divisors are positive.

Let $\mathbb{1}$ denote the identity object $h^0(\mathbb{P}^0)$ in $\mathscr{M}_{\sim}(k)$. Then, almost by definition,

$$A^r_H(V) \simeq \mathrm{Hom}(\mathbb{1}, h^{2r}(V)(r)).$$

Therefore $V \rightsquigarrow h^r(V)$ has the properties expected of an "abstract" Weil cohomology theory.

## Alternatives to the Hodge, Tate, and Standard Conjectures

In view of the absence of progress on the Hodge, Tate, or standard conjectures since they were stated more than fifty years ago, Deligne has suggested that, rather than attempting to proving these conjectures, we should look for a good theory of motives, based on "algebraically-defined", but not necessarily algebraic, cycles. I discuss two possibilities for such algebraically-defined of cycles.

### Absolute Hodge Classes and Rational Tate Classes

Consider an algebraic variety $V$ over an algebraically closed field $k$ of characteristic zero. If $k$ is not too big, then we can choose an embedding $\sigma\colon k\to\mathbb{C}$ of $k$ in $\mathbb{C}$ and define a cohomology class on $k$ to be *Hodge relative to* $\sigma$ if it becomes Hodge on $\sigma V$. The problem with this definition is that it depends on the choice of $\sigma$. To remedy this, Deligne defines a cohomology class on $V$ to be *absolutely Hodge* if it is Hodge relative to every embedding $\sigma$. The problem with this definition is that, a priori, we know little more about absolute Hodge classes than we do about algebraic classes. To give substance to his theory, Deligne proved that all relative Hodge classes on abelian varieties are absolute. Hence they satisfy the standard conjectures and the Hodge conjecture, and so we have a theory of abelian motives over fields of characteristic zero that is much as Grothendieck envisaged it (Deligne 1982).

However, as Deligne points out, his theory works only in characteristic zero, which limits its usefulness for arithmetic questions. Let $A$ be an abelian variety over the algebraic closure $k$ of a finite field, and lift $A$ in two different ways to abelian varieties $A_1$ and $A_2$ in characteristic zero; let $\gamma_1$ and $\gamma_2$ be absolute Hodge classes on $A_1$ and $A_2$ of complementary dimension; then $\gamma_1$ and $\gamma_2$ define $l$-adic cohomology classes on $A$ for all primes $l$, and hence intersection numbers $(\gamma_1\cdot\gamma_2)_l \in \mathbb{Q}_l$. The Hodge conjecture implies that $(\gamma_1\cdot\gamma_2)_l$ lies in $\mathbb{Q}$ and is independent of $l$, but this is not known.

However, the author has defined the notion of a "good theory of rational Tate classes" on abelian varieties over finite fields, which would extend Deligne's theory to mixed characteristic. It is known that there exists at most one such theory and, if it exists, the rational Tate classes it gives satisfy the standard conjectures and the Tate conjecture; thus, if it exists, we would have a theory of abelian motives in mixed characteristic that is much as Grothendieck envisaged it (Milne 2009a).

### Almost-Algebraic Classes

4.5. Let $V$ be an algebraic variety over an algebraically closed field $k$ of characteristic zero. An *almost-algebraic class* on $V$ of codimension $r$ is an absolute Hodge class $\gamma$ on $V$ of codimension $r$ such that there exists a cartesian square

$$\begin{tikzcd} \mathscr{V} \arrow[d, "f"] & V \arrow[l] \arrow[d] \\ S & \mathrm{Spec}\, k \arrow[l] \end{tikzcd}$$

and a global section $\tilde{\gamma}$ of $R^{2r}f_*\mathbb{A}(r)$ satisfying the following conditions (cf. Tate 1994, p. 76),

- $S$ is the spectrum of a regular integral domain of finite type over $\mathbb{Z}$;
- $f$ is smooth and projective;
- the fibre of $\tilde{\gamma}$ over $\mathrm{Spec}(k)$ is $\gamma$, and the reduction of $\tilde{\gamma}$ at $s$ is algebraic for all closed points $s$ in a dense open subset $U$ of $S$.

If the above data can be chosen so that $(p)$ is in the image of the natural map $U\to\mathrm{Spec}\,\mathbb{Z}$, then we say that

$\gamma$ is *almost-algebraic at* $p$—in particular, this means that $V$ has good reduction at $p$.

4.6. Note that the residue field $\kappa(s)$ at a closed point $s$ of $S$ is finite, and so the Künneth components of the diagonal are almost-algebraic (3.12). Therefore the space of almost-algebraic classes on $X$ is a graded $\mathbb{Q}$-subalgebra

$$AA^*(X) = \bigoplus_{r \geq 0} AA^r(X)$$

of the $\mathbb{Q}$-algebra of $AH^*(X)$ of absolute Hodge classes. For any regular map $f\colon Y \to X$ of complete smooth varieties, the maps $f_*$ and $f^*$ send almost-algebraic classes to almost-algebraic classes. Similar statements hold for the $\mathbb{Q}$-algebra of classes almost-algebraic at $p$.

### Beyond Pure Motives

In the above I considered only pure motives with rational coefficients. This theory should be generalized in (at least) three different directions. Let $k$ be a field.

- There should be a category of mixed motives over $k$. This should be an abelian category whose whose semisimple objects form the category of pure motives over $k$. Every mixed motive should be equipped with a weight filtration whose quotients are pure motives. Every algebraic variety over $k$ (not necessarily nonsingular or projective) should define a mixed motive.
- There should be a category of complexes of motives over $k$. This should be a triangulated category with a $t$-structure whose heart is the category of mixed motives. Each of the standard Weil cohomology theories lifts in a natural way to a functor from all algebraic varieties over $k$ to a triangulated category; these functors should factor through the category of complexes of motives.
- Everything should work mutatis mutandis over $\mathbb{Z}$.

Much of this was envisaged by Grothendieck.[39] There has been much progress on these questions, which I shall not attempt to summarize (see André 2004, Mazza et al. 2006, Murre et al. 2013).

## 5. Deligne's Proof of the Riemann Hypothesis over Finite Fields

Grothendieck attempted to deduce the Riemann hypothesis in arbitrary dimensions from the curves case,[40] but no "dévissage" worked for him.[41] After he announced the standard conjectures, the conventional wisdom became that, to prove the Riemann hypothesis in dimension $> 1$, one should prove the standard conjectures.[42] However, Deligne recognized the intractability of the standard conjectures and looked for other approaches. In 1973 he startled the mathematical world by announcing a proof of the Riemann hypothesis for all smooth projective varieties over finite fields.[43] How this came about is best described in the following conversation.[44]

*Gowers:* Another question I had. Given the clearly absolutely remarkable nature of your proof of the last remaining Weil conjecture, it does make one very curious to know what gave you the idea that you had a chance of proving it at all. Given that the proof was very unexpected, it's hard to understand how you could have known that it was worth working on.

*Deligne:* That's a nice story. In part because of Serre, and also from listening to lectures of Godement, I had some interest in automorphic forms. Serre understood that the $p^{11/2}$ in the Ramanujan conjecture should have a relation with the Weil conjecture itself. A lot of work had been done by Eichler and Shimura, and by Verdier, and so I understood the connection between the two. Then I read about some work of Rankin, which proved, not the estimate one wanted, but something which was a $1/4$ off—the easy results were $1/2$ off from what one wanted to have. As soon as I saw something like that I knew one had to understand what he was doing to see if one could do something similar in other situations. And so I looked at Rankin, and there I saw that he was using a result

[39] Certainly, Grothendieck envisaged mixed motives and motives with coefficients in $\mathbb{Z}$ (see the footnote on p. 5 of Kleiman 1994 and Grothendieck's letters to Serre and Illusie).

[40] Serre writes (email July 2015):

> He was not the first one. So did Weil, around 1965; he looked at surfaces, made some computations, and tried (vainly) to prove a positivity result. He talked to me about it, but he did not publish anything.

[41] "I have no comments on your attempts to generalize the Weil-Castelnuovo inequality…; as you know, I have a sketch of a proof of the Weil conjectures starting from the curves case." (Grothendieck, *Grothendieck-Serre Correspondence*, p. 88, 1959). Grothendieck hoped to prove the Weil conjectures by showing that every variety is birationally a quotient of a product of curves, but Serre constructed a counterexample. See *Grothendieck-Serre Correspondence*, pp. 145–148, 1964, for a discussion of this and Grothendieck's "second attack" on the Weil conjectures.

[42] "Pour aller plus loin et généraliser complètement les résultats obtenus par Weil pour le cas $n = 1$, il faudrait prouver les propriétés suivantes de la cohomologie $\ell$-adique …[the standard conjectures]" Dieudonné 1974, IX n°19, p. 224.

[43] A little earlier, he had proved the Riemann hypothesis for varieties whose motive, roughly speaking, lies in the category generated by abelian varieties (Deligne 1972).

[44] This is my transcription (slightly edited) of part of a telephone conversation which took place at the ceremony announcing the award of the 2013 Abel Prize to Deligne.

of Landau—the idea was that when you had a product defining a zeta function you could get information on the local factors out of information on the pole of the zeta function itself. The poles were given in various cases quite easily by Grothendieck's theory. So then it was quite natural to see what one could do with this method of Rankin and Landau using that we had information on the pole. I did not know at first how far I could go. The first case I could handle was a hypersurface of odd dimension in projective space. But that was a completely new case already, so then I had confidence that one could go all the way. It was just a matter of technique.

*Gowers:* It is always nice to hear that kind of thing. Certainly, that conveys the idea that there was a certain natural sequence of steps that eventually led to this amazing proof.

*Deligne:* Yes, but in order to be able to see those steps it was crucial that I was not only following lectures in algebraic geometry but some things that looked quite different (it would be less different now) the theory of automorphic forms. It was the discrepancy in what one could do in the two areas that gave the solution to what had to be done.

*Gowers:* Was that just a piece of good luck that you happened to know about both things.

*Deligne (emphatically):* Yes.

## Landau, Rankin, and the Ramanujan Conjecture

### Landau's Theorem

Consider a Dirichlet series $D(s) = \sum_{n=1}^{\infty} c_n n^{-s}$. Recall that there is a unique real number (possibly $\infty$ or $-\infty$) such that $D(s)$ converges absolutely for $\Re(s) > \sigma_0$ and does not converge absolutely for $\Re(s) < \sigma_0$. Landau's theorem states that, if the $c_n$ are real and nonnegative, then $D(s)$ has a singularity at $s = \sigma_0$. For example, suppose that

$$D(s) = \sum_{n\geq 1} c_n n^{-s} = \prod_{p \text{ prime}} \frac{1}{(1-a_{p,1}p^{-s})\cdots(1-a_{p,m}p^{-s})};$$

if the $c_n$ are real and nonnegative, and $\sum c_n n^{-s}$ converges absolutely for $\Re(s) > \sigma_0$, then

$$|a_{p,j}| \leq p^{\sigma_0}, \quad \text{all } p, j.$$

### Ramanujan's Conjecture

Let $f = \sum_{n\geq 1} c(n) q^n$, $c(1) = 1$, be a cusp form of weight $2k$ which is a normalized eigenfunction of the Hecke operators $T(n)$. For example, Ramanujan's function

$$\Delta(\tau) = \sum_{n=1}^{\infty} \tau(n) q^n \stackrel{\text{def}}{=} q \prod_{n=1}^{\infty} (1-q^n)^{24}$$

is such function of weight 12. Let

$$\Phi_f(s) = \sum_{n=1}^{\infty} c(n) n^{-s}$$

be the Dirichlet series associated with $f$. Because $f$ is an eigenfunction

$$\Phi_f(s) = \prod_{p \text{ prime}} \frac{1}{1 - c(p)p^{-s} + p^{2k-1-2s}}.$$

Write

$$(1 - c(p)T + p^{2k-1}T^2 = (1 - a_p T)(1 - a'_p T).$$

The Ramanujan-Petersson conjecture says that $a_p$ and $a'_p$ are complex conjugate. As $a_p a'_p = p^{2k-1}$, this says that

$$|a_p| = p^{k-1/2};$$

equivalently,

$$|c(n)| \leq n^{k-1/2} \sigma_0(n).$$

For $f = \Delta$, this becomes Ramanujan's original conjecture, $|\tau(p)| \leq 2p^{\frac{11}{2}}$. Hecke showed that, for a cusp form $f$ of weight $2k$,

$$|c(n)| = O(n^k).$$

There is much to be said about geometric interpretations of Ramanujan's function—see Serre 1968 and the letter from Weil to Serre at the end of the article.

### Rankin's Theorem

Let $f = \sum c(n) q^n$ be a cusp form of weight $2k$, and let $\mathscr{F}(s) = \sum_{n\geq 1} |c(n)|^2 n^{-s}$. Rankin (1939) shows that $\mathscr{F}(s)$ can be continued to a meromorphic function on the whole plane with singularities only at $s = k$ and $s = k-1$.[45] Using Landau's theorem, he deduced that

$$|c(n)| = O(n^{k-1/5}).$$

### A Remark of Langlands

Langlands remarked (1970, pp. 21–22) that Rankin's idea could be used to *prove* a generalized Ramanujan conjecture provided one knew enough about the poles of a certain family of Dirichlet series.[46]

[45] Selberg did something similar about the same time. Their approach to proving the analytic continuation of convolution $L$-functions has become known as the Rankin-Selberg method.

[46] "The remark about the consequences of functoriality for Frobenius-Hecke conjugacy classes of an automorphic representation, namely that their eigenvalues are frequently all of absolute value of 1, occurred to me on a train platform in Philadelphia, as I thought about the famous Selberg-Rankin estimate." Langlands 2015, p. 200.

Given an automorphic representation $\pi = \bigotimes \pi_p$ of an algebraic group $G$ and a representation $\sigma$ of the corresponding $L$-group, Langlands defines an $L$-function

$$L(s,\sigma,\pi)$$
$$= \prod_{\lambda} \left\{ (\text{power of } \pi) \cdot (\Gamma\text{−factor}) \cdot \prod_{p \text{ prime}} \frac{1}{1-\lambda(t_p)p^{-s}} \right\}^{m(\lambda)}$$

Here $\lambda$ runs over certain characters, $m(\lambda)$ is the multiplicity of $\lambda$ in $\sigma$, and $\{t_p\}$ is the (Frobenius) conjugacy class attached to $\pi_p$. Under certain hypotheses, the generalized Ramanujan conjecture states that, for all $\lambda$ and $p$,

$$|\lambda(t_p)| = 1.$$

Assume that, for all $\sigma$, the $L$-series $L(s,\sigma,\pi)$ is analytic for $\Re(s) > 1$. The same is then true of $D(s,\sigma) \stackrel{\text{def}}{=} \prod_\lambda \left\{ \prod_{p \text{ prime}} \frac{1}{1-\lambda(t_p)p^{-s}} \right\}^{m(\lambda)}$ because the $\Gamma$-function has no zeros. Let $\sigma = \rho \otimes \bar{\rho}$. The logarithm of $D(s,\sigma)$ is $\sum_p \sum_{n=1}^{\infty} \frac{\text{trace } \sigma^n(t_p)}{n} p^{-ns}$. As

$$\text{trace } \sigma^n(t_p) = \text{ trace } \rho^n(t_p) \cdot \text{ trace } \bar{\rho}^n(t_p) = |\text{trace } \rho^n(t_p)|^2,$$

the series for $\log D(s,\sigma)$ has positive coefficients. The same is therefore true of the series for $D(s,\sigma)$. We can now apply Landau's theorem to deduce that $|\lambda(t_p)| \leq p$. If $\lambda$ occurs in some $\sigma$, we can choose $\rho$ so that $m\lambda$ occurs in $\rho$. Then $(m\lambda)(t_p) = \lambda(t_p)^m$ is an eigenvalue of $\rho(t_p)$ and $\overline{\lambda(t_p)}^m$ is an eigenvalue of $\bar{\rho}$; hence $|\lambda(t_p)|^{2m}$ is an eigenvalue of $\sigma$, and $|\lambda(t_p)| \leq p^{1/2m}$ for all $m$. On letting $m \to \infty$, we see that $|\lambda(t_p)| \leq 1$ for all $\lambda$. Replacing $\lambda$ with $-\lambda$, we deduce that $|\lambda(t_p)| = 1$.

Note that it is the flexibility of Langlands's construction that makes this kind of argument possible. According to Katz (1976, p. 288), Deligne studied Rankin's original paper in an effort to understand this remark of Langlands.

### Grothendieck's Theorem

Let $U$ be a connected topological space. Recall that a *local system of* $\mathbb{Q}$*-vector spaces* on $U$ is a sheaf $\mathscr{E}$ on $U$ that is locally isomorphic to the constant sheaf $\mathbb{Q}^n$ for some $n$. For example, let $f\colon V \to U$ be a smooth projective map of algebraic varieties over $\mathbb{C}$; for $r \geq 0$, $R^r f_* \mathbb{Q}$ is a locally constant sheaves of $\mathbb{Q}$-vector spaces with fibre

$$(R^r f_* \mathbb{Q})_u \simeq H^r(V_u, \mathbb{Q})$$

for all $u \in U(\mathbb{C})$. Fix a point $o \in U$. There is a canonical (monodromy) action $\rho$ of $\pi_1(U,o)$ on the finite-dimensional $\mathbb{Q}$-vector space $\mathscr{E}_o$, and the functor $\mathscr{E} \rightsquigarrow (\mathscr{E}_o, \rho)$ is an equivalence of categories.

Now let $U$ be a connected nonsingular algebraic variety over a field $k$. In this case, there is a notion of a *local system of* $\mathbb{Q}_\ell$*-vector spaces* on $U$ (often called a smooth or lisse sheaf). For a smooth projective map of algebraic varieties $f\colon V \to U$ and integer $r$, the direct image sheaf $R^r f_* \mathbb{Q}_\ell$ on $U$ is a locally constant sheaf of $\mathbb{Q}_\ell$-vector spaces with fibre

$$(R^r f_* \mathbb{Q}_\ell)_u \simeq H^r(V_u, \mathbb{Q}_\ell)$$

for all $u \in U$.

The étale fundamental group $\pi_1(U)$ of $U$ classifies the finite étale coverings of $U$.[47] Let $\mathscr{E}$ be a local system on $U$, and let $E = \mathscr{E}_\eta$ be its fibre over the generic point $\eta$ of $U$. Again, there is a "monodromy" action $\rho$ of $\pi_1(U)$ on the finite-dimensional $\mathbb{Q}_\ell$-vector space $E$, and the functor $\mathscr{E} \rightsquigarrow (E,\rho)$ is an equivalence of categories.

Now let $U_0$ be a nonsingular geometrically-connected variety over finite field $k_0$; let $k$ be an algebraic closure of $k_0$, and let $U = (U_0)_k$. Then there is an exact sequence

$$0 \to \pi_1(U) \to \pi_1(U_0) \to \mathrm{Gal}(k/k_0) \to 0.$$

The maps reflect the fact that a finite extension $k'/k_0$ pulls back to a finite covering $U' \to U_0$ of $U_0$ and a finite étale covering of $U_0$ pulls back to a finite étale covering of $U$.

Let $\mathscr{E}$ be a local system of $\mathbb{Q}_\ell$-vector spaces on $U_0$. Grothendieck (1964)[48] proved the following trace formula

$$\sum_{u \in |U|^\pi} \mathrm{Tr}(\pi_u \mid \mathscr{E}_u) = \sum_r (-1)^r \mathrm{Tr}(\pi \mid H_c^r(U,\mathscr{E})). \tag{32}$$

Here $|U|$ denotes the set of closed points of $U$, $\pi_u$ denotes the local Frobenius element acting on the fibre $\mathscr{E}_u$ of $\mathscr{E}$ at $u$, and $\pi$ denotes the reciprocal of the usual Frobenius element of $\mathrm{Gal}(k/k_0)$. Let

$$Z(U_0,\mathscr{E}_0,T) = \prod_{u \in |U_0|} \frac{1}{\det(1-\pi_u T^{\deg(u)} \mid \mathscr{E}_u)};$$

written multiplicatively, (32) becomes

$$Z(U_0,\mathscr{E}_0,T) = \prod_r \det(1-\pi T \mid H_c^r(U,E))^{(-1)^{r+1}} \tag{33}$$

[47] When the base field is $\mathbb{C}$, the topological fundamental group of $V^{\text{an}}$ classifies the covering spaces of $V^{\text{an}}$ (not necessarily finite). The Riemann existence theorem implies that the two groups have the same finite quotients, and so the étale fundamental group is the profinite completion of the topological fundamental group.

[48] In fact, Grothendieck only sketched the proof of his theorem in this Bourbaki talk, but there are detailed proofs in the literature, for example, in the author's book on étale cohomology.

(cf. (25), p. 29). For the constant sheaf $\mathbb{Q}_\ell$, (33) becomes ((28), p. 32). Grothendieck proves (32) by a dévissage to the case that $U$ is of dimension 1.[49]

We shall need (33) in the case that $U_0$ is an affine curve, for example, $\mathbb{A}^1$. In this case it becomes

(34)
$$\prod_{u\in|U_0|}\frac{1}{\det(1-\pi_u T^{\deg(u)}\mid\mathscr{E}_u)}=\frac{\det(1-\pi T\mid H^1_c(U,E))}{\det(1-\pi T\mid E_{\pi_1(U)}(-1))}.$$

Here $E_{\pi_1(U)}$ is the largest quotient of $E$ on which $\pi_1(U)$ acts trivially (so the action of $\pi_1(U_0)$ on it factors through $\mathrm{Gal}(k/k_0)$).

### Proof of the Riemann Hypothesis for hypersurfaces of Odd Degree

Following Deligne, we first consider a hypersurface $V_0$ in $\mathbb{P}^{d+1}_{k_0}$ of odd degree $\delta$. For a hypersurface, the cohomology groups coincide with those of the ambient space except in the middle degree, and so

$$Z(V,T)=\frac{P_d(V,T)}{(1-T)(1-qT)\cdots(1-q^dT)},$$

with $P_d(V,T)=\det(1-\pi T\mid H^d(V,\mathbb{Q}_\ell))$. Note that

$$P_d(V,T)=Z(V,T)(1-T)\cdots(1-q^dT)\in\mathbb{Q}[T].$$

We embed our hypersurface in a one-dimensional family. The homogeneous polynomials of degree $\delta$ in $d+2$ variables, considered up to multiplication by a nonzero scalar, form a projective space $\mathbb{P}^N$ with $N=\binom{d+\delta+1}{\delta}$. There is a diagram

$$\begin{tikzcd} H \arrow[r, hook] \arrow[d, "f"'] & \mathbb{P}^N\times\mathbb{P}^{d+1} \arrow[dl] \\ \mathbb{P}^N & \end{tikzcd}$$

in which the fibre $H_P$ over a point $P$ of $\mathbb{P}^N(k)$ is the hypersurface (possibly reducible) in $\mathbb{P}^{d+1}$ defined by $P$. Let $P_0$ be the polynomial defining $V_0$. We choose a "general" line through $P_0$ in $\mathbb{P}^N$ and discard the finitely many points where the hypersurface is singular of not connected. In this way, we obtain a smooth projective map $f\colon\mathscr{V}_0\to U_0\subset\mathbb{P}^1$ whose fibres are hypersurfaces of degree $\delta$ in $\mathbb{P}^{d+1}$; let $o\in U_0$ be such that the fibre over $o$ is our given hypersurface $V_0$.

Let $\mathscr{E}_0=R^df_*\mathbb{Q}_\ell$ and let $E$ denote the corresponding $\pi_1(U_0)$-module. Then

(35)
$$Z(U_0,\mathscr{E}_0,T)=\prod_{u\in|U_0|}\frac{1}{P_d(V_u,T^{\deg(u)})}$$
$$=\frac{\det(1-\pi T\mid H^1_c(U,E))}{\det(1-\pi T\mid E_{\pi_1(U)}(-1))}.$$

There is a canonical pairing of sheaves

$$R^df_*\mathbb{Q}_\ell\times R^df_*\mathbb{Q}_\ell\to R^{2d}f_*\mathbb{Q}_\ell\simeq\mathbb{Q}_\ell(-d)$$

which, on each fibre becomes cup product

$$H^d(\mathscr{V}_u,\mathbb{Q}_\ell)\times H^d(\mathscr{V}_u,\mathbb{Q}_\ell)\to H^{2d}(\mathscr{V}_u,\mathbb{Q}_\ell)\simeq\mathbb{Q}_\ell(-d).$$

This gives a pairing

$$\psi\colon E_0\times E_0\to\mathbb{Q}_\ell(-d)$$

which is skew-symmetric (because $d$ is odd), nondegenerate (by Poincaré duality for the geometric generic fibre of $f$), and $\pi_1(U_0)$-invariant (because it arises from a map of sheaves on $U_0$). Deligne proves that, if the line through $P_0$ in $\mathbb{P}^N$ is chosen to be sufficiently general,[50] then the image of $\pi_1(U)$ in $\mathrm{Sp}(E,\psi)$ is dense for the Zariski topology (i.e., there is "big geometric monodromy"). Thus the coinvariants of $\pi_1(U)$ in $E$ are equal to the coinvariants of $\mathrm{Sp}(E,\psi)$, and the invariant theory of the symplectic group is well understood.

Note that

$$\log Z(U_0,\mathscr{E}_0,T)=\sum_{u\in|U_0|}\sum_n\mathrm{Tr}(\pi_u^n\mid E_u)\frac{(T^{\deg u})^n}{n}.$$

The coefficients $\mathrm{Tr}(\pi_u^n\mid E_u)$ are rational. When we replace $\mathscr{E}_0$ with $\mathscr{E}_0^{\otimes 2m}$, we replace $\mathrm{Tr}(\pi_u^n\mid E_u)$ with

$$\mathrm{Tr}(\pi_u^n\mid E_u^{\otimes 2m})=\mathrm{Tr}(\pi_u^n\mid E_u)^{2m}$$

which is $\geq 0$.

To apply Landau's theorem, we need to find the poles of $Z(U_0,\mathscr{E}_0^{\otimes 2m},q^{-s})$, which, according to Grothendieck's theorem (see (35)) are equal to the zeros of $\det(1-\pi T\mid E_{\pi_1(U)}(-1))$. Note that

$$\mathrm{Hom}(E^{\otimes 2m},\mathbb{Q}_\ell)^{\mathrm{Sp}(\psi)}=\mathrm{Hom}((E^{\otimes 2m})_{\mathrm{Sp}(\psi)},\mathbb{Q}_\ell).$$

The map

$$x_1\otimes\cdots\otimes x_{2m}\mapsto\psi(x_1,x_2)\cdots\psi(x_{2m-1},x_{2m})\colon E^{\otimes 2m}\to\mathbb{Q}_\ell(-dm)$$

is invariant under $\mathrm{Sp}(\psi)$, and $\mathrm{Hom}(E^{\otimes 2m},\mathbb{Q}_\ell)^{\mathrm{Sp}(\psi)}$ has a basis of maps $\{f_1,\ldots,f_M\}$obtained from this one by permutations. The map

(36)
$$a\mapsto(f_1(a),\ldots,f_M(a))\colon E^{\otimes 2m}\to\mathbb{Q}_\ell(-dm)^M$$

induces an isomorphism

$$(E^{\otimes 2m})_{\mathrm{Sp}(\psi)}\to\mathbb{Q}_\ell(-dm)^M.$$

[49] This proof of the rationality of the zeta function of an arbitrary variety is typical of Grothendieck: find a generalization that allows the statement to be proved by a "devissage" to the (relative) dimension one case.

[50] This may require a finite extension of the base field $k_0$.

The Frobenius element $\pi \in \mathrm{Gal}(k/k_0)$ acts on $\mathbb{Q}_\ell(-md)$ as $q^{md}$, and so it acts on $E_{\pi_1(U_0)}^{\otimes 2m}(-1)$ as $q^{md+1}$. We can now apply Landau's theorem to deduce that

$$\left|\alpha^{2m}\right| \leq q^{md+1}$$

for every eigenvalue $\alpha$ of $\pi_o$ acting on $\mathscr{E}_o = H^d(V_0, \mathbb{Q}_\ell)$. On taking the $2m$th root and letting $m \to \infty$, we find that $|\alpha| \leq q^{d/2}$. As $q^d/\alpha$ is also an eigenvalue of $\pi_o$ on $H^d(V_0, \mathbb{Q}_\ell)$, we deduce that $|\alpha| = q^{d/2}$.

### Proof of the Riemann Hypothesis for Nonsingular Projective Varieties

We shall prove the following statement by induction on the dimension of $V_0$. According to the discussion in (2.7), it completes the proof of Conjectures W1–W4.

**Theorem 5.1.** *Let $V_0$ be an nonsingular projective variety over $\mathbb{F}_q$. Then the eigenvalues of $\pi$ acting on $H^r(V, \mathbb{Q}_\ell)$ are algebraic numbers, all of whose complex conjugates have absolute value $q^{r/2}$.*

#### The Main Lemma (Restricted Form)

The following is abstracted from the proof of Riemann hypothesis for hypersurfaces of odd degree.

**Main Lemma 5.2.** *Let $\mathscr{E}_0$ be a local system of $\mathbb{Q}_\ell$-vector spaces on $U_0$, and let $E$ be the corresponding $\pi_1(U_0)$-module. Let $d$ be an integer. Assume:*

*(i) (Rationality.) For all closed points $u \in U_0$, the characteristic polynomial of $\pi_u$ acting on $\mathscr{E}_u$ has rational coefficients.*

*(ii) There exists a nondegenerate $\pi_1(U_0)$-invariant skew-symmetric form*

$$\psi \colon E \times E \to \mathbb{Q}_\ell(-d).$$

*(iii) (Big geometric monodromy.) The image of $\pi_1(U)$ in $Sp(E, \psi)$ is open.*

*Then:*

*(a) For all closed points $u \in U_0$, the eigenvalues of $\pi_u$ acting on $\mathscr{E}_u$ have absolute value $(q^{\deg u})^{d/2}$.*

*(b) The characteristic polynomial of $\pi$ acting on $H_c^1(U, \mathscr{E})$ is rational, and its eigenvalues all have absolute value $\leq q^{d/2+1}$.*

*Proof.* As before, $E_{\pi_1(U)}^{\otimes 2m}$ is isomorphic to a direct sum of copies of $\mathbb{Q}_\ell(-md)$, from which (a) follows. Now (b) follows from (34). $\square$

#### A Reduction

**Proposition 5.3.** *Assume that for all nonsingular varieties $V_0$ of even dimension over $\mathbb{F}_q$, every eigenvalue $\alpha$ of $\pi$ on $H^{\dim V}(V, \mathbb{Q}_\ell)$ is an algebraic number such that*

$$q^{\frac{\dim V}{2} - \frac{1}{2}} < |\alpha'| < q^{\frac{\dim V}{2} + \frac{1}{2}}$$

*for all complex conjugates $\alpha'$ of $\alpha$. Then Theorem 5.1 holds for all nonsingular projective varieties over $\mathbb{F}_q$.*

*Proof.* Let $V_0$ be a smooth projective variety of dimension $d$ (not necessarily even) over $\mathbb{F}_q$, and let $\alpha$ be an eigenvalue of $\pi$ on $H^d(V, \mathbb{Q}_\ell)$. The Künneth formula shows that $\alpha^m$ occurs among the eigenvalues of $\pi$ acting on $H^{dm}(V^m, \mathbb{Q}_\ell)$ for all $m \in \mathbb{N}$. The hypothesis in the proposition applied to an even $m$ shows that

$$q^{\frac{md}{2} - \frac{1}{2}} < |\alpha'|^m < q^{\frac{md}{2} + \frac{1}{2}}$$

for all conjugates $\alpha'$ of $\alpha$. On taking the $m$th root and letting $m$ tend to infinity over the even integers, we find that

$$|\alpha'| = q^{\frac{d}{2}}.$$

Now let $\alpha$ be an eigenvalue of $\pi$ acting on $H^r(V, \mathbb{Q}_\ell)$. If $r > d$, then $\alpha^d$ is an eigenvalue of $\pi$ acting on

$$H^r(V, \mathbb{Q}_\ell)^{\otimes d} \otimes H^0(V, \mathbb{Q}_\ell)^{\otimes r-d} \subset H^{rd}(V^r, \mathbb{Q}_\ell)$$

because $\pi$ acts as 1 on $H^0(V, \mathbb{Q}_\ell)$. Therefore $\alpha^d$ is algebraic and $|\alpha^d| = q^{\frac{rd}{2}}$, and similarly for its conjugates. The case $r < d$ can be treated similarly using that $\pi$ acts as $q^d$ on $H^{2d}(V, \mathbb{Q}_\ell)$, or by using Poincaré duality. $\square$

#### Completion of the Proof

To deduce Theorem 5.1 from (5.2), Deligne uses the theory of Lefschetz pencils and their cohomology (specifically vanishing cycle theory and the Picard-Lefschetz formula). In the complex setting, this theory was introduced by Picard for surfaces and by Lefschetz (1924) for higher dimensional varieties. It was transferred to the abstract setting by Deligne and Katz in SGA 7 (1967–1969). Deligne had earlier used these techniques to prove the following weaker result:

> let $V_0$ be a smooth projective variety over a finite field $k_0$ of odd characeristic that lifts, together with a polarization, to characteristic zero. Then the polynomials $\det(1 - \pi T \mid H^r(V, \mathbb{Q}_\ell))$ have integer coefficients independent of $\ell$ (Verdier 1972).

Thus, Deligne was already an expert in the application of these methods to zeta functions.

Let $V$ be a nonsingular projective variety $V$ of dimension $d \geq 2$, and embed $V$ into a projective space $\mathbb{P}^m$. The hyperplanes $H \colon \sum a_i T_i = 0$ in $\mathbb{P}^m$ form a projective space, called the *dual projective space* $\check{\mathbb{P}}^m$. A *pencil* of hyperplanes is a line $D = \{\alpha H_0 + \beta H_\infty \mid (\alpha \colon \beta) \in \mathbb{P}^1(k)\}$ in $\check{\mathbb{P}}^m$. The *axis* of the pencil is

$$A = H_0 \cap H_\infty = \bigcap_{t \in D} H_t.$$

Such a pencil is said to be a *Lefschetz pencil* for $V$ if (a) the axis $A$ of the pencil cuts $V$ transversally; (b) the hyperplane sections $V_t \overset{\text{def}}{=} V \cap D_t$ are nonsingular for all

$t$ in some open dense subset $U$ of $D$; (c) for all $t \notin U$, the hyperplane section $V_t$ has only a single singularity and that singularity is an ordinary double point. Given such a Lefschetz pencil, we can blow $V$ up along the $A \cap V$ to obtain a proper flat map

$$f\colon V^* \to D$$

such that the fibre over $t$ in $D$ is $V_t = V \cap H_t$.

We now prove Theorem 5.1 (and hence the Riemann hypothesis). Let $V_0$ be a nonsingular projective variety of even dimension $d \geq 2$ over a finite field $k_0$. Embed $V_0$ in a projective space. After possibly replacing the embedding with its square and $k_0$ with a finite extension, we may suppose that there exists a Lefschetz pencil and hence a proper map $f\colon V_0^* \to D = \mathbb{P}^1$. Recall (5.3) that we have to prove that

$$q^{d/2-1/2} < |\alpha| < q^{d/2+1/2}$$

for all eigenvalues $\alpha$ on $H^d(V, \mathbb{Q}_\ell)$. It suffices to do this with $V_0$ replaced by $V_0^*$. From the Leray spectral sequence,

$$H^r(\mathbb{P}^1, R^s f_* \mathbb{Q}_\ell) \implies H^{r+s}(V, \mathbb{Q}_\ell),$$

we see that it suffices to prove a similar statement for each of the groups

$$H^2(\mathbb{P}^1, R^{d-2} f_* \mathbb{Q}_\ell), \quad H^1(\mathbb{P}^1, R^{d-1} f_* \mathbb{Q}_\ell), \quad H^0(\mathbb{P}^1, R^d f_* \mathbb{Q}_\ell).$$

The most difficult group is the middle one. Here Deligne applies the Main Lemma to a certain quotient subquotient $\mathscr{E}$ of $R^{d-1} f_* \mathbb{Q}_\ell$. The hypothesis (i) of the Main Lemma is true from the induction hypothesis; the skew-symmetric form required for (ii) is provided by an intersection form; finally, for (iii), Deligne was able to appeal to a theorem of Kazhdan and Margulis. Now the Main Lemma shows that $|\alpha| \leq q^{d/2+1/2}$ for an eigenvalue of $\pi$ on $H^1(\mathbb{P}^1, \mathscr{E})$, and a duality argument shows that $q^{d-1/2} \leq |\alpha|$.

**Notes.** Deligne's proof of the Riemann hypothesis over finite fields is well explained in his original paper (Deligne 1974) and elsewhere. There is also a purely $p$-adic proof (Kedlaya 2006).

### Beyond the Riemann Hypothesis Over Finite Fields

In a seminar at IHES, Nov. 1973 to Feb. 1974, Deligne improved his results on zeta functions. In particular he proved stronger forms of the Main Lemma. These results were published in Deligne 1980, which has become known as Weil II. Even beyond his earlier results on the Riemann hypothesis, these results have found a vast array of applications, which I shall not attempt to summarize (see the various writings of Katz, especially Katz 2001, and the book Kiehl and Weissauer 2001).

## 6. The Hasse-Weil Zeta Function

### The Hasse-Weil Conjecture

Let $V$ be a nonsingular projective variety over a number field $K$. For almost all prime ideals $\mathfrak{p}$ in $\mathscr{O}_K$ (called good), $V$ defines a nonsingular projective variety $V(\mathfrak{p})$ over the residue field $\kappa(\mathfrak{p}) = \mathscr{O}_K/\mathfrak{p}$. Define the zeta function of $V$ to be

$$\zeta(V,s) = \prod_{\mathfrak{p}\text{ good}} \zeta(V(\mathfrak{p}), s).$$

For example, if $V$ is a point over $\mathbb{Q}$, then $\zeta(X,s)$ is the original Riemann zeta function $\prod_p \frac{1}{1-p^{-s}}$. Using the Riemann hypothesis for the varieties $V(\mathfrak{p})$, one sees that the that the product converges for $\Re(s) > \dim(V)+1$. It is possible to define factors corresponding to the bad primes and the infinite primes. The completed zeta function is then conjectured to extend analytically to a meromorphic function on the whole complex plane and satisfy a functional equation. The function $\zeta(V,s)$ is usually called the *Hasse-Weil zeta function* of $V$, and the conjecture the *Hasse-Weil conjecture.*

More precisely, let $r$ be a natural number. Serre (1970) defined:

(a) polynomials $P_r(V(\mathfrak{p}),T) \in \mathbb{Z}[T]$ for each good prime (namely, those occurring in the zeta function for $V(\mathfrak{p})$);
(b) polynomials $Q_\mathfrak{p}(T) \in \mathbb{Z}[T]$ for each bad prime $\mathfrak{p}$;
(c) gamma factors $\Gamma_v$ for each infinite prime $v$ (depending on the Hodge numbers of $V \otimes_k k_v$);
(d) a rational number $A > 0$.

Set

$$\xi(s) = A^{s/2} \cdot \prod_{\mathfrak{p}\text{ good}} \frac{1}{P_r(V(\mathfrak{p}), N\mathfrak{p}^{-1})} \cdot \prod_{\mathfrak{p}\text{ bad}} \frac{1}{Q_\mathfrak{p}(N\mathfrak{p}^{-1})} \cdot \prod_{v\text{ infinite}} \Gamma_v(s).$$

The Hasse-Weil conjecture says that $\zeta_r(s)$ extends to a meromorphic function on the whole complex plane and satisfies a functional equation

$$\xi(s) = w\xi(r+1-s), \quad w = \pm 1.$$

### History

According to Weil's recollections (Œuvres, II, p. 529),[51] Hasse defined the Hasse-Weil zeta function for an elliptic curve over $\mathbb{Q}$, and set the Hasse-Weil

[51] Peu avant la guerre, si mes souvenirs sont exacts, G. de Rham me raconta qu'un de ses étudiants de Genève, Pierre Humbert, était allé à Göttingen avec l'intention d'y travailler sous la direction de Hasse, et que celui-ci lui avait proposé un probléme sur lequel de Rham désirait mon avis. Une courbe elliptique $C$ étant donnée sur le corps des rationnels, il s'agis-

conjecture in this case as a thesis problem! Initially, Weil was sceptical of the conjecture, but he proved it for curves of the form $Y^m = aX^n + b$ over number fields by expressing their zeta functions in terms of Hecke $L$-functions.[52] In particular, Weil showed that the zeta functions of the elliptic curves $Y^2 = aX^3 + b$ and $Y^2 = aX^4 + b$ can be expressed in terms of Hecke $L$-functions, and he suggested that the same should be true for all elliptic curves with complex multiplication. This was proved by Deuring in a "beautiful series" of papers.

Deuring's result was extended to all abelian varieties with complex multiplication by Shimura and Taniyama and Weil.

In a different direction, Eichler and Shimura proved the Hasse-Weil conjecture for elliptic modular curves by identifying their zeta functions with the Mellin transforms of modular forms.

Wiles et al. proved Hasse's "thesis problem" as part of their work on Fermat's Last Theorem (for a popular account of this work, see Darmon 1999).

### Automorphic $L$-Functions

The only hope one has of proving the Hasse-Weil conjecture for a variety is by identifying its zeta function with a known function, which has (or is conjectured to have) a meromorphic continuation and functional equation. In a letter to Weil in 1967, Langlands defined a vast collection of $L$-functions, now called automorphic (Langlands 1970). He conjectures that *all* $L$-functions arising from algebraic varieties over number fields (i.e., all motivic $L$-functions) can be expressed as products of automorphic $L$-functions.[53] The above examples and results on the zeta functions of Shimura varieties have made Langlands very optimistic:

> With the help of Shimura varieties mathematicians certainly have, for me, answered one main question: is it possible to express all motivic $L$-functions as products of automorphic $L$-functions? The answer is now beyond any doubt, "Yes!". Although no general proof is available, this response to the available examples and partial proofs is fully justified.[54] (Langlands 2015, p. 205.)

### The Functoriality Principle and Conjectures on Algebraic Cycles

As noted earlier, Langlands attaches an $L$-function $L(s, \sigma, \pi)$ to an automorphic representation $\pi$ of a reductive algebraic group $G$ over $\mathbb{Q}$ and a representation $\sigma$ of the corresponding $L$-group ${}^LG$. The functoriality principle asserts that a homomorphism of $L$-groups ${}^LH \to {}^LG$ entails a strong relationship between the automorphic representations of $H$ and $G$. This remarkable conjecture includes the Artin conjecture, the existence of nonabelian class field theories, and many other fundamental statements as special cases. And perhaps even more.

Langlands doesn't share the pessimism noted earlier concerning the standard conjectures and the conjectures of Hodge and Tate. He has suggested that the outstanding conjectures in the Langlands program are more closely entwined with the outstanding conjectures on algebraic cycles than is usually recognized, and that a proof of the first may lead to a proof of the second.

> I believe that it is necessary first to prove functoriality and then afterwards, with the help of the knowledge and tools obtained, to develop a theory of correspondences and simultaneously of motives over $\mathbb{Q}$ and other global fields, as well as $\mathbb{C}$.[55] (Langlands 2015, p. 205).

In support of this statement, he mentions two examples (Langlands 2007, 2015). The first, Deligne's proof of the Riemann hypothesis over finite fields, has already been discussed in some detail. I now discuss the second example.

#### The Problem

Let $A$ be a polarized abelian variety with complex multiplication over $\mathbb{Q}^{\mathrm{al}}$. The theory of Shimura and Taniyama describes the action on $A$ and its torsion points of the Galois group of $\mathbb{Q}^{\mathrm{al}}$ over the reflex field of $A$. In the case that $A$ is an elliptic curve, the reflex field is a quadratic imaginary field; since one knows how complex conjugation acts, in this case we have

sait principalement, il me semble, d'étudier le produit infini des fonctions zêta des courbes $C_p$ obtenues en réduisant $C$ modulo $p$ pour tout nombre premier $p$ pour lequel $C_p$ est de genre 1; plus précisément, il fallait rechercher si ce produit possède un prolongement analytique et une équation fonctionnelle. J'ignore si Pierre Humbert, ou bien Hasse, avaient examiné aucun cas particulier. En tout cas, d'après de Rham, Pierre Humbert se sentait découragé et craignait de perdre son temps et sa peine.

[52] Weil also saw that the analogous conjecture over global function fields can sometimes be deduced from the Weil conjectures.

[53] Or perhaps there should even be an identification of the tannakian category defined by motives with a subcategory of a category defined by automorphic representations. ("Wenn man sich die Langlands-Korrespondenz als eine Identifikation einer durch Motive definierten Tannaka-Kategorie mit einer Unterkategorie einer durch automorphe Darstellungen definierten Kategorie vorstellt…" Langlands 2015, p. 201.)

[54] Mit Hilfe der Shimuravarietäten haben die Mathematiker gewiß eine, für mich, Hauptfrage beantwortet: wird es möglich sein, alle motivischen $L$-Funktionen als Produkte von automorphen $L$-Funktionen auszudrücken? Die Antwort ist jetzt zweifellos, "Ja!". Obwohl kein allgemeiner Beweis vorhanden ist, ist diese Antwort von den vorhanden Beispielen und Belegstücken her völlig berechtigt.

[55] Ich habe schon an verschiedenen Stellen behauptet, daßes meines Erachtens nötig ist, erst die Funktorialität zu beweisen und dann nachher, mit Hilfe der damit erschlossenen Kenntnisse und zur Verfügung gestellten Hilfsmittel, eine Theorie der Korrespondenz und, gleichzeitig, der Motive, über $\mathbb{Q}$ und anderen globalen Körper, sowie über $\mathbb{C}$ zu begründen.

a description of how the full Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ acts. Is it possible to find such a description in higher dimensions?

Shimura studied this question, but concluded rather pessimistically that "In the higher-dimensional case, however, no such general answer seems possible." However, Grothendieck's theory of motives suggests the framework for an answer. The Hodge conjecture implies the existence of tannakian category of CM-motives over $\mathbb{Q}$, whose motivic Galois group is an extension

$$1 \to S \to T \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q}) \to 1$$

of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ (regarded as a pro-constant group scheme) by the Serre group $S$ (a certain pro-torus); étale cohomology defines a section to $T \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ over the finite adèles. Let us call this entire system the *motivic Taniyama group*. This system describes how $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ acts on CM abelian varieties over $\mathbb{Q}$ and their torsion points, and so the problem now becomes that of giving an explicit description of the motivic Taniyama group.

#### The Solution

Shimura varieties play an important role in the work of Langlands, both as a test of his ideas and for their applications. For example, Langlands writes (2007):

> Endoscopy, a feature of nonabelian harmonic analysis on reductive groups over local or global fields, arose implicitly in a number of contexts... It arose for me in the context of the trace formula and Shimura varieties.

Langlands formulated a number of conjectures concerning the zeta functions of Shimura varieties.

One problem that arose in his work is the following. Let $S(G,X)$ denote the Shimura variety over $\mathbb{C}$ defined by a Shimura datum $(G,X)$. According to the Shimura conjecture $S(G,X)$ has a canonical model $S(G,X)_E$ over a certain algebraic subfield $E$ of $\mathbb{C}$. The $\Gamma$-factor of the zeta function of $S(G,X)_E$ at a complex prime $v\colon E \hookrightarrow \mathbb{C}$ depends on the Hodge theory of the complex variety $v(S(G,X)_E)$. For the given embedding of $E$ in $\mathbb{C}$, there is no problem because $v(S(G,X)_E) = S(G,X)$, but for a different embedding, what is $v(S(G,X)_E)$? This question leads to the following problem:

> Let $\sigma$ be an automorphism of $\mathbb{C}$ (as an abstract field); how can we realize $\sigma S(G,X)$ as the Shimura variety attached to another (explicitly defined) Shimura datum $(G',X')$?

In his Corvallis talk (1979), Langlands states a conjectural solution to this problem. In particular, he constructs a "one-cocycle" which explains how to twist $(G,X)$ to obtain $(G',X')$. When he explained his construction to Deligne, the latter recognized that the one-cocycle also gives a construction of a conjectural Taniyama group. The descriptions of the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ on CM abelian varieties and their torsion points given by the motivic Taniyama group and by Langlands's conjectural Taniyama group are both consistent with the results of Shimura and Taniyama. Deligne proved that this property characterizes the groups, and so the two are equal. This solves the problem posed above.

Concerning Langlands's conjugacy conjecture itself, this was proved in the following way. For those Shimura varieties with the property that each connected component can be described by the moduli of abelian varieties, Shimura's conjecture was proved in many cases by Shimura and his students and in general by Deligne. To obtain a proof for a general Shimura variety, Piatetski-Shapiro suggested embedding the Shimura variety in a larger Shimura variety that contains many Shimura subvarieties of type $A_1$. After Borovoi had unsuccessfully tried to use Piatetski-Shapiro's idea to prove Shimura's conjecture directly, the author used it to prove Langlands's conjugation conjecture, which has Shimura's conjecture as a consequence. No direct proof of Shimura's conjecture is known.

### Epilogue

Stepanov (1969) introduced a new elementary approach for proving the Riemann hypothesis for curves, which requires only the Riemann-Roch theorem for curves. This approach was completed and simplified by Bombieri (1974) (see also Schmidt 1973).

How would our story have been changed if this proof had been found in the 1930s?


## Acknowledgement

I thank F. Oort and J-P. Serre for their comments on the first draft of this article, and Serre for contributing the letter of Weil. It would not have been possible to write this article without the University of Michigan Science Library, which provided me with a copy of the 1953 thesis of Frank Quigley, and where I was able to find such works as Castelnuovo's *Memoire Scelte* ... and Severi's *Trattato* ... available on open shelves.


## References


"Colmez and Serre 2001" is cited as "*Grothendieck-Serre Correspondence*".

Abdulali, S. 1994. Algebraic cycles in families of abelian varieties. Canad. J. Math. 46, No. 6, 1121–1134.

André, Y. 1996. Pour une théorie inconditionnelle des motifs. Inst. Hautes Études Sci. Publ. Math. No. 83, 5–49.

André, Y. 2004. Une introduction aux motifs (motifs purs, motifs mixtes, périodes). Panoramas et Synthèses, 17. Société Mathématique de France, Paris.

Artin, M. 1962. Grothendieck topologies, Notes of a seminar, Spring 1962 (Harvard University, Department of Mathematics).

Artin, M. 1964. Théorème de Weil sur la construction d'un groupe à partir d'une loi rationelle. Schémas en Groupes (Sém. Géométrie Algébrique, Inst. Hautes Études Sci., 1963/64) Fasc. 5b, Expose 18, 22 pp. Inst. Hautes Études Sci., Paris.

Artin, M. 1986. Néron models. Arithmetic geometry (Storrs, Conn., 1984), 213–230, Springer, New York.

Berthelot, P. 1974. Cohomologie cristalline des schémas de caractéristique $p > 0$. Lecture Notes in Mathematics, Vol. 407, Springer-Verlag, Berlin-New York.

Bloch, S. 1977. Algebraic K-theory and crystalline cohomology. Inst. Hautes Études Sci. Publ. Math. No. 47, 187–268.

Bombieri, E. 1974. Counting points on curves over finite fields (d'après S. A. Stepanov). Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, pp. 234–241. Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974.

Bosch, S.; Lütkebohmert, W.; Raynaud, M. 1990. Néron models. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 21, Springer-Verlag, Berlin.

Brigaglia, A; Ciliberto, C; Pedrini, C. 2004. The Italian school of algebraic geometry and Abel's legacy. The legacy of Niels Henrik Abel, 295–347, Springer, Berlin.

Bronowski, J. 1938. Curves whose grade is not positive in the theory of the base. J. Lond. Math. Soc. 13, 86–90.

Castelnuovo, G. 1906. Sulle serie algebriche di gruppi di punti appartenenti ad una curva algebrica. Rom. Acc. L. Rend. (5) 15, No. 1, 337–344.

Chow, W-L. 1954. The Jacobian variety of an algebraic curve. Amer. J. Math. 76, 453–476.

Clemens, H. 1983. Homological equivalence, modulo algebraic equivalence, is not finitely generated. Inst. Hautes Études Sci. Publ. Math. No. 58, 19–38 (1984).

Colmez, P.; Serre, J-P. (Eds) 2001. Correspondance Grothendieck-Serre. Edited by Pierre Colmez and Jean-Pierre Serre. Documents Mathématiques (Paris), 2. Société Mathématique de France, Paris, 2001. (A bilingual edition is available.) Cited as *Grothendieck-Serre Correspondence*.

Darmon, H. 1999. A proof of the full Shimura-Taniyama-Weil conjecture is announced. Notices Amer. Math. Soc. 46, No. 11, 1397–1401.

Davenport, H.; Hasse, H. 1935. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. J. Reine Angew. Math. 172, 151–182.

Deligne, P. 1972. La conjecture de Weil pour les surfaces $K3$. Invent. Math. 15, 206–226.

Deligne, P. 1974. La conjecture de Weil. I. Inst. Hautes Études Sci. Publ. Math. No. 43, 273–307.

Deligne, P. 1980. La conjecture de Weil. II. Inst. Hautes Études Sci. Publ. Math. No. 52, 137–252.

Deligne, P. 1982. Hodge cycles on abelian varieties (notes by J. S. Milne). In: Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Math., Vol. 900, Springer-Verlag, 1982, pp. 9–100.

Deligne, P. 1990. Catégories tannakiennes. The Grothendieck Festschrift, Vol. II, 111–195, Progr. Math., 87, Birkhäuser Boston, Boston, MA.

Deligne, P.; Milne, J., 1982. Tannakian categories. In: Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Math., Vol. 900, Springer-Verlag, pp. 101–228.

Deuring, M. 1941. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ. 14, 197–272.

Dieudonné, J. 1974. Cours de géometrie algébriques, 1, Presses Universitaires de France.

Dwork, B. 1960. On the rationality of the zeta function of an algebraic variety. Amer. J. Math. 82, 631–648.

Fulton, W. 1984. Intersection theory. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 2. Springer-Verlag, Berlin.

Griffiths, P. 1969. On the periods of certain rational integrals. II. Ann. of Math. (2) 90, 496–541.

Grothendieck, A. 1957. Sur quelques points d'algèbre homologique. Tôhoku Math. J. (2) 9, 119–221.

Grothendieck, A. 1958a. Sur une note de Mattuck-Tate. J. Reine Angew. Math. 200, 208–215.

Grothendieck, A. 1958b. The cohomology theory of abstract algebraic varieties. 1960 Proc. Internat. Congress Math. (Edinburgh, 1958), pp. 103–118, Cambridge Univ. Press, New York.

Grothendieck, A. 1964. Formule de Lefschetz et rationalité des fonctions $L$. Séminaire Bourbaki, Vol. 9, Exp. No. 279, 41–55, Décembre 1964.

Grothendieck, A. 1966. On the de Rham cohomology of algebraic varieties. Inst. Hautes Études Sci. Publ. Math. No. 29, 95–103.

Grothendieck, A. 1968. Crystals and the de Rham cohomology of schemes. Dix Exposés sur la Cohomologie des Schémas, pp. 306–358, North-Holland, Amsterdam; Masson, Paris.

Grothendieck, A. 1969. Standard conjectures on algebraic cycles. Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), pp. 193–199, Oxford Univ. Press, London.

Hasse, H. 1936. Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II, III, J. Reine Angew. Math. 175, 55–62; ibid. 69–88; ibid. 193–208.

Hodge, W. 1937. Note on the theory of the base for curves on an algebraic surface. J. Lond. Math. Soc. 12, 58–63.

Honda, T. 1968. Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Japan 20, 83–95.

Hurwitz, A. 1887. Ueber algebraische Correspondenzen und das verallgemeinerte Correspondenzprincip. Math. Ann. 28, No. 4, 561–585.

Igusa, Jun-ichi. 1949. On the theory of algebraic correspondances and its application to the Riemann hypothesis in function-fields. J. Math. Soc. Japan 1, 147–197.

Igusa, Jun-ichi. 1955. On some problems in abstract algebraic geometry. Proc. Nat. Acad. Sci. U. S. A. 41, 964–967.

Illusie, L. 1983. Finiteness, duality, and Künneth theorems in the cohomology of the de Rham-Witt complex. Algebraic geometry (Tokyo/Kyoto, 1982), 20–72, Lecture Notes in Math., 1016, Springer, Berlin.

Illusie, L. 2010. Reminiscences of Grothendieck and his school. Notices Amer. Math. Soc. 57, No. 9, 1106–1115.

Illusie, L. 2014. Grothendieck et la cohomologie étale. Alexandre Grothendieck: a mathematical portrait, 175–192, Int. Press, Somerville, MA.

Jannsen, U. 1992. Motives, numerical equivalence, and semi-simplicity. Invent. Math. 107, No. 3, 447–452.

Jannsen, U. 2007. On finite-dimensional motives and Murre's conjecture. Algebraic cycles and motives. Vol. 2, 112–142, London Math. Soc. Lecture Note Ser., 344, Cambridge Univ. Press, Cambridge.

Kani, E. 1984. On Castelnuovo's equivalence defect. J. Reine Angew. Math. 352, 24–70.

Katz, N. 1976. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), pp. 275–305, Amer. Math. Soc., Providence, RI.

Katz, N. 2001. *L*-functions and monodromy: four lectures on Weil II. Adv. Math. 160, No. 1, 81–132.
Kedlaya, K. 2006. Fourier transforms and $p$-adic 'Weil II'. Compos. Math. 142, No. 6, 1426–1450.
Kiehl, R.; Weissauer, R, 2001. Weil conjectures, perverse sheaves and l'adic (sic) Fourier transform. Springer-Verlag, Berlin.
Kleiman, S. 1968. Algebraic cycles and the Weil conjectures. Dix exposés sur la cohomologie des schémas, pp. 359–386, North-Holland, Amsterdam; Masson, Paris.
Kleiman, S. 1994. The standard conjectures. Motives (Seattle, WA, 1991), 3–20, Proc. Sympos. Pure Math., 55, Part 1, Amer. Math. Soc., Providence, RI.
Kleiman, S. 2005. The Picard scheme. Fundamental algebraic geometry, 235–321, Math. Surveys Monogr., 123, Amer. Math. Soc., Providence, RI.
Lang, S. 1957. Divisors and endomorphisms on an abelian variety. Amer. J. Math. 79, 761–777.
Lang, S. 1959. Abelian varieties. Interscience Tracts in Pure and Applied Mathematics. No. 7 Interscience Publishers, Inc., New York; Interscience Publishers Ltd., London.
Langlands, R. 1970. Problems in the theory of automorphic forms. Lectures in modern analysis and applications, III, pp. 18–61. Lecture Notes in Math., Vol. 170, Springer, Berlin.
Langlands, R. 1979. Automorphic representations, Shimura varieties, and motives. Ein Märchen. Automorphic forms, representations and *L*-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 205–246, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, RI.
Langlands, R. 2007. Reflexions on receiving the Shaw Prize, September 2007.
Langlands, R. 2015, Funktorialität in der Theorie der automorphen Formen: Ihre Endeckung und ihre Ziele. In: Emil Artin and Beyond—Class Field Theory and *L*-Functions (Dumbaugh, D., and Schwermer, J.) E.M.S.
Lefschetz, S. 1924. L'Analysis situs et la géométrie algébrique, Gauthier-Villars, Paris.
Matsusaka, T. 1957. The criteria for algebraic equivalence and the torsion group. Amer. J. Math. 79, 53–66.
Mattuck, A.; Tate, J. 1958. On the inequality of Castelnuovo-Severi. Abh. Math. Sem. Univ. Hamburg 22, 295–299.
Mazza, C.; Voevodsky, V.; Weibel, C. 2006. Lecture notes on motivic cohomology. Clay Mathematics Monographs, 2. American Mathematical Society, Providence, RI; Clay Mathematics Institute, Cambridge, MA.
Milne, J. 1986. Jacobian varieties. Arithmetic geometry (Storrs, Conn., 1984), 167–212, Springer, New York.
Milne, J. 2002. Polarizations and Grothendieck's standard conjectures. Ann. of Math. (2) 155, No. 2, 599–610.
Milne, J. 2009a. Rational Tate classes. Mosc. Math. J. 9, No. 1, 111–141,
Milne, J. 2009b. Motives—Grothendieck's Dream. Mathematical Advances in Translation, Vol. 28, No. 3, 193–206, 2009 (Chinese). Reprinted (in English) in Open problems and surveys of contemporary mathematics. Surveys of Modern Mathematics, 6. International Press, Somerville, MA; 2013.
Murre, J.; Nagel, J.; Peters, C. 2013. Lectures on the theory of pure motives. University Lecture Series, 61. American Mathematical Society, Providence, RI.
Néron, A. 1964. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Inst. Hautes Études Sci. Publ. Math. No. 21, 128 pp.
Oort, F. and Schappacher, N., Early history of the Riemann Hypothesis in positive characteristic. In: The legacy of Bernhard Riemann after one hundred and fifty years, edited by Lizhen Ji, Frans Oort and Shing-Tung Yau, International Press, 2016.
Quigley, F. D. 1953. On Schubert's Formula, thesis, University of Chicago.
Rankin, R. 1939. Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. I. The zeros of the function $\sum_{n=1}^{\infty} \tau(n)/n^s$ on the line $\Re s = \frac{13}{2}$. II. The order of the Fourier coefficients of integral modular forms. Proc. Cambridge Philos. Soc. 35, 351–372.
Roquette, P. 1953. Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts. J. Reine Angew. Math. 191, 199–252.
Rosen, M. 1986. Abelian varieties over $\mathbb{C}$. Arithmetic geometry (Storrs, Conn., 1984), 79–101, Springer, New York.
Saavedra Rivano, N. 1972. Catégories Tannakiennes. Lecture Notes in Mathematics, Vol. 265. Springer-Verlag, Berlin-New York.
Schappacher, N. 2006. Seventy years ago: The Bourbaki Congress at El Escorial and other mathematical (non)events of 1936. The Mathematical Intelligencer, Special issue International Congress of Mathematicians, Madrid, August 2006, 8–15.
Scholl, A. 1994. Classical motives. Motives (Seattle, WA, 1991), 163–187, Proc. Sympos. Pure Math., 55, Part 1, Amer. Math. Soc., Providence, RI.
Schmidt, F. K. 1931. Analytische Zahlentheorie in Körpern der Charakteristik $p$. Math. Zeitschr. 33, 1–32. (Habilitationsschrift).
Schmidt, W. 1973. Zur Methode von Stepanov. Acta Arith. 24, 347–367.
Segel, J. 2009. Recountings. Conversations with MIT mathematicians. Edited by Joel Segel. A K Peters, Ltd., Wellesley, MA.
Segre, B. 1937. Intorno ad un teorema di Hodge sulla teoria della base per le curve di una superficie algebrica. Ann. Mat. pura appl., Bologna, (4) 16, 157–163.
Serre, J-P. 1954. Cohomologie et géométrie algébrique. Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, Vol. III, pp. 515–520. Erven P. Noordhoff N. V., Groningen; North-Holland Publishing Co., Amsterdam, 1956.
Serre, J-P. 1958. Quelques propriétés des variétés abéliennes en caractéristique $p$. Amer. J. Math. 80, 715–739.
Serre, J-P. 1960. Analogues kählériens de certaines conjectures de Weil. Ann. of Math. (2) 71, 392–394.
Serre, J-P. 1968. Une interprétation des congruences relatives à la fonction $\tau$ de Ramanujan. Séminaire Delange-Pisot-Poitou: 1967/68, Théorie des Nombres, Fasc. 1, Exp. 14, 17 pp. Secrétariat mathématique, Paris.
Serre, J-P. 1970. Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Séminaire Delange-Pisot-Poitou, 1969/70, n°19.
Serre, J-P. 2001. Exposés de séminaires (1950–1999). Documents Mathématiques, 1. Société Mathématique de France, Paris.
Severi, F. 1903. Sulle corrispondence fra i punti di una curva algebrica e sopra certi classi di superficie, Mem. R. Accad. Sci. Torino (2) 54.
Severi, F. 1926. Trattato di geometria algebrica. Vol. 1. N. Zanichelli.
Shafarevich, I. 1994. Basic algebraic geometry. 1. Varieties in projective space. Second edition. Translated from the 1988 Russian edition and with notes by Miles Reid. Springer-Verlag, Berlin.
Steenrod, N. 1957. The work and influence of Professor S. Lefschetz in algebraic topology. Algebraic geometry and topology. A symposium in honor of S. Lefschetz, pp. 24–43. Princeton University Press, Princeton, NJ.
Stepanov, S. 1969. The number of points of a hyperelliptic curve over a finite prime field. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 33, 1171–1181.

Tate, J. 1964. Algebraic cohomology classes, 25 pages. In: Lecture notes prepared in connection with seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, MA, July 6–July 31, 1964.
Tate, J. 1966a. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Séminaire Bourbaki, Vol. 9, Exp. No. 306, 415–440.
Tate, J. 1966b. Endomorphisms of abelian varieties over finite fields. Invent. Math. 2, 134–144.
Tate, J. 1968. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda) Séminaire Bourbaki 352, (1968/69).
Tate, J. 1994. Conjectures on algebraic cycles in $\ell$-adic cohomology. Motives (Seattle, WA, 1991), 71–83, Proc. Sympos. Pure Math., 55, Part 1, Amer. Math. Soc., Providence, RI.
Verdier, J-L. 1972. Indépendance par rapport à $\ell$ des polynômes caractéristiques des endomorphismes de Frobenius de la cohomologie $\ell$-adique (d'après P. Deligne). Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 423, pp. 98–115.
Voevodsky, V. 1995. A nilpotence theorem for cycles algebraically equivalent to zero. Internat. Math. Res. Notices 1995, No. 4, 187–198.
Weil, A. 1940. Sur les fonctions algébriques à corps de constantes fini. C. R. Acad. Sci. Paris 210, 592–594.
Weil, A. 1941. On the Riemann hypothesis in function-fields. Proc. Nat. Acad. Sci. U. S. A. 27, 345–347.
Weil, A. 1946. Foundations of Algebraic Geometry. American Mathematical Society Colloquium Publications, Vol. 29. American Mathematical Society, New York.
Weil, A. 1948a. Sur les courbes algébriques et les variétés qui s'en déduisent. Actualités Sci. Ind., No. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris.
Weil, A. 1948b. Variétés abéliennes et courbes algébriques. Actualités Sci. Ind., No. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris.
Weil, A. 1948c. On some exponential sums. Proc. Nat. Acad. Sci. U. S. A. 34, 204–207.
Weil, A. 1949. Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc. 55, 497–508.
Weil, A. 1950. Variétés abéliennes. Algèbre et théorie des nombres. Colloques Internationaux du Centre National de la Recherche Scientifique, No. 24, pp. 125–127. Centre National de la Recherche Scientifique, Paris.
Weil, A. 1952. Fibre spaces in algebraic geometry (Notes by A. Wallace). University of Chicago, (mimeographed) 48 pp.
Weil, A. 1955. On algebraic groups of transformations. Amer. J. Math. 77, 355–391.
Weil, A. 1958. Introduction à l'étude des variétés kählériennes. Publications de l'Institut de Mathématique de l'Université de Nancago, VI. Actualités Sci. Ind. No. 1267 Hermann, Paris.
Weil, A., Œuvres Scientifiques, Collected papers. Springer-Verlag, New York-Heidelberg, Corrected second printing 1980. (For the first printing (1979), it may be necessary to subtract 4 from some page numbers.)
Zariski, O. 1952. Complete linear systems on normal varieties and a generalization of a lemma of Enriques-Severi. Ann. of Math. (2) 55, 552–592.

Finally, I append a letter from Weil to Serre concerning the "variété de Ramanujan". At the request of the editors, I include a translation.

12th February, 1960.

My dear Serre,

Let $V$ be a (complete, nonsingular) polarized variety; let $f$ be a morphism from $V$ to $V$ multiplying the fundamental class by $q = q(f)$; let $E = E(f,d)$ be the endomorphism determined by $f$ on the homology group of $V$ of topological dimension $d$; let $F(t) = F_{f,d}(t)$ be the characteristic polynomial of $E$, $\det(1-t.E)$. As you skillfully proved, the roots of $F(t)$ have absolute value of $q^{d/2}$.

Suppose that there exists a $V$, defined over $Z$, with the following wondrous property: when we reduce $V$ modulo $p$, and we take $d$ to be $11$ and $f$ to be the Frobenius morphism of $V$ reduced mod.$p$, then

$$F(t) = 1 - \tau(p).t + p^{11}t^2$$

with $\tau(p)$ the Ramanujan function. It is known that this satisfies remarkable congruences, which I shall write in my way. Put, for a given $p$ and arbitrary $i$, $q = p^i$, $f_q = f^i$ ($i$th iterate of the Frobenius, i.e., the Frobenius over the field with $q$ elements), $F_q = F_{f_q,11}(t)$. Then we have: $F_q(1) \equiv 0\ (691)$; $F_q(1) \equiv 0\ (2^8)$ if $p \neq 2$; $F_q(1) \equiv 0\ (23)$ if $(q/23) = -1$ (quadratic residue symbol; I find no indication in the literature for other values of $q$); $q.F_q(q^{-1}) \equiv 0\ (5^2.7)$; $q^2.F_q(q^{-2}) \equiv 0\ (3^2)$. As far as I know, this is the complete list of known congruences.

Questions: (a) can one prove, in the classical case, congruences for $F(t)$ having the general shape of the ones I have just written? (b) can one, starting from there, predict what should be the variety $V$ corresponding, in the way described above, to the Ramanujan function?

Note that $691$ is the numerator of $B_6$, and that the product $23.691$ appears in Milnor's formula for the number of differentiable structures on $S^{23}$! As Hirzebruch told me that $691$ appears only beginning in topological dimension $24$, this suggests that the "Ramanujan variety" may have dimension $12$ (??? of course $\tau$ corresponds to a modular form of degree $12$ as everyone knows).

Best regards, A. W.

THE INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY

Le 12 février 1960.

SCHOOL OF MATHEMATICS

Mon cher Serre,

Soit V une variété (complète, non singulière) ~~pxa~~ polarisée; soit f un morphisme de V dans V, multipliant la classe fondamentale par $q = q(f)$; soit $E = E(f,d)$ l'endomorphisme déterminé par f sur le groupe d'homologie de V de dimension topologique d; soit $F(t) = F_{f,d}(t)$ le polynome caractéristique de E, $\det(1 - t.E)$. Comme tu l'as savamment démontré, les racines de F(t) sont de valeur absolue $q^{d/2}$.

Admettons qu'il existe V, définie ~~xurxixx~~ sur Z, avec la mirifique propriété suivante: si on réduit V modulo p, et qu'on prenne $d = 11$, et $f$ = morphisme de Frobenius pour V réduite mod.p, alors $F(t) = 1 - \tau(p).t + p^{11}t^2$, avec $\tau(p)$ = la fonction de Ramanujan. Il est connu que celle-ci satisfait à des congruences remarquables, que je vais écrire à ma manière. Posons, pour un p donné et un i quelconque, $q = p^i$, $f_q = f^i$ (i-ième itérée de Frobenius, i.e. Frobenius sur le corps à q éléments), $F_q = F_{f_q,11}(t)$. Alors on a: $F_q(1) \equiv 0\ (691)$; $F_q(1) \equiv 0\ (2^8)$ si $p \neq 2$; $F_q(1) \equiv 0\ (23$ si $(q/23) = -1$ (symbole de résidu quadratique; je ne trouve pas d'indication dans la littérature pour les autres valeurs de q); $q.F_q(q^{-1}) \equiv 0\ (5^2.7)$; $q^2.F_q(q^{-2}) \equiv 0\ (3^2)$. Autant que je sais, c'est la liste complète des congruences connues.

Questions: (a) peut-on démontrer, dans le cas classique, des congruences pour F(t), qui aient l'allure générale de celles que je viens d'écrire ? (b) peut-on, en partant de là, deviner ce que pourrait être une variété V correspondant à la fonction de Ramanujan de la manière décrite ci-dessus ?

A noter que 691 est le numérateur de $B_6$ , et que le produit 23.691 apparaît dans la formule de Milnor sur le nombre de structures différentiables sur $S^{23}$ ! Comme Hirzebruch me dit que 691 n'apparaît qu'à partir de la dimension topologique 24, cela suggère que la "variété de Ramanujan" pourrait avoir la dimension 12 (??? bien entendu, $\tau$ est lié à $\Delta$ qui est une forme modulaire de degré 12 comme chacun sait).

Meilleures amitiés A.W.