The Weil conjectures

Noah Held

09.05.2019

1 ℓ-adic cohomology

Let X be a scheme and ℓ a prime number.

Definition 1. *The ℓ-adic cohomology modules of X are*

$$\mathrm{H}^i(X, \mathbb{Z}_\ell) := \lim_{n \in \mathbb{N}} \mathrm{H}^i(X, \mathbb{Z}/\ell^n\mathbb{Z});$$

they are naturally $\mathbb{Z}_\ell$-modules, so we can extend coefficients to $\mathbb{Q}_\ell$:

$$\mathrm{H}^i(X, \mathbb{Q}_\ell) := \mathrm{H}^i(X, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

1.1 Finiteness theorem

Theorem 2. *If X is proper over a separably closed field K, then $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ is a finitely generated $\mathbb{Z}_\ell$-module for every i.*

Lemma 3. *Let $M = \lim_n M_n$ be a limit of finite torsion $\mathbb{Z}_\ell$-modules. Then M is finitely generated if and only if $M/\ell M$ is finite.*

Proof. "Only if" is clear, so we assume that $M/\ell M$ is finite.

We first prove that M is ℓ-adically complete, i.e. that the canonical morphism of topological $\mathbb{Z}_\ell$-modules

$$\gamma \colon M \longrightarrow \widehat{M} := \lim_{n \in \mathbb{N}} M/\ell^n M$$

is an isomorphism. The subgroups $\ell^n M$ are closed, because they are quasi-compact in the Hausdorff space M. Hence $\widehat{M}$ is Hausdorff in the limit topology. Note that $\gamma(M)$ is dense in $\widehat{M}$; because γ maps from a quasi-compact to a Hausdorff space, it is closed, and thus surjective. It now suffices to show that γ is injective. But

$$\ker(\gamma) = \bigcap_{n=0}^{\infty} \ell^n M$$

consists of those elements of M which are divisible by arbitrary powers of ℓ; the only such element is 0, because each M_n is annihilated by a power of ℓ.

Choose a continuous $\mathbb{Z}_\ell$-linear surjection

$$\mathbb{Z}_\ell^{\oplus r} \longrightarrow\!\!\!\!\!\rightarrow (\mathbb{Z}/\ell\mathbb{Z})^{\oplus r} \longrightarrow\!\!\!\!\!\rightarrow M/\ell M.$$

It lifts to some

$$\mathbb{Z}_\ell^{\oplus r} \longrightarrow\!\!\!\!\!\rightarrow (\mathbb{Z}/\ell^2\mathbb{Z})^{\oplus r} \longrightarrow M/\ell^2 M,$$

which must be surjective by Nakayama's Lemma. Continuing inductively, we find a continuous $\mathbb{Z}_\ell$-linear map $\mathbb{Z}_\ell^{\oplus r} \to \widehat{M}$ that is surjective by the same topological arguments as above. $\square$

Lemma 4. *Cofiltered limits of profinite groups are exact.*

Proof. Basically because cofiltered limits of nonempty quasi-compact Hausdorff spaces are nonempty. $\square$

Proof of Theorem 2. By Lemma 3, it suffices to show that there is an exact sequence

$$\mathrm{H}^i(X, \mathbb{Z}_\ell) \xrightarrow{\ell} \mathrm{H}^i(X, \mathbb{Z}_\ell) \to \mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}). \tag{$*$}$$

Because of the indirect definition of $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ we cannot use the short exact sequence

$$0 \to \mathbb{Z}_\ell \xrightarrow{\ell} \mathbb{Z}_\ell \to \mathbb{Z}/\ell\mathbb{Z} \to 0$$

directly. But multiplication by ℓ on $\mathbb{Z}_\ell$ is the limit of multiplication by ℓ on $\mathbb{Z}/\ell^n\mathbb{Z}$, so we first consider these finite levels and then pass to the limit. For every $n \geqslant 2$ we have the commutative diagram

$$\begin{tikzcd}
 & & 0 \arrow[dr] & & 0 & & \\
 & & & \ell\mathbb{Z}/\ell^n\mathbb{Z} \arrow[ur] \arrow[dr] & & & \\
 & & \mathbb{Z}/\ell^n\mathbb{Z} \arrow[ur] \arrow[rr, "\ell"] & & \mathbb{Z}/\ell^n\mathbb{Z} \arrow[r] & \mathbb{Z}/\ell\mathbb{Z} \arrow[r] & 0, \\
 & \ell^{n-1}\mathbb{Z}/\ell^n\mathbb{Z} \arrow[ur] & & & & & \\
0 \arrow[ur] & & & & & &
\end{tikzcd}$$

where the two paths of length 4 between 0's are short exact sequences. Note that $\lim_n \mathrm{H}^i(X, \ell^{n-1}\mathbb{Z}/\ell^n\mathbb{Z}) = 0$ for each i, because the transition morphisms are 0. Taking the limit of the long exact sequence induced by the diagonal short exact sequence, it follows that the induced morphism

$$\mathrm{H}^i(X, \mathbb{Z}_\ell) \to \lim_{n\in\mathbb{N}} \mathrm{H}^i(X, \ell\mathbb{Z}/\ell^n\mathbb{Z})$$

is an isomorphism. Thus we get the desired exact sequence ($*$) by taking the limit of the long exact sequences associated to the second short exact sequence in the diagram. $\square$

1.2 ℓ-adic Galois representations from cohomology

Let K be a field, $\overline{K}$ a separable closure of K, G_K the absolute Galois group of K, $\varphi\colon X \longrightarrow \mathrm{Spec}(K)$ a proper morphism of schemes. Form the cartesian square

$$\begin{tikzcd} \overline{X} \arrow[r] \arrow[d, "\overline{\varphi}"] & X \arrow[d, "\varphi"] \\ \mathrm{Spec}(\overline{K}) \arrow[r] & \mathrm{Spec}(K). \end{tikzcd}$$

We wish to equip the finite-dimensional vector spaces $\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)$ with the structure of a continuous G_K-module. By the theorem of proper base change applied to the cartesian square above, there is a natural isomorphism

$$\mathrm{R}^i\overline{\varphi}_*(\mathbb{Z}/\ell^n\mathbb{Z}) \cong (\mathrm{R}^i\varphi_*(\mathbb{Z}/\ell^n\mathbb{Z}))_{\overline{K}}.$$

But the group on the right-hand side is naturally a continuous dicrete G_K-module via the equivalence of categories

$$\mathbf{\acute{E}t}(\mathrm{Spec}(K)) \xrightarrow{\simeq} G_K\text{-}\mathbf{Mod}, \quad \mathcal{F} \longmapsto \mathcal{F}_{\overline{K}}.$$

In particular, taking limits, we obtain a continuous action of G_K on $\mathrm{H}^i(\overline{X}, \mathbb{Z}_\ell)$, at least if the latter is endowed with the profinite topology; but the profinite topology on $\mathrm{H}^i(\overline{X}, \mathbb{Z}_\ell)$ agrees with its natural ℓ-adic topology by Lemma 3. Now extend coefficients to get a continuous homomorphism

$$G_K \longrightarrow \mathrm{GL}(\mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)),$$

as desired.

2 Zeta functions of schemes

2.1 The ζ-function

Let $X \longrightarrow \mathrm{Spec}(\mathbb{Z})$ be a morphism of finite type, and denote by $|X|$ the set of closed points of X.

Lemma 5. *The residue field $\kappa(x)$ of any $x \in |X|$ is finite.*

Proof. Let $A := \mathcal{O}_X(U)$ for an affine open neighborhood of U of x in X, and let $\mathfrak{m}_x$ be the maximal ideal of A corresponding to x. Since the composite morphism

$$\mathbb{Z} \longrightarrow A \twoheadrightarrow A/\mathfrak{m}_x = \kappa(x)$$

is of finite type, $\kappa(x)$ cannot contain $\mathbb{Q}$. Hence x lies over a prime p, and its residue field must be a finite extension of $\mathbb{F}_p$. $\square$

Definition 6. *The* Hasse-Weil zeta function of X *is the Euler product*

$$\zeta(X,s) := \prod_{x\in|X|} (1-\mathrm{Card}(\kappa(x))^{-s})^{-1}.$$

Example 7. If X is the spectrum of the ring of integers of a number field K, then $\zeta(X,s)$ is the Dedekind zeta function of K.

2.2 The Z-function

Assume now that X is of finite type over a finite field $\mathbb{F}_q$, and write

$$\deg(x) := [\kappa(x) : \mathbb{F}_q] \quad (x \in |X|).$$

Lemma 8. *For any* $n \in \mathbb{Z}^{\geqslant 0}$ *there are only finitely many* $x \in |X|$ *with* $\deg(x) \leqslant n$.

Proof. Because this is true for any affine space over $\mathbb{F}_q$, it is also true if X is affine; for the general case, cover X by finitely many affine open subsets. □

Definition 9. *We define*

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

Remark 10. $Z(X,q^{-s}) = \zeta(X,s)$.

Lemma 11. *The above formula for* $Z(X,T)$ *defines an element of* $Z[\![T]\!]$.

Proof. Observe that

$$Z(X,T) = \prod_{x\in|X|} \sum_{i=0}^{\infty} T^{i\deg(x)}.$$

Modulo T^n, only those finitely many $x \in |X|$ with $\deg(x) \leqslant n$ contribute to the product. Hence the formula for $Z(X,T)$ defines an element of

$$Z[\![T]\!] = \lim_{n\in\mathbb{N}} \mathbb{Z}[T]/(T^n).$$ □

Remark 12. $Z(X,T)$ is the generating function associated with the sequence

$a_n :=$ the number of effective 0-cycles on X of degree n.

2.3 The logarithmic derivative

Lemma 13. *Let* R *be a ring. The map*

$$\mathrm{dlog}\colon (1+R[\![T]\!]T,\cdot,1) \to (R[\![T]\!],+,0), \quad F \mapsto F'/F,$$

where F' *denotes the formal derivative of* F*, is a continuous group homomorphism.*

Proof. Because $R[\![T]\!]$ is a normed ring, inversion is continuous. The map $F \mapsto F'$ is also continuous, so continuity of dlog follows. If $F, G \in 1 + R[\![T]\!]T$, then

$$\operatorname{dlog}(FG) = \frac{(FG)'}{FG} = \frac{F'G + FG'}{FG} = \frac{F'}{F} + \frac{G'}{G} = \operatorname{dlog}(F) + \operatorname{dlog}(G).$$

Hence dlog is also compatible with the group structures. □

Lemma 14. *If R is torsion-free as a $\mathbb{Z}$-module, then* dlog *is injective.*

Proof. Then $F \mapsto F'$ is injective. □

Proposition 15. *We have*

$$T \operatorname{dlog}(Z(X,T)) = \sum_{n=1}^{\infty} \operatorname{Card}(X(\mathbb{F}_{q^n}))T^n.$$

Proof. Since dlog is a continuous group homomorphism,

$$T \operatorname{dlog}(Z(X,T)) = T \sum_{x \in |X|} \operatorname{dlog}((1 - T^{\deg(x)})^{-1}).$$

A direct calculation, using the fact that dlog is a group homomorphism, shows that

$$\operatorname{dlog}((1 - T^{\deg(x)})^{-1}) = \frac{\deg(x)T^{\deg(x)-1}}{1 - T^{\deg(x)}}.$$

Thus

$$\begin{aligned}
T \operatorname{dlog}(Z(X,T)) &= \sum_{x \in |X|} \deg(x)T^{\deg(x)} \sum_{i=0}^{\infty} T^{i \deg(x)} \\
&= \sum_{x \in |X|} \deg(x) \sum_{i=1}^{\infty} T^{i \deg(x)} \\
&= \sum_{n=1}^{\infty} \sum_{\deg(x) \mid n} \deg(x)T^n \\
&= \sum_{n=1}^{\infty} \operatorname{Card}(X(\mathbb{F}_{q^n}))T^n,
\end{aligned}$$

as desired. □

Example 16. (a) If $X = \mathbb{A}^m_{\mathbb{F}_q}$, then

$$\begin{aligned}\sum_{n=1}^{\infty} \mathrm{Card}(X(\mathbb{F}_{q^n}))T^n &= \sum_{n=1}^{\infty} q^{mn}T^n \\ &= \frac{1}{1-q^mT} - 1 \\ &= \frac{q^mT}{1-q^mT} \\ &= T\,\mathrm{dlog}((1-q^mT)^{-1}).\end{aligned}$$

Hence $Z(X,T) = (1-q^mT)^{-1}$.

(b) If $X = \mathbb{P}^m_{\mathbb{F}_q}$, then the stratification of X by affine spaces yields the decomposition

$$|X| = \coprod_{d=0}^{m} |\mathbb{A}^d_{\mathbb{F}_q}|,$$

and therefore

$$Z(X,T) = \prod_{d=0}^{m} Z(\mathbb{A}^d_{\mathbb{F}_q}, T) = \prod_{d=0}^{m} \frac{1}{1-q^dT}.$$

3 The conjectures

We now fix:

X	a scheme, proper and smooth of relative dimension d over $\mathbb{F}_q$,
$\mathbb{F}$	an algebraic closure of $\mathbb{F}_q$,
$\overline{X}$	the base change of X to $\mathbb{F}$,
ℓ	a prime not dividing q,
σ	the geometric Frobenius, i.e. the inverse of $x \mapsto x^q$ in $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$.

Weil conjectured, in his article [Weil], that:

(1) $Z(X,T)$ is a rational function in T.

(2) $Z(X,T)$ satisfies the functional equation

$$Z(X,(q^dT)^{-1}) = \pm q^{d\chi}T^{\chi}Z(X,T),$$

where χ is the Euler–Poincaré characteristic of X.

(3) We have

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

with $P_0 = 1 - T$, $P_{2d} = 1 - q^d T$, and more generally

$$P_i = \prod_{j=1}^{B_i} (1 - \alpha_{ij} T)$$

for algebraic integers α_{ij} of complex absolute value $q^{i/2}$.

(4) If X arises as the reduction of a nonsingular projective variety X_η over a number field, then B_i is the i^{th} Betti number of $X_\eta(\mathbb{C})$.

The excellent review [Katz] of [Deligne] by Katz summarizes the subsequent developments. Rationality of $Z(X,T)$ was first proven by Dwork in [Dwork], for arbitrary schemes of finite type over $\mathbb{F}_q$. Grothendieck later gave a cohomological interpretation of $Z(X,T)$ and a proof of its rationality. Abbreviate $\mathrm{H}^i := \mathrm{H}^i(\overline{X}, \mathbb{Q}_\ell)$. For every i, define

$$P_i := \det(\mathrm{id}_{\mathrm{H}^i} - \sigma T) \in 1 + \mathbb{Q}_\ell[T].$$

Theorem 17 (Grothendieck)**.** *We have*

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

in $\mathbb{Q}_\ell[\![T]\!]$.

Corollary 18. $Z(X,T) \in \mathbb{Q}(T)$.

This follows immediately from the following general fact:

Lemma 19 (Hankel[1])**.** *Let K be a field, $F = \sum_{i=0}^{\infty} a_i T^i \in K[\![T]\!]$, and L a field extension of K. Then F is rational over K if and only if it is rational over L.*

Proof. Note that F is rational over K if and only if there exist nonnegative integers M and N such that the linear subspace V_K of K^{N+1} spanned by the vectors

$$(a_i, a_{i+1}, \dots, a_{i+N}) \quad (i \geqslant M)$$

lies in a linear hypersurface, i.e. $\dim_K(V_K) < N+1$; same with L in place of K. But $V_L = L \otimes_K V_K$, so $\dim_K(V_K) < N+1$ if and only if $\dim_L(V_L) < N+1$. □

Grothendieck also proved the following theorem, which together with the preceding one implies conjecture (2):

[1] http://www-personal.umich.edu/~mmustata/zeta_book.pdf, Proposition 4.13.

Theorem 20 (Grothendieck)**.** *The map $\lambda \mapsto q^d/\lambda$ induces a bijection between the eigenvalues of σ on H^i and the eigenvalues of σ on H^{2d-i}, preserving algebraic multiplicity.*

In view of Grothendieck's theorems, conjecture (3) follows from:

Theorem 21 (Deligne)**.** *Every eigenvalue λ of σ on H^i is an algebraic number, and the absolute value of each of its complex conjugates is $q^{i/2}$.*

Corollary 22. *Each P_i has integral coefficients and is independent of ℓ.*

Lemma 23. *The content*

$$\mathrm{cont}\colon \mathbb{Z}[T] \to \mathbb{Z}^{\geqslant 0}, \quad \sum_{i=0}^{r} a_i T^i \mapsto \gcd(a_i)$$

extends to a multiplicative map

$$\mathrm{cont}\colon Z[\![T]\!] \to \mathbb{Z}^{\geqslant 0}, \quad \sum_{i=0}^{\infty} a_i T^i \mapsto \gcd(a_i).$$

Proof. As for polynomials, it suffices to show that the product of primitive (i.e., of content 1) power series is primitive. That is so because $\mathbb{F}_p[\![T]\!]$ is an integral domain for any prime p. □

Lemma 24 (Fatou[2])**.** *If $F \in \mathbb{Z}[\![T]\!] \cap \mathbb{Q}(T)$, then there exist coprime $P, Q \in \mathbb{Z}[T]$ such that $F = P/Q$ and $Q(0) = 1$.*

Proof. We can write $F = P/Q$ with $P, Q \in \mathbb{Z}[T]$ coprime. We will show that $Q(0) = \pm 1$; the lemma follows upon replacing (P, Q) by $(Q(0)P, Q(0)Q)$.

Let us first prove that Q is primitive. Indeed, if m were to divide each coefficient of Q, i.e. $(1/m)Q \in \mathbb{Z}[T]$, then $(1/m)QF = (1/m)P \in \mathbb{Z}[T]$, contradicting the assumption that P and Q are coprime.

Since P and Q are coprime in $\mathbb{Q}[T]$, there are $U, V \in \mathbb{Z}[T]$ and a positive integer m such that $UP + VQ = m$. But $UP + VQ = (UF + V)Q$, so

$$\mathrm{cont}(UF + V) = \mathrm{cont}((UF + V)Q) = m$$

since Q is primitive. Hence $m \mid (UF + V)(0)$ and $m = (UF + V)(0)Q(0)$, which can only happen if $Q(0) = \pm 1$. □

Proof of Corollary 22. Note that the polynomials P_i are pairwise coprime, because they don't share any roots in $\overline{\mathbb{Q}}_\ell$. Applying the preceding lemma, write $Z(X, T) = P/Q$ for coprime $P, Q \in \mathbb{Z}[T]$ with $P(0) = 1 = Q(0)$. Since P and Q are still coprime in $\mathbb{Q}_\ell[T]$, we must have

$$P = P_1 P_3 \cdots P_{2d-1}, \quad Q = P_0 P_2 \cdots P_{2d}.$$

[2] http://www-math.mit.edu/~rstan/ec/ec1.pdf, p. 629.

(equality holds because the constant coefficients agree). Let $K \subset \overline{\mathbb{Q}}_\ell$ be the splitting field of PQ over $\mathbb{Q}$. The roots of P_i in K are the roots of PQ of complex absolute value $q^{i/2}$. Because this condition is Galois-invariant, P_i is stable under the action of $\mathrm{Gal}(K/\mathbb{Q})$, i.e. $P_i \in \mathbb{Q}[T]$. By Gauss's Lemma, $P_i \in \mathbb{Z}[T]$. Finally, because this description of the roots of P_i—among the roots of PQ, which do not depend on ℓ—is independent of ℓ, so is P_i itself. $\square$

References

[Deligne] Deligne, Pierre, *La conjécture de Weil I*, Inst. Hautes Études Sci. Publ. Math., 43 (1974), 273–307.

[Dwork] Dwork, Bernard, *On the Rationality of the Zeta Function of an Algebraic Variety*, Amer. J. Math., 82 (1960), 631–648

[Groth] Grothendieck, Alexander, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, Vol. 9, Exp. No. 279 (1966), 41–55

[Katz] Katz, Nicholas M., MR0340258, https://mathscinet.ams.org/mathscinet-getitem?mr=340258

[Weil] Weil, André, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497–508