ÉTALE COHOMOLOGY READING GROUP

NOTES: ROSS PATERSON

Disclaimer. These notes are attempts at live note-taking during sessions of a study group held at the University of Bristol during October–December 2023. The speakers name is listed at the start of each lecture. All errors are the fault of the transcriber. Thanks to Matthew Bisatt and Farhad Babaee for some corrections, and to the speakers for excellent talks!

Lecture 1 (Céline): Towards Étale Cohomology

Place yourself in the 1930's and 40's, thinking as if you were Weil in those days. How did Weil think of the conjectures?

I: Historical Background

(1) Finite Fields. Consider a system V of homogeneous polynomials (say, over $\mathbb{Z}$). As number theorists, we have an obvious goal.

Goal. *Understand the integer solutions $V(\mathbb{Z})$.*

Remark 1. Gauss first introduced the idea of working modulo some prime p, in particular, that if $V(\mathbb{F}_p) = \emptyset$ then $V(\mathbb{Z}) = \emptyset$.

Assume that the ideal generated by the system V, $\langle V \rangle \neq \langle 1 \rangle$. Then the nullstellensatz implies that the algebraic variety $V(\overline{\mathbb{F}}_q)$ is non-empty. From the equality $\overline{\mathbb{F}}_q = \bigcup_{r \in \mathbb{Z}_{\geq 0}} \mathbb{F}_{q^r}$, we obtain that the system has a solution over $\mathbb{F}_{q^r}$ for some r. Now note that the polynomial $x^p - x \in \mathbb{F}_{p^r}[x]$ has at most p roots in any algebraic extension of $\mathbb{F}_p$, and all the elements of $\mathbb{F}_p$ satisfy this equation. Therefore, from here we can look for Frobenius invariant points to find points over $\mathbb{F}_q$.

Goal. *Find $V(\mathbb{F}_{q^r})$ for some r, and then take fixed points under the Frobenius map $x \mapsto x^q$ to find points in $V(\mathbb{F}_q)$.*

We begin by seeking an understanding of $\#V(\mathbb{F}_{q^r})$ for some r. In fact, using generating functions, it turns out to be easier to study $\#V(\mathbb{F}_q)$ for all r simultaneously. With this in mind, Hasse and Weil introduce the Zeta function

$$Z(V,T) := \exp\left(\sum_{r \geq 1} \#V(\mathbb{F}_q^r)\frac{T^r}{r}\right).$$

(2) Topology of Algebraic Varieties. If $V(\mathbb{F}_q) \neq \emptyset$ for every q, then $V(\mathbb{C}) \neq \emptyset$, and in fact $V(\mathbb{C})$ is a complex analytic variety. Indeed, if V is smooth then $V(\mathbb{C})$ is a complex manifold, and we will write $d := \dim_{\mathbb{R}} V(\mathbb{C})$.

Poincaré, Alexandroff, Noether et al. defined homology groups $H_i(V(\mathbb{C}), \mathbb{Q})$, together with an intersection product

$$H_i(V(\mathbb{C}), \mathbb{Q}) \times H_{d-i}(V(\mathbb{C}), \mathbb{Q}) \to \mathbb{Q},$$

such that there is a vector space basis $\{e_{i,j}\}$ of $H_i(V(\mathbb{C}), \mathbb{Q})$ with

$$e_{i,a} \cdot e_{d-i,b} = \begin{cases} 1 & \text{if } a = b, \\ 0 & \text{else.} \end{cases}.$$

The ith Betti number is defined to be $b_i := \dim H_i(V(\mathbb{C}), \mathbb{Q})$.

Example 2. If $V = \mathbb{P}^n_{\mathbb{C}}$, then $b_i = \begin{cases} 1 & \text{if } i \leq d \text{ and is even,} \\ 0 & \text{else.} \end{cases}$

Example 3. If $V(\mathbb{C})$ is homeomorphic to a torus with g holes then

$$(b_0, b_1, b_2) = (1, 2g, 1).$$

Now consider a (continuous) map $F : V(\mathbb{C}) \to V(\mathbb{C})$. Then Lefshetz proved that the fixed points $L(F)$ under this map are (in an appropriate sense) counted by the formula

$$L(F) := \sum_{i=0}^{d} (-1)^i \left(\sum_{k \geq 0} F_*(e_{i,k}) \cdot e_{d-i,k} \right),$$

where F_* is the induced map on the homology groups. This formula can be understood as the number of intersection points, counted with the multiplicity of the diagonal, $\Delta = \{(x, x) : x \in V(\mathbb{C})\}$ and the graph of F, $\Gamma_F = \{(x, F(x)) : x \in V(\mathbb{C}))\}$. Note that, if F is the identity map then this formula returns the Euler characteristic $L(F) = \chi(V(\mathbb{C}))$, which can be understood as the self-intersection number of $V(\mathbb{C})$.

Weil then thinks: if only we had a nice topology and (co)homology theory on $V(\mathbb{F}_q)$, where we could use this Lefshetz fixed point theorem together with F being the Frobenius map.

II: Weil Conjectures

We now begin by stating the Weil conjectures.

Theorem 4 (Weil Conjectures). *Let $X/\mathbb{F}_q$ be a smooth projective variety of dimension n. Then the following properties hold.*

(1) (Rationality) $Z(X, T)$ is a rational function in T, and moreover

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

where $P_i \in \mathbb{Z}[T]$ with $P_i(T) = \prod_{j=1}^{b_i} 1 - a_{ij} T$, for some $b_i \in \mathbb{Z}_{\geq 0}$.

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

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

where $\chi = \sum_{i=0}^{2n} (-1)^i b_i$ is the Euler characteristic.

(3) (Reimann Hypothesis) The numbers $a_{i,j}$ are q-Weil numbers of weight i, meaning that

$$|a_{i,j}| = q^{i/2},$$

for all $0 \leq i \leq 2n$, $1 \leq j \leq b_i$.

Remark 5. If X is the reduction of a variety defined over a subfield $K \subseteq \mathbb{C}$ which is algebraic over $\mathbb{Q}$, then the b_i above are the Betti numbers over $\mathbb{C}$.

Example 6. (1) If $X = \mathbb{P}^n_{\mathbb{F}_q}$, then

$$\begin{aligned} Z(X,T) &= \exp\left(\sum_{r\geq 1} \frac{\#X(\mathbb{F}_{q^r})}{r} T^r\right) \\ &= \exp\left(\sum_{r\geq 1} \frac{q^{r(n+1)}-1}{q^r-1}\frac{T^r}{r}\right) \\ &= \exp\left(\sum_{i=1}^{n}\sum_{r\geq 1}\frac{T^r}{r}q^{ri}\right) \\ &= \exp\left(\sum_{i=1}^{n} -\log\left(1-q^iT\right)\right) \\ &= \prod_{i=1}^{n}\frac{1}{1-q^iT} \end{aligned}$$

(2) If $X = \mathbb{A}^n_{\mathbb{F}_q}$, then

$$Z(X,T) = \exp\left(\sum_{r\geq 1}\frac{q^{rn}}{r}T^r\right) = \frac{1}{1-q^n}$$

III: Applications

(1) It is clear from how things have been set up that these form a sort of Local–Global principle, relating cohomology of varieties over $\mathbb{C}$ to that over finite fields $\mathbb{F}_q$.
(2) The Lang–Weil theorem is an application of the Weil conjectures.

Theorem 7. *Given non-negative integers n, d, r, with $d > 0$, then there exists a constant $A = A(n,d,r) > 0$ such that for all finite fields k and all geometrically irreducible subvarieties $X \subseteq \mathbb{P}^n_k$ of dimension r and degree d, we have*

$$|\#X(k) - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + Aq^{r-1}.$$

(3) We can use this, together with Hensel's lemma, to deduce the existence of local points on varieties.

Lecture 2 (Eda): Weil Conjectures for Elliptic Curves

Recollections

Let $n \geq 1$ be an integer, q be a prime power, and consider $V \subseteq \mathbb{P}^n_{\mathbb{F}_q}$ a projective variety given by solutions to some polynomials $F_1(x_0,\dots,x_n),\dots,F_m(x_0,\dots,x_n)$ with coefficients in $\mathbb{F}_q$.

Definition 8. The Zeta function is

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

Note that $\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log(Z(V/\mathbb{F}_q,T))|_{T=0}$ can be recovered from this.

Theorem 9 (Weil Conjectures)**.** *Let $V/\mathbb{F}_q$ be a projective variety of dimension N, then the following hold.*

(1) (Rationality) $Z(V/\mathbb{F}_q, T) \in \mathbb{Q}(T)$;

(2) (Functional Equation) There is $\varepsilon \in \mathbb{Z}$, the Euler characteristic of V, satisfying

$$Z(V/\mathbb{F}_q, \frac{1}{q^N T}) = \pm q^{N\varepsilon/2} T^{\varepsilon} Z(V/\mathbb{F}_q, T).$$

(3) (Riemann Hypothesis) $Z(V/\mathbb{F}_q, T) = \frac{P_1(T)\dots P_{2N-1}(T)}{P_0(T)\dots P_{2N}(T)}$ for each $0 \leq i \leq 2n$, the polynomials P_i factor over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{i,j}T)$$

with $|\alpha_{i,j}| = \sqrt{q}^{\,i}$.

(4) (Betti Number) The b_i above are the Betti numbers.

Some Basics

Let K be a field. An elliptic curve is a pair $(E/K, \mathcal{O})$ of a (smooth, projective) genus 1 curve E/K and a base point $\mathcal{O} \in E$. Such curves have a natural group structure, and always have an affine model of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

An isogeny is a morphism (of algebraic varieties) $\phi : E_1 \to E_2$ satisfying $\phi(\mathcal{O}_1) = \mathcal{O}_2$. Such maps are, in fact, group homomorphisms, and the set of them $\mathrm{Hom}(E_1, E_2)$ is a torsion free $\mathbb{Z}$-module. Moreover, every isogeny is either the 0 map or surjective! If $E_1 = E_2$ then we write $\mathrm{End}(E) := \mathrm{Hom}(E, E)$.

If K is a finite field (or indeed, a field of characteristic $p > 0$), then we have the Frobenius endomorphisms given by

$$\pi : E \to E; \qquad (x, y) \mapsto (z^q, y^q).$$

We denote by $E[m]$ the m-torsion points on E, and recall that this group is well understood.

Theorem 10. *If $\mathrm{char}(K) \nmid m$ then, as abelian groups, we have an isomorphism*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

So the m-torsion is often a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2.

Definition 11. For a prime number ℓ, the ℓ-adic Tate module of E/K is defined to be

$$T_\ell E := \lim_{\leftarrow n} E[\ell^n],$$

with inverse limit taken over the natural maps given by multiplication by ℓ.

Immediately from the above, we have the following.

Proposition 12. *If $\ell \neq \mathrm{char}(K)$ then*

$$T_\ell E \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

The Weil Pairing

In order to prove the Weil conjectures, we will require the use of the Weil pairing, which is a very useful pairing on Tate modules of elliptic curves. Recall that the Abel-Jacobi map

$$E \to \mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{div}(\overline{K}(E))$$

given by $P \mapsto (P) - (\mathcal{O})$ is an isomorphism of groups. We shall make use of this fact in the construction of the Weil pairing below.

Definition 13 (Weil pairing)**.** Let E be an elliptic curve, and $m > 1$ be an integer. The Weil pairing is a map

$$e_m : E[m] \times E[m] \mapsto \mu_m.$$

For two points $P, Q \in E[m]$, the image $e_m(P, Q)$ is defined as follows.

Firstly, since multiplication by m is an isogeny and so surjective, there exists $Q' \in E$ such that $mQ' = Q$. Consider the divisor

$$[m]^*(Q) - [m]^*(\mathcal{O}) = \sum_{R \in E[m]} (Q' + R) - \sum_{R \in E[m]} (R)$$

On the elliptic curve this sum is equivalent to

$$\sum_{R \in E[m]} Q' = m^2 Q' = \mathcal{O},$$

and so there is $g \in \overline{K}(E)$ such that $\mathrm{div}(g) = \sum_{R \in E[m]} (Q' + R) - (R)$.

Secondly, since $mQ = \mathcal{O}$, there is a function $f \in \overline{K}(E)$ such that

$$\mathrm{div}(f) = m(Q) - m(\mathcal{O}).$$

Note that

$$\mathrm{div}(g^m) = m\mathrm{div}(g) = \sum_{R \in E[m]} m(Q' + R) - m(R) = \mathrm{div}(f \circ [m]).$$

Thus these functions must differ by a constant, which we scale to 1, so $f \circ [m] = g^m$.

In summary: from $Q \in E[m]$, we have constructed functions $f, g \in \overline{K}(E)$ with

$$\begin{aligned} \mathrm{div}(f) &= m(Q) - m(\mathcal{O}); \\ \mathrm{div}(g) &= \sum_{R \in E[m]} (Q' + R) - (R). \end{aligned}$$

and $f \circ [m] = g^m$.

Now to define the Weil pairing: for every $X \in E$, since $P \in E[m]$

$$g(X + P)^m = f(mX + mP) = f(mX) = g^m(X).$$

In particular, choosing X such that $g(X) \neq 0, \infty$, $\frac{g(X+P)}{g(X)}$ is an mth root of unity! The set of such roots of unity will be denoted μ_m. Using this we now define the

Weil pairing

$$\begin{aligned} e_m : E[m] \times E[m] &\mapsto \mu_m \\ (P, Q) &\mapsto \frac{g(P+X)}{g(X)}. \end{aligned}$$

Remark 14. One can check that this pairing is independent of the choice of X, and that for $n \mid m$, the pairings e_n, e_m are compatible via multiplication by m/n.

Definition 15 (ℓ-adic Weil pairing)**.** If $\ell \neq \mathrm{char}(K)$ is a prime, then the ℓ-adic pairing is a pairing induced by the compatible system of Weil pairings e_{ℓ^n} above

$$e : T_\ell E \times T_\ell E \to T_\ell \mu,$$

were $T_\ell \mu$ is the ℓ-adic Tate module of $\overline{K}^\times$ (inverse limit of μ_{ℓ^d} over d and with usual multiplication maps).

Lemma 16. *The Weil pairing has several properties. It is*

- *bilinear,*
- *alternating,*
- *non-degenereate, and*
- *Galois-equivariant.*

In addition, dual isogenies are adjoint with respect to the Weil pairing.

The Characteristic Polynomial of Frobenius

Lemma 17. *Let $\phi \in \mathrm{End}(E)$, then there is a map $\phi : T_\ell E \to T_\ell E$ induced on the Tate module. We choose a $\mathbb{Z}_\ell$-basis $\{P, Q\}$ for $T_\ell E$, and write*

$$\phi(P) = [a]P + [b]Q, \qquad \phi(Q) = [c]P + [d]Q,$$

so that we can represent ϕ by the matrix $\phi_\ell := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Then $\det(\phi_\ell) = \deg(\phi)$*, and* $\mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi)$.

Remark 18. We often write $\det(\phi)$ and $\mathrm{tr}(\phi)$ for these quantities, since it is implicit in this lemma that they are independent of ℓ.

Proof. Using properties of the ℓ-adic Weil pairing stated above in Lemma 16, and writing $\widehat{\phi}$ for the dual isogeny to ϕ (so $\widehat{\phi}\phi = [\deg(\phi)]$)

$$\begin{aligned} e(P, Q)^{\deg(\phi)} &= e([\deg(\phi)]P, Q) \\ &= e(\widehat{\phi}\phi(P), Q) \\ &= e(\phi(P), \phi(Q)) \\ &= e([a]P + [b]Q, [c]P + [d]Q) \\ &= e(P, Q)^{ad-bc} \\ &= e(P, Q)^{\det(\phi_\ell)}. \end{aligned}$$

Since the Weil pairing is surjective onto $T_\ell \mu$, this shows the first claim. For the trace, we directly compute

$$\begin{aligned}1 + \deg(\phi) - \deg(1-\phi) &= 1 + \det(\phi_\ell) - \deg(1-\phi_\ell)\\ &= 1 + ad - bc - (1-a)(1-d) + bc\\ &= a + d\\ &= \mathrm{tr}(\phi_\ell)\end{aligned}$$

□

Proposition 19. *Let $E/\mathbb{F}_q$ be an elliptic curve and $\pi : E \to E$ be the qth power frobenius. Let $a = q + 1 - \#E(\mathbb{F}_q)$. Then the characteristic polynomial for the action of π_ℓ on $T_\ell E$ is given by*

$$C(T) = T^2 - aT + q,$$

and moreover if $\alpha, \beta \in \mathbb{C}$ are the roots of $C(T)$ then α and β are a complex conjugate pair such that $|\alpha| = |\beta| = q^{1/2}$, and for every $n \geq 1$

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

Proof. For $P \in E(\overline{\mathbb{F}_q})$, $P \in E(\mathbb{F}_q)$ if and only if $\pi(P) = P$. In particular, $E(\mathbb{F}_q) = \ker(1-\pi)$ and $1 - \pi$ is a seperable morphism. Thus

$$\#E(\mathbb{F}_q) = \#\ker(1-\pi) = \deg(1-\pi),$$

and $\det(\pi_\ell) = \deg(\pi) = q$, and so by Lemma 17

$$\mathrm{tr}(\pi) = 1 + \deg(\pi) - \deg(1-\pi) = 1 + q - \#E(\mathbb{F}_q) = a.$$

Thus $C(T)$ is the characteristic polynomial for the action of π on the ℓ-adic Tate module, and α, β are the eigenvalues of this action. Note that for every pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0}$ it follows from Lemma 17

$$C(m/n) = \det(m/n - \pi_\ell) = \frac{\det(m - n\pi_\ell)}{n^2} = \frac{\deg([m] - n\pi)}{n^2} \geq 0.$$

In particular, C is a quadratic polynomial taking no negative values on $\mathbb{Q}$ (equivalently on $\mathbb{R}$), and so must have either no roots in $\mathbb{R}$ or a double root in $\mathbb{R}$. In particular, the claim that α, β are complex conjugates holds. Moreover, since $\alpha\beta = q$, we must have $|\alpha| = |\beta| = \sqrt{q}$.

Now to produce the point counting formula we again note (now replacing q with q^n), that the characteristic polynomial of π_ℓ^n is

$$\det(T - \pi_\ell^n) = T^2 - \mathrm{tr}(\pi_\ell^n)T + \det(\pi_\ell^n).$$

In particular, by classical linear algebra, the eigenvalues of π_ℓ^n are α^n, β^n and so

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \pi^n) = \det(1 - \pi_\ell^n) = 1 - (\alpha^n + \beta^n) + q^n,$$

as required. □

The Weil Conjectures

We are now ready to give the proof of the Weil conjectures for elliptic curves.

Theorem 20 (Weil Conjectures for Elliptic Curves)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve, then the following statements are true.*

(i) (Rationality) $Z(E/\mathbb{F}_q, T) \in \mathbb{Q}(T)$.

(ii) (Functional Equation) The Euler characteristic of a smooth lift of E to $\mathbb{C}$ is $\varepsilon = 0$, and

$$Z(E/\mathbb{F}_q, \frac{1}{qT}) = \pm Z(E/\mathbb{F}_q, T).$$

(iii) (Riemann Hypothesis) $Z(E/\mathbb{F}_q, T) = \frac{P_1(T)}{P_0(T)P_2(T)}$, and the polynomials P_i factor over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{i,j} T)$$

with $|\alpha_{i,j}| = \sqrt{q}^{\,i}$.

(iv) (Betti Number) The b_i above are the Betti numbers, given by

$$(b_0, b_1, b_2) = (1, 2, 1).$$

Proof. We will make extensive use of Proposition 19 in proving this. Directly computing, with α, β the eigenvalues of Frobenius acting on the ℓ-adic Tate module:

$$\begin{aligned} Z(E/\mathbb{F}_q, T) &= \exp\left(\sum_{r \geq 1} \#E(\mathbb{F}_{q^r}) \frac{T^r}{r} \right) \\ &= \exp\left(\sum_{r \geq 1} (1 + q^r - \alpha^r - \beta^r) \frac{T^r}{r} \right) \\ &= \exp\left(-\log(1-T) - \log(1-qT) + \log(1-\alpha T) + \log(1 - \beta T) \right) \\ &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}, \end{aligned}$$

in particular, writing $a(E) = q + 1 - \#E(\mathbb{F}_q) \in \mathbb{Z}$, it follows from Proposition 19 that

$$Z(E/\mathbb{F}_q, T) = \frac{1 - a(E)T + qT^2}{(1-T)(1-qT)}. \tag{1}$$

We now verify each claim.

(i) Immediate from (1).

(ii) We note that the Betti numbers of a complex torus are

$$(b_0, b_1, b_2) = (1, 2, 1),$$

which is an elementary computation in algebraic topology. From this we see that the Euler characteristic $\varepsilon = 0$, and that we must prove $Z(E/\mathbb{F}_q, T) = Z(E/\mathbb{F}_1, 1/qT)$. This is also clear from (1) since

$$Z\left(E/\mathbb{F}_q, \frac{1}{qT}\right) = \frac{1 - \frac{a(E)}{qT} + \frac{q}{q^2T^2}}{\left(1 - \frac{1}{qT}\right)\left(1 - \frac{q}{qT}\right)} = \frac{qT^2 - a(E)T + 1}{(qT-1)(T-1)} = Z(E/\mathbb{F}_q, T).$$

(iii) Follows from (1): the claim for the numerator, $P_1(T) = (1 - \alpha T)(1 - \beta T)$ follows from Proposition 19, and for P_0, P_2 this is apparent.
(iv) We have already computed the Betti numbers above, and the degrees of P_i clearly match up appropriately.

□

Lecture 3 (Gergely): Proving the Weil Conjectures (Assuming Cohomology Exists!)

In the first talk we defined the Zeta function of a variety over a finite field

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

and stated the Weil conjectures. Today we will focus on rationality, as the others are more involved. The statement is as follows.

Theorem 21. *For every smooth, complete variety over a finite field $\mathbb{F}_q$, then $Z(X/\mathbb{F}_q, T) \in \mathbb{Q}(T)$*

For a field K of characteristic 0, a cohomology theory is a contravariant functor

$$\left\{\substack{\text{nice varieties} \\ \text{over } k}\right\} \xrightarrow{H^*} \left\{\text{Graded } K\text{-algebras}\right\}.$$

where we decompose $H^*(X) = \bigoplus_{i \in \mathbb{Z}} H^i(X)$, with $h_i \cdot h_j \in H^{i+j}(X)$. Moreover, since this is a functor, maps of varieties go to maps of K-algebras. The Weil axioms are then the following.

Definition 22. H^* satisfies the Weil axioms if for every variety X of dimension d

(1) $H^i(X)$ is finite dimensional over K.
(2) If $i < 0$ or $i > 2d$ then $H^i(X) = 0$.
(3) $H^{2d}(X) \cong K$.
(4) (Poincaré Duality) there is a perfect pairing

$$H^i(X) \times H^{2d-i}(X) \to H^{2d}(X) \cong K.$$

(5) (Künneth isomorphism)

$$H^*(X) \otimes_K H^*(Y) \cong H^*(X \times Y).$$

(6) (Lefschetz trace formula) We will not define this yet.

Theorem 23. *There exists a cohomology theory $H^*_{ét}$ which satisfies the Weil axioms when k is algebraically closed and $K = \mathbb{Q}_\ell$ for some prime ℓ such that $\ell \nmid \mathrm{char}(k)$.*

Definition 24. We now state the Lefschetz trace formula. For a morphism of varieties $\phi : X \to X$, we define:

- $\Gamma_\phi \subseteq X \times X$ to be the graph of the morphism.
- $\Delta := \{(x, x)\} \subseteq X \times X$ to be the diagonal.

Then the Lefschetz formula is

$$(\Gamma_\phi \cdot \Delta) = \sum_{i=0}^{2 \dim X} (-1)^i \mathrm{tr}\left(\phi_r | H^r_{\text{ét}}(X; \mathbb{Q}_\ell)\right),$$

where the left hand side is the intersection pairing.

Lemma 25. *Assume that for all $P \in X$, both* $\det(\mathrm{Id} - \partial_P \phi) \neq 0$ *and* $(\Gamma_\phi \cdot \Delta)_P = 1$. *Then*

$$(\Gamma_\phi \cdot \Delta) = \#\Gamma_\phi \cap \Delta$$

Note that this will allow us to count fixed points under ϕ! Consider the qth power Frobenius automorphism F, and its action on $X(\overline{\mathbb{F}_q})$ for a variety $X/\mathbb{F}_q$.

Theorem 26 (Rationality, version 2)**.** $Z(X/\mathbb{F}_q, T) = \frac{P_0(T)...P2d-1(T)}{P_1(T)...P_{2d}(T)}$, *where*

$$P_r(T) = \det\left(1 - FT | H^r_{\acute{e}t}(X, \mathbb{Q}_\ell)\right).$$

Note that this almost implies rationality – it proves that $Z(X/\mathbb{F}_q, T) \in \mathbb{Q}_\ell(T)$.

Proof. **Claim 1** F^n is nondegenerate and $\det(\mathrm{Id} - \partial_P F^n) \neq 0$ for all $P \in X$.

Claim 2 $\#X(\mathbb{F}_{q^n})$ is the set of fixed points under F^n.

These two claims, together with the Lefschetz trace formula, show that

$$\#X(\mathbb{F}_{q^n}) = \sum_{r=0}^{2d} (-1)^r \mathrm{tr}\left(F^n | H^r_{\text{ét}}(X, \mathbb{Q}_\ell)\right).$$

We then compute

$$\begin{aligned} Z(X/\mathbb{F}_q, T) &= \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \sum_{r=0}^{2d} (-1)^r \mathrm{tr}\left(F^n | H^r_{\text{ét}}(X, \mathbb{Q}_\ell)\right) \frac{T^n}{n}\right) \\ &= \prod_{r=0}^{2d} \exp\left(\sum_{n=1}^{\infty} \mathrm{tr}\left(F^n | H^r_{\text{ét}}(X, \mathbb{Q}_\ell)\right) \frac{T^n}{n}\right)^{(-1)^r}. \end{aligned}$$

We then use the following claims

Claim 3 For any linear map of vector spaces ϕ,

$$\log\left(\frac{1}{\det(1 - \phi T)}\right) = \sum_{n \geq 1} \mathrm{tr}(\phi^m) \frac{T^m}{m}$$

Claim 4 If $\det(1 - \phi T) = \prod_i (1 - c_i T)$ then $\mathrm{tr}(\phi^m) = \sum_i c_i^m$.

Using these we obtain

$$\begin{aligned} &\prod_{r=0}^{2d} \exp\left(\sum_{n=1}^{\infty} \mathrm{tr}\left(F^n | H^r_{\text{ét}}(X, \mathbb{Q}_\ell)\right) \frac{T^n}{n}\right)^{(-1)^r} \\ &= \prod_{r=0}^{2d} \exp\left(\log\left(\frac{1}{\det(1 - FT)}\right)\right)^{(-1)^r} \\ &= \prod_{r=0}^{2d} \det(1 - FT)^{(-1)^{r+1}}. \end{aligned}$$

as required. □

It now remains to show that our Zeta function is in fact in $\mathbb{Q}(T)$. This follows from the lemma below.

Lemma 27. *If K is a subfield of L, and $f \in K[[T]] \cap L(T)$ then $f \in K(T)$.*

Proof. Write $f = \sum_{i \geq 0} a_i T$ for some $a_i \in K$. Then it is a rational function if and only if there exists $\lambda_1, \ldots, \lambda_r$ and D such that for all $n \geq D$ $\sum_i \lambda_i a_{n+i-1} = 0$. Which shows rationality. □

Lecture 4 (Besfort): Étale Cohomology I

Recap and Motivation

So far we have shown (or rather plausibly sketched the proofs of) the Weil conjectures for elliptic curves, as well as the Weil conjectures in some more generality assuming the existence of a suitable cohomology theory. To come up with a cohomology theory in the case of elliptic curves, say, one might be tempted to regard a fixed elliptic curve E as a variety over $\overline{\mathbb{F}}_p$ with the Zariski topology (with the defining property that zero sets of polynomials are closed) and work with singular cohomology with $\mathbb{Z}$-coefficients. Unfortunately, this turns out not to work, for we will sketch a proof that $H^r(X; \mathbb{Z}) = 0$ for $r > 0$ if X is an irreducible variety (in fact we will sketch the proof of a slightly stronger statement).

Before we get onto this, let us take a brief detour and say something about the assumption $l \nmid \operatorname{char} k$ in the theorem assuring the existence of a suitable cohomology theory from the previous lecture.

Lemma 28 (Serre). *There cannot exist a cohomology theory with coefficients in $\mathbb{R}$ (satisfying the Weil axioms from the previous lecture) which associates graded $\mathbb{R}$-vector spaces to "nice" varieties over an algebraically closed field k of characteristic $p > 0$, with the property that $H^1 E \cong \mathbb{R}^2$ for all elliptic curves E.*

Proof sketch. Let E be a *supersingular* elliptic curve (for our purposes, this means that $\operatorname{End}_k E \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{H}$, where $\mathbb{H}$ is the division algebra of quaternions – this is equivalent to E having no non-trivial p-torsion points). Then $\operatorname{End}_k E$ acts on E so if a cohomology theory satisfying the conditions stated in the lemma were to exist, we would get a $\operatorname{End}_k E$-module structure on $H^1 E$. Extending the scalars by tensoring with $\mathbb{R}$, we get a $\mathbb{H}$-module structure on $H^1 E \cong \mathbb{R}^2$, which is impossible since $\mathbb{H}$ has real dimension 4. □

The same proof goes through if we replace $\mathbb{R}$ with $\mathbb{Q}$ or $\mathbb{Q}_p$ for $p = \operatorname{char} k$, whereas for $\mathbb{Q}_\ell$ with $\ell \neq p$, we no longer get the division algebra of quaternions.

Sheaf Cohomology

In the 19th and 20th centuries, there were a number of existing cohomology theories of topological spaces. They were eventually unified by Eilenberg and Steenrod in 1953, who showed that for a suitable category of pairs of topological spaces, there exists a unique cohomology theory satisfying a list of natural axioms. Perhaps one downside of this theory is that the underlying coefficient group is essentially fixed. This is where *sheaf cohomology* enters the picture, where rather than unifying cohomology theory of varying topological spaces, the goal now is to systematically track algebraic data that is (locally) associated to a fixed topological space X.

More precisely, consider the category $\mathrm{O}X$ of open subsets of a fixed topological space X, with morphisms given by inclusions $U \hookrightarrow V$. A *presheaf* is simply a local assignment of algebraic data respecting restriction, that is, a contravariant functor $\mathcal{F} : \mathrm{O}X \to \mathrm{Ab}$, where Ab is the category of abelian groups. Elements of $\mathcal{F}U$ for U

open in X are called *sections* of $\mathcal{F}$ over U. For $U \hookrightarrow V$, we denote the image of a section s in $\mathcal{F}V$ under the map $\mathcal{F}V \to \mathcal{F}U$ by $s|_U$. A *sheaf* is then a presheaf where global sections are determined by local sections and such that there is local consistency. More precisely:

Definition 29. Let X be a topological space. A *sheaf* over X is a presheaf $\mathcal{F} : \mathrm{O}X \to \mathrm{Ab}$ such that for every U open in X and every open cover $\{U_i\}_{i\in I}$ of U, the sequence

$$0 \to \mathcal{F}U \to \prod_{i\in I} \mathcal{F}U_i \to \prod_{i,j\in I} \mathcal{F}(U_i \cap U_j)$$

is exact, where the first (non-trivial) map is the natural one, whereas the second is the map $(f_i)_{i\in I} \mapsto (f_i|_{U_i\cap U_j} - f_j|_{U_i\cap U_j})_{i,j}$.

Example 30. One natural example of a sheaf on a topological space X is the assignment of continuous maps $U \to \mathbb{C}$ to each open subset U of X. Here for $U \hookrightarrow V$ and s a section over V (i.e. a continuous map $V \to \mathbb{C}$), $s|_U$ is genuinely the restriction of the map s to U.

Example 31. Let G be an abelian group with the discrete topology. As above, for a topological space X and any open subset U of X, let $\mathcal{F}U$ be the set of continuous maps $U \to G$. These must be locally constant and as such they factor through the space $\pi_0 U$ of connected components of U. Therefore $\mathcal{F}U$ may be identified with $G^{\pi_0 U}$. This sheaf is called the *constant* sheaf defined by G. This will allow us to recover singular cohomology with G-coefficients.

It turns out (a theorem proven by Grothendieck) that the category of sheaves on X with the natural morphisms is an *abelian* category. We shall not define what an abelian category is precisely, but for our purposes it suffices to say that the notions of injective and surjective morphisms are particularly well behaved and not too different from the usual notions. In this regard, we have (we will call the following a definition but perhaps more correctly it should be called a lemma):

Definition 32. Let $\mathcal{B}$ and $\mathcal{C}$ be sheaves over a topological space X.

A morphism $\mathcal{B} \to \mathcal{C}$ is *injective* if for any U open in X, the homomorphism $\mathcal{B}U \to \mathcal{C}U$ is injective.

A morphism $m : \mathcal{B} \to \mathcal{C}$ is *surjective* if for any U open in X, any $s \in \mathcal{C}U$ and any $x \in U$, there exists an open $x \in V \subseteq U$ such that $s|_V = m(s')$ for some $s' \in \mathcal{B}V$.

Note the subtlety in the definition of *surjective* – we only require that sections of $\mathcal{C}$ lift *locally* to a section of $\mathcal{B}$. But now a very natural question arises: given a surjective morphism $\mathcal{B} \to \mathcal{C}$, do *all* sections of $\mathcal{C}$ arise from sections of $\mathcal{B}$ (globally)? If not, to what extent does this fail? This is a very general model encapsulating many local versus global questions in geometry and number theory, and sheaf cohomology provides an answer to this.

Note that a surjective morphism $\mathcal{B} \to \mathcal{C}$ gives rise to (or may be equivalently rewritten as) a short exact sequence of sheaves

$$0 \to \mathcal{A} \to \mathcal{B} \to \mathcal{C} \to 0,$$

where $\mathcal{A}$ is the kernel of the morphism $\mathcal{B} \to \mathcal{C}$. If everything is right with the world, this “should” induce a long exact sequence of cohomology groups and we need to figure out how. A reasonable start is to move to the category of abelian groups via the functor $\mathcal{F} \mapsto \mathcal{F}X \in \mathrm{Ab}$. However, while this functor is left-exact (i.e. $0 \to \mathcal{A}X \to \mathcal{B}X \to \mathcal{C}X$ is exact), it is not right-exact (i.e. we cannot add a 0 at the end of the sequence just written). We would like to continue the exact sequence of abelian groups and a method in category theory that is built to do this is through *right derived functors.* In order to work, this requires the existence of "enough injectives" in the category of sheaves, another fact proven by Grothendieck. This allows us, for any starting sheaf $\mathcal{F}$, to construct an *injective resolution*, that is, an exact sequence

$$0 \to \mathcal{F} \to \mathcal{I}^0 \to \mathcal{I}^1 \mapsto \mathcal{I}^2 \mapsto \cdots ,$$

where each $\mathcal{I}^r$ is injective (i.e. any morphism $\mathcal{A} \to \mathcal{I}^r$ extends to a morphism $\mathcal{B} \to \mathcal{I}^r$ for any sheaf $\mathcal{B}$ containing $\mathcal{A}$ – the key point here is obtaining a resolution, but we want the cohomology groups defined below to be independent of the resolution and this is where injectivity comes in). Passing to the category of abelian groups, we obtain a chain complex of abelian groups, namely

$$0 \to \mathcal{I}^0 X \to \mathcal{I}^1 X \to \mathcal{I}^2 X \to \cdots .$$

Finally, we define

$$H^r(X;\mathcal{F}) = \ker(\mathcal{I}^r X \to \mathcal{I}^{r+1} X)/\operatorname{im}(\mathcal{I}^{r-1} X \to \mathcal{I}^r X).$$

With this definition, we get the induced long exact sequence

$$0 \to H^0(X;\mathcal{A}) \to H^0(X;\mathcal{B}) \to H^0(X;\mathcal{C}) \to H^1(X;\mathcal{A}) \to \cdots ,$$

as desired.

Before we go back to varieties, we need one more definition.

Definition 33. A sheaf $\mathcal{F}$ over a topological space X is called *flabby* if the morphisms $\mathcal{F}V \to \mathcal{F}U$ are surjective for any $U \subseteq V$.

A key lemma that we will use without proof is the following (although this should not come as a surprise – the definition of flabby is in some sense a lifting of local sections to global ones, so the cohomology groups "should" vanish).

Lemma 34. *If $\mathcal{F}$ is a flabby sheaf over a topological space X, then $H^r(X;\mathcal{F}) = 0$ for $r > 0$.*

The Inadequacy of Zariski Topology

After all this work, we show that equipping an irreducible variety X with the Zariski topology (irreducible means that no two non-empty open sets are disjoint) actually produces trivial cohomology groups with respect to constant sheaves.

Theorem 35 (Grothendieck)**.** *If X is an irreducible topological space, then the cohomology groups $H^r(X;\mathcal{F})$ vanish for $r > 0$ if $\mathcal{F}$ is a constant sheaf defined by a discrete group G.*

Proof. We apply Lemma 34. Let U be a non-empty open subset in X. Since X is irreducible, we have that U is connected, i.e. $\pi_0 U$ is trivial. As such, by Example 31 we have $\mathcal{F}U = G$ for every non-empty U in X. This obviously implies that $\mathcal{F}$ is flabby, thus the conclusion follows by Lemma 34. □

Étale Covers

Now that we have proved Theorem 35, it remains to discuss what modifications need to be made to define a suitable cohomology theory. We begin with the following definition.

Definition 36. Let X and Y be nonsingular algebraic varieties over an algebraically closed field k. A regular (i.e. locally represented by polynomials) map $\varphi : X \to Y$ is said to be *étale at* x if $\mathrm{d}\varphi : T_xX \to T_{\varphi x}Y$ is an isomorphism. We call φ *étale* if it is étale at x for every $x \in X$.

Note that in analogy with differential geometry, étale maps are supposed to capture "local sameness" (but this analogy fails when X and Y are equipped with the Zariski topology). It turns out, that upon replacing the notion of topology with a more general framework, namely replacing open sets and inclusions by étale maps $U \to X$, one obtains a suitable cohomology theory. To define sheaves similarly as before, we need a notion of covering – this will simply be a family of étale maps $(\varphi_i : U_i \to U)_{i\in I}$ such that $U = \bigcup_{i\in I} \varphi_i(U_i)$. Now consider the category

$$X_{\text{ét}}$$

consisting of étale maps $U \to X$ and morphisms $(U \to X) \to (V \to X)$ given by a map $U \to V$ such that

$$(U \to V \to X) \equiv (U \to X)\,.$$

(It is a simple exercise to show that the map $U \to V$ is automatically étale.) One then defines presheaves, sheaves and the cohomology groups $H^r_{\text{ét}}(X; \mathcal{F})$ in much the same way as before.

In comparison with the complex topology on $X(\mathbb{C})$ for a complex nonsingular algebraic variety X, one can show that for every finite abelian group G, we have $H^r_{\text{ét}}(X; G) \cong H^r(X(\mathbb{C}); G)$. We may extend this to $H^r_{\text{ét}}(X; \mathbb{Q}_l) \cong H^r(X(\mathbb{C}); \mathbb{Q}_\ell)$ for any prime ℓ by taking $G = \mathbb{Z}/\ell^n\mathbb{Z}$, passing to the inverse limit over n and then tensoring with $\mathbb{Q}_\ell$ (viewed as a $\mathbb{Z}_\ell$-module).

Lecture 5 (Ross): Étale Cohomology II

We recall sheaf cohomology briefly below, since today and next week will be concerned with a generalisation of this. We begin with a topological space X.

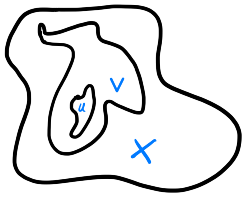
Categorification. We begin with the following category.

Name:	OX
Objects:	open sets $U \subseteq X$
Morphisms:	inclusions of open sets.

For example, a diagram in $\mathrm{O}X$ may look like:

$$\begin{tikzcd}
V \arrow[r, hook] & X \\
U \arrow[u, hook] \arrow[ur, hook] &
\end{tikzcd}$$

$=$



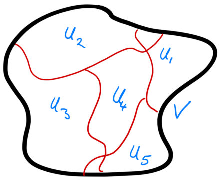
A *presheaf* on OX is a contravariant functor $\mathcal{F} : \mathrm{O}X \to \mathrm{Ab}$. If U is an open set, then we think of elements of $\mathcal{F}(U)$ as functions on U. The contravariance of $\mathcal{F}$ simply reverses the direction of morphisms. This is to mimic the idea that the inclusion $U \subseteq V$ corresponds to a "restriction" of a function

$$\mathcal{F}(V) \ni f \mapsto f|_U \in \mathcal{F}(U).$$

Sheaf. A presheaf is a sheaf if for every open covering $V = \bigcup_i U_i$ in OX the natural equaliser diagram below is exact:

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{F}(V) \arrow[r] & \prod_i \mathcal{F}(U_i) \arrow[r, shift left] \arrow[r, shift right] & \prod_{i,j} \mathcal{F}(U_i \cap U_j) \end{tikzcd} .$$

The conditions of exactness are interpreted below as though the elements are functions on the space for intuition.



• Exactness at $\mathcal{F}(V)$: If $f \in \mathcal{F}(V)$ is zero when restricted to every U_i, then since these cover V it is zero on V.
• Exactness at $\prod_i \mathcal{F}(U_i)$: If $(f_i)_i$ is a collection of functions which agree wherever their domains overlap (i.e. $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$), then can assemble a well defined function $f \in \mathcal{F}(V)$ such that $f|_{U_i} = f_i$ for every i.

Cohomology. Given X and a sheaf $\mathcal{F}$ as above, we build the cohomology groups $H^n(X, \mathcal{F})$ as follows. Take an injective resolution of sheaves:

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I}^{(0)} \longrightarrow \mathcal{I}^{(1)} \longrightarrow \mathcal{I}^{(2)} \longrightarrow \mathcal{I}^{(3)} \longrightarrow \dots \qquad \text{(Exact sequence of sheaves)}$$

We then evaluate this sequence at X and delete $\mathcal{F}$, to produce the complex

$$0 \longrightarrow \mathcal{I}^{(0)} \longrightarrow \mathcal{I}^{(1)}(X) \longrightarrow \mathcal{I}^{(2)}(X) \longrightarrow \mathcal{I}^{(3)}(X) \longrightarrow \dots \qquad \text{(complex of abelian groups)}$$

The nth sheaf cohomology group is then the nth homology of this sequence, i.e.

$$H^n(X; \mathcal{F}) := \frac{\ker\left(\mathcal{I}^{(n)}(X) \to \mathcal{I}^{(n+1)}(X)\right)}{\operatorname{im}\left(\mathcal{I}^{(n-1)}(X) \to \mathcal{I}^{(n)}(X)\right)}.$$

Problem. $H^n(X; \mathcal{F}) = 0$ for $n > 0$ when X is irreducible and $\mathcal{F}$ is flabby.

Today. We replace OX with a different category where this does not happen.

Étale Maps

We begin by introducing the notion of étaleness.

Definition 37. Define the following.

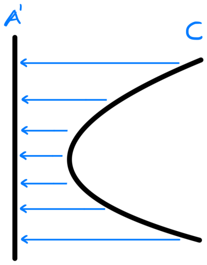
- A morphism $f : A \to B$ of rings is Étale if it is given by
$$A \to B = \frac{A[x_1, \dots, x_n]}{\langle f_1, \dots, f_n \rangle},$$
where $\det\left(\frac{\partial f_i}{\partial x_j}\right) \in B^\times$.
- A map of varieties (or schemes) $f : X \to Y$ is étale at $x \in X$ if it is locally given by an étale ring map. That is, if there exist open affine patches $x \in U \subseteq X$ and $V \subseteq Y$ with $f(U) \subseteq V$ and such that the induced map on rings of regular functions $k[V] \to k[U]$ is étale.
- We say that a map of varieties (or schemes) $X \to Y$ is étale if it is étale at every point $x \in X$

Example 38.
Let $C = \{y^2 = x\} \subseteq \mathbb{A}^2$ be the parabola. Consider the projection map onto the y-axis:

$$f : C \to \mathbb{A}^1, \qquad (x, y) \mapsto y.$$

The rings of regular functions, and corresponding map, are given by the natural inclusion

$$f^* : k[y] \to k[C] = \frac{k[y][x]}{\langle x - y^2 \rangle}.$$



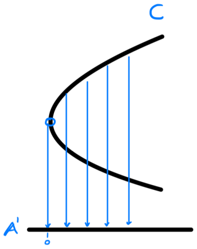
We now compute $\frac{\partial}{\partial x}(x - y^2) = 1 \in k[C]^\times$, and so this projection is étale.

Nonexample 39.
Continuing with the parabola $C = \{y^2 = x\} \subseteq \mathbb{A}^2$, consider the projection map onto the x-axis:

$$f : C \to \mathbb{A}^1, \qquad (x, y) \mapsto x.$$

Geometrically this looks different to the projection onto y – locally near the turning point at $(0, 0)$ there is a sharp turn. The rings of regular functions and corresponding map are given by the natural inclusion

$$f^* : k[x] \to k[C] = \frac{k[x][y]}{\langle y^2 - x \rangle}.$$



We now compute $\frac{\partial}{\partial y}(y^2 - x) = 2y \notin k[C]^\times$. Let us assume that we are not in characteristic 2, so that this is not simply 0. In every affine open containing $(0, 0)$, the function y is not invertible, and so the map cannot be invertible at $(0, 0)$ and so is *not* étale. On $C \backslash \{(0, 0)\}$ (where the ring of regular functions is $k[C][\frac{1}{y}]$), we have $2y \in k[C]^\times$ and so the map is étale on $C \backslash \{(0, 0)\}$.

There are some equivalent definitions of étaleness, which may be more or less illuminating for you depending on your background. These may give you alternative ways to verify or think of the concept of étaleness.

Proposition 40. *The following are equivalent for a morphism $f : X \to Y$ of varieties (or schemes)*

(i) f is étale
(ii) f is flat and unramified
(iii) f is smooth and unramified

Denote the local ring at $x \in X$ by $\mathcal{O}_{X,x}$ (and similarly for $f(x) \in Y$), and recall that $f : X \to Y$ induces a map of rings $f^* : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$. Then, at x, f is:

- *unramified* if all of the following hold.
  - f^* is of finite type.
  - f^* takes the maximal ideal to the maximal ideal, i.e.

$$f^*(\mathfrak{m}_{f(x)}) \cdot \mathcal{O}_{X,x} = \mathfrak{m}_x$$

  - f^* induces a finite separable extension of the residue fields, i.e. the induced field extension below is finite and separable:

$$\frac{\mathcal{O}_{X,x}}{\mathfrak{m}_x} \Big/ \frac{\mathcal{O}_{Y,f(x)}}{\mathfrak{m}_{f(x)}}.$$

- *flat* if the functor $- \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{O}_{X,x}$ induced by f^* is exact.
- *smooth* (of relative dimension r) if it can be presented as

  $$A \mapsto B = \frac{A[x_1, \dots, x_n]}{\langle f_1, \dots, f_{n-r} \rangle}$$

  with rank $\left(\frac{\partial f_i}{\partial x_j} \right)_{i,j} = r$.

Remark 41. Note that étaleness is being smooth with relative dimension 0.

Example 42. A field extension L/K (i.e. $\mathrm{Spec}(L) \to \mathrm{Spec}(K)$) is étale if and only if it is finite and separable. In general, a K-algebra A is étale if and only if it is a finite product of finite separable field extensions. That is,

$$A \cong \prod_{i=1}^{r} L_i$$

for some $r \geq 1$ with each L_i/K being a finite separable field extension. One can see this, for example, using Proposition 40(iii).

Example 43. Let L/K be a finite extension of number fields, and consider the inclusion of rings of integers $\mathcal{O}_K \to \mathcal{O}_L$. This is étale if and only if it is everywhere unramified. One can see this by Proposition 40(ii). Indeed, one only needs to check flatness: if S is a finite set of primes which cover the class group of K then $\mathcal{O}_{L,S}$ is free over $\mathcal{O}_{K,S}$, and so we are locally flat at every prime $\mathfrak{p} \notin S$. Choosing a second such S which is disjoint from the first we obtain flatness at the remaining primes.

Example 44. Let $f : E \to E'$ be a (nonzero) isogeny of elliptic curves, then f is étale if and only if it is separable. One can see this via Proposition 40(iii).

We conclude our discussion of étale maps with some properties of them.

Proposition 45. *The following properties hold.*

(i) Base change preserves étaleness.

(ii) Given a commutative triangle of morphisms

$$\begin{tikzcd} X \arrow[d, "f"'] \arrow[dr, "g"] & \\ Y \arrow[r, "h"'] & Z \end{tikzcd},$$

then

- *f, g étale $\implies$ h étale.*
- *g, h étale $\implies$ f étale.*

(iii) if $f : X \to Y$ is étale, then $f(X) \subseteq Y$ is open.

Étale Sheaves

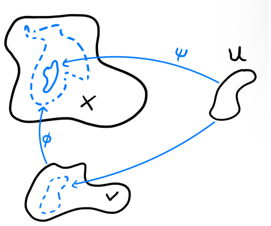
Let X be a variety (or scheme). We will mirror the sheaf cohomology summary.

Categorification. We replace OX with the following category.

Name:	$X_{\text{ét}}$
Objects:	étale X-schemes (schemes equipped with an étale map to X)
Morphisms:	morphisms of X-schemes (maps $U \to V$ which commute with the structural étale maps to X)

Note that by Proposition 45(ii) the morphisms in this category are automatically étale. For example, a diagram in $X_{\text{ét}}$ may look like:

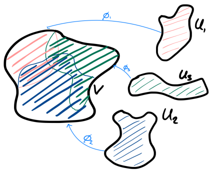
$$\begin{tikzcd}
V \arrow[r, "\phi"] & X \\
U \arrow[u] \arrow[ur, "\psi"'] &
\end{tikzcd} \quad =$$



where $V \to X$ and $U \to X$ (and so necesarily $U \to V$) are étale maps.
Much like before, a *presheaf* is a contravariant functor $\mathcal{F} : X_{\text{ét}} \to \text{Ab}$. The contravariance mimics pulling back functions as before: given a function $f \in \mathcal{F}(V)$ and a map $\phi : U \to V$, we obtain a function $\phi^* f \in \mathcal{F}(U)$ (thought of as $f \circ \phi$).

Sheaves. There are two concepts in the sheaf condition for OX which we will need to replace in $X_{\text{ét}}$ (since they don't make sense here!). One is the idea of covering a subspace V with a collection of open U_i; the other is the idea of intersecting open sets.

Étale Covers. In $X_{\text{ét}}$ we replace the idea of covering V with opens, with the idea of covering it with étale schemes! Naturally, an étale cover of $V \in X_{\text{ét}}$ is a collection of $U_i \in X_{\text{ét}}$ and morphisms in $X_{\text{ét}}$ $\phi_i : U_i \to V$ such that (as a topological space) $V = \cup_i \phi_i(U_i)$.



Intersections. It does not make sense to intersect two étale X-schemes, so we must do some soul searching about what 'intersection' means as a categorical concept in OX. One way to characterise the intersection $U_i \cap U_j$ of two opens in X is that it is the open set which contains every open set W which is contained in both U_i and U_j. This is a trivial rephrasing, but it intentionally mimics the definition of a *fibre product* (cf Definition 87). In other words, $U_i \cap U_j = U_i \times_V U_j$ in OX, and so we replace intersections with fibre products (which exist in $X_{\text{ét}}$).

Sheaf Condition. We can now state the sheaf condition. A presheaf $\mathcal{F}$ is a sheaf if for every étale cover $V = \bigcup_i \phi_i(U_i)$ in $X_{\text{ét}}$ the induced equaliser diagram below is exact:

$$0 \longrightarrow \mathcal{F}(V) \longrightarrow \prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \times_V U_j) \ .$$

Next time we will discuss cohomology.

Lecture 5.5 (Ross) Étale Cohomology II.5

To conclude our discussion last time, we will briefly define Étale cohomology and give a couple of examples. Recall our setup: Let X be a variety (or scheme).

Categorification. We work with the following category

Name:	$X_{\text{ét}}$
Objects:	étale X-schemes (schemes equipped with an étale map to X)
Morphisms:	morphisms of X-schemes (maps $U \to V$ which commute with the structural étale maps to X)

By Proposition 45(ii) the morphisms in this category are automatically étale. An *étale presheaf* is a contravariant functor $\mathcal{F} : X_{\text{ét}} \to \text{Ab}$.

Sheaves. An étale presheaf $\mathcal{F}$ is a sheaf if for every étale cover $V = \bigcup_i \phi_i(U_i)$ in $X_{\text{ét}}$ the induced equaliser diagram below is exact:

$$0 \longrightarrow \mathcal{F}(V) \longrightarrow \prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \times_V U_j)\ .$$

Cohomology. Given X and an étale sheaf $\mathcal{F}$, we construct the étale cohomology groups $H^n_{\text{ét}}(X; \mathcal{F})$ as follows. Take an injective resolution of étale sheaves

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I}^{(0)} \longrightarrow \mathcal{I}^{(1)} \longrightarrow \mathcal{I}^{(2)} \longrightarrow \mathcal{I}^{(3)} \longrightarrow \dots \quad \text{(Exact sequence of étale sheaves)}$$

We then evaluate this sequence at X (viewed as an étale X-scheme via the identity map $X \to X$) and delete $\mathcal{F}$, to produce the complex

$$0 \longrightarrow \mathcal{I}^{(0)} \longrightarrow \mathcal{I}^{(1)}(X) \longrightarrow \mathcal{I}^{(2)}(X) \longrightarrow \mathcal{I}^{(3)}(X) \longrightarrow \dots \quad \text{(complex of abelian groups)}$$

The nth sheaf cohomology group is then the nth homology of this sequence, i.e.

$$H^n(X; \mathcal{F}) := \frac{\ker\left(\mathcal{I}^{(n)}(X) \to \mathcal{I}^{(n+1)}(X)\right)}{\operatorname{im}\left(\mathcal{I}^{(n-1)}(X) \to \mathcal{I}^{(n)}(X)\right)}.$$

One thing we have not discussed is what exactness means for étale sheaves.

Definition 46. A complex of sheaves on $X_{\text{ét}}$

$$\mathcal{F} \xrightarrow{\ \alpha\ } \mathcal{G} \xrightarrow{\ \beta\ } \mathcal{H}$$

is exact in the middle position if for every étale X-scheme U and every element $\alpha \in \ker\left(\mathcal{G}(U) \to \mathcal{H}(U)\right)$, there is an étale cover $\{U_i \to U\}$ such that

$$\alpha|_{U_i} \in \operatorname{im}(\mathcal{F}(U_i) \to \mathcal{G}(U_i))$$

Some Properties. Below we point out some properties of étale cohomology, all of which can be deduced from the definition above by diagram chasing homological algebra arguments and the properties of étale maps from last time.

Proposition 47. *Given a variety (or scheme) X and étale sheaf $\mathcal{F}$ on $X_{ét}$, the étale cohomology groups $H^n(X; \mathcal{F})$ satisfy the following.*

(1) $H^0_{ét}(X; \mathcal{F}) = \mathcal{F}(X)$

(2) They are functorial in $\mathcal{F}$: if $\mathcal{F} \to \mathcal{G}$ is a morphism of étale sheaves on $X_{ét}$ then it induces a homomorphism of groups $H^n(X; \mathcal{F}) \to H^n(X; \mathcal{F})$.

(3) short exact sequences of sheaves induce long exact sequences of cohomology: given a short exact sequence of étale sheaves on $X_{ét}$

$$0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0,$$

the maps (and snake lemma) induce a long exact sequence

$$0 \to H^0(X; \mathcal{F}_1) \to H^0(X; \mathcal{F}_2) \to H^0(X; \mathcal{F}_3) \to H^1(X; \mathcal{F}_1) \to \dots.$$

(4) They are (contravariantly) functorial in X: if $Y \to X$ is an étale morphism of varieties (or schemes), and $\mathcal{F}$ is an étale sheaf on $X_{ét}$ then there is an induced map

$$H^n(X;\mathcal{F}) \to H^n(Y;\phi^*\mathcal{F}),$$

where $\phi^*\mathcal{F}$ is the étale sheaf on $Y_{ét}$ given by pullback: $(V \to Y) \mapsto \mathcal{F}(V \to Y \to X)$.

Example

We will now get our hands dirty with a particularly interesting sheaf: $\mathbb{G}_m$. Beforehand we introduce some words for everyones benefit.

Remark 48. For a scheme X, we have an associated structure sheaf $\mathcal{O}_X$. This is a functor which takes in open subsets $U \subseteq X$ and returns a ring $\mathcal{O}_X(U)$. We often refer to $\mathcal{O}_X(X)$ as the global sections on X. If you prefer to think of varieties, you may think that X/k is a variety and $\mathcal{O}_X(U) = k[U]$ is the ring of regular functions on an open subset U.

Definition 49. Let X be a scheme, and let $\mathbb{G}_m$ be the functor which sends a scheme U to the group of units of its global sections $\mathcal{O}_U(U)^*$. For an integer $n \geq 2$, let μ_n be the functor $U \mapsto \{x \in \mathcal{O}_U(U) \ : \ x^n = 1\}$.

Consider the sequence of sheaves

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{\times n} \mathbb{G}_m \longrightarrow 0. \tag{2}$$

Clearly by construction, μ_n is the kernel of the nth power map, and so this sequence is exact if and only if $\times n$ surjects (as a morphism of sheaves on $X_{\text{ét}}$).

Example 50. If $X = \operatorname{Spec}(K)$ is the spectrum of a field, then X is a singleton set, equipped with the structure sheaf $\mathcal{O}_X$ for which $\mathcal{O}_X(X) = K$.

Lemma 51. *Let $X = \operatorname{Spec}(K)$ for a perfect field K, then* (2) *is:*

- *Not necessarily exact on OX*
- *Exact on $X_{ét}$*

Proof. For OX: the definition of exactness is that the sequence is locally exact (i.e. on a neighbourhood of a point). Since X is a singleton set, the only open set is $X = \operatorname{Spec}(K)$, and the map $x \mapsto x^n$ is not surjective on $K^\times$ in general, for example if $K = \mathbb{Q}$. Hence the sequence is not necessarily exact. Of course if $K = \overline{\mathbb{Q}}$ (or indeed is just closed under taking nth roots), then the sequence *is* exact.

For $X_{\text{ét}}$ we now need to check surjectivity étale-locally. Refining coverings by finite disjoint unions of points to those just by points, it is equivalent to show that for every L/K separable and every $x \in L^\times$ there is a finite separable extension M/L such that $x \in M^{\times n}$. Since K is perfect, so is every finite extension of K, so hence so is L. In particular, we take $M := L(\sqrt[n]{x})$, and so the claim holds. □

Example 52. If K were not perfect, and $\operatorname{char}(K) \mid n$ then (2) can fail to be exact! Consider $K = \mathbb{F}_p(T)$, $n = p$, and $x = T$. Then the sequence being exact would require that there is a finite separable extension L/K such that $T \in L^{\times p}$. In other words, $L \supseteq \mathbb{F}_p(T)(\sqrt[p]{T}) \supseteq \mathbb{F}_p(T)$. However this intermediate extension is inseparable, so the total extension cannot be separable, so no such L exists. Hence (2) is not exact on $X_{\text{ét}}$.

Lecture 6 (Jenny): Étale Cohomology III

We will now look at étale cohomology over a field, and discuss its relationship with Galois cohomology. Denote by K a field, $\overline{K}$ its separable closure, $G_K := \mathrm{Gal}(\overline{K}/K)$.

Recall that $X/\mathrm{Spec}(K)$ is étale if and only if $X = \bigsqcup_{i=1}^r \mathrm{Spec}(L_i) = \mathrm{Spec}(\prod_{i=1}^r L_i)$ with L_i/K a finite separable field extension.

Definition 53. If $\mathcal{F}$ is a sheaf on $\mathrm{Spec}(K)_{\text{ét}}$ then we define the abelian group

$$\mathcal{F}(\overline{K}) := \varinjlim_{\substack{L/K \\ \text{fin. sep.}}} \mathcal{F}(L).$$

Remark 54. Note that we could also have taken the limit over finite Galois extensions, and this would have defined the same group.

Note that if L/K is finite Galois, and $\mathcal{F}$ is a sheaf on $\mathrm{Spec}(K_{\text{ét}})$ then there is a natural Galois action on $\mathcal{F}(L)$. Indeed, each $\sigma \in G_K$ induces a field automorphism $\sigma : L \to L$. Such a map is an isomorphism, so is étale, and so induces an isomorphism $\sigma : \mathcal{F}(L) \to \mathcal{F}(L)$. The fact that this is a group action is then immediate from the fact that $\mathcal{F}$ takes compositions of maps to compositions of maps. Moreover, since $\sigma : L \to L$ is compatible with inclusion into larger Galois extensions, the group actions on $\mathcal{F}(L)$ are compatible, and so $\mathcal{F}(\overline{K})$ is a (discrete continuous) G_K-module (continuity for the discrete topology follows from this module being a limit of those acted on by finite quotients).

Theorem 55 (Étale cohomology over a field)**.** *We have*

(i) The following is an equivalence of categories

$$\{\text{abelian sheaves on } \mathrm{Spec}(K)_{ét}\} \to \{\text{(discrete) continuous } G_K \text{ modules}\}$$
$$\mathcal{F} \mapsto \mathcal{F}(\overline{K}),$$

where the global section functor on the left corresponds to the G_K-fixed point functor on the right.

(ii) An inverse equivalence is defined by

$$\{\text{(discrete) continuous } G_K \text{ modules}\} \to \{\text{abelian sheaves on } \mathrm{Spec}(K)_{ét}\}$$
$$M \mapsto \mathcal{F}_M,$$

where for every finite separable extension L/K we define $\mathcal{F}_M(L) := M^{\mathrm{Gal}(\overline{K}/L)}$.

(iii) As a consequence, for every (continuous discrete) G_K-module M:

$$H^n_{ét}(X; \mathcal{F}_M) \cong H^n(G_K, M),$$

where the right hand side is continuous group cohomology (better known as Galois cohomology).

Proof. (1) We consider the two functors

$$\{\text{(discrete) continuous } G_K \text{ modules}\} \to \{\text{abelian sheaves on } \mathrm{Spec}(K)_{\text{ét}}\}$$
$$M \mapsto^g \mathcal{F}_M,$$
$$\mathcal{F}(\overline{K}) \leftarrow^f \mathcal{F}$$

We want to show that

(i) f is well defined
(ii) g is well defined

(iii) $f \circ g = \mathrm{Id}$
(iv) $g \circ f = \mathrm{Id}$

(i) is clear from our discussion above, in that we have already argued that $\mathcal{F}(\overline{K})$ is a continuous discrete G_K-module. For (ii) we need to check that we have a presheaf and then that it is a sheaf.

Presheaf: It is clear that the natural inclusions $M^{G_L} \to M^{G_F}$ for every F/L finite separable are the required contravariant pairs of morphisms.

Sheaf: Take an étale cover $V = \bigcup_i \phi_i(U_i)$ in $X_{\text{ét}}$, we seek exactness of

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{F}(V) \arrow[r] & \prod_i \mathcal{F}(U_i) \arrow[r, shift left] \arrow[r, shift right] & \prod_{i,j} \mathcal{F}(U_i \times_V U_j) \end{tikzcd} .$$

Note that $V = \bigsqcup_{i=1}^r \mathrm{Spec}(L_i)$, and refining the cover we may assume that $V = \mathrm{Spec}(L)$, $U_i = \mathrm{Spec}(L_i)$ for some finite separable extensions L_i/L. Moreover, $\mathrm{Spec}(L_i) \times_{\mathrm{Spec}(L)} \mathrm{Spec}(L_j) = \mathrm{Spec}(L_i \otimes_L L_j)$, which is a union of finitely many compositums $L_i \cdot L_j$. Thus our sequence we need exactness of is

$$\begin{tikzcd} 0 \arrow[r] & M^{G_L} \arrow[r] & \prod_i M^{G_{L_i}} \arrow[r, shift left] \arrow[r, shift right] & \prod_{i,j} M^{G_{L_i \cdot L_j}} \end{tikzcd} .$$

Exactness of this is immediately clear: injectivity is immediate since $m \mapsto (m, m, \ldots, m)$; the compatibility condition is then that if $(m_i)_i \in \prod_i M^{G_{L_i}}$ is such that $m_i = m_j$ for all i, j then it is in the image of $m \mapsto (m, \ldots, m)$ which is trivial.

We now prove (iii) We map $\mathcal{G} \mapsto \mathcal{G}(\overline{K}) \mapsto \mathcal{F}_{\mathcal{G}(\overline{K})}$, and we would like to see that we have obtained $\mathcal{G}$ back. We simply evaluate with the definitions:

$$\mathcal{F}_{\mathcal{G}(\overline{K})}(L) = \mathcal{G}(\overline{K})^{G_L} = \mathcal{G}(L).$$

Finally we check (iv). Mapping a module $M \mapsto \mathcal{F}_M \mapsto \mathcal{F}_M(\overline{K})$ we must check that we get M back. However,

$$\mathcal{F}_M(\overline{K}) = \varinjlim_{\substack{L/K \\ \text{fin. sep}}} \mathcal{F}_M(L) = \varinjlim_{\substack{L/K \\ \text{fin. sep}}} M^{\mathrm{Gal}(\overline{K}/K)} = \bigcup_{\substack{L/K \\ \text{fin. sep}}} M^{\mathrm{Gal}(\overline{K}/L)},$$

M is a discrete continuous module, so the stabiliser of each point $m \in M$ is open in G_K, and hence given by $\mathrm{Gal}(\overline{K}/L)$ for some finite separable L/K. In particular,

$$M = \bigcup_{\substack{L/K \\ \text{fin. sep}}} M^{\mathrm{Gal}(\overline{K}/L)},$$

as required. □

Lecture 6.5 (Jenny) Étale Cohomology III.5

Last time we established a bijection between abelian sheaves on $\mathrm{Spec}(K)_{\text{ét}}$ and (continuous, discrete) G_K-modules, given as follows:

$$\{\text{abelian sheaves on } \mathrm{Spec}(K)_{\text{ét}}\} \to \{\text{(discrete) continuous } G_K \text{ modules}\}$$
$$\mathcal{F} \mapsto \mathcal{F}(\overline{K}),$$
$$\mathcal{F}_M \leftarrow M.$$

where for L/K finite separable $\mathcal{F}_M(L) = M^{\mathrm{Gal}(K_s/L)}$, and $\mathcal{F}(\overline{K}) = \varinjlim_{\substack{L/K \\ \text{fin. sep.}}} \mathcal{F}(L)$.

Moreover, we claimed that for each module M,

$$H^i_{\text{ét}}(\mathrm{Spec}(K), \mathcal{F}_M) \cong H^i(G_K, M),$$

where the right hand side is Galois cohomology. It remains to prove this claim. Note that to define étale cohomology we have to take an injective resolution of $\mathcal{F}_M$, take global sections and remove $\mathcal{F}_M(X)$:

$$0 \to \mathcal{I}^{(0)}(\mathrm{Spec}(K)) \to \mathcal{I}^{(1)}(\mathrm{Spec}(K)) \to \dots.$$

Meanwhile to definie Galois cohomology we take an injective resolution of M as a G_K-module, take G_K-fixed points and remove M:

$$0 \to I_0^{G_K} \to I_1^{G_K} \to \dots.$$

In particular, since the fixed point functor corresponds to the global sections functor, the homologies are the same.

However, we have a problem. In general $H^n(G_K, M) \neq 0$ for $n > 0$, and since $\mathrm{Spec}(K)$ is a single point (so 0 dimensional), the Weil cohomology axioms would force us to want $H^n(\mathrm{Spec}(K), \mathcal{F}) = 0$ for all $n > 0$. How do we resolve this? Take a variety X/K, and consider the base change to $X_{\overline{K}} = X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K})$, together with the pullback $\mathcal{F}$ on $\overline{K}$ instead.

Definition 56. For a variety X/K, note that $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z})$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module. We then define

- $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_\ell) := \varprojlim_n H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z})$ is a $\mathbb{Z}_\ell$-module.
- $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell) := H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a $\mathbb{Q}_\ell$-vector space.

Each of these comes with a G_K-functions.

Example 57. Take X/K to be a variety of finite type, and J to be the set of connected components of $X_{\overline{K}}$. Then

$$H^0(X_{\overline{K}}, A) = A^J,$$

as an abelian group, for $A \in \{\mathbb{Z}/\ell^n\mathbb{Z}, \mathbb{Z}_\ell, \mathbb{Q}_\ell\}$.

Theorem 58. *Let X/K be a separated scheme of finite type, and $\ell \nmid \mathrm{char}(K)$. Then $H^n(X_{\overline{K},\mathbb{Z}/\ell^n\mathbb{Z}})$ are:*

- *finite for all n;*
- *invariant under extension from $\overline{K}$ to any larger algebraically closed field;*
- *0 for $n > 2\dim(X)$;*
- *0 for $n > \dim(X)$ if X is affine;*
- *$H^n_{\text{top}}(X(\mathbb{C}), \mathbb{Z}/\ell^n\mathbb{Z})$ canonically for $K = \mathbb{C}$.*

Moreover they satisfy the properties of a Weil cohomology theory.

Lecture 7 (Sam): Étale Cohomology IV

Today we'll start looking at $H^1_{\text{ét}}(X, \mathbb{G}_m)$ and $H^2(X, \mathbb{G}_m)$, and possibly also $H^1(X, \mathbb{Z}_\ell)$ (time-permitting).

Recall that for an étale X-scheme $U \to X$, we define $\mathbb{G}_m(U) := \mathcal{O}_U(U)^\times$.

Concerning $H^1_{ét}(X, \mathbb{G}_m)$

Weil divisors.

Hypothesis 59. *Let X be an integral, noetherian, separated, regular in codimension 1 scheme ("not too singular").*

Recall the following concepts associated to Weil divisors.

- Prime divisors: $Z \subset X$ which are closed integral subschemes of codimension 1.
- Weil divisors: (finite) formal sums of prime divisors, we denote the group of these by $\operatorname{Div}(X)$.
- Principal divisors: for $f \in K(X)^\times$, we write $\operatorname{Div}(f) = \sum\limits_{Z \text{ prime}} v_Z(f)Z \in \operatorname{Div}(X)$. Here $v_Z(f)$ is the order of vanishing of f along Z (this uses Hypothesis 59, as $\mathcal{O}_{X,\eta_Z}$ is a DVR and v_Z is the valuation).
- Divisor class group: $\operatorname{Cl}(X) := \operatorname{Div}(X)/\sim$ where $D \sim D'$ if $D - D' = \operatorname{Div}(f)$ for some $f \in K(X)^\times$.

Cartier Divisors. Now X is any scheme, and for $U \subset X$ an open subscheme we define $S(U)$ to be the non-zero divisors in $\mathcal{O}_X(U)$, and sheafify the functor $U \mapsto S(U)^{-1}\mathcal{O}_U(U)$. Then we get a sheaf $\mathcal{K}$ of 'local rational functions'.

Our Cartier notion of divisors is then the following.

Definition 60. A Cartier divisor is a global section of $\mathcal{K}^\times/\mathcal{O}_X^\times$. Formally: this is an equivalence class of compatible pairs $\{(U_i, f_i)\}_i$ where U_i is an open cover of X, $f_i \in \mathcal{K}(U)^\times$, $f_i/f_j \in \mathcal{O}_X(U_i \cap U_j)^\times$.

We then have the notions

- The notion of principality for Cartier divisors is then the elements of $\mathcal{K}^\times$.
- The Cartier divisor class group is the group of Cartier divisors modulo the principal ones, denoted $\operatorname{CaCl}(X)$;

We add the hypothesis below.

Hypothesis 61. *Let X be an integral, separated, noetherian, locally factorial (all local rings are UFDs).*

Proposition 62. *Under Hypothesis 61, we have*

$$\operatorname{CaCl}(X) \cong \operatorname{Cl}(X).$$

Moreover this is attained through the map $\{(U_i, f_i)\}_i \mapsto \sum_Z v_Z(f_i)Z$ for any f_i with $Z \cap U_i \neq \emptyset$.

Line Bundles. An $\mathcal{O}_X$-module is a sheaf $\mathcal{F}$ such that $\mathcal{F}(U)$ is always an $\mathcal{O}_X(U)$-module. Such things are:

- locally free if $\forall x \in X$ there is an open neighbourhood $x \in U \subseteq X$ such that $\mathcal{F}(U) \cong \mathcal{O}_X(U)^{\oplus n}$ where $n := \operatorname{rk}(\mathcal{F})$ is constant on connected X.
- a line bundle if it is locally free of rank 1 (which makes it invertible under $\otimes$).

We now define

- $\operatorname{Pic}(X)$ is the set of isomorphism classes of line bundles.

Proposition 63. *There is an injection* $\operatorname{CaCl}(X) \to \operatorname{Pic}(X)$ *fiven by $D \mapsto \mathcal{L}(D)$, where $\mathcal{L}(D)(U_i) = \langle f_i^{-1} \rangle \leq \mathcal{K}(U_i)^\times$. Under Hypothesis 61,* $\operatorname{CaCl}(X) \cong \operatorname{Pic}(X)$.

They're all the same thing – and it is Étale cohomology!

Proposition 64. $\mathrm{Pic}(X) \cong H^1_{\acute{e}t}(X, \mathbb{G}_m)$.

Proof. Take the long exact sequence of étale sheaves

$$1 \to \mathbb{G}_{m,X} \to j_* \mathbb{G}_{m,k(X)} \to \bigoplus_{\substack{D \in X^{(1)} \\ \text{codim. } 1}} (\iota_x)_* \mathbb{Z} \to 1.$$

where $j : \mathrm{Spec}(K(X)) \to X$ is the inclusion of the generic point, take cohomology and apply Hilbert 90 to obtain the claim. □

Lecture 7.5 (Sam): Brauer Groups et al

Last time we were focussed on $H^1_{\text{ét}}(X, \mathbb{G}_m) = \mathrm{Pic}(X)$. This time we will look at $H^2_{\text{ét}}(X, \mathbb{G}_m)$, $H^i(X, \mu_{\ell^n})$, and $H^i_{\text{ét}}(X, \mathbb{Z}_\ell)$.

Brauer Groups

Azumaya Algebras.

Definition 65. Let K be a field, and let $0 \neq A$ be a finite dimensional associative K-algebra. We say that A is central if

$$Z(A) := \{a \in A \ : \ ab = ba \ \forall b \in A\} = K.$$

We say that A is simple if the only 2-sided ideals are 0 and A. We abbreviate the phrase central simple algebra to CSA.

Example 66. For $a, b \in K^\times$ we have the quaternion algebra $Q_K(a,b) = \langle 1, i, j, k \rangle_K$ where $i^2 = a,\ j^2 = b,\ ij = k = -ji$. For example, Hamiltons quaternions $\mathbb{H} = Q_{\mathbb{R}}(-1,-1)$.

Theorem 67. *If A is a K-algebra then it is a CSA if and only if $A \otimes_K K_s \cong M_n(K_s)$ for some n*

Definition 68. Replacing K by a commutative ring R, simplicity by separability (multiplication has a section $\sigma : A \to A \otimes_R A$, $\sigma(1)$='separability idempotent'), we arrive at the definition of an Azumaya algebra. We denote the set of these by $\mathrm{Az}(R)$.

Definition 69. Say that $A, B \in \mathrm{Az}(R)$ are similar, denoted $A \sim B$, if $A \otimes_R M_n(R) \cong B \otimes_R M_m(R)$ for some $n, m \geq 1$.

Definition 70. The Brauer group of R is $\mathrm{Br}_{\mathrm{Az}}(R) = (\mathrm{Az}(R)/\sim, \otimes)$.

Definition 71. The cohomological Brauer group of a scheme X is $H^2_{\text{ét}}(X, \mathbb{G}_m)$, denoted $\mathrm{Br}(X)$.

Example 72. Let $X = \mathrm{Spec}(K)$. Then $\mathrm{Br}(K) = \mathrm{Br}(\mathrm{Spec}(K)) = H^2(K, K_s^\times)$. Take the long exact sequence of Galois cohomology

$$0 \to K_s^\times \to \mathrm{GL}_n(K_s) \to \mathrm{PGL}_n(K_s) \to 0.$$

(note that we have to use a slightly unusual form of cohomology here, since GL and PGL are not abelian and so don't form modules as such, but there exist nonabelian analogues of H^1 and H^2). The long exact sequence is

$$1 \to K_s^\times \to \mathrm{GL}_n(K) \to \mathrm{PGL}_n(K) \to 1 \to 1 \to H^1(K, \mathrm{PGL}_n(K_s)) \to \mathrm{Br}(K),$$

where we have used Hilberts theorem 90 (and a result from Poonens book §1.3,1.5) to see that $H^1(K, K_s^\times) = H^1(K, \mathrm{GL}_n(K_s)) = 0$. Thus we have an inclusion $H^1(K, \mathrm{PGL}_n(K_s)) \subseteq \mathrm{Br}(K)$.

We also have a map $\mathrm{Az}_n(K) \to H^1(K, \mathrm{PGL}_n(K_s))$ (the former is the set of n^2-dimensional algebras) given by

$$\mathrm{Az}_n(K) \ni \phi \mapsto \eta \in H^1(K, \mathrm{PGL}_n(K_s)),$$

where

$$\eta_\sigma = \phi^{-1}({}^\sigma\phi) \in \mathrm{Aut}(M_n(K_s)) \cong \mathrm{PGL}_n(K_s),$$

where the isomorphism follows from the Skolem–Noether theorem.

Then we in fact have an injection $\mathrm{Az}_n(K)/\cong$ into $\mathrm{Br}(K)$ which induces an isomorphism $\mathrm{Br}_{\mathrm{Az}}(K) \cong \mathrm{Br}(K)$ (see Serre's local fields chapter X§5).

In general for a reasonable scheme

$$\mathrm{Br}_{\mathrm{Az}}(X) \cong H^2_{\text{ét}}(X, \mathbb{G}_m)_{\mathrm{tors}} = H^2_{\text{ét}}(X, \mathbb{G}_m) = \mathrm{Br}(X),$$

where the formed is the group of Azumaya $\mathcal{O}_X$-algebras: sheaves $\mathcal{F}$ of $\mathcal{O}_X$-algebras such that on every étale open U we have $\mathcal{F}(U)$ is an Azumaya algebra over $\mathcal{O}_X(U)$.

Why do we care? The Brauer–Manin obstruction is given by a pairing

$$X(\mathbb{A}_K) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}$$

where the left kernel is $X(\mathbb{A}_K)^{\mathrm{Br}} \supseteq X(K)$. Moreover, this is closed. In particular, if the Brauer group pairs trivially with nothing then we cannot possibly have rational points! Also if it is a proper subset then we cannot have weak approximation (that the rational points are dense in the adelic points).

Theorem 73. *The following are facts.*

- $\mathrm{Br}(K_s) = 0$
- $\mathrm{Br}(\mathbb{R}) = \langle \mathbb{H}_{\mathbb{R}} \rangle \cong \mathbb{Z}/2\mathbb{Z}$
- *for a number field K,* $\mathrm{Br}(K_v) \cong \mathbb{Q}/\mathbb{Z}$ *via the invariant map if v is a finite place of K.*

Coefficients in μ_{ℓ^n}

For ℓ invertible on X, we have a short exact sequence on $X_{\text{ét}}$:

$$1 \to \mu_{\ell^n} \to \mathbb{G}_m \to \mathbb{G}_m \to 1 \tag{3}$$

Assume that X/K is a projective variety, then

$$H^0_{\text{ét}}(X, \mathbb{G}_m) = \mathcal{O}_X(X)^\times = K^\times$$
$$H^0_{\text{ét}}(X, \mu_{\ell^n}) = K^\times[\ell^n] = \mu_{\ell^n}(K).$$

Taking the long exact sequence on (3) we get

$$\begin{tikzcd}
1 \arrow[r] & \mu_{\ell^n}(K) \arrow[r] & K^\times \arrow[r, "\times \ell^n"] & K^\times \arrow[dlll] \\
H^1_{\text{ét}}(X, \mu_{\ell^n}) \arrow[r] & \mathrm{Pic}(X) \arrow[r, "\times \ell^n"] & \mathrm{Pic}(X) \arrow[dll] & \\
H^2_{\text{ét}}(X, \mu_{\ell^n}) \arrow[r] & \mathrm{Br}(X) \arrow[r, "\times \ell^n"] & \mathrm{Br}(X). &
\end{tikzcd}$$

Thus $H^1_{\text{ét}}(X_{K_s}, \mu_{\ell^n}) = \operatorname{Pic}(X_{K_s})[\ell^n]$. Assume that $X = C$ is a curve of genus g then we have a short exact sequence

$$0 \longrightarrow \operatorname{Pic}^0(C) \longrightarrow \operatorname{Pic}(C) \longrightarrow \mathbb{Z};$$

when $C(K) \neq \emptyset$ then the degree map is surjective and this splits: $\operatorname{Pic}(C) \cong \operatorname{Pic}^0(C) \oplus \mathbb{Z}$. Furthermore $\operatorname{Pic}^0(C_{\overline{K}}) \cong \operatorname{Jac}(C)(\overline{K})$, multiplication by ℓ^n is surjective and the kernel is $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$.

Also, $\operatorname{Br}(C_{\overline{K}}) = 0$ by Tsen's theorem, and we get

$$H^i_{\text{ét}}(C_{\overline{K}}, \mu_{\ell^n}) = \begin{cases} \mu_{\ell^n}(\overline{K}) & i = 0 \\ (\mathbb{Z}/\ell^n\mathbb{Z})^{2g} & i = 1 \\ \mathbb{Z}/\ell^n\mathbb{Z} & i = 2 \\ 0 & i \geq 3. \end{cases}$$

$$H^1(E_{\overline{K}}, \mathbb{Z}_\ell)$$

Let E/K be an elliptic curve, then recall

$$H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Z}_\ell) := \varprojlim_n H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z}).$$

We claim that this is dual to the Tate module $T_\ell(E) = \varprojlim_n E(\overline{K})[\ell^n]$ as follows. There is a pairing

$$H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z}) \times H^1_{\text{ét}}(E_{\overline{K}}, \mu_{\ell^n}) \xrightarrow{\cup} H^2_{\text{ét}}(E_{\overline{K}}, \mu_{\ell^n}) = \mu_{\ell^n}(\overline{K}).$$

The right hand term is $E[\ell^n]$ by our above discussion, so taking a limit we get a pairing between $H^1(E_{\overline{K}}, \mathbb{Z}_\ell)$ and $T_\ell(E)$ which maps to $\mathbb{Z}_\ell(1) = \varprojlim_n \mu_{\ell^n}(\overline{K})$. It turns out that this pairing is perfect, and hence the duality follows.

Lecture 8 (Matt): Curves over Local Fields

Throughout, K is a local field with residue characteristic $p \neq \ell$. For all such K, we write

- $\mathcal{O}_K$ for the ring of integers in K;
- $\mathbb{F}_K$ for the residue field of K;
- G_K for the absolute Galois group;
- v_K for the valuation on K.

Recap of Galois Theory

Let F/K be a finite Galois extension, and π be a uniformiser of F. Then the inertia and wild inertia subgroups are:

$$I := \{\sigma \in \operatorname{Gal}(F/K) \ : \ \sigma(\alpha) \equiv \alpha \mod \pi \ \forall \alpha \in \mathcal{O}_F\}$$
$$P := \left\{\sigma \in \operatorname{Gal}(F/K) \ : \ \sigma(\alpha) \equiv \alpha \mod \pi^2 \ \forall \alpha \in \mathcal{O}_F\right\}.$$

These have some well known properties:

- I and P are normal subgroups of $\operatorname{Gal}(F/K)$;
- P is the Sylow p-subgroup of I;
- I/P is a cyclic group of order coprime to p;
- $\operatorname{Gal}(F/K)/I \cong \operatorname{Gal}(\mathbb{F}_F/\mathbb{F}_K)$ via a canonical isomorphism.

- $\mathrm{Gal}(\mathbb{F}_F/\mathbb{F}_K)$ is cyclic and generated by (arithmetic) Frobenius $\varphi : x \mapsto x^{\#\mathbb{F}_K}$.

A lift of the Frobenius element for the residue extension to $\mathrm{Gal}(F/K)$ is called an arithmetic Frobenius element and denoted Frob.

Good Reduction

Let E/K be an elliptic curve with good reduction (meaning $\Delta_{E,\min} \in \mathcal{O}_K^\times$).

Question 74. *What is $H^1_{\acute{e}t}(E_{\overline{K}}, \mathbb{Q}_\ell) \cong (T_\ell E \otimes \mathbb{Q}_\ell)^\vee$, as a G_K-representation? More generally for a curve, we ask about:*

$$H^1_{\acute{e}t}(C_{\overline{K}}, \mathbb{Q}_\ell) \cong H^1_{\acute{e}t}(\mathrm{Jac}(C), \mathbb{Q}_\ell) \cong (T_\ell(\mathrm{Jac}(C)) \otimes \mathbb{Q}_\ell)^\vee .$$

Lemma 75 (Silverman AEC §VII.3.1)**.** *Let E/K be an elliptic curve with good reduction, then the reduction map induces an injective homomorphism for all $n \geq 0$*

$$E(K)[\ell^n] \to \tilde{E}(\mathbb{F}_K).$$

Note that since good reduction is stable under base change, the inertia subgroup acts trivially. This gives a G_K-isomorphism $T_\ell E \cong T_\ell \tilde{E}$, where the right hand side is the Tate module of $\tilde{E}/\mathbb{F}_K$. In particular, since the absolute Galois group of $\mathbb{F}_K$ is procyclic and (topologically) generated by the Frobenius, it only remains to understand the action of Frobenius.

Let $\alpha, \beta \in \overline{\mathbb{Q}}_\ell$ be the eigenvalues of Frobenius acting on $T_\ell E \otimes \mathbb{Q}_\ell$. Then by results in previous lectures, the Weil conjectures in particular, we know that

$$\begin{aligned} \alpha\beta &= \#\mathbb{F}_K \\ \alpha + \beta &= \#\mathbb{F}_K + 1 - \tilde{E}(\mathbb{F}_K). \end{aligned}$$

This allows us to determine α, β completely from the structure of $\tilde{E}(\mathbb{F}_K)$.

Grothendieck's Monodromy Theorem

Definition 76. An ℓ-adic representation V of G_K is:

- unramified (or has good reduction) if inertia acts trivially;
- semistable if inertia acts unipotently (meaning every eigenvalue is 1; equivalently the semisimplification is unramified);
- potentially $(*)$ if V is $(*)$ as a G_F-representation for some finite extension F/K.

Definition 77. An ℓ-adic representation of G_K is said to *arise from geometry* if it is a subquotient of (a Tate twist of) $H^n(X_{\overline{K}}, \mathbb{Q}_\ell)$ for some smooth projective variety X/K.

Definition 78. Tate twists are defined as follows: $\mathbb{Q}_\ell(n) := (T_\ell\mu)^{\otimes n} \otimes \mathbb{Q}_\ell$. For a representation V, the n-th Tate twist is $V(n) = V \otimes \mathbb{Q}_\ell(n)$.

Theorem 79 (Grothendieck's ℓ-adic Monodromy Theorem)**.** *Every ℓ-adic representation of G_K that arises from geometry is potentially semistable.*

Theorem 80 (Raynaud's criterion)**.** *Let A/K be an abelian variety, and suppose $A[12] \subseteq A(K)$. Then $H^n_{\acute{e}t}(A_{\overline{K}}, \mathbb{Q}_\ell)$ is semistable for all n.*

Remark 81. In fact, for abelian varieties

$$H^n_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell) = \bigwedge^n H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell),$$

so in particular understanding $H^1_{\text{ét}}$ is enough to understand $H^n_{\text{ét}}$.

Tate Curves

Recall that for an elliptic curve $E/\mathbb{C}$, the complex points form a torus: there is some rank 2 lattice $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau \subset \mathbb{C}$ such that

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda,$$

as complex Lie groups. We would like to mimic this for E/K but cannot do this since K has no discrete subgroups. Instead note that the exponential map gives an isomorphism

$$\mathbb{C}/\Lambda \cong \mathbb{C}^\times / e^{2\pi i \tau \mathbb{Z}}.$$

This version carries over to K with some adjustments. Indeed $K^\times$ does have some interesting discrete subgroups: those of the form $q^{\mathbb{Z}}$ for some $q \in K^\times$ with $v_K(q) \neq 0$. Moreover, the 'modular functions' (a special class of related functions) converge so long as $v_K(q) > 0$.

(Split) Multiplicative Reduction. Let $v_K(q) > 0$ and consider the elliptic curve

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q),$$

where $a_4(q) = -5 \sum\limits_{n \geq 1} \frac{n^3 q^n}{1-q^n}$ and $a_6(q) = -\frac{1}{12} \sum\limits_{n \geq 1} \frac{(7n^5+5n^3)q^n}{1-q^n}$.

Theorem 82 (Tate)**.** *The following hold.*

1. *There is a (rigid analytic) G_K-isomorphism*
$$E_q(\overline{K}) \cong \overline{K}^\times / q^{\mathbb{Z}}.$$
2. *E_q has split multiplicative reduction (in particular $v_K(j(E)) < 0$).*
3. *Every elliptic curve E with split multiplicative reduction over K is K-isomorphic to E_q for some q.*

In particular, understanding elliptic curves with (split) multiplicative reduction is the same as looking at these Tate curves.

Question 83. *What is $T_\ell E_q$ as a G_K-mod?*

The answer now is not too hard:

$$E[\ell^n] = \overline{K}^\times / q^{\mathbb{Z}} = \left\langle \zeta_{\ell^n}, q^{1/\ell^n} \right\rangle.$$

As $p \neq \ell$, $K(\zeta_{\ell^n})/K$ is unramified for all $n \in \mathbb{Z}$ and so inertia acts trivially on that part of the Tate module. Moreover, $\text{Frob}(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\#\mathbb{F}_K}$, and so we completely understand the action on the submodule obtained from ζ_{ℓ^n}.

What about the rest? For simplicity, assume that $\ell \nmid v(q)$. Note that for an inertia element σ, we have

$$\sigma(q^{1/\ell^n}) = \zeta_{\ell^n}^{t_\ell(\sigma)} q^{1/\ell^n},$$

for some $t_\ell(\sigma) \in \mathbb{Z}/\ell^n\mathbb{Z}$. Moreover, these $t_\ell(\sigma)$ are compatible as n grows. If $\sigma \in P_K$, the wild inertia, then $t_\ell(\sigma) = 0$ since σ has order a power of $\#\mathbb{F}_K$ which is coprime to ℓ. Hence we can quotient out by wild inertia and only consider the action of I/P. In fact, since $\ell \nmid v(q)$, $t_\ell(\sigma)$ is coprime to ℓ and so the action is

$$\sigma = \begin{pmatrix} 1 & t_\ell(\sigma) \\ 0 & 1 \end{pmatrix} \qquad\qquad \text{Frob} = \begin{pmatrix} \#\mathbb{F}_K & 0 \\ 0 & 1 \end{pmatrix},$$

for some suitable choice of Frobenius element Frob. Now we are done, having completely described $H^1_{\text{ét}}(E_q, \mathbb{Q}_\ell)$. Moreover, we can see that this representation is semistable but not unramified.

Lecture 9 (Bober): Zeta and L-functions

Let $X/\mathbb{Z}$ be a scheme of finite type. Then the zeta function is

$$\zeta(X,s) := \prod_{x\in\overline{X}} \left(1 - \frac{1}{N(x)^s}^{-1}\right),$$

where $\overline{X}$ is our notation for the set of (Zariski) closed points of X. Closed points are precisely those for which $\#k(x) < \infty$, and we define this norm $N(x) := \#k(x)$.

Example 84 ('Trivial' example)**.** $\zeta(\mathrm{Spec}(\mathbb{Z}), s) = \zeta(s)$ is the Riemann zeta function, since the closed points are $\langle p\rangle$ for each prime p and the size of the residue field is p. Similarly rings of integers of number fields lead to Dedekind zeta functions of number fields.

Exercise 85. Make sense of this for elliptic curves.

Exercise 86. This is something we've seen before when $X/\mathbb{F}_q$ is a variety over a finite field. In fact: $\zeta(X,s) = Z(X, q^{-s})$ where

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

and one must check that $Z(X,T) = \exp\left(\sum_{n\geq 1} \frac{\#X(\mathbb{F}_{q^n})T^n}{n}\right)$.

This gives us a natural product decomposition over the closed points of $\mathrm{Spec}(\mathbb{Z})$ (i.e. the primes!)

$$\zeta(X,s) = \prod_p \zeta(X_p, s),$$

which is the original definition of the Hasse-Weil zeta function attached to a variety.

Varieties

We now return to varieties and the Hasse-Weil zeta function, all over $\mathbb{Q}$. Then we could 'define'

$$\zeta(V,s) = \prod_p Z(V/\mathbb{F}_p, p^{-s}).$$

This doesn't really make sense: $V/\mathbb{Q}$ doesn't immediately have a notion of reduction mod p. We need to choose a model for $V/\mathbb{Z}$, and then we can reduce mod p. Note that this choice may change things at finitely many p!

At least we may say something like, up to finitely many factors,

$$\zeta(V,s) = \prod_{p\text{ 'good'}} Z(V/\mathbb{F}_p, p^{-s}).$$

Elliptic Curves

From lecture 2,

$$Z(E/\mathbb{F}_p, T) = \frac{1 - a_pT + pT^2}{(1-T)(1-pT)}.$$

So

$$\zeta(E,s) \approx \prod_{\text{some } p} \frac{1}{1-p^{-s}} \prod \frac{1}{1-p^{1-s}} \prod \left(1 - a_pp^{-s} + p^{-2s+1}\right) \approx \frac{\zeta(s)\zeta(s-1)}{L(E,s)}.$$

From lecture 3, Theorem 26, we know for a variety $V/\mathbb{F}_q$ of dimension d,

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T) \dots P_{2d-1}(T)}{P_0(T) \dots P_{2d}(T)}.$$

Where $P_r(T) = \det\left(1 - T\mathrm{Frob} \mid H^r_{\text{ét}}(V, \mathbb{Q}_\ell)\right)$. For example, for an elliptic curve we get the numerator having the factor corresponding to $L(E, s)$, and the denominator having factors corresponding to $\zeta(s)$ and $\zeta(s-1)$.

Then we can define $L(E, s)$ by replacing $H^1_{\text{ét}}(E_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$ with $H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)^{I_p}$, and taking the products of these.

For each ℓ we have a new Galois representation for $H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$. As $\ell \neq p$ varies we obtain a compatible system of such representations, meaning that the characteristic polynomials are all the same and so the L-function is independent of ℓ. Generalising this we arrive at motives.

Appendix: Useful things

Definition 87. Given a diagram in a category

$$\begin{tikzcd}
 & C \arrow[d] \\
A \arrow[r] & B
\end{tikzcd}$$

the fibre product (if it exists) is an object denoted $A \times_B C$, equipped with morphisms $A \times_B C \to A$ and $A \times_B C \to C$ such that every commutative square containing the diagram factors through $A \times_B C$:

$$\begin{tikzcd}
X \arrow[dr, dotted, "\exists"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
 & A \times_B C \arrow[r] \arrow[d] & C \arrow[d] \\
 & A \arrow[r] & B
\end{tikzcd}$$