# Abelian Varieties over Finite Fields

## Tate's Theorem

Arieh Zimmerman

Hebrew University

March 2023

# Overview

Setup

- $X$ is an Abelian variety over $k$
- $\mathrm{char} k \neq \ell$ a prime
- $k_s$ is the separable closure of $k$
- Recall that the Tate module is

$$\mathbb{Z}_\ell^{2g} \cong T_\ell X = \lim_{\leftarrow} X(k_s)[\ell^n],$$

and define $V_\ell X := \mathbb{Q}_\ell \otimes T_\ell X$

# Overview

Goal

- Recall that $T_\ell$ is functorial, and there is a $\mathbb{Z}_\ell$-linear

$$T_\ell : \mathbb{Z}_\ell \otimes \mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y)$$

- Tate's Theorem: this is an isomorphism
- What we know: this map is injective with torsion-free cokernel

# Reductions

It suffices to show that

$$V_\ell : \mathbb{Q}_\ell \otimes \mathrm{Hom}(X, Y) \to \mathbb{Q}_\ell \otimes \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y)$$

is an isomorphism

## Proof.

$\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$, so

$$T_\ell \text{ injective} \Rightarrow V_\ell \text{ injective}$$
$$\mathrm{Coker}(T_\ell) = 0 \Leftrightarrow \mathbb{Q}_\ell \otimes \mathrm{Coker}(T_\ell) = 0$$
$$\mathbb{Q}_\ell \otimes \mathrm{Coker}(T_\ell) = \mathrm{Coker}(V_\ell).$$

Hence $V_\ell$ surjective $\Rightarrow$ $T_\ell$ surjective.

# Reductions

It suffices to show that, for any Abelian variety $Z$,

$$V_\ell : \mathbb{Q}_\ell \otimes \mathrm{End}(Z) \to \mathbb{Q}_\ell \otimes \mathrm{End}_{\mathrm{Gal}(k_s/k)}(T_\ell Z)$$

is an isomorphism.

## Proof.

Given $X, Y$, put $Z = X \times Y$. Then $T_\ell$ respects the decomposition

$$\mathrm{End}(Z) = \mathrm{End}(X) \oplus \mathrm{Hom}(X, Y) \oplus \mathrm{Hom}(Y, X) \oplus \mathrm{End}(Y).$$

If this has an isomorphism to $\mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell Z)$, its second component is an isomorphism to $\mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(V_\ell X, V_\ell Y)$.

# Strategy

- We now assume $k = \mathbb{F}_q$, so $k_s = \overline{k}$
- Fix $X$ over $k$
- The crux of the argument is a key lemma
- The lemma will also yield an important fact: $V_\ell X$ is semisimple as a $\mathrm{Gal}(\overline{k}/k)$-representation.

## Lemma

*For all $Gal(\overline{k}/k)$-subrepresentations $W \subseteq V_\ell X$, there is some $u \in \mathbb{Z}_\ell \otimes End(X)$ such that $V_\ell(u) V_\ell X = W$.*

We will use: There are finitely many isomorphism classes of Abelian varieties of dimension $g$ over $\mathbb{F}_q$

# Proof of Key Lemma: $\forall W \subseteq V_\ell$ subreps $\exists u \in \mathbb{Z}_l \otimes \mathrm{End}(X)$ s.t. $V_\ell(u) V_\ell X = W$

Facts we will use:

- There is a correspondence between étale $k$-group schemes and $\mathrm{Gal}(k_s/k)$-groups (group action by automorphisms) and we can consider $\mathscr{H}_n$ as the $k_s$-points of a subgroup scheme $H_n \subseteq X[\ell^n]$
- For any isogeny $f : X \to Y$ with kernel $N$ and $\ell$-Sylow subgroup $N_\ell(k_s)$, there is an exact sequence

$$0 \to T_\ell X \xrightarrow{T_\ell(f)} T_\ell Y_n \to N_\ell(k_s) \to 0.$$

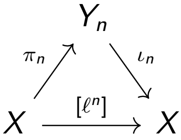
# Proof of Key Lemma: $\forall W \subseteq V_\ell$ subreps $\exists u \in \mathbb{Z}_l \otimes \mathrm{End}(X)$ s.t. $V_\ell(u)V_\ell X = W$

We will move to $\mathbb{Z}_\ell$ coefficients and use lattices!
Notation:

- $W' := W \cap T_\ell X$ a $\mathrm{Gal}(\overline{k}/k)$-stable sublattice
- $U_n := W' + \ell^n T_\ell X$ a $\mathrm{Gal}(\overline{k}/k)$-stable sublattice
- $\mathscr{H}_n \subseteq X(\overline{k})[\ell^n]$ is the image of $U_n$ under the quotient $T_\ell X \to T_\ell X/\ell^n T_\ell X \cong X(\overline{k})[l^n]$

# Proof of Key Lemma: $\forall W \subseteq V_\ell$ subreps $\exists u \in \mathbb{Z}_l \otimes \mathrm{End}(X)$ s.t. $V_\ell(u)V_\ell X = W$

Define a quotient $\pi_n : X \to X/H_n =: Y_n$. Knowing $[\ell^n]H_n = 0$ and $Y_n$ is a categorical quotient, we have a factorization




for some homomorphism $\iota_n$. Since $\pi_n$ is surjective and $[\ell^n]$ has finite kernel, we have $\iota_n$ is surjective with finite kernel, hence an isogeny. By the exact sequence above, $T_\ell(\iota_n) : T_\ell Y_n \to T_\ell X$ is injective. After identifying $T_\ell Y_n \subseteq T_\ell X$, we identify $T_\ell(\pi_n) = [\ell^n]$.

# Proof of Key Lemma: $\forall W \subseteq V_\ell$ subreps $\exists u \in \mathbb{Z}_l \otimes \mathrm{End}(X)$ s.t. $V_\ell(u) V_\ell X = W$

$|H_n(k_s)|$ divides $|X(\bar{k})[\ell^n]| = \ell^{2gn} \Rightarrow$
$H_n(k_s)$ is its own $\ell$-Psylow subgroup $\Rightarrow$

$$0 \to T_\ell X \xrightarrow{T_\ell \pi_n} T_\ell Y_n \to H_n(k_s) \to 0$$

is exact $\Rightarrow$
$\ell^n T_\ell X \subseteq T_\ell Y_n \subset T_\ell X$ and $T_\ell Y_n / \ell^n T_\ell X = U_n / \ell^n T_\ell X \Rightarrow$
$T_\ell Y_n \cong U_n$ (as sublattices and Galois representations).

# Proof of Key Lemma: $\forall W \subseteq V_\ell$ subreps $\exists u \in \mathbb{Z}_l \otimes \mathrm{End}(X)$ s.t. $V_\ell(u)V_\ell X = W$

There are finitely many isomorphism classes pigeonholing $\{Y_n\}_{n\in\mathbb{N}}$, yielding an increasing $\{n_i\}_{i\in\mathbb{N}}$ such that there are isomorphisms $\{\alpha_i : Y_{n_1} \xrightarrow{\sim} Y_{n_i}\}_{i\in\mathbb{N}}$. Define $u_i$ by compositions

$$\begin{array}{ccc} Y_{n_1} & \xrightarrow{\alpha_i} & Y_{n_i} \\ \pi_{n_1}\uparrow & & \downarrow\iota_{n_i} \\ X & \xrightarrow{u_i} & X \end{array} \quad \text{and apply } T_\ell \Rightarrow \quad \begin{array}{ccc} T_\ell Y_{n_1} & \xrightarrow{T_\ell(\alpha_i)} & T_\ell Y_{n_i} \\ \ell^n\cdot\uparrow & & \downarrow \\ T_\ell X & \xrightarrow{T_\ell(u_i)} & T_\ell X. \end{array}$$

Key Observation: $\mathbb{Z}_l \otimes \mathrm{End}(X)$ is compact! Moving to a subsequence, we can assume $u_i \to u \in \mathbb{Z}_l \otimes \mathrm{End}(X)$

# Proof of Key Lemma: $\forall W \subseteq V_\ell$ subreps $\exists u \in \mathbb{Z}_l \otimes \mathrm{End}(X)$ s.t. $V_\ell(u) V_\ell X = W$

- Recall $U_n = W' + \ell^n T_\ell X$, so $U_n \cong Y_n$ descending sets, hence $T_\ell(u) T_\ell X \subset \bigcap_{i \in \mathbb{N}} U_{n_i} = W'$.
- Claim: $\ell^{n_1} W' \subseteq T_\ell(u) T_\ell X$. Assume $x \in \ell^{n_1} W'$. Then $\exists y_i \in T_\ell X$ with $T_\ell(u_i)(y_i) = x$, so

$$T_\ell(u)(y_i) - x = T_\ell(u - u_i)(y_i) \to 0$$

  But the image of $T_\ell(u)$ is closed. This proves the claim.
- Tensoring

$$\ell^{n_1} W' \subseteq T_\ell(u) T_\ell X \subseteq W'$$

  with $\mathbb{Q}_\ell$ proves the lemma.

# Semisimplicity of $\rho_\ell$

For our fixed $X$, let $\rho_\ell : \mathrm{Gal}(\overline{k}/k) \to GL(V_\ell X)$ be the action on $V_\ell X$.

## Proposition

*The representation $\rho_\ell$ is semisimple.*

## Proof.

This amounts to finding a complement to any subrepresentation $W$. Take $u$ from the lemma.

$$\begin{aligned} \mathbb{Q}_\ell \otimes \mathrm{End}(X) \text{ semisimple} \Rightarrow \\ \exists e \in \mathbb{Q}_\ell \otimes \mathrm{End}(X) \text{ idempotent} : \ (u) = (e) \Rightarrow \\ \exists a, b : e = ua, \ u = eb \end{aligned}$$

# Semisimplicity of $\rho_\ell$

**Proof.**

Note $(1-e) \in Z(\mathbb{Q}_\ell \otimes \mathrm{End}(X))$ (also idempotent), so $V_\ell(1-e)V_\ell X$ is Galois-stable. It is a compliment to $V_\ell(e)V_\ell X$.
Claim: $V_\ell(e)V_\ell X = V_\ell(u)V_\ell X$

$$W = V_\ell(u)V_\ell X = V_\ell(e)V_\ell(b)V_\ell X \subseteq \\ V_\ell(e)V_\ell X = V_\ell(u)V_\ell(a)V_\ell X \subseteq V_\ell(u)V_\ell X = W$$

# Main Theorem

## Theorem (Tate)

*The functor $T_\ell$ is an isomorphism on Hom-sets.*

## Proof.

We know injectivity.
Surjectivity strategy: characterize image $R \subseteq \operatorname{End} V_\ell X$ of $\mathbb{Q}_\ell \otimes \operatorname{End}(X)$ using double centralizer theorem. It says

$$R = Z_{\operatorname{End}(V_\ell X)}(R)$$

(because everything is semisimple). So it suffices to show

$$\forall c \in \operatorname{End}_R(V_\ell X)\ \forall \varphi \in \operatorname{Gal}(\overline{k}/k) : \ c\rho_\ell(\varphi) = \rho_\ell(\varphi)c$$

# Main Theorem

## Proof.

Define the graph $V_\ell X \oplus V_\ell X \supseteq \Gamma_\varphi := \{(v, \rho_\ell(\varphi)v)\}_{v \in V_\ell X}$ a Galois-stable subspace. Take the corresponding $u \in \mathbb{Q}_\ell \otimes End(X \times X)$ from the lemma, and define

$$\gamma := \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \in M_2(R) \subseteq \mathrm{End}(V_\ell X \oplus V_\ell X).$$

Then $\gamma$ is central in $M_2(R)$, but $V_\ell(u)$ is also in $M_2(R)$. So $V_\ell(u)\gamma = \gamma V_\ell(u)$ and

$$\gamma \Gamma_\varphi = \gamma V_\ell(u)(V_\ell X \oplus V_\ell X) = V_\ell(u)\gamma(V_\ell X \oplus V_\ell X) \subseteq \Gamma_\varphi.$$

Taking the bottom-right entry of the matrix, this means

$$\forall v \in V_\ell X : \; c\rho_\ell(\varphi)v = \rho_\ell(\varphi)cv.$$