Sato-Tate groups of genus 2 curves

Kiran S. Kedlaya

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org

Arithmetic of Hyperelliptic Curves
NATO Advanced Study Institute
Ohrid, Macedonia, August 25–September 5, 2014

These slides: http://kskedlaya.org/slides/ohrid2014.pdf.
Lecture notes: http://kskedlaya.org/papers/nato-notes-2014.pdf.

Contents

Contents

Elliptic curves over finite fields and Hasse's theorem

Let E be an elliptic curve over a finite field $\mathbb{F}_q$.

Theorem (Hasse)

We have $\#E(\mathbb{F}_q) = q + 1 - a_q$ *where* $|a_q| \leq 2\sqrt{q}$.

For example, if E is in Weierstrass form

$$y^2 = x^3 + Ax + B$$

then Hasse's theorem is consistent with the natural guess from probability theory. (If the residue symbol of $x^3 + Ax + B$ were an independent random variable for each $x \in \mathbb{F}_q$, one would expect $q + 1 - \#E(\mathbb{F}_q)$ to be bounded by a fixed multiple of $\sqrt{q}$ with high probability.)

Elliptic curves over finite fields and Hasse's theorem

Let E be an elliptic curve over a finite field $\mathbb{F}_q$.

Theorem (Hasse)

We have $\#E(\mathbb{F}_q) = q + 1 - a_q$ *where* $|a_q| \leq 2\sqrt{q}$.

For example, if E is in Weierstrass form

$$y^2 = x^3 + Ax + B$$

then Hasse's theorem is consistent with the natural guess from probability theory. (If the residue symbol of $x^3 + Ax + B$ were an independent random variable for each $x \in \mathbb{F}_q$, one would expect $q + 1 - \#E(\mathbb{F}_q)$ to be bounded by a fixed multiple of $\sqrt{q}$ with high probability.)

Elliptic curves over finite fields and Hasse's theorem

Let E be an elliptic curve over a finite field $\mathbb{F}_q$.

Theorem (Hasse)

We have $\#E(\mathbb{F}_q) = q + 1 - a_q$ where $|a_q| \leq 2\sqrt{q}$.

For example, if E is in Weierstrass form

$$y^2 = x^3 + Ax + B$$

then Hasse's theorem is consistent with the natural guess from probability theory. (If the residue symbol of $x^3 + Ax + B$ were an independent random variable for each $x \in \mathbb{F}_q$, one would expect $q + 1 - \#E(\mathbb{F}_q)$ to be bounded by a fixed multiple of $\sqrt{q}$ with high probability.)

Statistics for fixed q

For fixed q, let us view a_q as a random variable on the (finite) probability space of (isomorphism classes of) elliptic curves over $\mathbb{F}_q$, and ask questions about its distribution.

It is useful to study the probability distribution via the *moments*

$$M_d(a_q) := \mathbb{E}(a_q^d) \qquad (d = 1, 2, \ldots; \mathbb{E} = \text{expected value}).$$

Theorem (Birch)

For $q = p \geq 5$, there is a formula

$$M_{2d}(a_p) = \frac{(2d)!}{d!(d+1)!} p^d + O(p^{d-1}),$$

where the error term can be written explicitly in terms of coefficients of modular forms. (Note that the coefficient of p^d is a Catalan number!)

Statistics for fixed q

For fixed q, let us view a_q as a random variable on the (finite) probability space of (isomorphism classes of) elliptic curves over $\mathbb{F}_q$, and ask questions about its distribution.

It is useful to study the probability distribution via the *moments*

$$M_d(a_q) := \mathbb{E}(a_q^d) \qquad (d = 1, 2, \dots; \mathbb{E} = \text{expected value}).$$

Theorem (Birch)

For $q = p \geq 5$, there is a formula

$$M_{2d}(a_p) = \frac{(2d)!}{d!(d+1)!} p^d + O(p^{d-1}),$$

where the error term can be written explicitly in terms of coefficients of modular forms. (Note that the coefficient of p^d is a Catalan number!)

Statistics for a fixed curve

Let's now take E to be an elliptic curve over a number field K. For each prime ideal $\mathfrak{q}$ (with finitely many exceptions), we can reduce E modulo $\mathfrak{q}$ to get an elliptic curve over the residue field $\mathbb{F}_q$ of $\mathfrak{q}$. (Here q equals the absolute norm of $\mathfrak{q}$.)

Write $\#E(\mathbb{F}_q) = q + 1 - a_\mathfrak{q}$ and $\overline{a}_\mathfrak{q} := a_\mathfrak{q}/\sqrt{q}$. We can now ask how the $\overline{a}_\mathfrak{q}$ are distributed across $[-2, 2]$; more precisely, for each $N > 0$ we can ask this for primes $\mathfrak{q}$ with $q \leq N$, and then try to observe a limiting distribution as $N \to \infty$.

Before formalizing this mathematically, let's try a visualization courtesy of:

`http://math.mit.edu/~drew/g1SatoTateDistributions.html`

Statistics for a fixed curve

Let's now take E to be an elliptic curve over a number field K. For each prime ideal $\mathfrak{q}$ (with finitely many exceptions), we can reduce E modulo $\mathfrak{q}$ to get an elliptic curve over the residue field $\mathbb{F}_q$ of $\mathfrak{q}$. (Here q equals the absolute norm of $\mathfrak{q}$.)

Write $\#E(\mathbb{F}_q) = q + 1 - a_\mathfrak{q}$ and $\overline{a}_\mathfrak{q} := a_\mathfrak{q}/\sqrt{q}$. We can now ask how the $\overline{a}_\mathfrak{q}$ are distributed across $[-2, 2]$; more precisely, for each $N > 0$ we can ask this for primes $\mathfrak{q}$ with $q \leq N$, and then try to observe a limiting distribution as $N \to \infty$.

Before formalizing this mathematically, let's try a visualization courtesy of:

`http://math.mit.edu/~drew/g1SatoTateDistributions.html`

Statistics for a fixed curve

Let's now take E to be an elliptic curve over a number field K. For each prime ideal $\mathfrak{q}$ (with finitely many exceptions), we can reduce E modulo $\mathfrak{q}$ to get an elliptic curve over the residue field $\mathbb{F}_q$ of $\mathfrak{q}$. (Here q equals the absolute norm of $\mathfrak{q}$.)

Write $\#E(\mathbb{F}_q) = q + 1 - a_\mathfrak{q}$ and $\overline{a}_\mathfrak{q} := a_\mathfrak{q}/\sqrt{q}$. We can now ask how the $\overline{a}_\mathfrak{q}$ are distributed across $[-2, 2]$; more precisely, for each $N > 0$ we can ask this for primes $\mathfrak{q}$ with $q \leq N$, and then try to observe a limiting distribution as $N \to \infty$.

Before formalizing this mathematically, let's try a visualization courtesy of:

`http://math.mit.edu/~drew/g1SatoTateDistributions.html`

Equidistribution in a probability space

Let $x_1, x_2, \dots$ be a sequence of points in a topological space X. The *equidistribution measure* on X is (if it exists) the unique measure μ on X such that for any continuous function $f : X \to \mathbb{R}$,

$$\int_\mu f = \lim_{n\to\infty} \frac{f(x_1) + \cdots + f(x_n)}{n}.$$

We also say that the sequence is *equidistributed* for μ.

Example (Weyl)

For $\alpha \in \mathbb{R} - \mathbb{Q}$, then the fractional parts $\{n\alpha\} = n\alpha - \lfloor n\alpha \rfloor$ are equidistributed in $[0, 1)$ for Lebesgue measure.

For $M_{d,n}(f)$ the d-th moment of f on $\{x_1, \dots, x_n\}$, the *limit moment* is

$$M_d(f) := \lim_{n\to\infty} M_{d,n}(f) = \int_\mu f^d.$$

Equidistribution in a probability space

Let $x_1, x_2, \ldots$ be a sequence of points in a topological space X. The *equidistribution measure* on X is (if it exists) the unique measure μ on X such that for any continuous function $f : X \to \mathbb{R}$,

$$\int_\mu f = \lim_{n \to \infty} \frac{f(x_1) + \cdots + f(x_n)}{n}.$$

We also say that the sequence is *equidistributed* for μ.

Example (Weyl)

For $\alpha \in \mathbb{R} - \mathbb{Q}$, then the fractional parts $\{n\alpha\} = n\alpha - \lfloor n\alpha \rfloor$ are equidistributed in $[0, 1)$ for Lebesgue measure.

For $M_{d,n}(f)$ the d-th moment of f on $\{x_1, \ldots, x_n\}$, the *limit moment* is

$$M_d(f) := \lim_{n \to \infty} M_{d,n}(f) = \int_\mu f^d.$$

Equidistribution in a probability space

Let $x_1, x_2, \ldots$ be a sequence of points in a topological space X. The *equidistribution measure* on X is (if it exists) the unique measure μ on X such that for any continuous function $f : X \to \mathbb{R}$,

$$\int_\mu f = \lim_{n\to\infty} \frac{f(x_1) + \cdots + f(x_n)}{n}.$$

We also say that the sequence is *equidistributed* for μ.

Example (Weyl)

For $\alpha \in \mathbb{R} - \mathbb{Q}$, then the fractional parts $\{n\alpha\} = n\alpha - \lfloor n\alpha \rfloor$ are equidistributed in $[0,1)$ for Lebesgue measure.

For $M_{d,n}(f)$ the d-th moment of f on $\{x_1, \ldots, x_n\}$, the *limit moment* is

$$M_d(f) := \lim_{n\to\infty} M_{d,n}(f) = \int_\mu f^d.$$

Equidistribution for $\overline{a}_{\mathfrak{q}}$: the Sato-Tate conjecture

The equidistribution of the $\overline{a}_{\mathfrak{q}}$ depends on the arithmetic of the elliptic curve E. But only a little!

Conjecture (Sato-Tate)

The $\overline{a}_{\mathfrak{q}}$ are equidistributed with respect to one of exactly three measures, according as to whether:

- *E has complex multiplication by an imaginary quadratic field in K;*
- *E has complex multiplication by an imaginary quadratic field not in K;*
- *E does not have complex multiplication.*

Theorem (see notes for attributions)

The conjecture is true in the CM cases for any K, and in the non-CM case for K totally real.

Equidistribution for $\overline{a}_{\mathfrak{q}}$: the Sato-Tate conjecture

The equidistribution of the $\overline{a}_{\mathfrak{q}}$ depends on the arithmetic of the elliptic curve E. But only a little!

Conjecture (Sato-Tate)

The $\overline{a}_{\mathfrak{q}}$ are equidistributed with respect to one of exactly three measures, according as to whether:

- *E has complex multiplication by an imaginary quadratic field in K;*
- *E has complex multiplication by an imaginary quadratic field not in K;*
- *E does not have complex multiplication.*

Theorem (see notes for attributions)

The conjecture is true in the CM cases for any K, and in the non-CM case for K totally real.

Equidistribution for $\overline{a}_{\mathfrak{q}}$: the Sato-Tate conjecture

The equidistribution of the $\overline{a}_{\mathfrak{q}}$ depends on the arithmetic of the elliptic curve E. But only a little!

Conjecture (Sato-Tate)

The $\overline{a}_{\mathfrak{q}}$ are equidistributed with respect to one of exactly three measures, according as to whether:

- *E has complex multiplication by an imaginary quadratic field in K;*
- *E has complex multiplication by an imaginary quadratic field not in K;*
- *E does not have complex multiplication.*

Theorem (see notes for attributions)

The conjecture is true in the CM cases for any K, and in the non-CM case for K totally real.

Analogy: the Chebotarev density theorem

Let $f \in K[T]$ be irreducible of degree n. For each $\mathfrak{q}$ (with finitely many exceptions), factor the image of f in $\mathbb{F}_q[T]$; call the degrees of the irreducible factors $d_1, ..., d_k$.

Let L be the splitting field of f and put $G := \mathrm{Gal}(L/K) \subseteq S_n$. By class field theory, we get a Frobenius conjugacy class $g_\mathfrak{q} \in \mathrm{Conj}(G)$; its cycle structure in S_n is $d_1, \ldots, d_k$.

Theorem (Chebotarev)

The sequence $g_\mathfrak{q}$ is equidistributed for the measure on $\mathrm{Conj}(G)$ which weights each class proportional to its cardinality.

Corollary

As $N \to \infty$, the proportion of $\mathfrak{q}$ with $q \leq N$ for which f factors in $\mathbb{F}_q[T]$ with degree sequence $d_1, \ldots, d_k$ tends to the probability that a random element of G has cycle structure $d_1, \ldots, d_k$ in S_n.

Analogy: the Chebotarev density theorem

Let $f \in K[T]$ be irreducible of degree n. For each $\mathfrak{q}$ (with finitely many exceptions), factor the image of f in $\mathbb{F}_q[T]$; call the degrees of the irreducible factors $d_1, \dots, d_k$.

Let L be the splitting field of f and put $G := \mathrm{Gal}(L/K) \subseteq S_n$. By class field theory, we get a Frobenius conjugacy class $g_{\mathfrak{q}} \in \mathrm{Conj}(G)$; its cycle structure in S_n is $d_1, \dots, d_k$.

Theorem (Chebotarev)

The sequence $g_{\mathfrak{q}}$ is equidistributed for the measure on $\mathrm{Conj}(G)$ which weights each class proportional to its cardinality.

Corollary

As $N \to \infty$, the proportion of $\mathfrak{q}$ with $q \leq N$ for which f factors in $\mathbb{F}_q[T]$ with degree sequence $d_1, \dots, d_k$ tends to the probability that a random element of G has cycle structure $d_1, \dots, d_k$ in S_n.

Analogy: the Chebotarev density theorem

Let $f \in K[T]$ be irreducible of degree n. For each $\mathfrak{q}$ (with finitely many exceptions), factor the image of f in $\mathbb{F}_q[T]$; call the degrees of the irreducible factors $d_1, ..., d_k$.

Let L be the splitting field of f and put $G := \mathrm{Gal}(L/K) \subseteq S_n$. By class field theory, we get a Frobenius conjugacy class $g_{\mathfrak{q}} \in \mathrm{Conj}(G)$; its cycle structure in S_n is $d_1, \dots, d_k$.

Theorem (Chebotarev)

The sequence $g_{\mathfrak{q}}$ is equidistributed for the measure on $\mathrm{Conj}(G)$ which weights each class proportional to its cardinality.

Corollary

As $N \to \infty$, the proportion of $\mathfrak{q}$ with $q \leq N$ for which f factors in $\mathbb{F}_q[T]$ with degree sequence $d_1, \dots, d_k$ tends to the probability that a random element of G has cycle structure $d_1, \dots, d_k$ in S_n.

Analogy: the Chebotarev density theorem

Let $f \in K[T]$ be irreducible of degree n. For each $\mathfrak{q}$ (with finitely many exceptions), factor the image of f in $\mathbb{F}_q[T]$; call the degrees of the irreducible factors $d_1, ..., d_k$.

Let L be the splitting field of f and put $G := \mathrm{Gal}(L/K) \subseteq S_n$. By class field theory, we get a Frobenius conjugacy class $g_\mathfrak{q} \in \mathrm{Conj}(G)$; its cycle structure in S_n is $d_1, \dots, d_k$.

Theorem (Chebotarev)

The sequence $g_\mathfrak{q}$ is equidistributed for the measure on $\mathrm{Conj}(G)$ which weights each class proportional to its cardinality.

Corollary

As $N \to \infty$, the proportion of $\mathfrak{q}$ with $q \leq N$ for which f factors in $\mathbb{F}_q[T]$ with degree sequence $d_1, \dots, d_k$ tends to the probability that a random element of G has cycle structure $d_1, \dots, d_k$ in S_n.

Equidistribution in groups and the Sato-Tate conjecture

Suppose E does not have CM. The fact that $|\overline{a}_{\mathfrak{q}}| \leq 2$ means that

$$T^2 - \overline{a}_{\mathfrak{q}} T + 1$$

has roots on the unit circle which are complex conjugates. Such polynomials are exactly the characteristic polynomials of matrices in

$$\mathrm{SU}(2) = \{A \in \mathrm{GL}_2(\mathbb{C}) : A^{-1} = A^*, \det(A) = 1\}.$$

Moreover, the trace defines a bijection $\mathrm{Conj}(\mathrm{SU}(2)) \to [-2, 2]$.

The equidistribution measure predicted by Sato-Tate, viewed on $\mathrm{Conj}(\mathrm{SU}(2))$, is exactly the image of Haar measure on $\mathrm{SU}(2)$! That is, the integral of any f against this measure can be computed by pulling back to $\mathrm{SU}(2)$ and integrating against the translation-invariant measure.

By the way, the even moments of this measure are Catalan numbers! So Birch's distributions converge to this one as $p \to \infty$.

Equidistribution in groups and the Sato-Tate conjecture

Suppose E does not have CM. The fact that $|\overline{a}_{\mathfrak{q}}| \leq 2$ means that

$$T^2 - \overline{a}_{\mathfrak{q}} T + 1$$

has roots on the unit circle which are complex conjugates. Such polynomials are exactly the characteristic polynomials of matrices in

$$\mathrm{SU}(2) = \{A \in \mathrm{GL}_2(\mathbb{C}) : A^{-1} = A^*, \det(A) = 1\}.$$

Moreover, the trace defines a bijection $\mathrm{Conj}(\mathrm{SU}(2)) \to [-2, 2]$.

The equidistribution measure predicted by Sato-Tate, viewed on $\mathrm{Conj}(\mathrm{SU}(2))$, is exactly the image of Haar measure on $\mathrm{SU}(2)$! That is, the integral of any f against this measure can be computed by pulling back to $\mathrm{SU}(2)$ and integrating against the translation-invariant measure.

By the way, the even moments of this measure are Catalan numbers! So Birch's distributions converge to this one as $p \to \infty$.

Equidistribution in groups and the Sato-Tate conjecture

Suppose E does not have CM. The fact that $|\overline{a}_{\mathfrak{q}}| \leq 2$ means that

$$T^2 - \overline{a}_{\mathfrak{q}} T + 1$$

has roots on the unit circle which are complex conjugates. Such polynomials are exactly the characteristic polynomials of matrices in

$$\mathrm{SU}(2) = \{A \in \mathrm{GL}_2(\mathbb{C}) : A^{-1} = A^*, \det(A) = 1\}.$$

Moreover, the trace defines a bijection $\mathrm{Conj}(\mathrm{SU}(2)) \to [-2, 2]$.

The equidistribution measure predicted by Sato-Tate, viewed on $\mathrm{Conj}(\mathrm{SU}(2))$, is exactly the image of Haar measure on $\mathrm{SU}(2)$! That is, the integral of any f against this measure can be computed by pulling back to $\mathrm{SU}(2)$ and integrating against the translation-invariant measure.

By the way, the even moments of this measure are Catalan numbers! So Birch's distributions converge to this one as $p \to \infty$.

Equidistribution in groups and the exceptional cases

In case E has CM, the equidistribution measure is the image of Haar measure not on SU(2), but on a smaller group G:

- if the CM field is in K, the group SO(2);
- otherwise, the normalizer of SO(2) in SU(2). This group has two connected components; on the nonidentity component, the trace is identically zero. This creates a zero-width spike in the distribution of area $1/2$, corresponding to half of the primes being supersingular.

But one can do better: one can lift the classes in Conj(SU(2)) from the previous slide to classes in G, and prove equidistribution there. This allows for a uniform statement of the conjecture, in which equidistribution always happens in some group G determined by the arithmetic of E.

This framework generalizes to abelian varieties of arbitrary dimension! This will be discussed in the second lecture.

Equidistribution in groups and the exceptional cases

In case E has CM, the equidistribution measure is the image of Haar measure not on SU(2), but on a smaller group G:

- if the CM field is in K, the group SO(2);
- otherwise, the normalizer of SO(2) in SU(2). This group has two connected components; on the nonidentity component, the trace is identically zero. This creates a zero-width spike in the distribution of area $1/2$, corresponding to half of the primes being supersingular.

But one can do better: one can lift the classes in Conj(SU(2)) from the previous slide to classes in G, and prove equidistribution there. This allows for a uniform statement of the conjecture, in which equidistribution always happens in some group G determined by the arithmetic of E.

This framework generalizes to abelian varieties of arbitrary dimension! This will be discussed in the second lecture.

Equidistribution in groups and the exceptional cases

In case E has CM, the equidistribution measure is the image of Haar measure not on SU(2), but on a smaller group G:

- if the CM field is in K, the group SO(2);
- otherwise, the normalizer of SO(2) in SU(2). This group has two connected components; on the nonidentity component, the trace is identically zero. This creates a zero-width spike in the distribution of area $1/2$, corresponding to half of the primes being supersingular.

But one can do better: one can lift the classes in Conj(SU(2)) from the previous slide to classes in G, and prove equidistribution there. This allows for a uniform statement of the conjecture, in which equidistribution always happens in some group G determined by the arithmetic of E.

This framework generalizes to abelian varieties of arbitrary dimension! This will be discussed in the second lecture.

Equidistribution in groups and the exceptional cases

In case E has CM, the equidistribution measure is the image of Haar measure not on SU(2), but on a smaller group G:

- if the CM field is in K, the group SO(2);
- otherwise, the normalizer of SO(2) in SU(2). This group has two connected components; on the nonidentity component, the trace is identically zero. This creates a zero-width spike in the distribution of area $1/2$, corresponding to half of the primes being supersingular.

But one can do better: one can lift the classes in Conj(SU(2)) from the previous slide to classes in G, and prove equidistribution there. This allows for a uniform statement of the conjecture, in which equidistribution always happens in some group G determined by the arithmetic of E.

This framework generalizes to abelian varieties of arbitrary dimension! This will be discussed in the second lecture.

Equidistribution in groups and the exceptional cases

In case E has CM, the equidistribution measure is the image of Haar measure not on SU(2), but on a smaller group G:

- if the CM field is in K, the group SO(2);
- otherwise, the normalizer of SO(2) in SU(2). This group has two connected components; on the nonidentity component, the trace is identically zero. This creates a zero-width spike in the distribution of area $1/2$, corresponding to half of the primes being supersingular.

But one can do better: one can lift the classes in Conj(SU(2)) from the previous slide to classes in G, and prove equidistribution there. This allows for a uniform statement of the conjecture, in which equidistribution always happens in some group G determined by the arithmetic of E.

This framework generalizes to abelian varieties of arbitrary dimension! This will be discussed in the second lecture.

Contents

The zeta function of an algebraic variety over a finite field

Let X be an algebraic variety over a finite field $\mathbb{F}_q$. Weil introduced the *zeta function*

$$\zeta(X,s) = \prod_{x \in X^\circ} (1 - q^{-s\deg(x)})^{-1} \qquad (\mathrm{Re}(s) \gg 0)$$

where X° is the set of closed points of X. Equivalently, x runs over Galois orbits of $\overline{\mathbb{F}_q}$-points and $\deg(x)$ is the size of the orbit.

As a formal power series in q^{-s}, we also have

$$\zeta(X,s) = \exp\left(\sum_{n=1}^{\infty} \frac{q^{-ns}}{n} \#X(\mathbb{F}_{q^n})\right).$$

Theorem (Dwork, Grothendieck)

The function $\zeta(X,s)$ is a rational function in q^{-s}.

The zeta function of an algebraic variety over a finite field

Let X be an algebraic variety over a finite field $\mathbb{F}_q$. Weil introduced the *zeta function*

$$\zeta(X,s) = \prod_{x \in X^\circ} (1 - q^{-s\deg(x)})^{-1} \qquad (\mathrm{Re}(s) \gg 0)$$

where X° is the set of closed points of X. Equivalently, x runs over Galois orbits of $\overline{\mathbb{F}_q}$-points and $\deg(x)$ is the size of the orbit.

As a formal power series in q^{-s}, we also have

$$\zeta(X,s) = \exp\left(\sum_{n=1}^{\infty} \frac{q^{-ns}}{n} \# X(\mathbb{F}_{q^n})\right).$$

Theorem (Dwork, Grothendieck)

The function $\zeta(X,s)$ is a rational function in q^{-s}.

The zeta function of an algebraic variety over a finite field

Let X be an algebraic variety over a finite field $\mathbb{F}_q$. Weil introduced the *zeta function*

$$\zeta(X, s) = \prod_{x \in X^\circ} (1 - q^{-s\deg(x)})^{-1} \qquad (\mathrm{Re}(s) \gg 0)$$

where X° is the set of closed points of X. Equivalently, x runs over Galois orbits of $\overline{\mathbb{F}_q}$-points and $\deg(x)$ is the size of the orbit.

As a formal power series in q^{-s}, we also have

$$\zeta(X, s) = \exp\left(\sum_{n=1}^{\infty} \frac{q^{-ns}}{n} \# X(\mathbb{F}_{q^n})\right).$$

Theorem (Dwork, Grothendieck)

The function $\zeta(X, s)$ is a rational function in q^{-s}.

The zeta function of a curve over a finite field

Theorem (Weil)

Let C be a (smooth, projective, geometrically irreducible) curve of genus g over $\mathbb{F}_q$. Then

$$\zeta(C, s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

where $P(T) \in \mathbb{Z}[T]$ and $\overline{P}(T) := P(T/\sqrt{q})$ factors over $\mathbb{C}$ as $(1-\alpha_1 T)\cdots(1-\alpha_{2g}T)$ with $|\alpha_i| = 1$ and $\alpha_{g+i} = \overline{\alpha_i}$.

Note also that

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - q^{n/2}(\alpha_1^n + \cdots + \alpha_{2g}^n) \qquad (n = 1, 2, \dots).$$

For $g = 1$, C is an elliptic curve and $\overline{P}(T) = 1 - \overline{a}_q T + T^2$.

The zeta function of a curve over a finite field

Theorem (Weil)

Let C be a (smooth, projective, geometrically irreducible) curve of genus g over $\mathbb{F}_q$. Then

$$\zeta(C, s) = \frac{P(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

where $P(T) \in \mathbb{Z}[T]$ and $\overline{P}(T) := P(T/\sqrt{q})$ factors over $\mathbb{C}$ as $(1 - \alpha_1 T) \cdots (1 - \alpha_{2g} T)$ with $|\alpha_i| = 1$ and $\alpha_{g+i} = \overline{\alpha_i}$.

Note also that

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - q^{n/2}(\alpha_1^n + \cdots + \alpha_{2g}^n) \qquad (n = 1, 2, \dots).$$

For $g = 1$, C is an elliptic curve and $\overline{P}(T) = 1 - \overline{a}_q T + T^2$.

The zeta function of a curve over a finite field

Theorem (Weil)

Let C be a (smooth, projective, geometrically irreducible) curve of genus g over $\mathbb{F}_q$. Then

$$\zeta(C, s) = \frac{P(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

where $P(T) \in \mathbb{Z}[T]$ and $\overline{P}(T) := P(T/\sqrt{q})$ factors over $\mathbb{C}$ as $(1 - \alpha_1 T) \cdots (1 - \alpha_{2g} T)$ with $|\alpha_i| = 1$ and $\alpha_{g+i} = \overline{\alpha_i}$.

Note also that

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - q^{n/2}(\alpha_1^n + \cdots + \alpha_{2g}^n) \qquad (n = 1, 2, \ldots).$$

For $g = 1$, C is an elliptic curve and $\overline{P}(T) = 1 - \overline{a}_q T + T^2$.

The zeta function of an abelian variety over a finite field

Theorem (Weil)

Let A be an abelian variety of genus g over $\mathbb{F}_q$. Then

$$\zeta(A,s) = \frac{P_1(q^{-s})\cdots P_{2g-1}(q^{-s})}{P_0(q^{-s})\cdots P_{2g}(q^{-s})}$$

where

$$P_k(T) = \prod_{1 \leq i_1 < \cdots < i_k \leq 2g} (1 - q^{k/2}\alpha_{i_1}\cdots\alpha_{i_k} T) \in \mathbb{Z}[T]$$

for some $\alpha_1, \dots, \alpha_{2g} \in \mathbb{C}$ with $|\alpha_i| = 1$ and $\alpha_{g+i} = \overline{\alpha_i}$. Moreover, if A is the Jacobian of a curve C, then $P_1(T) = P(T)$.

Note also that

$$\#A(\mathbb{F}_{q^n}) = (1 - q^{n/2}\alpha_1^n)\cdots(1 - q^{n/2}\alpha_{2g}^n) \qquad (n = 1, 2, \dots).$$

The zeta function of an abelian variety over a finite field

Theorem (Weil)

Let A be an abelian variety of genus g over $\mathbb{F}_q$. Then

$$\zeta(A, s) = \frac{P_1(q^{-s}) \cdots P_{2g-1}(q^{-s})}{P_0(q^{-s}) \cdots P_{2g}(q^{-s})}$$

where

$$P_k(T) = \prod_{1 \leq i_1 < \cdots < i_k \leq 2g} (1 - q^{k/2} \alpha_{i_1} \cdots \alpha_{i_k} T) \in \mathbb{Z}[T]$$

for some $\alpha_1, \dots, \alpha_{2g} \in \mathbb{C}$ with $|\alpha_i| = 1$ and $\alpha_{g+i} = \overline{\alpha_i}$. Moreover, if A is the Jacobian of a curve C, then $P_1(T) = P(T)$.

Note also that

$$\#A(\mathbb{F}_{q^n}) = (1 - q^{n/2}\alpha_1^n) \cdots (1 - q^{n/2}\alpha_{2g}^n) \qquad (n = 1, 2, \dots).$$

An equidistribution problem for abelian varieties

Let A be an abelian variety of dimension g over a number field K. For $\mathfrak{q}$ a prime ideal of K (at which A has good reduction), we may reduce modulo $\mathfrak{q}$ to obtain an abelian variety over $\mathbb{F}_q$. Write its zeta function as

$$\frac{P_1(q^{-s}) \cdots P_{2g-1}(q^{-s})}{P_0(q^{-s}) \cdots P_{2g}(q^{-s})}.$$

Put $\overline{P}_{\mathfrak{q}}(T) := P_1(T/\sqrt{q})$; this polynomial has the form

$$1 + \overline{a}_{\mathfrak{q},1} T + \cdots + \overline{a}_{\mathfrak{q},2g-1} T^{2g-1} + T^{2g} = \prod_{i=1}^{2g} (1 - \alpha_{\mathfrak{q},i} T),$$

where

$$\overline{a}_{\mathfrak{q},i} \in \mathbb{R}, \qquad \overline{a}_{\mathfrak{q},2g-i} = \overline{a}_{\mathfrak{q},i}, \qquad |\alpha_{\mathfrak{q},i}| = 1.$$

An equidistribution problem for abelian varieties

Let A be an abelian variety of dimension g over a number field K. For $\mathfrak{q}$ a prime ideal of K (at which A has good reduction), we may reduce modulo $\mathfrak{q}$ to obtain an abelian variety over $\mathbb{F}_q$. Write its zeta function as

$$\frac{P_1(q^{-s}) \cdots P_{2g-1}(q^{-s})}{P_0(q^{-s}) \cdots P_{2g}(q^{-s})}.$$

Put $\overline{P}_{\mathfrak{q}}(T) := P_1(T/\sqrt{q})$; this polynomial has the form

$$1 + \overline{a}_{\mathfrak{q},1} T + \cdots + \overline{a}_{\mathfrak{q},2g-1} T^{2g-1} + T^{2g} = \prod_{i=1}^{2g} (1 - \alpha_{\mathfrak{q},i} T),$$

where

$$\overline{a}_{\mathfrak{q},i} \in \mathbb{R}, \qquad \overline{a}_{\mathfrak{q},2g-i} = \overline{a}_{\mathfrak{q},i}, \qquad |\alpha_{\mathfrak{q},i}| = 1.$$

Moments for abelian varieties

We will study the distribution of the polynomial

$$\overline{P}_{\mathfrak{q}}(T) = 1 + \overline{a}_{\mathfrak{q},1} T + \cdots + \overline{a}_{\mathfrak{q},2g-1} T^{2g-1} + T^{2g}$$

as $\mathfrak{q}$ varies. For A the Jacobian of a curve C, we have

$$\# C(\mathbb{F}_q) = q + 1 - q^{1/2} \overline{a}_{\mathfrak{q},1}$$

but the joint distribution of $\overline{a}_{\mathfrak{q},1}, \dots, \overline{a}_{\mathfrak{q},g}$ carries more information.

In principle, one must consider all of the *joint moments*

$$\# \mathbb{E}(\overline{a}_{\mathfrak{q},1}^{d_1} \dots \overline{a}_{\mathfrak{q},g}^{d_g}) : d_1, \dots, d_g = 0, 1, \dots.$$

For the group-theoretic distributions we consider, these will all be integers.

In practice, it is (mostly) sufficient to look at the individual moments of the $\overline{a}_{\mathfrak{q},i}$, together with the discrete components of the distributions. These only occur at 0 for i odd, but can occur at other integers for i even.

Moments for abelian varieties

We will study the distribution of the polynomial

$$\overline{P}_{\mathfrak{q}}(T) = 1 + \overline{a}_{\mathfrak{q},1} T + \cdots + \overline{a}_{\mathfrak{q},2g-1} T^{2g-1} + T^{2g}$$

as $\mathfrak{q}$ varies. For A the Jacobian of a curve C, we have

$$\# C(\mathbb{F}_q) = q + 1 - q^{1/2} \overline{a}_{\mathfrak{q},1}$$

but the joint distribution of $\overline{a}_{\mathfrak{q},1}, \dots, \overline{a}_{\mathfrak{q},g}$ carries more information.

In principle, one must consider all of the *joint moments*

$$\# \mathbb{E}(\overline{a}_{\mathfrak{q},1}^{d_1} \dots \overline{a}_{\mathfrak{q},g}^{d_g}) : d_1, \dots, d_g = 0, 1, \dots.$$

For the group-theoretic distributions we consider, these will all be integers.

In practice, it is (mostly) sufficient to look at the individual moments of the $\overline{a}_{\mathfrak{q},i}$, together with the discrete components of the distributions. These only occur at 0 for i odd, but can occur at other integers for i even.

Moments for abelian varieties

We will study the distribution of the polynomial

$$\overline{P}_{\mathfrak{q}}(T) = 1 + \overline{a}_{\mathfrak{q},1} T + \cdots + \overline{a}_{\mathfrak{q},2g-1} T^{2g-1} + T^{2g}$$

as $\mathfrak{q}$ varies. For A the Jacobian of a curve C, we have

$$\#C(\mathbb{F}_q) = q + 1 - q^{1/2}\overline{a}_{\mathfrak{q},1}$$

but the joint distribution of $\overline{a}_{\mathfrak{q},1}, \dots, \overline{a}_{\mathfrak{q},g}$ carries more information.

In principle, one must consider all of the *joint moments*

$$\#\mathbb{E}(\overline{a}_{\mathfrak{q},1}^{d_1} \dots \overline{a}_{\mathfrak{q},g}^{d_g}) : d_1, \dots, d_g = 0, 1, \dots.$$

For the group-theoretic distributions we consider, these will all be integers.

In practice, it is (mostly) sufficient to look at the individual moments of the $\overline{a}_{\mathfrak{q},i}$, together with the discrete components of the distributions. These only occur at 0 for i odd, but can occur at other integers for i even.

An equidistribution conjecture in the generic case

Consider the *unitary symplectic group*

$$\mathrm{USp}(2g) := \{A \in \mathrm{GL}_{2g}(\mathbb{C}) : A^{-1} = A^*, A^T J A = J\}$$

where J is the matrix defining a standard symplectic form

$$J := \begin{pmatrix} J_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & J_1 \end{pmatrix}, \qquad J_1 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Conjecture (Serre, Katz-Sarnak)

For A having "no extra structure", the $\overline{P}_{\mathfrak{q}}(T)$ are equidistributed for the image of the Haar measure on $\mathrm{USp}(2g)$ via the characteristic polynomial map. (This is consistent with Sato-Tate because $\mathrm{USp}(2) = \mathrm{SU}(2)$.)

An equidistribution conjecture in the generic case

Consider the *unitary symplectic group*

$$\mathrm{USp}(2g) := \{A \in \mathrm{GL}_{2g}(\mathbb{C}) : A^{-1} = A^*, A^T J A = J\}$$

where J is the matrix defining a standard symplectic form

$$J := \begin{pmatrix} J_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & J_1 \end{pmatrix}, \qquad J_1 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Conjecture (Serre, Katz-Sarnak)

For A having "no extra structure", the $\overline{P}_{\mathfrak{q}}(T)$ are equidistributed for the image of the Haar measure on $\mathrm{USp}(2g)$ *via the characteristic polynomial map. (This is consistent with Sato-Tate because* $\mathrm{USp}(2) = \mathrm{SU}(2)$*.)*

What is extra structure?

For $g = 1$, "no extra structure" means no complex multiplication.

For $g = 2, 3$, "no extra structure" similarly means that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. In particular, this will be the case throughout the third lecture.

For $g \geq 4$, "no extra structure" needs a subtler definition: there must be no "unexpected algebraic cycles" on any of the self-products $A_{\overline{K}} \times \cdots \times A_{\overline{K}}$. Just like endomorphisms, such cycles impose restrictions on the action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on torsion points, and hence on the zeta functions.

What is extra structure?

For $g = 1$, "no extra structure" means no complex multiplication.

For $g = 2, 3$, "no extra structure" similarly means that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. In particular, this will be the case throughout the third lecture.

For $g \geq 4$, "no extra structure" needs a subtler definition: there must be no "unexpected algebraic cycles" on any of the self-products $A_{\overline{K}} \times \cdots \times A_{\overline{K}}$. Just like endomorphisms, such cycles impose restrictions on the action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on torsion points, and hence on the zeta functions.

What is extra structure?

For $g = 1$, "no extra structure" means no complex multiplication.

For $g = 2, 3$, "no extra structure" similarly means that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. In particular, this will be the case throughout the third lecture.

For $g \geq 4$, "no extra structure" needs a subtler definition: there must be no "unexpected algebraic cycles" on any of the self-products $A_{\overline{K}} \times \cdots \times A_{\overline{K}}$. Just like endomorphisms, such cycles impose restrictions on the action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on torsion points, and hence on the zeta functions.

A group-theoretic reformulation

The conditions on $\overline{P}_{\mathfrak{q}}(T)$ guarantee not only that it is in the image of the characteristic polynomial map on $\mathrm{USp}(2g)$, but also that its inverse image is a single conjugacy class $g_{\mathfrak{q}}$. The previous conjecture can thus be interpreted as saying that for A having "no extra structure", the $g_{\mathfrak{q}}$ are equidistributed in $\mathrm{Conj}(\mathrm{USp}(2g))$ via the image of Haar measure.

Conjecture (after Serre)

For arbitrary A, there are a particular closed subgroup $\mathrm{ST}(A)$ of $\mathrm{USp}(2g)$ and a particular sequence $g_{\mathfrak{q}}$ in $\mathrm{Conj}(\mathrm{ST}(A))$ whose characteristic polynomials are the $\overline{P}_{\mathfrak{q}}(T)$, for which equidistribution holds for the image of Haar measure on $\mathrm{ST}(A)$.

We call $\mathrm{ST}(A)$ the *Sato-Tate group* of A.

A group-theoretic reformulation

The conditions on $\overline{P}_{\mathfrak{q}}(T)$ guarantee not only that it is in the image of the characteristic polynomial map on $\mathrm{USp}(2g)$, but also that its inverse image is a single conjugacy class $g_{\mathfrak{q}}$. The previous conjecture can thus be interpreted as saying that for A having "no extra structure", the $g_{\mathfrak{q}}$ are equidistributed in $\mathrm{Conj}(\mathrm{USp}(2g))$ via the image of Haar measure.

Conjecture (after Serre)

For arbitrary A, there are a particular closed subgroup $\mathrm{ST}(A)$ of $\mathrm{USp}(2g)$ and a particular sequence $g_{\mathfrak{q}}$ in $\mathrm{Conj}(\mathrm{ST}(A))$ whose characteristic polynomials are the $\overline{P}_{\mathfrak{q}}(T)$, for which equidistribution holds for the image of Haar measure on $\mathrm{ST}(A)$.

We call $\mathrm{ST}(A)$ the *Sato-Tate group* of A.

A group-theoretic reformulation

The conditions on $\overline{P}_{\mathfrak{q}}(T)$ guarantee not only that it is in the image of the characteristic polynomial map on $\mathrm{USp}(2g)$, but also that its inverse image is a single conjugacy class $g_{\mathfrak{q}}$. The previous conjecture can thus be interpreted as saying that for A having "no extra structure", the $g_{\mathfrak{q}}$ are equidistributed in $\mathrm{Conj}(\mathrm{USp}(2g))$ via the image of Haar measure.

Conjecture (after Serre)

For arbitrary A, there are a particular closed subgroup $\mathrm{ST}(A)$ of $\mathrm{USp}(2g)$ and a particular sequence $g_{\mathfrak{q}}$ in $\mathrm{Conj}(\mathrm{ST}(A))$ whose characteristic polynomials are the $\overline{P}_{\mathfrak{q}}(T)$, for which equidistribution holds for the image of Haar measure on $\mathrm{ST}(A)$.

We call $\mathrm{ST}(A)$ the *Sato-Tate group* of A.

Sketch of the construction: the group

Choose an embedding $K \hookrightarrow \mathbb{C}$, let $V := H_1(A^{\mathrm{an}}_{\mathbb{C}}, \mathbb{Q})$ be singular homology, and choose a symplectic basis of V for the cup product. Then $\mathrm{USp}(2g)$ acts on $V_{\mathbb{C}}$.

The connected part $\mathrm{ST}(A)^\circ$ of $\mathrm{ST}(A)$ is the subgroup of $\mathrm{USp}(2g)$ which, for each positive integer m, fixes the subspace of $V^{\otimes 2m}$ corresponding to algebraic cycles on $A^{\otimes m}_{\overline{K}}$. For $g \leq 3$, it is enough to impose commutation with the action of endomorphisms of $A_{\overline{K}}$.

The full group $\mathrm{ST}(A)$ consists of elements of $\mathrm{USp}(2g)$ which act on the homology classes of algebraic cycles as some element of G_K. Again, for $g \leq 3$, one has a similar definition using endomorphisms of $A_{\overline{K}}$.

In particular, $\mathrm{ST}(A)^\circ$ is invariant under base change, while $\mathrm{ST}(A)/\mathrm{ST}(A)^\circ$ is a finite group canonically identified with $\mathrm{Gal}(L/K)$ for some finite extension L of K. The field L contains the minimal field of definition of endomorphisms of $A_{\overline{K}}$, and is equal for $g \leq 3$.

Sketch of the construction: the group

Choose an embedding $K \hookrightarrow \mathbb{C}$, let $V := H_1(A_{\mathbb{C}}^{\mathrm{an}}, \mathbb{Q})$ be singular homology, and choose a symplectic basis of V for the cup product. Then $\mathrm{USp}(2g)$ acts on $V_{\mathbb{C}}$.

The connected part $\mathrm{ST}(A)^\circ$ of $\mathrm{ST}(A)$ is the subgroup of $\mathrm{USp}(2g)$ which, for each positive integer m, fixes the subspace of $V^{\otimes 2m}$ corresponding to algebraic cycles on $A_{\overline{K}}^{\otimes m}$. For $g \leq 3$, it is enough to impose commutation with the action of endomorphisms of $A_{\overline{K}}$.

The full group $\mathrm{ST}(A)$ consists of elements of $\mathrm{USp}(2g)$ which act on the homology classes of algebraic cycles as some element of G_K. Again, for $g \leq 3$, one has a similar definition using endomorphisms of $A_{\overline{K}}$.

In particular, $\mathrm{ST}(A)^\circ$ is invariant under base change, while $\mathrm{ST}(A)/\mathrm{ST}(A)^\circ$ is a finite group canonically identified with $\mathrm{Gal}(L/K)$ for some finite extension L of K. The field L contains the minimal field of definition of endomorphisms of $A_{\overline{K}}$, and is equal for $g \leq 3$.

Sketch of the construction: the group

Choose an embedding $K \hookrightarrow \mathbb{C}$, let $V := H_1(A_{\mathbb{C}}^{\mathrm{an}}, \mathbb{Q})$ be singular homology, and choose a symplectic basis of V for the cup product. Then $\mathrm{USp}(2g)$ acts on $V_{\mathbb{C}}$.

The connected part $\mathrm{ST}(A)^\circ$ of $\mathrm{ST}(A)$ is the subgroup of $\mathrm{USp}(2g)$ which, for each positive integer m, fixes the subspace of $V^{\otimes 2m}$ corresponding to algebraic cycles on $A_{\overline{K}}^{\otimes m}$. For $g \leq 3$, it is enough to impose commutation with the action of endomorphisms of $A_{\overline{K}}$.

The full group $\mathrm{ST}(A)$ consists of elements of $\mathrm{USp}(2g)$ which act on the homology classes of algebraic cycles as some element of G_K. Again, for $g \leq 3$, one has a similar definition using endomorphisms of $A_{\overline{K}}$.

In particular, $\mathrm{ST}(A)^\circ$ is invariant under base change, while $\mathrm{ST}(A)/\mathrm{ST}(A)^\circ$ is a finite group canonically identified with $\mathrm{Gal}(L/K)$ for some finite extension L of K. The field L contains the minimal field of definition of endomorphisms of $A_{\overline{K}}$, and is equal for $g \leq 3$.

Sketch of the construction: the group

Choose an embedding $K \hookrightarrow \mathbb{C}$, let $V := H_1(A^{\mathrm{an}}_{\mathbb{C}}, \mathbb{Q})$ be singular homology, and choose a symplectic basis of V for the cup product. Then $\mathrm{USp}(2g)$ acts on $V_{\mathbb{C}}$.

The connected part $\mathrm{ST}(A)^\circ$ of $\mathrm{ST}(A)$ is the subgroup of $\mathrm{USp}(2g)$ which, for each positive integer m, fixes the subspace of $V^{\otimes 2m}$ corresponding to algebraic cycles on $A^{\otimes m}_{\overline{K}}$. For $g \leq 3$, it is enough to impose commutation with the action of endomorphisms of $A_{\overline{K}}$.

The full group $\mathrm{ST}(A)$ consists of elements of $\mathrm{USp}(2g)$ which act on the homology classes of algebraic cycles as some element of G_K. Again, for $g \leq 3$, one has a similar definition using endomorphisms of $A_{\overline{K}}$.

In particular, $\mathrm{ST}(A)^\circ$ is invariant under base change, while $\mathrm{ST}(A)/\mathrm{ST}(A)^\circ$ is a finite group canonically identified with $\mathrm{Gal}(L/K)$ for some finite extension L of K. The field L contains the minimal field of definition of endomorphisms of $A_{\overline{K}}$, and is equal for $g \leq 3$.

Sketch of the construction: the sequence

Fix a prime number ℓ. We then have an action of G_K on the ℓ-adic Tate module

$$T_\ell(A) = \varprojlim_{n \to \infty} A(\overline{K})[\ell^n].$$

Any Frobenius element in G_K associated to $\mathfrak{q}$ acts on $T_\ell(A)$, and again acts on elements of $T_\ell(A)^{\otimes 2m}$ corresponding to algebraic cycles on $A_{\overline{K}}^{\otimes m}$ as some element of G_K (namely itself).

Using some trickery (including an algebraic embedding of $\mathbb{Q}_\ell$ into $\mathbb{C}$), one gets a well-defined conjugacy class in $\mathrm{ST}(A)$.

Good news: the exact nature of this definition is not so crucial! Given another definition with the appropriate properties, one can transfer equidistribution back and forth using Serre's criterion (see next slide).

Sketch of the construction: the sequence

Fix a prime number ℓ. We then have an action of G_K on the ℓ-adic Tate module

$$T_\ell(A) = \varprojlim_{n \to \infty} A(\overline{K})[\ell^n].$$

Any Frobenius element in G_K associated to $\mathfrak{q}$ acts on $T_\ell(A)$, and again acts on elements of $T_\ell(A)^{\otimes 2m}$ corresponding to algebraic cycles on $A_{\overline{K}}^{\otimes m}$ as some element of G_K (namely itself).

Using some trickery (including an algebraic embedding of $\mathbb{Q}_\ell$ into $\mathbb{C}$), one gets a well-defined conjugacy class in $\mathrm{ST}(A)$.

Good news: the exact nature of this definition is not so crucial! Given another definition with the appropriate properties, one can transfer equidistribution back and forth using Serre's criterion (see next slide).

Sketch of the construction: the sequence

Fix a prime number ℓ. We then have an action of G_K on the ℓ-adic Tate module

$$T_\ell(A) = \varprojlim_{n \to \infty} A(\overline{K})[\ell^n].$$

Any Frobenius element in G_K associated to $\mathfrak{q}$ acts on $T_\ell(A)$, and again acts on elements of $T_\ell(A)^{\otimes 2m}$ corresponding to algebraic cycles on $A_{\overline{K}}^{\otimes m}$ as some element of G_K (namely itself).

Using some trickery (including an algebraic embedding of $\mathbb{Q}_\ell$ into $\mathbb{C}$), one gets a well-defined conjugacy class in $\mathrm{ST}(A)$.

Good news: the exact nature of this definition is not so crucial! Given another definition with the appropriate properties, one can transfer equidistribution back and forth using Serre's criterion (see next slide).

Sketch of the construction: the sequence

Fix a prime number ℓ. We then have an action of G_K on the ℓ-adic Tate module

$$T_\ell(A) = \varprojlim_{n \to \infty} A(\overline{K})[\ell^n].$$

Any Frobenius element in G_K associated to $\mathfrak{q}$ acts on $T_\ell(A)$, and again acts on elements of $T_\ell(A)^{\otimes 2m}$ corresponding to algebraic cycles on $A_{\overline{K}}^{\otimes m}$ as some element of G_K (namely itself).

Using some trickery (including an algebraic embedding of $\mathbb{Q}_\ell$ into $\mathbb{C}$), one gets a well-defined conjugacy class in $\mathrm{ST}(A)$.

Good news: the exact nature of this definition is not so crucial! Given another definition with the appropriate properties, one can transfer equidistribution back and forth using Serre's criterion (see next slide).

How to prove equidistribution

For each $\mathbb{C}$-linear representation ρ of $\mathrm{ST}(A)$, define the *L-function*

$$L(\rho, s) = \prod_{\mathfrak{q}} \det(1 - \rho(\tilde{g}_{\mathfrak{q}}) q^{-s})^{-1} \qquad (\Re(s) > 1)$$

where $\tilde{g}_{\mathfrak{q}} \in \mathrm{ST}(A)$ is any element of the class $g_{\mathfrak{q}}$. For ρ the trivial representation, this is (almost) the Dedekind zeta function of K, and so has a simple pole at $s = 1$.

Theorem (Serre, after Hadamard and de la Vallée Poussin)

Suppose that for each nontrivial irreducible ρ, $L(\rho, s)$ extends to a holomorphic nonvanishing function on some neighborhood of $s = 1$. Then the $g_{\mathfrak{q}}$ are equidistributed in $\mathrm{Conj}(\mathrm{ST}(A))$ for the image of Haar measure, and so the generalized Sato-Tate conjecture holds for A.

How to prove equidistribution

For each $\mathbb{C}$-linear representation ρ of $\mathrm{ST}(A)$, define the *L-function*

$$L(\rho, s) = \prod_{\mathfrak{q}} \det(1 - \rho(\tilde{g}_{\mathfrak{q}}) q^{-s})^{-1} \qquad (\Re(s) > 1)$$

where $\tilde{g}_{\mathfrak{q}} \in \mathrm{ST}(A)$ is any element of the class $g_{\mathfrak{q}}$. For ρ the trivial representation, this is (almost) the Dedekind zeta function of K, and so has a simple pole at $s = 1$.

Theorem (Serre, after Hadamard and de la Vallée Poussin)

Suppose that for each nontrivial irreducible ρ, $L(\rho, s)$ extends to a holomorphic nonvanishing function on some neighborhood of $s = 1$. Then the $g_{\mathfrak{q}}$ are equidistributed in $\mathrm{Conj}(\mathrm{ST}(A))$ for the image of Haar measure, and so the generalized Sato-Tate conjecture holds for A.

Contents

Overview

Throughout this lecture, let A be an abelian surface over a number field K, e.g., the Jacobian of a genus 2 curve.

Theorem (Fité–Kedlaya–Rotger–Sutherland)

There are exactly 52 subgroups of $\mathrm{USp}(4)$, up to conjugation, which occur as Sato-Tate groups of abelian surfaces over K; all can be realized using Jacobians of genus 2 curves over K. Of these, exactly 34 occur for $K = \mathbb{Q}$; all can be realized using Jacobians of genus 2 curves over $\mathbb{Q}$.

In this lecture, we will give a partial breakdown of this classification, together with some indications of to what extent the arithmetic of A determines $\mathrm{ST}(A)$ and vice versa. But first, some more visualization:

`http://math.mit.edu/~drew/g2SatoTateDistributions.html`

(Historical note: the numerics came first!)

Overview

Throughout this lecture, let A be an abelian surface over a number field K, e.g., the Jacobian of a genus 2 curve.

Theorem (Fité–Kedlaya–Rotger–Sutherland)

There are exactly 52 *subgroups of* $\mathrm{USp}(4)$, *up to conjugation, which occur as Sato-Tate groups of abelian surfaces over* K*; all can be realized using Jacobians of genus 2 curves over* K*. Of these, exactly* 34 *occur for* $K = \mathbb{Q}$*; all can be realized using Jacobians of genus 2 curves over* $\mathbb{Q}$*.*

In this lecture, we will give a partial breakdown of this classification, together with some indications of to what extent the arithmetic of A determines $\mathrm{ST}(A)$ and vice versa. But first, some more visualization:

`http://math.mit.edu/~drew/g2SatoTateDistributions.html`

(Historical note: the numerics came first!)

Overview

Throughout this lecture, let A be an abelian surface over a number field K, e.g., the Jacobian of a genus 2 curve.

Theorem (Fité–Kedlaya–Rotger–Sutherland)

There are exactly 52 *subgroups of* $\mathrm{USp}(4)$, *up to conjugation, which occur as Sato-Tate groups of abelian surfaces over* K; *all can be realized using Jacobians of genus 2 curves over* K. *Of these, exactly* 34 *occur for* $K = \mathbb{Q}$; *all can be realized using Jacobians of genus 2 curves over* $\mathbb{Q}$.

In this lecture, we will give a partial breakdown of this classification, together with some indications of to what extent the arithmetic of A determines $\mathrm{ST}(A)$ and vice versa. But first, some more visualization:

`http://math.mit.edu/~drew/g2SatoTateDistributions.html`

(Historical note: the numerics came first!)

The classification of connected parts

Theorem

There are exactly 6 subgroups of $\mathrm{USp}(4)$*, up to conjugation, which occur as connected parts of Sato-Tate groups of abelian surfaces over* K*:*

$$\mathrm{SO}(2), \mathrm{SU}(2), \mathrm{SO}(2) \times \mathrm{SO}(2), \mathrm{SO}(2) \times \mathrm{SU}(2), \mathrm{SU}(2) \times \mathrm{SU}(2), \mathrm{USp}(4).$$

Of these, all 6 occur for $K = \mathbb{Q}$.

Let E_1, E_1' be nonisogenous elliptic curves with CM; let E_2, E_2' be nonisogenous elliptic curves over K without CM; let A be an abelian surface such that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. Then the Sato-Tate groups of

$$E_1 \times E_1,\ E_2 \times E_2,\ E_1 \times E_1',\ E_1 \times E_2,\ E_2 \times E_2',\ A$$

have the connected parts listed in the theorem.

However, it is also possible to realize all of the connected parts using absolutely simple abelian surfaces! We will see this later.

The classification of connected parts

Theorem

There are exactly 6 subgroups of $\mathrm{USp}(4)$*, up to conjugation, which occur as connected parts of Sato-Tate groups of abelian surfaces over* K*:*

$$\mathrm{SO}(2), \mathrm{SU}(2), \mathrm{SO}(2) \times \mathrm{SO}(2), \mathrm{SO}(2) \times \mathrm{SU}(2), \mathrm{SU}(2) \times \mathrm{SU}(2), \mathrm{USp}(4).$$

Of these, all 6 occur for $K = \mathbb{Q}$*.*

Let E_1, E_1' be nonisogenous elliptic curves with CM; let E_2, E_2' be nonisogenous elliptic curves over K without CM; let A be an abelian surface such that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. Then the Sato-Tate groups of

$$E_1 \times E_1,\ E_2 \times E_2,\ E_1 \times E_1',\ E_1 \times E_2,\ E_2 \times E_2',\ A$$

have the connected parts listed in the theorem.

However, it is also possible to realize all of the connected parts using absolutely simple abelian surfaces! We will see this later.

The classification of connected parts

Theorem

There are exactly 6 subgroups of USp(4)*, up to conjugation, which occur as connected parts of Sato-Tate groups of abelian surfaces over* K*:*

$$\mathrm{SO}(2), \mathrm{SU}(2), \mathrm{SO}(2) \times \mathrm{SO}(2), \mathrm{SO}(2) \times \mathrm{SU}(2), \mathrm{SU}(2) \times \mathrm{SU}(2), \mathrm{USp}(4).$$

Of these, all 6 occur for $K = \mathbb{Q}$*.*

Let E_1, E_1' be nonisogenous elliptic curves with CM; let E_2, E_2' be nonisogenous elliptic curves over K without CM; let A be an abelian surface such that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. Then the Sato-Tate groups of

$$E_1 \times E_1,\ E_2 \times E_2,\ E_1 \times E_1',\ E_1 \times E_2,\ E_2 \times E_2',\ A$$

have the connected parts listed in the theorem.

However, it is also possible to realize all of the connected parts using absolutely simple abelian surfaces! We will see this later.

The classification of component groups

Connected part	Component groups
$\mathrm{SO}(2)$	$C_1, C_2, C_2, C_2, C_3, C_4, C_4, C_6, C_6, C_6, D_2, D_2, D_2, D_3, D_3, D_4, D_4, D_4, D_6, D_6, D_6, D_6, A_4, S_4, S_4, C_4 \times C_2, C_6 \times C_2, D_2 \times C_2, D_4 \times C_2, D_6 \times C_2, A_4 \times C_2, S_4 \times C_2$
$\mathrm{SU}(2)$	$C_1, C_2, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6$
$\mathrm{SO}(2) \times \mathrm{SO}(2)$	C_1, C_2, C_2, C_4, D_2
$\mathrm{SO}(2) \times \mathrm{SU}(2)$	C_1, C_2
$\mathrm{SU}(2) \times \mathrm{SU}(2)$	C_1, C_2
$\mathrm{USp}(4)$	C_1

Corollary (improves a bound of Silverberg)

The endomorphisms of $A_{\overline{K}}$ are all defined over a Galois extension L of K with $[L : K] \leq 48$. This bound is achieved by the Jacobian of $y^2 = x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$. (Silverberg's bound is 11520.)

The classification of component groups

Connected part	Component groups
$\mathrm{SO}(2)$	$C_1, C_2, C_2, C_2, C_3, C_4, C_4, C_6, C_6, C_6, D_2, D_2, D_2,$ $D_3, D_3, D_4, D_4, D_4, D_6, D_6, D_6, D_6, A_4, S_4, S_4,$ $C_4 \times C_2, C_6 \times C_2, D_2 \times C_2, D_4 \times C_2, D_6 \times C_2,$ $A_4 \times C_2, S_4 \times C_2$
$\mathrm{SU}(2)$	$C_1, C_2, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6$
$\mathrm{SO}(2) \times \mathrm{SO}(2)$	C_1, C_2, C_2, C_4, D_2
$\mathrm{SO}(2) \times \mathrm{SU}(2)$	C_1, C_2
$\mathrm{SU}(2) \times \mathrm{SU}(2)$	C_1, C_2
$\mathrm{USp}(4)$	C_1

Corollary (improves a bound of Silverberg)

The endomorphisms of $A_{\overline{K}}$ are all defined over a Galois extension L of K with $[L:K] \leq 48$. This bound is achieved by the Jacobian of $y^2 = x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$. (Silverberg's bound is 11520.)

Moment sequences

One cannot distinguish the 52 Sato-Tate groups using moments of $\overline{a}_{\mathfrak{q},1}$ alone. For instance, the 34 groups that occur over $\mathbb{Q}$ give rise to only 26 distinct distributions of $\overline{a}_{\mathfrak{q},1}$.

Corollary (of the classification)

One can use the individual moments of $\overline{a}_{\mathfrak{q},1}$ and $\overline{a}_{\mathfrak{q},2}$ (with no joint moments) to distinguish all 52 groups.

In practice, one needs fewer moments if one also considers

$$z_1 = \mathrm{Prob}(\overline{a}_{\mathfrak{q},1} = 0), \qquad z_2 = [\mathrm{Prob}(\overline{a}_{\mathfrak{q},2} = j) : j = -2, -1, 0, 1, 2].$$

This reduces the amount of numerical data needed to match a given curve against the classification: it (more than) suffices to consider $M_{2d}(\overline{a}_{\mathfrak{q},1})$ and $M_d(\overline{a}_{\mathfrak{q},2})$ for $d = 1, 2, 3, 4, 5$ together with z_1, z_2; but without z_1, z_2 more moments are needed.

Moment sequences

One cannot distinguish the 52 Sato-Tate groups using moments of $\overline{a}_{\mathfrak{q},1}$ alone. For instance, the 34 groups that occur over $\mathbb{Q}$ give rise to only 26 distinct distributions of $\overline{a}_{\mathfrak{q},1}$.

Corollary (of the classification)

One can use the individual moments of $\overline{a}_{\mathfrak{q},1}$ and $\overline{a}_{\mathfrak{q},2}$ (with no joint moments) to distinguish all 52 groups.

In practice, one needs fewer moments if one also considers

$$z_1 = \mathrm{Prob}(\overline{a}_{\mathfrak{q},1} = 0), \qquad z_2 = [\mathrm{Prob}(\overline{a}_{\mathfrak{q},2} = j) : j = -2, -1, 0, 1, 2].$$

This reduces the amount of numerical data needed to match a given curve against the classification: it (more than) suffices to consider $M_{2d}(\overline{a}_{\mathfrak{q},1})$ and $M_d(\overline{a}_{\mathfrak{q},2})$ for $d = 1, 2, 3, 4, 5$ together with z_1, z_2; but without z_1, z_2 more moments are needed.

Moment sequences

One cannot distinguish the 52 Sato-Tate groups using moments of $\overline{a}_{\mathfrak{q},1}$ alone. For instance, the 34 groups that occur over $\mathbb{Q}$ give rise to only 26 distinct distributions of $\overline{a}_{\mathfrak{q},1}$.

Corollary (of the classification)

One can use the individual moments of $\overline{a}_{\mathfrak{q},1}$ and $\overline{a}_{\mathfrak{q},2}$ (with no joint moments) to distinguish all 52 groups.

In practice, one needs fewer moments if one also considers

$$z_1 = \mathrm{Prob}(\overline{a}_{\mathfrak{q},1} = 0), \qquad z_2 = [\mathrm{Prob}(\overline{a}_{\mathfrak{q},2} = j) : j = -2, -1, 0, 1, 2].$$

This reduces the amount of numerical data needed to match a given curve against the classification: it (more than) suffices to consider $M_{2d}(\overline{a}_{\mathfrak{q},1})$ and $M_d(\overline{a}_{\mathfrak{q},2})$ for $d = 1, 2, 3, 4, 5$ together with z_1, z_2; but without z_1, z_2 more moments are needed.

Moment sequences

One cannot distinguish the 52 Sato-Tate groups using moments of $\overline{a}_{\mathfrak{q},1}$ alone. For instance, the 34 groups that occur over $\mathbb{Q}$ give rise to only 26 distinct distributions of $\overline{a}_{\mathfrak{q},1}$.

Corollary (of the classification)

One can use the individual moments of $\overline{a}_{\mathfrak{q},1}$ and $\overline{a}_{\mathfrak{q},2}$ (with no joint moments) to distinguish all 52 groups.

In practice, one needs fewer moments if one also considers

$$z_1 = \mathrm{Prob}(\overline{a}_{\mathfrak{q},1} = 0), \qquad z_2 = [\mathrm{Prob}(\overline{a}_{\mathfrak{q},2} = j) : j = -2, -1, 0, 1, 2].$$

This reduces the amount of numerical data needed to match a given curve against the classification: it (more than) suffices to consider $M_{2d}(\overline{a}_{\mathfrak{q},1})$ and $M_d(\overline{a}_{\mathfrak{q},2})$ for $d = 1, 2, 3, 4, 5$ together with z_1, z_2; but without z_1, z_2 more moments are needed.

Real endomorphism algebras

Let $\mathrm{End}(A_{\overline{K}})$ be the (possibly noncommutative) endomorphism ring of $A_{\overline{K}}$.

Theorem (Fité-Rotger-Kedlaya-Sutherland)

(a) *The group* $\mathrm{ST}(A)^\circ$ *(up to conjugation within* $\mathrm{USp}(4)$*) uniquely determines, and is uniquely determined by, the* $\mathbb{R}$*-algebra* $\mathrm{End}(A_{\overline{K}})_{\mathbb{R}} = \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{R}$.

(b) *The group* $\mathrm{ST}(A)$ *(up to conjugation within* $\mathrm{USp}(4)$*) uniquely determines, and is uniquely determined by, the* $\mathbb{R}$*-algebra* $\mathrm{End}(A_{\overline{K}})_{\mathbb{R}}$ *equipped with its* G_K*-action.*

The options for $\mathrm{End}(A_{\overline{K}})_{\mathbb{R}}$ are distinguished by a labeling called the *absolute type*. To distinguish the G_K-action, we add extra data to the label to obtain the *Galois type*.

Real endomorphism algebras

Let $\mathrm{End}(A_{\overline{K}})$ be the (possibly noncommutative) endomorphism ring of $A_{\overline{K}}$.

Theorem (Fité-Rotger-Kedlaya-Sutherland)

(a) *The group* $\mathrm{ST}(A)^\circ$ *(up to conjugation within* $\mathrm{USp}(4)$*) uniquely determines, and is uniquely determined by, the* $\mathbb{R}$*-algebra* $\mathrm{End}(A_{\overline{K}})_{\mathbb{R}} = \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{R}$.

(b) *The group* $\mathrm{ST}(A)$ *(up to conjugation within* $\mathrm{USp}(4)$*) uniquely determines, and is uniquely determined by, the* $\mathbb{R}$*-algebra* $\mathrm{End}(A_{\overline{K}})_{\mathbb{R}}$ *equipped with its* G_K*-action.*

The options for $\mathrm{End}(A_{\overline{K}})_{\mathbb{R}}$ are distinguished by a labeling called the *absolute type*. To distinguish the G_K-action, we add extra data to the label to obtain the *Galois type*.

The absolute type

Absolute type	$\mathrm{ST}(A)^\circ$	$\mathrm{End}(A_{\overline{K}})_{\mathbb{R}}$
A	$\mathrm{USp}(4)$	$\mathbb{R}$
B	$\mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{R}$
C	$\mathrm{SO}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{C}$
D	$\mathrm{SO}(2) \times \mathrm{SO}(2)$	$\mathbb{C} \times \mathbb{C}$
E	$\mathrm{SU}(2)$	$\mathrm{M}_2(\mathbb{R})$
F	$\mathrm{SO}(2)$	$\mathrm{M}_2(\mathbb{C})$

Note that tensoring $\mathrm{End}(A_{\overline{K}})$ with $\mathbb{R}$ loses some distinctions between split and nonsplit cases. For instance, an abelian surface with CM by a quartic field has absolute type **D**; an abelian surface with quaternionic multiplication (QM) has absolute type **E** or **F**.

The absolute type

Absolute type	$\mathrm{ST}(A)^\circ$	$\mathrm{End}(A_{\overline{K}})_{\mathbb{R}}$
A	$\mathrm{USp}(4)$	$\mathbb{R}$
B	$\mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{R}$
C	$\mathrm{SO}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{C}$
D	$\mathrm{SO}(2) \times \mathrm{SO}(2)$	$\mathbb{C} \times \mathbb{C}$
E	$\mathrm{SU}(2)$	$\mathrm{M}_2(\mathbb{R})$
F	$\mathrm{SO}(2)$	$\mathrm{M}_2(\mathbb{C})$

Note that tensoring $\mathrm{End}(A_{\overline{K}})$ with $\mathbb{R}$ loses some distinctions between split and nonsplit cases. For instance, an abelian surface with CM by a quartic field has absolute type **D**; an abelian surface with quaternionic multiplication (QM) has absolute type **E** or **F**.

The Galois type

Most Galois type have labels of the form $\mathbf{L}[G]$, where $\mathbf{L} \in \{\mathbf{A}, \dots, \mathbf{F}\}$ is the absolute type and $G = \mathrm{Gal}(L/K)$ for L the minimal field of definition of endomorphisms.

For $\mathbf{L} = \mathbf{D}, \mathbf{E}$, the label $\mathbf{L}[\mathrm{C}_2]$ is ambiguous; we instead write

$$\mathbf{L}[\mathrm{C}_2, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{\mathrm{C}_2}].$$

For $\mathbf{L} = \mathbf{F}$, the ring $\mathrm{End}(A_{\overline{K}})_{\mathbb{Q}}$ is a quaternion algebra (or matrix algebra) over some imaginary quadratic field M. When $M \not\subseteq K$, we use labels of the form

$$\mathbf{F}[G, H, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{H}], \qquad G = \mathrm{Gal}(L/K), H = \mathrm{Gal}(L/KM).$$

Corollary (of the classification)

Each Galois type receives a unique label under this scheme.

The Galois type

Most Galois type have labels of the form $\mathbf{L}[G]$, where $\mathbf{L} \in \{\mathbf{A}, \dots, \mathbf{F}\}$ is the absolute type and $G = \mathrm{Gal}(L/K)$ for L the minimal field of definition of endomorphisms.

For $\mathbf{L} = \mathbf{D}, \mathbf{E}$, the label $\mathbf{L}[\mathrm{C}_2]$ is ambiguous; we instead write

$$\mathbf{L}[\mathrm{C}_2, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{\mathrm{C}_2}].$$

For $\mathbf{L} = \mathbf{F}$, the ring $\mathrm{End}(A_{\overline{K}})_{\mathbb{Q}}$ is a quaternion algebra (or matrix algebra) over some imaginary quadratic field M. When $M \not\subseteq K$, we use labels of the form

$$\mathbf{F}[G, H, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{H}], \qquad G = \mathrm{Gal}(L/K), H = \mathrm{Gal}(L/KM).$$

Corollary (of the classification)

Each Galois type receives a unique label under this scheme.

The Galois type

Most Galois type have labels of the form $\mathbf{L}[G]$, where $\mathbf{L} \in \{\mathbf{A}, \dots, \mathbf{F}\}$ is the absolute type and $G = \mathrm{Gal}(L/K)$ for L the minimal field of definition of endomorphisms.

For $\mathbf{L} = \mathbf{D}, \mathbf{E}$, the label $\mathbf{L}[\mathrm{C}_2]$ is ambiguous; we instead write

$$\mathbf{L}[\mathrm{C}_2, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{\mathrm{C}_2}].$$

For $\mathbf{L} = \mathbf{F}$, the ring $\mathrm{End}(A_{\overline{K}})_{\mathbb{Q}}$ is a quaternion algebra (or matrix algebra) over some imaginary quadratic field M. When $M \not\subseteq K$, we use labels of the form

$$\mathbf{F}[G, H, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{H}], \qquad G = \mathrm{Gal}(L/K), H = \mathrm{Gal}(L/KM).$$

Corollary (of the classification)

Each Galois type receives a unique label under this scheme.

The Galois type

Most Galois type have labels of the form $\mathbf{L}[G]$, where $\mathbf{L} \in \{\mathbf{A}, \ldots, \mathbf{F}\}$ is the absolute type and $G = \mathrm{Gal}(L/K)$ for L the minimal field of definition of endomorphisms.

For $\mathbf{L} = \mathbf{D}, \mathbf{E}$, the label $\mathbf{L}[\mathrm{C}_2]$ is ambiguous; we instead write

$$\mathbf{L}[\mathrm{C}_2, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{\mathrm{C}_2}].$$

For $\mathbf{L} = \mathbf{F}$, the ring $\mathrm{End}(A_{\overline{K}})_{\mathbb{Q}}$ is a quaternion algebra (or matrix algebra) over some imaginary quadratic field M. When $M \not\subseteq K$, we use labels of the form

$$\mathbf{F}[G, H, \mathrm{End}(A_{\overline{K}})_{\mathbb{R}}^{H}], \qquad G = \mathrm{Gal}(L/K), H = \mathrm{Gal}(L/KM).$$

Corollary (of the classification)

Each Galois type receives a unique label under this scheme.

Comments on the proof

The proof of the FKRS classification consists of three main ingredients.

- A classification of subgroups of USp(4) up to conjugation satisfying certain constraints imposed by Hodge theory (the *Sato-Tate axioms*). This yields the 52 groups in the theorem, plus three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$.
- An enumeration of Galois types and matching of these to subgroups of USp(4). The three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$ remain unmatched.
- Verification that particular Jacobians of genus 2 curves realize all 52 of the remaining groups.

Comments on the proof

The proof of the FKRS classification consists of three main ingredients.

- A classification of subgroups of USp(4) up to conjugation satisfying certain constraints imposed by Hodge theory (the *Sato-Tate axioms*). This yields the 52 groups in the theorem, plus three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$.
- An enumeration of Galois types and matching of these to subgroups of USp(4). The three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$ remain unmatched.
- Verification that particular Jacobians of genus 2 curves realize all 52 of the remaining groups.

Comments on the proof

The proof of the FKRS classification consists of three main ingredients.

- A classification of subgroups of USp(4) up to conjugation satisfying certain constraints imposed by Hodge theory (the *Sato-Tate axioms*). This yields the 52 groups in the theorem, plus three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$.
- An enumeration of Galois types and matching of these to subgroups of USp(4). The three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$ remain unmatched.
- Verification that particular Jacobians of genus 2 curves realize all 52 of the remaining groups.

Comments on the proof

The proof of the FKRS classification consists of three main ingredients.

- A classification of subgroups of USp(4) up to conjugation satisfying certain constraints imposed by Hodge theory (the *Sato-Tate axioms*). This yields the 52 groups in the theorem, plus three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$.
- An enumeration of Galois types and matching of these to subgroups of USp(4). The three extra groups with connected part $\mathrm{SO}(2) \times \mathrm{SO}(2)$ remain unmatched.
- Verification that particular Jacobians of genus 2 curves realize all 52 of the remaining groups.

Beyond dimension 2

One might hope to treat abelian threefolds using similar methods. This looks challenging; there are probably hundreds (thousands) of distinct groups that occur! (However, recent algorithms of Harvey–Sutherland and Harvey should make it possible to do numerics efficiently on both hyperelliptic and planar genus 3 curves.)

Some other cases may be easier. For instance, with Fité and Sutherland we gave a partial classification of Sato-Tate groups arising from weight 3 motives having the Hodge numbers of the symmetric cube of an elliptic curve. Such motives arise in mirror symmetry, e.g., from the Dwork pencil of quintic threefolds:

$$x_0^5 + x_1^5 + x_2^5 + x_3^5 + x_4^5 = \lambda x_0 x_1 x_2 x_3 x_4.$$

Beyond dimension 2

One might hope to treat abelian threefolds using similar methods. This looks challenging; there are probably hundreds (thousands) of distinct groups that occur! (However, recent algorithms of Harvey–Sutherland and Harvey should make it possible to do numerics efficiently on both hyperelliptic and planar genus 3 curves.)

Some other cases may be easier. For instance, with Fité and Sutherland we gave a partial classification of Sato-Tate groups arising from weight 3 motives having the Hodge numbers of the symmetric cube of an elliptic curve. Such motives arise in mirror symmetry, e.g., from the Dwork pencil of quintic threefolds:

$$x_0^5 + x_1^5 + x_2^5 + x_3^5 + x_4^5 = \lambda x_0 x_1 x_2 x_3 x_4.$$