The Riemann Hypothesis for Hypersurfaces

Ziquan Yang

Harvard University

October 26, 2020

RH for Hypersurfaces

- Let $\mathbb{F}_q$ be our base field. Let X_0 be a smooth projective variety over $\mathbb{F}_q$ and set $X := X_0 \otimes \bar{\mathbb{F}}_q$.

RH for Hypersurfaces

- Let $\mathbb{F}_q$ be our base field. Let X_0 be a smooth projective variety over $\mathbb{F}_q$ and set $X := X_0 \otimes \bar{\mathbb{F}}_q$.
- Recall that the RH for X_0 states that every eigenvalue α_i of the Frobenius action on $\mathrm{H}^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ has $|\iota(\alpha_i)| = q^{i/2}$ for every embedding $\iota : \bar{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$.

RH for Hypersurfaces

- Let $\mathbb{F}_q$ be our base field. Let X_0 be a smooth projective variety over $\mathbb{F}_q$ and set $X := X_0 \otimes \bar{\mathbb{F}}_q$.
- Recall that the RH for X_0 states that every eigenvalue α_i of the Frobenius action on $\mathrm{H}^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ has $|\iota(\alpha_i)| = q^{i/2}$ for every embedding $\iota : \bar{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$.
- Today we prove the RH for $X_0 \subset \mathbb{P}^{n+1}$ a smooth hypersurface of degree d. As usual we start with understanding the cohomology.

RH for Hypersurfaces

- Let $\mathbb{F}_q$ be our base field. Let X_0 be a smooth projective variety over $\mathbb{F}_q$ and set $X := X_0 \otimes \bar{\mathbb{F}}_q$.
- Recall that the RH for X_0 states that every eigenvalue α_i of the Frobenius action on $\mathrm{H}^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ has $|\iota(\alpha_i)| = q^{i/2}$ for every embedding $\iota : \bar{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$.
- Today we prove the RH for $X_0 \subset \mathbb{P}^{n+1}$ a smooth hypersurface of degree d. As usual we start with understanding the cohomology.
- First of all, we recall the cohomology of $\mathbb{P}^n$: $\mathrm{H}^*(\mathbb{P}^n) \cong \mathbb{Z}[h]/h^{n+1}$ where H is the class of a hyperplane H.

Lefschetz Hyperplane Theorem

Theorem (Lefschetz Hyperplane Theorem)

Let X be a smooth ample divisor of a smooth projective variety Y with $\dim Y = n+1$. Suppose the base field k is algebraically closed. Write $\mathrm{H}^j(-)$ for $\mathrm{H}^j_{\acute{e}t}((-), \mathbb{Q}_\ell)$, $\ell \neq \mathrm{char}\, \mathsf{k}$.

1. *$\mathrm{H}^j(Y) \to \mathrm{H}^j(X)$ is bijective for $j < n$ and injective for $j = n$.*
2. *$H_j(X) \to H_j(Y)$ is bijective for $j < n$ and surjective for $j = n$.*

Lefschetz Hyperplane Theorem

Theorem (Lefschetz Hyperplane Theorem)

Let X be a smooth ample divisor of a smooth projective variety Y with $\dim Y = n + 1$. Suppose the base field k is algebraically closed. Write $\mathrm{H}^j(-)$ for $\mathrm{H}^j_{ét}((-), \mathbb{Q}_\ell)$, $\ell \neq \mathrm{char}\,\mathsf{k}$.

1. $\mathrm{H}^j(Y) \to \mathrm{H}^j(X)$ *is bijective for $j < n$ and injective for $j = n$.*
2. $H_j(X) \to H_j(Y)$ *is bijective for $j < n$ and surjective for $j = n$.*

- Let's view $H_j(X)$ simply as $H^j(X)^\vee$.

Lefschetz Hyperplane Theorem

Theorem (Lefschetz Hyperplane Theorem)

Let X be a smooth ample divisor of a smooth projective variety Y with $\dim Y = n+1$. Suppose the base field k is algebraically closed. Write $\mathrm{H}^j(-)$ for $\mathrm{H}^j_{ét}((-), \mathbb{Q}_\ell)$, $\ell \neq \mathrm{char}\, \mathsf{k}$.

1. $\mathrm{H}^j(Y) \to \mathrm{H}^j(X)$ *is bijective for $j < n$ and injective for $j = n$.*
2. $H_j(X) \to H_j(Y)$ *is bijective for $j < n$ and surjective for $j = n$.*

- Let's view $H_j(X)$ simply as $H^j(X)^\vee$.
- Apply the above to $Y := \mathbb{P}^{n+1}$. Again let h denote the class of a hyperplane. For all $j \neq n$, we have $\mathrm{H}^j(X) \cong \mathbb{Q}_\ell(h^j) \cong \mathbb{Q}_\ell(j)$.

Lefschetz Hyperplane Theorem

Theorem (Lefschetz Hyperplane Theorem)

Let X be a smooth ample divisor of a smooth projective variety Y with $\dim Y = n+1$. Suppose the base field k is algebraically closed. Write $\mathrm{H}^j(-)$ for $\mathrm{H}^j_{ét}((-), \mathbb{Q}_\ell)$, $\ell \neq \mathrm{char}\,\mathsf{k}$.

1. $\mathrm{H}^j(Y) \to \mathrm{H}^j(X)$ *is bijective for* $j < n$ *and injective for* $j = n$.
2. $H_j(X) \to H_j(Y)$ *is bijective for* $j < n$ *and surjective for* $j = n$.

- Let's view $H_j(X)$ simply as $H^j(X)^\vee$.
- Apply the above to $Y := \mathbb{P}^{n+1}$. Again let h denote the class of a hyperplane. For all $j \neq n$, we have $\mathrm{H}^j(X) \cong \mathbb{Q}_\ell(h^j) \cong \mathbb{Q}_\ell(j)$.
- The only interesting part of the cohomology of X is $H^n(X)$.

Zeta Function of Hypersurfaces

- Back to our situation when $X_0 \subset \mathbb{P}^{n+1}$ is a hypersurface of degree d, and $X := X_0 \otimes \bar{\mathbb{F}}_q$.

Zeta Function of Hypersurfaces

- Back to our situation when $X_0 \subset \mathbb{P}^{n+1}$ is a hypersurface of degree d, and $X := X_0 \otimes \bar{\mathbb{F}}_q$.
- Let $h \in \mathrm{H}^2(X)$ be the hyperplane section. Consider the primitive cohomology

$$\mathrm{P}^n(X) = \mathrm{H}^n(X) \text{ if } n \text{ is odd, and } \mathrm{P}^n(X) = \mathrm{H}^n(X)/\langle h^{n/2} \rangle \text{ if } n \text{ is even.}$$

Then we have $H^*(X) \cong H^*(\mathbb{P}^n) \oplus \mathrm{P}^n(X)$.

Zeta Function of Hypersurfaces

- Back to our situation when $X_0 \subset \mathbb{P}^{n+1}$ is a hypersurface of degree d, and $X := X_0 \otimes \bar{\mathbb{F}}_q$.
- Let $h \in \mathrm{H}^2(X)$ be the hyperplane section. Consider the primitive cohomology

  $$\mathrm{P}^n(X) = \mathrm{H}^n(X) \text{ if } n \text{ is odd, and } \mathrm{P}^n(X) = \mathrm{H}^n(X)/\langle h^{n/2} \rangle \text{ if } n \text{ is even.}$$

  Then we have $H^*(X) \cong H^*(\mathbb{P}^n) \oplus \mathrm{P}^n(X)$.
- The Zeta function $Z(X_0, T)$ is given by

  $$\frac{P(T)}{\prod_{i=0}^{n}(1 - q^i T)} (n \text{ odd}), \text{ or } \frac{1}{P(T)\prod_{i=0}^{n}(1 - q^i T)} (n \text{ even})$$

  with $P(T) := \det(1 - T\mathrm{Frob}_q|_{\mathrm{P}^n(X_0)})$.

Zeta Function of Hypersurfaces

- Back to our situation when $X_0 \subset \mathbb{P}^{n+1}$ is a hypersurface of degree d, and $X := X_0 \otimes \bar{\mathbb{F}}_q$.
- Let $h \in \mathrm{H}^2(X)$ be the hyperplane section. Consider the primitive cohomology

  $$\mathrm{P}^n(X) = \mathrm{H}^n(X) \text{ if } n \text{ is odd, and } \mathrm{P}^n(X) = \mathrm{H}^n(X)/\langle h^{n/2} \rangle \text{ if } n \text{ is even.}$$

  Then we have $H^*(X) \cong H^*(\mathbb{P}^n) \oplus \mathrm{P}^n(X)$.
- The Zeta function $Z(X_0, T)$ is given by

  $$\frac{P(T)}{\prod_{i=0}^n (1 - q^i T)} (n \text{ odd}), \text{ or } \frac{1}{P(T) \prod_{i=0}^n (1 - q^i T)} (n \text{ even})$$

  with $P(T) := \det(1 - T\mathrm{Frob}_q|_{\mathrm{P}^n(X_0)})$.
- In either case, we see that $P(T)$ has integer coefficients. In particular, the coefficients are totally real.

Reduction to Point Counting

- Since $\alpha \mapsto q^n/\alpha$ defines an involution on the eigenvalues of Frob_q, it suffices to show that every eigenvalue of Frob_q on $\mathrm{P}^n(X)$ has ι-norm $\leq q^{n/2}$, for any $\iota : \bar{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$.

Reduction to Point Counting

- Since $\alpha \mapsto q^n/\alpha$ defines an involution on the eigenvalues of Frob_q, it suffices to show that every eigenvalue of Frob_q on $\mathrm{P}^n(X)$ has ι-norm $\leq q^{n/2}$, for any $\iota : \bar{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$.
- Recall that $H^*(X) \cong H^*(\mathbb{P}^n) \oplus \mathrm{P}^n(X)$, so that

$$\#X_0(\mathbb{F}_{q^r}) = \#\mathbb{P}^n(\mathbb{F}_{q^r}) + (-1)^r \mathrm{tr}((\mathrm{Frob}_q)^r|_{\mathrm{P}^n(X)})$$

by the point counting formula.

Reduction to Point Counting

- Since $\alpha \mapsto q^n/\alpha$ defines an involution on the eigenvalues of Frob_q, it suffices to show that every eigenvalue of Frob_q on $\mathrm{P}^n(X)$ has ι-norm $\leq q^{n/2}$, for any $\iota : \bar{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$.
- Recall that $H^*(X) \cong H^*(\mathbb{P}^n) \oplus \mathrm{P}^n(X)$, so that

$$\#X_0(\mathbb{F}_{q^r}) = \#\mathbb{P}^n(\mathbb{F}_{q^r}) + (-1)^r \mathrm{tr}((\mathrm{Frob}_q)^r|_{\mathrm{P}^n(X)})$$

  by the point counting formula.
- It suffices to show that

$$\#X_0(\mathbb{F}_{q^r}) = \#\mathbb{P}^n(\mathbb{F}_{q^r}) + O(q^{rn/2})$$

  as $r \geq 1$ varies.

Reduction to a Single Hypersurface

- Just as what we did last time, we first reduce to treating one hypersurface via deformation.

Reduction to a Single Hypersurface

- Just as what we did last time, we first reduce to treating one hypersurface via deformation.
- Let U_0 be an affine, smooth, and geometrically connected curve over $\mathbb{F}_q$ and $\mathcal{F}$ be an ℓ-adic local system (lisse $\bar{\mathbb{Q}}_\ell$-sheaf) on U_0.

Reduction to a Single Hypersurface

- Just as what we did last time, we first reduce to treating one hypersurface via deformation.
- Let U_0 be an affine, smooth, and geometrically connected curve over $\mathbb{F}_q$ and $\mathcal{F}$ be an ℓ-adic local system (lisse $\bar{\mathbb{Q}}_\ell$-sheaf) on U_0.
- For each closed point $u \in U_0$, we have a pullback $\mathcal{F}|_u$, which is an ℓ-adic local system on $\operatorname{Spec} \mathsf{k}(u)$.

Reduction to a Single Hypersurface

- Just as what we did last time, we first reduce to treating one hypersurface via deformation.
- Let U_0 be an affine, smooth, and geometrically connected curve over $\mathbb{F}_q$ and $\mathcal{F}$ be an ℓ-adic local system (lisse $\bar{\mathbb{Q}}_\ell$-sheaf) on U_0.
- For each closed point $u \in U_0$, we have a pullback $\mathcal{F}|_u$, which is an ℓ-adic local system on $\mathrm{Spec}\, \mathsf{k}(u)$.
- Recall that to giving such a local system amounts to giving a represention $\mathrm{Gal}_{\mathsf{k}(u)} \to \mathrm{GL}(\mathcal{F}_{\bar{u}})$ for the geometric point $\bar{u}$ over u.

Reduction to a Single Hypersurface

- Just as what we did last time, we first reduce to treating one hypersurface via deformation.
- Let U_0 be an affine, smooth, and geometrically connected curve over $\mathbb{F}_q$ and $\mathcal{F}$ be an ℓ-adic local system (lisse $\bar{\mathbb{Q}}_\ell$-sheaf) on U_0.
- For each closed point $u \in U_0$, we have a pullback $\mathcal{F}|_u$, which is an ℓ-adic local system on $\operatorname{Spec} \mathsf{k}(u)$.
- Recall that to giving such a local system amounts to giving a represention $\mathrm{Gal}_{\mathsf{k}(u)} \to \mathrm{GL}(\mathcal{F}_{\bar{u}})$ for the geometric point $\bar{u}$ over u.
- Let Frob_u be the generator of $\mathrm{Gal}_{\mathsf{k}(u)}$ given by $\lambda \mapsto \lambda^{\#\mathsf{k}(u)}$. Set

$$P_{\mathcal{F},u}(T) := \det(1 - T^{[\mathsf{k}(u):k]}\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}})$$

and

$$L_{\mathcal{F}}(T) := \prod_{u \in U} P_{\mathcal{F},u}(T)^{-1}.$$

Reduction to a Single Hypersurface

- Recall that last time we proved

Theorem

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u \in U_0$, every eigenvalue $\alpha_{i,u}$ of $\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}$ satisfies $|\iota(\alpha_{i,u})| \leq 1$. Then the same is true for any other closed point $u' \in U_0$.

Reduction to a Single Hypersurface

- Recall that last time we proved

Theorem

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u \in U_0$, every eigenvalue $\alpha_{i,u}$ of $\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}$ satisfies $|\iota(\alpha_{i,u})| \leq 1$. Then the same is true for any other closed point $u' \in U_0$.

- We also showed that the above theorem holds with $|\iota(\alpha_{i,u})| \leq 1$ replaced by $|\iota(\alpha_{i,u})| = 1$ (persistence of purity).

Reduction to a Single Hypersurface

- Recall that last time we proved

Theorem

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u \in U_0$, every eigenvalue $\alpha_{i,u}$ of $\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}$ satisfies $|\iota(\alpha_{i,u})| \leq 1$. Then the same is true for any other closed point $u' \in U_0$.

- We also showed that the above theorem holds with $|\iota(\alpha_{i,u})| \leq 1$ replaced by $|\iota(\alpha_{i,u})| = 1$ (persistence of purity).
- We first argue that given this, we can complete the reduction step.

Reduction to a Single Hypersurface

- Recall that last time we proved

Theorem

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u \in U_0$, every eigenvalue $\alpha_{i,u}$ of $\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}$ satisfies $|\iota(\alpha_{i,u})| \leq 1$. Then the same is true for any other closed point $u' \in U_0$.

- We also showed that the above theorem holds with $|\iota(\alpha_{i,u})| \leq 1$ replaced by $|\iota(\alpha_{i,u})| = 1$ (persistence of purity).
- We first argue that given this, we can complete the reduction step.
- Given two homogenous polynomials F_0, F_1, we can consider the pencil $tF_0 + (1-t)F_1$, thereby obtaining a family over $\mathbb{A}^1$. If F_0, F_1 are smooth, by removing singular fibers, we obtain a family $f : \mathcal{X} \to U$ containing F_0, F_1.

Reduction to a Single Hypersurface

- Recall that last time we proved

Theorem

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u \in U_0$, every eigenvalue $\alpha_{i,u}$ of $\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}$ satisfies $|\iota(\alpha_{i,u})| \leq 1$. Then the same is true for any other closed point $u' \in U_0$.

- We also showed that the above theorem holds with $|\iota(\alpha_{i,u})| \leq 1$ replaced by $|\iota(\alpha_{i,u})| = 1$ (persistence of purity).
- We first argue that given this, we can complete the reduction step.
- Given two homogenous polynomials F_0, F_1, we can consider the pencil $tF_0 + (1-t)F_1$, thereby obtaining a family over $\mathbb{A}^1$. If F_0, F_1 are smooth, by removing singular fibers, we obtain a family $f : \mathcal{X} \to U$ containing F_0, F_1.
- Apply the proposition to $\mathcal{F} := \mathbb{R}^n f_* \bar{\mathbb{Q}}_\ell(n/2)$. (Recall that the Zeta function ensures that our $\mathcal{F}$ is in fact integral.)

Interlude : Algebraic Groups

- Let k be a field and G be a k-variety. Let $m : G \times G \longrightarrow G$ be a morphism and $e : \mathrm{Spec}\, k \to G$ be a k-point.

Interlude : Algebraic Groups

- Let k be a field and G be a k-variety. Let $m : G \times G \to G$ be a morphism and $e : \mathrm{Spec}\, k \to G$ be a k-point.
- We say that (G, m, e) gives an algebraic group if m satisfies the group axioms with e being the identity.

Interlude : Algebraic Groups

- Let k be a field and G be a k-variety. Let $m : G \times G \to G$ be a morphism and $e : \operatorname{Spec} k \to G$ be a k-point.
- We say that (G, m, e) gives an algebraic group if m satisfies the group axioms with e being the identity.
- We say that G is a linear algebraic group it is isomorphic to a subgroup of GL_n for some n. An algebraic group is linear if and only if it is affine.

Interlude : Algebraic Groups

- Let k be a field and G be a k-variety. Let $m : G \times G \to G$ be a morphism and $e : \operatorname{Spec} k \to G$ be a k-point.
- We say that (G, m, e) gives an algebraic group if m satisfies the group axioms with e being the identity.
- We say that G is a linear algebraic group it is isomorphic to a subgroup of GL_n for some n. An algebraic group is linear if and only if it is affine.
- If $\operatorname{Spec} \mathcal{O}_G$ is equipped with the structure of an algebraic group, then $\mathcal{O}_G$ is equipped with a distinguished $\mathcal{O}_G \to k$ and a co-multiplication structure $\Delta : \mathcal{O}_G \to \mathcal{O}_G \otimes \mathcal{O}_G$.

Interlude : Algebraic Groups

- Let k be a field and G be a k-variety. Let $m : G \times G \to G$ be a morphism and $e : \mathrm{Spec}\, k \to G$ be a k-point.
- We say that (G, m, e) gives an algebraic group if m satisfies the group axioms with e being the identity.
- We say that G is a linear algebraic group it is isomorphic to a subgroup of GL_n for some n. An algebraic group is linear if and only if it is affine.
- If $\mathrm{Spec}\, \mathcal{O}_G$ is equipped with the structure of an algebraic group, then $\mathcal{O}_G$ is equipped with a distinguished $\mathcal{O}_G \to k$ and a co-multiplication structure $\Delta : \mathcal{O}_G \to \mathcal{O}_G \otimes \mathcal{O}_G$.
- For example, $\mathbb{G}_m$ is given by $\mathcal{O}_G := k[T^{\pm}]$ and $\Delta(T) = T \otimes T$.

Interlude : Algebraic Groups

- Let k be a field and G be a k-variety. Let $m : G \times G \to G$ be a morphism and $e : \operatorname{Spec} k \to G$ be a k-point.
- We say that (G, m, e) gives an algebraic group if m satisfies the group axioms with e being the identity.
- We say that G is a linear algebraic group it is isomorphic to a subgroup of GL_n for some n. An algebraic group is linear if and only if it is affine.
- If $\operatorname{Spec} \mathcal{O}_G$ is equipped with the structure of an algebraic group, then $\mathcal{O}_G$ is equipped with a distinguished $\mathcal{O}_G \to k$ and a co-multiplication structure $\Delta : \mathcal{O}_G \to \mathcal{O}_G \otimes \mathcal{O}_G$.
- For example, $\mathbb{G}_m$ is given by $\mathcal{O}_G := k[T^{\pm}]$ and $\Delta(T) = T \otimes T$.
- A *character* of a group G is a morphism $G \to \mathbb{G}_m$. The group of characters is denoted by $X^*(G)$.

Interlude : Groups of Multiplicative Type

- Given a finitely generated abelian group M. Consider the functor $\mathrm{Hom}(M, \mathbb{G}_m) : \mathsf{Alg}/k \to \mathsf{Grp}$ defined by $R \mapsto \mathrm{Hom}(M, R^\times)$.

Interlude : Groups of Multiplicative Type

- Given a finitely generated abelian group M. Consider the functor $\mathrm{Hom}(M, \mathbb{G}_m) : \mathsf{Alg}/k \to \mathsf{Grp}$ defined by $R \mapsto \mathrm{Hom}(M, R^\times)$.
- This functor is represented by a commutative algebraic group. When $M = \mathbb{Z}$, $\mathrm{Hom}(M, \mathbb{G}_m) = \mathbb{G}_m$.

Interlude : Groups of Multiplicative Type

- Given a finitely generated abelian group M. Consider the functor $\mathrm{Hom}(M, \mathbb{G}_m) : \mathsf{Alg}/k \to \mathsf{Grp}$ defined by $R \mapsto \mathrm{Hom}(M, R^\times)$.
- This functor is represented by a commutative algebraic group. When $M = \mathbb{Z}$, $\mathrm{Hom}(M, \mathbb{G}_m) = \mathbb{G}_m$.
- Groups obtained this way are said to be of *multiplicative type*.

Interlude : Groups of Multiplicative Type

- Given a finitely generated abelian group M. Consider the functor $\mathrm{Hom}(M, \mathbb{G}_m) : \mathsf{Alg}/k \to \mathsf{Grp}$ defined by $R \mapsto \mathrm{Hom}(M, R^\times)$.
- This functor is represented by a commutative algebraic group. When $M = \mathbb{Z}$, $\mathrm{Hom}(M, \mathbb{G}_m) = \mathbb{G}_m$.
- Groups obtained this way are said to be of *multiplicative type*.
- $\mathrm{Hom}(-, \mathbb{G}_m)$ and $X^*(-)$ are quasi-inverses to each other and defines an equivalence between the category groups of multiplicative type and the category of finitely generated abelian groups.

Interlude : Groups of Multiplicative Type

- Given a finitely generated abelian group M. Consider the functor $\mathrm{Hom}(M, \mathbb{G}_m) : \mathsf{Alg}/k \to \mathsf{Grp}$ defined by $R \mapsto \mathrm{Hom}(M, R^\times)$.
- This functor is represented by a commutative algebraic group. When $M = \mathbb{Z}$, $\mathrm{Hom}(M, \mathbb{G}_m) = \mathbb{G}_m$.
- Groups obtained this way are said to be of *multiplicative type*.
- $\mathrm{Hom}(-, \mathbb{G}_m)$ and $X^*(-)$ are quasi-inverses to each other and defines an equivalence between the category groups of multiplicative type and the category of finitely generated abelian groups.
- A morphism $G \to Q$ of algebraic groups is called a quotient map if it is *faithfully flat*.

Interlude : Groups of Multiplicative Type

- Given a finitely generated abelian group M. Consider the functor $\mathrm{Hom}(M, \mathbb{G}_m) : \mathsf{Alg}/k \to \mathsf{Grp}$ defined by $R \mapsto \mathrm{Hom}(M, R^\times)$.
- This functor is represented by a commutative algebraic group. When $M = \mathbb{Z}$, $\mathrm{Hom}(M, \mathbb{G}_m) = \mathbb{G}_m$.
- Groups obtained this way are said to be of *multiplicative type*.
- $\mathrm{Hom}(-, \mathbb{G}_m)$ and $X^*(-)$ are quasi-inverses to each other and defines an equivalence between the category groups of multiplicative type and the category of finitely generated abelian groups.
- A morphism $G \to Q$ of algebraic groups is called a quotient map if it is *faithfully flat*.
- Fact: Every normal algebraic group N of G arises the kernel of a quotient map $G \to Q$.

Interlude: Galois cohomology

- If $0 \to N \to G \to Q \to 0$ is an exact sequence, then the induced sequence $0 \to N(\bar{k}) \to G(\bar{k}) \to Q(\bar{k}) \to 0$ is exact.

Interlude: Galois cohomology

- If $0 \to N \to G \to Q \to 0$ is an exact sequence, then the induced sequence $0 \to N(\bar{k}) \to G(\bar{k}) \to Q(\bar{k}) \to 0$ is exact.
- To obtain information on k-points, we need to apply Galois cohomology $H^i(\mathrm{Gal}_k, -), i = 0, 1$,

$$0 \to N(k) \to G(k) \to Q(k) \to \mathrm{H}^1(k, N(\bar{k})) \to \cdots$$

Interlude: Galois cohomology

- If $0 \to N \to G \to Q \to 0$ is an exact sequence, then the induced sequence $0 \to N(\bar{k}) \to G(\bar{k}) \to Q(\bar{k}) \to 0$ is exact.
- To obtain information on k-points, we need to apply Galois cohomology $H^i(\mathrm{Gal}_k, -), i = 0, 1$,

$$0 \to N(k) \to G(k) \to Q(k) \to \mathrm{H}^1(k, N(\bar{k})) \to \cdots$$

- Hilbert theorem 90: $\mathrm{H}^1(k, \mathbb{G}_m(\bar{k})) = 0$ for any field k.

Interlude: Galois cohomology

- If $0 \to N \to G \to Q \to 0$ is an exact sequence, then the induced sequence $0 \to N(\bar{k}) \to G(\bar{k}) \to Q(\bar{k}) \to 0$ is exact.
- To obtain information on k-points, we need to apply Galois cohomology $H^i(\mathrm{Gal}_k, -), i = 0, 1,$

$$0 \to N(k) \to G(k) \to Q(k) \to \mathrm{H}^1(k, N(\bar{k})) \to \cdots$$

- Hilbert theorem 90: $\mathrm{H}^1(k, \mathbb{G}_m(\bar{k})) = 0$ for any field k.
- Example: $\mathrm{H}^1(k, \mu_n(\bar{k})) = k^\times/(k^\times)^n$, for $\mu_n := \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m)$.

Interlude : Gauss Sums

- Let $\mathbb{F}_q$ be a finite field. $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a mutliplicative character and $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be an additive character.

Interlude : Gauss Sums

- Let $\mathbb{F}_q$ be a finite field. $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a mutliplicative character and $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be an additive character.
- Set $\mu(\chi, \psi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x)$.

Interlude : Gauss Sums

- Let $\mathbb{F}_q$ be a finite field. $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a mutliplicative character and $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be an additive character.
- Set $\mu(\chi, \psi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x)$.
- It is hard to compute $\mu(\chi, \psi)$ in general, but we know its norm:

Theorem

If χ and ψ are both nontrivial, then $|\mu(\chi, \psi)| = \sqrt{q}$.

Interlude : Gauss Sums

- Let $\mathbb{F}_q$ be a finite field. $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a mutliplicative character and $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be an additive character.
- Set $\mu(\chi, \psi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x)$.
- It is hard to compute $\mu(\chi, \psi)$ in general, but we know its norm:

Theorem

If χ and ψ are both nontrivial, then $|\mu(\chi, \psi)| = \sqrt{q}$.

- The proof uses orthogonality relaitions in the character theory of finite groups, as well as some elementary tricks of rearranging the order of summations.

Interlude : Gauss Sums

- Let $\mathbb{F}_q$ be a finite field. $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a mutliplicative character and $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be an additive character.
- Set $\mu(\chi, \psi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x)$.
- It is hard to compute $\mu(\chi, \psi)$ in general, but we know its norm:

Theorem

If χ and ψ are both nontrivial, then $|\mu(\chi, \psi)| = \sqrt{q}$.

- The proof uses orthogonality relaitions in the character theory of finite groups, as well as some elementary tricks of rearranging the order of summations.
- Reference: Kowalski's notes `https://people.math.ethz.ch/~kowalski/exp-sums.pdf`.

Point Counting

- Recall that it suffices to show that for some smooth hypersurface X_0 of degree d in $\mathbb{P}^{n+1}$, we have the point-count estimate:

$$\#X_0(\mathbb{F}_{q^r}) = \#\mathbb{P}^n(\mathbb{F}_{q^r}) + O(q^{rn/2})$$

as $r \to \infty$.

Point Counting

- Recall that it suffices to show that for some smooth hypersurface X_0 of degree d in $\mathbb{P}^{n+1}$, we have the point-count estimate:

  $$\#X_0(\mathbb{F}_{q^r}) = \#\mathbb{P}^n(\mathbb{F}_{q^r}) + O(q^{rn/2})$$

  as $r \to \infty$.
- If $p \nmid d$, we can just use the Fermat hypersurface $x_0^d + \cdots + x_{n+1}^d = 0$. Weil provided a formula for the number of solutions $\sum_{i=0}^r a_i x_i^{n_i} = b$ in $\mathbb{A}^{r+1}$, so the bound can be checked by hand.

Point Counting

- Recall that it suffices to show that for some smooth hypersurface X_0 of degree d in $\mathbb{P}^{n+1}$, we have the point-count estimate:

$$\#X_0(\mathbb{F}_{q^r}) = \#\mathbb{P}^n(\mathbb{F}_{q^r}) + O(q^{rn/2})$$

  as $r \to \infty$.
- If $p \nmid d$, we can just use the Fermat hypersurface $x_0^d + \cdots + x_{n+1}^d = 0$. Weil provided a formula for the number of solutions $\sum_{i=0}^r a_i x_i^{n_i} = b$ in $\mathbb{A}^{r+1}$, so the bound can be checked by hand.
- We treat the case $d = 2$ separately (this only matters when $p = 2$).

$$\mathrm{H}^n(X) = \begin{cases} \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell, & \text{if } n \text{ is even,} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

Point Counting

- Recall that it suffices to show that for some smooth hypersurface X_0 of degree d in $\mathbb{P}^{n+1}$, we have the point-count estimate:

$$\#X_0(\mathbb{F}_{q^r}) = \#\mathbb{P}^n(\mathbb{F}_{q^r}) + O(q^{rn/2})$$

  as $r \to \infty$.
- If $p \nmid d$, we can just use the Fermat hypersurface $x_0^d + \cdots + x_{n+1}^d = 0$. Weil provided a formula for the number of solutions $\sum_{i=0}^r a_i x_i^{n_i} = b$ in $\mathbb{A}^{r+1}$, so the bound can be checked by hand.
- We treat the case $d = 2$ separately (this only matters when $p = 2$).

$$\mathrm{H}^n(X) = \begin{cases} \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell, & \text{if } n \text{ is even,} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

- To compute $\dim \mathrm{H}^n(X)$, it suffices to compute the Euler characteristic. Moreover, when n is even, $\mathrm{H}^n(X)$ is spanned by algebraic classes. (e.g., $X \simeq \mathbb{P}^1 \times \mathbb{P}^1$ when $n = 2$.)

Gabber's Hypersurface

- If $d \geq 3$ and $p \mid d$, use Gabber's hypersurface

$$X_0^d + \sum_{i=0}^{n} X_i X_{i+1}^{d-1} = 0.$$

Gabber's Hypersurface

- If $d \geq 3$ and $p \mid d$, use Gabber's hypersurface

$$X_0^d + \sum_{i=0}^{n} X_i X_{i+1}^{d-1} = 0.$$

- We consider the affine cone $H_0^{\mathrm{aff}} \subset \mathbb{A}^{n+2}$ defined by the same equation. It suffices to show that

$$\# H_0^{\mathrm{aff}}(\mathbb{F}_{q^r}) = q^{r(n+1)} + O(q^{r(n+2)/2})$$

Gabber's Hypersurface

- If $d \geq 3$ and $p \mid d$, use Gabber's hypersurface

$$X_0^d + \sum_{i=0}^{n} X_i X_{i+1}^{d-1} = 0.$$

- We consider the affine cone $H_0^{\mathrm{aff}} \subset \mathbb{A}^{n+2}$ defined by the same equation. It suffices to show that

$$\# H_0^{\mathrm{aff}}(\mathbb{F}_{q^r}) = q^{r(n+1)} + O(q^{r(n+2)/2})$$

- For an N-tuple $W = (w_1, \cdots, w_N)$ of nonnegative integers, we write X^W for the monomial $X_1^{w_1} \cdots X_N^{w_N}$.

Theorem

Let $N \geq 1$, and $X^{W_1}, \cdots, X^{W_N}$ be N monomials in N variables with W_i's linearly independent over $\mathbb{Q}$. Suppose that each variable X_i occurs in at most two of these monomials. Then for $V := \sum_i X^{W_i} = 0$ in $\mathbb{A}^N$, we have $\# V(\mathbb{F}_q) = q^{N-1} + O(q^{N/2})$.

Delsarte's Theorem

Theorem (Delsarte)

Let $N > k \geq 0$ and suppose given $N-k$ linearly independent monomials $X^{W_1}, \cdots, X_N^{W_N}$ in N variables. Let $V := \{\sum_i X_i^{W_i} = 0\}$ and $V^* := V \cap (\mathbb{G}_m^N \cap \mathbb{A}_m^N)$. Then $\#V^*(\mathbb{F}_q) = q^{-1}(q-1)^N + O(q^{(N+k)/2})$.

Delsarte's Theorem

Theorem (Delsarte)

Let $N > k \geq 0$ and suppose given $N - k$ linearly independent monomials $X^{W_1}, \cdots, X_N^{W_N}$ in N variables. Let $V := \{\sum_i X_i^{W_i} = 0\}$ and $V^* := V \cap (\mathbb{G}_m^N \cap \mathbb{A}_m^N)$. Then $\#V^*(\mathbb{F}_q) = q^{-1}(q-1)^N + O(q^{(N+k)/2})$.

- We omit the reduction step to Delsarte's theorem (This step uses that each variable X_i occurs in at most two of the variables.)

Delsarte's Theorem

Theorem (Delsarte)

Let $N > k \geq 0$ and suppose given $N-k$ linearly independent monomials $X^{W_1}, \cdots, X_N^{W_N}$ in N variables. Let $V := \{\sum_i X_i^{W_i} = 0\}$ and $V^* := V \cap (\mathbb{G}_m^N \cap \mathbb{A}_m^N)$. Then $\#V^*(\mathbb{F}_q) = q^{-1}(q-1)^N + O(q^{(N+k)/2})$.

- We omit the reduction step to Delsarte's theorem (This step uses that each variable X_i occurs in at most two of the variables.)
- We view the $N-k$ linearly independent vectors W_i as giving rise to an surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{F}_q$: $(X_1, \cdots, X_N) \mapsto (X^{W_1}, \cdots, X^{W_{N-k}})$. Then we only need to show:

Delsarte's Theorem

Theorem (Delsarte)

Let $N > k \geq 0$ and suppose given $N-k$ linearly independent monomials $X^{W_1}, \cdots, X_N^{W_N}$ in N variables. Let $V := \{\sum_i X_i^{W_i} = 0\}$ and $V^* := V \cap (\mathbb{G}_m^N \cap \mathbb{A}_m^N)$. Then $\#V^*(\mathbb{F}_q) = q^{-1}(q-1)^N + O(q^{(N+k)/2})$.

- We omit the reduction step to Delsarte's theorem (This step uses that each variable X_i occurs in at most two of the variables.)
- We view the $N-k$ linearly independent vectors W_i as giving rise to an surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{F}_q$: $(X_1, \cdots, X_N) \mapsto (X^{W_1}, \cdots, X^{W_{N-k}})$. Then we only need to show:

Theorem

Let $N > k \geq 0$, and suppose given a surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{F}_q$. Denote by $\Sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$ the sum of coordinates. Then

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

Count Points on Tori

Theorem

Let $N > k \geq 0$, and suppose given a surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{Z}$. Denote by $\Sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$ the sum of coordinates. Then

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

Count Points on Tori

Theorem

Let $N > k \geq 0$, and suppose given a surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{Z}$. Denote by $\Sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$ the sum of coordinates. Then

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

- By taking characters, ϕ is given by an injective group homomorphism $\phi^\vee : \mathbb{Z}^{N-k} \hookrightarrow \mathbb{Z}^N$ which sends e_i to W_i.

Count Points on Tori

Theorem

Let $N > k \geq 0$, and suppose given a surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{Z}$. Denote by $\Sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$ the sum of coordinates. Then

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

- By taking characters, ϕ is given by an injective group homomorphism $\phi^\vee : \mathbb{Z}^{N-k} \hookrightarrow \mathbb{Z}^N$ which sends e_i to W_i.
- We have that $T^*(\ker(\phi)) = \operatorname{coker}(\phi^\vee)$. Denote it by M.

Count Points on Tori

Theorem

Let $N > k \geq 0$, and suppose given a surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{Z}$. Denote by $\Sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$ the sum of coordinates. Then

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

- By taking characters, ϕ is given by an injective group homomorphism $\phi^\vee : \mathbb{Z}^{N-k} \hookrightarrow \mathbb{Z}^N$ which sends e_i to W_i.
- We have that $T^*(\ker(\phi)) = \operatorname{coker}(\phi^\vee)$. Denote it by M.
- $\dim M \otimes \mathbb{Q} = k$ and consider $0 \to M_{\mathrm{tor}} \to M \to M/M_{\mathrm{tor}} \cong \mathbb{Z}^k \to 0$.

Count Points on Tori

Theorem

Let $N > k \geq 0$, and suppose given a surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{Z}$. Denote by $\Sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$ the sum of coordinates. Then

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

- By taking characters, ϕ is given by an injective group homomorphism $\phi^\vee : \mathbb{Z}^{N-k} \hookrightarrow \mathbb{Z}^N$ which sends e_i to W_i.
- We have that $T^*(\ker(\phi)) = \mathrm{coker}(\phi^\vee)$. Denote it by M.
- $\dim M \otimes \mathbb{Q} = k$ and consider $0 \to M_{\mathrm{tor}} \to M \to M/M_{\mathrm{tor}} \cong \mathbb{Z}^k \to 0$.
- Taking $\mathrm{Hom}(-, \mathbb{G}_m)$, we obtain $0 \to \mathbb{G}_m^k \to \ker(\phi) \to \mu_{M_{\mathrm{tor}}} \to 0$.

Count Points on Tori

Theorem

Let $N > k \geq 0$, and suppose given a surjection $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ of split tori over $\mathbb{Z}$. Denote by $\Sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$ the sum of coordinates. Then

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

- By taking characters, ϕ is given by an injective group homomorphism $\phi^\vee : \mathbb{Z}^{N-k} \hookrightarrow \mathbb{Z}^N$ which sends e_i to W_i.
- We have that $T^*(\ker(\phi)) = \operatorname{coker}(\phi^\vee)$. Denote it by M.
- $\dim M \otimes \mathbb{Q} = k$ and consider $0 \to M_{\mathrm{tor}} \to M \to M/M_{\mathrm{tor}} \cong \mathbb{Z}^k \to 0$.
- Taking $\operatorname{Hom}(-, \mathbb{G}_m)$, we obtain $0 \to \mathbb{G}_m^k \to \ker(\phi) \to \mu_{M_{\mathrm{tor}}} \to 0$.
- We first treat the free part.

Counting Points on Tori

Recall the sequence $0 \to \mathbb{G}_m^k \to \ker(\phi) \to \mu_{M_{\mathrm{tor}}} \to 0$

Counting Points on Tori

Recall the sequence $0 \to \mathbb{G}_m^k \to \ker(\phi) \to \mu_{M_{\mathrm{tor}}} \to 0$

- The composite inclusion $\mathbb{G}_m^k \to \ker(\phi) \subset \mathbb{G}^N$ sits inside an exact sequence

$$0 \to \mathbb{G}_m^k \to \mathbb{G}_m^N \xrightarrow{\pi} \mathbb{G}_m^{N-k} \to 0.$$

Counting Points on Tori

Recall the sequence $0 \to \mathbb{G}_m^k \to \ker(\phi) \to \mu_{M_{\mathrm{tor}}} \to 0$

- The composite inclusion $\mathbb{G}_m^k \to \ker(\phi) \subset \mathbb{G}^N$ sits inside an exact sequence

$$0 \to \mathbb{G}_m^k \to \mathbb{G}_m^N \xrightarrow{\pi} \mathbb{G}_m^{N-k} \to 0.$$

- By Hilbert theorem 90 ($\mathrm{H}^1(\mathsf{k}, \mathbb{G}_m) = 0$ for any field k),

$$0 \to \mathbb{G}_m^k(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\pi} \mathbb{G}_m^{N-k}(\mathbb{F}_q) \to 0.$$

Counting Points on Tori

Recall the sequence $0 \to \mathbb{G}_m^k \to \ker(\phi) \to \mu_{M_{\mathrm{tor}}} \to 0$

- The composite inclusion $\mathbb{G}_m^k \to \ker(\phi) \subset \mathbb{G}^N$ sits inside an exact sequence
$$0 \to \mathbb{G}_m^k \to \mathbb{G}_m^N \xrightarrow{\pi} \mathbb{G}_m^{N-k} \to 0.$$
- By Hilbert theorem 90 ($\mathrm{H}^1(\mathrm{k}, \mathbb{G}_m) = 0$ for any field k),
$$0 \to \mathbb{G}_m^k(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\pi} \mathbb{G}_m^{N-k}(\mathbb{F}_q) \to 0.$$
- By construction, ϕ factors as $\mathbb{G}_m^N \xrightarrow{\pi} \mathbb{G}_m^{N-k} \xrightarrow{\bar{\phi}} \mathbb{G}_m^{N-k}$. Hence
$$|\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\}| = (q-1)^k |\{x \in \mathbb{G}_m^{N-k}(\mathbb{F}_q) : \Sigma(\bar{\phi}(x)) = 0\}|.$$

Counting Points on Tori

Recall the sequence $0 \to \mathbb{G}_m^k \to \ker(\phi) \to \mu_{M_{\mathrm{tor}}} \to 0$

- The composite inclusion $\mathbb{G}_m^k \to \ker(\phi) \subset \mathbb{G}^N$ sits inside an exact sequence
$$0 \to \mathbb{G}_m^k \to \mathbb{G}_m^N \xrightarrow{\pi} \mathbb{G}_m^{N-k} \to 0.$$
- By Hilbert theorem 90 ($\mathrm{H}^1(\mathrm{k}, \mathbb{G}_m) = 0$ for any field k),
$$0 \to \mathbb{G}_m^k(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\pi} \mathbb{G}_m^{N-k}(\mathbb{F}_q) \to 0.$$
- By construction, ϕ factors as $\mathbb{G}_m^N \xrightarrow{\pi} \mathbb{G}_m^{N-k} \xrightarrow{\bar{\phi}} \mathbb{G}_m^{N-k}$. Hence
$$|\{x \in \mathbb{G}_m^N(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\}| = (q-1)^k |\{x \in \mathbb{G}_m^{N-k}(\mathbb{F}_q) : \Sigma(\bar{\phi}(x)) = 0\}|.$$
- Recall that we want a big O estimate of the LHS, now we reduce to considering the RHS. Hence we reduce to the case $k = 0$.

Counting Points on Tori

- Our new goal: Given $0 \to \mu_{M_{\mathrm{tor}}} \to \mathbb{G}_m^N \xrightarrow{\phi} \mathbb{G}_m^N \to 0$, estimate $T := \#\{x \in \mathbb{G}_m^N(\mathbb{F}_q)(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\}$. Let's write $\mu_{M_{\mathrm{tor}}}$ simply as μ.

Counting Points on Tori

- Our new goal: Given $0 \to \mu_{M_{\mathrm{tor}}} \to \mathbb{G}_m^N \xrightarrow{\phi} \mathbb{G}_m^N \to 0$, estimate $T := \#\{x \in \mathbb{G}_m^N(\mathbb{F}_q)(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\}$. Let's write $\mu_{M_{\mathrm{tor}}}$ simply as μ.
- Hilbert theorem 90 gives a four term SES

$$0 \to \mu(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\phi} \mathbb{G}_m^N(\mathbb{F}_q) \to \mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q)) \to 0.$$

Note that $\#\mu(\mathbb{F}_q) = \#\mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q))$

Counting Points on Tori

- Our new goal: Given $0 \to \mu_{M_{\mathrm{tor}}} \to \mathbb{G}_m^N \xrightarrow{\phi} \mathbb{G}_m^N \to 0$, estimate $T := \#\{x \in \mathbb{G}_m^N(\mathbb{F}_q)(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\}$. Let's write $\mu_{M_{\mathrm{tor}}}$ simply as μ.
- Hilbert theorem 90 gives a four term SES

$$0 \to \mu(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\phi} \mathbb{G}_m^N(\mathbb{F}_q) \to \mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q)) \to 0.$$

  Note that $\#\mu(\mathbb{F}_q) = \#\mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q))$
- $T = (\#\mu(\mathbb{F}_q)) \cdot (\#\{t \in \mathbb{G}_m^N(\mathbb{F}_q) : \sum_i t_i = 0, t \in \mathrm{im}(\phi)\})$

Counting Points on Tori

- Our new goal: Given $0 \to \mu_{M_{\mathrm{tor}}} \to \mathbb{G}_m^N \xrightarrow{\phi} \mathbb{G}_m^N \to 0$, estimate $T := \#\{x \in \mathbb{G}_m^N(\mathbb{F}_q)(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\}$. Let's write $\mu_{M_{\mathrm{tor}}}$ simply as μ.
- Hilbert theorem 90 gives a four term SES

$$0 \to \mu(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\phi} \mathbb{G}_m^N(\mathbb{F}_q) \to \mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q)) \to 0.$$

  Note that $\#\mu(\mathbb{F}_q) = \#\mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q))$
- $T = (\#\mu(\mathbb{F}_q)) \cdot (\#\{t \in \mathbb{G}_m^N(\mathbb{F}_q) : \sum_i t_i = 0, t \in \mathrm{im}(\phi)\})$
- Consider $\mathcal{K} := \ker(\mathrm{Hom}(\mathbb{G}_m^N(\mathbb{F}_q), \mathbb{C}^\times) \to \mathrm{Hom}(\mathbb{G}_m^N(\mathbb{F}_q), \mathbb{C}^\times))$. Then

$$\sum_{\chi \in \mathcal{K}} \chi(t) = \#\mu(\mathbb{F}_q) \text{ if } t \in \mathrm{im}(\phi)\text{, and 0 otherwise.}$$

Counting Points on Tori

- Our new goal: Given $0 \to \mu_{M_{\mathrm{tor}}} \to \mathbb{G}_m^N \xrightarrow{\phi} \mathbb{G}_m^N \to 0$, estimate $T := \#\{x \in \mathbb{G}_m^N(\mathbb{F}_q)(\mathbb{F}_q) : \Sigma(\phi(x)) = 0\}$. Let's write $\mu_{M_{\mathrm{tor}}}$ simply as μ.
- Hilbert theorem 90 gives a four term SES

$$0 \to \mu(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\phi} \mathbb{G}_m^N(\mathbb{F}_q) \to \mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q)) \to 0.$$

  Note that $\#\mu(\mathbb{F}_q) = \#\mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q))$
- $T = (\#\mu(\mathbb{F}_q)) \cdot (\#\{t \in \mathbb{G}_m^N(\mathbb{F}_q) : \sum_i t_i = 0, t \in \mathrm{im}(\phi)\})$
- Consider $\mathcal{K} := \ker(\mathrm{Hom}(\mathbb{G}_m^N(\mathbb{F}_q), \mathbb{C}^\times) \to \mathrm{Hom}(\mathbb{G}_m^N(\mathbb{F}_q), \mathbb{C}^\times))$. Then

$$\sum_{\chi \in \mathcal{K}} \chi(t) = \#\mu(\mathbb{F}_q) \text{ if } t \in \mathrm{im}(\phi), \text{ and 0 otherwise.}$$

- Therefore, we get

$$T = \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q), \sum_i t_i = 0} \sum_{\chi \in \mathcal{K}} \chi(t).$$

Gauss Sums

- Take a nontrivial additive character $\psi : \mathbb{G}_a(\mathbb{F}_q) = \mathbb{F}_q \to \mathbb{C}^\times$. We have

$$\sum_{a \in \mathbb{F}_q} \psi(ax) = q \text{ if } x = 0 \text{ and } 0 \text{ otherwise.}$$

Gauss Sums

- Take a nontrivial additive character $\psi : \mathbb{G}_a(\mathbb{F}_q) = \mathbb{F}_q \to \mathbb{C}^\times$. We have

$$\sum_{a\in\mathbb{F}_q} \psi(ax) = q \text{ if } x = 0 \text{ and } 0 \text{ otherwise.}$$

- Now we rewrite the sum as

$$T = \frac{1}{q} \sum_{a\in\mathbb{F}_q} \sum_{\chi\in\mathcal{K}} \sum_{t\in\mathbb{G}_m^N(\mathbb{F}_q)} \chi(t)\psi(a \sum_i t_i).$$

Gauss Sums

- Take a nontrivial additive character $\psi : \mathbb{G}_a(\mathbb{F}_q) = \mathbb{F}_q \to \mathbb{C}^\times$. We have

$$\sum_{a \in \mathbb{F}_q} \psi(ax) = q \text{ if } x = 0 \text{ and } 0 \text{ otherwise.}$$

- Now we rewrite the sum as

$$T = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi(a \sum_i t_i).$$

- Recall that we have

Theorem (Modulus of Gauss sums)

For any nontrivial additive character ψ and nontrivial multiplicative character χ on $\mathbb{F}_q$, $|\sum_{t \in \mathbb{F}_q^\times} \chi(t)\psi(t)| = \sqrt{q}$.

Gauss Sums

$$T = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi(a \sum_i t_i)$$

Gauss Sums

$$T = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi(a \sum_i t_i)$$

- The $a = 0$ term is $q^{-1} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) = q^{-1}(q-1)^N$.

Gauss Sums

$$T = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi(a \sum_i t_i)$$

- The $a = 0$ term is $q^{-1} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) = q^{-1}(q-1)^N$.
- For the other a's, the term has norm $q^{N/2}$ (a product of N Gauss sums). There are $\#\mathcal{K} = \#\mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q)) \leq \# M_{\mathrm{tor}}$ of them.

Gauss Sums

$$T = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi(a \sum_i t_i)$$

- The $a = 0$ term is $q^{-1} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) = q^{-1}(q-1)^N$.
- For the other a's, the term has norm $q^{N/2}$ (a product of N Gauss sums). There are $\#\mathcal{K} = \#\mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q)) \leq \#M_{\mathrm{tor}}$ of them.
- To sum up, we have

$$|T - \frac{(q-1)^N}{q}| \leq \frac{q-1}{q} \# M_{\mathrm{tor}} q^{N/2}.$$

Gauss Sums

$$T = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) \psi(a \sum_i t_i)$$

- The $a = 0$ term is $q^{-1} \sum_{\chi \in \mathcal{K}} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t) = q^{-1}(q-1)^N$.
- For the other a's, the term has norm $q^{N/2}$ (a product of N Gauss sums). There are $\#\mathcal{K} = \#\mathrm{H}^1(\mathbb{F}_q, \mu(\bar{\mathbb{F}}_q)) \leq \#M_{\mathrm{tor}}$ of them.
- To sum up, we have

$$|T - \frac{(q-1)^N}{q}| \leq \frac{q-1}{q} \#M_{\mathrm{tor}} q^{N/2}.$$

- Now we are done!

(From now on optional) Torsors

- Let G be a group and S be a set on which G acts on the right. We say that S is a G-torsor if for every $s \in S$, the map $G \longrightarrow S$ defined by $g \mapsto sg$ is a bijection.

(From now on optional) Torsors

- Let G be a group and S be a set on which G acts on the right. We say that S is a G-torsor if for every $s \in S$, the map $G \to S$ defined by $g \mapsto sg$ is a bijection.
- Now suppose X is a scheme, $\mathcal{G}$ is a sheaf of groups on $X_{\text{ét}}$ and $\mathcal{S}$ is a sheaf of sets on $X_{\text{ét}}$. We say that $\mathcal{S}$ is a $\mathcal{G}$-torsor if
  - for some covering $\{U_i\} \to X$, $\mathcal{S}(U_i) \neq \emptyset$ for each U_i;
  - for every $U \to X$ étale and $s \in \Gamma(U, \mathcal{S})$, the map $g \mapsto sg : \mathcal{G}|_U \to \mathcal{S}|_U$ is an isomorphism of sheaves.

(From now on optional) Torsors

- Let G be a group and S be a set on which G acts on the right. We say that S is a G-torsor if for every $s \in S$, the map $G \longrightarrow S$ defined by $g \mapsto sg$ is a bijection.
- Now suppose X is a scheme, $\mathcal{G}$ is a sheaf of groups on $X_{\text{ét}}$ and $\mathcal{S}$ is a sheaf of sets on $X_{\text{ét}}$. We say that $\mathcal{S}$ is a $\mathcal{G}$-torsor if
  - for some covering $\{U_i\} \longrightarrow X$, $\mathcal{S}(U_i) \neq \emptyset$ for each U_i;
  - for every $U \longrightarrow X$ étale and $s \in \Gamma(U, \mathcal{S})$, the map $g \mapsto sg : \mathcal{G}|_U \longrightarrow \mathcal{S}|_U$ is an isomorphism of sheaves.
- Assume that every finite subset of X is contained in an open affine and X is quasi-compact (e.g., X is a quasi-projective variety). Then for any sheaf of abelian groups $\mathcal{F}$, Čech cohomology agrees with derived functor cohomology, so that elements $\mathrm{H}^1(X_{\text{ét}}, \mathcal{F})$ correspond bijectively to isomorphism classes of $\mathcal{F}$-torsors.

(From now on optional) Torsors

- Let G be a group and S be a set on which G acts on the right. We say that S is a G-torsor if for every $s \in S$, the map $G \to S$ defined by $g \mapsto sg$ is a bijection.
- Now suppose X is a scheme, $\mathcal{G}$ is a sheaf of groups on $X_{\text{ét}}$ and $\mathcal{S}$ is a sheaf of sets on $X_{\text{ét}}$. We say that $\mathcal{S}$ is a $\mathcal{G}$-torsor if
  - for some covering $\{U_i\} \to X$, $\mathcal{S}(U_i) \neq \emptyset$ for each U_i;
  - for every $U \to X$ étale and $s \in \Gamma(U, \mathcal{S})$, the map $g \mapsto sg : \mathcal{G}|_U \to \mathcal{S}|_U$ is an isomorphism of sheaves.
- Assume that every finite subset of X is contained in an open affine and X is quasi-compact (e.g., X is a quasi-projective variety). Then for any sheaf of abelian groups $\mathcal{F}$, Čech cohomology agrees with derived functor cohomology, so that elements $\mathrm{H}^1(X_{\text{ét}}, \mathcal{F})$ correspond bijectively to isomorphism classes of $\mathcal{F}$-torsors.
- Torsors of a finite group G over X are representable by a Galois cover of X (not necessarily connected).

(From now on optional) Torsors

- Let G be a group and S be a set on which G acts on the right. We say that S is a G-torsor if for every $s \in S$, the map $G \to S$ defined by $g \mapsto sg$ is a bijection.
- Now suppose X is a scheme, $\mathcal{G}$ is a sheaf of groups on $X_{\text{ét}}$ and $\mathcal{S}$ is a sheaf of sets on $X_{\text{ét}}$. We say that $\mathcal{S}$ is a $\mathcal{G}$-torsor if
  - for some covering $\{U_i\} \to X$, $\mathcal{S}(U_i) \neq \emptyset$ for each U_i;
  - for every $U \to X$ étale and $s \in \Gamma(U, \mathcal{S})$, the map $g \mapsto sg : \mathcal{G}|_U \to \mathcal{S}|_U$ is an isomorphism of sheaves.
- Assume that every finite subset of X is contained in an open affine and X is quasi-compact (e.g., X is a quasi-projective variety). Then for any sheaf of abelian groups $\mathcal{F}$, Čech cohomology agrees with derived functor cohomology, so that elements $\mathrm{H}^1(X_{\text{ét}}, \mathcal{F})$ correspond bijectively to isomorphism classes of $\mathcal{F}$-torsors.
- Torsors of a finite group G over X are representable by a Galois cover of X (not necessarily connected).
- If G is a profinite abelian group, then there is a canonical identification $\mathrm{H}^1(X_{\text{ét}}, G) = \mathrm{Hom}_{\text{cts}}(\pi_1^{\text{ét}}(X), G)$.

Persistence of purity

- We go over the persistence of purity theorem with a bit more detail.

Theorem (Persistence of Purity)

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u_0 \in U_0$, every eigenvalue α_{i,u_0} of $\mathrm{Frob}_{u_0}|_{\mathcal{F}_{\bar{u}_0}}$ satisfies $|\iota(\alpha_{i,u_0})| = 1$. Then the same is true for any other closed point $u \in U_0$.

Persistence of purity

- We go over the persistence of purity theorem with a bit more detail.

Theorem (Persistence of Purity)

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u_0 \in U_0$, every eigenvalue α_{i,u_0} of $\mathrm{Frob}_{u_0}|_{\mathcal{F}_{\bar{u}_0}}$ satisfies $|\iota(\alpha_{i,u_0})| = 1$. Then the same is true for any other closed point $u \in U_0$.

- We already know that $|\iota(\alpha_{i,u'})| \leq 1$ for every i. Therefore, it suffices to prove that $|\iota(\det(\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}))| = 1$.

Persistence of purity

- We go over the persistence of purity theorem with a bit more detail.

Theorem (Persistence of Purity)

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u_0 \in U_0$, every eigenvalue α_{i,u_0} of $\mathrm{Frob}_{u_0}|_{\mathcal{F}_{\bar{u}_0}}$ satisfies $|\iota(\alpha_{i,u_0})| = 1$. Then the same is true for any other closed point $u \in U_0$.

- We already know that $|\iota(\alpha_{i,u'})| \leq 1$ for every i. Therefore, it suffices to prove that $|\iota(\det(\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}))| = 1$.
- We reduce to proving that $\det(\mathcal{F})$ is ι-pure of weight 0 if $\det(\mathcal{F}|_{u_0})$ is.

Persistence of purity

- We go over the persistence of purity theorem with a bit more detail.

Theorem (Persistence of Purity)

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u_0 \in U_0$, every eigenvalue α_{i,u_0} of $\mathrm{Frob}_{u_0}|_{\mathcal{F}_{\bar{u}_0}}$ satisfies $|\iota(\alpha_{i,u_0})| = 1$. Then the same is true for any other closed point $u \in U_0$.

- We already know that $|\iota(\alpha_{i,u'})| \leq 1$ for every i. Therefore, it suffices to prove that $|\iota(\det(\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}))| = 1$.
- We reduce to proving that $\det(\mathcal{F})$ is ι-pure of weight 0 if $\det(\mathcal{F}|_{u_0})$ is.
- In order to do this, we may of course replace $\det(\mathcal{F})$ by any power $\det(\mathcal{F})^{\otimes m}$ for any $m \geq 1$. Therefore, it suffices to prove the following:

Persistence of purity

- We go over the persistence of purity theorem with a bit more detail.

Theorem (Persistence of Purity)

Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $u_0 \in U_0$, every eigenvalue α_{i,u_0} of $\mathrm{Frob}_{u_0}|_{\mathcal{F}_{\bar{u}_0}}$ satisfies $|\iota(\alpha_{i,u_0})| = 1$. Then the same is true for any other closed point $u \in U_0$.

- We already know that $|\iota(\alpha_{i,u'})| \leq 1$ for every i. Therefore, it suffices to prove that $|\iota(\det(\mathrm{Frob}_u|_{\mathcal{F}_{\bar{u}}}))| = 1$.
- We reduce to proving that $\det(\mathcal{F})$ is ι-pure of weight 0 if $\det(\mathcal{F}|_{u_0})$ is.
- In order to do this, we may of course replace $\det(\mathcal{F})$ by any power $\det(\mathcal{F})^{\otimes m}$ for any $m \geq 1$. Therefore, it suffices to prove the following:

Lemma

Let $\mathcal{L}$ be an ℓ-adic local system on U_0 of rank 1. Then for some power $\mathcal{L}^{\otimes m}$, there exists $\alpha \in \bar{\mathbb{Q}}_\ell^\times$ such that $\mathrm{Frob}_u|_{\mathcal{L}^{\otimes m}} = \alpha^{\deg u}$.

Generalities

Generalities

- Put $\mathsf{k} = \mathbb{F}_q$ and choose an algebraic closure $\bar{\mathsf{k}}/\mathsf{k}$. The sequence $U \to U_0 \to \operatorname{Spec} \mathsf{k}$ induces a short exact sequence

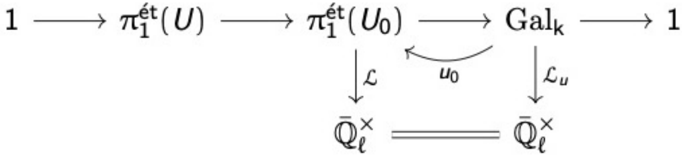
$$1 \to \pi_1^{\text{ét}}(U, \bar{u}_0) \to \pi_1^{\text{ét}}(U_0, \bar{u}_0) \to \pi_1^{\text{ét}}(\operatorname{Spec} \mathsf{k}, \bar{u}_0) \to 1.$$

Generalities

- Put $\mathsf{k} = \mathbb{F}_q$ and choose an algebraic closure $\bar{\mathsf{k}}/\mathsf{k}$. The sequence $U \to U_0 \to \operatorname{Spec} \mathsf{k}$ induces a short exact sequence
$$1 \to \pi_1^{\text{ét}}(U, \bar{u}_0) \to \pi_1^{\text{ét}}(U_0, \bar{u}_0) \to \pi_1^{\text{ét}}(\operatorname{Spec} \mathsf{k}, \bar{u}_0) \to 1.$$
- Assume that u_0 is defined over k. Then $(u_0, \bar{u}_0) \to (U, \bar{u}_0)$ induces a splitting
$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathsf{k}, \bar{u}_0) = \operatorname{Gal}_{\mathsf{k}} \to \pi_1^{\text{ét}}(U_0, \bar{u}_0).$$

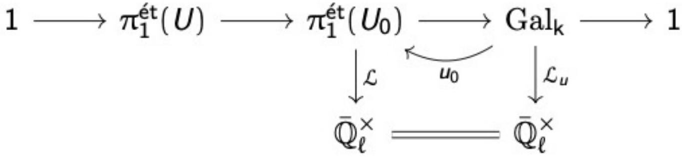
Generalities

- Put $\mathsf{k} = \mathbb{F}_q$ and choose an algebraic closure $\bar{\mathsf{k}}/\mathsf{k}$. The sequence $U \to U_0 \to \operatorname{Spec} \mathsf{k}$ induces a short exact sequence
$$1 \to \pi_1^{\text{ét}}(U, \bar{u}_0) \to \pi_1^{\text{ét}}(U_0, \bar{u}_0) \to \pi_1^{\text{ét}}(\operatorname{Spec} \mathsf{k}, \bar{u}_0) \to 1.$$
- Assume that u_0 is defined over k. Then $(u_0, \bar{u}_0) \to (U, \bar{u}_0)$ induces a splitting
$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathsf{k}, \bar{u}_0) = \mathrm{Gal}_{\mathsf{k}} \to \pi_1^{\text{ét}}(U_0, \bar{u}_0).$$
- We now have a picture



Generalities

- Put $\mathsf{k} = \mathbb{F}_q$ and choose an algebraic closure $\bar{\mathsf{k}}/\mathsf{k}$. The sequence $U \to U_0 \to \operatorname{Spec} \mathsf{k}$ induces a short exact sequence
$$1 \to \pi_1^{\text{ét}}(U, \bar{u}_0) \to \pi_1^{\text{ét}}(U_0, \bar{u}_0) \to \pi_1^{\text{ét}}(\operatorname{Spec} \mathsf{k}, \bar{u}_0) \to 1.$$
- Assume that u_0 is defined over k. Then $(u_0, \bar{u}_0) \to (U, \bar{u}_0)$ induces a splitting
$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathsf{k}, \bar{u}_0) = \mathrm{Gal}_{\mathsf{k}} \to \pi_1^{\text{ét}}(U_0, \bar{u}_0).$$
- We now have a picture



- Via the splitting, $\mathrm{Gal}_{\mathsf{k}}$ acts by conjugation on $\pi_1^{\text{ét}}(U)$, and hence on $\pi_1^{\text{ét}}(U)$-representations. This action fixes $\mathcal{L}|_{\pi_1^{\text{ét}}(U)}$.

Proof of Persistence of Purity

- Since $\pi_1^{\text{ét}}(U_0)$ is compact, $\mathcal{L} : \pi_1^{\text{ét}}(U_0) \to \bar{\mathbb{Q}}_\ell^\times$ lands in $\mathcal{O}_{E_\lambda}^\times$ for some finite extension $E_\lambda/\mathbb{Q}_\ell$. Let $\mathbb{F}_\lambda$ be the residue field, where $\lambda \in \ell^\infty$.

Proof of Persistence of Purity

- Since $\pi_1^{\text{ét}}(U_0)$ is compact, $\mathcal{L} : \pi_1^{\text{ét}}(U_0) \to \bar{\mathbb{Q}}_\ell^\times$ lands in $\mathcal{O}_{E_\lambda}^\times$ for some finite extension $E_\lambda/\mathbb{Q}_\ell$. Let $\mathbb{F}_\lambda$ be the residue field, where $\lambda \in \ell^\infty$.
- Up to replacing $\mathcal{L}$ by its $\#\mathbb{F}_\lambda^\times$-power, $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \mathfrak{m}_\lambda$, where $\mathfrak{m}_\lambda \subset \mathcal{O}_{E_\lambda}$ is the maximal ideal.

Proof of Persistence of Purity

- Since $\pi_1^{\text{ét}}(U_0)$ is compact, $\mathcal{L} : \pi_1^{\text{ét}}(U_0) \to \bar{\mathbb{Q}}_\ell^\times$ lands in $\mathcal{O}_{E_\lambda}^\times$ for some finite extension $E_\lambda/\mathbb{Q}_\ell$. Let $\mathbb{F}_\lambda$ be the residue field, where $\lambda \in \ell^\infty$.
- Up to replacing $\mathcal{L}$ by its $\#\mathbb{F}_\lambda^\times$-power, $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \mathfrak{m}_\lambda$, where $\mathfrak{m}_\lambda \subset \mathcal{O}_{E_\lambda}$ is the maximal ideal.
- Up to replacing $\mathcal{L}$ again by its ℓ-th power, we may assume $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \ell\mathfrak{m}_\lambda$, which is isomorphic to $\ell\mathfrak{m}_\lambda \subset \bar{\mathbb{Q}}_\ell$ via the logarithm. Hence $\mathcal{L}$ gives rise to an element in $\mathrm{Hom}_{\mathrm{cts}}(U_0, \bar{\mathbb{Q}}_\ell)$.

Proof of Persistence of Purity

- Since $\pi_1^{\text{ét}}(U_0)$ is compact, $\mathcal{L} : \pi_1^{\text{ét}}(U_0) \to \bar{\mathbb{Q}}_\ell^\times$ lands in $\mathcal{O}_{E_\lambda}^\times$ for some finite extension $E_\lambda/\mathbb{Q}_\ell$. Let $\mathbb{F}_\lambda$ be the residue field, where $\lambda \in \ell^\infty$.
- Up to replacing $\mathcal{L}$ by its $\#\mathbb{F}_\lambda^\times$-power, $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \mathfrak{m}_\lambda$, where $\mathfrak{m}_\lambda \subset \mathcal{O}_{E_\lambda}$ is the maximal ideal.
- Up to replacing $\mathcal{L}$ again by its ℓ-th power, we may assume $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \ell\mathfrak{m}_\lambda$, which is isomorphic to $\ell\mathfrak{m}_\lambda \subset \bar{\mathbb{Q}}_\ell$ via the logarithm. Hence $\mathcal{L}$ gives rise to an element in $\mathrm{Hom}_{\mathrm{cts}}(U_0, \bar{\mathbb{Q}}_\ell)$.
- Recall that $\mathrm{Hom}_{\mathrm{cts}}(U_0, \bar{\mathbb{Q}}_\ell)$ is identified with $\mathrm{H}^1(U_0, \bar{\mathbb{Q}}_\ell)$, so we may view $\mathcal{L}$ as an element of $\mathrm{H}^1(U_0, \bar{\mathbb{Q}}_\ell)$. Similarly, $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} \in \mathrm{H}^1(U, \bar{\mathbb{Q}}_\ell)$.

Proof of Persistence of Purity

- Since $\pi_1^{\text{ét}}(U_0)$ is compact, $\mathcal{L} : \pi_1^{\text{ét}}(U_0) \to \bar{\mathbb{Q}}_\ell^\times$ lands in $\mathcal{O}_{E_\lambda}^\times$ for some finite extension $E_\lambda/\mathbb{Q}_\ell$. Let $\mathbb{F}_\lambda$ be the residue field, where $\lambda \in \ell^\infty$.
- Up to replacing $\mathcal{L}$ by its $\#\mathbb{F}_\lambda^\times$-power, $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \mathfrak{m}_\lambda$, where $\mathfrak{m}_\lambda \subset \mathcal{O}_{E_\lambda}$ is the maximal ideal.
- Up to replacing $\mathcal{L}$ again by its ℓ-th power, we may assume $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \ell\mathfrak{m}_\lambda$, which is isomorphic to $\ell\mathfrak{m}_\lambda \subset \bar{\mathbb{Q}}_\ell$ via the logarithm. Hence $\mathcal{L}$ gives rise to an element in $\mathrm{Hom}_{\mathrm{cts}}(U_0, \bar{\mathbb{Q}}_\ell)$.
- Recall that $\mathrm{Hom}_{\mathrm{cts}}(U_0, \bar{\mathbb{Q}}_\ell)$ is identified with $\mathrm{H}^1(U_0, \bar{\mathbb{Q}}_\ell)$, so we may view $\mathcal{L}$ as an element of $\mathrm{H}^1(U_0, \bar{\mathbb{Q}}_\ell)$. Similarly, $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} \in \mathrm{H}^1(U, \bar{\mathbb{Q}}_\ell)$.
- We have argued that $\mathcal{L}|_{\pi_1^{\text{ét}}(U)}$ is Frob_q-invariant. However, the RH for curves implies that eigenvalues of Frob_q on $H^1(U, \bar{\mathbb{Q}}_\ell) \cong H_c^1(U, \bar{\mathbb{Q}}_\ell)^\vee$ have absolute value $\geq q^{1/2} > 1$.

Proof of Persistence of Purity

- Since $\pi_1^{\text{ét}}(U_0)$ is compact, $\mathcal{L} : \pi_1^{\text{ét}}(U_0) \to \bar{\mathbb{Q}}_\ell^\times$ lands in $\mathcal{O}_{E_\lambda}^\times$ for some finite extension $E_\lambda/\mathbb{Q}_\ell$. Let $\mathbb{F}_\lambda$ be the residue field, where $\lambda \in \ell^\infty$.
- Up to replacing $\mathcal{L}$ by its $\#\mathbb{F}_\lambda^\times$-power, $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \mathfrak{m}_\lambda$, where $\mathfrak{m}_\lambda \subset \mathcal{O}_{E_\lambda}$ is the maximal ideal.
- Up to replacing $\mathcal{L}$ again by its ℓ-th power, we may assume $\mathcal{L}(\pi_1^{\text{ét}}(U_0)) \subseteq 1 + \ell\mathfrak{m}_\lambda$, which is isomorphic to $\ell\mathfrak{m}_\lambda \subset \bar{\mathbb{Q}}_\ell$ via the logarithm. Hence $\mathcal{L}$ gives rise to an element in $\mathrm{Hom}_{\mathrm{cts}}(U_0, \bar{\mathbb{Q}}_\ell)$.
- Recall that $\mathrm{Hom}_{\mathrm{cts}}(U_0, \bar{\mathbb{Q}}_\ell)$ is identified with $\mathrm{H}^1(U_0, \bar{\mathbb{Q}}_\ell)$, so we may view $\mathcal{L}$ as an element of $\mathrm{H}^1(U_0, \bar{\mathbb{Q}}_\ell)$. Similarly, $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} \in \mathrm{H}^1(U, \bar{\mathbb{Q}}_\ell)$.
- We have argued that $\mathcal{L}|_{\pi_1^{\text{ét}}(U)}$ is Frob_q-invariant. However, the RH for curves implies that eigenvalues of Frob_q on $H^1(U, \bar{\mathbb{Q}}_\ell) \cong H_c^1(U, \bar{\mathbb{Q}}_\ell)^\vee$ have absolute value $\geq q^{1/2} > 1$.
- Therefore, $\mathcal{L}|_{\pi_1^{\text{ét}}(U)}$ is trivial.

Proof of Persistence of Purity

- Recall that our goal is to show that for every closed point $u \in U_0$, $\mathrm{Frob}_u|_{\mathcal{L}_{\bar{u}}} = (\alpha)^{\deg u}$ for some $\alpha \in \bar{\mathbb{Q}}^\times$. The the point is that α is uniform over all points. ($\mathcal{L}$ has already been replaced by a power.)

Proof of Persistence of Purity

- Recall that our goal is to show that for every closed point $u \in U_0$, $\mathrm{Frob}_u|_{\mathcal{L}_{\bar{u}}} = (\alpha)^{\deg u}$ for some $\alpha \in \bar{\mathbb{Q}}^\times$. The the point is that α is uniform over all points. ($\mathcal{L}$ has already been replaced by a power.)
- This is a consequence of $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} = 0$ and α is just $\mathrm{Frob}_{u_0}|_{\mathcal{L}_{\bar{u}_0}}$.

Proof of Persistence of Purity

- Recall that our goal is to show that for every closed point $u \in U_0$, $\mathrm{Frob}_u|_{\mathcal{L}_{\bar{u}}} = (\alpha)^{\deg u}$ for some $\alpha \in \bar{\mathbb{Q}}^{\times}$. The the point is that α is uniform over all points. ($\mathcal{L}$ has already been replaced by a power.)
- This is a consequence of $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} = 0$ and α is just $\mathrm{Frob}_{u_0}|_{\mathcal{L}_{\bar{u}_0}}$.
- Up to replacing U by $U \otimes \mathsf{k}(u)$, we reduce to the case $\deg u = 1$.

Proof of Persistence of Purity

- Recall that our goal is to show that for every closed point $u \in U_0$, $\mathrm{Frob}_u|_{\mathcal{L}_{\bar{u}}} = (\alpha)^{\deg u}$ for some $\alpha \in \bar{\mathbb{Q}}^\times$. The the point is that α is uniform over all points. ($\mathcal{L}$ has already been replaced by a power.)
- This is a consequence of $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} = 0$ and α is just $\mathrm{Frob}_{u_0}|_{\mathcal{L}_{\bar{u}_0}}$.
- Up to replacing U by $U \otimes \mathsf{k}(u)$, we reduce to the case $\deg u = 1$.
- Consider the abelianization $\pi_1^{\text{ét}}(U_0)^{\mathrm{ab}} := \pi_1^{\text{ét}}(U_0, \bar{u}_0)^{\mathrm{ab}}$.

Proof of Persistence of Purity

- Recall that our goal is to show that for every closed point $u \in U_0$, $\mathrm{Frob}_u|_{\mathcal{L}_{\bar{u}}} = (\alpha)^{\deg u}$ for some $\alpha \in \bar{\mathbb{Q}}^\times$. The the point is that α is uniform over all points. ($\mathcal{L}$ has already been replaced by a power.)
- This is a consequence of $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} = 0$ and α is just $\mathrm{Frob}_{u_0}|_{\mathcal{L}_{\bar{u}_0}}$.
- Up to replacing U by $U \otimes \mathsf{k}(u)$, we reduce to the case $\deg u = 1$.
- Consider the abelianization $\pi_1^{\text{ét}}(U_0)^{\mathrm{ab}} := \pi_1^{\text{ét}}(U_0, \bar{u}_0)^{\mathrm{ab}}$.
- If we choose another geometric point $\bar{u}$ on U, and étale path $\bar{u}_0 \rightsquigarrow \bar{u}$, then we have an isomorphism $\pi_1^{\text{ét}}(U_0, \bar{u}_0) \xrightarrow{\sim} \pi_1^{\text{ét}}(U_0, \bar{u})$, which descends to $\pi_1^{\text{ét}}(U_0, \bar{u}_0)^{\mathrm{ab}} \xrightarrow{\sim} \pi_1^{\text{ét}}(U_0, \bar{u})^{\mathrm{ab}}$.

Proof of Persistence of Purity

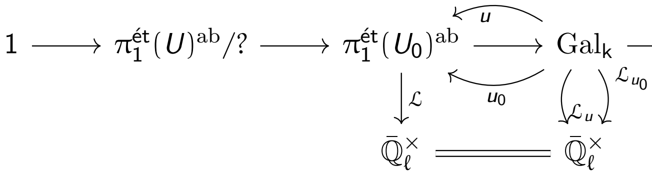
- Recall that our goal is to show that for every closed point $u \in U_0$, $\mathrm{Frob}_u|_{\mathcal{L}_{\bar{u}}} = (\alpha)^{\deg u}$ for some $\alpha \in \bar{\mathbb{Q}}^\times$. The the point is that α is uniform over all points. ($\mathcal{L}$ has already been replaced by a power.)
- This is a consequence of $\mathcal{L}|_{\pi_1^{\text{ét}}(U)} = 0$ and α is just $\mathrm{Frob}_{u_0}|_{\mathcal{L}_{\bar{u}_0}}$.
- Up to replacing U by $U \otimes \mathrm{k}(u)$, we reduce to the case $\deg u = 1$.
- Consider the abelianization $\pi_1^{\text{ét}}(U_0)^{\mathrm{ab}} := \pi_1^{\text{ét}}(U_0, \bar{u}_0)^{\mathrm{ab}}$.
- If we choose another geometric point $\bar{u}$ on U, and étale path $\bar{u}_0 \rightsquigarrow \bar{u}$, then we have an isomorphism $\pi_1^{\text{ét}}(U_0, \bar{u}_0) \xrightarrow{\sim} \pi_1^{\text{ét}}(U_0, \bar{u})$, which descends to $\pi_1^{\text{ét}}(U_0, \bar{u}_0)^{\mathrm{ab}} \xrightarrow{\sim} \pi_1^{\text{ét}}(U_0, \bar{u})^{\mathrm{ab}}$.
- The point is that the second isomorphism does not depend on the choice of the path $\bar{u}_0 \rightsquigarrow \bar{u}$.

Proof of Persistence of Purity

- Suppose we have another k-point $u \in U$. Then we have two sections.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1^{\text{ét}}(U)^{\mathrm{ab}}/? & \longrightarrow & \pi_1^{\text{ét}}(U_0)^{\mathrm{ab}} & \underset{u_0}{\overset{u}{\rightleftarrows}} & \mathrm{Gal}_{\mathsf{k}} & \longrightarrow & 1 \\ & & & & \downarrow \mathcal{L} & & \downarrow \mathcal{L}_u \ \downarrow \mathcal{L}_{u_0} & & \\ & & & & \bar{\mathbb{Q}}_\ell^\times & = & \bar{\mathbb{Q}}_\ell^\times & & \end{array}$$

- Suppose we have another k-point $u \in U$. Then we have two sections.

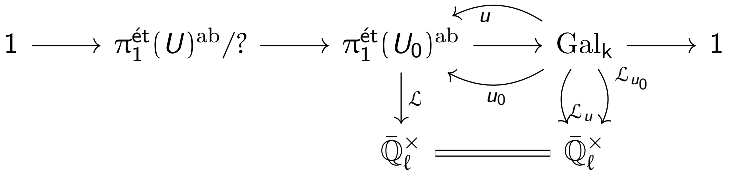


- Now the representation $\mathcal{L}_{u_0} - \mathcal{L}_u : \mathrm{Gal}_{\mathsf{k}} \to \bar{\mathbb{Q}}_\ell^\times$ is induced by

$$\mathrm{Gal}_{\mathsf{k}} \overset{u_0 - u}{\to} \pi_1^{\text{ét}}(U_0)^{\mathrm{ab}} \to \bar{\mathbb{Q}}_\ell^\times.$$

Proof of Persistence of Purity

- Suppose we have another k-point $u \in U$. Then we have two sections.



- Now the representation $\mathcal{L}_{u_0} - \mathcal{L}_u : \mathrm{Gal}_{\mathsf{k}} \to \bar{\mathbb{Q}}_\ell^\times$ is induced by

$$\mathrm{Gal}_{\mathsf{k}} \stackrel{u_0 - u}{\longrightarrow} \pi_1^{\text{ét}}(U_0)^{\mathrm{ab}} \to \bar{\mathbb{Q}}_\ell^\times.$$

- Since $u_0 - u$ lands in $\pi_1^{\text{ét}}(U)^{\mathrm{ab}}/?$, the above composition vanishes.