Sato–Tate groups of abelian threefolds: adventures in SU(3)

Kiran S. Kedlaya

joint with Francesc Fité and Andrew Sutherland (arXiv:2106.13759)

Department of Mathematics, University of California San Diego
kedlaya@ucsd.edu
These slides are available from https://kskedlaya.org/slides/.

Poznań–Szczecin arithmetic geometry seminar (virtual)
July 8, 2021

L-functions of algebraic varieties

Let k be a number field with absolute Galois group G_k. For each finite place $\mathfrak{p}$ of k, choose a decomposition group $G_{\mathfrak{p}} \subset G_k$, let $I_{\mathfrak{p}} \subset G_{\mathfrak{p}}$ be the inertia subgroup, and let $\mathrm{Frob}_{\mathfrak{p}} \in G_{\mathfrak{p}}/I_{\mathfrak{p}}$ be the Frobenius element.

Let X be a smooth proper scheme of dimension d over k. For $i = 0, \ldots, 2d$, the Weil conjectures imply that the L-**polynomial**

$$L_{X,i,\mathfrak{p}}(T) = \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}}, H^i_{\mathrm{et}}(X_{\overline{k}}, \mathbb{Q}_\ell)^{I_{\mathfrak{p}}})$$

belongs to $1 + T\mathbb{Z}[T].$*

The L-**function** $L_{X,i}(s)$ is defined for $\mathrm{Real}(s) \gg 0$, then (conjecturally) meromorphically extended to $\mathbb{C}$, by setting

$$L_{X,i}(s) = \prod_{\mathfrak{p}} L_{X,i,\mathfrak{p}}(\mathrm{Norm}(\mathfrak{p})^{-s})^{-1}.$$

---

*If the weight-monodromy conjecture holds for X, then this does not depend on ℓ.

L-polynomials of algebraic varieties

Hereafter, we consider only finite places $\mathfrak{p}$ at which X admits a smooth model, with mod-$\mathfrak{p}$ reduction $X_{\mathfrak{p}}$. For $q = \mathrm{Norm}(\mathfrak{p})$, the zeta function of $X_{\mathfrak{p}}$ has the form

$$Z(X_{\mathfrak{p}}, T) = \exp\left(\sum_{n=1}^{\infty} \#X_{\mathfrak{p}}(\mathbb{F}_{q^n}) \frac{T^n}{n}\right) = \prod_{i=0}^{2d} L_{X,i,\mathfrak{p}}(T)^{(-1)^{i+1}}.$$

By the Weil conjectures, the roots of $L_{X,\mathfrak{p},i}$ have $\mathbb{C}$-absolute value $q^{-i/2}$. It is thus natural to consider the **normalized *L*-polynomial**

$$\overline{L}_{X,i,\mathfrak{p}}(T) = L_{X,i,\mathfrak{p}}(Tq^{-i/2}) \in 1 + T\mathbb{R}[T]$$

which has roots on the circle $|T| = 1$.

The Sato-Tate group of an abelian variety

Hereafter, we take $X = A$ to be an abelian variety of dimension g and take $i = 1$. Then there exist a compact Lie group $\mathrm{ST}(A)$ contained in $\mathrm{USp}(2g)$ (the group of unitary symplectic $2g \times 2g$ matrices) and a sequence of conjugacy classes $F_{\mathfrak{p}} \in \mathrm{Conj}(\mathrm{ST}(A))$ such that

$$\overline{L}_{A,1,\mathfrak{p}}(T) = \det(1 - TF_{\mathfrak{p}}).$$

For generic A we have $\mathrm{ST}(A) = \mathrm{USp}(2g)$.

The **generalized Sato–Tate conjecture** for A is that the $F_{\mathfrak{p}}$ are uniformly distributed[†] in $\mathrm{Conj}(\mathrm{ST}(A))$ for the image of Haar measure. This would follow from the analytic continuation of "enough" arithmetic L-functions.

[†]This is a strictly stronger assertion than the statement that the characteristic polynomials are equidistributed, due to fusion from $\mathrm{ST}(A)$ to $\mathrm{USp}(2g)$. We will see later that this fusion can conflate different groups; to separate them one must work with representations of $\mathrm{USp}(2g)$ other than the standard one.

The case of dimension 1

For $A = E$ an elliptic curve, we have

$$L_{A,1,\mathfrak{p}}(T) = 1 - a_\mathfrak{p} T + q T^2, \qquad |a_\mathfrak{p}| \le 2\sqrt{q}.$$

There are three possibilities for $ST(A)$ as a conjugacy class of subgroups of $SU(2) = USp(2)$.

- If E does not have complex multiplication, then $ST(A) = SU(2)$.
- If E has complex multiplication by a quadratic field contained in k, then $ST(A) = SO(2)$.
- If E has complex multiplication by a quadratic field not contained in k, then $ST(A)$ is the normalizer of $SO(2)$ in $SU(2)$. This is a **disconnected** compact Lie group; the component group $\pi_0(ST(A))$ is cyclic of order 2.

Relationship with the motivic Galois group

Under suitable motivic conjectures, the Sato–Tate group can be described in terms of the **motivic Galois group** of the 1-motive of A (Serre). This can be made more concrete and explicit (Banaszak–K) precisely in cases where the Mumford–Tate conjecture is known (Commelin–Cantoral Farfán).

In this talk, we will be interested in the case $g \leq 3$. Then things simplify because all Hodge classes on powers of A are linear combinations of powers of hyperplane classes, so the Mumford–Tate group and the Sato–Tate group are both controlled by endomorphisms.

Endomorphisms

Pick an embedding $k \hookrightarrow \mathbb{C}$ and equip $H_1(X_{\mathbb{C}}^{\mathsf{an}}, \mathbb{Q})$ with the symplectic form ψ coming from the cup product. For $g \leq 3$,[‡] we can characterize $\mathsf{ST}(A)$ as the subgroup of $\mathsf{USp}(2g)$ consisting of those elements which carry

$$\mathsf{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q} \subset \mathsf{End}(H^1(X_{\mathbb{C}}^{\mathsf{an}}, \mathbb{C}))$$

to itself via the action of some element of G_k.

From the construction, we have a canonical group isomorphism

$$\pi_0(\mathsf{ST}(A)) \cong \mathsf{Gal}(L/k)$$

where L is the **endomorphism field** of A: the minimal field of definition of all endomorphisms of $A_{\overline{k}}$.

[‡] For $g > 3$, a similar statement holds provided that the Mumford–Tate group is controlled by endomorphisms. Otherwise, one must replace endomorphisms with the algebra of absolute Hodge cycles.

The case of surfaces

Theorem (Fité–K–Rotger–Sutherland, 2012)

There are 52 conjugacy classes of closed subgroups of USp(4) *which occur as* ST(A) *for some abelian surface A over some number field K.*

- This includes 6 options for $ST(A)^\circ$; see next slide.
- $\#\pi_0(ST(A))$ divides $48 = 2^4 \times 3$ (and this value occurs).
- The 52 cases correspond to distinct distributions of $\overline{L}_\mathfrak{p}$.
- The theorem is quantified over all K. If we require $K = \mathbb{Q}$, then 34 cases occur. If we require K to be totally real, then 35 cases occur.
- There is a field K over which all 52 cases occur (Fité–Guitart).
- Nothing changes if we restrict to principally polarized abelian surfaces or even Jacobians. FKRS give explicit genus 2 curves in all cases.

Identity components vs. extensions: the case of surfaces

$\mathrm{End}(A_{\overline{\mathbb{Q}}})_{\mathbb{R}}$	$\mathrm{ST}(A)^{\circ}$	Extensions	Maximal
$\mathbb{R}$	$\mathrm{USp}(4)$	1	1
$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(2)$	2	1
$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2)$	2	1
$\mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1)$	5	2
$\mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2)_2$	10	2
$\mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1)_2$	32	2
Total		52	9

Here $*_2$ denotes the diagonal embedding.

Warning: if A is geometrically simple, $\mathrm{ST}(A)^{\circ}$ can still be decomposable because it only depends on $\mathrm{End}(A_{\overline{k}}) \otimes_{\mathbb{Z}} \mathbb{R}$. For example, if A has CM by a quartic field K, then $\mathrm{End}(A_{\overline{k}}) \otimes_{\mathbb{Z}} \mathbb{R} \cong K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C} \times \mathbb{C}$.

The case of threefolds

Theorem (Fité–K–Sutherland, 2021 preprint)

There are 410 *conjugacy classes of closed subgroups of* USp(6) *which occur as* ST(A) *for some abelian threefold* A *over some number field* K.

- This includes 14 options for ST(A)$^\circ$ (Moonen–Zarhin).
- $\#\pi_0(\text{ST}(A))$ divides[§] one of $192 = 2^6 \times 3$, $336 = 2^4 \times 3 \times 7$, $432 = 2^4 \times 3^3$ (and these values occur).
- The 410 cases correspond to only 409 distinct distributions of $\overline{L}_\mathfrak{p}$. The two cases that collide have distinct component groups.
- We do not know what happens if we restrict K.
- We do not know what happens if we require a principal polarization.[¶]

[§] This refines earlier estimates by Silverberg and Guralnick-K, the latter computing the LCM of all values of $\#\pi_0(\text{ST}(A))$.

[¶] I previously announced that all cases can be realized with a principal polarization; we no longer believe this. Our examples include polarizations of degree 1, 2, 3, 6.

Identity components vs. extensions: the case of threefolds

End$(A_{\overline{\mathbb{Q}}})_{\mathbb{R}}$	ST$(A)^{\circ}$	Extensions	Maximal
$\mathbb{R}$	USp(6)	1	1
$\mathbb{C}$	U(3)	2	1
$\mathbb{R} \times \mathbb{R}$	SU(2) × USp(4)	1	1
$\mathbb{C} \times \mathbb{R}$	U(1) × USp(4)	2	1
$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	SU(2) × SU(2) × SU(2)	4	1
$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	U(1) × SU(2) × SU(2)	5	1
$\mathbb{C} \times \mathbb{C} \times \mathbb{R}$	U(1) × U(1) × SU(2)	5	2
$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	U(1) × U(1) × U(1)	13	3
$\mathbb{R} \times M_2(\mathbb{R})$	SU(2) × SU(2)$_2$	10	2
$\mathbb{R} \times M_2(\mathbb{C})$	SU(2) × U(1)$_2$	32	2
$\mathbb{C} \times M_2(\mathbb{R})$	U(1) × SU(2)$_2$	31	2
$\mathbb{C} \times M_2(\mathbb{C})$	U(1) × U(1)$_2$	122	2
$M_3(\mathbb{R})$	SU(2)$_3$	11	2
$M_3(\mathbb{C})$	U(1)$_3$	171	12
Total		410	33

An initial subdivision

For each candidate G° for $\mathrm{ST}(A)^\circ$, candidates for G correspond to conjugacy classes of finite subgroups of N/G° where N is the normalizer of G° in $\mathrm{USp}(6)$. We distinguish four subcases.

- **Indecomposable:** $G^\circ = \mathrm{USp}(6), \mathrm{U}(3)$. In these cases, the only options are $\mathrm{USp}(6), \mathrm{U}(3), N(\mathrm{U}(3))$.

- **Split product:** G° factors as a nontrivial product $G_1^\circ \times G_2^\circ$ with no shared factors between the two sides (i.e., $\mathrm{U}(1) \times * \times \mathrm{SU}(2)$ or $* \times *_2$). In these cases, N splits as $N_1 \times N_2$, so we can reduce to the classification for elliptic curves and abelian surfaces.

- **Triple products**: $G^\circ = \mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2), \mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$. In these cases, N/G° is finite.

- **Triple diagonals**: $G^\circ = \mathrm{SU}(2)_3, \mathrm{U}(1)_3$. In these cases, N/G° is infinite, but there is a bound on the order of elements in N/G° coming from the **rationality condition** (see below).

The upper bound: a group-theoretic classification

For each candidate G° for $\mathrm{ST}(A)^\circ$, we identify all extensions of G° within $\mathrm{USp}(6)$ satisfying the **rationality condition**: for every representation of $\mathrm{USp}(6)$, the average trace on each coset of G° is in $\mathbb{Z}$.

This gives the correct upper bound except when G° includes multiple factors of $\mathrm{U}(1)$, in which case one must rule out some cases using Shimura's theory of CM types. (For $G^\circ = \mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$, $[N : G^\circ] = 48$ but $[G : G^\circ] \leq 8$.)

Most of the work occurs when $G^\circ = \mathrm{U}(1)_3$; in this case $N = \mathrm{U}(3) \rtimes \mathrm{C}_2$. More on this later.

The lower bound: realization by PPAVs

By base extension, for each G° it suffices to realize each **maximal** candidate for G using some abelian threefold over $\mathbb{Q}$.

- For G° indecomposable, use generic hyperelliptic and Picard curves.
- For G° a split product, use products of lower-dimensional examples. In all cases except $G^\circ = U(1) \times U(1)_2$, we also find explicit examples of genus 3 curves.
- For $G^\circ = SU(2) \times SU(2) \times SU(2), U(1) \times U(1) \times U(1), SU(2)_3$, we find explicit examples of genus 3 curves.
- For $G^\circ = U(1)_3$, we realize G by twisting either the cube of an elliptic curve with CM by an imaginary quadratic field M, or an isogenous abelian variety. The twist uses a Galois cocycle valued in a subgroup[‖] of $GL(3, \mathfrak{o}_M)$ with projective image G/G°.

[‖] These are almost all complex reflection groups, which makes it easy to solve the embedding problem needed to construct the cocycle. To make explicit examples, we use the LMFDB tables of number fields.

The case $G^\circ = U(1)_3$

We classify groups G which can occur as the Sato–Tate group of an abelian threefold with $G^\circ = U(1)_3$. The normalizer N of G° in $USp(6)$ is

$$U(3) \rtimes C_2 = \left\{ \begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix} \right\} \rtimes \langle J \rangle, \qquad J = \begin{pmatrix} 0 & I_3 \\ -I_3 & 0 \end{pmatrix}.$$

We identify finite subgroups of $H = N/G^\circ = U(3)/U(1)_3 \rtimes C_2$ satisfying

$$\begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix} \in H \cap U(3)/U(1)_3 \implies |\mathrm{Trace}(A)|^2 \in \mathbb{Z};$$

this is the rationality condition for the representation $\wedge^2 \mathbb{C}^6$ of $USp(6)$.

The inclusion $SU(3) \subset U(3)$ induces an isomorphism

$$PSU(3) = SU(3)/\mu_3 \cong U(3)/U(1)_3.$$

We may thus assume that $H \subset SU(3)/\mu_3 \rtimes C_2$, then replace H with its inverse image in $SU(3) \rtimes C_2$ (and remember that it contains μ_3).

The finite subgroups of SU(3)

The finite subgroups of SU(3) containing μ_3 were classified in 1916 by Blichfeldt–Dickson–Miller. They come in four infinite families:

(A) abelian groups, which conjugate into the diagonal torus;

(B) subgroups of SU(2) which are projectively D_n, A_4, S_4, A_5;

(C) groups projectively of the form $* \rtimes C_3$;

(D) groups projectively of the form $* \rtimes S_3$;

together with six exceptional cases which we label by their projective orders:

$$E(36), E(72), E(216), E(60), E(360), E(168).$$

Of these, the first three are an increasing sequence of solvable groups ending with the **Hessian** group; the last three have simple projective images $A_5, A_6, \mathrm{PSL}(2,7)$.

The rationality condition for cyclic groups

To impose the (restricted) rationality condition for cyclic groups, it is enough to treat the group generated by a diagonal matrix $\mathrm{Diag}(a, b, c)$ where a, b, c are roots of unity with $abc = 1$. The rationality condition for $\wedge^2 \mathbb{C}^6$ implies that $|a^n + b^n + c^n|^2 \in \mathbb{Z}$. For $x = a/b, y = b/c, z = c/a$, this becomes

$$\left(x^n + x^{-n}\right) + \left(y^n + y^{-n}\right) + \left(z^n + z^{-n}\right) \in \mathbb{Z} \qquad (n = 1, 2, \dots).$$

We resolve the case $n = 1$ using the classification of short additive relations among roots of unity (Mann, Włodarski, Conway–Jones). In particular, either $(a + b)(b + c)(c + a) = 0$ or $a^m = b^m = c^m = 1$ for some $m \leq 90$.

We then formally deduce the general case. We find that $a^m = b^m = c^m = 1$ for some $m \leq 36$.

The rationality condition for noncyclic groups

From the previous calculation, we obtain a finite set S of conjugacy classes in SU(3) with the property: a finite subgroup of SU(3) satisfies the (restricted) rationality condition iff it is contained in the union over S.

At this point, it is "straightforward" to step through the classification of finite subgroups of SU(3) to impose rationality. We obtain 63 groups in all.

Extensions: standard, split, and nonsplit

Fix a subgroup $H \subset SU(3)$ in our classification. How can it occur as the intersection with $SU(3)$ of a finite subgroup of $SU(3) \rtimes C_2$?

In our classification, we construct explicit representatives such that in all but one case, H is stable under complex conjugation. We thus get one extension of the form $H \cup JH$, which we call **standard**.

We then classify additional extensions by computing the normalizer N_H of H in $SU(3)$. We call these **split** or **nonsplit** according to whether they are of the form $H \rtimes C_2$. (Warning: an extension group is **not** uniquely determined by its extension class!)

For any given H, we obtain at most one extension of each type (standard, split, nonsplit)

Table of results

Case	H	J	J_s	J_n	Total
Abelian groups	22	22	15	9	60
Extensions by C_2	18	18	12	0	48
Exceptional groups from SU(2)	6	5	4	0	15
Extensions by A_3	7	7	5	0	19
Extensions by S_3	6	6	0	0	12
Solvable exceptional groups	3	3	0	1	7
Simple exceptional groups	1	1	0	0	2
Total	63	62	36	10	171

Numbers of finite subgroups of $SU(3) \rtimes C_2$ accounted for at the various stages of the classification. The columns H, J, J_s, J_n count subgroups of SU(3), standard extensions, split nonstandard extensions, and nonsplit nonstandard extensions.

Moment statistics

For G a closed subgroup of $\mathrm{USp}(6)$ and e_1, e_2, e_3 nonnegative integers, the **moment** M_{e_1, e_2, e_3} of G can be interpreted either as:

- the expected value of $a_1^{e_1} a_2^{e_2} a_3^{e_3}$ where $1 + a_1 T + \cdots + T^6$ is the charpoly of a random element of G;
- the dimension of the G-fixed subspace of $(\mathbb{C}^6)^{\otimes e_1} \otimes (\wedge^2 \mathbb{C}^6)^{\otimes e_2} \otimes (\wedge^3 \mathbb{C}^6)^{\otimes e_3}$. (This is a nonnegative integer!)

For our 410 groups, we obtain 409 distinct collections** of moments. The collision comes from two cases with identity component $\mathrm{U}(1)_3$ whose π_0's are distinct groups of order 54 with a common index-2 subgroup.

**It suffices to consider triples with $e_1 + e_2 + e_3 \leq 6$.

Other statistics

An alternative to moments was suggested by Shieh: for a given representation V, compute the dimension of the G-fixed subspace of $V \otimes V$. These **diagonal character norms** give statistics with better convergence than moments.

When comparing to L-function data, it is useful to also record the density of points on which a_1, a_2, a_3 are constant; e.g., for a non-CM elliptic curve, $a_1 = 0$ with density $1/2$. (By parity, only the value 0 can occur for a_1, a_3 with positive density, but a_2 can take other integer values.)

Averaging over Sato–Tate groups

Let G be a closed subgroup of $\mathrm{USp}(6)$. We say G is of **central type** if G can be written as $\langle G^\circ, H \rangle$ for some finite subgroup H such that for each $h \in H$, the map

$$G^\circ \to \mathbb{R}[T], \qquad g \mapsto \det(1 - ghT)$$

is a class function.

In this case, averaging a class function over a component of G can be achieved by averaging a related class function over G°. We can then use the Weyl character formula again to do the averaging.

This leaves a few sticky cases, notably $N(\mathrm{U}(3))$. In this case we use a method of Lee–Oh based on work of Bump–Gamburd. More on this in Francesc's talk...