C. R. Acad. Sci. Paris, Ser. I 357 (2019) 823–826

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory

Arithmetic invariants from Sato–Tate moments

Invariants arithmétiques provenant des moments de Sato–Tate

Edgar Costa, Francesc Fité, Andrew V. Sutherland

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, MA 02139, United States

A R T I C L E I N F O

Article history:
Received 8 October 2019
Accepted after revision 19 November 2019
Available online 27 November 2019

Presented by the Editorial Board

A B S T R A C T

We give some arithmetic-geometric interpretations of the moments $\mathrm{M}_2[a_1]$, $\mathrm{M}_1[a_2]$, and $\mathrm{M}_1[s_2]$ of the Sato–Tate group of an abelian variety A defined over a number field by relating them to the ranks of the endomorphism ring and Néron–Severi group of A.

R É S U M É

Nous donons des interprétations arithmético-géométriques des moments $\mathrm{M}_2[a_1]$, $\mathrm{M}_1[a_2]$, et $\mathrm{M}_1[s_2]$ du groupe de Sato–Tate d'une variété abélienne A definie sur un corps de nombres en les rapportant aux rangs de l'anneau d'endomorphismes et du groupe de Néron–Severi de A.

Let A be an abelian variety of dimension $g \geq 1$ defined over a number field k. For a rational prime ℓ, let

$$\rho_{A,\ell}\colon G_k \to \mathrm{Aut}(V_\ell(A))$$

denote the ℓ-adic representation attached to A given by the action of the absolute Galois group of G_k on the rational Tate module of A. Let G_ℓ denote the Zariski closure of the image of $\rho_{\ell,A}$, viewed as a subgroup scheme of GSp_{2g}, let G_ℓ^1 denote the kernel of the restriction to G_ℓ of the similitude character, and fix an embedding ι of $\mathbb{Q}_\ell$ into $\mathbb{C}$. The *Sato–Tate group* $\mathrm{ST}(A)$ of A is a maximal compact subgroup of the $\mathbb{C}$-points of the base change $G_\ell^1 \times_{\mathbb{Q}_\ell,\iota} \mathbb{C}$ (see [4, §2] and [8, Chap. 8]).

Throughout this note, we shall assume that the algebraic Sato–Tate conjecture of Banaszak and Kedlaya [1, Conjecture 2.1] holds for A. This conjecture is known, for example, when $g \leq 3$ (see [1, Thm. 6.11]), or more generally, whenever the Mumford–Tate conjecture holds for A (see [2]). It predicts the existence of an algebraic reductive group $\mathrm{AST}(A)$ defined over $\mathbb{Q}$ such that

$$\mathrm{AST}(A) \times_{\mathbb{Q}} \mathbb{Q}_\ell \simeq G_\ell^1$$

E-mail addresses: edgarc@mit.edu (E. Costa), ffite@mit.edu (F. Fité), drew@math.mit.edu (A.V. Sutherland).
URLs: https://edgarcosta.org (E. Costa), https://math.mit.edu/~ffite/ (F. Fité), https://math.mit.edu/~drew/ (A.V. Sutherland).

https://doi.org/10.1016/j.crma.2019.11.008
1631-073X/

for every prime ℓ. In this case, $\mathrm{ST}(A)$ can be defined as a maximal compact subgroup of the $\mathbb{C}$-points of $\mathrm{AST}(A) \times_{\mathbb{Q}} \mathbb{C}$, which depends neither on the choice of a prime ℓ nor on the choice of an embedding ι.

By construction, $\mathrm{ST}(A)$ comes equipped with a faithful self-dual representation

$$\rho : \mathrm{ST}(A) \to \mathrm{GL}(V),$$

where V is a $\mathbb{C}$ vector space of dimension $2g$. We call ρ the standard representation of $\mathrm{ST}(A)$ and use it to view $\mathrm{ST}(A)$ as a compact real Lie subgroup of $\mathrm{USp}(2g)$.

In this note, we are interested in the following three virtual characters of $\mathrm{ST}(A)$:

$$a_1 = \mathrm{Tr}\left(V\right), \qquad a_2 = \mathrm{Tr}\left(\wedge^2 V\right), \qquad s_2 = a_1^2 - 2a_2 \,.$$

For a nonnegative integer j, define the jth moment of a virtual character φ as the virtual multiplicity of the trivial representation in φ^j. In particular, we have

$$\begin{aligned} \mathrm{M}_2[a_1] &= \dim_{\mathbb{C}} \left(V^{\otimes 2}\right)^{\mathrm{ST}(A)}, \\ \mathrm{M}_1[a_2] &= \dim_{\mathbb{C}} \left(\wedge^2 V\right)^{\mathrm{ST}(A)}, \\ \mathrm{M}_1[s_2] &= \mathrm{M}_2[a_1] - 2\mathrm{M}_1[a_2]. \end{aligned} \tag{1}$$

Let $\mathrm{End}(A)$ denote the ring of endomorphisms of A (defined over k).

Proposition 1. *We have*

$$\mathrm{M}_2[a_1] = \mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(A)) \,.$$

Proof. By Faltings' isogeny theorem [3], we have

$$\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(A)) = \dim_{\mathbb{Q}_\ell}(\mathrm{End}(A) \otimes \mathbb{Q}_\ell) = \dim_{\mathbb{Q}_\ell}(\mathrm{End}_{G_\ell}(V_\ell(A))) \,.$$

Observing that homotheties centralize $V_\ell(A) \otimes V_\ell(A)^\vee$ and that Weyl's unitarian trick allows us to pass from G_ℓ^1 to the maximal compact subgroup $\mathrm{ST}(A)$, we obtain

$$\dim_{\mathbb{Q}_\ell} \left(V_\ell(A) \otimes V_\ell(A)^\vee\right)^{G_\ell} = \dim_{\mathbb{Q}_\ell} \left(V_\ell(A) \otimes V_\ell(A)^\vee\right)^{G_\ell^1} = \dim_{\mathbb{C}} \left(V \otimes V^\vee\right)^{\mathrm{ST}(A)} .$$

The proposition follows from the definition of $\mathrm{M}_2[a_1]$ and the self-duality of V. □

Let $\mathrm{NS}(A)$ denote the Néron–Severi group of A.

Proposition 2. *We have*

$$\mathrm{M}_1[a_2] = \mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A)) \,.$$

Proof. As explained in [9, §2] (and in [10, Eq. (9)] using the same argument over finite fields), Faltings isogeny theorem provides an isomorphism

$$\mathrm{NS}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \left(H^2_{\text{ét}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)(1)\right)^{G_k} \simeq \left(\left(\wedge^2 V_\ell(A)\right)(-1)\right)^{G_\ell},$$

where we have denoted Tate twists in the usual way and we have used the isomorphism $V_\ell(A) \simeq H^1_{\text{ét}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)(1)$. Then, as in the proof of Proposition 1, we have

$$\mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A)) = \dim_{\mathbb{Q}_\ell} \left(\left(\wedge^2 V_\ell(A)\right)(-1)\right)^{G_\ell^1} = \dim_{\mathbb{C}} \left(\wedge^2 V\right)^{\mathrm{ST}(A)} = \mathrm{M}_1[a_2],$$

which completes the proof. □

In order to obtain a description of $\mathrm{M}[s_2]$, we will first relate $\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(A))$ with $\mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A))$. There are three division algebras over $\mathbb{R}$: the quaternions $\mathbb{H}$, the complex field $\mathbb{C}$, and the real field $\mathbb{R}$ itself. By Wedderburn's theorem we have

$$\mathrm{End}(A) \otimes \mathbb{R} \simeq \prod_i \mathrm{M}_{t_i}(\mathbb{R}) \times \prod_i \mathrm{M}_{n_i}(\mathbb{H}) \times \prod_i \mathrm{M}_{p_i}(\mathbb{C}) \,, \tag{2}$$

for some nonnegative integers t_i, n_i, p_i, where M_n denotes the $n \times n$ matrix ring.

Table 1
$\mathbb{R}$-algebra dimensions for isotypic A by Albert type.

Type	$\dim_{\mathbb{R}}(\mathrm{End}(A)\otimes\mathbb{R})$	$\dim_{\mathbb{R}}\left((\mathrm{End}(A)\otimes\mathbb{R})^{\dagger}\right)$	$2\sum_i n_i - \sum_i t_i$
(I)	er^2	$er(r+1)/2$	$-er$
(II)	$4er^2$	$e(r+2r^2)$	$-2er$
(III)	$4er^2$	$e(-r+2r^2)$	$2er$
(IV)	$2er^2d^2$	er^2d^2	0

Lemma 3. *With the notation of equation* (2)*, we have*

$$\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(A)) - 2\cdot \mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A)) = 2\sum_i n_i - \sum_i t_i\,.$$

In particular, we have the following inequality

$$2\cdot \mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A)) - g \le \mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(A)) \le 2\cdot \mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A)) + g\,. \tag{3}$$

Proof. Let † denote the Rosati involution of $\mathrm{End}(A)\otimes\mathbb{R}$. As explained in [6, p. 190], we have $\mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A)) = \dim_{\mathbb{R}}((\mathrm{End}(A)\otimes\mathbb{R})^{\dagger})$. For the first part of the lemma, it thus suffices to prove

$$\dim_{\mathbb{R}}(\mathrm{End}(A)\otimes\mathbb{R}) - 2\cdot\dim_{\mathbb{R}}\left((\mathrm{End}(A)\otimes\mathbb{R})^{\dagger}\right) = 2\sum_i n_i - \sum_i t_i\,. \tag{4}$$

We say that an abelian variety defined over k is isotypic if it is isogenous (over k) to the power of a simple abelian variety. Since both the left-hand and right-hand sides of (4) are additive in the isotypic components of A, we may reduce to the case where A is isotypic. We thus may assume that A is the rth power of a simple abelian variety B. By Albert's classification of division algebras with a positive involution [6, Thm. 2, §21], there are four possibilities for $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{R}$, namely

$$\text{(I) } \mathrm{M}_r(\mathbb{R}^e)\,,\qquad \text{(II) } \mathrm{M}_r(\mathrm{M}_2(\mathbb{R})^e)\,,\qquad \text{(III) } \mathrm{M}_r(\mathbb{H}^e)\,,\qquad \text{(IV) } \mathrm{M}_r(\mathrm{M}_d(\mathbb{C})^e)\,,$$

where e and d are nonnegative integers. The action of the Rosati involution † on $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{R}$ is also described in [6, Thm. 2, §21], and the dimension of its fixed subspace can be easily read from the parameter η listed on [6, Table on p. 202]. The first part of the lemma then follows from the computations listed in Table 1.

For the second part of the lemma, we need to show that

$$-g \le 2\sum_i n_i - \sum_i t_i \le g. \tag{5}$$

All sides of (5) are additive in the isotypic components of A, thus the result follows from Table 1 once we take into account that $e \le \dim(B)$ for type (I), and that $2e \le \dim(B)$ for types (II) and (III) (see [6, Table on p. 202]). □

As an immediate consequence of Proposition 1, Proposition 2, and Lemma 3, we obtain the following corollary.

Corollary 4. *With the notation of equation* (2)*, we have*

$$\mathrm{M}_1[s_2] = 2\sum_i n_i - \sum_i t_i\,.$$

Remark 5. The moment $\mathrm{M}_1[s_2]$ can also be interpreted as a Frobenius–Schur indicator, which allows us to give an alternative proof of (4), conditional on the Mumford–Tate conjecture, which does not make use of Albert's classification. Recall that $\rho : \mathrm{ST}(A)\to \mathrm{GL}(V)$ denotes the standard representation of $\mathrm{ST}(A)$ and let $\Psi^2(\rho)$ be the central function defined as $\Psi^2(\rho)(g) = \rho(g^2)$ for every $g\in \mathrm{ST}(A)$; note that s_2 is simply $\mathrm{Tr}\,\Psi^2(\rho)$. Thus, the moment $\mathrm{M}_1[s_2]$ is the Frobenius–Schur indicator $\mu(\rho)$ of the standard representation ρ, which is just the multiplicity of the trivial representation in $\Psi^2(\rho)$. Inequality (4) simply asserts that the trivial bound $|\mu(\rho)|\le 2g$ can be improved to the sharper bound $|\mu(\rho)|\le g$. Recall that the Frobenius–Schur indicator of an irreducible representation can only take the values 1, −1, and 0, depending on whether the representation is realizable over $\mathbb{R}$, has real trace, but it is not realizable over $\mathbb{R}$, or has trace taking some value in $\mathbb{C}\setminus\mathbb{R}$, respectively (see [7, p. 108]). To obtain the sharper bound, it suffices to show that any irreducible constituent σ of the standard representation ρ having real trace must have dimension at least 2. This follows from our assumption that the Mumford–Tate conjecture holds for A.

The results in this note explain, in particular, certain redundancies in Table 8 of [4], which Seoyoung Kim used to prove Proposition 1 in the case where A is an abelian surface [5, Proof of Thm. 3.4].

Acknowledgements

The main results of this paper were discovered during the *Arithmetic of Curves* workshop held at Baskerville Hall in Hay-on-Wye, Wales, in August 2018. We thank the organizers, Alexander Betts, Tim and Vladimir Dokchitser, and Celine Maistret for their kind invitation to participate. We also thank Seoyoung Kim for her interest in this note. The authors were financially supported by the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation via Simons Foundation grant 550033. Fité was partially supported by MTM2015-63829-P (Ministerio de Economía y Competitividad).

References

[1] G. Banaszak, K.S. Kedlaya, An algebraic Sato–Tate group and Sato–Tate conjecture, Indiana Univ. Math. J. 64 (2015) 245–274.

[2] V. Cantoral Farfán, J. Commelin, The Mumford–Tate conjecture implies the algebraic Sato–Tate conjecture of Banaszak and Kedlaya, arXiv:1905.04086.

[3] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983) 349–366.

[4] F. Fité, K.S. Kedlaya, A.V. Sutherland, V. Rotger, Sato–Tate distributions and Galois endomorphism modules in genus 2, Compos. Math. 148 (2012) 1390–1442.

[5] S. Kim, The Sato–Tate conjecture and Nagao's conjecture, arXiv:1712.02775.

[6] D. Mumford, Abelian Varieties, Tata Institute of Fundamental Research, Bombay, Oxford University Press, 1970.

[7] J.-P. Serre, Linear Representations of Finite Groups, Springer-Verlag, New York, 1977.

[8] J.-P. Serre, Lectures on $N_X(p)$, CRC Press, Boca Raton, FL, USA, 2012.

[9] J. Tate, Algebraic cycles and poles of zeta functions, in: Arithmetical Algebraic Geometry, Proceedings of a Conference Held at Purdue University, IN, USA, 5–7 December 1963, Harper & Row, New York, 1965, pp. 93–110.

[10] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.