MUYD 2016: Etale cohomology and the Weil conjectures

David Roe, transcribed by Soham

August 2016

Stuff I know that I'm not writing: varieties, sheaves, equalizer exact sequence, local rings, lrs, schemes

0.1 Background

Let X be a smooth projective variety. We denote the number of points on it over a finite field as $\#X(\mathbb{F}_q)$. These numbers are of arithmetic interest since they give us an analogue of the Riemann hypothesis, using a new zeta function.

We can assemble these into a generating function

$$\zeta(X,t) = \exp\left(\frac{t^n}{m}\#X(\mathbb{F}_q)\right)$$

The Weil conjectures are a series of unexpected-sounding statements about ζ that parallel the Riemann hypothesis.

0.2 Weil cohomology theories

Let K be a field of char 0.

Definition 1. A *Weil cohomology theory* is a contravariant functor

$$H^* : \{\text{smooth proj varieties over } k = \mathbb{F}_p\} \to \{\text{graded } K\text{-algebras}\}$$

such that, with $\dim X = n$,

- $H^i(X)$ is a finite-dimensional K-vector space
- $H^r(X) = \begin{cases} 0, & i = 0 \\ K, & i = 2n \\ 0, & i > 2n \end{cases}$
- Poincaré duality: there is a nondegenerate pairing

  $$H^i(X) \times H^{2n-i}(X) \to H^{2n}(X) = K$$

  Note the similarity to de Rham cohomology:

  $$H^i(X) \times H^{n-i}(X) \to H^n(X) \xrightarrow{\int_M} \mathbb{R}$$

- Künneth formula:

  $$H^*(X \times Y) = H^*(X) \otimes H^*(Y)$$

- "Some condition" on algebraic cycles: there is a *cycle class map*

  $$Z^i(X) \to H^{2i}(X)$$

- "Weak Lefschetz." If $H \subset \mathbb{P}^m$ is a hyperplane and $W = H \cap X$, the map $W \to X$ gives an isomorphism

  $$H^i(X) \to H^i(W)$$

  for $i \leq n-2$, and an injection $i = n-1$.

- Let $w \in H^2(X)$ be the image of the cycle W under the cycle class map. Define

  $$L : H^i(X) \to H^{i+2}(X)$$

  sending x to $x \cdot w$. Then $L^i : H^{n-i}(X) \to H^{n+i}(X)$ is an isomorphism.

David: "So, this is the definition of a Weil cohomology theory. ... Sweet."
Frobenius is a map $X(\overline{k}) \to X(\overline{k})$. It acts as the qth power on coordinates.
Now define

$$X(R) = \mathsf{Hom}_{\mathsf{Sch}/k}(\operatorname{Spec} R, X)$$

Let X be a smooth projective variety over an algebraically closed field, and $\varphi : X \to X$.

$$\#\text{fixed points of } \varphi = \sum (-1)^i \operatorname{Tr}(\varphi | H^i(X))$$

Let $\varphi = \text{Frob}$. Then the fixed points are exactly the points of $X(\mathbb{F}_q)$. (Replacing with Frob^m gives you $X(\mathbb{F}_{q^m})$.)

Lemma 1. If $\psi : V \to V$ is a linear map of vector spaces, with characteristic polynomial

$$\det(1 - \psi T | V) = P_\psi(T)$$

and $P_\psi(T) = \prod_i (1 - c_i T)$, then

$$\operatorname{Tr}(\psi^m | V) = \sum c_i^m.$$

Thus

$$\log \frac{1}{P_\psi(T)} = \sum_{m=1}^{\infty} \operatorname{Tr}(\psi^m | V) \frac{T^m}{m}.$$

Theorem 1.

$$\zeta(X, T) = \prod P_i(T)^{(-1)^{i+1}}$$

where

$$P_i(T) = \det(1 - \operatorname{Frob} T | H^i(X))$$

Proof.

$$\begin{aligned}
\zeta(X, T) &= \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} T^m\right) && (0.1)\\
&= \exp\left(\sum_m \sum_{r=0}^{2n} (-1)^r \operatorname{Tr}(\text{Frob}^m | H^r(X)) \frac{T^m}{m}\right) && (0.2)\\
&= \prod_{r=0}^{2n} \exp\left(\operatorname{Tr}(\text{Frob}^m | H^r(X)) \frac{T^m}{m}\right)^{(-1)^r} && (0.3)\\
&= \prod_{r=0}^{2n} P_i(T)^{(-1)^{r+1}}. && (0.4)
\end{aligned}$$

□

Idea: etale maps are the analogues of local diffeomorphisms. If X, Y are smooth varieties, $\varphi : X \to Y$ is etale if it is an isomorphism on each tangent space.

Definition 2. If R is a ring, and $0 \to A \to B \to C \to 0$ is an exact sequence of R-modules, then a ring map $R \to S$ is *flat* if

$$0 \to A \otimes_R S \to B \otimes_R S \to C \otimes_R S \to 0$$

is exact.

Definition 3. A map $f : R \to S$ is etale if

1. S is fg as an R-algebra
2. S is a flat R-algebra
3. For every maximal ideal $\mathfrak{m}$ of S, let $\mathfrak{p} = f^{-1}(\mathfrak{m})$. Then $S_\mathfrak{m}/f(\mathfrak{p})S_\mathfrak{p}$ is a finite and separable field extension of $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$.

- If $R = k$ is a field, the etale maps are $k \to \prod_i L_i$ with L_i/k finite and separable. (In fact, such products are called *etale algebras*.)
- If R is a Dedekind domain, L a finite separable extension of $k := \operatorname{Frac} R$, S the integral closure of R in L, let $y \in \bigcap$ ramified primes of S. Then $S[1/y]$ is etale, and every etale R-algebra is a product of such.

Picture of etale maps: finitely branched coverings, a la $\mathbb{C} \setminus \{0\} \to \mathbb{C}^2$, $z \mapsto z^2$. 0 is a ramification point; kill it with fire.

0.3 Sites

Definition 4. A *site* is a category C with distinguished collections of maps $(U_i \to U)_{i \in I}$ called coverings such that

1. Given a diagram

$$\begin{tikzcd} V_i \arrow[r] \arrow[d] & U_i \arrow[d] \\ V \arrow[r] & U \end{tikzcd}$$

pullbacks exist and $(V_i := V \times_U U_i \to V)_{i \in I}$ is a covering.

2. If $(U_i \to U)$ is a covering and $(V_{ij} \to U_i)$ are coverings, then

$$(V_{ij} \to U_i \to U)$$

is too.

3. $(U \to U)$ is a covering.

Sites that matter:

- Zariski site: open sets in the Zariski topology
- Small etale site of X: objects are maps $U \overset{\text{et}}{\to} X$
- fppf, fpqc, big etale

A covering is a collection of maps

$$U_i \to U$$

which is locally finite (look at a point, look at an affine open around it; want that finitely many images of U_i intersect the affine open) and jointly surjective (as a set, $U = \cup \operatorname{im}(U_i \to U)$).

$\mathsf{Shv}_{\mathsf{Ring}}(\mathsf{Et}(X))$ is an abelian category.

There is a functor

$$\mathsf{Shv}_{\mathsf{Ring}}(\mathsf{Et}(X)) \to \mathsf{Ring}$$

of the form

$$F \mapsto \Gamma(F, X) := F(X \overset{\text{id}}{\to} X)$$

which is left-exact.

If

$$0 \to F \to G \to H \to 0$$

is exact, then

$$0 \to \Gamma(F, X) \to \Gamma(G, X) \to \Gamma(H, X) \to \cdots \to ???$$

We say a sheaf I is *injective* if

$$\begin{tikzcd} F \arrow[r, dashed] & I \\ F' \arrow[u] \arrow[ur] & \end{tikzcd}$$

If F is an etale sheaf then there exists an injective etale sheaf I and a map

$$0 \to F \hookrightarrow I_1 \to I_2 \to \cdots$$

where you take cokernels and embed into injectives at every step (start by noticing that $0 \to F$ is not surjective, so you have a nontrivial cokernel, etc)

Can take F to be the constant sheaf $\mathbb{Z}/l^m$, then get $H^r(X, \mathbb{Z}/l^m)$. Take an inverse limit to get

$$H^r(X, \mathbb{Q}_l) = H^r(\mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

0.4 Also, let's just prove Fermat's last theorem

0.4.1 (because why not)

Note that we can assume $n = 4$ or $n = l$ prime. $n = 3, 4$ are classical descent arguments of Fermat and Euler.

Suppose $a^l + b^l = c^l$ is a solution. Consider

$$E : y^2 = x(x - a^l)(x - b^l)$$

(complete later; I went to breakfast at this point)