INTRODUCTION TO WEIL CONJECTURES, PART II: VARIETIES

JORI MERIKOSKI

Abstract. This is the second part of an introduction to Weil conjectures, which concern the number of points on varieties over a finite field. We begin by recalling and expanding some basic definitions from first part, and then proceed to state the Weil conjectures (a theorem despite its name). After this we give an informal discussion of cohomology of varieties; this gives us a natural way to interpret the Weil conjectures. We do not assume that the reader is familiar with cohomology theories, so we will try to motivate this by examples. We then briefly discuss what goes into the construction of the so called ℓ-adic cohomology; to put it simply, cohomology of a variety is just a collection of finite dimensional vector spaces with some nice properties. After stating some of these properties we find that only linear algebra is needed to prove some parts of the Weil conjectures. We then describe some applications of these ideas, and give some reading suggestions. Same disclaimer as last time is in place; I do not consider myself an expert in this topic, so it is likely that the note contains some inaccuracies.

Contents

1. Statement of the Weil conjectures

We begin by recalling some definitions from the first part; let k be a field. We define an affine algebraic set to be a set of common zeros of a finite collection of polynomials $\{f_1, \dots, f_m\} \subseteq k[X_1, \dots, X_n]$, that is,

$$V = V(f_1, \dots, f_m) := \{x \in k^n : f_j(x) = 0 \ \forall j = 1, 2 \dots, m\}.$$

For example, the affine n-space over k is $\mathbb{A}_k^n = V(\{0\})$. Given such a variety V, the ideal of definition and the coordinate ring are defined as

$$\mathcal{I}(V) := \{g \in k[X_1, \dots, X_n] : g(x) = 0 \ \forall x \in V\} \subseteq k[X_1, \dots, X_n],$$
$$\mathcal{P}(V) := k[X_1, \dots, X_n]/\mathcal{I}(V).$$

We say that V is irreducible if the ideal of definition $\mathcal{I}(V)$ is a prime ideal. Intuitively, this means that V is not a non-trivial finite union of algebraic sets.

Recall that for any extension $k \subseteq K$, we can look at the points on V with coordinates in K

$$V(K) := \{x \in K^n : f_j(x) = 0 \ \forall j = 1, 2 \ldots, m\} \supseteq V(k).$$

Then V is said to be absolutely irreducible if $V(\overline{k})$ is irreducible, where $\overline{k}$ is the algebraic closure of k. An affine variety over k is then defined to be an absolutely irreducible algebraic set with coordinates in k, defined by polynomials with coefficients in k.

Example 1. The set $V(Y^2 - X^2) \subseteq \mathbb{A}_k^2$ is not irreducible, it is a union of two varieties $V(Y - X)$ and $V(Y + X)$. If $k = \mathbb{F}_p$ and $a \in \mathbb{F}_p$ is not a square, then $V(Y^2 - aX^2) \subseteq \mathbb{A}_k^2$ is irreducible but not absolutely irreducible.

Similarly as in the first part, we will focus on projective varieties; a projective variety is an absolutely irreducible algebraic subset of $\mathbb{P}_k^n$ defined by a set of homogeneous polynomial equations. Any affine variety in $\mathbb{A}_k^n$ defines a projective variety in $\mathbb{P}_k^n$ by homogenization of the polynomials; one should think of this as the original affine variety with additional 'points at infinity'.

Roughly speaking, a variety is of dimension d if it is defined by m equations in an $(m + d)$-dimensional space.

We also need to recall the definition of a non-singular variety. For example, a curve

$$V = \{x \in \mathbb{A}_k^2 : f(x) = 0\}$$

is non-singular if for all $(x, y) \in V$ either $\partial_x f(x, y) \neq 0$ or $\partial_y f(x, y) \neq 0$. If both partial derivatives vanish, such a point is said to be a singular point. The notion of non-singularity can be generalized to higher-dimensional varieties by using the Jacobian matrix $J_V(x) = (\partial f_i / \partial x_j(x))$, where $f_1, \ldots, f_m$ are the polynomials defining the variety $V \subset \mathbb{A}_k^n$; a point $(x_1, \ldots, x_n) \in V$ is non-singular if the matrix $J_V(x)$ is of rank $n - d$, where d is the dimension of the variety (some care is needed in making this rigorous).

We are now prepared to state the Weil conjectures (a theorem despite its name); fix $q = p^m$, and let X be a non-singular projective variety defined over $\mathbb{F}_q$. Let d denote the dimension of X. Define

$$N_n := |X(\mathbb{F}_{q^n})|,$$

the number of points with coordinates in $\mathbb{F}_q^n$. Then the zeta function of X is

$$Z_X(T) := \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right),$$

so that the logarithmic derivative of $Z_X(T)$ is the generating function of N_n; it is a complex function, which can be continued meromorphically to the whole plane. The Weil conjectures then are as follows:

1. Rationality. $Z_X(T)$ is a rational function of T, that is, a quotient of polynomials with rational coefficients.

2. Functional equation. There is an integer E such that

$$Z_X\left(\frac{1}{q^d T}\right) = \pm q^{dE/2} T^E Z_X(T)$$

3. Riemann hypothesis for X. We have

$$Z_X(T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)},$$

where $P_0(T) = 1 - T$, $P_{2d} = 1 - q^qT$, and for every i the polynomial $P_i(T)$ has integer coefficients, and

$$P_i(T) = \prod_j (1 - \alpha_{ij}T),$$

where α_{ij} are algebraic integers with $|\alpha_{ij}| = q^{i/2}$.

We note here that if we set $T = q^{-s}$ and $\zeta_X(s) := Z_X(q^{-s})$, then the third part implies that $\zeta_X(s)$ has its poles and zeros on the vertical lines $\{\Re\, s = i/2\}$, $i = 0, 1, \ldots, 2d$, with poles on integer values and zeros on half-integer values of the real part. This is analogous to the Riemann hypothesis, which states that if s is a non-trivial zero of $\zeta(s)$, then $\Re\, s = 1/2$.

Exercise 1. If $X = \mathbb{P}^d_{\mathbb{F}_q}$, then $N_n = q^{nd} + q^{n(d-1)} + \cdots + q^n + 1$, and

$$Z_{\mathbb{P}^d_{\mathbb{F}_q}}(T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^dT)}.$$

On their own the three parts to the conjecture may look somewhat mystifying. However, there is a fourth part to the Weil conjectures, which will eventually motivate the other three.

4. Betti numbers. We have $E = \sum_{i=0}^{2d}(-1)^i \deg P_i$ in the functional equation. Futhermore, if $q = p$ and X is a good reduction modulo p, then $\deg P_i = B_i$, the i^{th} Betti number of $X(\mathbb{C})$, so that E is the Euler characteristic of $X(\mathbb{C})$.

Let us clarify what the above means. By reduction modulo p we mean the following: suppose, for example, that $f(X, Y) \in \mathbb{Z}[X, Y]$ is a polynomial with integer coefficients. Then by taking the residue class modulo p of each coefficient, we can view f as an element of $\mathbb{F}_p[X, Y]$. The curve $X = \{x \in \mathbb{F}_p^2 : f(x) = 0\}$ is then a reduction modulo p. Since f has integer coefficients, we can also consider the complex points

$$X(\mathbb{C}) = \{x \in \mathbb{C}^2 : f(x) = 0\}.$$

Then the Betti numbers say something about the topology of $X(\mathbb{C})$; roughly, B_i is the number of 'i-dimensional holes' on $X(\mathbb{C})$. All of this discussion generalizes to higher dimensional varieties in an obvious way. As an example, the Betti numbers of $\mathbb{P}^d_{\mathbb{C}}$ are $B_i = 1$, if $i \leq 2d$ is even, and $B_i = 0$, if $i \leq 2d$ is odd, and $B_i = 0$ for $i > 2d$. (Some care is needed to make the above discussion rigorous, for example, the reduction of $f(X, Y) = pX + pY$ modulo p is just 0; these technicalities are swept under the rug by inserting the word 'good' before 'reduction modulo p').

This striking idea, that the geometry of the complex points should affect the number of points modulo p, is perhaps the deepest insight of Weil's conjectures; making this rigorous was a key motivation for the developments in algebraic geometry through 1950's to 1970's. To understand this fourth part and its relation to the other parts, we need to make an excursion into cohomology.

2. ℓ-ADIC COHOMOLOGY

The Weil conjectures cannot be reasonably discussed without mentioning cohomology. Various kinds of cohomology theories have been developed in different parts of mathematics; they can be thought be an attempt to characterize of 'obstructions' of some sort.

What we seek is a cohomology theory for varieties over finite fields. There are standard ways of developing cohomology theories for varieties over complex numbers by using their 'analytic' topology (a non-singular variety over $\mathbb{C}$ is also a smooth manifold). To prove the fourth part of the Weil conjectures, these two cohomologies should be comparable in some way.

We first give an informal description of a certain cohomology theory for topological spaces. We then sketch how this can be used to define a cohomology theory for varieties over finite fields; this requires us to broaden what we mean by a topology, to the so called étale topology. Étale cohomology is then defined as the cohomology with respect to the étale topology. ℓ-adic cohomology is defined using étale cohomology. Lastly, we will list some basic properties of ℓ-adic cohomology.

If this section feels quite abstract and highbrow, fear not; in the next section we will use only some basic linear algebra, to deduce the parts one, two and (almost) four of the Weil conjecture, using the basic properties of the cohomology. For that purpose it is sufficient to say that the ℓ-adic cohomology consists of a collection of finite dimensional vector spaces with some convenient properties. We still feel obliged to give at least a flavour of what goes into this construction. All the discussion in this section is informal and we will refrain from rigorous definitions for the sake of the reader, for it would require us to dwell on category theory and other abstract nonsense for far too long.

2.1. **Cohomology.**

In this section we will discuss a cohomology theory of topological spaces called Čech cohomology.

Consider the following basic problem: recall that two topological spaces X and Y are said to be homoemorphic if there exists a continuous bijection $f : X \to Y$ whose inverse is also continuous (the intuition here is that X and Y are homeomorphic if one is continuously deformable in to another). Define the annulus and the disk on the real plane

$$A := \{(x, y) \in \mathbb{R}^2 : 1/4 < x^2 + y^2 < 1\}, \qquad D := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}.$$

Suppose that someone asks us to show to show that A is not homeomorphic to D. The obvious way to do this is to note that every closed path in the disk D can be continuously shrunk to a point; on the other hand, if a closed path in A 'winds around' the hole once, then such a path cannot be continuously deformed to a point (since the 'winding number' of a closed path remains fixed in continuous deformations), cf. Figure 1.

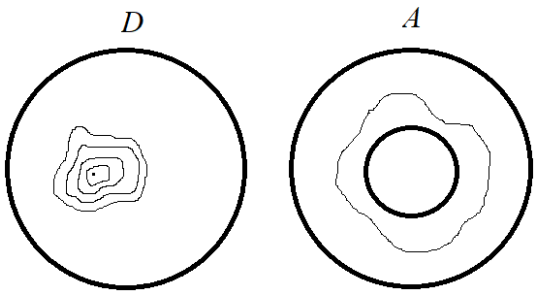

FIGURE 1. Closed paths in D and A.

Suppose then that someone (an evil supervillain perhaps?) demands we give a proof without using the notion of a path, since this does not generalizes well to arbitrary spaces (recall that we are concerned with varieties over finite fields, which are finite sets of points). Another way to approach this problem is by considering open coverings:

Recall first that for any topological space, an open subset $U \subseteq X$ is said to be connected if for any two non-empty open sets V, W such that $U = V \cup W$, we have $V \cap W \neq \emptyset$ (this means that U has only one connected component).

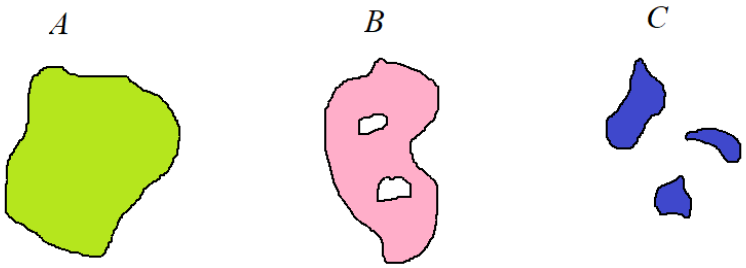

FIGURE 2. The first two sets are connected but the last one is not.

The disk D enjoys the following property (although this is not completely obvious): let $U, V \subseteq D$ be two non-empty open connected subsets such that $D = U \cup V$. Then $U \cap V$ is connected.

However, for the annulus A there is a covering by two open connected subsets $U, V \subseteq A$ such that $U \cap V$ is not connected, but consists of two components. This implies then that A cannot be homeomorphic to D, since for homoemorphic spaces the is a one-to-one correspondence between open coverings.

To push this further, if we have a disk with n holes, then there exists an open covering by two connected open subsets U, V such that $U \cap V$ has $n + 1$ connected components (somehow the number of holes seems to be determined by what is the worst number of components we can get).

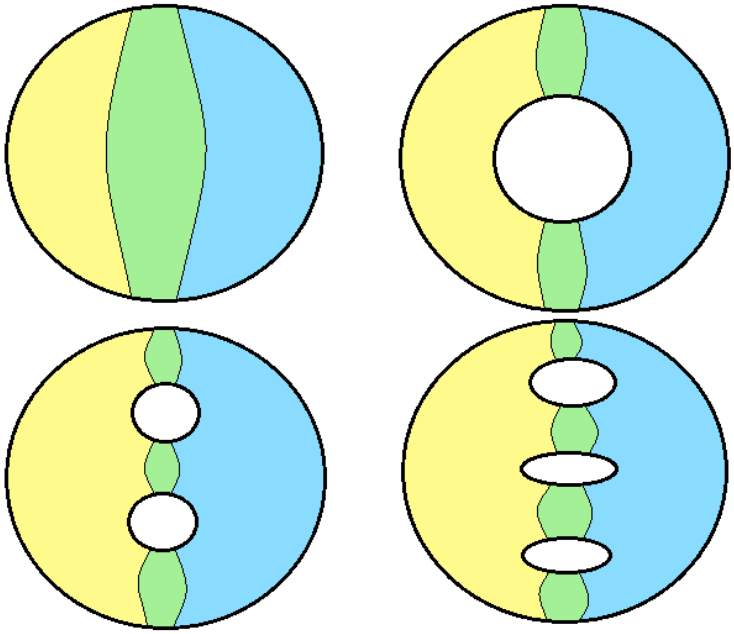

FIGURE 3. The intersection $U \cap V$ shown in green.

The moral of the story is that we can say something about the topology of a space by considering open coverings and intersections. By making this idea precise one ends up with the definition of Čech cohomology; for a topological space X and for any group G, such a construction gives a sequence of groups called the Čech cohomology groups

$$H^0(X,G),\ H^1(X,G),\ldots,H^i(X,G),\ldots$$

The group G is called the group of coefficients; typical choices include $\mathbb{Z},\mathbb{Q},\mathbb{C},\mathbb{Z}/n\mathbb{Z}$, for example. (We note that the open sets in a covering here need not be connected; the construction of Čech cohomology is defined as a certain 'quotient' which automatically tracks the number of components of the intersections versus the number of components of the open sets in the covering. Thus, the notion connectedness is not really required for the definition, only open coverings and intersections).

The intuition is that $H^i(X,G)$ decodes something about the i-dimensional structure of X. For example, $H^0(X,G)$ is a direct sum of n copies of G if X has n connected components. Roughly speaking, $H^i(X,G)$ is $G^{B_i(X)}$, where $B_i(X)$ is the number of i-dimensional holes on X (the i^{th} Betti number, two dimensional holes are cavities, for example). In the previous example,

$$H^i(D,\mathbb{Z}) = \begin{cases} \mathbb{Z}, & i=0 \\ 0, & i>0, \end{cases} \qquad H^i(A,\mathbb{Z}) = \begin{cases} \mathbb{Z}, & i=0,1 \\ 0, & i>1. \end{cases}$$

The fact that A and D are not homeomorphic is evident from that their cohomology groups disagree for $i=1$ (however, it is possible to have non-homeomorphic spaces whose cohomology groups are the same, so that this is not a complete characterization).

The reader who is not familiar with cohomology may wonder what is the relevance of the group of coefficients G, that is, can't we just count the number of i-dimensional holes and pat ourselves on the back? The point is that having more algebraic structure makes

the theory much more powerful; in our case we will choose the coefficient group to be a field, which means that the cohomology groups become vector spaces. It so happens that a map of spaces $f : Y \to X$ induces maps in cohomology $f^* : H^i(X, G) \to H^i(Y, G)$ (for each i), which are then linear maps of vector spaces; these induced maps will play a vital role. For topological spaces, the induced map is defined by noting that if $\{U_i\}$ is an open covering of X and $f : Y \to X$ is continuous, then $\{f^{-1}(U_i)\}$ is an open covering of Y.

Another way of motivating Čech cohomology is that it measures the amount of obstructions in going from 'local solutions' to 'global solutions', that is, if we can solve some problem in any sufficiently small open set, can we also find a global solution? Such an approach is often used, for example, when solving differential equations. As an example, the equation $e^{f(x)} = x$ has a complex analytic solution in a sufficiently small neighborhood of any point in the annulus $A \subset \mathbb{C}$, but the equation fails to have a global analytic solution in the whole of A. Looking at open coverings and intersections seems to be a very natural approach to try to understand such obstructions.

2.2. **Étale topology.** For any variety V there is a natural topology called the Zariski topology; $U \subseteq V$ is an open set if it is a complement of a finite collection of algebraic subsets of V. For example, open subsets of $\mathbb{A}^2_k$ are complements of finite collections of points and curves. Unfortunately this topology is insufficient for development of a cohomology. In fact, one can even show for this topology that $H^i(V, G) = 0$ for all $i > 0$; there simply are not enough open sets (strictly speaking, there is a way to define a so-called sheaf cohomology by using the Zariski topology, which replaces the coefficient group G by a more general object called a sheaf, but this is not suited for our purposes).

A variety over a finite field is just a finite collection of points, so that one could argue that any topology for such a variety is too trivial to yield interesting cohomological theory. A brilliant idea of Grothendieck was that we need to extend what we mean by a topology; recall that to define Čech cohomology, we essentially needed two concepts, (1) open covering, and (2) intersection. It turns out that both of these make sense if we replace open subsets $i : U \hookrightarrow X$ by more general mappings $f : Y \to X$, that need not be injective:

(1) A collection of maps $\{f_i : U_i \to X\}$ is said to be a covering, if $X = \bigcup f_i(U_i)$

(2) Given two maps $f : U \to X$ and $g : V \to X$, their 'intersection' is defined to be the fiber product over X

$$U \times_X V := \{(u, v) \in U \times V : f(u) = g(v)\}$$

(technically the fiber product depends also on the maps f, g but this is usually ignored to lighten the notation).

Exercise 2. (i) If $i : U \hookrightarrow X$ and $j : V \hookrightarrow X$ are two injections of open subsets of X, then their fiber product $U \times_X V$ can be naturally identified with $U \cap V$.

(ii) Give sets U and X and a function $f : U \to X$ so that the 'self-intersection' $U \times_X U$ is not U.

Suppose then that we are given some property E of maps. Then the E-topology of X is just the collection of all maps $f : U \to X$ satisfying E, and an E-covering is a covering $\{f_i : U_i \to X\}$ where each map satisfies E. The intersections are understood to mean the

fiber products. (Strictly speaking, we need to specify the underlying category, that is, the objects and the morphims, e.g. sets and functions, topological spaces and continuous maps, vartieties and morphisms of varieties. This generalization of topology, properly defined, is generally known as Grothendieck topology). Given such an E-topology, we can use the Čech construction to define cohomology with respect to the E-topology.

The question then is, what property E we should choose to define topology for a variety $X/\mathbb{F}_q$? There are many options ($E =$ 'flat', 'fppf', 'fpqc', ...), all of which yield interesting cohomologies, but for our purpose the choice is $E =$ 'étale'. We will not give here a rigorous definition for a map of varieties to be étale; the intuition is that $f : Y \to X$ is étale if it is 'smooth' and a 'local isomorphism', in some sense. We give examples of étale morphisms:

Example 2. If we have two non-singular varieties over complex numbers $Y/\mathbb{C}$ and $X/\mathbb{C}$, then they have the structures of complex manifolds. Then a map of varieties $f : Y \to X$ is étale if and only if it is a local isomorphism (with respect to their analytic topology).

Example 3. (At this point the temptation to mention schemes becomes unbearable momentarily, apologies for this lapse. This example is not terribly important in what follows). Suppose that k is an algebraically closed field. Recall that by Hilbert's Nullstellensatz (cf. Part I, Section 2), points on an affine variety X/k are in one-to-one correspondence with the maximal ideals of the coordinate ring $\mathcal{P}(X)$. An affine scheme over a commutative ring A is then essentially the pair $(\operatorname{Spec} A, A)$, where

$$\operatorname{Spec} A := \{\mathfrak{p} \subset A \text{ a prime ideal}\}$$

is the set of prime ideals of A (recall that maximal ideals are prime ideals). Thus, $\operatorname{Spec} \mathcal{P}(X)$ corresponds to the variety X (prime ideals that are not maximal correspond to subvarieties of X). Then any homomorphism of rings $f : A \to B$ defines a morphism of schemes

$$\operatorname{Spec} B \to \operatorname{Spec} A \qquad \mathfrak{p} \to f^{-1}(\mathfrak{p}).$$

(Exercise: check that pre-image of a prime ideal is prime). By definition, a morphism of affine schemes consists of a pair of maps like this, $A \to B$ and $\operatorname{Spec} B \to \operatorname{Spec} A$.

For any field k, there is an associated scheme $\operatorname{Spec} k = \{(0)\}$. Then a field extension $f : k \hookrightarrow K$ defines a map of schemes $\operatorname{Spec} K \to \operatorname{Spec} k$ which is étale if the field extension is separable. Thus, an étale morphism is a generalization of a separable field extension.

The exact definition of an étale map is most natural to give in the framework of schemes. For example, let A be a ring, $P_1, \ldots, P_n \in A[X_1, \ldots, X_n]$ be polynomials, and define the quotient ring

$$B = A[X_1, \ldots, X_n]/(P_1, \ldots, P_n).$$

Let $f : \operatorname{Spec} B \to \operatorname{Spec} A$ be the map defined by the composition

$$A \hookrightarrow A[X_1, \ldots, X_n] \to B,$$

where the latter map is the quotient map. Then f is étale if and only if the image of the Jacobian determinant $\det(\partial P_i/\partial X_j)$ in B is a unit, that is, has a multiplicative inverse in B. This is analogous to the inverse function theorem of multivariable calculus; a continuously differentiable function $F : \mathbb{R}^n \to \mathbb{R}^n$ is a local isomorphism (has an inverse

on sufficiently small neighborhood of every point) if its Jacobian determinant is non-zero at every point. This justifies the previous example of complex manifolds, since the inverse function theorem holds also for manifolds.

Another way of thinking about étale topology is by localization: for a usual topological space X and a point $x \in X$, we can think about problems 'locally' at sufficiently small open neighborhoods of x; a local problem is often easier to solve than a global problem. For étale topology on a variety X, an étale neighborhood of a point x is an étale map $f : U \to X$ such that $x \in f(U)$. For two étale neighborhoods U and V, neighborhood V is considered to be smaller than U if $V \to X$ factors through U as $V \to U \to X$. Then by considering smaller neighborhoods we can in some sense 'zoom in' at the point x. Local problems are again easier; in the framework of the previous example, étale maps of spectrum of fields correspond separable field extensions, and any problem on a field k is usually easier to solve for the algebraic closure $\overline{k}$, which is in the étale-sense a 'localization' of the problem.

Finally, we will denote by $H^i_{\text{ét}}(X, G)$ the Čech cohomology with respect to the étale topology.

2.3. **ℓ-adic cohomology.** There is still the subtle point of what is the correct choice for the group of coefficients G in our cohomology? For technical reasons we want to choose it to be a field with characteristic zero, but it turns out that for the obvious choices $\mathbb{Q}$ or $\mathbb{C}$ étale cohomology is not well-behaved; after all of the above constructions, a piece is of the puzzle is missing.

However, for a variety over $\mathbb{F}_q$ with $q = p^m$, étale cohomology with the coefficient groups $\mathbb{Z}/\ell^n\mathbb{Z}$ behave nicely for any given prime $\ell \neq p$ and any natural number n. This allows us to define the so-called ℓ-adic cohomology by

$$H^i(X, \mathbb{Q}_\ell) := \left(\lim_{\leftarrow} H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell. \tag{2.1}$$

We now proceed to explain what the above notations mean, although this will probably not be very enlightening (especially since we have not even given the proper definition of Čech cohomology). The main point here is that $\mathbb{Q}_\ell$ is a field with characteristic 0, and $H^i(X, \mathbb{Q}_\ell)$ is a $\mathbb{Q}_\ell$-vector space for every i.

We begin with the limit notation. Roughly speaking, within a category, it is possible to define a limit of a sequence of objects with morphisms between them, to be an object with certain properties; this may not always exist. For example, in the category of sets, suppose that we have a sequence of sets indexed by the integers

$$\cdots \subseteq U_{-1} \subseteq U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots.$$

We then have injections $f_{ij} : U_i \hookrightarrow U_j$ for any $j \geq i$. Then the direct limit and the inverse limit of this sequence are simply

$$\lim_{\rightarrow} U_i = \bigcup_i U_i, \qquad \lim_{\leftarrow} U_i = \bigcap_i U_i;$$

the dirction of the arrow indicates whether the object is 'terminal' or 'initial' to the given sequence. Another example is that the algebraic closure $\overline{\mathbb{F}}_q$ is the direct limit of $\mathbb{F}_{q^n}$ in the category of fields. A limit is in some sense 'the most efficient solution' for some problem, for instance, $\overline{\mathbb{F}}_q$ is the smallest field containing all fields $\mathbb{F}_{q^n}$.

Given any prime ℓ and any natural number n, there are natural (projection) ring homomorphisms $\mathbb{Z}/\ell^m\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$, for any $m \geq n$, that is, we have surjective maps

$$\mathbb{Z}/\ell\mathbb{Z} \leftarrow \mathbb{Z}/\ell^2\mathbb{Z} \leftarrow \mathbb{Z}/\ell^3\mathbb{Z} \leftarrow \cdots$$

Then the ℓ-adic integers are the inverse limit of this sequence in the category of rings

$$\mathbb{Z}_\ell = \lim_{\leftarrow} \mathbb{Z}/\ell^n\mathbb{Z}.$$

Concretely, we have

$$\mathbb{Z}_\ell = \left\{ \sum_{n \geq 0} a_n \ell^n : a_n \in \{0, 1, \ldots, \ell - 1\} \right\},$$

where the series may be infinite. Then $\mathbb{Q}_\ell$ is the quotient field of $\mathbb{Z}_\ell$, which is just

$$\mathbb{Q}_\ell = \left\{ \sum_{n \geq k} a_n \ell^n : k > -\infty,\ a_n \in \{0, 1, \ldots, \ell - 1\} \right\}.$$

It turns out that the maps $\mathbb{Z}/\ell^m\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$ induce maps in cohomology

$$H^i_{\text{ét}}(X, \mathbb{Z}/\ell^m\mathbb{Z}) \to H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z}),$$

and the inverse limit in (2.1) exists in the category of rings. This gives the limit a structure of a $\mathbb{Z}_\ell$-module, which means that we can take the tensor product $\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$; this in turn makes $H^i(X, \mathbb{Q}_\ell)$ into a $\mathbb{Q}_\ell$-vector space. The properties of $H^i(X, \mathbb{Q}_\ell)$ we next describe are inherited from the properties of $H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})$.

2.4. **Some basic properties.** The reason that the various different cohomology theories are called cohomologies is that they all satisfy some basic properties; we will list some of them here. In addition, there are some properties which are special to the étale cohomology included in the below; the list is by far not complete. In the below, we fix a non-singular projective variety X over $\overline{\mathbb{F}}_p$ and a prime $\ell \neq p$ (the choice of the prime is not important).

Finiteness. $H^i(X, \mathbb{Q}_\ell)$ is a finite dimensional vector space for all $i \geq 0$.

Cohomological dimension. If X is of dimension d, then $H^i(X, \mathbb{Q}_\ell) = 0$ for $i > 2d$ (we get $2d$ here since a d-dimensional complex variety is a $2d$-dimensional object; cf. the comparison property below).

Comparison. If X is a non-singular projective variety over $\mathbb{C}$, then there is an isomorphism

$$H^i(X, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \simeq H^i_{\text{an}}(X, \mathbb{C}),$$

where the latter cohomology is with respect to the analytic topology of the complex manifold $X(\mathbb{C})$ (this is an object which is much easier to understand).

Base change. If X is a good reduction modulo p, then

$$H^i(X, \mathbb{Q}_\ell) \simeq H^i(X(\mathbb{C}), \mathbb{Q}_\ell)$$

Functoriality. A morphism of varieties $f : X \to Y$ induces a map (of vector spaces) in cohomology for all $i \geq 0$

$$f^* : H^i(Y, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$$

(it is common to ignore in the notation that f^* depends on i).

Leschetz fixed-point formula. Under some assumptions, if $f : X \to X$ has a finite number $L(f, X)$ of fixed points (that is, points so that $x = f(x)$), then

$$L(f, X) = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(f^*;\, H^i(X, \mathbb{Q}_\ell)),$$

where f^* is the induced linear map $H^i(X, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$, and Tr is the trace (this part is one of the reasons why we want to have cohomology with coefficients in a field of characteristic 0; the quantity on the left is an integer).

Poincaré duality. For any $0 \leq i \leq 2d$, the cohomology $H^i(X, \mathbb{Q}_\ell)$ is the vector space dual of $H^{2d-i}(X, \mathbb{Q}_\ell)$. In particular, we have

$$\dim H^i(X, \mathbb{Q}_\ell) = \dim H^{2d-i}(X, \mathbb{Q}_\ell), \quad \dim H^0(X, \mathbb{Q}_\ell) = \dim H^{2d}(X, \mathbb{Q}_\ell) = 1.$$

It is noteworthy that by the time Weil formulated his conjectures, the counterparts of the above propoerties were known for the cohomology of complex analytic manifolds with respect to their analytic topologies; in that setting the theorems are not too difficult, but for ℓ-adic cohomology the above are all deep statements, whose proofs require a lot of care.

In the language of schemes, étale cohomology makes sense also for $\operatorname{Spec} k$, the spectrum of a field k. In that instance it turns out that the étale cohomology groups are exactly the so called Galois cohomology groups, which have been studied independently. Noting the comparison theorem above, we start to get a sense why theorems in étale cohomology lie deep; on one hand étale cohomology says something about complex manifolds, which are just about as continuous and smooth as anything can be. On the other hand, it also describes 'one point spaces' $\operatorname{Spec} k$, which is just about as discrete as possible. Étale cohomology gives a bridge between these two extremes, which is convenient for us since varieties over finite fields lie somewhere in the middle.

3. Remarks on the proofs

Let us recap the situation thus far: for any d-dimensional non-singular projective variety X over $\overline{\mathbb{F}}_q$, we have a collection of finite dimensional $\mathbb{Q}_\ell$-vector spaces, called the ℓ-adic cohomology,

$$H^0(X, \mathbb{Q}_\ell),\ H^1(X, \mathbb{Q}_\ell), \ldots, H^{2d}(X, \mathbb{Q}_\ell),$$

which satisfy some cozy properties. We now use these properties sketch the proofs for parts 1,2, and (almost) 4 of the Weil conjectures. Similarly as in the outline of the proof Weil for curves (cf. Part 1) we begin with the Frobenius morphism:

Recall that on $\overline{\mathbb{F}_q}$ we define the Frobenius morphism as

$$\mathrm{Fr}_q : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}, \quad x \mapsto x^q.$$

Then $\mathbb{F}_{q^n}$ is the fixed points of $\mathrm{Fr}_q^n(x) = x^{q^n}$

$$\mathbb{F}_{q^n} = \{x \in \overline{\mathbb{F}_q} : x = \mathrm{Fr}_q^n(x)\}. \tag{3.1}$$

Let X be a non-singular projective variety over $\mathbb{F}_q$ and denote $\overline{X} := X(\overline{\mathbb{F}_q})$. Recall the 'freshman's dream' identity $(x+y)^q = x^q + y^q$, which holds for any $x, y \in \overline{\mathbb{F}_q}$. Then for any polynomial f we have $f(x^q) = (f(x))^q$. Hence, if $x = (x_1, \ldots, x_n)$ is a solution to a given set of polynomial equations, then so is

$$\mathrm{Fr}_q(x) := (x_1^q, \ldots, x_n^q).$$

Thus, the Frobenius defines a map $\mathrm{Fr}_q : \overline{X} \to \overline{X}$ by acting separately on each coordinate of a point. Hence, by (3.1)

$$X(\mathbb{F}_{q^n}) := \{x \in \overline{X} : x = \mathrm{Fr}_q^n(x)\}, \tag{3.2}$$

that is, we can capture the points over $\mathbb{F}_{q^n}$ as the fixed points of the Frobenius Fr_q^n.

By the functoriality property, the Frobenius Fr_q induces a linear map of vector spaces in cohomology denoted by

$$\Phi : H^i(\overline{X}, \mathbb{Q}_\ell) \to H^i(\overline{X}, \mathbb{Q}_\ell),$$

and the map induced by Fr_q^n is just Φ^n. Hence, by (3.2) and by the Lefschetz fixed-point formula

$$N_n = |X(\mathbb{F}_{q^n})| = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(\Phi^n;\, H^i(\overline{X}, \mathbb{Q}_\ell)).$$

Thus, we arrive at the following formula for the zeta function

$$Z_X(T) = \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right) = \prod_{i=0}^{2d} \left[\exp\left(\sum_{n=1}^{\infty} \mathrm{Tr}(\Phi^n;\, H^i(\overline{X}, \mathbb{Q}_\ell)) \frac{T^n}{n}\right)\right]^{(-1)^i} \tag{3.3}$$

We now require the following general lemma from linear algebra

Lemma 1. *Let V be a finite dimensional vector space, and let $\phi : V \to V$ be a linear map. Then we have the formal power series identity*

$$\exp\left(\sum_{n=1}^{\infty} \mathrm{Tr}(\phi^n; V) \frac{T^n}{n}\right) = \det(1 - \phi T; V)^{-1}.$$

We will not prove the above lemma, but note that if V is one-dimensional, then ϕ is just multiplication by a scalar λ so that the above is just the identity

$$\exp\left(\sum_{n=1}^{\infty} \lambda^n \frac{T^n}{n}\right) = \frac{1}{1 - \lambda T}.$$

Combining the above lemma with (3.3) we get

$$Z_X(T) = \frac{P_1(T) P_3(T) \cdots P_{2d-1}(T)}{P_0(T) P_2(T) \cdots P_{2d}(T)} \quad \text{for} \quad P_i(T) = \det(1 - \Phi T; H^i(\overline{X}, \mathbb{Q}_\ell)), \tag{3.4}$$

that is, $P_i(T)$ is the characteristic polynomial of Φ acting on the i^{th} cohomology. By the finiteness property, the $H^i(\overline{X}, \mathbb{Q}_\ell)$ are finite dimensional vector spaces, so that P_i are polynomials and

$$\deg P_i = \dim H^i(\overline{X}, \mathbb{Q}_\ell).$$

This essentially proves the first part of the Weil conjectures, which was to show that the zeta function is rational; strictly speaking, since $H^i(X, \mathbb{Q}_\ell)$ are $\mathbb{Q}_\ell$-vector spaces, we still need to check that we get a quotient of polynomials with rational coefficients. Let $\mathbb{Q}[[T]]$ denotes the ring of power series with coefficients in $\mathbb{Q}$, an let $\mathbb{Q}(T)$ and $\mathbb{Q}_\ell(T)$ denote the rings of quotients functions of polynomials with coefficients in $\mathbb{Q}$ and $\mathbb{Q}_\ell$, respectively. Then it holds that $\mathbb{Q}[[T]] \cap \mathbb{Q}_\ell(T) = \mathbb{Q}(T)$. By series expansion of the exponential we see that $Z_X(T) \in \mathbb{Q}[[T]]$. By (3.4) we see that also $Z_X(T) \in \mathbb{Q}_\ell(T)$. Hence, $Z_X(T) \in \mathbb{Q}(T)$, that is, $Z_X(T) = P(T)/Q(T)$ for some rational P and Q. Note that this does not yet show that any of the individual P_i has rational coefficients.

It is perhaps not difficult believe from the representation (3.4) that the functional equation

$$Z_X\left(\frac{1}{q^d T}\right) = \pm q^{dE/2} T^E Z_X(T)$$

is essentially a consequence of the Poincaré duality property, which states that $H^i(\overline{X}, \mathbb{Q}_\ell)$ and $H^{2d-i}(\overline{X}, \mathbb{Q}_\ell)$ are vector space duals (with some additional observations and linear algebra). From the proof we get (unsurprisingly) the formula for the constant

$$E = \sum_{i=0}^{2d} (-1)^i \dim H^i(\overline{X}, \mathbb{Q}_\ell),$$

which is very similar to the conjectured formula of part four of the Weil conjecture. Unfortunately, we do not yet know that any of the P_i are the ones conjectured by part three (since we do not even know that any of P_i has rational coefficients); that this is so is a deep result of Deligne.

However, given that this is true, we need to check that if X is a good reduction modulo p, then $\dim H^i(\overline{X}, \mathbb{Q}_\ell)$ is the i^{th} Betti number of $X(\mathbb{C})$, which is by definition

$$B_i := \dim H^i_{\text{an}}(X(\mathbb{C}), \mathbb{C}),$$

where the cohomology is with respect to the analytic topology. This now follows from the base change property, which allows us to change $\overline{X}$ to $X(\mathbb{C})$, combined with the comparison property.

By the formula $P_i(T) = \det(1 - \Phi T; H^i(\overline{X}, \mathbb{Q}_\ell))$ the Riemann hypothesis for X also has a new interpretation: the eigenvalues of Φ acting on $H^i(\overline{X}, \mathbb{Q}_\ell)$ are complex numbers of modulus $q^{i/2}$. This is what Deligne showed to be true. Unfortunately we are not able to discuss this further here, for it requires much deeper ideas (but more importantly due to my own lack of knowledge).

4. Applications

4.1. **Exponential sums.** Similarly as in the case of curves, the Weil conjectures have a big impact for the theory of exponential sums. However, in this instance the most important results do not follow directly from the Weil conjectures, but rather from

Deligne's proof of the Riemann hypothesis for varieties. We give some examples of such results before we elucidate the connection between exponential sums and cohomology described above.

Theorem 2. *Let $Q \in \mathbb{F}_p[X_1, \dots, X_n]$ be a polynomial of degree d satisfying certain smoothness conditions. Then (for $e(z) := e^{2\pi i z}$)*

$$\sum_{x_1,\dots,x_n \in \mathbb{F}_p} e\left(Q(x_1,\dots,x_n)/p\right) \leq (d-1)^n p^{n/2}.$$

This theorem is very impressive in that we get square root cancellation with respect to every variable in the sum. Another application is the generalization of the Weil bound to the Hyper-Kloosterman sums

$$\mathrm{Kl}_n(a;p) := \sum_{\substack{x_1,\dots,x_n \in \mathbb{F}_p \\ x_1 \cdots x_n \equiv a \,(\mathrm{mod}\, p)}} e((x_1 + \cdots + x_n)/p).$$

Note that this is a $(n-1)$-dimensional sum, since the condition $x_1 \cdots x_n \equiv a$ fixes one of the variables.

Theorem 3. *We have square root cancellation in $\mathrm{Kl}_n(a;p)$, that is,*

$$|\mathrm{Kl}_n(a;p)| \leq n p^{(n-1)/2}.$$

The theory of more general exponential sums, called trace functions, is an active area of research. It allows the study of bounds for the 'Fourier transform' of exponential sums, as well as study of correlations of exponential sums. For example,

Theorem 4. *If $a, b \in \mathbb{F}_p$, $a \neq 0$ and $(a,b) \neq (1,0)$ then*

$$\left| \sum_{x \in \mathbb{F}_p^\times} \mathrm{Kl}_3(x;p)\overline{\mathrm{Kl}_3(ax;p)} e(bx/p) \right| \ll p^{3-1/2}.$$

The theorem states that even in the correlations we get square root cancellation! This result can be applied to show that in equidistribution estimates for the ternary divisor function $d_3(n)$, we can go beyond the so called Bombieri-Vinogradov result. A result of similar type was used by Zhang to break the Bombieri-Vinogradov barrier for the equidistribution of primes in arithmetic progressions (under a slight modification); he then applied this to show (using the GPY-sieve) that there are inifitely many primes p_n such that $p_{n+1} - p_n \leq 70,000,000$, obtaining for the first time bounded gaps between primes.

A result of a different nature concerns the argument of the Gauss sums

$$G_\chi(a;p) := \sum_{x \in \mathbb{F}_p^\times} \chi(x) e(ax/p) = \overline{\chi(a)} G_\chi(1;p).$$

Recall that for all non-trivial characters χ we have $|G_\chi(1;p)| = \sqrt{p}$. A very difficult problem is to find the argument of a Gauss sum. However, we have

Theorem 5. *The sets $\{G_\chi(1;p)/\sqrt{p} : \chi \text{ non-trivial}\}$ becomes equidistributed on the unit circle as $p \to \infty$.*

We give a quick sketch of the proof for this: by Weil's equidistribution criterion, the theorem is equivalent to saying that for any fixed n

$$W_n(p) := \sum_{\chi \,(\mathrm{mod}\, p) \text{ non-trivial}} \left(\frac{G_\chi(1;p)}{\sqrt{p}} \right)^n = o(p).$$

as $p \to \infty$. By inserting the definition of Gauss sums and expanding we find that

$$\begin{aligned} W_n(p) &= \frac{1}{p^{n/2}} \sum_{x_1,\dots,x_n \in \mathbb{F}_p^\times} e((x_1 + \cdots + e_n)/p) \sum_{\chi \,(\mathrm{mod}\, p) \text{ non-trivial}} \chi(x_1 \cdots x_n) \\ &= \frac{p-1}{p^{n/2}} \mathrm{Kl}_n(1;p) \end{aligned}$$

by orthogonality of Dirichlet characters. Thus, by Theorem 3 we have $|W_n(p)| \ll p^{1/2}$, which is even stronger than what we required.

We now give a rough description of how the cohomological machinery is applied to obtain such results. For concreteness, suppose we have a one dimensional exponential sum of the form

$$S = \sum_{x \in U} \left(\text{some algebraic expression of } x \text{ involving characters} \right),$$

where U is $\mathbb{F}_q$ minus some special points; we do not specify here what sort of expressions are allowed, but as an example we might have

$$\sum_{x \in U} e(P(x)/p)\chi(Q(x)),$$

where P and Q are rational functions and U is $\mathbb{F}_p$ minus the poles of P and Q and the zeros of Q.

In general, the set U has a structure of a scheme as a subscheme of $\mathbb{A}^1_{\mathbb{F}_q}$, so we think of U as a curve of some sort. Associated to such an exponential sum there is an object called an ℓ-adic sheaf on U, denoted by $\mathcal{F}$; this is a generalization of the coefficient group in cohomology, which allows one to define the ℓ-adic sheaf cohomology groups (which are vector spaces over $\mathbb{Q}_\ell$)

$$H^0(\overline{U}, \mathcal{F}), \qquad H^1(\overline{U}, \mathcal{F}), \quad \text{and} \quad H^2(\overline{U}, \mathcal{F})$$

(technically we need to take 'cohomology with compact support H^i_c' but let us ignore this detail). The cohomology for $i > 2$ is zero since U is one dimensional. For our simplified exposition it suffices to say that for an exponential sum, there is a natural way to associate a collection of finite dimensional vector spaces $H^i(\overline{U}, \mathcal{F})$ over $\mathbb{Q}_l$.

In analogue to the Lefschetz fixed-point formula, we now have a trace formula for the exponential sum

$$S = \sum_{i=0}^{2} (-1)^i \mathrm{Tr}(\Phi;\, H^i(\overline{U}, \mathcal{F})), \tag{4.1}$$

where Φ is the map in cohomology induced by the Frobenius (cf. previous section). Under some smoothness conditions, Deligne's proof of the Riemann hypothesis gives:

The eigenvalues of Φ acting on $H^i(\overline{U}, \mathcal{F})$ are complex numbers of absolute value $q^{i/2}$.

Thus, using (4.1) we obtain the following dichotomy: if $\dim H^2(\overline{U}, \mathcal{F}) = 0$, then we get square root cancellation $|S| \ll q^{1/2}$. If $\dim H^2(\overline{U}, \mathcal{F}) \neq 0$, then we get a main term with square root cancellation for the error term $S = \alpha q + \mathcal{O}(q^{1/2})$; the constant α is determined by the eigenvalues of Φ on the second cohomology.

The second cohomology group is usually easy to compute by using Poincaré duality, which states that it is the dual of the zeroth cohomology group. In the case that the second cohomology is not zero, also the eigenvalues of Φ on it can be determined. A very difficult problem is to understand the Frobenius eigenvalues on the first cohomology; this is usually impossible, so that the implied constant in $\mathcal{O}(q^{1/2})$ bounded just by the dimension of the first cohomology.

All of this generalizes to higher dimensional exponential sums, with a trace formula

$$S = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(\Phi;\, H^i(\overline{U}, \mathcal{F})),$$

where $U \subseteq \mathbb{A}^d_{\mathbb{F}_q}$. For higher dimensional sums, under some conditions, Deligne shows that $H^i(\overline{U}, \mathcal{F})) = 0$ except for $i = d$ (here again we must take cohomology with compact support). This is how one gets square root cancellation with respect to every variable in the sum in the above sample theorems.

4.2. **Ramanujan conjecture.** There are analogues of the Riemann hypothesis for the coefficients of modular forms. An instance of this is the Ramanujan conjecture: define the discriminant modular form by

$$\Delta(z) := q \prod_{n=1}^{\infty} (1 - q^n)^{24} \quad \text{for} \quad q := e^{2\pi z}.$$

It is well known that this is a modular form of weight 12; this means that the function has a symmetry property that for any integers a, b, c, d such that $ad - bc = 1$

$$\Delta\left(\frac{az + b}{cz + d}\right) = (c + dz)^{12} \Delta(z).$$

Define the Ramanujan τ-function by

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n,$$

where $\tau(n)$ are integers.

Then we can associate to Δ a Dirichlet series

$$L(s, \tau) := \sum_{n=1}^{\infty} \tau(n) n^s.$$

Then the Ramanujan conjectures state that

(1) τ is multiplicative, that is, for all $(m, n) = 1$ we have $\tau(mn) = \tau(m)\tau(n)$

(2) For all primes p we have $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$, so that by combining this with (1) we have an Euler product

$$L(s,\tau) = \prod_p \left(1 - \frac{\tau(p)}{p^s} + \frac{p^{11}}{p^{2s}}\right)^{-1}$$

(3) We have the uppper bound $|\tau(p)| \leq 2p^{11/2}$.

To see the analogue with the Riemann hypothesis, write

$$L_p(s,\tau) := 1 - \frac{\tau(p)}{p^s} + \frac{p^{11}}{p^{2s}}$$

for the local factor, so that $L(s,\tau) = \prod_p L_p(s,\tau)^{-1}$. Then the third part implies that if $L_p(s,\tau) = 0$, then $\Re\, s = 11/2$. This is because by making the change of variables $u = p^{-s}$ we have to solve the quadratic equation

$$1 - \tau(p)u + p^{11}u^2 = 0.$$

Let α and β be the solutions. Then $p^{11}(u-\alpha)(u-\beta) = 1 - \tau(p)u + p^{11}u$, so that we have

$$p^{11}(\alpha+\beta) = \tau(p), \qquad p^{11}\alpha\beta = 1.$$

The bound (3) gives that the discriminant $\tau(p)^2 - 4p^{11} \leq 0$. Hence, α and β are complex conjugates, and combining with $p^{11}\alpha\beta = 1$ we get $|\alpha| = |\beta| = p^{-11/2}$, as claimed.

The first two parts were proven by Mordell in 1917 using so-called Hecke operators. The last part was proven by Deligne in 1974 using the ideas he had developed for the proof of the Weil Conjectures; the connection between the two is not obvious and is not discussed further here.

5. History and further reading suggestions

As was mentioned in the first part, the origin of the Weil conjectures is in Weil's article [8]. In there Weil noted that the conjecture holds for curves and gave examples to support his conjecture. In 1954 Weil gave a talk at ICM where he explained that the conjecture could be approached if only we had a cohomology theory with coefficients in a field of characteristic zero for varieties over finite field; this strategy is what we have tried to explain in the previous section. We again note that at the time such a cohomology theory already existed for varieties over complex numbers, by using their analytic topology.

To make progress, the theory of algebraic geometry needed to be developed in a more general framework. Starting from 1955, algebraic geometry was rewritten and developed in much greater generality by the likes of Serre, Grothendieck and Dieudonné. Serre was the first to try to construct the desired cohomology theory but with limited success. Building on Serre's work, Grothendieck had the insight that such a cohomology theory might be constructed using a more flexible notion of a topology, now known as a Grothendieck topology. In the 1960's, Grothendieck in collaboration with M. Artin started to develop the theory of étale cohomology.

It should be noted that in 1960, the rationality and the functional equation of the zeta function had been proven by Dwork using a different approach based on p-adic analysis

[4]. However, this approach did not give a way to prove the Riemann hypothesis for varieties, so that developing a cohomology theory that Weil had envisioned was still on the agenda.

After years of work, Grothendieck and Artin had developed the étale cohomology enough to give rigorous proof of the rationality and the functional equation in the spirit of Weil; this work was recorded in the famous SGA notes. Grothendieck formulated the so-called standard conjectures for étale cohomology, and noted that the last parts of the Weil conjectures would follow from these. However, proving these standard conjectures appeared to be inaccessible, and some parts of these conjectures still remain open.

It was Deligne who found a different route to the Weil conjectures [2], [3]. Deligne's proof relies heavily on the theory that had been developed, and is inspired by a construction of Lefschetz in classical algebraic geometry. It also makes use of the so called Rankin-Selberg convolution of L-functions, which had been used in the context of automorphic L-functions.

For texts on basic algebraic geometry and algebra, see the reading suggestions at the end of the first part.

For a more detailed description of étale cohomology and Deligne's proof of the Weil conjectures, see Kowalski's notes [5]. He assumes some background in algebraic geometry but most of it should be accessible.

For proofs of the basic theorems in étale cohomology, see Deligne's SGA notes [1] and Milne's lecture notes [7]. Both require good background on basic algebraic geometry. Chapter 6 of Deligne's notes contains a description of the theory of exponential sums from a cohomological perspective; this is quite readable even with relatively little theoretical background, at least if you are willing to accept the cohomological machinery as a black box.

For more on exponential sums and how to use them in applications of analytic number theory, see the recent notes of Michel [6].

References

[1] P. Deligne. SGA 4 1/2. URL: `https://publications.ias.edu/node/378`.
[2] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.
[3] P. Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.
[4] B. Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960.
[5] E. Kowalski. Trying to understand Deligne's proof of the weil conjectures. URL: `www.math.ethz.ch/~kowalski/deligne.pdf`.
[6] P. Michel. Lectures on applied ℓ-adic cohomology. URL: `https://arxiv.org/abs/1712.03173`.
[7] J. Milne. Lectures on étale cohomology. URL: `www.jmilne.org/math/CourseNotes/LEC.pdf`.
[8] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

Department of Mathematics and Statistics, University of Turku, FI-20014 University of Turku, Finland

E-mail address: `jori.e.merikoski@utu.fi`