§ Proof of the Weil conjectures.

· Notation: $\mathbb{F}_q$ field with $q = p^a$, p a prime.

$\mathbb{F} := \overline{\mathbb{F}_q}$.

X_0 var. $/\mathbb{F}_q$, $X := X_0 \times_{\mathbb{F}_q} \operatorname{Spec} \mathbb{F}$ var. $/\mathbb{F}$.

ℓ a prime $\neq p$.

Assume all varieties are abs. irred.

§ 1. Statement of the conjectures.

· Let X_0 be a nonsing. proj. var. $/\mathbb{F}_q$ of dim. d. Set for all $m \geq 1$,

$$N_m := \# X_0(\mathbb{F}_{q^m}).$$

· Def. 1. The zeta function of X_0 is

$$Z(X_0, t) := \exp\left(\sum_{m \geq 1} N_m \cdot \frac{t^m}{m} \right) =$$

$$= 1 + \sum_{m \geq 1} N_m \cdot \frac{t^m}{m} + \frac{1}{2!} \cdot \left(\sum_{m \geq 1} N_m \cdot \frac{t^m}{m} \right)^2 + \dots,$$

which is an element of $\mathbb{Q}[[t]]$.

· Note: $$\frac{d}{dt} \log Z(X_0, t) = \sum_{m \geq 1} N_m \cdot t^{m-1}.$$

· The Weil conjectures are the following:

(W1, Rationality). There exist polynomials $P_0(t), \dots, P_{2d}(t) \in \mathbb{Z}[t]$ s.t.

$$Z(X_0, t) = \frac{P_1(t) P_3(t) \cdots P_{2d-1}(t)}{P_0(t) P_2(t) \cdots P_{2d}(t)},$$

with $P_0(t) = 1 - t$ and $P_{2d}(t) = 1 - q^d t$.

(W2, Functional equation). $Z(X_0, t)$ satisfies the following functional eq.

$$Z\left(X_0, \frac{1}{q^d t}\right) = \pm q^{\frac{dx}{2}} \cdot t^x \cdot Z(X_0, t),$$

with $x = (\Delta \cdot \Delta)$ being the intersection number of the diagonal $\Delta \subseteq X \times X$ with itself.

(W3, Betti numbers). Assume that there exists a numb. field K and a smooth, proper var. $\mathcal{Y} / \mathcal{O}_K$ with fiber $\mathcal{Y}_{\mathfrak{p}} \cong X_0$ for some prime ideal $\mathfrak{p}$. Write $P_r(t) := \prod_{i=1}^{\beta_r} (1 - \alpha_{r,i} t)$ for some $\alpha_{r,i}, \beta_r$.

Then, the r-th top. Betti number of $\mathcal{Y}_{\mathbb{C}}$ coincides with its étale counterpart (the dim. of $H^r(X, \mathbb{Q}_\ell)$, which agrees with β_r).

(W4, Riemann hypothesis). The numbers $\alpha_{r,i}$ are algebraic integers, all of whose conjugates have absolute values $q^{r/2}$.

· In this talk: prove (W2), (W3), show that (W4) $\Rightarrow$ (W1), and give a reduction for proving (W4).

§ 2. Proof of the first Weil conjectures.

· Let A_0 be an affine $\mathbb{F}_q$-alg. We have a morph.

$$f_0 : A_0 \to A_0$$
$$a \mapsto a^q$$

of $\mathbb{F}_q$-algs., which can be extended to a morph. of $\mathbb{F}$-alg.

$$f : A \to A$$

for $A := A_0 \otimes_{\mathbb{F}_q} \mathbb{F}$. The corresponding (regular) map $F : \operatorname{Spec} A \to \operatorname{Spec} A$ is the Frobenius map.

· **Def. 2.** For a var. $X_0/\mathbb{F}_q$, the Frobenius map $F : X \to X$ is the unique regular map s.t. for every affine open $U_0 \subseteq X_0$, $F(U) \subseteq U$ and $F|_U$ is the Frobenius on U.

· **Rem. 3.**

(i) The Frobenius $F : \mathbb{A}^n \to \mathbb{A}^n$ is $(t_1, \dots, t_n) \mapsto (t_1^q, \dots, t_n^q)$.

(ii) The Frobenius $F : \mathbb{P}^n \to \mathbb{P}^n$ is $[t_0 : \dots : t_n] \mapsto [t_0^q : \dots : t_n^q]$.

(iii) For $\varphi : Y_0 \to X_0$ regular over $\mathbb{F}_q$,

$$\begin{array}{ccc} Y & \xrightarrow{\varphi} & X \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle F} \\ Y & \xrightarrow[\varphi]{} & X \end{array}$$

commutes.

(iv) From the previous statements, it follows that F acts on any subvariety of $\mathbb{A}^n$ as $(t_1, \dots, t_n) \mapsto (t_1^q, \dots, t_n^q)$ and on any subvar. of $\mathbb{P}^n$ as $[t_0 : \dots : t_n] \mapsto [t_0^q : \dots : t_n^q]$.

(v) Recall that $F: X \to X$ is a map of $\mathbb{F}$-schemes, and thus fixes $\mathbb{F}$. Moreover, we can see F as a base change by $\operatorname{Spec}\mathbb{F}$ of the Frobenius in $X_0 \to X_0$.

· Lemma 4. The Frobenius map $F: X \to X$ has degree q^d.

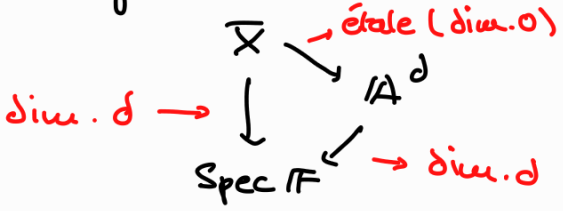
Proof] First, assume $X = \mathbb{A}^d$. Then, F is the map of $\mathbb{F}$-algebras

$$\mathbb{F}[T_1, \dots, T_d] \longrightarrow \mathbb{F}[T_1, \dots, T_d]$$
$$T_i \longmapsto T_i^q \quad \forall i.$$

This map has image $\mathbb{F}[T_1^q, \dots, T_d^q]$, and $\mathbb{F}[T_1, \dots, T_d]$ is free of rank q^d over it, since we have a basis $\{ T_1^{i_1} \cdots T_d^{i_d} : 0 \le i_j \le q-1 \ \forall j \}$. Therefore,

$$[\mathbb{F}(T_1, \dots, T_d) : \mathbb{F}(T_1^q, \dots, T_d^q)] = q^d.$$

In the general case, we may assume that X is smooth and that we have a diagram



Since the degree is multiplicative,

Since the map $X \to \mathbb{A}^d$ can be seen coming from a map $X_0 \to \mathbb{A}^d_{\mathbb{F}_p}$, Rem. 3 implies that the following diagram commutes:

$$\begin{array}{ccc} X & \longrightarrow & \mathbb{A}^d \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle F} \\ X & \longrightarrow & \mathbb{A}^d \end{array}$$

Since the horizontal maps are étale (and the degree is multiplicative), it follows that both vertical maps have the same degree, and by what we showed earlier, $\deg(F) = q^d$. ⊠

· Recall: Lefschetz's Fixed Point Formula. Let X be a complete non-sing. var./k, with $k=\bar{k}$, and $\varphi: X \to X$ a regular map. Then,

$$(\Gamma_\varphi \cdot \Delta) = \sum_{r \geq 0} (-1)^r \operatorname{Tr}(\varphi \mid H^r(X, \mathbb{Q}_\ell)),$$

with Γ_φ the graph of φ, Δ the diagonal in $X \times X$. Note that $(\Gamma_\varphi \cdot \Delta)$ is the number of fixed points of φ counted with multiplicities.

· In particular, we can count which fixed points have multiplicity 1, i.e., $(\Gamma_\varphi \cdot \Delta)_P = 1$. For this, we use:

·) Prop. Let Y_1, Y_2 be closed subvars. of a nonsing. var. X, and assume that the point P is an isol. comp. of $Y_1 \cap Y_2$. Then, $(Y_1 \cdot Y_2)_P = 1$ if:

(a) Y_1 and Y_2 are nonsing. at P,

(b) $\operatorname{Tgt}_P(Y_1) \cap \operatorname{Tgt}_P(Y_2) = 0$, and → Y_1 and Y_2 cross transversally at P.

(c) $\dim Y_1 + \dim Y_2 = \dim X$. → Y_1 and Y_2 intersect properly at P.

· Lemma 5. Let $\varphi: X \to X$ be a regular map, and $P \in X$ a fixed point of φ. Then $(\Gamma_\varphi \cdot \Delta)_P = 1$ if 1 is not an eigenvalue of

$$(d\varphi)_P : \operatorname{Tgt}_P(X) \to \operatorname{Tgt}_P(X).$$

Proof | ETS: (a), (b) and (c) hold for Γ_φ and Δ.

(a), (c)] Clear, since Γ_φ and Δ are isom. to X.

(b)] Note that $\operatorname{Tgt}_{(P,P)}(\Gamma_\varphi)$ is the graph of $(d\varphi)_P : \operatorname{Tgt}_P(X) \to \operatorname{Tgt}_P(X)$, and that $\operatorname{Tgt}_{(P,P)}(\Delta)$ is the graph of the identity map $\operatorname{Tgt}_P(X) \to \operatorname{Tgt}_P(X)$.

Thus,

$v \in Tgt_{(P,P)}(\Gamma_\varphi) \cap Tgt_{(P,P)}(\Delta)$ must be of the form $(v, (d\varphi)_P(v)) = (v,v)$, and thus such a $v \neq 0$ can only exist iff 1 is an eigenvalue of $(d\varphi)_P$. ⊠

- We now return to our setup.

- Lemma 6. The fixed points of F on X are the points of X_0 with coords. in $\mathbb{F}_q$. Moreover, each occurs with multiplicity 1 in $(\Gamma_F \cdot \Delta)$.

Proof | First, note that a closed point $\operatorname{Spec} \mathbb{F} \xrightarrow{x} X$ is fixed by F if and only if

$$\begin{array}{ccc} \operatorname{Spec} \mathbb{F} & \xrightarrow{x} & X \\ & \searrow^{x} & \downarrow F \\ & & X \end{array}$$

commutes.

There, we want to construct a bijection

$$\varphi : X_0(\mathbb{F}_q) \longrightarrow X(\mathbb{F})^F$$

$$x_0 \longmapsto x_0 \times_{\mathbb{F}_q} \operatorname{Spec} \mathbb{F}.$$

By Rem. 3, this map is well-def., since

$$\begin{array}{ccc} \operatorname{Spec} \mathbb{F} & \xrightarrow{x_0 \times_{\mathbb{F}_q} \operatorname{Spec} \mathbb{F}} & X \\ {\scriptstyle F = id} \downarrow & & \downarrow F \\ \operatorname{Spec} \mathbb{F} & \xrightarrow[x_0 \times_{\mathbb{F}_q} \operatorname{Spec} \mathbb{F}]{} & X \end{array}$$

commutes.

Now, let $x : \operatorname{Spec} \mathbb{F} \longrightarrow X$ be fixed by F. WLOG we may write $X = \operatorname{Spec} A$, with $A = A_0 \otimes_{\mathbb{F}_q} \mathbb{F}$ some $\mathbb{F}$-alg., and $X_0 = \operatorname{Spec} A_0$.

Moreover, we know that the Frobenius gives maps

$F_0 : A_0 \to A_0$, $a \mapsto a^q$; and $F : A \to A$ the base change of F_0 with $\mathbb{F}$.

Our map x then gives a map $\alpha : A \to \mathbb{F}$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & \mathbb{F} \\ {\scriptstyle F}\searrow & & \nearrow{\scriptstyle \alpha} \\ & A & \end{array}$$

Let $a_0 \in A_0$. Then,

$$\alpha(a_0 \otimes 1) = \alpha \circ F(a_0 \otimes 1) = \alpha(F_0(a_0) \otimes 1) = \alpha(a_0^q \otimes 1) = \alpha(a_0 \otimes 1)^q.$$

Therefore, $\alpha(a_0 \otimes 1) \in \mathbb{F}_q$, and this is true $\forall a_0 \in A$. Thus, we get a map of $\mathbb{F}_q$-algebras

$$\begin{aligned} \alpha_0 : A_0 &\longrightarrow \mathbb{F}_q \\ a_0 &\longmapsto \alpha(a_0 \otimes 1), \end{aligned}$$

which gives a point $x_0 : \operatorname{Spec} \mathbb{F}_q \to X_0$. Clearly, extending α_0 by scalars to a map of $\mathbb{F}_q$-algebras gives back α, so $\varphi(x_0) = x$.

$\therefore \varphi$ is surjective.

But by this exact reasoning, φ is injective, since α_0 is uniquely determined by α.

Lastly, for the second statement, it is ETS that $(dF)_P = 0$ at all the fixed points P of F (and then we conclude by Lemma 5).

As earlier, we assume X_0 is affine, $X_0 = \operatorname{Spec} A_0$ with $A_0 = \mathbb{F}_q[T_1, \dots, T_d]/I$, and we write $t_i := T_i + I$. Then, each t_i defines a map

$$t_i : X_0 \to \mathbb{A}^1,$$

and they satisfy that

$$\begin{array}{ccc} X_0 & \xrightarrow{F} & X_0 \\ & {\scriptstyle t_i^q}\searrow \quad \swarrow{\scriptstyle t_i} & \\ & \mathbb{A}^1 & \end{array}$$

commutes (looking at the affine case, $t_i \circ F$ is the map $\mathbb{F}_q[T] \to A_0$ given by $T \mapsto t_i \mapsto t_i^q$). Then,

$$(dt_i)_P \circ (dF)_P = (dt_i^q)_P = \underbrace{q t_i^{q-1}}_{0} (dt_i)_P = 0. \qquad \square$$

· Using this lemma, we can use the Lefschetz Fixed Point Formula to show:

· **Prop. 7.** Let X_0 be a complete nonsing. var./$\mathbb{F}_q$. $\forall m \geq 1$,

$$N_m = \sum_{r \geq 0} (-1)^r \cdot \mathrm{Tr}(F^m \mid H^r(X, \mathbb{Q}_\ell)).$$

Proof

$m = 1$: by Lemma 6, $(\Gamma_F \cdot \Delta) = N_1$, since

$$(\Gamma_F \cdot \Delta) = \sum_{x \in X^F} 1 = \# X^F = \# X_0(\mathbb{F}_q) = N_1$$

↑ only the fixed points of F appear on the sum, each with multiplicity 1

Then, the LFP gives the equality.

$m > 1$: same as the $m = 1$ case, observing that F^m is the Frobenius map of X relative to $X_0 \times_{\mathbb{F}_q} \mathrm{Spec}(\mathbb{F}_{q^m})$.

∎

· **Rem. 8.**

(a) X_0 comp. nonsing. var./$\mathbb{F}_q$. Then, $F : X \to X$ defines maps

$$F^*, F_* : H^r(X, \mathbb{Q}_\ell) \to H^r(X, \mathbb{Q}_\ell),$$

where F_* is the unique map s.t.

$$\eta_X(F_*(y) \cup x) = \eta_X(y \cup F^*(x))$$

$\forall x \in H_c^{2d-r}(X, \mathbb{Q}_\ell)$, $\forall y \in H^r(X, \mathbb{Q}_\ell)$, and with η_X being the iso. $H^{2d}(X, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$.

Furthermore, since F has degree q^d, $F_* \circ F^* = q^d$.

(b) If $\varphi: Y_0 \to X_0$ is a regular map of comp. nonsing. vars. / $\mathbb{F}_q$, then

$$F^* \varphi_* = q^{\dim X - \dim Y} \varphi_* F^*.$$

(Frob. of X; Frob. of Y)

Indeed, applying F_* on each side we get

$$F_*(F^* \varphi_*) = q^{\dim X} \varphi_*, \text{ and}$$
$$F_*\left(q^{\dim X - \dim Y} \varphi_* F^*\right) = q^{\dim X - \dim Y} \varphi_* F_* F^* = q^{\dim X} \varphi_*,$$

($F \circ \varphi = \varphi \circ F$)

and the unicity of $(-)_*$ shows that the original terms were equal.

Note that this also works when the coefficients are $\mathbb{F}_{q^n}/\mathbb{C}^{nt}$ for $q \neq p$.

· Lemma 9. For $\varphi: V \to V$ an endom. of f.-v.s., define its char. pol. as

$$P_\varphi(t) := \det(1 - \varphi t \mid V).$$

If $P_\varphi(t) = \prod (1 - c_i t)$, then we claim that:

(i) $\mathrm{Tr}(\varphi^m \mid V) = \sum c_i^m$,

(ii) In $k[[t]]$,

$$\log \frac{1}{P_\varphi(t)} = \sum_{m=1}^{\infty} \mathrm{Tr}(\varphi^m \mid V) \cdot \frac{t^m}{m}.$$

Proof

(i) By the expression of $P_\varphi(t)$, we can choose a basis of V s.t. φ is of the form

$$\begin{pmatrix} c_1 & & * \\ & \ddots & \\ 0 & & c_n \end{pmatrix},$$

from which (i) follows.

(ii) In $k[[t]]$, we have

$$\log \frac{1}{1 - c_i t} = \sum_{m=1}^{\infty} c_i^m \frac{t^m}{m}.$$

Taking the sum on both sides over i (and applying (i)) we obtain (ii). ⊠

· **Thm. 10.** Let X_0 be a comp. nonsing. var. X_0 of dim. d / $\mathbb{F}_q$. Then,

$$Z(X_0, t) = \frac{P_1(X_0,t) \cdot \ldots \cdot P_{2d-1}(X_0,t)}{P_0(X_0,t) \cdot \ldots \cdot P_{2d}(X_0,t)},$$

with $P_i(X_0,t) := \det(1 - Ft \mid H^r(X, \mathbb{Q}_\ell)) \in \mathbb{Q}_\ell[t]$.

Proof) By our previous results,

$$Z(X_0,t) \overset{\text{def.}}{=} \exp\left(\sum_{m \geq 1} N_m \cdot \frac{t^m}{m}\right)$$

$$\overset{\text{Prop. 7}}{=} \exp\left(\sum_{m \geq 1} \left(\sum_{r \geq 0} (-1)^r \operatorname{Tr}(F^m \mid H^r(X, \mathbb{Q}_\ell))\right) \frac{t^m}{m}\right) =$$

changing sums

$$= \prod_{r=0}^{2d} \left(\exp\left(\sum_{m \geq 1} \operatorname{Tr}(F^m \mid H^r(X, \mathbb{Q}_\ell)) \frac{t^m}{m}\right)\right)^{(-1)^r} =$$

$$= \prod_{r=0}^{2d} P_r(t)^{(-1)^r}, \text{ finishing the proof.}$$

Lemma 9

⊠

· **Rem. 11.** Since F acts as 1 on $H^0(X, \mathbb{Q}_\ell)$, and as q^d on $H^{2d}(X, \mathbb{Q}_\ell)$ (using that $F_* \circ F^* = q^d$, and when $r = 0$ or $2d$, one of them acts as the identity, since either $H^r(X, \mathbb{Q}_\ell)$ or $H_c^{2d-r}(X, \mathbb{Q}_\ell)$ is trivial), it follows that

$$P_0(X_0,t) = 1 - t, \quad P_{2d}(X_0,t) = 1 - q^d t.$$

In general, $P_i(X_0,t) = 1 + \cdots \in \mathbb{Q}_\ell[t]$.

· Cor. 12. The power series $Z(X_0, t) \in \mathbb{Q}[[t]]$ is in $\mathbb{Q}(t)$.

Proof | We need the following result:

·) Lemma. Let $k \subseteq K$ be fields, $f(t) \in k[[t]]$. Then,

$$f \in K(t) \Rightarrow f \in k(t).$$

See Milne's notes for a proof. |

By noting that $Z(X_0, t) \in \mathbb{Q}_\ell(t)$ by Thm. 10, this Lemma finishes the proof. ⊠

· Note: this does not imply that $P_i(X_0, t) \in \mathbb{Q}[t]$. Rather, this corollary shows that, after removing common factors, the quot. of Thm. 10 will be a quot. of $\mathbb{Q}$-polynomials (and independent of ℓ!).

· We now move towards proving that the P_i are integral polynomials.

· For any (closed) point x of X_0, the function field $K(x_0)$ is a fin. field ext. of $\mathbb{F}_q$, so we write

$$\deg x := [K(x) : \mathbb{F}_q].$$

Conversely, a point in $X_0(\mathbb{F}_{q^m})$ is a map $\operatorname{Spec} \mathbb{F}_{q^m} \to X_0$, but giving such a map with image $x \in X_0$ is equivalent to giving an $\mathbb{F}_q$-hom. $K(x) \to \mathbb{F}_{q^m}$. We define $N_m(x) := \#\{\mathbb{F}_q\text{-hom. } K(x) \to \mathbb{F}_{q^m}\}$ such that

$$N_m = \sum_{x \text{ cl.pt.}} N_m(x) .$$

The theory of finite fields shows that

$$N_m(x) = \begin{cases} \deg x & \text{if } \deg x \mid m \\ 0 & \text{otherwise.} \end{cases}$$

Since $\log\left(\frac{1}{1-s}\right) = \sum_{m \geq 1} \frac{s^m}{m}$, we have that

$$\log\left(\frac{1}{1-t^{\deg x}}\right) = \sum_{n \geq 1} \frac{t^{n \cdot \deg x}}{n} .$$

But note that, if we rewrite the summands:

$$\frac{t^{n \cdot \deg x}}{n} = \deg x \cdot \frac{t^{n \cdot \deg x}}{n \cdot \deg x} = \deg x \cdot \frac{t^m}{m}$$

$\uparrow$

$m := n \cdot \deg x$

And then, the sum over n becomes a sum over m where the terms are 0 if $\deg x \nmid m$ and $\deg x \cdot \frac{t^m}{m}$ otherwise.

Clearly,

$$\log\left(\frac{1}{1-t^{\deg x}}\right) = \sum_{m \geq 1} N_m(x) \cdot \frac{t^m}{m} .$$

Summing over all the closed points of X_0 and taking exponentials, it follows that

$$Z(X_0, t) = \sum_{m \geq 1} N_m \cdot \frac{t^m}{m} = \prod_{x \text{ cl.pt.}} \frac{1}{1-t^{\deg x}} .$$

Now, since

$$\frac{1}{1-t^{\deg x}} = \sum_{n \geq 0} t^{n \cdot \deg x} \in 1 + t \cdot \mathbb{Z}[\![t]\!], \text{ it follows that}$$

$$Z(X_0, t) \in 1 + t \cdot \mathbb{Z}[\![t]\!].$$

· Lemma 13. Let ℓ be a prime (possibly equal to p), and let $f(t) = g(t)/h(t)$, with

$$f(t) \in 1 + t \cdot \mathbb{Z}_\ell[\![t]\!], \text{ and } g(t), h(t) \in 1 + t \cdot \mathbb{Q}_\ell[\![t]\!].$$

If g and h are coprime, then they have coefficients in $\mathbb{Z}_\ell$.

Proof | Omitted (see Milne's notes). ⊠

· Prop. 14. Let

$$Z(X_0, t) = \frac{P(X_0, t)}{Q(X_0, t)}$$

with $P(X_0, t)$ and $Q(X_0, t)$ two polynomials in $\mathbb{Q}[t]$ which are coprime (they exist by Cor. 12). Then, if P and Q both have constant term 1, they have coefficients in $\mathbb{Z}$.

Proof | By Lemma 13,

$$P, Q \in 1 + t \cdot \mathbb{Z}_\ell[\![t]\!]$$

for all primes ℓ (including p), so they are in $\mathbb{Z}[\![t]\!]$. ⊠

· Recall: Poincaré Duality. If Y is a nonsing. var. of dim. d over $k = \bar{k}$, and $\mathcal{F}$ is a loc. const. sheaf of $\Lambda = \mathbb{Z}/e\mathbb{Z}$-modules, then there exist perfect pairings of finite groups

$$H^r_c(Y, \mathcal{F}) \times H^{2d-r}(Y, \mathcal{F}^\vee(d)) \longrightarrow H^{2d}_c(Y, \Lambda(d)) \cong \Lambda.$$

If we consider now étale cohomology with $\mathbb{Q}_\ell$-coefficients, we get instead perfect pairings

$$H^r(Y, \mathbb{Q}_\ell) \times H^{2d-r}(Y, \mathbb{Q}_\ell) \longrightarrow H^{2d}(Y, \mathbb{Q}_\ell) \xrightarrow[\eta_Y]{\sim} \mathbb{Q}_\ell$$

(here we use that $H_c^r(Y, \mathbb{Q}_\ell) \cong H^r(Y, \mathbb{Q}_\ell)$).

- Using Poincaré Duality, it's easy to prove the functional equation.

- Thm. 15. For any complete nonsing. var. / $\mathbb{F}_q$,

$$Z\left(X_0, \frac{1}{q^d t}\right) = \pm q^{d\cdot\chi/2} \cdot t^\chi \cdot Z(X_0, t),$$

with $\chi := \sum_{r \geq 0} (-1)^r \beta_r = (\Delta \cdot \Delta)$.

$\beta_r = \dim_{\mathbb{Q}_\ell} H^r(X, \mathbb{Q}_\ell)$

Proof | By our definition of the Gysin map F_*, we have

$$\eta_{\bar{X}}(F_*(x) \cup x') = \eta_X(x \cup F^*(x')) \quad \forall x \in H^{2d-r}(\bar{X}, \mathbb{Q}_\ell), \forall x' \in H^r(\bar{X}, \mathbb{Q}_\ell).$$

Then, by the fact that

$$H^r(\bar{X}, \mathbb{Q}_\ell) \times H^{2d-r}(\bar{X}, \mathbb{Q}_\ell) \longrightarrow H^{2d}(\bar{X}, \mathbb{Q}_\ell) \xrightarrow[\eta_{\bar{X}}]{\sim} \mathbb{Q}_\ell$$

is a perfect pairing, it follows that the eigenvalues of F^* acting on $H^r(\bar{X}, \mathbb{Q}_\ell)$ are the same as those of F_* acting on $H^{2d-r}(\bar{X}, \mathbb{Q}_\ell)$.
But since $F_* \circ F^* = q^d$, then if $\alpha_1, \dots, \alpha_s$ are the eigenvalues of F^* on $H^r(\bar{X}, \mathbb{Q}_\ell)$, then $q^d/\alpha_1, \dots, q^d/\alpha_s$ are the eigenv. of F^* acting on $H^{2d-r}(\bar{X}, \mathbb{Q}_\ell)$.

Now specifically, write $\beta_r := \dim_{\mathbb{Q}_\ell} H^r(X, \mathbb{Q}_\ell)$ and $\{\alpha_{i,r}\}_{i=1}^{\beta_r}$ for the eigenvalues of F^* acting on $H^r(X, \mathbb{Q}_\ell)$. This shows that

$$\beta_r = \beta_{2d-r} \quad \text{and} \quad \{\alpha_{i,2d-r}\}_{i=1}^{\beta_{2d-r}} = \left\{ q^d / \alpha_{j,r} \right\}_{j=1}^{\beta_r} \quad (*)$$

for all $r = 0, \dots, 2d$.

Now, we want to compute $Z(X_0, \frac{1}{q^d t})$. For this, we first compute

$$P_r\left(X_0, \frac{1}{q^d t}\right) = \det\left(1 - F^* \cdot q^{-d} t^{-1} \mid H^r(X, \mathbb{Q}_\ell)\right) =$$

$$= \prod_{i=1}^{\beta_r} \left(1 - \alpha_{i,r} \cdot q^{-d} t^{-1}\right) \overset{(*)}{=} \prod_{i=1}^{\beta_{2d-r}} \left(1 - \alpha_{i,2d-r}^{-1} t^{-1}\right) =$$

$$= \prod_{i=1}^{\beta_{2d-r}} \left(\frac{\alpha_{i,2d-r}\, t - 1}{\alpha_{i,2d-r} \cdot t} \right) = \frac{(-1)^{\beta_{2d-r}} \cdot \prod_{i=1}^{\beta_{2d-r}} \left(1 - \alpha_{i,2d-r} t\right)}{t^{\beta_{2d-r}} \cdot \prod_{i=1}^{\beta_{2d-r}} \alpha_{i,2d-r}} =$$

$$= (-1)^{\beta_r} \cdot t^{-\beta_r} \left(\prod_{i=1}^{\beta_{2d-r}} \alpha_{i,2d-r} \right)^{-1} \cdot P_{2d-r}(X_0, t). \quad (\star)$$

Since $Z(X_0, t) = \prod_{r=0}^{2d} P_r(X_0, t)^{(-1)^{r+1}}$, we look at the product of the $(*)$ to these powers.

Firstly,

$$\prod_{r=0}^{2d} \left(t^{-\beta_r}\right)^{(-1)^{r+1}} = \prod_{r=0}^{2d} t^{(-1)^r \beta_r} = t^{\sum_{r=0}^{2d} (-1)^r \beta_r} =$$

$$= t^{\chi}.$$

↳ def. of χ

On the other hand, the fact that $F_* \circ F^* = q^d$ together with $(*)$ means that

$$q^{d\beta_r} = \alpha_{1,r} \cdot \ldots \cdot \alpha_{\beta_r, r} \cdot \alpha_{1,2d-r} \cdot \ldots \cdot \alpha_{\beta_{2d-r}, 2d-r},$$

det. of $q^d : H^r(X, \mathbb{Q}_\ell) \to H^r(X, \mathbb{Q}_\ell)$

It follows that we can group terms in the product

$$\prod_{r=0}^{2d} \left(\prod_{i=1}^{\beta_{2d-r}} \alpha_{i,2d-r} \right)^{(-1)(-1)^{r+1}},$$

in particular the terms of the form r and $2d-r$ for $r \neq d$ (note that $(-1)^{r+1} = (-1)^{2d-r+1}$), and we get that

$$\prod_{r=0}^{2d} \left(\prod_{i=1}^{\beta_{2d-r}} \alpha_{i,2d-r} \right)^{(-1)^r} = \left(\prod_{r=0}^{d-1} q^{(-1)^r d\beta_r} \right) \left(\prod_{i=1}^{\beta_d} \alpha_{i,d} \right)^{(-1)^d}.$$

But from our previous equality for $r=d$, we have that

$$q^{d\cdot\beta_d} = (\alpha_{1,d} \cdot \ldots \cdot \alpha_{\beta_d,d})^2 \Rightarrow \alpha_{1,d} \cdot \ldots \cdot \alpha_{\beta_d,d} = \pm q^{d\beta_d/2}.$$

Combining all of this, we see that

$$\prod_{r=0}^{2d} \left(\prod_{i=1}^{\beta_{2d-r}} \alpha_{i,2d-r} \right)^{(-1)^r} = \pm q^{(-1)^d d\beta_d} \cdot \prod_{r=0}^{d-1} q^{(-1)^r d\beta_r} =$$

$$= \pm q^{d\cdot\left(\sum_{r=0}^{d-1} (-1)^r \beta_r + (-1)^d \beta_r/2 \right)} = \pm q^{d\cdot\chi/2}.$$

$\chi/2$, since

$$\sum_{r=0}^{d-1} (-1)^r \beta_r = \sum_{r=d+1}^{2d} (-1)^r \beta_r$$

One obtains the desired functional equation by combining all of these results. ☒

- Summary: Let X_0 be a complete, nonsing. var. $/\mathbb{F}_q$.

(a) Then $Z(X_0,t) \in \mathbb{Q}(t)$, and it satisfies the functional eq.

$$Z\left(X_0, \tfrac{1}{q^d t}\right) = \pm q^{dx/2} \cdot t^x \cdot Z(X_0,t).$$

(This is conj. W2).

(b) For every prime $\ell \neq p$, we have an expression

$$Z(X_0,t) = \frac{P_{1,\ell}(t) \cdot \ldots \cdot P_{2d-1,\ell}(t)}{P_{0,\ell}(t) \cdot \ldots \cdot P_{2d,\ell}(t)},$$

with $P_{i,\ell}(t) \in \mathbb{Q}_\ell[t]$, and $P_{0,\ell}(t) = 1-t$, $P_{2d,\ell}(t) = 1-q^d t$.

(Not exactly conj. W1, we are missing integrality of the P_i).

(c) If, for a fixed ℓ, the $P_{r,\ell}$ are relatively prime pairwise, then, for $1 \leq r \leq 2d-1$,

$$P_{r,\ell}(t) = 1 + \sum a_{r,i} \cdot t^i \in \mathbb{Z}[t].$$

(This would finish the proof of W1).

(d) If for all primes $\ell \neq p$, the inverse roots of $P_{r,\ell}$ have abs. value $q^{r/2}$, then $P_{r,\ell}(t) \in 1 + t \cdot \mathbb{Z}[t]$ and they are independent of ℓ.

(e) Let $\beta_r = \deg P_r(t)$ as in the prev. proof. Then, $\chi = \sum (-1)^r \beta_r$, and if X_0 lifts to a var. X_1 in char. 0, then β_r are the Betti numbers of X_1 considered as a var. $/\mathbb{C}$.

(This would prove W3).

Proof

(a) Shown in Cor. 12 and Theo. 15.

(b) Shown in Theo. 10.

(c) If the $P_{r,\ell}(t)$ are relatively coprime in pairs, Prop. 14 shows that

$$\underbrace{\prod_{r \text{ odd}} P_{r,\ell}(t)}_{\text{numerator}} \in 1 + t \cdot \mathbb{Z}[t], \qquad \underbrace{\prod_{r \text{ even}} P_{r,\ell}(t)}_{\text{denominator}} \in 1 + t \cdot \mathbb{Z}[t].$$

It follows that the inverse roots of each $P_{r,\ell}(t)$ are alg. integers (they are a root of one of these prods), and thus

$$P_{r,\ell}(t) \in 1 + t \cdot \mathbb{Z}[t].$$

↑ all of its roots are alg. ints.

(d) If we show that all of the $P_{r,\ell}(t)$ are pairwise coprime, (c) would give us our result. But since the roots of $P_{r,\ell}(t)$ and $P_{s,\ell}(t)$ have abs. value $q^{r/2}$ and $q^{s/2}$ respectively, these two polynomials can't share a root unless $r = s$.

Furthermore, each $P_{r,\ell}(t)$ is uniquely characterized as the factor of the numerator / denominator with roots with abs. value $q^{r/2}$, and thus is independent of ℓ.

(e) When we say that X_0 can be lifted to char. 0, we mean that $\exists$ a DVR R with field of fractions K and res. field $\mathbb{F}$, and that $\exists$ a scheme $X_1 \longrightarrow \operatorname{Spec} R =: S$, proper and smooth over S,

such that $\mathcal{X}$ is its special fiber. Then, Proper and Locally acyclic base change shows that there is an iso.

$$R\Gamma(\mathcal{X}, \Lambda) \cong R\Gamma(\mathcal{X}_{\bar{s}}, \Lambda)$$

($\mathcal{X}$: special fibre of $\mathcal{X}_s$; $\mathcal{X}_{\bar{s}}$: generic fibre of $\mathcal{X}_s$)

for any finite gp. Λ of order prime to p.

More specifically, we get isos.

$$H^r(\mathcal{X}, \mathbb{Q}_\ell) \cong H^r(\mathcal{X}_{\bar{s}, K^{alg}}, \mathbb{C}) \quad \forall r \geq 0,$$

which proves (c). ⊠

· Notation: an element $\alpha \in K$, with $K \supseteq \mathbb{Q}$ a field is an algebraic number if it's the root of a poly. in $\mathbb{Q}[t]$. If we choose this poly. monic and irreducible, we call its other roots the complex conjugates of α.

· By this summary, if we prove the following result (which is W4), we will also prove W2, and will have then proved all of the Weil conjectures.

· Thm. 16. Let X_0 be a nonsing. proj. var. / $\mathbb{F}_q$. Then the eigenvalues of F acting on $H^r(\mathcal{X}, \mathbb{Q}_\ell)$ are alg. numbers, all of whose complex conjugates have abs. value $q^{r/2}$.

§ 3. Some reductions.

· **Lemma 17.** It suffices to prove Thm. 16 after replacing $\mathbb{F}_q$ by $\mathbb{F}_{q^m}$.

Proof The Frob. map $F_m : X \to X$ defined relatively to $X_0, \mathbb{F}_{q^m}$ is F^m, the m-th power of F. Therefore, if $\alpha_1, \dots, \alpha_s$ are the eigenvalues of F on $H^r(X, \mathbb{Q}_\ell)$, then $\alpha_1^m, \dots, \alpha_s^m$ will be those of F_m. Clearly, if α_i^m satisfies the condition of Thm. 16 for q^m, then α_i does w.r.t. q. ⊠

· **Recall: Künneth formula.** If Y_1, Y_2 are complete varieties over $k = \bar{k}$, then exist isoms.

$$\bigoplus_{r+s=n} H^r(Y_1, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} H^s(Y_2, \mathbb{Q}_\ell) \xrightarrow{\sim} H^n(Y_1 \times Y_2, \mathbb{Q}_\ell).$$

· We will now show that we only need to prove a weaker version of Thm. 16, by proving that the abs. values of the roots are in a range, rather than being a precise value.

· **Prop. 18.** Assume that, for all nonsing. proj. vars. X_0 of even dim. d over $\mathbb{F}_q$, every eigenvalue α of F on $H^d(\bar{X}, \mathbb{Q}_\ell)$ is an alg. number s.t.

$$q^{\frac{d}{2} - \frac{1}{2}} < |\alpha'| < q^{\frac{d}{2} + \frac{1}{2}}$$

for all complex conjugates α' of α. Then, Thm. 16 holds for all nonsing.

proj. varieties.

Proof: Let X_0 be a smo. proj. var. of dim. d (not nec. even!) over $\mathbb{F}_q$, and α an eigenvalue of F on $H^d(X, \mathbb{Q}_\ell)$.
By the Künneth formula, α^m is one of the eigenvalues of $H^{dm}(X^m, \mathbb{Q}_\ell)$ for all $m \geq 1$. By taking m even, we can apply our hypothesis to see that

$$q^{\frac{md}{2} - \frac{1}{2}} < |\alpha'|^m < q^{\frac{md}{2} + \frac{1}{2}}$$

for all complex conjugates α' of α.
If one takes the m-th root and the limit as $m \to \infty$ over the even integers, it follows that

$$|\alpha'| = q^{d/2} .$$

We will now prove Thm. 16 by induction on the dim. of X_0.

·) dim $X_0 = 0$: the only non-trivial coh. group is $H^0(X, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$, on which F acts as the identity (and $|1| = q^0$).

·) dim $X_0 = 1$: since $P_0(t) = 1 - t$, $P_2(t) = 1 - q^2 t$, there is nothing to show for these two. For $r = 1$, one uses our prev. reasoning for $d = 1$.

·) $d \geq 2$: as we saw in the proof of Thm. 15, if α is an eigenvalue for F acting on $H^r(X, \mathbb{Q}_\ell)$, then q^d/α is an eigenvalue for $H^{2d-r}(X, \mathbb{Q}_\ell)$. Thus, we may just prove Thm. 16 for $r > d$ (the case $r = d$ was proven above).

By Bertini's thm., $\exists$ a hyperplane $H \subseteq \mathbb{P}^m$ s.t. $Z := H \cap X$ is a nonsingular variety. By Lemma 17, we may assume that H (and thus Z) is defined over $\mathbb{F}_q$. Then, the Gysin sequence is of the form

$$\cdots \to H^{r-2}(Z, \mathbb{Q}_\ell(-1)) \to H^r(X, \mathbb{Q}_\ell) \to H^r(X \setminus Z, \mathbb{Q}_\ell) \to \cdots$$

Since $X \setminus Z \cong H$ is affine, $H^r(X \setminus Z, \mathbb{Q}_\ell) = 0$ for all $r > d$ (weak Lefschetz thm.). It follows that the Gysin map

$$i_* : H^{r-2}(Z, \mathbb{Q}_\ell(-1)) \to H^r(X, \mathbb{Q}_\ell)$$

is surj. for all $r > d$. By induction, the eigenvalues of F on $H^{r-2}(Z, \mathbb{Q}_\ell)$ are alg. numbers whose conjugates have abs. value $q^{(r-2)/2}$. Since

$$F^* \circ i_* = q \cdot (i_* \circ F^*), \quad \text{(Remm. 8(b))}$$

the eigenvalues of F acting on $H^r(X, \mathbb{Q}_\ell)$ are alg. numbers with abs. value $q^{(r-2)/2} \cdot q = q^{r/2}$. ⊠