These notes on the Weil conjectures are a blend of the exposition in Poonen [3, Chap. 7], Milne [1, Chap. II] and Mustaţă [2]. In this lecture we sketch the proof of the first two parts of the Weil conjectures for projective varieties of arbitrary dimension. The proof uses étale cohomology; proving that it has the properties we require is beyond the scope of the course. Hopefully seeing how it can be applied will help motivate the use of cohomology in arithmetic geometry more generally.

We rephrase part of the Weil conjecture in a form amenable to applying cohomology.

Theorem 34.9. *Suppose that X is a smooth, geometrically irreducible, projective variety of dimension n defined over $\mathbb{F}_q$.*

1. *(Rationality) There is a decomposition*

$$Z_X(T) = \frac{P_1(T)\dots P_{2n-1}(T)}{P_0(T)\dots P_{2n}(T)},$$

where each $P_i(T) \in \mathbb{Z}[T]$ can be factored over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i}(1-\alpha_{i,j}T).$$

2. *(Functional equation) There is an integer χ so that*

$$Z_X\left(\frac{1}{q^nT}\right) = \pm q^{n\chi/2}T^{\chi}Z_X(T).$$

35.1 Weil cohomology theories

The core idea of the proof is that we can study rational points as fixed points of a Frobenius map:

$$X(\mathbb{F}_q) = X(\bar{\mathbb{F}}_q)^F.$$

The easiest way to describe the map $F : X \to X$ is to embed $X \hookrightarrow \mathbb{P}^n$ into projective space and define F on $\mathbb{P}^n$ by $(a_0 : a_1 : \dots : a_n) \mapsto (a_0^q : a_1^q : \dots : a_n^q)$. Since the defining equations of X inside $\mathbb{P}^n$ have coefficients in $\mathbb{F}_q$, F induces a map $X \to X$.

In order to study F, we use a cohomology ring $H^*(X)$. This is will be a graded vector space: for each non-negative integer i there is a cohomology space $H^i(X)$, and there is a cup product $\cup : H^i(X) \times H^j(X) \to H^{i+j}(X)$. While cohomology has many properties that will be important to us, the fundamental one is that it is *functorial*: if X and Y are varieties and $f : X \to Y$ is a morphism then there is a morphism $f^* : H^*(Y) \to H^*(X)$. Moreover, $\mathrm{id}^* = \mathrm{id}$ and $(f \circ g)^* = g^* \circ f^*$. We will study $X(\mathbb{F}_q)$ by studying $F^* : H^*(X) \to H^*(X)$.

In order to prove the Weil conjectures, we will need much more than functoriality. We encode the desired properties of $H^*(X)$ into the following set of axioms.

Definition 35.1. Fix an algebraically closed field k (which will be $\bar{\mathbb{F}}_q$ for us) and a characteristic 0 field K. Below, X and Y will refer to nonsingular, connected, projective varieties. A *Weil cohomology theory* [2, §4.1] is given by the following data:

(D1) A contravariant functor $X \to H^*(X) = \sum_i H^i(X)$ from nonsingular, connected, projective varieties over k to graded commutative K-algebras. Graded commutative means that if $\alpha \in H^i(X)$ and $\beta \in H^j(X)$ then $\alpha \cup \beta = (-1)^{ij} \beta \cup \alpha$.

(D2) For every X, a linear trace map $\mathrm{Tr} = \mathrm{Tr}_X : H^{2\dim(X)}(X) \to K$.

(D3) For every X and for every closed irreducible subvariety $Z \subseteq X$ of codimension c, a *cohomology class* $\mathrm{cl}(Z) \in H^{2c}(X)$.

We require that the following axioms be satisfied:

(A1) For every X, all $H^i(X)$ have finite dimension over K. Moreover, $H^i(X) = 0$ unless $0 \leq i \leq 2\dim(X)$.

(A2) (Künneth property) For every X, Y, if $p_X : X \times Y \to X$ and $p_Y : X \times Y \to Y$ are the canonical projections, then

$$H^*(X) \otimes_K H^*(Y) \to H^*(X \times Y), \alpha \otimes \beta \mapsto p_X^*(\alpha) \cup p_Y^*(\beta)$$

is an isomorphism.

(A3) (Poincaré duality) For every X, the trace map $\mathrm{Tr} : H^{2\dim(X)}(X) \to K$ is an isomorphism, and for $0 \leq i \leq 2\dim(X)$, the bilinear map

$$H^i(X) \otimes_K H^{2\dim(X)-i}(X) \to K, \alpha \otimes \beta \mapsto \mathrm{Tr}_X(\alpha \cup \beta)$$

is a perfect pairing (i.e. it induces an isomorphism $H^{2\dim(X)-i}(X) \cong \mathrm{Hom}(H^i(X), K)$).

(A4) (Trace maps and products) For every X and Y, if $\alpha \in H^{2\dim(X)}(X)$ and $\beta \in H^{2\dim(Y)}(Y)$, we have

$$\mathrm{Tr}_{X\times Y}(p_X^*(\alpha) \cup p_Y^*(\beta)) = \mathrm{Tr}_X(\alpha)\,\mathrm{Tr}_Y(\beta).$$

(A5) (Exterior product of cohomology classes) For every X and Y and closed irreducible $Z \subseteq X$ and $W \subseteq Y$, we have

$$\mathrm{cl}(Z \times W) = p_X^*(\mathrm{cl}(Z)) \cup p_Y^*(\mathrm{cl}(W)).$$

(A6) (Pushforward of cohomology classes) For every morphism $f : X \to Y$, every irreducible closed $Z \subseteq X$ and every $\alpha \in H^{2\dim(Z)}(Y)$ we have

$$\mathrm{Tr}_X(\mathrm{cl}(Z) \cup f^*(\alpha)) = \deg(Z/f(Z)) \cdot \mathrm{Tr}_Y(\mathrm{cl}(f(Z)) \cup \alpha).$$

(A7) (Pullback of cohomology classes)[1] Let $f : X \to Y$ be a morphism and $Z \subseteq Y$ irreducible and closed, satisfying the following conditions:

a) All irreducible components $W_1, \ldots, W_r$ of $f^{-1}(Z)$ have dimension $\dim(Z) + \dim(X) - \dim(Y)$.

b) Either f is flat in a neighborhood of Z, or Z is *generically transverse* to f in the sense that $f^{-1}(Z)$ is generically smooth.

[1] We haven't defined all of the terms used in this axiom (such as flatness or the multiplicity of a component of $f^{-1}(Z)$). It is included for completeness, and we won't be using it directly.

Under these assumptions, if $[f^{-1}(Z)] = \sum_{i=1}^{r} m_i W_i$, then $f^*(\mathrm{cl}(Z)) = \sum_{i=1}^{r} m_i \,\mathrm{cl}(W_i)$.[2]

(A8) (Case of a point) If $x = \mathrm{Spec}(k)$ then $\mathrm{cl}(x) = 1$ and $\mathrm{Tr}_x(1) = 1$.

There are a number of known Weil cohomology theories: singular cohomology if $k = \mathbb{C}$ and étale and rigid cohomology if $k = \bar{\mathbb{F}}_q$. When X is defined over a perfect field k that is not algebraically closed (such as $\mathbb{F}_q$), we will write $H^i(X)$ for the cohomology of the base change of X to $\bar{k}$.

In order to count points that are fixed by Frobenius we will be looking at the intersection of its graph with the diagonal inside $X \times X$. We need some basic results from intersection theory (which will also help clarify the comment about χ being in the self intersection of the diagonal in $X \times X$).

Let Z and W be two closed irreducible subvarieties of X (or later, of $X \times X$). Recall that $\mathrm{codim}(Z) = \dim(X) - \dim(Z)$. We say that Z and W *intersect properly* if $\mathrm{codim}(Z \cap W) = \mathrm{codim}(Z) + \mathrm{codim}(W)$. We say that Z and Z' are *rationally equivalent*[3] if there is a subvariety $V \subseteq X \times \mathbb{P}^1$ so that

1. The projection $V \to \mathbb{P}^1$ is dominant. This implies that V intersects properly with $X \times \{0\}$ and with $X \times \{\infty\}$.
2. $Z = V \cap (X \times \{0\})$
3. $Z' = V \cap (X \times \{\infty\})$.

The benefit of considering rational equivalence is that we may use it to move one of Z or W if they don't intersect properly.

Lemma 35.2 (Chow's Moving Lemma)**.** *For any irreducible Z and W closed irreducible subvarieties of X, there is*[4] *a Z' that is rationally equivalent to Z that intersects properly with W; moreover, the intersection $Z' \cap W$ is well defined up to rational equivalence.*

We may thus define the intersection product $(Z \cdot W)$ to be the rational equivalence class of $Z' \cap W$. When $\dim(Z) + \dim(W) = \dim(X)$, the intersection $Z' \cap W$ will have dimension 0 and we will also write $(Z \cdot W) \in \mathbb{Z}$ for the degree of $(Z \cdot W)$. Note that it is possible for $(Z \cdot W)$ to be negative, since the moving lemma sometimes produces a linear combination of subvarieties with negative coefficients.

We can now state the trace formula, which provides a way of computing intersection numbers in terms of cohomology:

Theorem 35.3 (Trace formula)**.** *If $\phi : X \to X$ is an endomorphism and if $\Gamma_\phi, \Delta \subset X \times X$ are the graphs of ϕ and of the identity, then*

$$(\Gamma_\phi \cdot) = \sum_{i=0}^{2\dim(X)} (-1)^i \,\mathrm{Tr}(\phi^* \mid H^i(X)).$$

In particular, if Γ_ϕ and Δ intersect transversely (all the points have multiplicity 1) then the right hand side computes $\#\{x \in X : \phi(x) = x\}$.

[2] if Z is generically transverse to f then $m_i = 1$ for all i

[3] the actual definition is a bit more involved; see [5] for details

[4] One actually needs to work with cycles rather than just subvarieties: cycles are formal linear combinations of subvarieites

Corollary 35.4. *If $\Delta \subset X \times X$ is the diagonal, then*

$$(\Delta \cdot \Delta) = \sum_{i=0}^{2n} (-1)^i \dim_K H^i(X).$$

For a proof of Theorem 35.3 using the axioms of a Weil cohomology theorem see [2, §4.1].

35.2 Rationality of the Hasse-Weil zeta function

We can now prove the rationality of the zeta function. We start with two lemmas.

Lemma 35.5. *If ϕ is an endomorphim of a finite dimensional K-vector space then*

$$\det(\mathrm{id} - T\phi) = \exp\left(- \sum_{m \geq 1} \mathrm{Tr}(\phi^m \mid V) \frac{T^m}{m} \right).$$

Proof. We may assume that K is algebraically closed (otherwise we can base change everything to the algebraic closure). Choose a basis of V so that ϕ is given by an upper triangular matrix with diagonal entries $a_1, \dots, a_d$. Clearly we have $\det(\mathrm{id} - T\phi) = (1 - a_1 T) \dots (1 - a_d T)$. We also have

$$\begin{aligned} \exp\left(- \sum_{m \geq 1} \mathrm{Tr}(\phi^m \mid V) \frac{T^m}{m} \right) &= \exp\left(- \sum_{m \geq 1} \sum_{i=1}^{d} \frac{a_i^m T^m}{m} \right) \\ &= \exp\left(\sum_{i=1}^{d} \log(1 - a_i T) \right) = \prod_{i=1}^{d} (1 - a_i T). \end{aligned}$$

□

Lemma 35.6. *Let L be a field and $f = \sum_{m \geq 0} a_m T^m \in L[[T]]$. Then $f \in L(T)$ if and only if there exist $M, N \in \mathbb{Z}_{\geq 0}$ so that the linear span of the vectors*

$$\{(a_i, a_{i+1}, \dots, a_{i+N}) \in L^{\oplus(N+1)} | i \geq M\}$$

is a proper subspace of $L^{\oplus(N+1)}$. As a consequence, if L'/L is a field extension then $f \in L'(T)$ if and only if $f \in L(T)$.

Proof. We have $f \in L(T)$ if and only if there are $M, N \in \mathbb{Z}_{\geq 0}$ and $c_0, \dots, c_N \in L$ not all zero such that $f(T) \cdot \sum_{i=0}^{N} c_i T^i$ is a polynomial of degree less than $M + N$. This occurs precisely when $\sum_{j=0}^{N} c_{N-j} a_{i+j} = 0$ for all $i \geq M$, a condition that gives a nonzero linear function vanishing on the linear span of the vectors in the statement. The assertion that $f \in L'(T)$ if and only if $f \in L(T)$ follows from the fact that a set of vectors $v_1, \dots, v_r$ is linearly independent in an L-vector space V if only if $v_1 \otimes 1, \dots, v_r \otimes 1$ are linearly independent over L' in $V \otimes_L L'$. □

Theorem 35.7. *If X is a nonsingular, geometrically irreducible, n-dimensional projective variety over $\mathbb{F}_q$, set $P_i(T) = \det(\mathrm{id} - TF^* | H^i(X))$ for $0 \leq i \leq 2n$. Then*

$$Z_X(T) = \frac{P_1(T) \dots P_{2n-1}(T)}{P_0(T) \dots P_{2n}(T)}.$$

In particular, $Z_X(T) \in \mathbb{Q}(T)$.

Proof. Write $\bar{X}$ for the base change of X to $\bar{\mathbb{F}}_q$. We have that $N_m = \#\{x \in X(\bar{\mathbb{F}}_q) : F^m(x) = x\}$. Moreover, the graph $\Gamma_m \subset \bar{X} \times \bar{X}$ of F^m is transverse to the diagonal.[5] So by the trace formula we have

$$N_m = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}((F^m)^* | H^i(\bar{X})).$$

Applying Lemma 35.5 we get that $Z_X(T) = \prod_{i=0}^{2n} P_i(T)^{(-1)^{i+1}}$ and thus $Z_X(T) \in K(T)$. But since $Z_X(T)$ is a power series with rational coefficients, by Lemma 35.6 $Z_X(T) \in \mathbb{Q}(T)$. $\square$

35.3 The functional equation for the Hasse-Weil zeta function

We start with a lemma from linear algebra

Lemma 35.8. *Let $\phi : V \times W \to K$ be a perfect pairing of r-dimensional K-vector spaces. If $\lambda \in K^\times$, $f \in \operatorname{End}_K(V)$ and $g \in \operatorname{End}_K(W)$ satisfy $\phi(f(v), g(w)) = \lambda\phi(v, w)$ for all $v \in V$ and $w \in W$ then*

$$\det(\operatorname{id} - Tg|W) = \frac{(-1)^r \lambda^r T^r}{\det(f|V)} \det(\operatorname{id} - \lambda^{-1} T^{-1} f|V)$$

and

$$\det(g|W) = \frac{\lambda^r}{\det(f|V)}.$$

Proof. We may assume that K is algebraically closed and that $e_1, \ldots, e_r$ is a basis of V so that f has an upper triangular matrix. Let $e'_1, \ldots, e'_r$ be the basis of W so that $\phi(e_i, e'_j) = \delta_{i,j}$.

Note that g is invertible: if $g(w) = 0$ then $0 = \phi(f(v), g(w)) = \lambda\phi(v, w)$ for all $v \in V$ so $w = 0$ since ϕ is a perfect pairing. Since f is upper triangular, for $j < i$ we have $\phi(f(e_i), e'_j) = 0$ and thus $\phi(e_i, g^{-1}(e'_j)) = 0$. We get that the matrix for g^{-1} is lower triangular with respect to the basis $\{e'_j\}$. We can also relate the diagonals of the matrices $(a_{i,j})_{i,j}$ for f and $(b_{i,j})_{i,j}$ for g^{-1} since

$$a_{i,i} = \phi(f(e_i), e'_i) = \lambda\phi(e_i, g^{-1}(e'_i)) = \lambda b_{i,i}.$$

Writing $\det(f|V) = \prod_{i=1}^r a_{i,i}$ and $\det(g|W) = \prod_{i=1}^r b_{i,i}^{-1} = \lambda^r / \prod_{i=1}^r a_{i,i}$ we get the second statement.

We also have

$$\begin{aligned}
\det(\operatorname{id} - Tg|W) &= \det(g|W) \det(g^{-1} - T \operatorname{id}|W) \\
&= \frac{\lambda^r}{\det(f|V)} \cdot \prod_{j=1}^r (a_{j,j}\lambda^{-1} - T) \\
&= \frac{(-1)^r \lambda^r T^r}{\det(f|V)} \cdot \prod_{j=1}^r (1 - a_{j,j}\lambda^{-1} T^{-1}) \\
&= \frac{(-1)^r \lambda^r T^r}{\det(f|V)} \det(\operatorname{id} - \lambda^{-1} T^{-1} f|V).
\end{aligned}$$

$\square$

[5] See [2, Prop 2.4].

We also need some facts about the degree of the Frobenius morphism and how F^* acts on the top-dimensional cohomology space.

Lemma 35.9. *If $f : X \to Y$ is a generically finite, surjective morphism of degree d between smooth, connected projective varieties then $\mathrm{Tr}_X(f^*(\alpha)) = d\cdot\mathrm{Tr}_Y(\alpha)$ for all $\alpha \in H^{2\dim(Y)}(Y)$. In particular, if $X = Y$ then f^* acts as multiplication by d on $H^{2\dim(X)}(X)$.*

Proof. This is [2, Prop 4.1.iv]. □

Lemma 35.10. *If X is a smooth variety of dimension n over $\mathbb{F}_q$ then the degree of Frobenius is q^n.*

Proof. This is [4, Lemma 33.35.10]. □

Theorem 35.11. *If X is a nonsingular, geometrically irreducible, n-dimensional projective variety over $\mathbb{F}_q$, and $E = (\Delta \cdot \Delta)$ then*

$$Z_X(\frac{1}{q^n T}) = \pm q^{nE/2} T^E Z_X(T).$$

Proof. As in the proof of Theorem 35.7, we write $\bar{X}$ for the base change of X to $\bar{\mathbb{F}}_q$. We apply Lemma 35.8 to the perfect pairing

$$\phi_i : H^i(\bar{X}) \otimes H^{2n-i}(\bar{X}) \to H^{2n}(\bar{X}) \to K, \qquad \phi_i(\alpha \otimes \beta) = \mathrm{Tr}(\alpha \cup \beta)$$

given by Poincaré duality. By Lemmas 35.9 and 35.10, F^* acts as multiplication by q^n on $H^{2n}(\bar{X})$. Thus

$$\phi_i(F^*(\alpha), F^*(\beta)) = \mathrm{Tr}_{\bar{X}}(F^*(\alpha \cup \beta)) = \mathrm{Tr}_{\bar{X}}(q^n \alpha \cup \beta) = q^n \phi_i(\alpha, \beta)$$

for all $\alpha \in H^i(\bar{X})$ and $\beta \in H^{2n-i}(\bar{X})$. Now Lemma 35.8 implies that if we set $b_i = \dim_K H^i(\bar{X})$ and $P_i(T) = \det(\mathrm{id} - TF^*|H^i(\bar{X}))$ then

$$\det(F^*|H^{2n-i}(\bar{X})) = \frac{q^{nb_i}}{\det(F^*|H^i(\bar{X}))} \tag{35.1}$$

$$P_{2n-i}(T) = \frac{(-1)^{b_i} q^{nb_i} T^{b_i}}{\det(F^*|H^i(\bar{X}))} P_i\left(\frac{1}{q^n T}\right). \tag{35.2}$$

Using Theorem 35.7 and the fact that $E = \sum_{i=0}^{2n} (-1)^i b_i$ by Corollary 35.4, we get

$$\begin{aligned} Z_X\left(\frac{1}{q^n T}\right) &= \prod_{i=0}^{2n} P_i\left(\frac{1}{q^n T}\right)^{(-1)^{i+1}} \\ &= \prod_{i=0}^{2n} P_{2n-i}(T)^{(-1)^{i+1}} \cdot \frac{(-1)^E q^{nE} T^E}{\prod_{i=0}^{2n} \det(F^*|H^i(\bar{X}))^{(-1)^i}} \\ &= \pm Z_X(T) \cdot \frac{q^{nE} T^E}{q^{nE/2}} = \pm q^{nE/2} T^E Z_X(T). \end{aligned}$$

□

Note that the sign in the functional equation is $(-1)^{E+a}$, where $a = 0$ if $\det(F^*|H^n(\bar{X})) = q^{nb_n/2}$ and $a = 1$ if $\det(F^*|H^n(\bar{X})) = -q^{nb_n/2}$. If we write $P_n(T) = \prod_{j=1}^{b_n} (1 - \alpha_{n,j} T)$, (35.2) for $i = n$ implies that the multiset $\{\alpha_{n,1}, \ldots, \alpha_{n,b_n}\}$ is invariant under $\alpha \mapsto q^{b_n}/\alpha$, and $\prod_{j=1}^{b_n} \alpha_{n,j} = (-1)^a q^{nb_n/2}$. Thus a has the same parity as the number of $\alpha_{n,j}$ equal to $-q^{n/2}$.

References

[1] James Milne. *Lectures on étale cohomology*. https://www.jmilne.org/math/CourseNotes/LEC.pdf

[2] Mircea Mustaţă. *Zeta functions in algebraic geometry*. http://www-personal.umich.edu/~mmustata/zeta_book.pdf

[3] Bjorn Poonen. *Rational points on varieties*. Graduate Studies in Mathematics 186. Amer. Math. Soc., Providence, 2017. https://math.mit.edu/~poonen/papers/Qpoints.pdf

[4] The Stacks Project Authors. *Stacks Project: Frobenii*. https://stacks.math.columbia.edu/tag/0CC6

[5] The Stacks Project Authors. *Stacks Project: Rational Equivalence*. https://stacks.math.columbia.edu/tag/0AZG