1. September 30, 2019

In this lecture, we discuss the “prehistory” of the Weil conjectures from Gauss/Jacobi and Riemann/Dirichlet to Artin to Weil.

Readings 1.1. The primary source for this lecture is Weil’s 1949 paper [34]. We will assume some familiarity with basic facts about algebraic number theory; there are many references for this, but we generally will follow Neukirch [26].

Since this topic is old and well-studied, many other expositions of it are available. A particularly detailed one has been given by Milne [24].

For context, let’s start by formulating the Riemann hypothesis for Dedekind zeta functions.

Definition 1.2. Let $K$ be a number field, i.e., a finite-degree field extension of the field of rational numbers $\mathbb{Q}$. Let $\mathcal{O}_K$ be the ring of integers of $K$, which is to say the integral closure of $\mathbb{Z}$ in $K$ (more concretely, the elements of $K$ which are roots of monic polynomials with integer coefficients). A basic fact about $\mathcal{O}_K$ is that it is a Dedekind domain, and so every nonzero ideal can be written uniquely as a product of powers of maximal ideals. (Note: we say “maximal ideals” rather than “prime ideals” only to exclude the zero ideal.)
The Dedekind zeta function of $K$ is defined initially as the formal expression
\[ \zeta_K(s) := \prod_{p \subseteq \mathcal{O}_K} \frac{1}{1 - \text{Norm}_{K/Q}(p)^{-s}}, \]
where the product is over all the maximal ideals of $\mathcal{O}_K$ and $\text{Norm}_{K/Q}(p)$ is the cardinality of the quotient ring $\mathcal{O}_K/p$. For $s \in \mathbb{C}$ with $\text{Re}(s) > 1$, the product converges absolutely and so defines a holomorphic function without zeroes in that region. By unique factorization, we can rewrite the product as a sum
\[ \zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \text{Norm}_{K/Q}(I)^{-s} \]
where $I$ now runs over all nonzero ideals of $\mathcal{O}_K$.

**Theorem 1.3** (Dedekind). The function $\zeta_K(s)$ extends meromorphically to $\mathbb{C}$, with a simple pole at $s = 1$ and no other poles.

When $K = \mathbb{Q}$, $\zeta_K(s)$ is the usual Riemann zeta function. Like the latter, $\zeta_K(s)$ satisfies a functional equation relating its values at $s$ and $1 - s$. The cleanest way to conceptualize this is to use the language of **places**, as follows.

**Definition 1.4.** Each maximal ideal $p$ of $\mathcal{O}_K$ corresponds to a dense embedding of $K$ into a field complete with respect to a multiplicative absolute value, namely the fraction field of the $p$-adic completion of $\mathcal{O}_K$. These embeddings are called **finite places** of $K$. By Ostrowski’s theorem, the only other dense embeddings of $K$ into a field complete with respect to a (nontrivial) multiplicative absolute value are embeddings into $\mathbb{R}$ or $\mathbb{C}$, of which there are only finitely many; these are called **infinite places** of $K$. (For $K = \mathbb{Q}$, there is a unique infinite place, because $\mathbb{Q}$ maps in only one way into $\mathbb{R}$. Each prime number $b$ corresponds to the embedding of $\mathbb{Q}$ into the $p$-adic numbers $\mathbb{Q}_p$.)

One may then define a **completed zeta function** $\Lambda_K(s)$ by adding to the product a suitable factor for each infinite place. This factor has the form
\[ \pi^{-s/2} \Gamma(s/2) \text{ or } 2(2\pi)^{-s} \Gamma(s) \]
(where $\Gamma$ is Gauss’s meromorphic interpolation of the factorial function) depending on whether the completion of $\mathbb{Q}$ is isomorphic to $\mathbb{R}$ (a real place) or $\mathbb{C}$ (a complex place). With these factors in place, the functional equation has the form
\[ \Lambda_K(s) = \Lambda_K(1 - s). \]

**Conjecture 1.5** (Riemann Hypothesis). All nontrivial zeroes of $\zeta_K(s)$ (i.e., the ones not forced by the functional equation for $\Lambda_K(s)$) lie on the line $\text{Re}(s) = 1/2$.

It was suggested by Artin that there should be a close analogy between number fields and function fields. This grows out of the observation that for any finite field $\mathbb{F}_q$, the ring of integers $\mathbb{Z}$ and the polynomial ring $\mathbb{F}_q[t]$ are both Euclidean domains and their maximal ideals have finite residue fields. To build out this perspective, let’s make the following definition.

**Definition 1.6.** Fix a finite field $\mathbb{F}_q$. Let $K$ be a function field, by which I mean a finite-degree extension of the field of rational functions $\mathbb{F}_q(t)$. We may then define the ring of integers $\mathcal{O}_K$ and the Dedekind zeta function $\zeta_K(s)$ using exactly the same formulas as in the number field case; the analogue of Dedekind’s theorem also holds (with one minor quibble; see Remark 1.8). However, there is a key difference: in this case, the residue fields $\mathcal{O}_K/p$ all contain $\mathbb{F}_q$, so $\zeta_K(s)$ is a power series in $q^{-s}$ rather than a more general Dirichlet series.

The discussion of places, and the definition of and functional equation for the completed zeta function $\Lambda_K(s)$, also extend to this setting, but again there is a key difference the “infinite places” in the function field setting look just like finite places after a change of coordinates, so there is no need to give a separate definition for the missing factors in the completed zeta function. We will come back to this point in Remark 1.8.

The analogue of the Riemann hypothesis for function fields was formulated by Artin. A proof was announced by Weil in 1940 [30], and a second proof in 1941 [31], but due to the precarious state of both Weil’s life and world events in that period, the missing details from these announcements did not see print until 1948 [32, 33].
Theorem 1.7. For $K$ a function field, all nontrivial zeroes of $\zeta_K(s)$ (i.e., the ones not forced by the functional equation for $\Lambda_K(s)$) lie on the line $\text{Re}(s) = 1/2$.

Remark 1.8. The analogue of the Riemann zeta function here is the Dedekind zeta function for $K = \mathbb{F}_q(t)$, which one may easily calculate to be

$$\zeta_K(s) = \frac{1}{1 - q^{1-s}}$$

(see for example Definition 1.9 below). In this case, $\zeta_K(s)$ has no zeroes at all, so the Riemann hypothesis holds for particularly trivial reasons. Note however that $\zeta_K(s)$ has poles not only at $s = 1$, but also at $s = 1 + 2\pi in/\log q$ for any $n \in \mathbb{Z}$. The completed zeta function is

$$\Lambda_K(s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})}.$$  

For a general function field $K$, we will have

$$\zeta_K(s) = \text{polynomial in } q^{-s}$$

and

$$\Lambda_K(s) = \text{polynomial in } q^{-s}$$

From a modern point of view, we see that the properties of $\zeta_K(s)$ and $\lambda_K(s)$ amount to concrete statements about points on a certain algebraic curve over a finite field, whose proofs rely on now-standard techniques in algebraic geometry. For example, the proof of the functional equation for $\Lambda_K(s)$ uses the Riemann-Roch theorem for curves; Weil’s first proof of the Riemann hypothesis uses the embedding of a curve in its Jacobian variety; and Weil’s second proof uses the Hodge index theorem on the product of a curve with itself over the base field.

What one should keep in mind here is that none of this perspective was available to Weil. At the time he began his work, the subject of algebraic geometry only included varieties over the complex numbers; many of its best results did not comport with modern standards of rigor; commutative algebra had not yet developed to the point where it could be used to plug some of the gaps; and the key insights of Zariski, Serre, and Grothendieck needed to adapt sheaf theory into the modern foundations of algebraic geometry still lay years in the future. As a result, the completion of Weil’s announcements was delayed not just by geopolitical events, but also by Weil’s need to build interim foundations on which to base his work. While these foundations are no longer in widespread use, and modern accounts of Weil’s work typically reformulate his arguments using the theory of schemes, these reformulations are considered translations rather than completions.

In light of Remark 1.8, we now take the next step and reformulate the previous discussion in the language of algebraic geometry.

Definition 1.9. For $K$ a function field, let $X$ be the normalization of $\mathbb{A}^1_{\mathbb{F}_q}$ in $K$ and let $X^0$ be the set of closed points in $K$. Then we have

$$\zeta_K(s) = \prod_{P \in X^0} \frac{1}{1 - \#\kappa(P)^{-s}} = \prod_{P \in X^0} \frac{1}{1 - q^{-d_P s}}$$

where $\kappa(P)$ denotes the residue field of $P$ and $d_P = [\kappa(P) : \mathbb{F}_q]$. This can be rearranged to

$$\zeta_K(s) = \exp \left( \sum_{n=1}^{\infty} \frac{q^{-ns}}{n \# X(\mathbb{F}_q^n)} \right)$$

For example, for $K = \mathbb{F}_q(t)$, $X = \mathbb{A}^1_{\mathbb{F}_q}$ and so $X(\mathbb{F}_q^n) = q^n$ for all $n$; this recovers our earlier formula for $\zeta_K(s)$ in this case.

Remark 1.11. In the language of schemes, the previous discussion also applies in the case where $K$ is a number field, taking $X$ to be the normalization of $\text{Spec} \mathbb{Z}$ in $\text{Spec} \mathcal{O}_K$. In particular, (1.10) carries over.
Definition 1.12. Following Weil, we now let $X$ be an algebraic variety over $\mathbb{F}_q$ (or in modern language, a scheme of finite type over $\mathbb{F}_q$) and define $\zeta_X(s)$ as in (1.10):

$$
\zeta_X(s) := \prod_{P \in X^s} \frac{1}{1 - \#K(P)^{-s}} = \prod_{P \in X^s} \frac{1}{1 - q^{-d_P s}} = \exp \left( \sum_{n=1}^{\infty} \frac{q^{-ns}}{n} \#X(\mathbb{F}_q^n) \right).
$$

We then ask whether $\zeta_X(s)$ shares any of the previously observed properties when $\dim(X) > 1$. To get some clarity on this question, we consider some examples.

Example 1.13. Let $X = \mathbb{P}^2_q$. Then

$$
\zeta_X(s) = \frac{1}{(1 - \tau)(1 - q\tau) \cdots (1 - q^n \tau)}, \quad \tau = q^{-s}.
$$

We now consider a key example of Weil. At this point, our chain of inquiry, which so far has flowed naturally from the Riemann zeta function, links up with another thread from elementary number theory.

Example 1.14. Consider the diagonal hypersurface (or Fermat hypersurface)

$$
a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} = b \quad (n_i > 0, a_i, b \in \mathbb{F}_q).
$$

Over $\mathbb{Q}$, rational points on varieties of this form were considered first by Gauss in the setting where $q = p$ is prime, $r = 2$, and $n_0, n_1, n_2$ are small. For example, Gauss proved that for $p \neq 2$, the equation $x^2 - y^2 = 1$ has $p - 1$ solutions in $\mathbb{F}_p$.

Definition 1.15. Let $p$ be the characteristic of the finite field $\mathbb{F}_q$. Let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a multiplicative character and $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be an additive character (where $\mathbb{F}_p \to \mathbb{C}^\times$ is the map $x \mapsto e^{2\pi i x/p}$). The Gauss sum $g(\chi) = g(\chi, \psi)$ associated to $\chi$ is given by

$$
g(\chi) := \sum_{x \in \mathbb{F}_q} \chi(x) \psi(x) \in \mathbb{Z} \subset \mathbb{C}.
$$

(We have $g(\chi) \in \mathbb{Z}$ because $g(\chi)$ is a sum of roots of unity.)

Theorem 1.16. The Gauss sum $g(\chi)$ has the following properties.

1. (Gauss) We have $|g(\chi)|^2 = g(\chi)g(\overline{\chi}) = q$.
2. (Davenport–Hasse) For an extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$, put $\chi' := \chi \circ \text{Norm}_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ and $\psi' := \psi \circ \text{Trace}_{\mathbb{F}_{q^r}/\mathbb{F}_q}$. Then

$$
-g(\chi') = (-g(\chi))^{q^r}.
$$

Note that the conjugates of $g(\chi)$ are all themselves Gauss sums for other characters for the same $q$; consequently, $g(\chi)$ is an algebraic integer all of whose conjugates in $\mathbb{C}$ have absolute value $\sqrt{q}$.

Theorem 1.17 (Weil). Consider the Fermat hypersurface

$$
a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} = 0 \quad (n_i > 0, a_i \in \mathbb{F}_q).
$$

Then the number of points over $\mathbb{F}_q$ is given by

$$
q^r + \frac{q - 1}{q} \sum_{(\chi_0, \ldots, \chi_r)} \chi_0(a_0)^{-1} \cdots \chi_r(a_r)^{-1} g(\chi_0) \cdots g(\chi_r)
$$

where $(\chi_0, \ldots, \chi_r)$ runs over all tuples in which $\chi_i$ is a multiplicative character of $\mathbb{F}_q$ of order dividing $\gcd(n_i, q - 1)$ and $\chi_0 \cdots \chi_r = 1$.

By combining this with the Davenport-Hasse relation, we see that if we fix the hypersurface and count points over $\mathbb{F}_q^r$ for varying $r$, the answer is of the form $\sum \pm \alpha_r^q$. This forms a prototype for the Weil conjectures, to be introduced in the next lecture.
In this lecture, we give the full statement of Weil’s conjecture together with some small examples.

**Readings 2.1.** We roughly follow [17, Appendix C].

**Definition 2.2.** Let $k = \mathbb{F}_q$ be a finite field of $q$ elements, and $X/k$ be a quasi-projective algebraic variety (or more generally, any $k$-scheme of finite type; we will add hypotheses later in the statement). For any integer $r \geq 1$, let $k_r = \mathbb{F}_{q^r}$ be one field extension of $k$ with degree $r$ (which is unique up to noncanonical isomorphism). Write the zeta function (or more generally, any isomorphism). Let $\zeta_X(s)$ as $Z(X,q^{-s})$ for

$$Z(X,T) := \exp \left( \sum_{r=1}^{\infty} \frac{T^r}{r} \#X(k_r) \right) \in \mathbb{Z}[T].$$

(The containment $Z(X,T) \in \mathbb{Q}[T]$ is more obvious here, but the prior description of $\zeta_X(s)$ as an infinite product shows that $Z(X,T) \in \mathbb{Z}[T]$.)

**Theorem 2.3 (Weil conjectures).** The series $Z(X,T)$ has the following properties.

1. (Rationality) The series $Z(X,T)$ represents a rational function of $T$. We will often make a minor misuse of language and say that $Z(X,T)$ is a rational function of $T$.
2. (Functional equation) Suppose in addition that $X$ is smooth and projective of (pure) dimension $n$. Then

$$Z \left( X, \frac{1}{q^nT} \right) = \pm q^{nE/2}T^E Z(X,T)$$

for some integer $E$.
3. (Analogue of the Riemann hypothesis) Suppose in addition that $X$ is smooth and projective of (pure) dimension $n$. Then there is a unique factorization

$$Z(X,T) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) \cdots P_{2n}(T)}$$

in which $P_i(T)$ factors over $\mathbb{C}$ as $\prod_j (1 - \alpha_{ij}T)$ where $|\alpha_{ij}| = q^{j/2}$ for all $j$. In particular, the integer $E$ from (2) equals

$$E = \sum (-1)^i \deg(P_i).$$

Moreover, if $X$ is geometrically irreducible, then $P_0(T) = 1 - T$ and $P_{2n}(T) = 1 - q^nT$.

4. (Betti numbers) Suppose in addition that there exist a number field $K$, a finite set $S$ of prime ideals of $\mathcal{O}_K$, a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ not contained in $S$ with residue field isomorphic to $k$, and a smooth projective scheme $\mathfrak{X}$ over $\mathcal{O}_{K,S}$ (the localization of $\mathcal{O}_K$ at the primes in $S$) such that $X$ is isomorphic to the base extension $\mathfrak{X} \times_{\mathcal{O}_{K,S}} k$. (Informally, $X$ is the “reduction of $\mathfrak{X}$ modulo $\mathfrak{p}$.”) Then for any embedding $K \rightarrow \mathbb{C}$, the $i$-th Betti number of the topological space $(\mathfrak{X} \times_{\mathcal{O}_{K,S}} \mathbb{C})^{an}$ equals $\deg(P_i)$.

**Example 2.4.** If $X$ is set-theoretically the disjoint union of an open subscheme $Y$ and a closed subscheme $S$, then $X(k_r)$ is likewise the disjoint union of $Y(k_r)$ and $S(k_r)$, so formally

$$Z(X,T) = Z(Y,T) \cdot Z(S,T).$$

Let us apply this to the decomposition $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$. We obtain:

$$Z(\mathbb{P}^n,T) = Z(\mathbb{A}^n,T) \cdot Z(\mathbb{P}^{n-1},T) = \frac{1}{1-q^nT} \cdot Z(\mathbb{P}^{n-1},T)$$

. In particular, as we have seen before,

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

and similarly for $\mathbb{P}^n$ (see Set 2 exercises).

**Example 2.5.** For $X = C$ an elliptic curve, it can be shown by (relatively) elementary methods that

$$Z(C,T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$
where $a$ is an integer depending on $C$. It was shown by Hasse that moreover $|a| \leq 2q^{1/2}$; see [27, Chapter V] for an efficient proof.

**Remark 2.6.** Let’s see in detail what the Weil conjectures say for $\mathbb{P}^1$ and $C$.

1. Rationality is obviously true in both cases.
2. The functional equation for $\mathbb{P}^1$:
\[
Z(\mathbb{P}^1, \frac{1}{qT}) = \frac{qT^2}{(1-T)(1-qT)} \quad E = 2.
\]
   The functional equation for $C$:
\[
Z(C, \frac{1}{qT}) = \frac{1-aT+qT^2}{(1-T)(1-qT)} \quad E = 0.
\]
3. The factorization for $\mathbb{P}^1$ is obvious, and the analogue of the Riemann hypothesis carries no new information. The factorization for $C$ gives something nontrivial:
\[
P_i(T) = \begin{cases} 
1 - T & i = 0 \\
1 - aT + qT^2 & i = 1 \\
1 - qT & i = 2.
\end{cases}
\]
   The analogue of the Riemann hypothesis asserts that the roots of $P_1(T)$ lie on the circle $|T| = q^{-1/2}$; given the shape of the factorization, this is equivalent to the Hasse bound.
4. The Betti numbers of a topological $\mathbb{P}^1$ are 1, 0, 1. The Betti numbers of a topological elliptic curve are 1, 2, 1.

**Remark 2.7.** The factorization assertion was largely inspired by the example of Fermat hypersurfaces considered in the previous lecture. In that example, the numbers $\alpha_{ij}$ are the products of Gauss sums appearing in Weil’s formula.

**Remark 2.8.** The Betti number statement is a proxy for a stronger statement that Weil was not in a position to formulate precisely: what we wanted is to have $P_i(T) = \det(1 - FT, V_i)$ where $V_i$ is some “naturally occurring” vector space over a field and $F : V_i \to V_i$ is some endomorphism of the vector space. This perspective gives rise to the notion of *Weil cohomology* around which this course is centered.

But before we get there, note that the Betti number statement has a fair bit of power on its own. One important example computed by Weil in [34] is that of Grassmannian varieties, whose points correspond to subspaces of a fixed vector space. It is elementary to compute the number of points on a Grassmannian over a finite field (see Set 1 exercises); according to the Weil conjectures, this should then predict the Betti numbers of a Grassmannian over $\mathbb{C}$. These had been computed previously by Ehresmann using totally different methods.

Now that the Weil conjectures are a theorem, one can go further with this logic: in some cases, the first known computation of the Betti numbers of a topological space have used the Weil conjecture. A famous example is the Hilbert schemes of points on a smooth projective surface, by Göttscche [11].

We conclude this lecture with a very brief summary of how the Weil conjectures became a theorem. We will spend much of the course partially unpacking this summary.

1. The rationality was first proved in 1958 by Dwork [9] using an interpretation of $Z(X, T)$ in terms of $p$-adic analysis (where $p$ is the characteristic of the finite field).
2. During the 1960s, Grothendieck [13, 14] led a heroic effort to develop modern foundations of algebraic geometry, including a theory of *étale cohomology* that was meant to simulate the role of topological (singular) cohomology for complex algebraic varieties. This led to a new proof of rationality (via a form of the Lefschetz trace formula as per Remark 2.8), together with the first proofs of the functional equation (arising from Poincaré duality) and the Betti number condition (arising from a comparison theorem with singular cohomology).
3. Grothendieck proposed an approach to the analogue of the Riemann hypothesis via the so-called “Standard Conjectures”, but this approach never bore fruit.
In the 1970s, Deligne [7] came up with a more ad hoc approach for part (3) and proved it. Shortly thereafter, he gave a more robust proof [8]; this paper (commonly known as “Weil II”) is itself foundational in the study of zeta functions.

An important simplification of “Weil II” was discovered by Laumon [22], inspired by the stationary phase approximation from classical analysis.

Subsequently, Dwork’s methods were adapted to give a parallel cohomology theory, again based on $p$-adic analysis, in which the entire étale-cohomological proof of the Weil conjectures can be emulated. For example, a $p$-adic adaption of Laumon’s argument was given by Kedlaya [20].

3. October 7, 2019

In the previous lecture, we stated the Weil conjectures for an algebraic variety (or a scheme of finite type) $X$ over a finite field $F_q$, which imply that the zeta function

$$Z(X,T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \#X(F_{q^n})\right)$$

has properties that we identified as follows:

1. (rationality)
2. (functional equation)
3. (Riemann Hypothesis)
4. (Betti numbers)

As we pointed out in Remark 2.8, Weil went further and suggested an approach to these conjectures inspired by algebraic topology. In this lecture, we explain this approach.

Readings 3.1. We continue to follow [17, Appendix C].

Definition 3.2. Let $R$ be a commutative algebra over $F_q$; then the map $x \to x^q$ is an $F_q$-homomorphism from $R$ to itself. For any scheme $X$ over $F_q$, this construction induces a morphism $F : X \to X$ of $F_q$-schemes, called the absolute Frobenius of $X$ (more precisely, of $X$ over $F_q$). One easily sees that we have an action of $F$ on the set $X(F_q)$, whose set of fixed points is exactly $X(F_q)$. Also if we consider the action of $F^n$ on $X(F_q)$, then the fixed points would be $X(F_{q^n})$.

Remark 3.3. The inspiration for what follows is the general principle that the problem of counting fixed points of a self-map on a space should have something to do with computing traces of some associated linear map. A simple example of this principle is the following: if $\sigma$ is a permutation of $\{1, \ldots, n\}$, then the number of fixed points of $\sigma$ is equal to the trace of the permutation matrix associated to $\sigma$.

A vastly more sophisticated example is the Lefschetz trace formula. Let $T : S \to S$ be a continuous self-map of a topological space. Under suitable conditions, the quantity

$$\sum_i (-1)^i \text{Trace}(T, H^i(S))$$

gives a weighted count of the fixed points of $T$; in particular, the nonvanishing of this quantity can be used to establish the existence of a fixed point of $T$ (as in the Brouwer fixed point theorem).

With the above considerations Weil proposed the following.

Metaconjecture 3.4. (Weil) For some field $K$ of characteristic 0, there is a series of contravariant “cohomology” functors

$$H^i : \{\text{algebraic varieties over } F_q\} \to \{\text{finite dimensional vector spaces over } K\}$$

satisfying the following formula: for $i = 0, \ldots, 2d = 2 \dim(X)$, satisfying the formula

$$\#X(F_{q^n}) = \sum_{i=0}^{2d} (-1)^i \text{Trace}(F^n|H^i(X))$$

for every positive integer $n$, where $F^n : H^i(X) \to H^i(X)$ denotes (by abuse of notation) the linear transformation induced by the morphism $F^n : X \to X$. (One can also formulate a similar metaconjecture in terms of a sequence of covariant “homology” functors $H_i$.)
Remark 3.5. Let us see what the metaconjecture says, or could say with some refinement, about the Weil conjectures.

Firstly, it immediately implies rationality because
\[ Z(X, T) = \prod \det(1 - FT, \mathcal{H}^i(X))^{(-1)^{i+1}}. \]
Note that here, we use crucially that \( K \) is of characteristic 0; otherwise, we would only get this relation modulo the characteristic of \( K \).

Secondly, the functional equation would hold if the functors \( \mathcal{H}^i(X) \) satisfied “Poincaré Duality”, in the sense of admitting a perfect, \( F \)-equivariant pairing
\[ \mathcal{H}^i(X) \times \mathcal{H}^{2d-i}(X) \to K(-d) \]
where \( K(-d) \) denotes the field \( K \) with the “twisted” \( F \)-action, sending 1 to \( q^d \).

Thirdly, the Betti number statement would follow from an equality of dimensions between our \( \mathcal{H}^i(X) \) and the usual singular cohomology groups of the analytification.

It is not clear where the Riemann hypothesis would come from in this framework. We will discuss this later.

Let us note that we haven’t talked much about the field of coefficients \( K \) which plays an important role in our cohomology theory here (except to note that it must be of characteristic 0). The following example shows that we cannot hope to take \( K = \mathbb{Q} \).

Example 3.6. Suppose the metaconjecture holds for some \( K \). Let \( X/\mathbb{F}_q \) be a supersingular elliptic curve; we then have an action of \( \text{End}(X) \) on \( \mathcal{H}^1(X) \). As we have seen in the previous lecture, \( \mathcal{H}^1(X) \) is of dimension 2. However, if the endomorphisms of \( X_{\overline{\mathbb{F}_q}} \) are all defined over \( \mathbb{F}_q \), then \( \text{End}(X) \) whereas \( \text{End}(X) \) is a \( \mathbb{Z} \)-module of rank 4 contained in a (nonsplit) quaternion algebra over \( \mathbb{Q} \). However, a quaternion algebra over \( \mathbb{Q} \) cannot act on a 2-dimensional \( \mathbb{Q} \)-vector space unless it splits (i.e., is isomorphic to the matrix ring \( M_2(\mathbb{Q}) \)). Thus we cannot have \( K = \mathbb{Q} \).

In this example, the quaternion algebra in question remains nonsplit after tensoring over \( \mathbb{Q} \) with either \( \mathbb{R} \) or \( \mathbb{Q}_p \) (where \( p \) is the characteristic of \( \mathbb{F}_q \)). Consequently, the same argument rules out the possibility of satisfying the metaconjecture with \( K = \mathbb{R} \) or \( K = \mathbb{Q}_p \) (but it does not rule out extensions of these fields).

Remark 3.7. There are essentially two known approaches to constructing a Weil cohomology theory over a finite field of characteristic \( p \).

- For \( K = \mathbb{Q}_\ell \) where \( \ell \neq p \) is prime (which is not precluded by Example 3.6), the construction of étale cohomology by Grothendieck et al. will satisfy the metaconjecture.
- For \( K = \mathbb{Q}_p \), the construction of rigid cohomology developed by Berthelot et al. will satisfy the metaconjecture. (Note that we cannot take \( K = \mathbb{Q}_p \) because of Example 3.6.)

More on both of these later.

October 9, 2019

In this lecture, we study zeta functions for curves and abelian varieties.

Readings 4.1. We follow [23, Chapters VIII–IX]. For background on abelian varieties, see also [25].

Definition 4.2. Throughout this lecture, let \( X \) be a geometrically irreducible smooth projective curve of genus \( g \) over the finite field \( k = \mathbb{F}_q \) of characteristic \( p \). The field of rational functions \( k(t) \) is finite over \( k(t) \) for any element \( x \in k(X) \) which is not in \( k \) (or equivalently, which is not integral over \( k \)); note that the geometrically irreducible condition implies that \( k \) is integrally closed in \( k(t) \)).

Let \( \text{Div}(X) \) be the free abelian group generated by the closed points \( X^\circ \) of \( X \); the elements of \( \text{Div}(X) \) are called divisors on \( X \). We have a degree map
\[ \deg : \text{Div}(X) \to \mathbb{Z} \]
\[ \sum a_i [P_i] \mapsto \sum a_i [\kappa(P_i) : k] \]
where \( \kappa(P) \) denotes the residue field of \( P \). A divisor is called effective if it is a nonnegative linear combination of closed points; the degree of an effective divisor is also nonnegative.

8
Denote $\text{Div}^0(X) := \deg^{-1}(0)$. Then for $f \in k(X)^\times$, the divisor
\[
\text{div}(f) = \sum_{P \in X^\circ} \text{ord}_P(f)[P]
\]associated to $f$ belongs to $\text{Div}^0(X)$, hence
\[
\text{Pic}^0(X) := \text{coker} \left( \text{div} : k(X)^\times \to \text{Div}^0(X) \right)
\]is well-defined.

**Remark 4.3.** In what follows, it is helpful to bifurcate the discussion based on whether or not $X(k) = \emptyset$. For an example with $X(k) = \emptyset$, take the genus-2 curve
\[
y^2 = 2x^6 - 2x^2 + 2
\]over $\mathbb{F}_3$. (Note: it is impossible to have $X(k) = \emptyset$ for a curve of genus 1 over a finite field; see the supplementary exercises.)

Suppose now that $X(k) \neq \emptyset$; then the degree map $\deg : \text{Div}(X) \to \mathbb{Z}$ is evidently surjective. Specifically, if we fix a choice of $O \in X(k)$, we can define a map
\[
\text{cl} : \text{Effective divisors of degree } d \to \text{Pic}^0(X)
\]
\[
D \mapsto [D - dO]
\]
which is surjective. For $d \geq 2g-1$, each fibre has order $\frac{d-g+1}{q-1}$ for $d \geq 2g-1$; this follows from the Riemann-Roch theorem, which implies that $h^0(X,\mathcal{L}) = \deg(\mathcal{L}) - g + 1$ for a line bundle $\mathcal{L}$ with $\deg(\mathcal{L}) \geq 2g - 1$. (We will use the full strength of Riemann-Roch a bit later.)

Now write
\[
Z(X,T) = \prod_{x \in X^\circ} \frac{1}{1 - T^{\deg(x)}} = \sum_{D \geq 0} T^{\deg(D)}
\]where the last sum is over the effective divisors $D$ on $X$ (this is analogous to the equality between the sum and product representations of a Dedekind zeta function). Breaking this sum into two parts according to whether $\deg(D) \geq 2g - 1$ or $\deg(D) \leq 2g - 1$ leads to the following proposition.

**Proposition 4.4.** If $X(k) \neq \emptyset$, then $Z(X,T) = \frac{f(T)}{(1-T)(1-qT)}$ for some polynomial $f$ with $\deg(f) \leq 2g$ and $f(1) = \# \text{Pic}^0(X)$.

**Remark 4.5.** The equality $f(1) = \# \text{Pic}^0(X)$, which crucially implies that $f$ does not have a zero at $T = 1$, is analogous to a property of Dedekind zeta functions which we did not comment on earlier. For $K$ a number field, the residue of $\zeta_K(s)$ at $s = 1$ (where the function has a simple pole) is given by the class number formula. It includes factors coming from the class number of $\mathcal{O}_K$ and the regulator of the unit lattice of $K$. In this context, there are no infinite places and so we see only a class number contribution.

Let us now see about getting rid of the condition that $X(k) \neq \emptyset$. Obviously $X$ has points over some finite extension of $k$, so let us try passing from $X$ to its base extension $X_{\mathbb{F}_q^n}$ for some positive integer $n$ chosen so that $X(\mathbb{F}_q^n) \neq \emptyset$. We can then try to recover information about $X$ using the identity
\[
Z \left( X_{\mathbb{F}_q^n}, T^n \right) = \prod_{i=0}^{n-1} Z \left( X, \zeta_q^i T \right)
\]where $\zeta_q$ is a primitive $n$-th root of unity.

However, there is a strict loss of information between $Z(X,T)$ and $Z \left( X_{\mathbb{F}_q^n}, T \right)$, even for curves.

**Example 4.6.** If $Z(X_1,T) = \frac{1-qT+T^2}{(1-T)(1-qT)}$, $Z(X_2,T) = \frac{1+qT+T^2}{(1-T)(1+qT)}$ then $Z \left( X_1, x^2, t \right) = Z \left( X_2, x^2, t \right)$. This occurs when $X_1$ is an elliptic curve and $X_2$ is a quadratic twist; to make this explicit (assuming $p > 2$), let $X_1$ be a curve of the form
\[
y^2 = x^3 + ax^2 + bx + c
\]and let $X_2$ be the curve
\[
dy^2 = x^3 + ax^2 + bx + c
\]
where \( d \) is a nonsquare in \( \mathbb{F}_q^\times \).

A key observation is that the previous proof in the case \( X(\mathbb{F}_q) \neq \emptyset \) only relies on the surjectivity of the degree map. Hence if could show such surjectivity always hold (without assuming \( X(\mathbb{F}_q) \neq \emptyset \)), then we do not have to worry about the existence of \( O \in X(\mathbb{F}_q) \). Fortunately, this is the case.

**Proposition 4.7.** The degree map \( \deg : \text{Div}(X) \to \mathbb{Z} \) is always surjective, whether or not \( X(k) \neq \emptyset \).

**Proof.** Since the degree map is clearly nonzero, we have \( \deg(\text{Pic}(X)) = e\mathbb{Z} \) for some positive integer \( e \). Let us again compute \( Z(X, T) = \sum_{D \geq 0} T^{\deg(D)} \) by breaking the sum in two as before; the second sum then runs over \( T^{de} \) with \( d \geq d_0 \), where \( d_0 \) is the smallest integer such that \( d_0 e \geq 2g - 1 \). As a result, we have

\[
Z(X, T) = \frac{f(t^e)}{(1 - T^e)(1 - q^e T^e)}
\]

and \( f(1) = \# \text{Pic}^e(X) \neq 0 \). In particular, \( Z(X, T) \) has a pole of order 1 at \( T = 1 \).

The same logic applies also to \( X_{\mathbb{F}_q} \), so \( Z(X_{\mathbb{F}_q}, T) \) has a pole of order 1 at \( T = 1 \). As a result, \( Z(X_{\mathbb{F}_q}, T^e) \) has a pole of order 1 at \( T = 1 \). On the other hand,

\[
Z(X_{\mathbb{F}_q}, T^e) = \prod_{i=0}^{e-1} Z(X, \zeta_i^e) = Z(X, T)^e.
\]

Comparing the pole orders at \( T = 1 \), we deduce that \( e = 1 \), which finishes the proof. \( \square \)

**Remark 4.8.** Using the full strength of the Weil conjectures, one can prove more: for any fixed \( X \), we have \( X(\mathbb{F}_q^n) \neq \emptyset \) for every sufficiently large \( n \). See the supplementary exercises.

Given Proposition 4.7, we can now reprise the proof of Proposition 4.4 to deduce the following.

**Proposition 4.9.** For any \( X \), \( Z(X, T) = \frac{f(T)}{(1 - T)(1 - qT)} \) for some polynomial \( f \) with \( \deg(f) \leq 2g \) and \( f(1) = \# \text{Pic}^0(X) \).

Note that we currently only know that \( \deg(f) \leq 2g \), whereas we expect equality. To resolve this, we must prove the functional equation using the Riemann-Roch theorem.

**Proposition 4.10.** We have \( Z(X, 1/(qT)) = q^{-g}T^{2g-2}Z(X, T) \). Consequently, \( f(q^{-1}T^{-1}) = q^{-g}T^{-2g}f(T) \) and \( \deg(f) = 2g \).

**Proof.** Write \( (q-1)Z(X, T) \) as a sum of two terms:

\[
\alpha(T) := \sum_{0 \leq \deg(L) \leq 2g-2} q^{h^0(L)}T^{\deg(L)}
\]

\[
\beta(T) := \sum_{\deg(L) \geq 2g-1} q^{h^0(L)}T^{\deg(L)} - \sum_{\deg(L) \geq 0} T^{\deg(L)}.
\]

We will prove that each of these satisfies the same functional equation that we desire for \( Z(X, T) \). For \( \beta(T) \), using the weak form of Riemann-Roch used earlier, we obtain

\[
\beta(T) = \# \text{Pic}^0(X) \left( q^g T^{2g-1} \frac{1}{1-qT} - \frac{1}{1-T} \right)
\]

and the functional equation is clear. To analyze \( \alpha(T) \), we must use Riemann-Roch at full strength: for \( \Omega \) the sheaf of Kähler differentials on \( X \) and \( L \) any line bundle on \( X \),

\[
h^0(X, L) = \deg(L) + 1 - g + h^0(\Omega \otimes L^{-1}).
\]

Since \( \deg(\Omega) = 2g - 2 \), we may rewrite \( \alpha(T) \) by substituting \( \Omega \otimes L^{-1} \) for \( L \). Using Riemann-Roch, we then obtain

\[
\alpha(T) = \sum_{0 \leq \deg(L) \leq 2g-2} q^{h^0(\Omega \otimes L^{-1})}T^{\deg(\Omega \otimes L^{-1})}
\]

\[
= \sum_{0 \leq \deg(L) \leq 2g-2} q^{h^0(L) - \deg(L) - 1 + g}T^{2g-2 - \deg(L)}
\]

and again read off the desired functional equation. \( \square \)
We will show a bit later, using the Riemann-Roch theorem, that $Z(X, T)$ satisfies the functional equation; this will also show that $\deg(f) = 2g$. One can also establish the Riemann hypothesis in this framework, but we postpone this to a later lecture.

In the remainder of this lecture, we describe (without proofs) the relationship between curves and abelian varieties, and between the Weil conjectures in these two cases.

**Definition 4.11.** An abelian variety over a field $k$ is a smooth, projective, geometrically connected $k$-scheme equipped with a commutative group structure. It turns out that the commutativity hypothesis is superfluous; see [25].

**Example 4.12.** Elliptic curves over $k$ are abelian varieties of dimension 1. Products of elliptic curves give examples of higher-dimensional abelian varieties.

**Definition 4.13.** Given a curve of genus $g$, there are two different constructions giving rise to a $g$-dimensional abelian variety.

- The **Albanese construction:**

  pointed curve $X/k$ of genus $g \rightarrow \text{Alb}(X)$

  This is a covariant functor, and comes with a (functorial) map $X \rightarrow \text{Alb}(X)$ sending the marked point to the identity. This map does not factor through any abelian subvariety of $\text{Alb}(X)$, and induces a homomorphism

  \[
  \text{Div}^0(X) \rightarrow \text{Alb}(X)(k)
  \]

  which factors through $\text{Pic}^0(X)$.

- The **Picard construction:**

  curve $X/k$ of genus $g \rightarrow \text{Pic}^0(X) := \text{Moduli space of degree-0 line bundles on } X$.

  This is a contravariant functor. The following universal property holds: maps from an abelian variety $S$ over $k$ to $\text{Pic}^0(X)$ correspond to line bundles on $S \times_k X$ whose restriction to every fiber $s \times X$ has degree 0.

**Remark 4.14.** These two construction are related by the **Abel-Jacobi map:**

\[
\text{Alb}^\vee(X) \cong \text{Pic}^0(X)
\]

where for an abelian variety $A$, the **dual variety** $A^\vee$ is defined as $\text{Pic}^0(A)$. Using the **Poincaré bundle**, we obtain a natural isomorphism $(A^\vee)^\vee \cong A$.

For a general abelian variety $A$ over $k$, $A$ and $A^\vee$ need not be isomorphic (although they are necessarily isogenous). However, one can construct a principal polarization giving rise to an isomorphism

\[
\text{Alb}(X) \cong \text{Pic}^0(X).
\]

**Example 4.15.** Over $\mathbb{C}$, every abelian variety arises analytically as a complex torus $\mathbb{C}^g/\Lambda$. The dual variety is then $(\mathbb{C}^g/\Lambda)^\vee \cong \mathbb{C}^g/\Lambda^\vee$, where $\Lambda^\vee := \{\mu : \text{Hom}_R(\mathbb{C}^g, \mathbb{R})| \mu(\Lambda) \subset \mathbb{Z}\}$.

The zeta functions of a curve $A$ and its Jacobian $\text{Jac}(X) := \text{Pic}^0(X)$ are related as follows.

**Theorem 4.16.** Suppose $A$ is an abelian variety over $k = \mathbb{F}_q$ of dimension $g$.

1. The zeta function for $A$ is

   \[
   Z(A, T) = \frac{P_1(T) \cdots P_{2g-1}(T)}{P_0(T) \cdots P_{2g}(T)}
   \]

   where $P_0(T) = 1 - T$, $P_{2g}(T) = 1 - q^gT$, and $P_i(T) = \wedge^i P_1(T)$ for $i = 1, \ldots, 2g$ in the sense that if $P_1(T) = \prod_i (1 - \alpha_i T)$, then $P_i(T) = \prod_{j_1 < \cdots < j_i} (1 - \alpha_{j_1} \cdots \alpha_{j_i} T)$. Note that this implies

   \[
   \#X(k) = P_1(1) = \prod_{j=1}^q (1 - \alpha_j).
   \]

2. If $A \cong \text{Jac}(X)$, then $Z(X, T) = \frac{P_1(T)}{(1-T)(1-qT)}$ for the same $P_1$. 

In this lecture we examine two of the three “elementary” approaches to the Riemann hypothesis for curves over finite fields (that is, the approaches that do not require Weil cohomology).

1. Comparison of a curve with its Jacobian. This is the first proof announced by Weil.
2. Intersection theory on the self-product of the curve. This is the second proof announced by Weil.
3. Clever use of Riemann-Roch. This approach was introduced by Stepanov for hyperelliptic curves \[28\] and generalized to all curves by Bombieri [4].

This list is given in order of first appearance, but we will proceed in the opposite order, focusing in this lecture on the Bombieri–Stepanov method and then the second proof of Weil. We will turn to the first proof of Weil in a subsequent lecture.

**Readings 5.1.** For the Bombieri–Stepanov method, we continue to follow [23, Chapters VIII–IX]. For the second method of Weil, we follow [17, Exercise V.1.10].

Throughout this lecture, let \( X \) be a geometrically irreducible smooth projective curve of genus \( g \) over the finite field \( k = \mathbb{F}_q \) of characteristic \( p \), and write \( q = p^a \). Let us first summarize what we established in the previous lecture.

**Proposition 5.2.** We have
\[
Z(X, T) = \frac{P(T)}{(1 - T)(1 - qT)},
\]
where \( P(T) \in \mathbb{Z}[T] \) is a polynomial satisfying:

- \( P(0) = 1 \);
- \( \deg(P(T)) = 2g \);
- \( P(T) = 1 + a_1 T + \cdots + a_{2g-1} T^{2g-1} + q^g T^{2g} \), with \( a_{g+i} = q^i a_{g-i} \).

Our goal is therefore to prove the Riemann hypothesis for \( X \), which amounts to the assertion that the roots of \( P(T) \) lie on the circle \( |T| = q^{-1/2} \).

We give some initial preparation the Bombieri-Stepanov method.

**Remark 5.3.** Recall that if we can prove the Riemann Hypothesis for a base extension \( X_{\mathbb{F}_{q^n}} \) of \( X \), then this will imply the Riemann hypothesis for \( X \) because the zeroes and poles of \( Z(X_{\mathbb{F}_{q^n}}, T) \) are the \( n \)-th powers of the zeroes and poles of \( Z(X, T) \). In particular, we can arrange for \( q \) to be “sufficiently large” compared to \( g \).

**Definition 5.4.** Let \( \alpha_1^{-1}, \ldots, \alpha_{2g}^{-1} \) be the roots of \( P(T) \), labeled so that \( |\alpha_1| \leq \cdots \leq |\alpha_{2g}| \); the functional equation implies that \( q/\alpha_i = \alpha_{2g+i} \). Utilizing the equality
\[
\log \left( \frac{P(T)}{(1 - T)(1 - qT)} \right) = \sum_{N=0}^{\infty} \frac{\#X(\mathbb{F}_{q^N})}{N} T^N,
\]
expanding power series, and matching coefficients, we obtain
\[
\#X(\mathbb{F}_{q^N}) = q^N + 1 - \sum_{i=1}^{2g} \alpha_i^N
\]
for all \( N \geq 1 \). In particular, the Riemann Hypothesis would imply
\[
|\#X(\mathbb{F}_{q^N}) - q^N - 1| \leq C q^{N/2}
\]
for \( N \geq 1 \) and \( C \) a constant (we can take \( C = 2g \)). A key point here is that the reverse implication is also true!

**Lemma 5.5.** Assume there exists an integer \( d \geq 1 \) and a constant \( C_0 \) for which
\[
|\#X(\mathbb{F}_{q^{dN}}) - q^{dN} - 1| \leq C_0 q^{dN/2}
\]
for all \( N \). Then the Riemann Hypothesis for \( X \) holds.
Proof. The hypothesis implies that
\[ \sum_{N=0}^{\infty} (\alpha_1^{dN} + \cdots + \alpha_2^{dN}) T^N \]
converges in the open disc $|T| < q^{-d/2}$ (say, by the root test). In particular, the power series
\[ \sum_{i=1}^{2g} (1 - \alpha_i dT)^{-1} \]
converges uniformly on $|T| < q^{-d/2}$ (i.e., there are no poles), so that $|\alpha_i| \geq q^{-1/2}$. The functional equation then tells us that $\alpha_{2g-i} = \alpha_i/q$, and hence we obtain $|\alpha_i| = q^{-1/2}$ for all $i$. \hfill \Box

We are thus reduced to proving an upper bound and a lower bound on $\#X(\mathbb{F}_q)$. We start with the former, again keeping in mind that we may apply this after performing a base change.

**Theorem 5.6.** Let $q = p^s$, with $s$ even and $q > (g + 1)^4$. Then
\[ \#X(\mathbb{F}_q) \leq q + 1 + (2g + 1)\sqrt{q}. \]

Proof. There is nothing to verify if $\#X(\mathbb{F}_q)$ is empty, so assume there is an $\mathbb{F}_q$-rational point on $X$ and call it $\infty$. The goal is to write down a rational function on $X$ with a controlled pole at $\infty$ and with zeroes at $X(\mathbb{F}_q) \setminus \{\infty\}$; this would then imply $\#X(\mathbb{F}_q) \leq 1 + P$, where $P$ denotes the pole order of the function at $\infty$. To this end, let
\[ H_m := \{ f \in K(X) : \text{div}(f) \geq -m\infty \} \]
\[ H^p_m := \{ f^p^\mu : f \in H_m \}. \]

Let us consider a function
\[ f = \sum \nu_i s_i^q, \]
with $\nu_i \in H^p_m$ and $s_i \in H^m$. Suppose that $f$ is not identically zero and that $\delta(f) = \sum \nu_i s_i = 0$. It follows that $f$ vanishes on $X(\mathbb{F}_q) \setminus \{\infty\}$. If we assume moreover that $p^\mu < q$, then $f$ is a perfect $p^\mu$-th power and hence vanishes to order $p^\mu$ at each of its zeroes; in particular, we obtain
\[ \#X(\mathbb{F}_q) \leq 1 + \deg(f)/p^\mu \leq 1 + l + mq/p^\mu. \]

Now we examine when such an $f$ exists. By polar expansion around infinity, one may show that the map
\[ \delta : H^p_m \cdot H^q_m \to H_{lp^\mu + m} \]
is in fact a well-defined linear morphism; moreover, if we assume additionally that $lp^\mu < q$, a straightforward calculation gives an isomorphism $H^p_1 \cdot H^q_m \cong H^p_1 \otimes H^q_m$, and hence
\[ \dim_{\mathbb{F}_q} H^p_1 \cdot H^q_1 = \dim_{\mathbb{F}_q}(H^p_1) \dim_{\mathbb{F}_q}(H^q_1). \]

By Riemann-Roch,
\[ \dim_{\mathbb{F}_q} H^p_1 = \dim_{\mathbb{F}_q} H_1 \geq \max\{1, l + 1 - g\}. \]

Hence $\delta$ will have a nontrivial kernel whenever
\[ (l + g - 1)(m + 1 - g) - (lp^\mu + m + 1 - g) > 0. \]

To optimize this, choose $\mu = s/2$ and $m = \sqrt{q} + 2g$. All of the requisite conditions will be satisfied if we can choose an integer $l$ for which
\[ q + \frac{g}{g + 1} \sqrt{q} < l < \sqrt{q}. \]

This is possible so long as $q > (g + 1)^4$; with these choices of $l, m, \mu$ the bound reduces to
\[ \#X(\mathbb{F}_q) \leq 1 + \sqrt{q} + (\sqrt{q} + 2g)\sqrt{q} \]
as desired. \hfill \Box

The previous method does not directly give a lower bound. Instead, we use a trick to convert the lower bound problem into a collection of upper bound problems that can be treated as before.
Definition 5.7. For a Galois cover of curves \( \pi : X \to S \) and an element \( \sigma \in \text{Gal}(X/S) \), let \( N(X/S, \sigma) \) denote the number of points \( P \in X(\mathbb{F}_q) \) which lie above a point of \( S(\mathbb{F}_q) \) in an unramified way and for which \( \sigma \) acts as the Frobenius on \( P \).

Lemma 5.8. Let \( \pi : X \to S \) be a Galois cover of curves defined over \( \mathbb{F}_q \), with \( q > (g(X) + 1)^4 \). Then \( N(X/S, \sigma) < q + 1 + (2g(X) + 1)\sqrt{q} \).

Proof. Let \( \infty \) be a point counted by \( N(X/S, \sigma) \) (if there are no such points there is nothing to prove). Consider the endomorphism \( \phi := \sigma^{-1} \circ \text{Frob on } X \); it suffices to bound the fixed points of \( \phi \) on \( X_{\mathbb{F}_q} \).

Maintaining the notation of Theorem 5.6, any nonconstant function in \( \overline{\sigma}^*(H_m) \) has a pole solely at \( \infty \), since \( \overline{\sigma}^*(H_m) \subset H_{qm} \). Consider \( f = \sum v_i \overline{\sigma}^*(s_i) \) in \( H^0_{\overline{\sigma}^*}(H_m) \), and set \( \delta(f) = \sum v_i s_i \). As in the previous proof, if there exists a nonzero function \( f \) for which \( \delta(f) = 0 \), it follows that \( f \) vanishes at all points counted by \( N(X/S, \sigma) \). One then proceeds as before to show that \( \delta \) must have a nontrivial kernel once \( q \) is suitably chosen with respect to \( g \). \( \square \)

This becomes helpful when we combine all of the automorphisms \( \sigma \).

Lemma 5.9. Let \( \pi : X \to S \) be a Galois cover of curves defined over \( \mathbb{F}_q \). Then

\[
\left| \sum_{\sigma \in \text{Gal}(X/S)} N(X/S, \sigma) - \# \text{Gal}(X/S) \# S(\mathbb{F}_q) \right|
\]

is bounded by a constant depending only on \( g(X) \) and \( \text{deg}(\pi) \).

Proof. Both \( \sum_{\sigma \in \text{Gal}(X/S)} N(X/S, \sigma) \) and \( \# \text{Gal}(X/S) \# S(\mathbb{F}_q) \) can be written as a sum over points \( P_0 \in S(\mathbb{F}_q) \). If \( P_0 \) is not a branch point of \( \pi \), then \( P_0 \) makes identical contributions to both quantities. Thus the discrepancy comes only from fibers containing branch points, the number of which is controlled by the Riemann-Hurwitz formula. \( \square \)

We now derive the desired lower bound, thus completing the Bombieri-Stepanov proof of the Riemann hypothesis for curves.

Lemma 5.10. There exist an integer \( d \geq 1 \) and a constants \( C_0 \) for which for all positive integers \( N \),

\[
\# X(\mathbb{F}_{q^dN}) \geq q^{dN} - C_0 q^{dN/2}.
\]

Proof. If \( X \) itself can be written as a Galois cover of \( \mathbb{P}^1 \) via some map \( \pi \), then Lemma 5.9 implies that an upper bound on \( N(X/S, \sigma) \) for each nontrivial automorphism \( \sigma \) implies a lower bound on \( N(X/S, \text{id}_X) = \# X(\mathbb{F}_q) \). So in this case, we just apply Lemma 5.8 and we are done.

In general, \( X \) cannot always be written as a Galois cover of \( \mathbb{P}^1 \) (e.g., if it has trivial automorphism group and positive genus). However, we can always choose a finite separable morphism \( X \to \mathbb{P}^1 \) (perhaps after extending the base field, although this isn’t really needed) and then take its Galois closure to obtain a Galois cover \( Z \to X \) for which \( Z \to X \to \mathbb{P}^1 \) is also Galois. By applying Lemma 5.9 to both \( Z \to X \) and \( Z \to \mathbb{P}^1 \), we may again reduce the desired lower bound to some instances of Lemma 5.8. \( \square \)

We now shift our attention to Weil’s second method, whose main tools are the intersection pairing on surfaces and the Hodge index theorem. We briefly recall these two objects.

Definition 5.11. Let \( S \) be a smooth projective surface over a field \( k \). There is a unique bilinear pairing

\[
\text{Div}(S) \times \text{Div}(S) \to \mathbb{Z},
\]

called the intersection pairing, with the following properties.

- If \( D_1 \) and \( D_2 \) are effective divisors on \( S \) without common components, then

\[
D_1 \cdot D_2 = \text{length}_k(D_1 \times_k D_2).
\]

In other words, the pairing measures usual intersections when possible.

- The pairing depends solely on linear equivalence; i.e. if \( D_1 \sim_{\text{lin}} D'_1 \) and \( D_2 \sim_{\text{lin}} D'_2 \), then \( D_1 \cdot D_2 = D'_1 \cdot D'_2 \).
The intersection pairing furthermore can be shown to satisfy the *adjunction formula*: if \( C \hookrightarrow S \) is a closed immersion and \( C \) is a smooth, projective, geometrically irreducible curve of genus \( g \) over \( k \), then
\[
C \cdot (C + K) = 2g - 2,
\]
where \( K \) is the canonical divisor (or rather, “a” canonical divisor) on \( S \). See [17, §V.1].

Having set up the intersection pairing on surfaces, we can state the Hodge Index Theorem [17, Theorem V.1.9].

**Theorem 5.12** (Hodge Index Theorem). Let \( H \) be an ample divisor on the surface \( S \). Then for any divisor \( D, D \cdot H = 0 \) implies \( D \cdot D \leq 0 \).

With this setup, we can proceed with Weil’s proof. The idea is to apply the previous two theorems with \( S = X \times_k X \). The surface \( S \) comes equipped with two natural divisors:

- \( \Delta \), the diagonal embedding \( X \hookrightarrow X \times_k X \);
- \( \Gamma \), the graph of the Frobenius morphism.

One can verify (by working locally) that \( \Delta \) and \( \Gamma \) have no common component and intersect transversally. Furthermore, the intersection \( \Delta \times_S \Gamma \) is naturally identified with \( X(\mathbb{F}_q) \). Thus utilizing the intersection pairing we can write
\[
\#X(\mathbb{F}_q) = \Delta \cdot \Gamma.
\]

We need the following preparatory lemma.

**Lemma 5.13.** Let \( H \) be an ample divisor, and \( D \) an arbitrary divisor, on \( S = X \times_k X \). Let \( \sigma(1,0) \) and \( \sigma(0,1) \) be the divisors obtained by pulling back a hyperplane section on \( X \) from the first and second projections respectively.

1. We have \( D^2 H^2 \leq (D \cdot H)^2 \)
2. For \( S = X \times X, D^2 \leq 2(D \cdot \sigma(1,0))(D \cdot \sigma(0,1)) \), with equality if and only if \( D = a \sigma(1,0) + b \sigma(0,1) \).

**Proof.** For the first statement, we may take an orthogonal decomposition of the space of divisors to write \( D = aH + bE \), where \( E \cdot H = 0 \). Then \( D^2 H^2 = (aH)^2 + (bE)^2 \) \( H^2 \). By the Hodge index theorem, \( (bE)^2 \leq 0 \), so \( D^2 H^2 \leq (aH)^2 H^2 \). But now \( (aH)^2 H^2 = (H \cdot (aH + bE))^2 = (D \cdot H)^2 \) as desired. For the second statement, apply the first statement to the ample divisor \( \sigma(1,1) = \sigma(0,1) + \sigma(1,0) \). □

To finish Weil’s proof we now need the following computations, which follow from adjunction:
\[
\begin{align*}
\Delta^2 &= 2 - 2g \\
\Gamma^2 &= q(2 - 2g) \\
\Delta \cdot \sigma(1,0) &= 1 \\
\Delta \cdot \sigma(0,1) &= 1 \\
\{\Gamma \cdot \sigma(1,0), \Gamma \cdot \sigma(0,1)\} &= \{1, q\}.
\end{align*}
\]

Now apply the previous lemma to \( a \Gamma + b \Delta \) to obtain
\[
a^2 \Gamma^2 + 2ab \Gamma \cdot \Delta + b^2 \Delta^2 \leq 2(a \Gamma + b \Delta) \cdot \sigma(0,1)(a \Gamma + b \Delta) \cdot \sigma(1,0).
\]

Simplifying gives
\[
0 \leq 2(a + b)(qa + b) - a^2 q(2 - 2g) - b^2 (2 - 2g) - 2ab \#X(\mathbb{F}_q).
\]

In other words, we have a semi-positive quadratic form in \( a \) and \( b \) represented by the matrix
\[
\begin{pmatrix}
q(2g - 1) & 2(q + 1) - 2ab \#X(\mathbb{F}_q) \\
2(q + 1) - 2ab \#X(\mathbb{F}_q) & (2g - 1)
\end{pmatrix};
\]
by Sylvester’s criterion, semi-positivity implies
\[
\frac{q(2g - 1)^2}{4} - (q + 1 - \#X(\mathbb{F}_q))^2 \geq 0,
\]
giving a bound as in Lemma 5.5 and thus completing the proof.
6. Exercises


(1) Let $k$ be a finite field of order $q$ and fix an additive character (homomorphism) $\psi : k \to \mathbb{C}^\times$. For $\chi : k^\times \to \mathbb{C}^\times$ a nontrivial multiplicative character, define the Gauss sum

$$G_\psi(\chi) = \sum_{x \in k^\times} \chi(x)\psi(x).$$

Prove that $G_\psi(\chi)G_\psi(\overline{\chi}) = q$, where $\overline{\chi}$ is the character for which $\overline{\chi}(x)$ is the complex conjugate of $\chi(x)$. (Hint: write the product as a sum over $y \in k^\times$, then regroup terms by the value of $x/y$.)

(2) Fix a choice of $\chi$ as above. For $P(T) = T^n + P_{n-1}T^{n-1} + \cdots + P_0 \in k[T]$ a monic polynomial, define

$$\lambda(P) = \chi(P_0)\psi(P_{n-1}).$$

(In particular, $\lambda(1) = 1$.) Show that

$$\lambda(P_1P_2) = \lambda(P_1)\lambda(P_2) \quad (P_1, P_2 \in k[T])$$

and deduce that for each positive integer $n$, in $\mathbb{C}[U]$ we have

$$\sum_{P \in k[T]} \lambda(P)U^{\deg(P)} = \prod_{Q \in k[T]} (1 - \lambda(Q)U^{\deg(Q)})^{-1}.$$

(3) Show that for $n$ a nonnegative integer,

$$\sum_{P \in k[T]} \lambda(P)U^{\deg(P)} = \begin{cases} 1 & n = 0 \\ G_\psi(\chi)U & n = 1 \\ 0 & n > 1. \end{cases}$$

(4) With notation as in the previous problem, let $k'$ be an extension of $k$ of degree $\nu$. Let $\psi' : k' \to \mathbb{C}^\times$ be the additive character given by $\psi' \circ \text{Trace}_{k'/k}$. Given $\chi$, let $\chi'$ be the multiplicative character given by $\chi \circ \text{Norm}_{k'/k}$. For $P' \in k'[T]$ monic, define $\chi'$ by analogy with $\lambda$.

For $P \in k[T]$ monic irreducible, let $P'$ run over the irreducible factors of $P$ in $k'[T]$. Prove that

$$\prod_{P'} (1 - \chi'(P')U^{\deg(P')}) = \prod_{\nu \geq 0} (1 - \lambda(P)(e^{2\pi i \nu}/\nu)U^{\deg(P')}).$$

(Hint: let $-\xi$ be a root of one of the factors $P'$, and consider the field extensions $k(\xi)/k$ and $k'/(\xi)/k'$.)

(5) Using all of the above, deduce the Davenport-Hasse relation

$$-G_\psi(\chi') = (-G_\psi(\chi))^\nu.$$

6.2. Set 2. Throughout, let $\mathbb{F}_q$ denote a finite field of characteristic $p$.

(1) For $X$ an algebraic variety over $\mathbb{F}_q$, we write the zeta function of $X$ as $Z(X, q^{-s})$ for

$$Z(X, T) = \prod_{x \in X^\circ} (1 - T^{\deg(x)})^{-1},$$

where $X^\circ$ denotes the set of Galois orbits of $\mathbb{F}_q$-points and $\deg(x)$ is the cardinality of such an orbit. Prove that in $\mathbb{Q}[T]$, we have the equality

$$Z(X, T) = \exp \left( \sum_{n=1}^{\infty} \frac{T^n}{n} \# X(\mathbb{F}_q^n) \right).$$

(2) For $X$ equal to the $n$-dimensional projective space over $\mathbb{F}_q$, compute that

$$Z(X, T) = \frac{1}{(1 - T)(1 - qT) \cdots (1 - q^nT)}.$$

(3) Prove that the following statements are equivalent.

(i) The power series $Z(X, T)$ represents a rational function in $T$.

(ii) There exist $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \mathbb{C}$ such that

$$\# X(\mathbb{F}_q^n) = \alpha_1^n + \cdots + \alpha_r^n - \beta_1^n - \cdots - \beta_s^n \quad (n = 1, 2, \ldots).$$
(4) Let $X$ be the Grassmannian of $k$-dimensional subspaces of $m$-space over $\mathbb{F}_q$.

(i) Compute $\# X(\mathbb{F}_q^n)$; your answer should be a polynomial in $q^n$ depending on $k$ and $m$. (Hint: count bases of subspaces, then divide by the number of bases of a given subspace.)

(ii) Compute $Z(X, T)$.

(5) Choose $a_1, \ldots, a_r \in \mathbb{F}_q^×$. For $d$ a positive integer dividing $q - 1$, let $X_d$ be the projective hypersurface $a_0x_0^d + \cdots + a_rx_r^d = 0$.

(i) Let $G_d$ be the group of homomorphisms $\chi : \mathbb{F}_q^× \to \mathbb{C}^×$ of order $d$. For $\chi \in G_d$, extend the definition of $\chi$ to $\mathbb{F}_q$ by setting $\chi(0) = 1$ if $\chi = 1$ and $\chi(0) = 0$ otherwise. Show that

$$1 + (q - 1)\# X_d(\mathbb{F}_q) = \sum_{(u_0, \ldots, u_r) \in X_1, \chi_0, \ldots, \chi_r \in G_d} \prod_{i=0}^{r} \chi_i(u_i).$$

(ii) Show that $\chi_0, \ldots, \chi_r \in G_d$ are neither all equal to 1 or all distinct from 1, then

$$\sum_{(u_0, \ldots, u_r) \in X_1} \prod_{i=0}^{r} \chi_i(u_i) = 0.$$

(iii) Let $T$ be the set of tuples $(\chi_0, \ldots, \chi_r) \in G_d \setminus \{1\}$ with $\chi_0 \cdots \chi_r = 1$. For $(\chi_0, \ldots, \chi_r) \in T$, define the Jacobi sum

$$j(\chi_0, \ldots, \chi_r) = \frac{1}{q-1} \sum_{u_0, \ldots, u_r \in \mathbb{F}_q, u_0 + \cdots + u_r = 0} \chi_0(u_0) \cdots \chi_r(u_r).$$

Deduce from above that

$$\# X_d(\mathbb{F}_q) = 1 + q + \cdots + q^{r-1} + \sum_{(\chi_0, \ldots, \chi_r) \in T} \chi_0(a_0^{-1}) \cdots \chi_r(a_r^{-1}) j(\chi_0, \ldots, \chi_r).$$

(iv) Fix an additive character $\psi : \mathbb{F}_q \to \mathbb{C}^×$. Show that

$$j(\chi_0, \ldots, \chi_r) = \frac{1}{q} G(\chi_0, \psi) \cdots G(\chi_r, \psi)$$

where $G(\chi, \psi)$ denotes the Gauss sum.

(6) Keep notation as in the previous exercise, but assume only that $d$ is not divisible by $p$ (not that it divides $q - 1$).

(i) Show that $\# X_d(\mathbb{F}_q) = \# X_1(\mathbb{F}_q)$ for $e = \gcd(d, q - 1)$.

(ii) Using the Davenport-Hasse relation, show that the rationality, functional equation, and Riemann hypothesis hold for $Z(X_d, T)$.

6.3. **Set 3.** Throughout, let $\mathbb{F}_q$ denote a finite field of characteristic $p$. Assume the Weil conjectures for curves and abelian varieties unless otherwise specified.

(1) Let $X$ be a nonzero abelian variety over $\mathbb{F}_q$. Prove that if $q \geq 5$, the group $X(\mathbb{F}_q)$ is nontrivial.

(2) Let $X$ be a curve over $\mathbb{F}_q$ such that $\# X(\mathbb{F}_q) = 1$.

(a) If $q = 3$ or $q = 4$, prove that

$$Z(X, T) = \frac{1 - qT + qT^2}{(1 - T)(1 - qT)}.$$

(b) If $q = 2$, prove that the genus of $X$ is at most 4, and that there are at most 6 possibilities for $Z(X, T)$.

(c) Optional: show that each of the 8 possibilities occurs for a unique $X$ up to isomorphism.

(3) Let $X$ be an abelian variety of dimension $g$ over $\mathbb{F}_q$. Assuming only the existence of complex numbers $\alpha_1, \ldots, \alpha_{2g}$ such that

$$X(\mathbb{F}_q^n) = (1 - \alpha_1^n) \cdots (1 - \alpha_{2g}^n) \quad (n = 1, 2, \ldots),$$

compute $Z(X, T)$.

(4) Using the Honda-Tate theorem, prove that if $A_1, A_2$ are abelian varieties over $\mathbb{F}_q$ and $P_1(A_1, T)$ divides $P_1(A_2, T)$, then $A_1$ is isogenous to the product of $A_2$ with some other abelian variety.
(5) Let $X$ be a curve of genus $g$ over $\mathbb{F}_q$. Prove the following refinement of the Weil bound due to Serre:

$$|\#X(\mathbb{F}_q) - q - 1| \leq g|2\sqrt{q}|.$$

Hint: apply AM-GM to the numbers $|2\sqrt{q}| + 1 + \alpha + \overline{\alpha}$ where $\alpha$ runs over the Frobenius eigenvalues.

(6) Let $P(T) = \sum_{i=0}^{2g} a_i T^i$ be a polynomial over $\mathbb{Z}$ such that $a_0 = 1$, $a_g + i = q^i a_{g-i}$ for all $i$, all roots of $P(T)$ in $\mathbb{C}$ lie on the circle $|T| = q^{-1/2}$, and $a_g$ is not divisible by $p$ (that is, $P$ is an ordinary Weil polynomial). Use the Honda-Tate theorem to show that $P(T)$ occurs as $P_1(A, T)$ for some abelian variety $A$ over $\mathbb{F}_q$ (without raising $P$ to a power).

6.4. Set 4.

(1) Let $K$ be a number field. Using the Chebotarev density theorem, prove that the Frobenius elements corresponding to maximal ideals of $\mathfrak{o}_K$ are dense in the absolute Galois group $G_K$. (This is just an exercise in unwinding the definitions.)

(2) In this exercise, we prove the theorem of Borel stated in class on November 3.

(a) Let $f(T) = \sum_{n=0}^{\infty} a_n T^n$ be a power series over an arbitrary field $K$. Prove that $f(T)$ represents a rational function over $K$ if and only if for some positive integer $m$, the determinants of the $(m+1) \times (m+1)$ matrices $A_{n,m} = (a_{n+i+j})_{i,j=0}^m$ vanish for all sufficiently large $n$.

(b) Let $f(T) = \sum_{n=0}^{\infty} a_n T^n$ be a power series over $\mathbb{Z}$. Let $r > 0$ be a real number such that over $\mathbb{Q}_p$, there exists a polynomial $P(T)$ of degree $d < m$ such that $P(T)f(T)$ converges for $|T| < r + \epsilon$ for some $\epsilon > 0$. (We do not assume that $P$ has coefficients in $\mathbb{Z}$.) Prove that for some $C > 0$, $|\det(A_{n,m})|_p \leq C r^{-n(m-d)}$ for all $n$.

(c) Let $f(T) = \sum_{n=0}^{\infty} a_n T^n$ be a power series over $\mathbb{Z}$. Let $R$ and $r$ be real numbers with $Rr > 1$ such that over $\mathbb{C}$, $f(T)$ converges for $|T| < R$; and over $\mathbb{Q}_p$, $f(T)$ is the ratio of two series that converge for $|T| < r$. Prove that $f$ represents a rational function. (Hint: apply (b) with $r$ replaced by $r - \epsilon$ for which $(R-\epsilon)(r-\epsilon) > 1$, then combine with a trivial bound on $|\det(A_{n,m})|_p$.)

(3) Let $\pi$ be an element of an algebraic closure of $\mathbb{Q}_p$ satisfying $\pi^{p-1} = -p$. (You may use without proof the fact that $\mathbb{Z}_p[\pi]$ is a discrete valuation ring with maximal ideal $(\pi)$. Define the power series

$$E_n(T) = \exp(\pi(T - T^p)) \in \mathbb{Q}_p[[T]].$$

(a) Prove that $E_n(T) \in 1 + \pi \mathbb{Z}_p[[T]]$.

(b) Prove that $E_n(T)$ has radius of convergence strictly greater than 1. In particular, it makes sense to evaluate it at any element of $\mathbb{Z}_p[\pi]$.

(c) Prove that if $t \in \mathbb{Z}_p$ satisfies $t^p = t$, then $E_n(t)^p = 1$. (Hint: check that in the identity

$$E_n(T)^p = \exp(\pi p T) \exp(-\pi p T)$$

it is valid to substitute $t$ separately into the two factors on the right.)

(4) With notation as in the previous problem, let $n$ be a positive integer and define

$$E_n(T) := \exp(\pi(T - T^{p^n})) = E_{p^n}(T)E_{p^n}(T^{p^n}) \cdots E_{p^n}(T^{p^n-1}) \in \mathbb{Q}_p[[T]].$$

Show that the formula $t \mapsto E_n([t])$ defines a nontrivial additive character on $\mathbb{F}_p^n$, where $[t]$ denotes the unique element of $\mathbb{Z}_p^n$ (the finite étale extension of $\mathbb{Z}_p$ with residue field $\mathbb{F}_p$) lifting $t$ and satisfying $t^{p^n} = t$.

(5) Set $q = p^n$ and let $f = \sum_{I=(i_1,\ldots,i_d)} a_I x_1^{i_1} \cdots x_d^{i_d} \in \mathbb{F}_q[x_1,\ldots,x_d]$ be a polynomial. Prove that for any positive integer $m$, the number of points $(x_1,\ldots,x_d) \in (\mathbb{F}_q^m)^d$ for which $f(x_1,\ldots,x_d) = 0$ equals

$$\frac{(q^m - 1)^d}{q^m} \left( 1 + (q^m - 1) \sum_{x_0,\ldots,x_d \in \mathbb{F}_q^m} \prod_{I: a_I \neq 0} \prod_{j=0}^{m-1} E_\pi(a_I([x_0]^i \cdots [x_d]^i)q^j) \right).$$
6.5. Set 5.

(1) Define the rings

\[ R = \mathbb{Z}[x_1, y_1, x_2, y_2, \ldots], \quad R' = \mathbb{Q}[x_1, y_1, x_2, y_2, \ldots], \quad F = \text{Frac}(R) = \text{Frac}(R'). \]

Define the power series \( x = 1 + x_1T + x_2T^2 + \cdots \), \( y = 1 + y_1T + y_2T^2 + \cdots \), and

\[ f = 1/\exp(\log(1/x) \ast \log(1/y)) \in R'[T] \]

where \( \ast \) denotes the Hadamard product:

\[ (a_1T + a_2T^2 + \cdots) \ast (b_1T + b_2T^2 + \cdots) = a_1b_1T + a_2b_2T^2 + \cdots \]

(a) Let \( V_1, V_2 \) be two finite-dimensional vector spaces over \( F \) equipped with endomorphisms \( \varphi_1, \varphi_2 \) satisfying, for some positive integer \( n \),

\[ \det(1 - \varphi_1T, V_1)^{-1} \equiv 1 + x_1T + \cdots + x_nT^n \pmod{T^{n+1}F[T]}, \]

\[ \det(1 - \varphi_2T, V_2)^{-1} \equiv 1 + y_1T + \cdots + y_nT^n \pmod{T^{n+1}F[T]}, \]

Prove that

\[ \det(1 - (\varphi_1 \otimes \varphi_2)T, V_1 \otimes F V_2)^{-1} \equiv f \pmod{T^{n+1}F[T]). \]

(Hint: pass to an algebraic closure of \( F \) and write everything in terms of eigenvalues. Remember that \( f \) is determined \( \pmod{T^{n+1}F[T]} \) by \( x_1, \ldots, x_n, y_1, \ldots, y_n \).)

(b) Deduce that \( f \in R[T] \).

(2) Using the previous exercise, prove that there is a unique functor \( \Lambda \) from rings to rings with the following properties.

(a) The underlying functor from rings to additive groups takes \( R \) to \( \Lambda(R) = 1 + TR[T] \) with the usual series multiplication.

(b) For any ring \( R \), the multiplication map \( \ast \) on \( \Lambda(R) \) satisfies

\[ (1 - aT)^{-1} \ast (1 - bT)^{-1} = (1 - abT)^{-1} \quad (a, b \in R). \]

The ring \( \Lambda(R) \) is a (form of) the ring of big Witt vectors with coefficients in \( R \).

(3) Let \( X_1, X_2 \) be two varieties over \( \mathbb{F}_q \). Prove that in \( \Lambda(\mathbb{Z}) \), we have

\[ Z(X_1 \times_{\mathbb{F}_q} X_2, T) = Z(X_1, T) \ast Z(X_2, T). \]

(4) Let \( K \) be a field of characteristic 0. Let \( P(x) \in K[x] \) be a monic polynomial of degree \( 2g + 1 \) with no repeated roots.

(a) Let \( X \) be the affine scheme \( \text{Spec} K[x, y]/(y^2 - P(x)) \). Prove that \( \Omega^1_{X/K} \) is freely generated by \( dx/y \). (Hint: it suffices to check that \( dx/y \) is a nowhere vanishing section of \( \Omega^1_{X/K} \). Treat the points where \( y = 0 \) and \( y \neq 0 \) separately.)

(b) Prove that \( H^1_{\text{dR}}(X) \) admits the basis

\[ x^i \frac{dx}{y} \quad (i = 0, \ldots, 2g - 1). \]

(Hint: for each integer \( d \geq 2g \), write down a relation of the form \( Q(x)dx/y \) with \( \deg(Q) = d \).)

(c) Let \( Y \) be the affine scheme \( \text{Spec} K[x, y, z]/(y^2 - P(x), yz - 1) \). Prove that \( H^1_{\text{dR}}(Y) \) admits the basis

\[ x^i \frac{dx}{y}, \quad (i = 0, \ldots, 2g - 1); \quad x^i \frac{dx}{y^2}, \quad (i = 0, \ldots, 2g). \]

(5) Let \( p > 2 \) be a prime. Let \( \mathcal{P} \in \mathbb{F}_p[x] \) be a monic polynomial of degree \( 2g + 1 \) with no repeated roots.

(a) Put \( X = \text{Spec} \mathbb{F}_p[x, y]/(y^2 - \mathcal{P}(x)) \). Prove that \( H^1_{\text{MW}}(X) \) admits the basis

\[ x^i \frac{dx}{y} \quad (i = 0, \ldots, 2g - 1). \]

(b) Put \( Y = \text{Spec} \mathbb{F}_p[x, y, z]/(y^2 - \mathcal{P}(x), yz - 1) \). Prove that \( H^1_{\text{MW}}(Y) \) admits the basis

\[ x^i \frac{dx}{y}, \quad (i = 0, \ldots, 2g - 1); \quad x^i \frac{dx}{y^2}, \quad (i = 0, \ldots, 2g). \]
6.6. **Supplementary exercises.** These exercises were not assigned during the course, but were added subsequently.

1. Using the Weil conjectures for curves, show that a curve $X$ of genus 1 over a finite field $k$ cannot satisfy $X(k) = \emptyset$.

2. Let $X$ be a geometrically irreducible variety over a finite field $\mathbb{F}_q$. Using the Weil conjectures, show that there exists an integer $N$ such that $X(\mathbb{F}_{q^n}) \neq \emptyset$ for all $n \geq N$.

**References**


