

The Weil Conjectures

Nir Elber

Fall 2025

Abstract

This document records the STAGE seminar for the fall of 2025.

Contents

Contents	1
1 September 11: Statements of the Weil Conjectures	2
1.1 Some History	2
1.2 ζ -Functions	3
1.3 Proof for Curves	4
1.4 Intersection Theory on a Surface	5
2 September 18th: The Étale Site	7
2.1 Étale Morphisms	7
2.2 The Fundamental Group	9
2.3 Grothendieck Topologies	10
3 October 2: The Lefschetz Trace Formula	12
3.1 The Tools	12
3.2 The Lefschetz Trace Formula	13
3.3 Some Weil Conjectures	14
4 October 9: Constructible Sheaves, Base Change, and L-functions	15
4.1 Constructible Sheaves	15
4.2 Proper Base Change	16
4.3 L -Functions	18
5 October 16: Katz's Proof of the Riemann Hypothesis for Curves	19
5.1 Review	19
5.2 Reduction to a Single Curve	20
5.3 Computations on a Family of Curves	22
5.4 Persistence of Purity	23
6 October 23: The Riemann Hypothesis for Hypersurfaces	23
6.1 Spreading Out for Hypersurfaces	23
6.2 A Single Example	25
7 October 30: Deligne's Proof of Weil I and the Main Lemma	28
7.1 The Étale Fundamental Group	28
7.2 The Main Lemma	29
7.3 Applications	31

8 November 6: Lefschetz Principles	32
8.1 Fibrations, Diffeomorphically	32
8.2 Lefschetz Pencils	33
8.3 Symplectic Monodromy	34
9 November 13: The Riemann Hypothesis	36
9.1 Reduction to the Blowup	36
9.2 The Three Groups	38
10 November 20: The Statement of Weil II	39
10.1 The Statement	39
10.2 Reductions	40
10.3 Sketch	42
11 December 4: Local Monodromy	43
11.1 Grothendieck's Monodromy Theorem	43
11.2 The Monodromy Operator	44
11.3 The Weight Filtration	45
12 December 11: Applications of Weil II	46
12.1 Semisimplicity	46
12.2 Equidistribution	47

1 September 11: Statements of the Weil Conjectures

This talk was given by Ari Krishna and Sophie Zhu at MIT for the STAGE seminar.

1.1 Some History

For today, X will be a smooth proper variety over a finite field \mathbb{F}_q . Let's give a statement of the Weil conjectures in the spirit of counting points.

Conjecture 1 (Weil). Fix a finite field \mathbb{F}_q .

- (a) Fix a scheme X of finite type over a field \mathbb{F}_q . Then there are algebraic integers $\{\alpha_1, \dots, \alpha_r\}$ and $\{\beta_1, \dots, \beta_s\}$ such that

$$\#X(\mathbb{F}_{q^n}) = (\alpha_1^n + \dots + \alpha_r^n) - (\beta_1^n + \dots + \beta_s^n)$$

for all $n \geq 0$.

- (b) Rationality: suppose further that X is proper of equidimension d . Then we can arrange these algebraic integers as

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{2d} (-1)^i \left(\sum_{j=0}^{b_i} \alpha_{ij}^n \right).$$

- (c) Poincaré duality: with X proper, the multi-sets $\{\alpha_{2d-i,j} : 1 \leq j \leq b_i\}$ and $\{q^d/\alpha_{ij} : 1 \leq j \leq b_i\}$ agree.

- (d) Riemann hypothesis: with X proper, $|\alpha_{ij}| = q^{i/2}$ for all i and j .

- (e) Betti numbers: with X proper, if X admits an integral model \mathcal{X} over some subring $R \subseteq \mathbb{C}$, then b_i is the i th Betti number of $\mathcal{X}(\mathbb{C})$.

The history of these conjectures is long and fraught.

- In the 1930s, Artin, Hasse, and Schmidt proved everything but the Riemann hypothesis for curves, and they proved the Riemann hypothesis for curves of genus at most 1.
- In 1948, Weil proved the Weil conjectures for curves of any genus. This arose by combining two observations: first, counting $\#X(\mathbb{F}_{q^n})$ should equal the number of fixed points of F^n , and second, these counts could be understood in terms of intersection theory with the graph of the Frobenius.
- In 1949, Weil proved the Riemann hypothesis for other varieties, namely certain Fermat varieties. At this point, the conjectures were finally stated.
- In the 1950s, Grothendieck and many others developed the theory of étale cohomology. By rather formal arguments, this proves everything but the Riemann hypothesis.
- In 1974, Deligne finishes his first proof of the Weil conjectures.
- In 1980, Deligne strengthens his proof of the Weil conjectures.

1.2 ζ -Functions

The Weil conjectures admit an important reformulation in terms of ζ -functions. Let's begin with the classical ζ -function.

Definition 2. The Riemann ζ -function $\zeta(s)$ is defined as the analytic continuation of the series

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The Riemann ζ -function admits the following properties.

- Euler product: one can write $\zeta(s)$ as a product

$$\zeta(s) = \prod_{\text{prime } p} \frac{1}{1 - p^{-s}}.$$

- Continuation: there is a meromorphic continuation to the plane, and it has only a simple pole at $s = 1$.
- Functional equation: upon completing the ζ -function as

$$\xi(s) := (s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}+1\right)\zeta(s),$$

we have the functional equation $\xi(s) = \xi(1-s)$.

- Riemann hypothesis: it is expected that the only zeroes of ζ occur at the negative integer integers and along $\{s \in \mathbb{C} : \operatorname{Re} s = 1/2\}$.

This generalizes as follows.

Definition 3. Fix a scheme X of finite type over \mathbb{Z} . Then we define the arithmetic ζ -function $\zeta_X(s)$ as

$$\zeta_X(s) := \prod_{\text{closed } \mathfrak{p} \in X} \frac{1}{1 - \#\kappa(\mathfrak{p})^{-s}}.$$

Example 4. The Euler product implies that $\zeta(s) = \zeta_{\operatorname{Spec} \mathbb{Z}}(s)$.

In order to relate this to point-counts, we produce the following definition.

Definition 5. Fix a scheme X of finite type over \mathbb{F}_q . Then we define

$$Z_X(T) := \exp \left(\sum_{n \geq 1} \#X(\mathbb{F}_q) \frac{T^n}{n} \right).$$

Remark 6. A direct calculation shows that $Z_X(q^{-s}) = \zeta_X(s)$.

We are now able to rewrite the Weil conjectures.

Conjecture 7 (Weil). Fix a finite field \mathbb{F}_q .

- (a) Fix a scheme X of finite type over \mathbb{F}_q . There are algebraic integers $\{\alpha_1, \dots, \alpha_r\}$ and $\{\beta_1, \dots, \beta_s\}$ such that

$$Z_X(T) \frac{(1 - \beta_1 T) \cdots (1 - \beta_s T)}{(1 - \alpha_1 T) \cdots (1 - \alpha_r T)}$$

for some algebraic integers α_i s and β_j s.

- (b) Rationality: let X be a smooth proper variety over \mathbb{F}_q of equidimension d . Then Z_X admits a factorization as

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

where $P_i \in 1 + T\mathbb{Z}[T]$ for each T .

- (c) Functional equation: with X proper, we have $Z_X(1/q^d T) = \pm q^{d\chi/2} T^\chi Z_X(T)$, where \pm is some sign, and χ is the Euler characteristic.

- (d) Riemann hypothesis: with X proper, we have $|\alpha_{ij}| = q^{i/2}$ for all i .

- (e) Betti numbers: with X proper, if X admits an integral model \mathcal{X} over some subring $R \subseteq \mathbb{C}$, then $\deg P_i$ is the i th Betti number of $\mathcal{X}(\mathbb{C})$.

These statements are shown to be equivalent by expanding out the definition of Z_X and taking logarithms.

1.3 Proof for Curves

We prove many of the Weil conjectures for curves. By keeping track of completions, we may as well assume that X is smooth and proper. Let's start with rationality.

Proposition 8. Fix a smooth proper curve X over \mathbb{F}_q . Then $Z_X(T)$ is a rational function of T .

Proof. The point is to write $Z_X(T)$ out in terms of divisors, which will allow us to use Riemann–Roch. Recall $Z_X(T)$ is the product

$$Z_X(T) = \prod_{\text{closed } p \in X} (1 - T^{\deg p})^{-1},$$

which then expands out into the sum

$$Z_X(T) = \sum_{\substack{D \in \text{Div } X \\ D \geq 0}} T^{\deg D},$$

where $D \geq 0$ means that D is effective. There are now two cases: if $\deg D \leq 2g - 2$, we will handle this separately. Otherwise, when $\deg D \geq 2g - 2$, then Riemann–Roch implies that the number of effective divisors with this degree is $(q^{d-g+1} - 1)/(q - 1)$. (Namely, Riemann–Roch allows one to compute the dimension of

the space of effective divisors with given degree; this is a finite vector space over \mathbb{F}_q , so we can now compute its size!) This finishes the proof upon rewriting this out as a geometric series. ■

Remark 9. By inputting more effort, one can use this proof to prove the functional equation. If one is careful, then one can achieve an expansion

$$Z_X(T) = \frac{f(T)}{(1-T)(1-qT)}$$

for some polynomial $f(T)$ of degree $2g$ with integral coefficients. Note that this includes the Betti numbers conjecture!

We now turn to the Riemann hypothesis, which of course is the hard part. This will depend on the following size bound.

Theorem 10 (Hasse–Weil). Fix a smooth proper curve C over a finite field \mathbb{F}_q . Then

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

Let's explain why this produces the Riemann hypothesis. Because we already have an expression

$$Z_X(T) = \frac{f(T)}{(1-T)(1-qT)},$$

we may factor $f(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$, and we note that we are trying to show $|\alpha_i| = \sqrt{q}$ for all i . By the functional equation, it is enough to show merely that $|\alpha_i| \leq \sqrt{q}$ for all i . Now, by definition of $Z_X(T)$, we see that

$$\sum_{n \geq 1} \#C(\mathbb{F}_{q^n}) T^n = \frac{d}{dT} \log Z_X(T),$$

which can be computed directly to be

$$\sum_{n \geq 1} \#C(\mathbb{F}_{q^n}) T^n = \sum_{i=1}^{2g} \left(\frac{-\alpha_i}{1 - \alpha_i T} + \frac{1}{1 - T} + \frac{1}{1 - qT} \right),$$

which after expanding out the geometric series becomes

$$\sum_{n \geq 1} \#C(\mathbb{F}_{q^n}) T^n = \sum_{n \geq 1} \left(q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n \right).$$

Thus, the Hasse–Weil bound shows that

$$\left| \sum_{i=1}^{2g} \alpha_i^n \right| \leq 2g\sqrt{q^n}.$$

Now, if $|\alpha_i| > \sqrt{q}$ for any i , then we can send $i \rightarrow \infty$ to achieve a contradiction because the left-hand side is too large.

1.4 Intersection Theory on a Surface

We will want to know something about intersection theory on a surface. We're in a talk, so we're allowed to just state the result we want.

Theorem 11. Fix a smooth projective surface X over an algebraically closed field k . Then there is a unique integral symmetric bilinear pairing (\cdot, \cdot) on $\text{Div } X$ such that any two transverse curves $C, C' \subseteq X$ have

$$(C, C') = \#(C \cap C').$$

There are many ways to the pairing (C, C') . The most geometric is to show that one can always wiggle one of the curves to make the intersection transverse.

For our bound, we need the following geometric input.

Theorem 12 (Hodge index). Fix a smooth projective surface X over an algebraically closed field k . Further, fix an ample line bundle H in $\text{Div } X$. If we are given a divisor D on X which is not linearly equivalent to 0 while $D \cdot H = 0$, then $D \cdot D < 0$.

Proof. We will prove this in steps.

1. Suppose instead that $D \cdot H > 0$ and $D^2 > 0$. Then we claim mD is linearly equivalent to an effective divisor for sufficiently large m . Well, because $D \cdot H > 0$, $(K_X - mD) \cdot H < 0$ for m sufficiently large, so $K_X - mD$ cannot be effective. Thus, $H^0(K_X - mD) = 0$, so $H^2(mD) = 0$ by Serre duality. However, by Riemann–Roch for surfaces, one has

$$h^0(mD) = h^1(mD) + \frac{1}{2}mD \cdot (mD - K_X) + \chi(\mathcal{O}_X),$$

which becomes positive for m large enough.

2. Now, suppose for the sake of contradiction that $D^2 > 0$. Then we can take $H' := D + nH$ to be ample for n large enough, from which we find $D \cdot H' = D^2 > 0$, so the lemma implies that mD is effective for m large enough, which contradicts having $D \cdot H = 0$.
3. Lastly, suppose for the sake of contradiction that $D^2 = 0$. Because $D \cdot H = 0$, we can find an effective divisor E such that $D \cdot E \neq 0$ while $E \cdot H = 0$. Now, consider $D' := nD + E$. One can calculate $(D')^2 > 0$ while $D' \cdot H = 0$, so we reduce to the previous step. ■

To apply this, we will want to understand ample divisors.

Theorem 13. Fix a divisor D on X . Then D is ample if and only if $D^2 > 0$ and $D \cdot C > 0$ for all irreducible curves C on X .

Here is how this is applied.

Theorem 14. Let $X = C \times C'$ where C and C' are smooth projective curves. Set $\ell := C \times \text{pt}$ and $m := \{\text{pt}\} \times C'$. Then for any divisor D , we have

$$D^2 \leq 2(D \cdot \ell)(D \cdot m).$$

Proof. As a lemma, we claim that if H is ample, then

$$(D^2) \cdot (H^2) \leq (D \cdot H)^2.$$

For this, one uses the Hodge index theorem on $E := (H^2)D - (H \cdot D)H$, from which one can calculate $E^2 < 0$. Thus, as long as $D \neq 0$, we get $(D^2)(H^2) - (D \cdot H)^2 < 0$; in all cases, we get the inequality.

Now, by Theorem 13, the divisor $H := \ell + m$ is ample. Applying the above argument with D' defined as

$$D' = (H^2)(E^2)D - (E^2)(D \cdot H)H - (H^2)(D \cdot E)E$$

where $E := \ell - m$. ■

We are now ready to prove the Hasse–Weil bound. We will do intersection theory on the surface $X := C \times C$. Let $\Delta \subseteq X$ be the diagonal, and let $\Gamma \subseteq X$ be the graph. Then $\#C(\mathbb{F}_q) = (\Delta \cdot \Gamma)$, which is what we want to bound. Here are our steps.

1. We claim $\Delta^2 = (2 - 2g)$. By the adjunction formula (note $\Delta \cong C$), we see

$$2g - 2 = \Delta^2 + \Delta \cdot K_X.$$

However, one can expand out K_X as $\text{pr}_1^*C + \text{pr}_2^*C$, which each have intersection number $2g - 2$ with Δ by using the adjunction formula, so the result follows.

2. We claim $\Gamma^2 = q(2 - 2g)$. By the adjunction formula (note $\Gamma \cong C$), we see

$$2g - 2 = \Gamma^2 + \Gamma \cdot K_X.$$

After doing the same expansion of K_X , one calculates that $\Gamma \cdot \text{pr}_1^*K_C = q(2g - 2)$ and $\Gamma \cdot \text{pr}_2^*K_C = 2g - 2$ by using the adjunction formula.

3. We now apply Theorem 14 to $X = C \times C$. Take large integers r and s , and set $D := r\Gamma + s\Delta$. Then $D \cdot \ell = rq + s$ and $D \cdot m = r + s$. From Theorem 14, one calculates that

$$|N - (q + 1)| \leq g \left(\frac{rg}{s} + \frac{s}{r} \right),$$

so the result follows by sending $\frac{r}{s} \rightarrow \frac{1}{\sqrt{q}}$.

2 September 18th: The Étale Site

This talk was given by Yutong Chen for the STAGE seminar at MIT.

2.1 Étale Morphisms

We will be interested in étale morphisms today. Intuitively, they are supposed to be the algebro-geometric version of a covering space in topology. Here is the easiest definition.

Definition 15 (étale). A morphism $f: X \rightarrow S$ of schemes is étale if and only if it is locally of finite presentation, flat, and unramified.

While locally of finite presentation and flatness are fairly common notions, we should define what it means for a morphism to be unramified. We will define this in steps.

Definition 16 (unramified). Fix an extension $A \subseteq B$ of discrete valuation rings with uniformizers π_A and π_B , respectively. Then $A \subseteq B$ is unramified if and only if $(\pi_B) = \pi_A \cdot B$ and the extension of residue fields is separable.

Definition 17 (unramified). Fix a map $f: A \subseteq B$ of local rings. Then f is unramified if and only if $f(\mathfrak{m}_A) = \mathfrak{m}_B$ and the field extension

$$A/\mathfrak{m}_A \rightarrow B/\mathfrak{m}_B$$

is separable.

Definition 18 (unramified). Fix a morphism $f: X \rightarrow S$ of schemes. Then f is unramified if and only if the local maps

$$\mathcal{O}_{S,f(x)} \rightarrow \mathcal{O}_{X,x}$$

are unramified for all $x \in X$.

Example 19. Open and closed immersions are unramified.

Non-Example 20. Consider the squaring map $\mathbb{A}_k^1 \rightarrow \mathbb{A}_k^1$ given by the ring map $k[t] \rightarrow k[t^2]$ defined by $t \mapsto t^2$. Then this map is not ramified at 0. Indeed, this map is locally given by

$$k[t^2]_{(t^2)} \rightarrow k[t]_{(t)},$$

but the maximal ideal fails to go to the maximal ideal.

There are many ways to think about étale morphisms.

Definition 21 (étale). A morphism $f: X \rightarrow S$ is étale if and only if it is smooth of relative dimension 0.

Here is one version of smoothness which is fairly hands-on.

Definition 22 (smooth). Fix a morphism $f: X \rightarrow S$. Given $x \in X$, we say that f is smooth at x if and only if the morphism locally looks like

$$\text{Spec } \frac{A[t_1, \dots, t_n]}{(g_{r+1}, \dots, g_n)} \rightarrow \text{Spec } A$$

and the corresponding Jacobian matrix has full rank $n - r$. We may also say that f is smooth of relative dimension r in this situation.

Of course, there are also many ways to define smoothness. Here is another useful criterion.

Proposition 23. Fix a flat morphism $f: X \rightarrow S$ of irreducible varieties over a field k , and set $r := \dim X - \dim S$. Then f is smooth of relative dimension r if and only if $\Omega_{X/S}$ is locally free of rank r .

Here are a few more ways to work with the yoga of étale morphisms.

Proposition 24. Fix a ring A , an extension $B = A[t]/(p)$ where $p \in A[t]$ is monic, and a localization $C = B[q^{-1}]$ for some q . If $p'(t) \in C^\times$, then the natural map $\text{Spec } C \rightarrow \text{Spec } A$.

We will not prove this (all of these proofs are horribly annoying), but we will content ourselves with an example.

Example 25. Fix $A := k[x]$ and $B := k[x, y]/(y^2 - x(x-1)(x+1))$. Then $\text{Spec } B \rightarrow \text{Spec } A$ is basically the projection from an elliptic curve to the affine line, so we expect to have some ramification at $(0, 0)$, $(1, 0)$, and $(-1, 0)$. Accordingly, if we localize out by $x^3 - x$, then we see that the map $\text{Spec } C \rightarrow \text{Spec } A$ is successfully étale, which can be checked because the derivative of $p(y) = y^2 - (x^3 - x)$ is in C^\times .

Remark 26. It turns out that all étale morphisms can locally be factored like Proposition 24.

Proposition 27. Fix a smooth morphism $f: X \rightarrow S$ of relative dimension r at a point $x \in X$. Further, fix some local functions $g_1, \dots, g_r \in \mathcal{O}_{X,x}$. Then the following are equivalent.

- (i) The elements dg_1, \dots, dg_r form a local basis for $\Omega_{X/S} \otimes k(x)$.
- (ii) The elements g_1, \dots, g_r extend to an open neighborhood U of x such that $(g_1, \dots, g_r): U \rightarrow \mathbb{A}_S^r$ is étale.

Remark 28. Property (i) is relatively easy to satisfy, so we know that such functions surely exist.

Remark 29. The point of (ii) is that f now factors as

$$X \supseteq U \rightarrow \mathbb{A}_S^r \rightarrow S,$$

where the map $U \rightarrow \mathbb{A}_S^r$ is étale. Thus, smooth morphisms are “just” projections up to an étale map.

2.2 The Fundamental Group

Continuing with our intuition that étale morphisms are covering spaces, we now try to define a fundamental group. It is difficult to make sense of paths in algebraic geometry, so instead we will use covering spaces. Here is the construction that we will try to generalize.

Example 30. For a nice topological space X (e.g., a manifold) with a basepoint $x \in X$, then there is a natural “fiber” functor

$$\text{Fib}_x: \text{Cover}(X) \rightarrow \text{Set}$$

from the category of covering spaces of X to sets given by sending $p: Y \rightarrow X$ to the fiber $p^{-1}(\{x\})$. By a path-lifting argument, one shows that

$$\pi_1(X, x) = \text{Aut}(\text{Fib}_x).$$

(In particular, path-lifting describes an action of $\pi_1(X, x)$ on all fibers in a compatible way.) We remark that this allows us to upgrade the fiber functor into an equivalence

$$\text{Fib}_x: \text{Cover}(X) \rightarrow \text{Set}(\pi_1(X, x)).$$

Remark 31. Topology is aided by the existence of a universal cover. For example, one has a universal cover of S^1 given by $\mathbb{R} \rightarrow S^1$, but this covering space fails to be finite; similarly, the universal cover of \mathbb{C}^\times is the exponential map $\exp: \mathbb{C} \rightarrow \mathbb{C}^\times$, which is not algebraic. Algebra is going to have some trouble producing coverings which are not finite (or algebraic), so we will have to content ourselves with some finite quotients.

Accordingly, we find that we are contenting ourselves to work with finite covering spaces, which amounts to working with finite étale covers.

Definition 32 (étale fundamental group). Fix a scheme X and a geometric point $\bar{x} \hookrightarrow X$, and consider the corresponding category $\text{Fin}\acute{\text{E}}\text{t}(X)$ of finite étale covers of X . Then we define the étale fundamental group $\pi_1(X, \bar{x})$ to be the automorphism group of the fiber functor

$$\text{Fib}_{\bar{x}}: \text{Fin}\acute{\text{E}}\text{t}(X) \rightarrow \text{Set}$$

given by sending the cover $p: Y \rightarrow X$ to the covering to the fiber $Y \times_p \bar{x}$.

Remark 33. As in the topological case, one finds that $\text{Fib}_{\bar{x}}$ upgrades to an equivalence

$$\text{Fib}_{\bar{x}}: \text{Fin}\acute{\text{E}}\text{t}(X) \rightarrow \text{Set}(\pi_1(X, \bar{x})).$$

As a sanity check, we note the following comparison theorem.

Theorem 34. Fix an irreducible variety X over \mathbb{C} . Then $Y \mapsto Y(\mathbb{C})$ upgrades to an equivalence of categories between the finite étale covers of X and the finite covers of $X(\mathbb{C})$.

Example 35. Consider $X = \mathbb{C}[x, x^{-1}]$ so that $X(\mathbb{C}) = \mathbb{C}^\times$. Then we see that $\pi_1^{\text{ét}}(X, \bar{1})$ will be $\widehat{\mathbb{Z}}$ because it is the colimit of the automorphism groups of the finite covers of \mathbb{C}^\times .

But now that we can do algebraic geometry, we can add in some arithmetic information.

Example 36. Consider the point $X = \text{Spec } k$ and an algebraic closure $\bar{x} = \text{Spec } \bar{k}$. Then a finite étale cover $Y \rightarrow X$ will be a finite disjoint union of points. To describe our category, we are allowed to work with just the connected covers of X , which amounts to making Y a point, so we may write $Y = \text{Spec } L$. In order for the map $Y \rightarrow X$ to be an étale cover, it is equivalent to ask for the induced field extension $k \subseteq L$ to be finite and separable. The fiber of such an L is given by

$$(Y \times \bar{x})(\bar{k}) = \text{Spec}(L \otimes \bar{k})(\bar{k}) = \text{Hom}_k(L, \bar{k}).$$

Thus, $\text{FÉt}(X)$ amounts to the category of finite separable extensions of k , and it is not hard to see that the automorphism group is simply $\text{Gal}(\bar{k}/k)$.

2.3 Grothendieck Topologies

The point of a Grothendieck topology is to recognize that what makes a topology important is not its open sets but instead the notion of covers. Thus, to specify a Grothendieck topology, we will try to specify the covers and make do with that.

Definition 37 (Grothendieck topology). Fix a category \mathcal{C} closed under finite products. A *Grothendieck topology* on \mathcal{C} is a collection of families \mathcal{T} of the form $\{f_i: U_i \rightarrow U\}_i$ and satisfying the following.

- (a) Isomorphisms: the family \mathcal{T} contains all isomorphisms.
- (b) Refinement: given a covering $\{U_i \rightarrow U\}_i$ in \mathcal{T} and some coverings $\{V_{ij} \rightarrow U_i\}_{j,i}$, then the composite $\{V_{ij} \rightarrow U_i \rightarrow U\}_{i,j}$ continues to be in \mathcal{T} .
- (c) Pullback: given a covering $\{U_i \rightarrow U\}_i$ in \mathcal{T} and some object V with a map $V \rightarrow U$, then the pullback $\{U_i \times_U V \rightarrow V\}_i$ is in \mathcal{T} .

In this situation, the pair $(\mathcal{C}, \mathcal{T})$ is a site.

Here is the motivating example.

Example 38 (Zariski site). If X is a topological space, then we can let \mathcal{C} be the category of open sets in X with morphisms given by inclusion. We can endow \mathcal{C} with the structure of a Grothendieck topology by letting the covers simply be the open covers. If X is a scheme, then this site is called the Zariski site.

Here is the site for today.

Definition 39 (small étale site). Fix a scheme X , and consider the category $\text{Ét}(X)$ of all étale covers of X . Then we endow $\text{Ét}(X)$ with the structure of a Grothendieck topology by saying that a collection of morphisms $\{U_i \rightarrow U\}_i$ is a covering if and only if $\bigsqcup_i U_i \rightarrow U$ is surjective. This is called the (small) étale site and is denoted $X_{\text{ét}}$.

Remark 40. It turns out that a morphism of étale covers of X is automatically étale. This can be proven using the usual techniques of cancellation.

Remark 41. By replacing the word étale with other adjectives, we also have an fppf site and fpqc site. We note that the Zariski site has the same definition where étale is replaced with open embeddings.

As usual, once we have an object, we want some morphisms.

Definition 42 (continuous). A *continuous map* $F: (\mathcal{C}', \mathcal{T}') \rightarrow (\mathcal{C}, \mathcal{T})$ is the data of a functor $F: \mathcal{C} \rightarrow \mathcal{C}'$ satisfying the following.

- (a) For any covering $\{U_i \rightarrow U\}_i$ in \mathcal{T} , we require that $\{FU_i \rightarrow FU\}_i$ to be in \mathcal{T}' .
- (b) Given a covering $\{U_i \rightarrow U\}_i$ in \mathcal{T} and a map $V \rightarrow U$, then we require that $F(V \times_U U_i) \rightarrow FV \times_{FU} FU_i$ to be an isomorphism.

Remark 43. If $f: X' \rightarrow X$ is a continuous map of topological spaces, then taking the pre-image induces a functor of the categories of open sets, and one can see directly that taking the pre-image produces a continuous map of the Grothendieck topologies.

Remark 44. For any scheme X , there is a continuous map between the étale site

$$X_{\text{fpqc}} \rightarrow X_{\text{fppf}} \rightarrow X_{\text{ét}} \rightarrow X_{\text{Zar}}.$$

The point of having a notion of topology is that it lets us do sheaf theory.

Definition 45. Fix a Grothendieck topology on a category \mathcal{C} . Then a presheaf $\mathcal{F}: \mathcal{C}^{\text{op}} \rightarrow \text{Ab}$ is a *sheaf* if and only if the usual exact sequence

$$\mathcal{F}(U) \rightarrow \prod_i \mathcal{F}(U_i) \rightarrow \prod_{i,j} \mathcal{F}(U_i \times_U U_j)$$

is exact for all covers $\{U_i \rightarrow U\}_i$.

Example 46. A sheaf on the Zariski site is the usual notion of sheaf in scheme theory.

Remark 47. Because open embeddings are already étale, fppf, and fpqc, we see that a sheaf on any of these sites must be a Zariski sheaf as well.

Remark 48. Because the sites we care about are closed under arbitrary coproduct, it is enough to check it on coverings which look like $U' \rightarrow U$, though of course one cannot require either U' or U to be connected.

We have yet to construct any sheaves! Here is the usual way to do so.

Definition 49. Fix a scheme X . For any Zariski quasicoherent sheaf \mathcal{F} on X , we define the étale presheaf $\mathcal{F}_{\text{ét}}$ on $X_{\text{ét}}$ by sending the cover $p: U \rightarrow X$ to

$$\mathcal{F}_{\text{ét}}(U) := \text{Hom}(p^*\mathcal{O}_X, p^*\mathcal{F}).$$

Remark 50. It turns out that this construction produces a sheaf. Something similar works for the fppf sites and fpqc sites. Let's explain this for the fpqc site. Indeed, fix a fpqc morphism $p: S' \rightarrow S$, so we set $S' := S' \times_S S'$ with projection $q: S'' \rightarrow S$, and we need to check that the usual sequence

$$\mathcal{F}_{\text{fpqc}}(S) \rightarrow \mathcal{F}_{\text{fpqc}}(S') \rightarrow \mathcal{F}_{\text{fpqc}}(S'')$$

is exact. Accordingly, we see that we may as well replace \mathcal{F} with the pullback to S (so that $X = S$), and we have left to check that

$$\text{Hom}(\mathcal{O}_S, \mathcal{F}) \rightarrow \text{Hom}(\mathcal{O}_{S'}, p^*\mathcal{F}) \rightarrow \text{Hom}(\mathcal{O}_{S''}, q^*\mathcal{F})$$

is exact. Exactness now follows from some notion of descent.

The last remark we should make about sheaves on a site is that we can do sheafification.

Definition 51 (sheafification). Fix a site \mathcal{C} . Then there is a left adjoint to the forgetful functor $\text{Sh}(\mathcal{C}) \rightarrow \text{PSh}(\mathcal{C})$, which we call sheafification.

3 October 2: The Lefschetz Trace Formula

This talk was given by Arav Karighattam for the STAGE seminar at MIT.

3.1 The Tools

We are going to use ℓ -adic cohomology to prove all the Riemann conjectures, with the exception of the Riemann hypothesis. We will recall the statements as we get to them.

Let's recall our Chow groups.

Definition 52 (Chow group). Fix a variety X over a field k of equidimension d . Then we define the *Chow group* $\text{CH}^\bullet(X)$ as the graded ring, where $\text{CH}^i(X)$ contains the codimension- i cycles (up to rational equivalence). The product $[A] \cdot [B]$ is given by the intersection $[A \cup B]$, which makes sense when A and B are generically transverse, meaning that a generic point x in $A \cap B$ has $T_x A + T_x B = T_x X$.

As usual, we will not bother to show that this product makes sense, which requires some notion of the Moving lemma or a different approach.

Our main tool will be ℓ -adic cohomology.

Definition 53 (ℓ -adic cohomology). Fix a variety X over a field k . For a prime ℓ distinct from $\text{char } k$, we define ℓ -adic cohomology as

$$H_\ell^i(X) := \left(\lim_{\leftarrow} H^i(X_{k^{\text{sep}}}; \underline{\mathbb{Z}/\ell^\bullet \mathbb{Z}}) \right) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

This cohomology groups assemble into a graded commutative ring $H_\ell^\bullet(X)$, where the product is given by the cup product.

Remark 54. As usual, the cup product can be defined on the level of Čech cocycles.

It turns out that H_ℓ^\bullet assembles into a Weil cohomology theory with coefficients in \mathbb{Q}_ℓ . Let's quickly review what we are given.

- The cohomology groups H_ℓ^\bullet are supported in degrees $[0, 2 \dim X]$.

- There is a Künneth formula

$$H_\ell^\bullet(X \times Y) \cong H_\ell^\bullet(X) \otimes H_\ell^\bullet(Y)$$

induced by the projections.

- If X has equidimension d , then the cup product produces a perfect pairing

$$H_\ell^i(X) \times H_\ell^i(X)(d) \rightarrow H_\ell^{2d}(X)(d) \rightarrow \mathbb{Q}_\ell,$$

where the last map is a trace map.

- There is a cycle class map $\text{cl}_X : \text{CH}^i(X) \rightarrow H^{2i}(X)(i)$.

These data are subject to many compatibilities.

3.2 The Lefschetz Trace Formula

Here is our theorem.

Theorem 55. Fix a regular endomorphism $\varphi : X \rightarrow X$ of a smooth projective variety X of equidimension d over a field k . Then

$$(\Gamma_\varphi \cdot \Delta_X) = \sum_{r=0}^{2d} (-1)^r \text{tr}(\varphi^*; H_\ell^r(X)).$$

Here, Γ_φ is the graph of φ , Δ_X is the diagonal, so $(\Gamma_\varphi \cdot \Delta_X)$ should be thought of as the number of fixed points of φ (counted with the correct multiplicities).

Proof. This is purely formal from the construction of a Weil cohomology theory. It turns out that the intersection number $(\Gamma_\varphi \cdot \Delta_X)$ agrees with the scalar

$$\text{cl}_{X \times X}(\Gamma_\varphi \cdot \Delta) \in H^{4d}(X \times X)(2d),$$

where the target is identified with \mathbb{Q}_ℓ via Poincaré duality. By a coherence property, we see that we want to evaluate $\text{cl}_{X \times X}(\Gamma_\varphi) \cup \text{cl}_{X \times X}(\Delta)$.

Let's explain how to compute $\text{cl}_{X \times X}(\Gamma_\varphi)$, and then one can compute $\text{cl}_{X \times X}(\Delta)$ by setting $\varphi = \text{id}_X$. Well, for each degree r , fix a basis $\{e_{i,r}\}$ of $H_\ell^r(X)$, which then has a dual basis $\{f_{i,2d-r}\}$ of $H_\ell^{2d-r}(X)(d)$. We will take $e_{i,r} \cup f_{2d-i,r} = 1$ as our sign convention. The Künneth formula explains that $H^\bullet(X \times X)$ can be identified with $H^\bullet(X) \otimes H^\bullet(X)$, so we get to write

$$\text{cl}_{X \times X}(\Gamma_\varphi) = \sum_{i,r} a_{i,r} \boxtimes f_{i,2d-r}$$

for some coefficients $a_{i,r}$ which we would like to solve for. To do so, we note that

$$\text{cl}_{X \times X}(\Gamma_\varphi) \cup (1 \boxtimes e_{j,r}) = a_{j,r} \boxtimes e_{2d},$$

where there graded commutative signs cancel out after expanding out \boxtimes as a cup product. Thus,

$$\text{pr}_{1*}(\text{cl}_{X \times X}(\Gamma_\varphi) \cup (1 \boxtimes e_{j,r})) = a_{j,r}.$$

We can now collapse the left-hand side. Note $\Gamma_\varphi = (\text{id}_X, \varphi)_* 1_X$, so we can rewrite this as

$$a_{j,r} = \text{pr}_{1*}((\text{id}_X, \varphi)_* 1_X \cup \text{pr}_2^* e_{j,r}).$$

By the projection formula, this collapses to $\varphi^* e_{j,r}$, so

$$\text{cl}_{X \times X}(\Gamma_\varphi) = \sum_{i,r} \varphi^* e_{j,r} \boxtimes f_{i,2d-r}.$$

Plugging in $\varphi = \text{id}_X$, we see similarly that

$$\text{cl}_{X \times X}(\Delta_X) = \sum_{i,r} e_{j,r} \boxtimes f_{i,2d-r}.$$

This is also

$$\text{cl}_{X \times X}(\Delta_X) = \sum_{i,r} (-1)^r f_{i,2d-r} \boxtimes e_{j,r},$$

so $\text{cl}_{X \times X}(\Gamma_\varphi) \cup \text{cl}_{X \times X}(\Delta)$ is

$$\sum_{j,r} (-1)^r (\varphi^* e_{j,r} \cup f_{j,2d-r}) \boxtimes e_{2d}$$

even after keeping track of signs in the graded commutativity. Now, the sum over j of the piece in parentheses is exactly the trace of φ^* acting on a given basis of $H_\ell^i(X)$, so we conclude. ■

3.3 Some Weil Conjectures

Here is the main input to our proofs.

Proposition 56. Fix a smooth projective variety X of equidimension d over \mathbb{F}_q . Then

$$|X(\mathbb{F}_q)| = \sum_{r=0}^{2d} (-1)^r \text{tr}(\text{Frob}_q^*; H_\ell^r(X)).$$

Proof. Let φ be the Frobenius. By Theorem 55, we only need to show that $(\Gamma_\varphi \cdot \Delta_X)$ is in fact $|X(\mathbb{F}_q)|$. Certainly the fixed points of the Frobenius acting on $X(\overline{\mathbb{F}}_q)$ is precisely $X(\mathbb{F}_q)$, so it remains to see that our intersection is actually transverse. This is true because all tangent spaces of Γ_φ are horizontal (the derivative of x^q vanishes in \mathbb{F}_q) while tangent spaces of Δ_X are diagonal. ■

Corollary 57. Fix a smooth projective variety X of equidimension d over \mathbb{F}_q . Then

$$Z(X, T) = \exp \left(\sum_{n=1}^{\infty} X(\mathbb{F}_{q^n}) \frac{T^n}{n} \right) = \prod_{r=0}^{2d} \det(1 - \text{Frob}_q^* T; H^r(X))^{(-1)^{r+1}}.$$

Proof. We start with a linear algebraic fact. In general, if $\varphi: V \rightarrow V$ is a linear operator over a field k , then we claim

$$-\log \det(1 - \varphi T; V) \stackrel{?}{=} \sum_{n=1}^{\infty} \text{tr}(\varphi^n; V) \frac{T^n}{n}.$$

Combining this linear algebraic fact with Proposition 56 completes the argument.

To see the claim, note that both sides of the identities are additive in the pair (V, φ) , and the case of scalars c acting on a one-dimensional space amounts to the Taylor expansion of \log as $-\log(1 - \lambda T) = \sum_{n \geq 1} \lambda^n T^n / n$. To complete the proof, we note that the identity is insensitive to changing the base field, so we may base-change to the algebraic closure, diagonalize φ , and reduce to the case of scalars. ■

We will now have achieved rationality as soon as we can show that the polynomials

$$P_i(T) := \det(1 - \text{Frob}_q^* T; H^i(X))$$

live in $1 + T\mathbb{Z}[T]$. Certainly it is in $1 + T\mathbb{Q}_\ell[T]$, and the alternating product of these polynomials is Z and therefore is in $1 + T\mathbb{Z}[[T]]$, so one can make an argument that the P_i s must be in $1 + T\mathbb{Z}[T]$.

It remains to prove the functional equation. This follows from Poincaré duality. Indeed, $\text{Frob}_*\text{Frob}^* = q^d$ on cohomology, so

$$\begin{aligned} Z(X, q^{-d}T^{-1}) &= \prod_{r=0}^{2d} \det(1 - q^{-d}\text{Frob}^*T^{-1}; H^i(X))^{(-1)^{r+1}} \\ &= \prod_{r=0}^{2d} \det(1 - q^{-d}\text{Frob}_*T^{-1}; H^{2d-i}(X)(d))^{(-1)^{r+1}}. \end{aligned}$$

This can be unwound into the functional equation.

4 October 9: Constructible Sheaves, Base Change, and L -functions

This talk was given by Mikayel Mkrtchyan for the STAGE seminar at MIT.

4.1 Constructible Sheaves

For today, all schemes will be finite type and separated over a field. Unless otherwise stated, X_0 and \mathcal{F}_0 will be objects defined over a finite field \mathbb{F}_q , and X and \mathcal{F} will be their base-changes to the algebraic closure $\overline{\mathbb{F}}_q$. This convention also holds for other similar letters. While we're here, we fix our characteristic to be $p > 0$, and we choose a prime $\ell \neq p$. We work with the étale topology throughout.

Let's begin by stating some foundational results.

Theorem 58. Fix a smooth proper morphism $f: X \rightarrow Y$ of qcqs schemes. For any ℓ -adic local system \mathcal{L} , the pushforward $R^i f_* \mathcal{L}$ is a local system on Y .

Remark 59. The topological intuition is that a proper submersion $f: X \rightarrow Y$ of real manifolds is a locally trivial fibration, which is known as Ehresmann's lemma.

We may be interested in upgrading this, removing properness or smoothness. One no longer expects to get local systems from higher pushforwards: instead, we get constructible sheaves.

Definition 60. Fix a sheaf \mathcal{F} on X with finite stalks coprime to p . Then \mathcal{F} is *constructible* if and only if there is a Zariski locally closed disjoint union $X = \bigsqcup_i X_i$ such that $\mathcal{F}|_{X_i}$ is a local system for each i .

Example 61. If $i: Z \rightarrow X$ is a closed subset, then $i_* \underline{\mathbb{Z}/\ell\mathbb{Z}}$ is constructible.

Remark 62. We can also choose a stratification $\bigsqcup_i X_i$ to be some étale locally closed disjoint union. The point is that one can check if a sheaf is a local system after étale base change.

Here are some indications that we have given a good definition.

Theorem 63 (finitude). Fix a morphism $f: X \rightarrow Y$ of qcqs schemes. If \mathcal{F} is constructible on X , then $R^i f_* \mathcal{F}$ is constructible.

Theorem 64. Fix an open subset $j: U \rightarrow X$, and set $i: Z \rightarrow X$ to be the complement. Then the data of a constructible sheaf on X is equivalent to the data of a triple $(\mathcal{F}_Z, \mathcal{F}_U, f)$, where \mathcal{F}_Z is a constructible sheaf on Z , and \mathcal{F}_U is a constructible sheaf on U , and f is a map $\mathcal{F}_Z \rightarrow i^* j_* \mathcal{F}_U$.

Sketch. It is not hard to build the triple from \mathcal{F} by restricting to Z and U . Given a triple $(\mathcal{F}_Z, \mathcal{F}_U, f)$, surely we know what the stalks are, and f tells us how to glue. ■

Example 65. Fix a smooth curve X over \mathbb{C} , and choose a finite subset $Z \subseteq X$ of “cusps,” and let $U := X \setminus Z$ be its kernel. Then a constructible sheaf on X has equivalent data to a local system \mathcal{L} on U (which is equivalent to the data of a representation $\pi_1(U) \rightarrow \mathrm{GL}(L)$ for some given vector space L), a finite group V_z at each $z \in Z$, and the last map $f: \mathcal{F}_Z \rightarrow i^* j_* \mathcal{F}_U$ amounts to a map $V_z \rightarrow L^{I_z}$. To see this last map, we see that $i^* j_* \mathcal{L}$ is the colimit of $\mathcal{L}(U \setminus z)$ where U is an open neighborhood of z , but these sections turn out to be given by L^{I_z} via the Riemann–Hilbert correspondence. In particular, the maps $V_z \rightarrow L^{I_z}$ vanishing corresponds to adding skyscraper sheaves.

Example 66. Similarly, let X_0 be a smooth curve over \mathbb{F}_q , let $U_0 \subseteq X_0$ be a nonempty open subset, and set $Z_0 := X_0 \setminus U_0$. Then the data of a constructible sheaf on X_0 is equivalent to the data of a local system \mathcal{L} on U_0 (which is the data of a representation of $\pi_1^{\text{\'et}}(U)$ on some L), a representation of $\mathrm{Gal}(\bar{k}(z)/k(z))$ on some V_z for each $z \in Z_0$, and a map $V_z \rightarrow L^{I_z}$ for each z . Here, I_z is the inertia subgroup which is the kernel of $\pi_1^{\text{\'et}}(U, z) \rightarrow \mathrm{Gal}(\bar{k}(z)/k(z))$.

We are now allowed to make the following central definition.

Definition 67 (ℓ -adic sheaf). An ℓ -adic sheaf is a compatible system of constructible sheaves of constructible sheaves of $(\mathbb{Z}/\ell^\bullet\mathbb{Z})$ -modules. Here, the compatibility requires that the locally closed stratifications stabilize for higher powers of ℓ . We think about this as by taking inverse limits over the compatible systems.

Remark 68. The stalks of an ℓ -adic sheaf are \mathbb{Z}_ℓ -modules. We will frequently (and silently) make these \mathbb{Q}_ℓ -vector spaces.

4.2 Proper Base Change

Suppose we have a commutative square as follows.

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ f' \downarrow & & \downarrow f \\ Y' & \xrightarrow{g} & Y \end{array}$$

Given an ℓ -adic sheaf \mathcal{F} on X , then there is a base-change morphism

$$g^* f_* \mathcal{F} \rightarrow f'_*(g')^* \mathcal{F}$$

defined by using various adjunctions: note

$$\begin{aligned} \mathrm{Hom}(g^* f_* \mathcal{F}, f'_*(g')^* \mathcal{F}) &= \mathrm{Hom}(f_* \mathcal{F}, g_* f'_*(g')^* \mathcal{F}) \\ &= \mathrm{Hom}(f_* \mathcal{F}, f_* g'_*(g')^* \mathcal{F}) \\ &\supseteq f_* \mathrm{Hom}(\mathcal{F}, g'_*(g')^* \mathcal{F}), \end{aligned}$$

and the last set has a canonical adjunction map. Using something about δ -functors, one can upgrade our given map to a base change map

$$g^* \mathrm{R}^i f_* \mathcal{F} \rightarrow \mathrm{R}^i f'_*(g')^* \mathcal{F}.$$

These maps are in general not isomorphisms.

Example 69. Consider the pullback square

$$\begin{array}{ccc} \emptyset & \xrightarrow{g'} & \mathbb{G}_m \\ f' \downarrow & & \downarrow f \\ 0 & \xrightarrow{g} & \mathbb{A}^1 \end{array}$$

of intersections. Then one can compute that $g^* f_* \underline{\mathbb{Q}_\ell} = \underline{\mathbb{Q}_\ell}$, but $f'_*(g')^* \underline{\mathbb{Q}_\ell}$ vanishes.

However, in good situations, the result holds.

Theorem 70 (Proper base change). If the square

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ f' \downarrow & & \downarrow f \\ Y' & \xrightarrow{g} & Y \end{array}$$

is a pullback with f proper, then the map $g^* R^i f_* \mathcal{F} \rightarrow R^i f'_* g^* \mathcal{F}$ is an isomorphism.

One application is that we can make sense of cohomology with compact supports.

Definition 71. Fix a Zariski open embedding $j: U \rightarrow X$ and a sheaf \mathcal{F} on U . Then there is a functor $j_!: \text{Sh}(U) \rightarrow \text{Sh}(X)$ which is left adjoint to j^* . It is given by the sheafification of the presheaf sending some étale open $V \rightarrow X$ to

$$\begin{cases} f(V) & \text{if } V \text{ factors through } U, \\ 0 & \text{else.} \end{cases}$$

Remark 72. One can see that $j_!$ is exact: indeed, its stalks are identity in U and vanish outside U .

Remark 73. For a sheaf \mathcal{F} on X , we let $j: U \rightarrow X$ be an open embedding and let $i: Z \rightarrow X$ be the complement. Then we have a short exact sequence

$$0 \rightarrow j_! j^* \mathcal{F} \rightarrow \mathcal{F} \rightarrow i_* i^* \mathcal{F} \rightarrow 0.$$

One can check exactness on stalks.

Definition 74. Fix a morphism $f: X \rightarrow Y$ of separated schemes over a field k . Then we define the functor $f_!: \text{Sh}(X) \rightarrow \text{Sh}(Y)$ as follows. By a theorem of Nagata, f factors through some compactification $j: X \rightarrow \overline{X}$ where the induced map $\overline{f}: \overline{X} \rightarrow Y$ is proper. Then we define

$$R^i f_! \mathcal{F} := R^i \overline{f}_* (j_! \mathcal{F}).$$

If X is separated over a field k , then we can define $H_c^i(X; \mathcal{F})$ as $R^i p_! \mathcal{F}$ where $p: X \rightarrow \text{Spec } k$ is the structure morphism.

Remark 75. One can use Theorem 70 (and the Leray spectral sequence) to show that this definition is independent of j .

Remark 76. The functor $R^i f_!$ sends constructible sheaves to constructible sheaves.

Remark 77. Given any Cartesian square

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ f' \downarrow & & \downarrow f \\ Y' & \xrightarrow{g} & Y \end{array}$$

then the base change maps $g^* Rf_! \rightarrow R^i f'_!(g')^*$ will always be an isomorphism.

Remark 78. The functors $R^i f_!$ are not the derived functors of $f_!$.

4.3 *L*-Functions

We now settle into our conventions, where X_0 is a variety over $k := \mathbb{F}_q$, and \mathcal{F}_0 is a sheaf on X_0 . Then one finds that there are Galois actions on $H^i(X; \mathcal{F})$ and $H_c^i(X; \mathcal{F})$ as follows: for $\sigma \in \text{Gal}(\bar{k}/k)$, then we have a morphism $(\sigma \times \text{id}_{X_0}): X \rightarrow X$, so we induce a map

$$H^i(X; \mathcal{F}) \rightarrow H^i(X; (\sigma \times \text{id}_{X_0})^* \mathcal{F}) = H^i(X; \mathcal{F}),$$

where the last identification holds because \mathcal{F} started its life over k .

Notation 79. We let $\text{Frob}_{\text{arith}} \in \text{Gal}(\bar{k}/k)$ be the arithmetic Frobenius $x \mapsto x^{[k]}$, and we let Frob be the geometric Frobenius.

The geometric Frobenius is convenient because it provides the correct morphism on points.

For calculations later, it will be helpful to have *L*-functions of general sheaves.

Definition 80. Fix a constructible ℓ -adic sheaf \mathcal{F}_0 on X_0 over a finite field $k := \mathbb{F}_q$. Then we define the zeta function

$$Z(X_0; \mathcal{F}_0, T) := \prod_{\text{closed } x \in X_0} \frac{1}{\det(1 - \text{Frob}T^{\deg x}; \mathcal{F}_x)}.$$

Remark 81. A short calculation shows that

$$Z(X_0, \mathcal{F}_0; T) = \exp \left(\sum_{m \geq 1} \left(\sum_{x \in X_0(\mathbb{F}_{q^m})} \text{tr}(\text{Frob}_x; \mathcal{F}_x) \right) \frac{T^m}{m} \right).$$

Here, $\text{Frob}_x \in \text{Gal}(\bar{k(x)}/k(x))$ is the geometric Frobenius, and it acts on the stalk of \mathcal{F}_x by viewing the stalk as the pullback to the point.

Example 82. One can check that $\mathcal{F}_0 = \underline{\mathbb{Z}_\ell}$ recovers the usual zeta function.

One still has a rationality result.

Theorem 83 (Grothendieck–Lefschetz trace formula). Fix a constructible ℓ -adic sheaf \mathcal{F}_0 on X_0 over a finite field $k := \mathbb{F}_q$. Then

$$Z(X_0; \mathcal{F}_0, T) = \prod_{i=0}^{2 \dim X} \det(1 - \text{Frob}T; H_c^i(X; \mathcal{F}))^{(-1)^{i+1}}.$$

Remark 84. One can view this as a “global expression” for the “locally defined” Euler product.

The result becomes more memorable if we pass through the sheaf-function dictionary.

Definition 85. Fix a constructible ℓ -adic sheaf \mathcal{F}_0 on X_0 over a finite field $k := \mathbb{F}_q$. Then we define the function $G_{\mathcal{F}_0}: X_0(\mathbb{F}_{q^m}) \rightarrow \overline{\mathbb{Q}}_\ell$ by

$$G_{\mathcal{F}_0}(x) := \text{tr}(\text{Frob}_x; \mathcal{F}_x).$$

Remark 86. Note $G: \text{Sh}(X) \rightarrow \text{Fun}(X(\mathbb{F}_{q^m}), \overline{\mathbb{Q}}_\ell)$ factors through the Grothendieck group $K_0(\text{Sh}(X))$.

This gives a relative version of the trace formula.

Theorem 87 (Grothendieck–Lefschetz trace formula). Fix a morphism $f_0: X_0 \rightarrow Y_0$ and a sheaf \mathcal{F}_0 . Then the diagram

$$\begin{array}{ccc} K_0(\text{Sh}(X_0)) & \xrightarrow{G} & \text{Fun}(X_0(\mathbb{F}_{q^m}), \overline{\mathbb{Q}}_\ell) \\ \text{R}f_! \downarrow & & \downarrow f \\ K_0(\text{Sh}(Y_0)) & \xrightarrow{G} & \text{Fun}(Y_0(\mathbb{F}_{q^m}), \overline{\mathbb{Q}}_\ell) \end{array} \quad \begin{array}{ccc} \mathcal{F} & \xrightarrow{\quad} & g \\ \downarrow & & \downarrow \\ \sum_i (-1)^i \text{R}^i f_! \mathcal{F} & \xrightarrow{\quad} & y \mapsto \sum_{g(x)=y} g(x) \end{array}$$

commutes.

5 October 16: Katz's Proof of the Riemann Hypothesis for Curves

This talk was given by Jane Shi at MIT for the STAGE seminar.

5.1 Review

Kat'z idea is to “spread out” the Riemann hypothesis over a family of curves. More precisely, suppose that we already have the Riemann hypothesis for a given curve C_0 over \mathbb{F}_q . Then given a family of curves $f: X \rightarrow U$ where one fiber is C_0 , then we will be able to prove the Riemann hypothesis for the full family.

Let's begin by reviewing some ℓ -adic cohomology. Fix a scheme X of finite type over \mathbb{F}_q . Then we have a zeta function

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

We already know rationality, which tells us that if X is smooth proper of equidimension d , then it can be written as an alternating product. Here is our goal.

Theorem 88. Fix a smooth projective irreducible curve X_0 over \mathbb{F}_q of genus g . Then

$$Z(X, T) = \frac{P_1(T)}{(1-T)(1-qT)},$$

where $P_1(T)$ is a polynomial of degree $2g$, where all roots have absolute value $q^{1/2}$.

Remark 89. Previously, we showed that we can take $P_1(T)$ to be

$$\det \left(1 - T \text{Frob}; H^1(X_{\overline{\mathbb{F}}_q}; \overline{\mathbb{Q}}_\ell) \right).$$

Let's be more precise about our Frobenius polynomials.

- There is an arithmetic Frobenius σ_q , which is the generator of $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.
- The inverse of the arithmetic Frobenius σ_q is the geometric Frobenius F_q .
- For our variety X defined over \mathbb{F}_q , the base-change $X_{\bar{\mathbb{F}}_q}$ admits a Frobenius morphism acting on the $\text{Spec } \bar{\mathbb{F}}_q$ factor.
- Given a closed point $x: \text{Spec } k \rightarrow X$ of a variety X over k , there is an induced map

$$\pi_1(\text{Spec } k) \rightarrow \pi_1(X)$$

of étale fundamental groups. Accordingly, if $k = \mathbb{F}_q$, then the left-hand group is $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, so we can choose a (geometric) Frobenius element generating it (well-defined up to conjugacy). We will call this element Frob_x .

Remark 90. Given an ℓ -adic local system \mathcal{F} , we produce a representation

$$\pi_1(X) \rightarrow \text{GL}(\mathcal{F}_{\bar{x}})$$

of the fiber. The target is some finite-dimensional \mathbb{Q}_{ℓ} -vector space, so we are allowed to consider the action of our Frobenius Frob_x on this vector space.

Remark 91. In the sequel, we will have reason to work with non-constant coefficients. Namely, we will be working with a family $f: X \rightarrow U$ of curves, so the sheaf $R^i f_* \mathbb{Q}_{\ell}$ will be interesting to us. In particular, by the Proper base change theorem, we know that

$$(R^i f_* \mathbb{Q}_{\ell})_s = H^i(X_{s, \bar{\mathbb{F}}_q}; \mathbb{Q}_{\ell})$$

for any point $s \hookrightarrow X$.

Let's apply the previous remark. For our family $f: X \rightarrow U$, we see that

$$\begin{aligned} L(R^i f_* \mathbb{Q}_{\ell}; T) &= \prod_{\text{closed } p \in U} \det(1 - T^{\deg p} \text{Frob}_p; (R^i f_* \mathbb{Q}_{\ell})_s)^{-1} \\ &= \prod_{\text{closed } p \in U} \det(1 - T^{\deg p} F_q; H^i_{\text{ét}}(X_{p, \bar{\mathbb{F}}_q}; \mathbb{Q}_{\ell}))^{-1}. \end{aligned}$$

By the trace formula (and Poincaré duality), if U is an affine curve, one can alternatively write

$$L(\mathcal{F}; T) = \frac{\det(1 - TF_q; H^1_c(U; \mathcal{F}))}{\det(1 - TF_q; H^2_c(U; \mathcal{F}))},$$

but by Poincaré duality, this last denominator is simply

$$\det(1 - qTF_q; \mathcal{F}_{\pi_1^{\text{geo}}}),$$

where we are silently keeping track of some Tate twist (which turns the TF_q into qTF_q). The subscript $(-)^{\text{geo}}$ refers to co-invariants.

5.2 Reduction to a Single Curve

For our reduction, we will require the notion of purity. Throughout, the base U is a smooth affine geometrically connected curve.

Definition 92. Fix an embedding $\iota: \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$. For an ℓ -adic local system \mathcal{F} on U , we say that \mathcal{F} is ι -pure of weight w if and only if

$$|\alpha| = N p^{w/2}$$

for all closed points $p \in U$ and all eigenvalues α of the action of Frob_p on \mathcal{F}_p . We say that \mathcal{F} is ι -real if and only if the characteristic polynomial

$$\iota \det(1 - T \text{Frob}_p; \mathcal{F}_p)$$

has real coefficients for all closed points $p \in U$.

Remark 93. For a family $f: X \rightarrow U$ of curves, our local system $\mathcal{F} = R^i f_* \mathbb{Q}_\ell$ is ι -real (for any ι) by Lefschetz trace formula arguments.

Here is our main result.

Theorem 94. Fix an ι -real ℓ -adic local system \mathcal{F} on a smooth affine geometrically connected curve U . Suppose that every eigenvalue β of F_q acting on $(\mathcal{F}^{\otimes 2k})_{\pi_1^{\text{geo}}}$ (for every p and k) has $|\beta| \leq 1$. Then for every closed point p , every eigenvalue α of Frob_p acting on \mathcal{F}_p has eigenvalue $|\alpha| \leq 1$.

Proof. We compare Euler factors of the L -function L_{2k} of $\mathcal{F}^{\otimes 2k}$ as k gets large. The Euler factor "at p " is

$$L_{p,2k} := \det(1 - T^{\deg p} \text{Frob}_p; \mathcal{F}^{\otimes 2k})^{-1} = \exp \left(\sum_{n \geq 1} \text{tr}(\text{Frob}_p^n; \mathcal{F})^{2k} \frac{T^{n \deg p}}{n} \right).$$

By looking at the roots and using the fact that \mathcal{F} is ι -real, we see that this Euler factor has nonnegative real coefficients, meaning it lives in $1 + T \mathbb{R}_{\geq 0}[[T]]$. Thus, by multiplying our Euler factors together, we see that the power series $L_{p,2k}$ is bounded above by L_{2k} term-wise.

Now, the radius of convergence of the full L -function L can be read off of a calculation with $\mathcal{F}_{\pi_1^{\text{geo}}}$, which is where we may apply the hypothesis. In particular, the radius of convergence is bounded above by 1, so we find that the eigenvalues of Frob_p acting on $\mathcal{F}^{\otimes 2k}$ has absolute value bounded above by $q^{\deg p}$. Sending $k \rightarrow \infty$ completes the proof. ■

Corollary 95. Fix an ι -real ℓ -adic local system \mathcal{F} on a smooth affine geometrically connected curve U . If there is a closed point p on U such that the eigenvalues of Frob_p on \mathcal{F}_p have eigenvalue bounded by 1, then the same is true for all eigenvalues.

Sketch. The key idea is that F_q^d acts by Frob_p on $(\mathcal{F}^{\otimes 2k})_{\pi_1^{\text{geo}}}$. (Roughly speaking, Frobenius can be transported to different points because the action will only differ by something in π_1^{geo} .) The result then follows from the theorem. ■

In light of the corollary, it remains to prove the Riemann hypothesis for a well-behaved curve and living in some rather general families.

Lemma 96. Fix a genus $g \geq 1$, and choose two smooth projective geometrically connected curves C_0 and C_1 over \mathbb{F}_q . After a field extension, there exists a smooth affine geometrically connected curve U and a family $f: C \rightarrow U$ so that C_0 and C_1 are some fibers of f .

Sketch. For genus 1, choose some $N \geq 4$, and one can use the moduli space $Y(N)$ of a pair of an elliptic curve along with a point of order N . For large N , one finds that U is a curve, and we can use the universal elliptic curve on $Y(N)$.

Now, for genus $g > 1$, we recall (from Deligne and Mumford) that there is a moduli space H_g° classifying genus g quasiprojective smooth geometrically connected curves. We can get the required U by choosing a generic curve which goes through every \mathbb{F}_q -point. ■

Let's now explain how the Riemann hypothesis gets transferred between curves.

Proof of Theorem 88 from a single curve. Suppose we have the Riemann hypothesis for a single curve C_0 of genus g , and we want to move it to any other curve C_1 of genus g . Then we get an upper bound on the eigenvalues of the Frobenius on the full family U , which comes down to the required upper bound $|\alpha| < q^{1/2}$ of eigenvalues α for C_1 . To complete the proof, we know that $\alpha \mapsto q/\alpha$ should be an involution of the roots by the functional equation, so the equality is forced! ■

5.3 Computations on a Family of Curves

We will compute with the Fermat curves. Choose some d coprime to q , and we define the smooth projective Fermat curve

$$F_d: X^d + Y^d = Z^d.$$

The Weil conjectures in this case are due to Weil.

Theorem 97 (Weil). The Riemann hypothesis holds for F_d if $\gcd(d, q) = 1$.

Sketch. This is an explicit calculation with some character sums. Given two characters $\chi_1, \chi_2: \mathbb{F}_q^\times \rightarrow \mathbb{C}^\times$, we define their Jacobi sum as

$$J(\chi_1, \chi_2) := \sum_{a \in \mathbb{F}_q} \chi_1(a)\chi_2(1-a).$$

If both χ_1 and χ_2 are nontrivial, then one can calculate $|J(\chi_1, \chi_2)|^2 = \sqrt{q}$.

Now, to calculate $\#F_d(\mathbb{F}_{q^n})$, this amounts to calculating the solutions to $x^m + y^m = 1$ and adding some points at infinity. Counting solutions to $x^m + y^m = 1$ turns into a sum over Jacobi sums, which can then be compared to

$$\#F_d(\mathbb{F}_{q^n}) = 1 + q^n - \sum_{\alpha} \alpha^n,$$

where the sum is over the eigenvalues α of the Frobenius. ■

Now, the genus of F_d is $\binom{d-1}{2}$, so we have many remaining genera, for which we will take quotients.

Remark 98. Note that a non-constant map $C \rightarrow C'$ will have the Riemann hypothesis transfer from C to C' . Indeed, the Frobenius eigenvalues of C' are a subset of the Frobenius eigenvalues of C . For example, one can see this by splitting $\text{Jac } C = \text{Jac } C' \oplus B$ for some other abelian variety B . Then, upon taking Tate modules, we find that the Frobenius eigenvalues of C are precisely the Frobenius eigenvalues of C' along with the Frobenius eigenvalues of B .

Lemma 99. For any genus $g \geq 1$, there is a Fermat curve F_d (with $\gcd(d, q) = 1$) and a curve C of genus g along with a quotient map $F_d \rightarrow C$.

Proof. If $p \neq 2$, then use the hyperelliptic curves $y^2 = x^d + 1$, where we choose $d \in \{2g+1, 2g+2\}$ to avoid p . If $p = 2$, we can use the curves $y^2 - y + x^{2g+1}$. A short calculation shows that these quotients recover all genera. ■

5.4 Persistence of Purity

We close the seminar by stating the following result.

Theorem 100. Fix an ι -real ℓ -adic local system \mathcal{F} on some smooth affine geometrically connected curve U . Suppose that there is a closed point p for which every Frobenius eigenvalue of Frob_p acting on \mathcal{F}_p has absolute value equal to 1. Then this is true for all closed points on \mathcal{F} .

We will say more about this result next week. It upgrades Theorem 94.

6 October 23: The Riemann Hypothesis for Hypersurfaces

This talk was given by Leonid Gorodetskii at MIT for the STAGE seminar.

6.1 Spreading Out for Hypersurfaces

Today, we are giving Katz's proof of the Riemann hypothesis for hypersurfaces of \mathbb{P}^{n+1} . The general idea is to spread out from a single example using moduli spaces. Let $f: X \rightarrow U$ be a smooth proper family over \mathbb{F}_q . Then $R^i f_* \mathbb{Q}_\ell$ defines some local system on U , and one has

$$\det(1 - T \text{Frob}_u; R^i f_* \mathbb{Q}_\ell) = \det(1 - T \text{Frob}_{q^{\deg u}}; H^i(X_u; \mathbb{Q}_\ell)),$$

where u is a closed point of U . We called this polynomial $P_i(X_u, T)$. With U a curve, we already know that P_0 and P_2 live in $1 + \mathbb{Z}[T]$, so the known rationality results imply that $P_1(X_u, T)$ is in $1 + \mathbb{Z}[T]$ as well.

Corollary 101. Fix everything as above. Then $R^i f_* \mathbb{Q}_\ell$ is real.

Lemma 102. Fix everything as above. Then the following are equivalent.

- (i) The Riemann hypothesis holds for X_u .
- (ii) $H^i(X_u; \mathbb{Q}_\ell)$ is pure of weight i .
- (iii) $R^i f_* \mathbb{Q}_\ell$ is pure of weight i at u .

Proof. Unwind the definitions of purity. ■

Our key spreading our result is the following.

Theorem 103 (Persistence of purity). Fix a smooth affine geometrically connected curve U over \mathbb{F}_q , and let \mathcal{F} be a real ℓ -adic local system on U . Then the following are equivalent.

- (i) The ℓ -adic local system \mathcal{F} is pure of weight $w \in \frac{1}{2}\mathbb{Z}$ at some point u .
- (ii) The ℓ -adic local system \mathcal{F} is pure of weight $w \in \frac{1}{2}\mathbb{Z}$ at all points u .

Sketch. By twisting, we may assume that $w = 0$. More precisely, we use the Tate twists $\mathbb{Q}_\ell(i)$, which are the ℓ -adic local systems in which the action by Frob_q in the étale fundamental group is given by q^{-i} . For example, we see that $\mathbb{Q}_\ell(i)$ is pure of weight $-2i$.¹ The result now follows from Theorem 94 and some careful duality. ■

In order to work with hypersurfaces, we need to know something about their cohomology. Here is the cohomology of projective space.

¹ Technically, we may need some half-integer twists, which requires us to consider field extensions of \mathbb{Q}_ℓ . This causes no problems as soon as we suitably generalize our definition of ℓ -adic system.

Theorem 104. Fix some $n \geq 0$. Then

$$H^i(\mathbb{P}^n; \mathbb{Q}_\ell) = \begin{cases} 0 & \text{if } i \text{ is odd,} \\ \mathbb{Q}_\ell(-i/2) & \text{if } i \text{ is even.} \end{cases}$$

In particular, the Riemann hypothesis holds.

Sketch. Use the Gysin sequence on the decomposition $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$, and induct on n . Note that the statement has no content for $n = 0$, and we also already know it for $n = 1$. Approximately speaking, the given even-dimensional classes arise because the whole cohomology ring is generated by the hyperplane class in the image of the cycle class map $CH^1(\mathbb{P}^n) \rightarrow H^2(\mathbb{P}^n; \mathbb{Q}_\ell)(1)$. ■

Remark 105. To check that this makes sense, we note that it gives $Z(\mathbb{P}^n; T)$ is

$$\prod_{i=0}^n \frac{1}{\det(1 - T \text{Frob}_q; \mathbb{Q}_\ell(-i))} = \prod_{i=0}^n \frac{1}{1 - q^i T},$$

which can then be expanded by hand.

Now, by the weak Lefschetz theorem and Poincaré duality, we are able to say something about the cohomology of hypersurfaces as well.

Theorem 106. Fix a smooth hypersurface $X \subseteq \mathbb{P}^{n+1}$.

- (a) For $i \in \{0, 1, \dots, 2n\} \setminus \{n\}$, we have $H^i(X; \mathbb{Q}_\ell) = H^i(\mathbb{P}^{n+1}; \mathbb{Q}_\ell)$.
- (b) For $i = n$, we have $H^n(X; \mathbb{Q}_\ell) \supseteq H^n(\mathbb{P}^{n+1}; \mathbb{Q}_\ell)$.

Proof. Omitted. ■

The hard Lefschetz theorem (which we do not currently know for étale cohomology at our point in the theory) motivates the following definition.

Definition 107. Fix a hypersurface $X \subseteq \mathbb{P}^{n+1}$. Then

$$\text{Prim}^n(X) = \begin{cases} H^n(X; \mathbb{Q}_\ell) & \text{if } n \text{ is odd,} \\ H^n(X; \mathbb{Q}_\ell)/\mathcal{L}^{n/2} & \text{if } n \text{ is even,} \end{cases}$$

where \mathcal{L} is some class coming from a hyperplane class.

Lemma 108. Fix a hypersurface $X \subseteq \mathbb{P}^{n+1}$ over \mathbb{F}_q . Then the Riemann hypothesis holds for X if and only if $\text{Prim}^n(X)$ is pure of weight n .

Proof. Define

$$P(T) := \det(1 - T \text{Frob}_q; \text{Prim}^n(X)).$$

Tracking through the definitions, we see that $Z(X; T)$ is $P(T)Z(\mathbb{P}^n; T)$ if n is odd and is $P(T)^{-1}Z(\mathbb{P}^n; T)$ if n is even. The result now follows because we already have the Riemann hypothesis for \mathbb{P}^n . ■

Thus, here is our spreading out result.

Theorem 109. Suppose there is a smooth hypersurface $X_0 \subseteq \mathbb{P}^{n+1}$ of degree d over \mathbb{F}_p satisfying the Riemann hypothesis. Then the Riemann hypothesis holds for all smooth hypersurfaces $X \subseteq \mathbb{P}^{n+1}$ of degree d over \mathbb{F}_q for any power q of p .

Proof. Quickly, note that we may immediately upgrade the Riemann hypothesis from X_0 to $X_0 \otimes \mathbb{F}_q$ by computing some eigenvalues. Thus, we may assume that X_0 is defined over \mathbb{F}_q .

Now, choose another smooth hypersurface $X_1 \subseteq \mathbb{P}^{n+1}$ of degree d over \mathbb{F}_q . Smoothness allows us to say that X_0 is cut out by a single equation F_0 , and X_1 is smooth over F_1 . Then the equation

$$tF_1(x) + (1-t)F_0(x)$$

defines a family of hypersurfaces in \mathbb{P}^{n+1} over \mathbb{A}^1 . After removing finitely many points $t \in \mathbb{A}^1$, we may assume that this is a smooth family of smooth hypersurfaces over some affine curve $U \subseteq \mathbb{A}^1$. The result now follows from Theorem 103 applied to $\mathcal{F} := R^i f_* \overline{\mathbb{Q}}_\ell(n/2)$. (The algebraic closure is desired here in order to take a half-twist.) ■

6.2 A Single Example

We are now reduced to proving the Riemann hypothesis for a single hypersurface.

Lemma 110. Fix a smooth hypersurface $X \subseteq \mathbb{P}^{n+1}$ of degree d over \mathbb{F}_p . Then the Riemann hypothesis is true for X if and only if

$$\#X(\mathbb{F}_q) = \#\mathbb{P}^n(\mathbb{F}_q) + O_X(q^{n/2})$$

for all powers q of p .

Proof. By Lemma 108, we only have to check the eigenvalues in the primitive part, and by Poincaré duality, we are allowed to only check that the eigenvalues α satisfy $|\alpha| \leq q^{n/2}$. Because we can expand out the size of $\#X(\mathbb{F}_q)$ as sum of some powers of the eigenvalues, it is enough to consider the sum of all these eigenvalues (otherwise we get some domination), and the result follows. ■

Let's now begin with our calculation. Here are the hypersurfaces used by Katz.

- If $p \nmid d$, then we can take the Fermat hypersurface cut out by the equation $\sum_{i=1}^{n+2} x_i^d = 0$. This calculation is due to Weil.
- If $p \mid d$ and $d \geq 3$, then we can use the Gabber hypersurface $x_1^d + \sum_{i=1}^{n+1} x_i x_{i+1}^{d-1} = 0$.
- If $p = d = 2$ and n is odd, then it turns out that $\text{Prim}^n(X) = 0$, so there is nothing to check.
- Lastly, if $p = d = 2$ and $n = 2m$ is even, then we can use $\sum_{i=1}^{m+1} x_i x_{m+1+i} = 0$.

We will only do the calculation in the Fermat case because the other ones are more or the same. We proceed in steps. Set $N := n + 2$ for brevity.

1. Because $X \subseteq \mathbb{P}^{n+1}$, it should be cut out by a single polynomial $F(x) = 0$. Accordingly, let $X^{\text{aff}} \subseteq \mathbb{A}^N$ be cut out by this same polynomial F , and we see that

$$\#X^{\text{aff}}(\mathbb{F}_q) = 1 + (q - 1)\#X(\mathbb{F}_q).$$

Thus, it is now enough to show that

$$\#X^{\text{aff}}(\mathbb{F}_q) = q^{n+1} + O_{d,n}(q^{(n+2)/2}).$$

2. Define $V^*(\mathbb{F}_q) \subseteq X^{\text{aff}}(\mathbb{F}_q) \cap \mathbb{G}_m(\mathbb{F}_q)^N$ to have the nonzero solutions. We claim that it is enough to achieve

$$\#V^*(\mathbb{F}_q) \stackrel{?}{=} \frac{1}{q}(q-1)^N + O_{d,n}\left(q^{N/2}\right).$$

This is a matter of stratifying X^{aff} . Indeed, for a subset $S \subseteq \{1, 2, \dots, N\}$, let V_S^* be the solutions in $X^{\text{aff}}(\mathbb{F}_q)$ whose nonzero entries are exactly in S . Then by choosing what our nonzero entries should be, we calculate

$$\begin{aligned} \#X^{\text{aff}}(\mathbb{F}_q) &= \sum_{S \subseteq \{1, \dots, N\}} \#V_S^*(\mathbb{F}_q) \\ &\stackrel{*}{=} \sum_{S \subseteq \{1, \dots, N\}} \left(\frac{1}{q}(q-1)^{\#S} + O_d\left(q^{\#S/2}\right) \right) \\ &= \frac{1}{q} \sum_{S \subseteq \{1, \dots, N\}} (q-1)^{\#S} + O\left(q^{N/2}\right), \end{aligned}$$

where the last error term holds because the smaller error terms get smaller exponentially (even though there are an exponential number of them). Notably, we have applied the hypothesis at $\stackrel{*}{=}$. The result now follows by noticing that the last sum collapses to $((q-1)+1)^N$ by the binomial theorem.

Before continuing with the calculation, we recall some facts about characters.

Definition 111 (character). Fix a finite abelian group G . Then a *character* is a homomorphism $G \rightarrow \mathbb{C}^\times$. We let G^\vee denote the group of characters.

Remark 112. Using the classification of finite abelian groups, one can check that G and G^\vee have the same size. There is also a non-canonical isomorphism between G and G^\vee .

Remark 113. The restriction maps induce a natural isomorphism $(G \times H)^\vee \rightarrow G^\vee \times H^\vee$. The inverse is given by sending the pair (χ_G, χ_H) to the character $\chi_G \chi_H$.

Remark 114. Note that there are the dual identities

$$\frac{1}{\#G} \sum_{g \in G} \chi(g) = \begin{cases} 1 & \text{if } \chi = 1, \\ 0 & \text{else,} \end{cases} \quad \text{and} \quad \frac{1}{\#G} \sum_{\chi \in G^\vee} \chi(g) = \begin{cases} 1 & \text{if } g = 1, \\ 0 & \text{else.} \end{cases}$$

Example 115. Because \mathbb{F}_q^\times is cyclic, it is fairly easy to write down its multiplicative characters.

Example 116. For any $a \in \mathbb{F}_q$, there is an additive character $\psi_a : \mathbb{F}_q \rightarrow \mathbb{C}$ given by

$$\psi_a(t) := \exp\left(\frac{2\pi i}{p} \cdot \text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)\right).$$

One can check that these characters are distinct, so these give all the characters.

Our bounds will come from knowledge of Gauss sums.

Definition 117 (Gauss sum). Fix an additive character ψ_a and a multiplicative character χ of \mathbb{F}_q . Then we define

$$g(\chi; \psi_a) := \sum_{t \in \mathbb{F}_q^\times} \chi(t) \psi_a(t).$$

Remark 118. These are in some sense analogous to the function

$$\Gamma(z) = \int_{\mathbb{R}^+} t^z e^{-t} \frac{dt}{t}.$$

Roughly speaking, we are integrating an additive and multiplicative character together over a multiplicative group.

Remark 119. Provided $a \neq 0$, one can calculate

$$|g(\chi; \psi_a)|^2 = \begin{cases} q & \text{if } \chi \neq 1, \\ 1 & \text{if } \chi = 1. \end{cases}$$

This sort of fact is used in many proofs of quadratic reciprocity, where one frequently takes χ to be the Legendre symbol (and receives a "quadratic Gauss sum.")

We now continue with our calculation.

3. To ease our calculation, we let $\varphi: \mathbb{G}_m^N \rightarrow \mathbb{G}_m^N$ be the d th power map, and we let $\sigma: \mathbb{G}_m^N \rightarrow \mathbb{A}^1$ be the summing (i.e., trace) map. As such, V^* is the zero locus of $\sigma \circ \varphi$. Accordingly, note that we have an exact sequence

$$1 \rightarrow \ker \varphi \rightarrow \mathbb{G}_m^N \xrightarrow{\varphi} \mathbb{G}_m^N \operatorname{coker} \varphi \rightarrow 1,$$

so for example we see that $\#\ker \varphi(\mathbb{F}_q)$ is $\#\mu_d^N(\mathbb{F}_q) \leq d^N$ does not depend on q . We now see that

$$\#V^*(\mathbb{F}_q) = \#\ker \varphi(\mathbb{F}_q) \cdot \#\{t \in \mathbb{G}_m^N(\mathbb{F}_q) : t \in \operatorname{im} \varphi(\mathbb{F}_q) \text{ and } \sigma(t) = 0\}.$$

4. We use our character theory. By the orthogonality relations, we know that

$$1_{\sum t_i=0} = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \psi_a(t_1 + \cdots + t_N) \quad \text{and} \quad 1_{t \in \operatorname{im} \varphi} = \frac{1}{\#\operatorname{coker} \varphi(\mathbb{F}_q)} \sum_{\chi \in \operatorname{coker} \varphi(\mathbb{F}_q)^\vee} \chi(t).$$

Thus, by cancelling out the kernel and cokernel, we see that

$$\#V^*(\mathbb{F}_q) = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\chi \in \operatorname{coker} \varphi(\mathbb{F}_q)^\vee} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi_a(t_1 + \cdots + t_n).$$

For example, we see that the $a = 0$ succeeds at being nonzero only when χ is trivial, where we receive $\frac{1}{q}(q-1)^N$.

5. It remains to handle the values $a \neq 0$, for which we use Gauss sums. Note that a character χ on $\operatorname{coker} \varphi$ can be lifted to \mathbb{G}_m^N and therefore can be factored into N characters $\chi_1 \cdots \chi_N$. Thus, we may factor

$$\sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi_a(t) = \prod_{i=1}^N \underbrace{\sum_{t_i \in \mathbb{F}_q^\times} \chi_i(t_i) \psi_a(t_i)}_{g(\chi_i; \psi_a)},$$

so we see that the entire product has absolute value bounded by $q^{N/2}$ because $|g(\chi; \psi_a)| \leq q^{N/2}$.

6. We conclude. Plugging in the previous two steps yields

$$\left| \#V^*(\mathbb{F}_q) - \frac{1}{q}(q-1)^N \right| \leq \frac{1}{q} \underbrace{(q-1)}_a \cdot \underbrace{\#\operatorname{coker} \varphi(\mathbb{F}_q)}_\chi \cdot q^{N/2}.$$

The term $\frac{1}{q}(q-1)$ dies, and the size of $\operatorname{coker} \varphi(\mathbb{F}_q)$ is the size of $\ker \varphi(\mathbb{F}_q)$ is bounded independently of q . The total error term comes out to $q^{N/2}$, so we are done!

7 October 30: Deligne's Proof of Weil I and the Main Lemma

This talk was given by Mohit Hulse at MIT for the STAGE seminar. The term "main lemma" is due to Milne; Deligne only names a consequence as "the fundamental estimate."

7.1 The Étale Fundamental Group

For today, we fix a connected scheme X of finite type over a field k .

Definition 120. Fix a scheme X of finite type over a field k . For a geometric point $\bar{x} \hookrightarrow X$, we define the fiber functor $\omega_{\bar{x}}: \text{FÉt}(X) \rightarrow \text{Sets}$ by

$$\omega_x(Y) := Y_{\bar{x}}.$$

We define $\pi_1^{\text{ét}}(X, \bar{x})$ as the automorphism group of ω_x .

Remark 121. Once $\pi_1^{\text{ét}}(X, \bar{x})$ has been defined, we may upgrade $\omega_{\bar{x}}$ to a functor

$$\omega_x: \text{FÉt}(X) \rightarrow \text{Sets}(\pi_1^{\text{ét}}(X, \bar{x})),$$

and this latter functor turns out to be an equivalence.

The theory of the étale fundamental group proves the following "pro-representability" result.

Theorem 122. Fix a scheme X of finite type over a field k , and choose a geometric point $\bar{x} \hookrightarrow X$. There is a cofiltered sequence $\{X_i\}$ of finite étale covers of X such that

$$\omega_{\bar{x}} = \operatorname{colim}_i \operatorname{Hom}_X(X_i, -).$$

In fact, one can choose the covers $X_i \rightarrow X$ to be Galois.

Corollary 123. Fix a scheme X of finite type over a field k , and choose a geometric point $\bar{x} \hookrightarrow X$. There is a cofiltered sequence $\{X_i\}$ of finite étale covers of X such that

$$\pi_1(X, \bar{x}) = \lim_i \operatorname{Aut}_X(X_i).$$

Example 124. If X is the point $\operatorname{Spec} k$, then one can choose the X_i to be finite Galois extensions of k , so we find that $\pi_1^{\text{ét}}(X, \bar{x}) = \operatorname{Gal}(k^{\text{sep}}/k)$.

Example 125. If X is a smooth projective variety over \mathbb{C} , then we see that $\pi_1^{\text{ét}}(X, \bar{x})$ is the profinite completion of $\pi_1(X, x)$. For example, $X = \mathbb{G}_m$ admits covers $\mathbb{G}_m \rightarrow \mathbb{G}_m$ by $x \mapsto x^n$ (where $\operatorname{char} k \nmid n$), allowing us to compute $\pi_1(X, \bar{x}) = \widehat{\mathbb{Z}}$ when $\operatorname{char} k = 0$. This sort of process works for general Riemann surfaces because the finite étale covers of a Riemann surface all come from varieties.

The reason we care about the étale fundamental group is that it will allow us to understand local systems.

Notation 126. Fix a scheme X of finite type over a field k . Then $\operatorname{Loc}(X_{\text{ét}}, \text{FinSet})$ consists of the locally constant étale sheaves on X valued in finite sets. In other words, there is an étale covering $\{U_i\}$ of X so that the sheaf is constant when restricted to any of the given U_i .

Theorem 127. Fix a scheme X of finite type over a field k , and choose a geometric point $\bar{x} \hookrightarrow X$. Then the fiber functor

$$\text{Loc}(X_{\text{ét}}, \text{FinSet}) \rightarrow \text{FinSet}(\pi_1^{\text{ét}}(X, \bar{x}))$$

given by $\mathcal{F} \mapsto \mathcal{F}_{\bar{x}}$ is an equivalence, and any sheaf on the left-hand side is representable.

Sketch. The point is to choose a cover trivializing the sheaf, and then one can prove representability over X explicitly by finding some descent datum. ■

Of course, we would like a way to extend this to ℓ -adic sheaves, which we do as follows.

Notation 128. Fix a scheme X of finite type over a field k . Then $\text{Loc}(X_{\text{ét}}, \mathbb{Q}_\ell)$ consists of the locally constant ℓ -adic étale sheaves on X , meaning that they are valued in finite-dimensional \mathbb{Q}_ℓ -vector spaces.

Theorem 129. Fix a scheme X of finite type over a field k , and choose a geometric point $\bar{x} \hookrightarrow X$. Then the fiber functor

$$\text{Loc}(X_{\text{ét}}, \mathbb{Q}_\ell) \rightarrow \text{Rep}_{\mathbb{Q}_\ell}(\pi_1^{\text{ét}}(X, \bar{x}))$$

given by $\mathcal{F} \mapsto \mathcal{F}_{\bar{x}}$ is an equivalence.

Proof. Unwind to the previous theorem. ■

Remark 130. If the corresponding representation on the right-hand side does not factor through a finite quotient of $\pi_1^{\text{ét}}(X, \bar{x})$, then one does not expect to be able to find a single cover trivializing the entire ℓ -adic local system.

Of course, in this seminar, we are interested in computing cohomology, so we pick up a few results to do so.

Lemma 131. Fix a scheme X of finite type over a field k , and choose a geometric point $\bar{x} \hookrightarrow X$. Then for any locally constant ℓ -adic sheaf \mathcal{F} , we have

$$H^0(X; \mathcal{F}) \cong (\mathcal{F}_{\bar{x}})^{\pi_1^{\text{ét}}(X, \bar{x})}.$$

Sketch. There is nothing to do if \mathcal{F} is constant. If \mathcal{F} is non-constant, then we can locally pass to a Galois étale cover $Y \rightarrow X$ where it is constant, and then we can compute $H^0(X; \mathcal{F})$ via Čech cohomology to prove the result. ■

7.2 The Main Lemma

Recall the following definition.

Notation 132. Fix a scheme X of finite type over \mathbb{F}_q , and let \mathcal{F} be an ℓ -adic local system. Then we define

$$Z(\mathcal{F}_0; T) := \prod_{\text{closed } x \in X} \frac{1}{\det(1 - F_{x_0} T^{\deg x_0}; \mathcal{F}_0)}.$$

Earlier, we proved the following formula.

Theorem 133 (Lefschetz trace formula). Fix a scheme X of finite type over $k := \mathbb{F}_q$, and let \mathcal{F} be an ℓ -adic local system. Then

$$Z(\mathcal{F}_0; T) = \prod_{i \geq 0} \det(1 - \text{Frob}_q T; H_c^i(X_{\bar{k}}; \mathcal{F}))^{(-1)^{i+1}}.$$

Example 134. If X is an affine curve, then $H_c^0(X_{\bar{k}}; -)$ vanishes, so we only have to worry about $H_c^1(X_{\bar{k}}; -)$ and $H_c^2(X; -)$. By Poincaré duality, we can recover $H_c^2(X_{\bar{k}}; \mathcal{F})$ as $H^0(X_{\bar{k}}; \mathcal{F})$ and compute via Lemma 131.

For the main lemma, we recover the following definition.

Definition 135 (weight). Fix an ℓ -adic local system \mathcal{F} on a scheme X of finite type over \mathbb{F}_q . Then \mathcal{F} is of weight β if and only if, for each closed point $x \in X$, the eigenvalues of the Frobenius F_x acting on $\mathcal{F}_{\bar{x}}$ are algebraic numbers all of whose Galois conjugates have absolute value $q^{\beta/2}$.

Theorem 136 (Main lemma). Fix an ℓ -adic local system \mathcal{F} on an affine curve U of finite type over \mathbb{F}_q . Choose an integer β , and assume the following.

- (a) Symplectic: there is a perfect alternating pairing $\psi: \mathcal{F} \otimes \mathcal{F} \rightarrow \mathbb{Q}_{\ell}(-\beta)$.
- (b) Big monodromy: the image of $\pi_1(U_{\bar{\mathbb{F}}_q}, \bar{u})$ in $\text{GL}(\mathcal{F}_{\bar{u}})$ is open in $\text{Sp}(\mathcal{F}_{\bar{u}}; \psi)$ in the ℓ -adic topology for some geometric point \bar{u} .
- (c) Rationality: the characteristic polynomials of $F_{\bar{u}}$ acting on $\mathcal{F}_{\bar{u}}$ are rational for all geometric points.

Then \mathcal{F} has weight β .

Example 137. Fix a family $\pi: Y \rightarrow U$ of smooth projective hypersurfaces in \mathbb{P}^{d+1} , where d is odd. Then we will apply Theorem 136 with $\mathcal{F} := R^d \pi_* \mathbb{Q}_{\ell}$.

- (a) Poincaré duality provides a pairing $R^d \pi_* \mathbb{Q}_{\ell} \times R^d \pi_* \mathbb{Q}_{\ell} \rightarrow R^{2d} \pi_* \mathbb{Q}_{\ell} = \mathbb{Q}_{\ell}(-d)$. This is symplectic because d is odd.
- (b) Big monodromy turns out to be hard to check (and of course, it is not always true: one can take a constant family).
- (c) Rationality follows from known cases of the Weil conjectures: the cohomology of the fiber of $R^d \pi_* \mathbb{Q}_{\ell}$ can be computed via proper base change to be $H^d(Y_u; \mathbb{Q}_{\ell})$, which is known to be rational because the full zeta function is rational (and this is the only interesting cohomology group!).

The point is that having big monodromy proves the Riemann hypothesis.

Proof of Theorem 136. We proceed in steps.

1. We can use hypotheses (a) and (b) to produce an isomorphism

$$H_c^2(U_{\bar{k}}, \mathcal{F}^{\otimes 2k}) \rightarrow \mathbb{Q}_{\ell}(-k\beta - 1)^{\oplus N}$$

for some integer N . Indeed, we chain together the isomorphisms

$$\begin{aligned} H_c^2(U_{\bar{k}}, \mathcal{F}^{\otimes 2k}) &= H^0(U_{\bar{k}}, \mathcal{F}^{\vee \otimes 2k})^{\vee}(-1) \\ &= (\mathcal{F}_{\bar{u}}^{\vee \otimes 2k})^{\pi_1^{\text{\'et}}(U; \bar{u}), \vee}(-1), \end{aligned}$$

where we have used Poincaré duality in the first line. We may identify \mathcal{F} with its dual by (a), so we may ignore the dual. By the big monodromy result, we will reduce ourselves to understanding

$$\mathrm{Hom}_{\mathrm{Sp}(\mathcal{F}_u)}(\mathcal{F}^{\otimes 2k}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(k\beta)^{\oplus N},$$

for some N , which completes the proof after tracking through the various twists. (The isomorphism here follows from some representation theory: more or less, one can explicitly construct functionals on $\mathcal{F}_u^{\otimes 2k}$ to be of the form $x_1 \otimes \cdots \otimes x_{2k} \mapsto \psi(x_1, x_2) \cdots \psi(x_{2k-1}, x_{2k})$.) Thus, we see that the main point is to check that π_1 -invariants are G -invariants, where $G := \mathrm{Sp}(\mathcal{F}_u)$. Let H be the Zariski closure of the image of π_1 in G ; then π_1 -invariants are H -invariants because fixing a vector is an algebraic equation. However, $H \subseteq G$ contains an ℓ -adic open subgroup, so $\dim H = \dim G$, so $H = G$ follows because G is connected.

2. We apply Rankin's trick. Our two versions of $Z(\mathcal{F}; T)$ show that

$$\prod_{\text{closed } u \rightarrow U} \frac{1}{\det(1 - F_u T^{\deg u}; \mathcal{F}^{\otimes 2k})} = \frac{\det(1 - \mathrm{Frob}_q T; H_c^1(U; \mathcal{F}^{\otimes 2k}))}{(1 - q^{k\beta+1})^N},$$

where the denominator in the right-hand side is computed from the first step. Now, the left-hand side is assumed to live in $\mathbb{Q}((t))$ (which we can see in fact needs to have positive coefficients), so the right-hand side also lives in $\mathbb{Q}((t))$. Thus, the radius of convergence of the left-hand side is at most the radius of convergence of each factor in the product. However, the radius of convergence of the right-hand side is just $1/q^{k\beta+1}$, so we conclude that the eigenvalues α of the determinants on the left-hand side must have

$$\frac{1}{|\alpha|^{2k/\deg u}} \geq \frac{1}{q^{k\beta+1}}.$$

Sending $k \rightarrow \infty$ (which is Rankin's trick!) implies that $|\alpha| \leq q^{k\beta/2}$. Because \mathcal{F}_u is symplectic, we can run the same argument for the dual, so \mathcal{F}_u also has the eigenvalue q^β/α . The result follows from comparing the two resulting inequalities. ■

Remark 138. The above proof basically features no algebraic geometry.

7.3 Applications

We now use Theorem 136 to derive some estimates.

Lemma 139. Embed an affine curve U over \mathbb{F}_q as $j: U \hookrightarrow \mathbb{P}^1$, and let S be the complement. Further, fix an ℓ -adic local system \mathcal{F} on U . Then Poincaré duality induces a perfect pairing

$$H^1(\mathbb{P}^1; j_* \mathcal{F}^\vee) \otimes H^1(\mathbb{P}^1; j_* \mathcal{F}) \rightarrow \mathbb{Q}_\ell(-1).$$

Proof. There is a pairing already for $Rj_* \mathcal{F}^\vee$ and $j_* \mathcal{F}$, but the differences between $j_* \mathcal{F}$ and $j_! \mathcal{F}$ turns out to be cancelled out. ■

Corollary 140. Embed an affine curve U over \mathbb{F}_q as $j: U \hookrightarrow \mathbb{P}^1$, and let S be the complement.

- (a) Let α be an eigenvalue of $H^1(\mathbb{P}^1; j_! \mathcal{F})$. Then

$$|\alpha| \leq q^{\frac{\beta+1}{2} + \frac{1}{2}}.$$

- (b) Let α be an eigenvalue of $H^1(\mathbb{P}^1; j_* \mathcal{F})$. Then

$$q^{\frac{\beta+1}{2} - \frac{1}{2}} \leq |\alpha| \leq q^{\frac{\beta+1}{2} + \frac{1}{2}}.$$

Proof. For (a), we start by noting $H^1(\mathbb{P}^1; j_! \mathcal{F}) = H^1(U, \mathcal{F})$. The same sort of calculation as in the first step of Theorem 136 shows that our (inverse) zeta function is

$$\prod_{\substack{\text{closed } u \in U}} \det(1 - F_{u_0} T^{\deg u}; \mathcal{F}_u) = \frac{1}{\det(1 - \text{Frob}_q T; H_c^1(U; \mathcal{F}))}.$$

Now, the left-hand product converges absolutely if and only if the sum of the individual eigenvalues converges absolutely. The moral is that

$$\sum_{\alpha} q^{\beta \deg u / 2} |t|^{\deg u} < \infty,$$

where the sum is taken over all eigenvalues α of all closed points $u \in U$. Now, one can bound the number of closed points of $U \subseteq \mathbb{A}^1$ and bound the geometric series to achieve (a).

For (b), one uses the exact sequence

$$0 \rightarrow j_! \mathcal{F} \rightarrow j_* \mathcal{F} \rightarrow i_* i^* j_* \mathcal{F} \rightarrow 0,$$

where $i: S \hookrightarrow \mathbb{P}^1$ is the inclusion. The right-hand term is supported on a finite set, so its H^1 vanishes, so we achieve a surjection

$$H^1(\mathbb{P}^1; j_! \mathcal{F}) \twoheadrightarrow H^1(\mathbb{P}^1; j_* \mathcal{F}).$$

We now get use the bound in (a), and the other bound follows from duality. ■

8 November 6: Lefschetz Principles

This talk was given by Jack Miller at MIT for the STAGE seminar.

8.1 Fibrations, Diffeomorphically

We are (still) trying to show the Riemann hypothesis part of the Weil conjectures. As usual, the veracity of the Riemann hypothesis is insensitive to base-change of the base finite field. After some reductions, it turns out that it will be enough to handle the middle-dimension cohomology of a smooth projective even-dimensional varieties. As such, we will let $n+1$ be the dimension of some varieties to be chosen later, where $n = 2m+1$ is odd.

As in our previous cases of the Weil conjectures, we are on the hunt for many fibrations $X \rightarrow \mathbb{P}^1$. Such fibrations are the algebro-geometric version of finding some smooth submersions $M \rightarrow \mathbb{R}$. In the real analytic case, this amounts to the following result.

Theorem 141 (Ehresmann). If $f: M \rightarrow N$ is a smooth submersion of closed manifolds, then f is a locally trivial fibration.

Corollary 142. Fix a closed manifold M . Every smooth map $M \rightarrow \mathbb{R}$ admits a critical point.

Remark 143. Of course, is not hard to prove the corollary directly: a smooth map $M \rightarrow \mathbb{R}$ must admit a maximum, which is critical.

Corollary 144. Fix a closed manifold M . If $M \rightarrow S^1$ is a submersion, then M is diffeomorphic to a mapping torus.

Thus, admitting a submersion to a curve places strong requirements on M .

Here is the algebro-geometric version of this.

Theorem 145 (Ehresmann). If $f: Y \rightarrow S$ is smooth proper, and \mathcal{F} is a locally constant constructible étale sheaf on Y , then the higher pushforwards $R^p f_* \mathcal{F}$ are locally constant constructible.

However, the real analytic version tells us that we are going to need to allow some singularities for our fibrations. Let's explain the sort of singularities one finds in the diffeomorphic setting.

Theorem 146 (Morse's lemma). Fix a d -dimensional closed manifold M . Then there is an open subset $U \subseteq \text{Fun}(M, \mathbb{R})$ (using the C^2 topology) satisfying the following for each function in U .

- There are finitely many critical points, and at most one in each fiber.
- The critical points p are non-degenerate, and each bad fiber $f^{-1}(\{p\})$ looks like a conic of the form

$$0 = x_1^2 + \cdots + x_i^2 - x_{i+1}^2 - \cdots - x_d^2.$$

In other words, the Hessian is non-degenerate.

Remark 147. Picard and Lefschetz proved a variant of this for complex manifolds.

8.2 Lefschetz Pencils

Let's now try to find our fibrations in the algebro-geometric setting.

Definition 148. Fix a projective variety X , and let \mathcal{L} be a very ample line bundle on X inducing $X \hookrightarrow \mathbb{P}\Gamma(X, \mathcal{L})$. Then a pencil D of (X, \mathcal{L}) is a 1-parameter line of hyperplanes of $\mathbb{P}\Gamma(X, \mathcal{L})^\vee$; in other words, D is a map $\mathbb{P}^1 \rightarrow \mathbb{P}\Gamma(X, \mathcal{L})^\vee$.

Definition 149. Fix a projective variety X , and let \mathcal{L} be a very ample line bundle on X . The axis of a pencil $D: \mathbb{P}^1 \rightarrow \mathbb{P}\Gamma(X, \mathcal{L})^\vee$ is

$$A(D) := \bigcap_t D_t.$$

Remark 150. In fact, $A = D_0 \cap D_\infty$

Definition 151. Fix a projective variety X , and let \mathcal{L} be a very ample line bundle on X . Then a pencil $D: \mathbb{P}^1 \rightarrow \mathbb{P}\Gamma(X, \mathcal{L})^\vee$ is Lefschetz if and only if it satisfies the following.

- Transverse: A intersects D transversely.
- Smoothness: the intersections $X \cap D_t$ are nonsingular for all but finitely many t . Let $S \subseteq \mathbb{P}^1$ be the singular locus.
- For each $t \in S$, the singularities P in X_t are single ordinary double points, meaning that

$$\hat{\mathcal{O}}_{X,p} = \frac{k[[x_1, \dots, x_d]]}{Q(x_1, \dots, x_{d+1})},$$

where $d = \dim X$ and Q is a non-degenerate quadratic.

This definition is a little involved, so we should make sure that such things exist.

Theorem 152. Fix a projective variety X over an algebraically closed field k of characteristic 0. For any very ample sheaf \mathcal{L} , there is a Lefschetz pencil.

Remark 153. If $\text{char } k > 0$, then there is a Lefschetz pencil for some tensor power of \mathcal{L} .

Sketch. Suppose $X \neq \mathbb{P}\Gamma(X, \mathcal{L})$, and we go ahead and assume that X is geometrically connected. As usual, set $d := \dim X$ and $N := \dim \Gamma(X, \mathcal{L})$. We are going to use incidence correspondence

$$\Phi := \{(x, H) : x \in H \text{ and } T_x X \subseteq H\}.$$

To explain this, note that the “enemy” is basically where a hyperplane is tangent to X ; otherwise, the intersection is automatically transverse! The condition $T_x X \subseteq H$ is equivalent to the tangency because H has codimension 1. Note that Φ is a correspondence fitting in the diagram

$$\begin{array}{ccc} & \Phi & \\ \text{pr}_1 \swarrow & & \searrow \text{pr}_2 \\ X & & \mathbb{P}\Gamma(X, \mathcal{L})^\vee \end{array}$$

so we let X^\vee denote the image of X in $\mathbb{P}\Gamma(X, \mathcal{L})^\vee$. (We call X^\vee the dual variety, though it notably also depends on \mathcal{L} .) Here are some properties of this correspondence.

- The projection $\text{pr}_1: \Phi \rightarrow X$ is a projective bundle. Indeed, at each $x \in X$, the fiber above x simply consists of the hyperplanes containing $T_x X \subseteq T_x \mathbb{P}\Gamma(X, \mathcal{L})$. As such, each fiber is isomorphic to \mathbb{P}^{N-d-1} , which we can see by working out some equations of hyperplanes. It follows that Φ is irreducible, projective, and has dimension $N - 1$.
- The projection $\text{pr}_2: \Phi \rightarrow X^\vee$ has fibers consisting of the singular locus in $H \cap X$. Indeed, the fiber above H is exactly the pairs (x, H) where H is tangent to X at x . Approximately speaking, the ramification behavior of pr_2 controls the singularities we see.

Let’s now sketch the rest of the proof. Bertini’s theorem lets us find a single valid H to start our Lefschetz pencil, so we just need to show that we can continue it to a pencil. Well, one simply controls the singularities of X (they have positive codimension at least 2), and then one argues that lines exist generically. ■

Blowing up produces fibrations.

Definition 154 (Lefschetz fibration). Fix a Lefschetz pencil D for (X, \mathcal{L}) . Then the *Lefschetz fibration* is the incidence correspondence X^* sitting in the following diagram.

$$\begin{array}{ccc} & X^* & \\ \swarrow & & \searrow \\ X & & D \end{array}$$

Remark 155. It turns out that X^* is the blow up of X along $X \cap A(D)$.

Remark 156. It also turns out that the map $X^* \rightarrow \mathbb{P}^1$ is proper, flat, and it admits a section.

8.3 Symplectic Monodromy

Let’s explain how we will get to use the Main lemma. Fix a nice variety $X \subseteq \mathbb{P}^N$ over \mathbb{F}_q , which we return to being n -dimensional, where $n = 2m + 1$. Then one can find a Lefschetz pencil over some extension of \mathbb{F}_q : first find it over the algebraic closure, and then descend everything.

Remark 157. It turns out that Lefschetz pencils also exist without doing the extensions. This is due to Poonen, Nguyen, and Gunther.

Now, let $S \subseteq \mathbb{P}^1$ be the collection of singular values, and we let $U \subseteq \mathbb{P}^1 \setminus S$ denote the complement. It turns out that the associated map $\pi: X^* \rightarrow \mathbb{P}^1$ is now smooth and proper over U , so the higher pushforward $\mathcal{V} := R^n \pi_* \mathbb{Q}_\ell$ is an ℓ -adic local system over U by the Proper base change theorem.

Thus, we are granted some representation

$$\pi_1(U) \rightarrow \mathrm{GL}(V),$$

where V is some fiber of \mathcal{V} . The tameness of the singularities of $X^* \rightarrow \mathbb{P}^1$ turns out to provide tameness of the representation. To be more precise, we say something about inertia.

Definition 158. For some ramified $s \in S$, let \mathbb{D}_s be the formal disk $\mathrm{Spec} \hat{\mathcal{O}}_{\mathbb{P}^1, s}$ so that the puncture \mathbb{D}_s° is its fraction field. Then the *inertia subgroup* is the image of the map

$$\pi_1(\mathbb{D}_s^\circ) \rightarrow \pi_1(U).$$

Remark 159. The map is only defined up to conjugation because it has suppressed moving some base-points around.

Example 160. We work over \mathbb{C} for psychological reasons. Consider the Legendre family $\mathcal{E} \rightarrow \mathbb{P}^1$ of elliptic curves given by

$$\mathcal{E}_\lambda: Y^2 Z = X(X - Z)(X - \lambda Z).$$

This admits singularities at $\{0, 1, \infty\}$, where we have nodal singularities. (There is something variable change one has to do to produce a definition at $\lambda = \infty$.) Thus, we see that this is a Lefschetz pencil! So we set $U := \mathbb{P}^1 \setminus \{0, 1, \infty\}$, and we get a representation

$$\pi_1(U) \rightarrow \mathrm{GL}_2(\mathrm{H}^1(E_\eta; \mathbb{Q}_\ell)),$$

where η is the generic point. It turns out that the monodromy loops γ_0 and γ_1 around 0 and 1 go to $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. There is apparently some geometric argument for this.

Remark 161. In general, for such tame representations, it turns out that each element of the monodromy fixes a codimension 1 subspace, and it modifies the remaining one-dimensional subspace in a controlled way; for example, it turns out that we should output a matrix of determinant 1. This is (definitionally) a transvection. Eventually, one can hope to use these transvections to prove a big monodromy result.

Remark 162. In the specialization

$$\mathrm{H}_1(\mathcal{E}_\eta; \mathbb{Q}_\ell) \rightarrow \mathrm{H}_1(\mathcal{E}_s; \mathbb{Q}_\ell),$$

there is a cyclic which vanishes. Appropriately, this may be called a vanishing cycle.

Thus, we see that we will be interested in some specializations. For example, letting $j: U \hookrightarrow \mathbb{P}^1$ denote the inclusion, we may be interested in when the canonical map $\mathcal{F} \rightarrow j_* j^* \mathcal{F}$ is an isomorphism. It turns out that this is equivalent to the injectivity of the cospecialization map

$$\mathcal{F}_s \rightarrow \mathcal{F}_\eta$$

and has image in $\mathcal{F}_\eta^{I_s^{\mathrm{tame}}}$.

Definition 163 (vanishing cycle). Fix everything as above and some $s \in S$. Then we define the space of vanishing cycles to be the kernel of

$$E_s := (\mathrm{H}^n(X_{\bar{\eta}}; \mathbb{Q}_\ell(n))^\vee \rightarrow \mathrm{H}^n(X_s; \mathbb{Q}_\ell(n))^\vee),$$

where this is the dual of the cospecialization map.

Remark 164. It turns out that E_s is one-dimensional and hence isomorphic to some Tate twist $\mathbb{Q}_\ell(m)$, so we may choose a generator $\delta_s(-m) \in E_s(-m)$.

Remark 165. It turns out that there is an exact sequence

$$0 \rightarrow \mathrm{H}^n(X_s; \mathbb{Q}_\ell) \rightarrow \mathrm{H}^n(X_{\bar{\eta}}; \mathbb{Q}_\ell) \xrightarrow{\delta_s} \mathbb{Q}_\ell(m-n) \rightarrow 0.$$

The point of all this is that we are able to compute some transvections.

Theorem 166 (Picard–Lefschetz). Fix everything as above, and choose $\sigma_s \in I_s$. For each $x \in \mathrm{H}^n(X_{\bar{\eta}}; \mathbb{Q}_\ell)$, we have

$$\sigma_s(x) = x \pm t(\sigma_s)(x \cup \delta_s)\delta_s.$$

Here, $t: I_s \rightarrow \mathbb{Z}_\ell(1)$ is the winding number; alternatively, it is the natural projection once I_s is identified with $\widehat{\mathbb{Z}}(1)^{(p)}$, where the superscript means we are taking prime-to- p roots of unity.

Remark 167. One can verify that the Tate twists work out.

Remark 168. The sign \pm is $(-1)^{(n+1)(n+2)/2}$. In particular, it only depends on $n \pmod{4}$.

Next time, we will show that these transvections to prove a big monodromy result.

9 November 13: The Riemann Hypothesis

This talk was given by Xinyu Zhou at MIT for the STAGE seminar.

9.1 Reduction to the Blowup

Today, we will use the technique of Lefschetz pencils in order to prove the Riemann hypothesis part of the Weil conjectures. In short, we would like to show that the action of the Frobenius on $\mathrm{H}^r(X; \mathbb{Q}_\ell)$ has eigenvalues α with magnitude $q^{r/2}$. Note that we are allowed to extend the base field to prove this result.

By embedding X diagonally into $X \times X$ and using the Künneth formula to expand out the cohomology in middle dimension d , we see that it is enough to prove the Riemann hypothesis for $\mathrm{H}^d(X \times X; \mathbb{Q}_\ell)$. Thus, we may assume that $\dim X = 2m + 2$, and we will prove the result for $\mathrm{H}^{m+1}(X; \mathbb{Q}_\ell)$. Additionally, by taking powers using a tensor-power trick, it is enough to merely check that each Frobenius eigenvalue α satisfies

$$q^{n/2} < |\alpha| < q^{n/2+1},$$

where $n + 1 = \dim X$.

We begin with a rather abstract result on weights.

Definition 169. We say that an operator F on a vector space V satisfies W_n if and only if all eigenvalues α of F have

$$q^{n/2} < |\alpha| < q^{n/2+1}.$$

Lemma 170. Fix an operator F on a vector space V .

- (a) If V satisfies W_n , and $W \subseteq V$ is some F -stable subspace, then both W and V/W satisfy W_n .
- (b) If there is an F -stable filtration

$$V \supseteq V_1 \supseteq \dots,$$

and each V_i/V_{i+1} satisfies W_n , then V satisfies W_n .

Proof. This is a linear algebra exercise. Namely, (a) follows by suitably upper-triangularizing F using W , and (b) follows similarly. ■

We now set up some notation around Lefschetz pencils. Fix a very ample line bundle \mathcal{L} on some X inducing an embedding $X \hookrightarrow \mathbb{P}\Gamma(X, \mathcal{L})$, and we know that there is a Lefschetz pencil $D: \mathbb{P}^1 \rightarrow \mathbb{P}\Gamma(X, \mathcal{L})^\vee$. The axis will be denoted $A = D_0 \cap D_\infty$, which is smooth, and we let X^* be the blow up of X along the axis. Thus, there is a surjection $\varphi: X^* \rightarrow X$ providing the blow-up, and there is a projection $\pi: X^* \rightarrow \mathbb{P}^1$ for which the fiber over $t \in \mathbb{P}^1$ is $X_t := X \cap D_t$.

Lemma 171. Fix everything as above. It suffices to prove the Riemann hypothesis for X^* .

Proof. Let $N_{X/(A \cap X)}$ be the normal bundle of $A \cap X$ in X . It is a property of the Lefschetz pencil that

$$\varphi^{-1}(A \cap X) = \mathbb{P}N_{X/(A \cap X)}.$$

For example, with $A \cap X$ of codimension in 2, we see that the normal bundle has rank 2.

Thus, some theory of Chern classes provides a decomposition

$$H^*(\varphi^{-1}(A \cap X); \mathbb{Q}_\ell) = H^*(A \cap X; \mathbb{Q}_\ell) \oplus H^{*-2}(A \cap X; \mathbb{Q}_\ell)(-1).$$

In short, one can choose a class $\xi \in H^2(\mathbb{P}_X^n; \mathbb{Q}_\ell)(1)$ corresponding to the line bundle $\mathcal{O}(1)$, so we get a Lefschetz decomposition

$$H^*(\mathbb{P}_X^n; \mathbb{Q}_\ell) = \bigoplus_{i=0}^n H^{*-2i}(X; \mathbb{Q}_\ell)(-i)\xi^i.$$

Indeed, this decomposition can be proven by reducing to the case where X is affine, and then it follows by careful calculations of the cohomology of projective space (as one does for fields). Something similar holds for $\mathbb{P}\mathcal{E}$ even when \mathcal{E} is no longer a trivial bundle, which is the requested decomposition.

For example, taking degree 0 shows that there is an isomorphism $\mathbb{Q}_\ell \rightarrow \varphi_* \mathbb{Q}_\ell$. Additionally, one finds that $R^\bullet \varphi_* \mathbb{Q}_\ell$ is supported on $A \cap X$ in higher degrees (because φ is an isomorphism away from $A \cap X$, so the fibers produce some trivial cohomology by proper base change). Further, the higher direct images $R^\bullet \varphi_* \mathbb{Q}_\ell$ vanishes outside degrees 0 and 2 (because the cohomology of the fiber at some $x \in A \cap X$ is cohomology of \mathbb{P}^1 , which is supported in degrees 0 and 2). Thus, the Leray spectral sequence

$$E_2^{pq} = H^p(X; R^q \varphi_* \mathbb{Q}_\ell) \Rightarrow H^{p+q}(X^*; \mathbb{Q}_\ell)$$

degenerates,² so we get a decomposition

$$H^*(X^*; \mathbb{Q}_\ell) = H^*(X; \mathbb{Q}_\ell) \oplus H^{*-2}(A \cap X; \mathbb{Q}_\ell)(-1)$$

from the spectral sequence. Thus, we obtain a splitting $H^*(X; \mathbb{Q}_\ell) \subseteq H^*(X^*; \mathbb{Q}_\ell)$, and the result follows by Lemma 170. ■

² It seems nontrivial to show that $d_3 = 0$, but it is true.

9.2 The Three Groups

We are now reduced to X^* , which we may understand by understanding the projection $\pi: X^* \rightarrow \mathbb{P}^1$. Once again, we have a spectral sequence

$$E_2^{pq} = H^p(\mathbb{P}^1; R^n \pi_* \mathbb{Q}_\ell) \Rightarrow H^{p+q}(X^*; \mathbb{Q}_\ell).$$

Note that \mathbb{P}^1 has cohomology supported in degrees $\{0, 1, 2\}$, so we only have $p \in \{0, 1, 2\}$. Additionally, we are only interested in $H^{n+1}(X^*; \mathbb{Q}_\ell)$, so we see that we are only interested in the groups

$$H^0(\mathbb{P}^1; R^{n+1} \pi_* \mathbb{Q}_\ell), \quad H^1(\mathbb{P}^1; R^n \pi_* \mathbb{Q}_\ell), \quad \text{and} \quad H^2(\mathbb{P}^1; R^{n-1} \pi_* \mathbb{Q}_\ell).$$

We would like to show all three groups satisfy W_n , so W_n is satisfied by any subquotient by Lemma 170, and the result will follow for $H^{n+1}(X^*; \mathbb{Q}_\ell)$.

Remark 172. Weil II tells us that each of the sheaves $R^\bullet \pi_* \mathbb{Q}_\ell$ have an expected weight. Thus, we see that the rest of the proof amounts to proving some special cases of Weil II. This explains why it is tricky: Weil II is genuinely hard!

Each of these groups will be handled separately. Let's quickly handle the left and right groups.

- To handle $H^2(\mathbb{P}^1; R^{n-1} \pi_* \mathbb{Q}_\ell)$, we recall that our vanishing cycles live in $H^n(X_t; \mathbb{Q}_\ell) = (R^n \pi_* \mathbb{Q}_\ell)_t$, where $t \in \mathbb{P}^1$, so we receive a specialization map

$$H^*(X_t; \mathbb{Q}_\ell) \rightarrow H^*(X_t^*; \mathbb{Q}_\ell)$$

which is an isomorphism. This amounts to saying that all the fibers of $R^{n-1} \pi_* \mathbb{Q}_\ell$ is constant on \mathbb{P}^1 , so we can compute its cohomology as

$$H^2(\mathbb{P}^1; R^{n-1} \pi_* \mathbb{Q}_\ell) = (R^{n-1} \pi_* \mathbb{Q}_\ell)_t(-1) = H^{n-1}(X_t; \mathbb{Q}_\ell)(-1).$$

Now, let $Y \subseteq X_t$ be some smooth hyperplane section so that $X_t \setminus Y$ is affine, so $H^{n-1}(X_t \setminus Y; \mathbb{Q}_\ell) = H^{n+1}(X_t \setminus Y; \mathbb{Q}_\ell) = 0$ by Poincaré duality, so excision tells us that we have an injection

$$H_c^{n-1}(X_t \setminus Y; \mathbb{Q}_\ell) \rightarrow H^{n-1}(X_t; \mathbb{Q}_\ell) \rightarrow H^{n-1}(Y; \mathbb{Q}_\ell).$$

We are thus reduced to proving the statement to Y , which has smaller dimension than X , so we may induct down.

- We omit details for the calculation for $H^0(\mathbb{P}^1; R^{n+1} \pi_* \mathbb{Q}_\ell)$ because it is done with similar tricks. In short, one again finds that $R^{n+1} \pi_* \mathbb{Q}_\ell$ is constant, and then the Gysin sequence provides a surjection

$$H^{n-1}(Y; \mathbb{Q}_\ell)(-1) \rightarrow H^{n+1}(X_t; \mathbb{Q}_\ell),$$

so we are done by an induction.

We now move on to the (hardest) middle cohomology group $H^1(\mathbb{P}^1; R^n \pi_* \mathbb{Q}_\ell)$. Let $S \subseteq \mathbb{P}^1$ be the locus of singular fibers, and let U be the complement of S , and we distinguish some basepoint $u \in U$. For brevity, set $V := (R^n \pi_* \mathbb{Q}_\ell)_u$, and we let $E \subseteq V$ be the vanishing cycles. The cup product provides a symplectic pairing $V \times V \rightarrow \mathbb{Q}_\ell(-n)$, so we may let $E^\perp \subseteq V$ be the orthogonal complement.

Remark 173. The Hard Lefschetz theorem would imply that $E \cap E^\perp = 0$. However, the first proof of the Hard Lefschetz theorem was strictly harder than the proof of the Riemann hypothesis.

Without knowing that $E \cap E^\perp$ is trivial, we can still consider the filtration

$$V \supseteq E \supseteq E \cap E^\perp \supseteq 0.$$

To start off, we note that any generator σ_s in the inertia subgroup at s of $\pi_1(U)$ has

$$\sigma_s(x) = x \pm t(\sigma_s)(x \cup \delta_s)\delta_s,$$

so one can check that $\pi_1(U)$ acts trivially on V/E and $E \cap E^\perp$. As such, we may extend the above filtration into

$$\mathcal{V} \supseteq \mathcal{E} \supseteq \mathcal{E} \cap \mathcal{E}^\perp = 0$$

of sheaves on U , where $\mathcal{V} = R^n\pi_*\mathbb{Q}_\ell|_U$. The aforementioned trivial action by π_1 implies that \mathcal{V}/\mathcal{E} and $\mathcal{E} \cap \mathcal{E}^\perp$ are both constant sheaves. Pushing forward along $j: U \rightarrow \mathbb{P}^1$, we get a filtration

$$R^n\pi_*\mathbb{Q}_\ell \supseteq j_*\mathcal{E} \supseteq j_*(\mathcal{E} \cap \mathcal{E}^\perp) = 0.$$

The main lemma is applied to the non-constant quotient.

Lemma 174. For each $x \in U$, the action of F_x on $\mathcal{E}/(\mathcal{E} \cap \mathcal{E}^\perp)$ is rational. In other words, the characteristic polynomial has rational coefficients.

Proof. Omitted. ■

From here, one applies the Main lemma to $E/(E \cap E^\perp)$. For example, the cup-product gives us our symplectic pairing, and it is a theorem of Kazhdan–Margulis that the monodromy group has open image, so we complete.

It remains to handle the constant sheaves. There are two cases: either $E/(E \cap E^\perp) \neq 0$ or $E \subseteq E^\perp$. We will focus on the first case because it is easier. It turns out that this means that there are no vanishing cycles in $E \cap E^\perp$ because having any vanishing cycles in $E \cap E^\perp$ implies that all of them are in there by the Picard–Lefschetz formula. Observe that there is an exact sequence

$$0 \rightarrow j_*\mathcal{E} \rightarrow j_*\mathcal{V} \rightarrow j_*(\mathcal{V}/\mathcal{E}) \rightarrow 0$$

of sheaves on \mathbb{P}^1 . Observe $j_*(\mathcal{V}/\mathcal{E})$ is constant, so the map $H^1(\mathbb{P}^1; j_*\mathcal{E}) \rightarrow H^1(\mathbb{P}^1; R^n\pi_*\mathbb{Q}_\ell)$, is surjective, so we are reduced to handling $H^1(\mathbb{P}^1; j_*\mathcal{E})$. For this, we note that we have a short exact sequence

$$0 \rightarrow j_*(\mathcal{E} \cap \mathcal{E}^\perp) \rightarrow j_*\mathcal{E} \rightarrow j_*(\mathcal{E}/\mathcal{E} \cap \mathcal{E}^\perp) \rightarrow 0.$$

Again, the left sheaf is constant, so we receive an injection

$$H^1(\mathbb{P}^1; j_*\mathcal{E}) \rightarrow H^1(\mathbb{P}^1; j_*(\mathcal{E}/\mathcal{E} \cap \mathcal{E}^\perp)).$$

Thus, we reduce to the quotient covered by the Main lemma.

10 November 20: The Statement of Weil II

This talk was given by Kenta Suzuki at MIT for the STAGE seminar.

10.1 The Statement

We have spent the last many lectures showing the following.

Theorem 175 (Deligne). Fix a smooth projective variety X over \mathbb{F}_q . Then each eigenvalue α of the Frobenius Frob_q acting on $H^i(X_{\overline{\mathbb{F}}_q}; \mathbb{Q}_\ell)$ has absolute value $q^{i/2}$.

Observe that $H^i(X_{\overline{\mathbb{F}}_q}; \mathbb{Q}_\ell)$ is $R^i f_* \mathbb{Q}_\ell$, where $f: X \rightarrow \text{Spec } \mathbb{F}_q$ is the structure morphism. Thus, we may want to find a relative analogue. Already, in the last lecture, we say that $H^i(\mathbb{P}^1; \mathcal{L})$ had some controlled weights, where \mathcal{L} was some local system.

Let's recall the notion of weight.

Definition 176 (weight). Fix a scheme X over \mathbb{F}_q of finite type. Choose a $\overline{\mathbb{Q}}_\ell$ -sheaf \mathcal{F} on X and an isomorphism $\tau: \overline{\mathbb{Q}}_\ell \rightarrow \mathbb{C}$.

- (a) Then \mathcal{F} is τ -pure of weight w if and only if all eigenvalues α of the Frobenius acting on \mathcal{F}_x have magnitude $|\tau(\alpha)| = q^{(\deg x)(w/2)}$ for all $x \in X(\mathbb{F}_q)$.
- (b) Then \mathcal{F} is τ -mixed if and only if it admits a filtration by τ -pure.

Similarly, pure means τ -pure for all τ , and mixed means it admits a filtration of pure sheaves.

Remark 177. A priori, it seems that being τ -mixed for all τ does not imply being mixed. It is unclear if these conditions are in fact equivalent.

Example 178. The Tate twist $\overline{\mathbb{Q}}_\ell(1)$ is pure of weight -2 . This sign convention appears because the geometric Frobenius is the inverse of $(-)^q$, and $(-)^q$ acts by q on $\lim \mu_{\ell^n}$.

Here is our statement.

Theorem 179 (Weil II). Fix a morphism $f: X \rightarrow Y$ of schemes of finite type over \mathbb{F}_q . If \mathcal{F} is a constructible $\overline{\mathbb{Q}}_\ell$ -sheaf on X which is τ -mixed with weights at most n , then for any $i \geq 0$, the sheaf $R^i f_! \mathcal{F}$ is τ -mixed with weights at most $n + i$.

Remark 180. Here, $f_! \mathcal{F}$ is the sheaf whose sections on an open subset U are those sections $s \in \mathcal{F}(f^{-1}U)$ with proper support. Equivalently, one can choose a compactification $j: X \hookrightarrow X'$ so that $f': X' \rightarrow Y$ is proper, and then $f_! = f'_* \circ j_!$.

As a corollary, let's recover the Riemann hypothesis.

Example 181. If we take $Y = \text{Spec } \mathbb{F}_q$, then $Rf_! \mathcal{F} = H_c^i(X_{\mathbb{F}_q}; \mathcal{F})$, which we see is mixed of weights at most $n + i$, we see $H_c^i(X_{\mathbb{F}_q}; \mathcal{F})$

Example 182. If X is smooth and equidimensional of dimension d , then Poincaré duality provides a perfect pairing

$$H^i(X_{\mathbb{F}_q}; \mathcal{F}) \times H^{2d-i}(X_{\mathbb{F}_q}; \mathcal{F}^\vee) \rightarrow \mathbb{Q}_\ell(-d).$$

Taking Y to be $\text{Spec } \mathbb{F}_q$ again, we find that if \mathcal{F} has weights at least n , then dualizing shows that \mathcal{F}^\vee has weights at most $-n$, so $H_c^{2d-i}(X_{\mathbb{F}_q}; \mathcal{F}^\vee)$ has weights at most $(2d - i) - n$, so the perfect pairing shows that $H^i(X_{\mathbb{F}_q}; \mathcal{F})$ has weights at least $n + i$.

Example 183. If X is smooth, proper, and equidimensional, and \mathcal{F} is pure of weight n , then $H_c^i(X_{\mathbb{F}_q}; \mathcal{F}) = H^i(X_{\mathbb{F}_q}; \mathcal{F})$ is pure of weight n by combining the two corollaries. Notably, $\mathcal{F} = \overline{\mathbb{Q}}_\ell$ recovers the Riemann hypothesis.

10.2 Reductions

We will spend the rest of the talk giving a very sketchy outline of the proof of Weil II. Let's start with some functoriality properties.

Lemma 184. Fix a morphism $f: X \rightarrow Y$ of schemes of finite type over \mathbb{F}_q .

- (a) If \mathcal{F} is pure of weight n on Y , then $f^*\mathcal{F}$ is pure of weight n on X .
- (b) Suppose f is finite. If \mathcal{F} is pure of weight n on X , then $f_*\mathcal{F}$ is pure of weight n on Y .
- (c) Weight is preserved by base-change.

Proof. For (a), simply note that $(f^*\mathcal{F})_x = \mathcal{F}_{f(x)}$ for each geometric point x . For (b), simply note that

$$(f_*\mathcal{F})_y = \bigoplus_{y \in f^{-1}(\{x\})} \mathcal{F}_x.$$

Lastly, for (c), one applies the argument of (b) to the morphism $X_{\mathbb{F}_{q'}} \rightarrow X_{\mathbb{F}_q}$ for any extension $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$. ■

Lemma 185. Fix a pure or mixed sheaf \mathcal{F} on X . Then the same is true for any subquotient of \mathcal{F} .

Proof. There is nothing to say for the pure case. In the mixed case, we separate the statement into two steps.

- For any subsheaf $\mathcal{F}' \subseteq \mathcal{F}$, one can intersect the pure filtration of \mathcal{F} with \mathcal{F}' .
- For any quotient $\mathcal{F} \twoheadrightarrow \mathcal{F}''$, one can project the pure filtration of \mathcal{F} onto \mathcal{F}'' . ■

Lemma 186. Given an exact sequence

$$\mathcal{F}' \rightarrow \mathcal{F} \rightarrow \mathcal{F}''$$

of sheaves, if \mathcal{F}' and \mathcal{F}'' are mixed, then \mathcal{F} is sheaf.

Proof. By replacing \mathcal{F}' with its image in \mathcal{F} and \mathcal{F}'' with the image of \mathcal{F} , we may pass to a short exact sequence

$$0 \rightarrow \mathcal{F}' \rightarrow \mathcal{F} \rightarrow \mathcal{F}'' \rightarrow 0.$$

Now, simply glue together the pure filtrations for \mathcal{F}' and \mathcal{F}'' to build a pure filtration of \mathcal{F} . ■

We now do some devisseage for Theorem 179.

1. Weights are preserved by field extensions, so we may extend \mathbb{F}_q at will.
2. Note that there is nothing to do if f is quasi-finite because the fibers $(f_!\mathcal{F})_x$ are given by $\bigoplus_{y \in f^{-1}(\{x\})} \mathcal{F}_y$.
3. Given a short exact sequence

$$0 \rightarrow \mathcal{F}' \rightarrow \mathcal{F} \rightarrow \mathcal{F}'' \rightarrow 0$$

of sheaves on X , if we have the theorem for \mathcal{F}' and \mathcal{F}'' , then we have it for \mathcal{F} . Indeed, we simply have to note that the long exact sequence provides us with an exact sequence

$$R^i f_! \mathcal{F}' \rightarrow R^i \mathcal{F} \rightarrow R^i \mathcal{F}'',$$

so the left and right being mixed (with the correct weights) implies the same for the middle.

4. Suppose we have an open subset $j: U \subseteq X$ with complement $i: Z \hookrightarrow X$. Then we claim that having the theorem for both $\mathcal{F}|_U$ and $\mathcal{F}|_Z$ yields the theorem for \mathcal{F} . To see this, one simply uses the short exact sequence

$$0 \rightarrow j_! j^* \mathcal{F} \rightarrow \mathcal{F} \rightarrow i_! i^* \mathcal{F} \rightarrow 0,$$

so we use the previous reduction for $j^* \mathcal{F} = \mathcal{F}|_U$ and $i^* \mathcal{F} = \mathcal{F}|_Z$.

5. We may replace X and Y with their reduced subschemes because they have the same étale sites.
6. Because \mathcal{F} is constructible, we see that we may replace it by some subquotients in order to assume that it is a local system.
7. Given morphisms $f: X \rightarrow Y$ and $g: Y \rightarrow Z$, if we have the theorem for both f and g , then we have it for $g \circ f$. To see this, one uses the Grothendieck spectral sequence

$$E_2^{pq} = R^p g_! (R^q f_! \mathcal{F}) \Rightarrow R^{p+q} (gf)_! \mathcal{F}.$$

The point is that the E_2 page is τ -mixed with weights at most $n + p + q$, and then the E_∞ page is simply subquotients of these, so they also have weights at most $n + p + q$. But now the E_∞ page filters $R^{p+q} (gf)_! \mathcal{F}$, so we conclude that this sheaf is still τ -mixed with weights at most $n + p + q$.

8. By Noetherian induction, one can use the previous reduction to assume that $f: X \rightarrow Y$ is smooth of relative dimension 1 (by fibering by curves). By some Noether normalization and other things, one can further reduce to the case that $f: X \rightarrow Y$ is a smooth, affine, surjective morphism whose fibers are geometrically connected irreducible smooth curves.

10.3 Sketch

To continue, we should recall the definition of a real sheaf.

Definition 187. A sheaf \mathcal{F} is τ -real if and only if each x has

$$\tau \det(1 - \text{Frob}T; \mathcal{F}_x) \in \mathbb{R}[t]$$

for all points x .

This is fairly restrictive, but we will be able to use it.

Lemma 188. Fix a local system \mathcal{G} which is τ -pure of weight w . Then \mathcal{G} is the direct summand of a τ -real, τ -pure local system of weight w .

Proof. Consider $\mathcal{G}^\vee = \underline{\text{Hom}}(\mathcal{G}, \overline{\mathbb{Q}_\ell})$, and choose some $b := \tau^{-1}(q^{2w})$. Then we may define a local system \mathcal{L}_b as being the Galois representation where Frob_b acts by b . Then one can take

$$\mathcal{F} := (\mathcal{G}^\vee \otimes \mathcal{L}_b) \oplus \mathcal{G}.$$

Indeed, for each eigenvalue α of \mathcal{G} , we get an additional eigenvalue $\bar{\alpha} = q^{4w}/\alpha$ from the left summand, so the fact that \mathcal{F} is real follows. ■

Lemma 189. Let \mathcal{F} be a local system on X . If \mathcal{F} is τ -real, then \mathcal{F} is τ -mixed.

Proof. One uses the Rankin–Selberg method. In other words, we obtain information about \mathcal{F} from $\mathcal{F}^{\otimes k}$ for large k . For sanity, we will only do this in the case that Y is a smooth affine geometrically irreducible curve and that X is a point. Observe that we may reduce to the case that \mathcal{F} is irreducible, so we want to show that \mathcal{F} is τ -pure.

We will need the following fact: for any real $A \in M_n(\mathbb{R})$, one can check that $\det(1 - (A \otimes \overline{A})T)^{-1}$ is a power series (in T) with nonnegative coefficients. Thus, we find that

$$\frac{1}{\tau \det(1 - \text{Frob}_q T; \mathcal{F}_x^{\otimes 2n})}$$

has nonnegative real coefficients for any positive n . On the other hand, the Lefschetz fixed point theorem tells us that

$$\prod_x \frac{1}{\tau \det(1 - \text{Frob}_q T; H_c^1(\mathcal{F}^{\otimes 2n}))} = \frac{\tau \det(1 - \text{Frob}_q T; H_c^1(\mathcal{F}^{\otimes 2n}))}{\tau \det(1 - \text{Frob}_q T; H_c^2(\mathcal{F}^{\otimes 2n}))}.$$

Now, the right-hand side absolutely converges for $|t| \geq q^{1/(n\beta+1)}$, where β is an appropriately defined maximal weight. Thus, we get the same convergence for the left-hand side, which lets us bound eigenvalues on the left-hand side because each power series has nonnegative coefficients. (This is basically the same argument as Theorem 94.) ■

11 December 4: Local Monodromy

This talk was given by Daniel Hu at MIT for the STAGE seminar.

11.1 Grothendieck's Monodromy Theorem

Fix a smooth proper variety X over a number field K , we may be interested in the étale cohomology groups $H^i(X_{\overline{K}}; \mathbb{Q}_{\ell})$. This is a Galois representation, and if X has good reduction at some finite place v , then the Galois action by $\text{Gal}(\overline{K}_v/K_v)$ is unramified. However, in the case of bad reduction, there is action by inertia, and it will give us a monodromy filtration.

Definition 190 (inertia subgroup). Let R be a Henselian discrete valuation ring with fraction field K and residue field $k := R/\mathfrak{m}$. Then the *inertia subgroup* I_K is the kernel of the map

$$\text{Gal}(\overline{K}/K) \rightarrow \text{Gal}(\overline{k}/k).$$

Remark 191. The given map is well-defined because the Galois action preserves the valuation. It turns out to be surjective.

The previous remark assembles into the following proposition.

Proposition 192 (Monodromy exact sequence). Let R be a Henselian discrete valuation ring with fraction field K and residue field $k := R/\mathfrak{m}$. Then there is an exact sequence

$$0 \rightarrow I_K \rightarrow \text{Gal}(\overline{K}/K) \rightarrow \text{Gal}(\overline{k}/k) \rightarrow 1.$$

Because Galois groups on residue fields tend to be easier, we turn our attention to understanding inertia.

Notation 193 (Tate twist). We write $\mathbb{Z}_{\ell}(1)$ for the dual of the Galois representation $\lim \mu_{\ell^n}$.

Proposition 194. Let R be a Henselian discrete valuation ring with fraction field K and residue field $k := R/\mathfrak{m}$. Then there is an exact sequence

$$1 \rightarrow P_K \rightarrow I_K \rightarrow \prod_{\ell' \neq p} \mathbb{Z}_{\ell'}(1) \rightarrow 1.$$

Proof. For a given prime ℓ , the map $I_K \rightarrow \mathbb{Z}_{\ell}(1)$ is given by its Galois action. ■

Thus, for a chosen prime ℓ , we receive a chain of field extensions

$$K \subseteq K^{\text{unr}} \subseteq K^{\text{tr}, \ell} \subseteq K^{\text{tr}} \subseteq \overline{K}.$$

Here, $\text{Gal}(\overline{K}/K^{\text{tr}}) = P_K$, $\text{Gal}(\overline{K}/K^{\text{tr},\ell}) = P_{K,\ell}$, and $\text{Gal}(\overline{K}/K^{\text{unr}}) = I_K$.

We will later be interested in studying lisse \mathbb{Q}_ℓ -sheaves, which we recall are in bijection with continuous representations of $\pi_1(X_{\text{ét}}; \bar{x})$. By passing to the generic point, we see that we will be interested in understanding representations of the absolute Galois group G_K .

Theorem 195 (Grothendieck monodromy). Let R be a Henselian discrete valuation ring with fraction field K and residue field $k := R/\mathfrak{m}$, and suppose that no finite extension of k contains every ℓ -power root of unity. Now, fix a representation $\rho \in \text{Rep}_{\mathbb{Q}_\ell}(G_K)$. Then there is an open subgroup $J \subseteq I_K$ such that $\rho(\sigma)$ is unipotent for all $\sigma \in J$.

Remark 196. The representations considered in the conclusion of the theorem are called potentially semistable. For example, we see that it turns out that $H^\bullet(X_{\overline{K}}; \mathbb{Q}_\ell)$ is always potentially semistable even if X is not of good reduction.

This result will follow from a general fact about maps of profinite groups.

Lemma 197. Fix a profinite group G and a prime ℓ so that the pro-order of G is coprime to ℓ . Then every continuous homomorphism $\rho: G \rightarrow \text{GL}_n(\mathbb{Q}_\ell)$ has finite image.

Proof. This comes down to an incompatibility of topologies. ■

Proof of Theorem 195. We start with some reductions.

- After replacing K by a finite extension (which will not affect the openness of a subgroup found later), we may use the previous lemma to see that ρ factors through the maximal pro- ℓ extension of K , which is contained in $K^{\text{tr},\ell}$. In particular, we may assume that the image is pro- ℓ , so $\rho|_{I_K}$ factors through $\mathbb{Z}_\ell(1) = \text{Gal}(K^{\text{tr},\ell}/K^{\text{unr}})$ by some group theory with our prior exact sequence.
- By taking another finite extension, we may further assume that ρ lands in $1 + \ell^2 M_n(\mathbb{Z}_\ell) \subseteq \text{GL}_n(\mathbb{Q}_\ell)$. The ℓ^2 allows exp and log to both be well-defined.

We now claim that I_K acts by unipotent matrices, so we have to show that $\log \rho(s)$ is nilpotent for any $s \in I_K$. In fact, we are really trying to understand a homomorphism $\mathbb{Z}_\ell(1) \rightarrow 1 + \ell^2 M_n(\mathbb{Z}_\ell)$, so it suffices to handle a choice of topological generator $s \in \mathbb{Z}_\ell(1)$. A calculation in Galois theory shows that s and $s^{\chi_\ell(t)}$ are conjugate for any t , where χ_ℓ is the cyclotomic character; here, the χ_ℓ -action is induced by the exact sequence

$$1 \rightarrow \text{Gal}(K^{\text{tr},\ell}/K^{\text{unr}}) \rightarrow \text{Gal}(K^{\text{tr},\ell}/K) \rightarrow \text{Gal}(K^{\text{unr}}/K) \rightarrow 1.$$

Taking a limit, we see that

$$\log \rho(s)^{\chi_\ell(t)} = \chi_\ell(t) \log \rho(s).$$

But because s and $s^{\chi_\ell(t)}$ are conjugate, we see that $\log \rho(s)$ and $\log \rho(s)^{\chi_\ell(t)}$ are conjugate, so $\log \rho(s)$ and $\chi_\ell(t) \log \rho(s)$ are conjugate. Now, to show that $\log \rho(s)$ is nilpotent, we pass to the characteristic polynomial, where we see that

$$a_i(\log \rho(s)) = a_i(\chi_\ell(t) \log \rho(s)) = \chi_\ell(t)^i a_i(\log \rho(s))$$

for each coefficient a_i . Thus, we will be done as soon as we know that there is some t for which $\chi_\ell(t)$ is not a root of unity. But this follows from the hypothesis on k , which implies that the subgroup $\text{im } \chi_\ell$ of $\mathbb{Z}_\ell^\times = \mu_{\ell-1} \times (1 + \ell\mathbb{Z}_\ell)$ is open. ■

11.2 The Monodromy Operator

We are now ready to define our monodromy filtration. It will arise from a certain nilpotent operator.

Lemma 198. Let R be a Henselian discrete valuation ring with fraction field K and residue field $k := R/\mathfrak{m}$, and suppose that no finite extension of k contains every ℓ -power root of unity. Now, fix a representation $\rho \in \text{Rep}_{\mathbb{Q}_\ell}(G_K)$. Then there is a unique $N: V(1) \rightarrow V$ for which

$$\rho(\sigma) = \exp(N \circ t_\ell(\sigma))$$

for all σ in a small enough open subgroup of I_K .

Proof. Track along the diagram

$$\begin{array}{ccccccc} J & \subseteq & I_K & \subseteq & G_K & \xrightarrow{\rho} & \text{GL}_{\mathbb{Q}_\ell}(V) \\ \downarrow & & \downarrow t_\ell & & & & \uparrow \exp \\ t_\ell(J) & \subseteq & \mathbb{Z}_\ell(1) & \hookrightarrow & \mathbb{Q}_\ell(1) & \xrightarrow{d\rho} & \text{End}_{\mathbb{Q}_\ell}(V) \end{array}$$

where $\mathbb{Q}_\ell(1)$ is being viewed as a 1-dimensional Lie algebra over \mathbb{Q}_ℓ . In particular, N arises from the image of $\bar{\rho}$. ■

Remark 199. Thus, we get a functor from continuous representations of $\text{Rep}_{\mathbb{Q}_\ell}(G_K)$ (where K is a p -adic local field) to pairs (V, N) where $N: V \rightarrow V$ is nilpotent. This upgrades to a functor to the \mathbb{Q}_ℓ -representations of the so-called Weil–Deligne group.

We now define our filtration from linear algebra.

Lemma 200. Fix a finite-dimensional vector space V , and choose a nilpotent operator N on V . Then there is a unique increasing filtration $\{M_\bullet\}$ satisfying the following.

- One has $N: M_i V \rightarrow M_{i-2} V$ for any i .
- The operator N^r induces an isomorphism $\text{gr}_r V \rightarrow \text{gr}_{-r} V$.

Proof. Write N into Jordan normal form (using the structure theory of a PID), and then it can be explicitly completed to an $\mathfrak{sl}(2)$ -triple (e, f, h) where $N = f$. Then the filtration is given by the weight filtration by h . ■

Remark 201. One can add Galois action everywhere: if N acts by $V(1) \rightarrow V$, then the filtration has $N: M_i V(1) \rightarrow M_{i-2} V$, and $N^r: \text{gr}_r V(r) \rightarrow \text{gr}_{-r} V$ is an isomorphism.

Example 202. If $N = 0$, then $M_0 = V$. This is what happens for good reduction.

11.3 The Weight Filtration

Recall that we reduced the proof of Weil II to the case where $X \rightarrow Y$ is smooth, affine, surjective and of relative dimension 1. By completing, we may assume that this family is instead projective. It turns out that one can further reduce to the case that Y is a point, and in fact, it is enough to show the following.

Theorem 203. Let Y be a smooth geometrically connected projective curve over \mathbb{F}_q with generic point η . Suppose \mathcal{F} is a smooth $\overline{\mathbb{Q}_\ell}$ -sheaf which is pointwise ι -pure of weight n on a dense open subset $U \subseteq Y$. Then $\text{gr}_i \mathcal{F}_{\overline{\eta}}$ is ι -pure of weight $n + i$.

The moral of the reduction is that pointwise purity should follow from Weil I, and then we are achieving some global monodromy on gr_i .

To prove the main case, let K be the function field of Y and set $k := \mathbb{F}_q$, and we recall the definition of the Weil groups W_K and W_k which fit into the following pullback

$$\begin{array}{ccccccc} 1 & \longrightarrow & I_K & \longrightarrow & W_K & \longrightarrow & W_k & \longrightarrow 1 \\ & & \parallel & & \downarrow & & \downarrow & \\ 1 & \longrightarrow & I_K & \longrightarrow & G_K & \longrightarrow & G_k & \longrightarrow 1 \end{array}$$

where W_k is cyclic generated by the Frobenius.

Remark 204. Via this sequence, there is an equivalence of categories

$$\text{Rep}_{\mathbb{Q}_\ell}(G_K) \rightarrow \text{Rep}_{\mathbb{Q}_\ell}(\text{WD}_K),$$

where the right-hand side consists of pairs (V, N) , where V is a representation of W_K , and $N: V(1) \rightarrow V$ is W_K -equivariant and nilpotent.

Definition 205 (weight filtration). Suppose that the weights of some representation V are integers. Then there is a unique weight filtration $\{W_\bullet\}$ of V which is W_K -stable and such that $\text{gr}_i V$ is pure of weight i .

Remark 206. Let's explain why this filtration ought to exist. Choose a lift $\Phi \in W_K$ of the Frobenius. Then define V'_i to be the generalized eigenspaces of Φ with weight i , and we may take W_i to be the sum of the V'_j 's for $j \leq i$. It turns out that this filtration does not depend on the choice of Φ .

Remark 207. One can show that $N(W_i(1)) \subseteq W_{i-2}$. It is an open problem if this filtration agrees with the monodromy filtration. One would need to check if $N^r: \text{gr}_r V(r) \rightarrow \text{gr}_{-r} V$ is an isomorphism. Deligne has shown this when K is the function field of a curve.

12 December 11: Applications of Weil II

This talk was given by Elia Gorokhovsky at MIT for the STAGE seminar. For today, we fix a finite field \mathbb{F}_q and a prime ℓ coprime to q . We also identify \mathbb{Q}_ℓ with \mathbb{C} whenever is convenient.

12.1 Semisimplicity

Here is our first main theorem for today.

Theorem 208 (Semisimplicity). Fix a smooth scheme X of finite type over $k := \mathbb{F}_q$, and choose some lisse pure sheaf \mathcal{F} on X . Then the associated representation

$$\pi_1(X) \rightarrow \text{GL}(\mathcal{F}_{\bar{x}})$$

is semisimple.

Proof. The idea is to use our weight machinery to show that any obstruction to semisimplicity vanishes. Indeed, let $\mathcal{F}'_{\bar{k}}$ be the maximal semisimple subsheaf, and set $\mathcal{F}''_{\bar{k}} := \mathcal{F}_{\bar{k}}/\mathcal{F}'_{\bar{k}}$. Our aim is to show that $\mathcal{F}''_{\bar{k}}$ vanishes. In fact, it is enough to show that the short exact sequence

$$0 \rightarrow \mathcal{F}'_{\bar{k}} \rightarrow \mathcal{F}_{\bar{k}} \rightarrow \mathcal{F}''_{\bar{k}} \rightarrow 0$$

merely splits: then any irreducible subsheaf of $\mathcal{F}_{\bar{k}}''$ could be moved into $\mathcal{F}_{\bar{k}'}'$, violating its maximality; instead, $\mathcal{F}_{\bar{k}}''$ must contain no irreducible subsheaves, implying that it vanishes.

Thus, it is enough to show that the corresponding class in $\mathrm{Ext}^1(\mathcal{F}_{\bar{k}}'', \mathcal{F}_{\bar{k}})$ vanishes. To this end, note that \mathcal{F} is defined over \mathbb{F}_q , and the irreducible subsheaves also live over \mathbb{F}_q , so everything descends to k . We conclude that our extension is Frobenius-invariant, so it is enough to check that

$$\mathrm{Ext}^1(\mathcal{F}_{\bar{k}}'', \mathcal{F}_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)} = 0.$$

To understand these invariants, we note that a spectral sequence calculation shows that

$$\mathrm{Ext}^1(\mathcal{F}_{\bar{k}}'', \mathcal{F}_{\bar{k}}) = H^1(X_{\bar{k}}; \underline{\mathrm{Hom}}(\mathcal{F}_{\bar{k}}'', \mathcal{F}_{\bar{k}})).$$

Thus, we would like to show that $H^1(X_{\bar{k}}; \underline{\mathrm{Hom}}(\mathcal{F}_{\bar{k}}'', \mathcal{F}_{\bar{k}}))$ admits no F -invariant vectors, so it is enough (by Weil II!) will be enough to show that $H^1(X_{\bar{k}}; \underline{\mathrm{Hom}}(\mathcal{F}_{\bar{k}}'', \mathcal{F}_{\bar{k}}))$ is mixed with weights at least 1.

We now use the smoothness of X . By Poincaré duality, one can turn H^1 into cohomology with compact supports, so Weil II tells us that it is enough to show that $\underline{\mathrm{Hom}}(\mathcal{F}_{\bar{k}}'', \mathcal{F}_{\bar{k}})$ is mixed of weights at least 0. Well, note

$$\underline{\mathrm{Hom}}(\mathcal{F}'', \mathcal{F}) \cong (\mathcal{F}'')^\vee \otimes \mathcal{F}'.$$

Both \mathcal{F}'' and \mathcal{F}' are pure of the same weight (because they came from the pure sheaf \mathcal{F}), the tensor product on the right-hand side is pure of weight 0, so we are done. ■

Here are some applications.

Corollary 209. Fix a smooth scheme X of finite type over $k := \mathbb{F}_q$. For any pure sheaf \mathcal{F} , the image of

$$\pi_1^{\text{ét}}(X_{\bar{k}}) \rightarrow \mathrm{GL}(\mathcal{F}_{\bar{x}})$$

is semisimple.

Proof. Reductivity follows from the above proof: this “tautological” faithful representation is semisimple. We will not explain why the center is finite. ■

Theorem 210 (Hard Lefschetz). Fix a smooth projective variety X over an algebraically closed field k of equidimension d , and choose an ample line bundle \mathcal{L} on X . Then the first Chern class $c_1(\mathcal{L}) \in H^2(X; \overline{\mathbb{Q}}_\ell)$ induces an isomorphism

$$(c_1(\mathcal{L})^i \cup -) :$$

Proof. Semisimplicity is used to understand the cohomology groups. In a few more words, one places X into a Lefschetz pencil, which gives some monodromy action on the cohomology groups. Then one uses semisimplicity. ■

12.2 Equidistribution

For motivation, we recall the following theorem.

Theorem 211 (Chebotarev). Fix a finite Galois extension L/K of number fields with Galois group G .

- (a) Existence: for any conjugacy class c of G , there is prime \mathfrak{p} of K for which the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ is c .
- (b) Equidistribution: for any subset $c \subseteq G$ stable under conjugacy,

$$\lim_{X \rightarrow \infty} \frac{\#\{\mathfrak{p} : \mathrm{Frob}_{\mathfrak{p}} \in C, N\mathfrak{p} \leq X\}}{\#\{\mathfrak{p} : N\mathfrak{p} \leq X\}} = \frac{\#C}{\#G}.$$

Here is a geometric way to view this theorem: $\mathrm{Spec} \mathcal{O}_L \rightarrow \mathrm{Spec} \mathcal{O}_K$ is some étale (open) cover with Galois group G . Then for any closed point \mathfrak{p} of $\mathrm{Spec} \mathcal{O}_K$, we get a Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in \pi_1(\mathrm{Spec} \mathcal{O}_K)$, which then embeds into G . Thus, the above theorem is a special case of a more general question about the equidistribution of Frobenius elements in monodromy groups.

Here is another such instance: recall that

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}$$

for any elliptic curve E over \mathbb{F}_p . Thus, we may be interested in understanding the distribution of the error term

$$a_p(E) := (p + 1) - \#E(\mathbb{F}_p).$$

Fixing E and letting p vary yields the Sato–Tate conjecture.

Conjecture 212 (Sato–Tate). Fix an elliptic curve E over \mathbb{Q} without potential complex multiplication. For each prime p of good reduction, choose $\theta_p \in [0, \pi]$ so that $2 \cos \theta_p = a_p$. Then $\theta_p \in [0, \pi]$ distribute according to $\frac{2}{\pi} \sin^2 \theta \, d\theta$.

Remark 213. In the form stated, this conjecture has been proven by Clozel–Harris–Taylor.

Remark 214. Here is a geometric incarnation: this turns out to be equivalent to the equidistribution of Frobenius elements for the smooth model $\mathcal{E} \rightarrow \mathrm{Spec} \mathbb{Z}[1/N]$ in the monodromy group of the representation $H^1(E_{\overline{\mathbb{Q}}}; \mathbb{Q}_{\ell})$.

Alternatively, one could fix p and let E vary, which basically amounts to replacing E with an elliptic surface. This produces the following theorem.

Theorem 215 (Deligne, Katz). Fix a smooth equidimensional scheme X of finite type over $k := \mathbb{F}_q$, and let \mathcal{F} be a smooth sheaf pure of weight 0. Let $\rho: \pi_1(X) \rightarrow \mathrm{GL}(\mathcal{F}_{\overline{x}})$ be the representation associated to \mathcal{F} , and let G be the Zariski closure of $\mathrm{im} \, \rho|_{\pi_1(X_{\bar{k}})}$, which we assume contains $\mathrm{im} \, \rho$. Then the elements

$$\{\mathrm{Conj} \, \rho(F_x)^{\mathrm{ss}}\}_{x \in X}$$

equidistribute in $\mathrm{Conj} \, K$, where K is the maximal compact subgroup of $G(\mathbb{C})$.

Here are some remarks explaining what this theorem means.

Remark 216. The maximal compact subgroup K of $G(\mathbb{C})$ exists because G was found to be semisimple.

Remark 217. The semisimple elements $\rho(F_x)$ have eigenvalues of absolute value 1, so they generate a compact torus in $G(\mathbb{C})$. This explains why the conjugacy classes of $\rho(F_x)^{\mathrm{ss}}$ can be moved into conjugacy classes of K . It turns out that the intersection of the conjugacy class $\mathrm{Conj} \, \rho(F_x)^{\mathrm{ss}} \subseteq G$ with K consists of a single K -conjugacy class. This follows from the Peter–Weyl theorem, which says that the characters of the finite-dimensional representations of K form an orthonormal basis of $L^2(K)$.

Remark 218. Let's explain why we don't miss much when we move to K : the finite-dimensional (algebraic) representations of $G(\overline{\mathbb{Q}}_{\ell})$ are equivalent to the finite-dimensional (continuous) representations of $G(\mathbb{C})$. Being finite-dimensional and hence algebraic then tells us that this is equivalent to the finite-dimensional representations of K .

Remark 219. Lastly, we should remark that “equidistribution” here means that our conjugacy classes equidistribute according to the pushforward of the Haar measure along the projection $K \twoheadrightarrow \text{Conj } K$.

Example 220. Suppose $G = \text{SL}(2)$, which is the case for generic elliptic curves. Then $K = \text{SU}(2)$. Because all unitary matrices are diagonalizable, each element of K is conjugate to a diagonal one, and it turns out that $\text{Conj } K$ is then homeomorphic to $\mathbb{Z}/\pi\mathbb{Z}$ by sending $\theta \in [0, \pi]$ to $\text{diag}(\exp(i\theta), \exp(-i\theta))$. The pushforward measure turns out to be $\frac{2}{\pi} \sin^2 \theta d\theta$, which one computes directly.

Remark 221. Let μ^\sharp be the pushforward to $\text{Conj } K$ of the Haar measure μ on K . Thus, Theorem 215 amounts to saying that there is a limit

$$\lim_{n \rightarrow \infty} \frac{1}{\#X(\mathbb{F}_{q^n})} \sum_{x \in X_0(\mathbb{F}_{q^n})} \delta_{\rho(F_x)^{\text{ss}}} = \mu^\sharp$$

in the weak sense.

Sketch of Theorem 215. There are two steps.

1. It is enough to check the weak convergence on continuous functions in $C(\text{Conj } K)$, but the Peter–Weyl theorem tells us that finite linear combinations of characters are dense in $C(\text{Conj } K)$. Thus, it is enough to check that

$$\lim_{n \rightarrow \infty} \frac{1}{\#X(\mathbb{F}_{q^n})} \sum_{x \in X_0(\mathbb{F}_{q^n})} \chi(\rho(F_x)^{\text{ss}}) \stackrel{?}{=} \int_K \chi \mu^\sharp$$

for any character χ . This is automatically true for the trivial character, so it only remains to deal with the nontrivial irreducible characters. Thus, by the orthogonality relations, it is enough to check that

$$\lim_{n \rightarrow \infty} \frac{1}{\#X(\mathbb{F}_{q^n})} \sum_{x \in X_0(\mathbb{F}_{q^n})} \chi(\rho(F_x)^{\text{ss}}) \stackrel{?}{=} 0.$$

Equivalently, we must check that

$$\sum_{x \in X_0(\mathbb{F}_{q^n})} \chi(\rho(F_x)^{\text{ss}}) \stackrel{?}{=} O(\#X(\mathbb{F}_{q^n})),$$

where χ is a nontrivial irreducible character of K . We may then extend this χ up to G , so we see that we are trying to show that

$$\sum_{x \in X_0(\mathbb{F}_{q^n})} \text{tr } \psi \rho(F_x)^{\text{ss}} \stackrel{?}{=} O(\#X(\mathbb{F}_{q^n})).$$

We may now ignore ψ entirely because it is enough to check that the sum vanishes for any representation $\psi\rho$ of $\pi_1(X)$ landing in G . Note that the corresponding lisse sheaf continues to have weight 0.

2. We are thus left to bound

$$\sum_{x \in X_0(\mathbb{F}_{q^n})} \text{tr } \rho(F_x)^{\text{ss}},$$

where ρ is some irreducible representation of $\pi_1(X)$. Let \mathcal{F} be the associate lisse sheaf, and then we see that this sum collapses to

$$\sum_{i=0}^{2 \dim X} (-1)^i \text{tr} (\text{Frob}_{q^n}; H_c^i(X_{\bar{k}}; \mathcal{F})).$$

By Weil II, we know that $H_c^i(X_{\bar{k}}; \mathcal{F})$ is mixed of weight at most i , so the eigenvalues of the Frobenius are at most $q^{in/2}$. We would like to bound this by $\#X(\mathbb{F}_{q^n})$, which by Noether normalization is approximately q^{nd} (up to some constants). Thus, we see that we only have to worry about top dimension in the above sum, which is handled separately: $H_c^{2d}(X; \mathcal{F}) = H^0(X; \mathcal{F}^\vee)$, which vanishes because such global sections correspond to invariant elements for ρ , which do not exist because ρ is irreducible. ■