Galois representations and Sato–Tate groups

Leonardo Colò and David Kohel

This research project will focus on Galois representations assocated to arithmetic geometric objects, with a view to understanding the Sato–Tate group of an elliptic curve — a projective curve with a structure of abelian group — and its generalization to higher genus curves and abelian varieties — higher dimensional analogues of elliptic curves.

The Sato–Tate group is a continuous real Lie group, which is constructed from a limit of finite Galois representations (whose image is a profinite group). In order to motivate the construction of the Sato–Tate group, we first discuss the Galois theory of number fields, their characters, and class functions (functions, such as characters, which are well-defined on a conjugacy class). After exploring the (finite) Galois groups of number fields, we turn to elliptic curves. An elliptic curve E is a plane curve (set of solutions (x, y) in the plane) of the form

$$y^2 = x^3 + ax + b.$$

For integers a and b, we can study the number of points over a finite field, $|E(\mathbb{F}_p)| = p + 1 - t$, and interpret the *trace of Frobenius* $t = t(p)$ as the value of a random variable (at group elements indexed by primes p). After suitable normalization, the sequence $(\tilde{t}(p))$ are character values on a compact Lie group G, called the Sato–Tate group, equidistributed respect to the Haar measure on that group. Finally we will consider generalizations to genus-2 curves $y^2 = f(x)$, where $\deg(f) = 5$ or 6, or more general curves or geometric objects. In an analogous fashion, we study the characteristic polynomial of Frobenius :

$$x^4 - a_1x^3 + a_2x^2 - pa_1x + p^2,$$

of a genus-2 curve, for which the normalized coefficients $(\tilde{a}_1, \tilde{a}_2)$ are the values of class functions of random elements in an underlying Sato-Tate group.

References

[1] D. A. Marcus, *Number fields*, Universitext, Springer, 2018.

This is a first introduction to number theory, covering prime decomposition, the Frobenius automorphism and Galois actions, and class and unit groups.

[2] J. H. Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer, 2009.

A classical reference to elliptic curves. In particular Chapter V treats elliptic curves over finite fields, begining with the number of rational points.

[3] J.-P. Serre, *Linear representations of finite groups*, GTM **42**, Springer, 1977.

Serre's book is a classical introduction to representation theory. Chapter 4 gives a preview of the generalization to compact Lie groups, subject of the Sato–Tate conjectures.

[4] L. Clozel, The Sato-Tate conjecture, in *Current developments in mathematics, 2006*, 1–34, Int. Press, Somerville, MA, 2006.

The original Sato–Tate conjecture for elliptic curves, is now a theorem. This article covers the approach(es) to its proof from an advanced perspective (beyond the scope of this school, but included here for completeness). The expository article of Mazur (below) gives a more intuitive approach to motivate the conjecture, and the experimentally driven work of Fité, Kedlaya and Sutherland explore the generalizations to higher dimensions.

[5] B. C. Mazur, Finding meaning in error terms, Bull. Amer. Math. Soc. **45**, no. 2, 185–228, 2008.

In this expository article, Mazur motivates the Sato–Tate conjecture as a probability distribution of an error term in number theory, and motivates the relation with L-functions and equidistribution.

[6] J.-P. Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, **11**, CRC Press, 2012.

Serre's book discusses the number of rational points $N_X(p)$, over a finite field $\mathbb{F}_p$, on a variety X defined by a system of polynomial equations over $\mathbb{Z}$. In particular, Chapter 3 concerns equidistribution properties of these quantities, given the conceptual framework under which one can generalize the Sato–Tate conjecture for elliptic curves.

[7] A. V. Sutherland, Sato–Tate distributions, in *Analytic methods in arithmetic geometry*, 197–248, Contemp. Math. Centre Rech. Math. Proc., **740**, Amer. Math. Soc., 2019. https://arxiv.org/abs/1604.01256

These are notes from a school, the Arizona Winter School, which treats the relations between Galois representations, L-functions, and the associated Mumford–Tate and Sato–Tate groups. It treats the subject from an explicit and computational perspective, in line with the next references which developped the computational and theoretical framework for classification of higher dimensional Sato-Tate groups (for $g = 2$ and $g = 3$).

[8] K. S. Kedlaya, Sato-Tate groups of genus 2 curves, in *Advances on superelliptic curves and their applications*, 117–136, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., **41**, 2015.

A first introduction to the generalization of the Sato-Tate conjectures to higher dimension (genus 2).

[9] F. Fité, K. S. Kedlaya, V. Rotger, and A. V. Sutherland, Sato-Tate distributions and Galois endomorphism modules in genus 2, Compos. Math. **148**, no. 5, 1390–1442, 2012.

A comprehensive classification of possible Sato–Tate groups arising for Jacobians of genus-2 curves, combining experimental and theoretical approaches to their investigation.

[10] F. Fité, K. S. Kedlaya, A. V. Sutherland, The Sato–Tate groups of abelian threefolds, arXiv, https://arxiv.org/abs/2106.13759, 2021.

This article concerns the classification of possible Sato–Tate groups of abelian threefolds.

[11] D. W. Bump, *Lie groups*, GTM **225**, Springer, 2013.

For a deeper understanding of Lie groups, this book of Bump is a definitive reference.

[12] N. M. Katz and P. C. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, **45**, Amer. Math. Soc., 1999.

To explore further, beyond the scope of this school, the book of Katz and Sarnak outlines the "philosophy" of the relation between random matrices (with respect to a Haar measure in a Lie group) and sequences of Frobenius eigenvalues (associated to a geometry variety or family of varieties).