MA8202 - Introduction to the Weil Conjectures

Jonathan Komada Eriksen

In this note we will state the Weil conjectures, which is a series of conjectures about the zeta function of smooth, projective varieties. Our first goal will therefore naturally be to define smooth, projective variates, as well as the dimension of a variety. We'll see that all of these terms can be easily defined with the tools we developed in the course.

1 Smooth, Projective Varieties

As the Weil-conjectures is a statement about **smooth**, **projective** varieties, our first goal will be to define these. As a warm up, recall that we defined **affine** algebraic sets as

$$V(I) = \{P \in \bar{k}^n \mid f(P) = 0, \forall f \in I\}$$

for some ideal $I \subseteq k[x_1, \ldots, x_n]$ (notice that this is the same definition as $V(I) \subseteq \operatorname{Spec}_{\mathfrak{m}} \bar{k}[x_1, \ldots, x_n]$, identitying $\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle = \mathfrak{m} \in \operatorname{Spec} \bar{k}[x_1, \ldots, x_n]$ with the point $P = (\alpha_1, \ldots, \alpha_n)$), and that given such a set $V \subseteq \bar{k}^n$, we definded **the ideal of** V to be the ideal

$$I(V) = \{f \in \bar{k}[x_1, \ldots, x_n] \mid f(P) = 0, \forall P \in V\}$$

The affine algebraic set V is said to be an **affine algebraic variety** if $I(V)$ is a prime ideal (in $\bar{k}[x_1, \ldots, x_n]$).

However, it turns out that when doing geometry, it is often more useful to work over projective space, which can be thought of as the right "completion" of affine space in this setting (e.g. statements like Bézout's theorem become true). Projective space has many (equivalent) definitions; we'll start by giving a purely algebraic definition of projective space over any field.

Definition 1.1. *We denote the projective n-space over k as*

$$\mathbb{P}^n(k) = k^{n+1} / \sim$$

where $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if there exists some $\lambda \in \bar{k}^\times$ such that $(x_0, \ldots, x_n) = (\lambda y_0, \ldots, \lambda y_n)$. We typically denote elements of $\mathbb{P}^n(k)$ as $(x_0 : \cdots : x_n)$.

Naturally, similarily to the affine case, projective algebraic sets are subsets of $\mathbb{P}^n(\bar{k})$ carved out by ideals of $k[x_0, \ldots, x_n]$. However, we must be a bit more careful; notice that for instance, if we set $I = \langle x - 1 \rangle \subseteq \bar{k}[x, y]$, and consider the projective point $(1 : 0) \subseteq \mathbb{P}^1(\bar{k})$. Then

$$f(1, 0) = 0, \forall f \in I$$

but, on the other hand

$$f(2, 0) = 1, f(x, y) = x - 1$$

even though the projective points $(1 : 0) = (2 : 0)$. We fix this, by recalling that $R = k[x_0, \ldots, x_n]$ has the structure of a graded ring, given by

$$R = \bigoplus R_i,$$

where R_n has the k-basis $\{x_0^{e_0} \ldots x_n^{e_n} \in k[x_0, \ldots, x_n] \mid e_0 + \cdots + e_1 = n\}$. If we now require I to be a **homogenous** ideal of R (i.e. an ideal where $x = I$ implies that all homogenous components are in I), then this will be fixed. To see this, notice that if $f \subseteq R_d$ is homogenous, then

$$f(\lambda P) = \lambda^d f(P), \quad \forall \lambda \in \bar{k}^*.$$

We can now more or less copy the affine definitions, but keeping the grading in mind, given a homogenous ideal $I \subseteq \bar{k}[x_0, \ldots, x_1]$, we define a **projective** algebraic set to be

$$V(I) = \{P \in \mathbb{P}^n(\bar{k}) \mid f(P) = 0, \forall f \in I\},$$

and given a projective algebraic set, we define its homogenous ideal to be

$$I(V) = \langle \{f \in \bar{k}[x_0, \ldots, x_n] \mid f \text{ homogenous}, f(P) = 0, \forall P \in V\} \rangle.$$

Then, again, we call the projective algebraic set V a **projective variety** if its homogenous ideal $I \subseteq \bar{k}[x_0, \ldots, x_n]$ is a prime ideal. If V can be generated by a (homogenous) ideal of $k[x_0, \ldots, x_n]$, we write V/k to signify this.

Notice that even if we're working over a non-algebraically closed field varieties are per definition subsets of $\mathbb{P}^n(\bar{k})$. But often we will only consider the part of a variety defined over a subfield. Given a variety V, we call the set

$$V(k) = V \cap \mathbb{P}^n(k)$$

the k**-rational points** of a variety V,

Example 1.2. *Consider the variety*

$$E/\mathbb{F}_5 : Y^2Z = X^3 - Z^3$$

(i.e $V(I)$ given by $I = \langle Y^2Z - X^3 - Z^3 \rangle \subseteq \mathbb{F}_5[X, Y, Z]$ in the notation above). While E itself contains infinitely many points, it can be verified that

$$E(\mathbb{F}_5) = \{(0:1:0), (2:3:1), (0:1:1), (4:0:1), (0:4:1), (2:2:1)\}$$

and that

$$\#E(\mathbb{F}_{5^2}) = 36, \#E(\mathbb{F}_{5^3}) = 126, \#E(\mathbb{F}_{5^4}) = 576, \ldots$$

The example above demonstrates something we are interested in: Counting the rational points of smooth, projective varieties (the example above is even a so-called **elliptic curve**, in which case one can ask even more specialized questions!). But, we are getting ahead of ourselves...

Next, we wish to define what it means for a projective variety to be **smooth**. In class, we briefly mentioned the definition of this, but lets do it more in detail.

The following definitions will given be in terms of affine varieties. Its is easy to turn any projective variety into an affine variety (though some information might be lost!). We denote such an affine variety by $V \cap k^n$ (called an **affine chart** of V), whose ideal is

$$I(V \cap k^n) = \{f(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \mid f \in I(V)\} \subseteq k[x_1, \ldots, x_n]$$

where the inclusion is obtained by renaiming the coefficients.

The definitions below is then simply extended to projective varieties by considering any non-empty affine chart of the projective variety V.

Definition 1.3. *Let V/k be an affine variety. The **coordinate ring** of V/k is defined as*

$$k[V] = k[x_1, \ldots, x_n]/I(V)$$

Notice that by definition of a variety, $k[V]$ is an integral domain. We then use the tools from commutative algebra to give two quick definition.

Definition 1.4. *The **dimension** of a variety V, denoted by $\dim V$ is defined to be the krull-dimension of $k[V]$.*

Next,, given any point $P \in V$, we define the **localization at** P as the localization at the maximal ideal

$$M_P = \{f \in \bar{k}[V] \mid f(P) = 0\}.$$

As was briefly mentioned in one of the lectures, a variety V is **smooth at a point** P if the localization at M_P is a regular local ring. This finally allows us to define

Definition 1.5. *Let V be an (affine) variety. Then V is said to be **smooth** if it is smooth at all points $P \in V$.*

2 The Weil Conjectures

Next, we state the Weil Conjectures, which is a set of statements (all of them now proven) encoding information about the number of points of a smooth projective variate over a finite fields. This number seems to behave rather elusively, and statements about it always seem to be very deep and meaningful. To motivate the story, let us consider the special case which typically receives a lot of attention, namely the case of **elliptic curves**, or smooth projective varieties of dimension 1 and **genus** 1 (don't worry about the last part. It is an invariant algebraic curves, typically defined in terms of the so-called Riemann-Roch theorem).

Let $E/\mathbb{F}_q$ be an elliptic curve. How does $\#E(\mathbb{F}_q)$ behave? That seems extremely hard to answer, but at least a famous theorem by Hasse bounds the number:

Theorem 2.1 (Hasse)**.** *Let E and q be as above. Then*

$$\#E(\mathbb{F}_q) = q + 1 - t$$

where $|t| \leq 2\sqrt{q}$.

What if we instead ask how the numbers $\#E(\mathbb{F}_q), \#E(\mathbb{F}_{q^2}), \#E(\mathbb{F}_{q^3}), \ldots$ relate? This question is completely answered by the Weil conjectures, which are in fact true much more generally than for elliptic curves. Weil himself managed to prove them in the special case of *abelian* varieties (i.e. projective varieties whose points have a natural group structure).

Finally, before we state the Weil conjectures, we might instead consider a different question: given a curve $E/\mathbb{Q}$, how does the numbers $\#E(\mathbb{F}_p)$ relate for all primes p? An answer to this is partly (and conjecturally!) given by the famous Birch and Swinnerton-Dyer conjecture, which is way outside the scope of this note.

The Weil Conjectures consists of four statements regarding the zeta-function of a variety defined over a finite field.

Definition 2.2. *Let $V/\mathbb{F}_q$ be a variety. The **(local) zeta-function** of $V/\mathbb{F}_q$ is defined as*

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \#V(\mathbb{F}_{q^n})\frac{T^n}{n}\right) \in \mathbb{Q}[[T]]$$

where $\exp(F(T)) = \sum_{k=0}^{\infty} F(T)^k/k!$ for any power series $F(T) \in \mathbb{Q}[[T]]$.

Remark 2.3. *This zeta function is indeed related to the Riemann-zeta function, though that story is quite long and complicated. To give a quick summary, one can generalize the Riemann zeta function to the ring of integers of any numberfield (by means of the Euler product).*

Further, the ring of integers of a number field is largely analogous to the coordinate ring of an algebraic curve, due to the fact that these coordinate rings are also Dedekind domains. Therefore, one can generalize the Riemann-zeta function to an algebraic curve. Then finally, one can again generalize the zeta function from these curves to arbitrary varieties, by a variable change relating the divisors of a curve to the number of rational points.

The following example is taken directly from Silverman:

Example 2.4. *Let $V(\langle 0\rangle)/\mathbb{F}_q$ (i.e. $V = \mathbb{P}^N(\bar{\mathbb{F}}_q)$). Notice that*

$$\#\mathbb{P}^N(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)-1}}{q^n - 1} = \sum_{i=0}^{N} q^n i.$$

We compute the zeta function

$$\begin{aligned} Z(\mathbb{P}^n/\mathbb{F}_q; T) &= \exp\left(\sum_{n=1}^{\infty}\left(\sum_{i=0}^{N} q^{ni}\right)\frac{T^n}{n}\right) \quad \textit{(Definition + formula above)} \\ &= \prod_{i=0}^{N} \exp\left(\sum_{n=1}^{\infty}\frac{(q^iT)^n}{n}\right) \\ &= \prod_{i=0}^{N} \exp(-\log(1-q^iT)) \quad \textit{(Look at the derivative of the sum)} \\ &= \prod_{i=0}^{N}\frac{1}{1-q^iT} \end{aligned}$$

which shows that

$$Z(\mathbb{P}^n/\mathbb{F}_q; T) = \frac{1}{(1-T)(1-qT)(1-q^2T)\dots(1-q^NT)}$$

The fact that above, the zeta function was actually a rational function is no coincidence! In fact, it is precicely the first Weil conjecture.

Theorem 2.5 (Weil Conjectures)**.** *Let $V/\mathbb{F}_q$ be a smooth, projective variety of dimension N.*

1. ***Rationality:*** *$Z(V/\mathbb{F}_q; T)$ is a rational function.*
2. ***Functional Equation:*** *There exists an integer ϵ, called the **Euler characteristic** of V, such that*

$$Z(V/\mathbb{F}_q; 1/q^NT) = \pm q^{\frac{N\epsilon}{2}} T^\epsilon Z(V/\mathbb{F}_q; T)$$

3. ***Riemann Hypothesis:*** *The zeta function factors as*

$$Z(V/\mathbb{F}_q;T) = \frac{P_1(T)P_3(T)\dots P_{2N-1}(T)}{P_0(T)P_2(T)\dots P_{2N}(T)}$$

where $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N T$, *and all* $P_i(T) \in \mathbb{Z}[T]$ *is of the form*

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

for $\alpha_{ij} \in \bar{\mathbb{Q}}$, *with absolute value* $q^{i/2}$.

Remark 2.6. *Under the interpretation of Remark 2.3, the "Riemann Hypothesis" above indeed corresponds to the fact that all zeroes of the zeta function lies on the critical strip (in this case under a change of variables).*

There is a very nice proof of the first Weil conjecture in Silverman, for the elliptic curve case (which is probably the "simplest" case; an elliptic curve is an abelian variety of dimension one). This proof, though more elementary, uses very specific arithmetic properties of elliptic curves that we have not touched upon, so we will instead try to give an idea of the proof in the general case, using Weil Cohomology.

2.1 Weil Cohomology

Weil cohomology, like any (co)homology theory defines a family of functors H^i. To get started, we must briefly mention what morphisms we look at between varieties. Funny enough, these are simply called **morphisms**.

Given two varieties, V_1, V_2, we define a **rational map** from V_1 to V_2 to be some map of the form

$$f : V_1 \to V_2$$
$$f(P) = (f_0(P) : \dots : f_n(P))$$

where $f_i \in \mathrm{Quot}(\bar{k}[V_1])$. A rational map is said to be **regular** at a point P if there exists some $g \in \mathrm{Quot}(\bar{k}[V_1])$ such that $(gf_i)(P) \in V_2$ for all i. A **morphism** is then a rational map, that is regular at all $P \in V_1$.

Definition 2.7. *Let* k *and* K *be fields, where characteristic of* $K = 0$. *A* ***Weil cohomology theory*** *is then a family of contravariant functors*

$$H^i : \{\textit{smooth, projective varieties over } k\} \to \mathrm{vec}\ K$$

satisfying a bunch of properties. In particular,

$$H^i(V) = 0$$

for all $i < 0, i > 2N$, *where* $N = \dim V$.

Many of the properties that this cohomology theory is supposed to satisfy is similar other cohomology-theories. For instance, there should exist a cup-product and Poincaré duality and Künneth's formula should be true. We omit the full definition, as we will only explicitly require the property above, while many of the others are "baked into" Lefschetz formula (whose proof we also omit anyway).

From topology, Lefschetz formula roughly counts the number of fixed points of a continuous map $f : X \to X$. The following theorem is the algebraic geometry version.

Theorem 2.8 (Lefschetz Formula)**.** *Let $V/\mathbb{F}_q$ be a smooth, projective variety, let $f : V \to V$ be an endomorphism (a morphism from a variety to itself), and let H^* be any Weil-cohomology. Under "reasonable assumptions" on f, we have that*

$$|\{x \in V \mid f(x) = x\}| = \sum_{i=0}^{2n} (-1)^i \mathrm{tr}(H^i(f))$$

The "reasonable assumptions" above are very technical, but in particular, they say that f must only have isolated fixed points.

We need one more Lemma from linear algebra

Lemma 2.9. *Let V be a finite dimensional vector space, and let $\phi : V \to V$ be a linear map. Then*

$$\det(1 - \phi T)^{-1} = \exp\left(\sum_{r=1}^{\infty} \mathrm{tr}(\phi^r)\frac{T^r}{r}\right)$$

as a formal power series in T.

Proof. Done by induction on the dimension. For $\dim V = 1$, ϕ correspond to scalar multiplication. Put $\phi = \alpha$. By the same computation as in Example 2.4, we have that

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

For the inductive step, note first that we may assume that K is algebraically closed (V possibly by extending the scalars of V). Then ϕ has invariant subspace V'. By a change of basis, ϕ can be put on the form

$$\left(\begin{array}{c|c} \phi_{11} & \phi_{12} \\ \hline 0 & \phi_{22} \end{array}\right)$$

where ϕ_{11} is the action of ϕ restricted to V'. By the induction hypothesis, the claim

is true for the linear maps ϕ_{11}, ϕ_{22}, so we get

$$\begin{aligned}\det(1-\phi T)^{-1} &= \det(1-\phi_{11}T)^{-1}\det(1-\phi_{22}T)^{-1} \\ &= \exp\left(\sum_{r=1}^{\infty}\operatorname{tr}(\phi_{11}^r)\frac{T^r}{r}\right)\exp\left(\sum_{r=1}^{\infty}\operatorname{tr}(\phi_{22}^r)\frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty}(\operatorname{tr}(\phi_{11}^r)+\operatorname{tr}(\phi_{22}^r))\frac{T^r}{r}\right) = \exp\left(\sum_{r=1}^{\infty}\operatorname{tr}(\phi^r)\frac{T^r}{r}\right)\end{aligned}$$

□

Finally, we show that the first Weil conjecture follows immidiately from the two lemmas above.

Theorem 2.10 (Weil Conjectures 1.)**.** *Let $V/\mathbb{F}_q$ be a smooth, projective variety of dimension N. Then $Z(V\mathbb{F}_q;T)$ is a rational function.*

Proof. Recall that

$$Z(V/\mathbb{F}_q;T) = \exp\left(\sum_{n=1}^{\infty}\#V(\mathbb{F}_{q^n})\frac{T^n}{n}\right).$$

Let $\pi : V \to V$ denote the q-power **frobenius endomorphism**, i.e. the morphism defined by

$$\pi(x_0 : \cdots : x_n) = \pi(x_0^q : \cdots : x_n^q),$$

and notice that $\#V(\mathbb{F}_{q^n}) = |V \cap \mathbb{P}^n(\mathbb{F}_{q^n})| = |\{x \in V \mid \pi(x) = x\}|$. Then, by Lefschetz formula, we get an expression for $\#V(\mathbb{F}_{q^n})$, so

$$\begin{aligned}Z(V/\mathbb{F}_q;T) &= \exp\left(\sum_{r=1}^{\infty}\#V(\mathbb{F}_{q^r})\frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty}\sum_{i=0}^{2N}(-1)^i\operatorname{tr}(H^i(\pi^r))\frac{T^r}{r}\right) \\ &= \prod_{i=0}^{2N}\exp\left(\sum_{r=1}^{\infty}(-1)^i\operatorname{tr}(H^i(\pi^r))\frac{T^r}{r}\right) \\ &= \prod_{i=0}^{2N}\exp\left(\sum_{r=1}^{\infty}\operatorname{tr}(H^i(\pi)^r)\frac{T^r}{r}\right)^{(-1)^i}\end{aligned}$$

Then, by using Lemma 2.9, we see that

$$Z(V/\mathbb{F}_q;T) = \prod_{i=0}^{2N} \det(1 - H^i(\pi)T)^{(-1)^{i+1}} = \frac{P_1(T)P_3(T)\dots P_{2N-1}(T)}{P_0(T)P_2(T)\dots P_{2N}(T)}$$

where $P_1(T) = \det(1 - H^i(\pi)T) \in \mathbb{Q}[T]$. □

This concludes the (outline of the) proof of the first Weil conjecture, **assuming that a Weil cohomology exists**. This idea started the search for the existence of a Weil cohomology. Historically, the first example of a Weil cohomology, the so-called **ℓ-adic cohomology** was developed by Grothendieck. The ℓ-adic cohomology is constructed as an inverse limit of what he called **étale cohomology**. This allowed Grothendieck to prove the Weil conjectures, with the exception of the Riemann Hypothesis, for which it would remain unsolved for another 10 years, before Deligne managed prove it.

For our question, asking how the $\mathbb{F}_{q^k}$-rational points relate, the answer is indeed given by the zeta function. For instance, using the above, one can show that the number of $\mathbb{F}_{q^k}$-rational points of an elliptic curve relies only on the number $\mathbb{F}_q$-rational points. See Silverman for details.