Galois representations and Sato–Tate groups
CIMPA School
Effective Algebra and the LMFDB
Makerere University, Uganda, 13–24 January 2025

Character theory for genus 2 curves.

Notation and background. Let $C : y^2 + h(x)y = f(x)/\mathbb{Q}$ be a hyperelliptic curve of genus 2: $h(x)^2 + 4f(x)$ is a squarefree polynomial of degree 5 or 6. There exists an analogous construction of the Galois representation on the Jacobian $J = \mathrm{Jac}(C)$ of C, an abelian surface associated to C. In particular we construct the Tate module

$$T_\ell(J) = \varprojlim_n J[\ell^n] \cong \mathbb{Z}_\ell^4,$$

preserving the nondegenerate alternating Weil pairing

$$T_\ell(J) \times T_\ell(J) \longrightarrow T_\ell(\mathbb{G}_m) = \varprojlim_n \mu_{\ell^n} \cong \mathbb{Z}_\ell.$$

The characteristic polynomial of Frobenius on $T_\ell(J)$ is a monic integer *Weil* polynomial:

$$F_p(x) = x^4 - a_1x^3 + (a_2 + 2p)x^2 - a_1px + p^2,$$

such that if α_i is a root, $|\alpha_i| = \sqrt{p}$, and $\overline{\alpha}_i$ is also a root. We set $\gamma_i = \alpha_i + \overline{\alpha}_i$, and define the real Weil polynomial

$$G_p(x) = x^2 - a_1x + a_2 = (x - \gamma_1)(x - \gamma_2).$$

This gives a decomposition of the quartic extension $\mathbb{Z}[\pi] = \mathbb{Z}[x]/(F_p(x))$ into towers of quadratic extensions:

$$\mathbb{Z}[\pi] = \frac{\mathbb{Z}[\gamma][x]}{(x^2 - \gamma x + p)} \text{ over } \mathbb{Z}[\gamma] = \frac{\mathbb{Z}[y]}{(G_p(y))}.$$

---

1. The roots of $F_p(x)$ satisfy $|\alpha_i| = \sqrt{p}$, from which the real roots γ_i of $G_p(x)$ satisfy the bounds $|\gamma_i| \le 2\sqrt{p}$. Use these bounds on γ_i to establish the identities:

$$0 \le a_1^2 - 4a_2 \le 4p,\ \ 4p - 2a_1\sqrt{p} + a_2 \ge 0,\ \ 4p + 2a_1\sqrt{p} + a_2 \ge 0.$$

Point counting. The Frobenius characteristic polynomial is determined by the number of points of C over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$:

$$N_C(p) = |C(\mathbb{F}_p)| = p + 1 - a_1, \text{ and } N_C(p^2) = |C(\mathbb{F}_{p^2})| = p^2 + 1 - a_1^2 + 2a_2 + 4p.$$

With a model for J, we can also recover (a_1, a_2) from $N_p(C)$ and the group order $N_p(J) = |J(\mathbb{F}_p)|$:

$$N_C(p) = |C(\mathbb{F}_p)| = p + 1 - a_1, \text{ and } N_J(p) = |J(\mathbb{F}_p)| = (p+1)^2 - a_1(p+1) + a_2.$$

---

2. The numbers of points of C and J over all extensions $\mathbb{F}_{p^r}$ are determined by the expressions

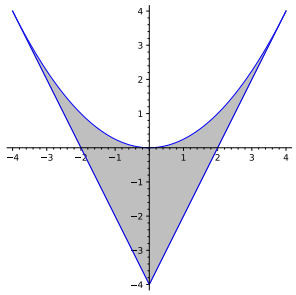
$$N_C(p^n) = |C(\mathbb{F}_{p^n})| = p^n + 1 - \mathrm{Tr}(\pi^n) \text{ and } N_J(p^n) = |J(\mathbb{F}_{p^n})| = \mathrm{N}(\pi^n - 1).$$

in the ring $\mathbb{Z}[\pi] = \mathbb{Z}[x]/(F_p(x))$. Determine the initial terms in the two sequences $(N_C(p^n))$ and $(N_J(p^n))$.

Frobenius distribution. The normalized Frobenius automorphism $\tilde{\phi}_p = \phi_p \otimes \frac{1}{\sqrt{p}}$ the satisfies the normalized Weil polynomial

$$\tilde{F}_p(x) = x^4 - \tilde{a}_1x^3 + (\tilde{a}_2 + 2)x^2 - \tilde{a}_1x + 1,$$

to which we associate a pair (ψ_1, ψ_2) of Galois characters on $\mathscr{G}_\mathbb{Q}$, taking values $(\tilde{a}_1, \tilde{a}_2)$. Under the map $\mathscr{P} \to \mathscr{G}_\mathbb{Q}$ sending p to any representative $\tilde{\phi}_p$ of its conjugacy class, we write $\psi_i(p)$ for its value $\tilde{a}_i$ at $\tilde{\phi}_p$. The Weil conjectures imply that $(\tilde{a}_1, \tilde{a}_2)$ lie in the region $\mathscr{R}$:



defined by the normalizations of the above bounds: $0 \le \tilde{a}_1^2 - 4\tilde{a}_2,\ \tilde{a}_2 - 2\tilde{a}_1 \ge -4,\ \tilde{a}_2 + 2\tilde{a}_1 \ge -4$.

The generalized Sato-Tate conjecture asserts that the polynomials $\tilde{F}_p(x)$, invariant of the conjugacy class of $\tilde{\phi}_p$, follows the distribution induced by the Haar measure on a compact Lie subgroup G of $\mathrm{USp}(4)$, the Sato-Tate group of C. Equivalently the pairs $(\psi_1(p), \psi_2(p)) = (\tilde{a}_1, \tilde{a}_2)$, are distributed over the above region with probability density dictated by G. In particular, with respect to the coordinates (s_1, s_2) (= (ψ_1, ψ_2)) the distribution functions for $\mathrm{USp}(4)$ are given on $\mathscr{R}$ by:

$$\frac{\sqrt{(s_1^2 - 4s_2)(4 - 2s_1 + s_2)(4 + 2s_1 + s_2)}}{4\pi^2}\, ds_1 ds_2,$$

for $\mathrm{SU}(2) \times \mathrm{SU}(2)$ by

$$\frac{\sqrt{(4 - 2s_1 + s_2)(4 + 2s_1 + s_2)}}{2\pi^2\sqrt{s_1^2 - 4s_2}}\, ds_1 ds_2,$$

and for $\mathrm{SO}(2) \times \mathrm{SO}(2)$, by

$$\frac{2 ds_1 ds_2}{\pi^2\sqrt{(s_1^2 - 4s_2)(4 - 2s_1 + s_2)(4 + 2s_1 + s_2)}}.$$

---

3. Numerical integration, with respect to the above probability measures for $\mathrm{USp}(4)$, $\mathrm{SU}(2) \times \mathrm{SU}(2)$ and $\mathrm{SO}(2) \times \mathrm{SO}(2)$, of the products $\psi_i \psi_j$, where ψ_i are the following virtual characters

$$(\psi_0, \psi_1, \psi_2, \psi_3) = (1, \psi_1, \psi_2, \psi_1^2 - \psi_2 - 2),$$

yields the respective inner product matrices $\langle \psi_i, \psi_j \rangle$:

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 4 \\ 2 & 0 & 4 & 12 \end{pmatrix}.$$

Give conjectural expressions for decomposition of these virtual characters in terms of irreducible characters on these groups.

4. Suppose that $G = \mathrm{SU}(2) \times \mathrm{SU}(2)$ or $G = \mathrm{SO}(2) \times \mathrm{SO}(2)$. Relate the virtual characters ψ_1 and ψ_2 to the pairs of fundamental characters (φ_1, φ_2) with respect to the projections to $\mathrm{SU}(2)$ or $\mathrm{SO}(2)$.

We can relate the theoretical Sato-Tate groups to the character theory of the Galois representations associated to genus-2 curves.

---

5. Identify the Sato-Tate group of the following genus-2 curves.

- $C_0 : y^2 + (x^3 + x + 1)y = -x^5$
- $C_1 : y^2 + (x^3 + x)y = x^4 - 7$
- $C_2 : y^2 + (x^3 + x)y = -1$
- $C_3 : y^2 + (x^3 + 1)y = x^4 + x^2$
- $C_4 : y^2 + y = x^5$
- $C_5 : y^2 + y = x^6$

Finally we consider the relation of the characters arising in genus-2 with characters on objects of lower dimension (elliptic curves and even number fields).

6. Identify which of the following elliptic curves are isogenous to quotients of one of the above genus-2 curves (that is, isogeny factors of their Jacobians).

   - $E_0 : y^2 + (x+1)y = x^3 - x$,
   - $E_1 : y^2 = x^3 - x^2 - 4$
   - $E_2 : y^2 = x^3 - x$
   - $E_3 : y^2 + xy = x^3 + x$
   - $E_4 : y^2 = x^3 + 4$
   - $E_5 : y^2 + y = x^3$

   Hint. First characterize the Sato-Tate groups as $\mathrm{SU}(2)$ or $\mathrm{N}(\mathrm{U}(1))$ in order to limit the possibilities, then compute the inner products with respect to the Frobenius trace character.

Next we can use the character theory of number fields to analyze the component group of an algebraic curve (or its Jacobian). We investigate the behavior of the twists of the Frobenius trace character when the component group is acted on by Galois group of a number field K.

7. Consider the dependency of the normalized Frobenius trace characters of the above genus-2 curves with respect to the quadratic characters on the Galois groups of the number fields $\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\sqrt{-3})$, or with respect to the characters on the Galois group of the cubic field $\mathbb{Q}[x]/(x^3-2)$. In particular, if $\chi_1, \ldots, \chi_t$ are the irreducible characters of (the Galois closure of) a number field K, and ψ_C the Frobenius trace character, then how do the inner product matrices $(\langle \chi_i, \chi_j \rangle)$ and $(\langle \psi\chi_i, \psi\chi_j \rangle) = (\langle \psi^2\chi_i, \chi_j \rangle)$ compare?