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

Character theory for elliptic curves.

The objective of these exercises is to give an introduction to the Galois representations attached to an elliptic curve $E/\mathbb{Q}$. We denote $\mathscr{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the *absolute* Galois group of $\mathbb{Q}$.

Notation and background. Associated to an elliptic curve $E/\mathbb{Q}$, we can associate its sequence of Frobenius traces (a_p), for $p \in \mathscr{P}$, such that

$$N_E(p) = |\overline{E}(\mathbb{F}_p)| = p + 1 - a_p,$$

satisfying the Hasse–Weil bound $|a_p| \leq 2\sqrt{p}$. We interpret the function

$$\psi_E(p) = \frac{p + 1 - N_E(p)}{\sqrt{p}} = \frac{a_p}{\sqrt{p}}$$

as a character on the absolute Galois group $\mathscr{G}_{\mathbb{Q}}$, which we call the normalized Frobenius trace character of E.

The action on the n-torsion subgroups

$$E[n] = \{P \in E(\overline{\mathbb{Q}}) \mid nP = O\} \cong (\mathbb{Z}/n\mathbb{Z})^2,$$

gives rise to a Galois representation on the n-torsion module:

$$\rho_{E,n} : \mathscr{G}_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

and, taking the limit, on the Tate module:

$$T(E) = \varprojlim_n E[n] \cong \prod_{\ell \in \mathscr{P}} T_\ell(E),$$

where

$$T_\ell(E) = \varprojlim_k E[\ell^k] \cong \varprojlim_k (\mathbb{Z}/\ell^k\mathbb{Z})^2 = \mathbb{Z}_\ell^2.$$

It follows that $T(E) \cong \hat{\mathbb{Z}}^2 \cong \prod_\ell \mathbb{Z}_\ell^2$, from which the isomorphism $\mathrm{Aut}(T(E)) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$ follows.

This gives a representation $\rho_E : \mathscr{G}_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T(E)) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$, such that for any lift ϕ_p of the Frobenius automorphism on $T(E)$, the characteristic polynomial of $\rho_E(\phi_p)$ is $x^2 - a_p x + p$, and in particular $a_p = \mathrm{Tr}(\rho_E(\phi_p))$. The action of the Frobenius lift coincides with the Frobenius endomorphism

$$\begin{aligned} \pi : \overline{E} &\longrightarrow \overline{E} \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

on the reduction $\overline{E}/\mathbb{F}_p$ of E to $\mathbb{F}_p$. In particular the subring $\mathbb{Z}[\pi] \subset \mathrm{End}(\overline{E})$ is isomorphic to $\mathbb{Z}[x]/(x^2 - a_p x + p)$ and a_p is an integer. This identifies the sequence (a_p) with an integer sequence of character values on the absolute Galois group.

---

1. Let $N_E(p^n) = |\overline{E}(\mathbb{F}_{p^n})|$. Show that $\overline{E}(\mathbb{F}_{p^n})$ is the set of fixed points of π^n and conclude that

$$\overline{E}(\mathbb{F}_{p^n}) = \ker(\pi^n - 1).$$

Conclude that $N_E(p^n) = \mathrm{N}(\pi^n - 1) = p^n + 1 - \mathrm{Tr}(\pi^n)$, where N and Tr are the norm and trace on the quadratic ring $\mathbb{Z}[\pi]$. Determine a recursion for the sequence $(t_n) = (\mathrm{Tr}(\pi^n))$.

In order to compare trace values at different primes, we construct the normalized sequence $(\tilde{a}_p) = (a_p/\sqrt{p})$, which takes values on a compact real Lie subgroup G, called the Sato-Tate group of E. We denote the underlying representation $\tilde{\rho}_E$. As above, for a character ψ we write $\psi(p)$ for the value at a Frobenius lift ϕ_p, and we can express the expectation of a character ψ on G (e.g. $\psi(p) = \tilde{a}_p$) as a limit over subsets $\mathscr{P}_N \subset \mathscr{P}$:

$$\mathbb{E}(\psi) = \lim_{N\to\infty} \frac{1}{N} \sum_{p\in\mathscr{P}_N} \psi(p).$$

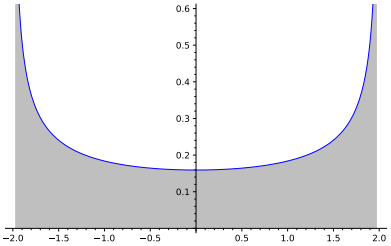
The orthogonality relations on irreducible characters ψ and χ on G takes the form

$$\langle \psi, \chi \rangle = \mathbb{E}(\psi\overline{\chi}) = \begin{cases} 1 & \text{if } \psi = \chi \\ 0 & \text{otherwise.} \end{cases}$$

Given two elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ the associated characters $\psi_E = \mathrm{Tr}\circ\tilde{\rho}_E$ and $\psi_{E'} = \mathrm{Tr}\circ\tilde{\rho}_{E'}$ are equal (up to a finite set up primes) if and only if E and E' are isogenous, and otherwise they are *independent*, defined by their orthogonality under the inner product on characters.

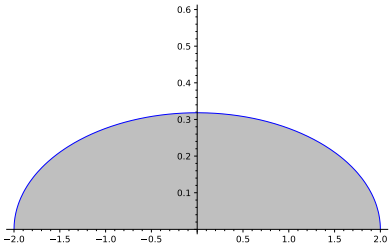
For an elliptic curve over $\mathbb{Q}$, the group G is either the special unitary group $\mathrm{SU}(2)$ or the normalizer in $\mathrm{SU}(2)$ of the subgroup $\mathrm{SO}(2)$, in which $\mathrm{SO}(2)$ is a connected component of index 2. The character values $(\tilde{a}_p)$ are equidistributed in the interval $[-2,2]$, in accordance with the probability distribution given by traces of Frobenius elements randomly distributed in G with respect to the Haar measure. The probability density functions for $\mathrm{SO}(2)$ and $\mathrm{SU}(2)$ are as follows.

$$\frac{1}{\pi\sqrt{4-t^2}}dt$$



SO(2)

$$\frac{\sqrt{4-t^2}}{2\pi}dt$$



SU(2)

N.B. To say that the normalized Frobenius traces follow the probability distibution $\mu(t) = f(t)dt$ means that the probability that a normalized trace $\tilde{a}_p$ falls in $I = [t_1, t_2]$ is:

$$P(\tilde{a}_p \in I) = \int_{t_1}^{t_2} \mu(t).$$

Naturally $\mu(t)$ being a probability distribution implies that $\displaystyle\int_{-2}^{2} \mu(t) = 1$.

---

2. Make the substitution $t = 2\cos(\theta)$. Find expressions for the probability distribution functions for $\mathrm{SU}(2)$ and for $\mathrm{SO}(2)$ in terms of $\theta \in [0,\pi]$. Note that $\cos(\theta) = \cos(-\theta)$, so that the trace (and conjugacy class)

$$\begin{array}{ccc} [0,\pi] & \longrightarrow & [-2,2] \\ \theta & \longmapsto & 2\cos(\theta) \end{array}$$

is a bijection. We refer to $[0,\pi]$ with its associated probability distribution the Frobenius angle space.

N.B. Showing that the trace sequence converges to such a probability density function is challenging, both graphically and numerically. A large amount of data is required to visually recognize the above curves. Instead we will use the orthogonality relations in terms of expectations of random sequences to identify discrete invariants of the underlying Sato-Tate groups.

CM elliptic curves. The Sato-Tate group of an elliptic curve with complex multiplication (CM) is much smaller than that of a generic elliptic curve, and can be explicitly constructed. Let $E/\mathbb{Q}$ have CM by $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ of discriminant D_K. The Frobenius automorphisms ϕ_p, apart from a finite number of p which ramify in $\mathrm{End}(E)$, split into two classes:

- If p is split in K, then ϕ_p is induced by lift to an endomorphism $\phi_p \in \mathrm{End}(E)$.
- If p is inert in K, then $\phi_p^2 = -p$ and the trace of Frobenius is 0.

Let $K \otimes \mathbb{R} \cong \mathbb{C} \cong \mathbb{R}^2$ be a fixed isomorphism. By the Chebotarev density theorem, each of the two cases represent half of the primes. In the first, case, the normalized Frobenius automorphisms

$$\tilde{\phi}_p = \phi_p \otimes \frac{1}{\sqrt{p}} \in K \otimes_{\mathbb{Q}} \mathbb{R}$$

form a sequence which is equidistributed along the unit circle

$$\mathrm{U}(1) = \{\mu \in \mathbb{C}^* : |\mu| = 1\} \cong \mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in [0, 2\pi] \right\}.$$

In the second case, the trace of $\tilde{\phi}_p$ is 0 and moreover $\tilde{\phi}_p^2 = -1$. These elements lie in the non-identity component of the normalizer $\mathrm{N}(\mathrm{SO}(2))$ of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$:

$$\mathrm{N}(\mathrm{SO}(2)) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \right\} \cup \left\{ i \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \right\} \subset \mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} : \alpha\overline{\alpha} + \beta\overline{\beta} = 1 \right\}.$$

This group admits quadratic character $\xi : \mathrm{N}(\mathrm{SO}(2))/\mathrm{SO}(2) \longrightarrow \{\pm 1\}$. Under the identification of $p \in \mathscr{P}$ with the normalized Frobenius $\tilde{\phi}_p$ at p, this character agrees with the Kronecker symbol

$$\xi(p) = \left(\frac{D_K}{p} \right).$$

This determines the partition of $\mathscr{P}$ into two sets $\xi^{-1}(1)$ and $\xi^{-1}(-1)$ of equal density such that $\tilde{a}_p$ follows the probability distribution $dt/\pi\sqrt{4-t^2}$ on $\xi^{-1}(1)$ and $\tilde{a}_p = 0$ on $\xi^{-1}(-1)$.

The subgroup $\mathrm{SO}(2)$ and its normalizer are diagonnalizable, by conjugation in $\mathrm{SU}(2)$, giving an isomorphism of $\mathrm{SO}(2)$ with the skew diagonal image of $\mathrm{U}(1)$ in $\mathrm{SU}(2)$:

$$\mathrm{SO}(2) \cong \mathrm{U}(1) \cong \left\{ \begin{pmatrix} \mu & 0 \\ 0 & \overline{\mu} \end{pmatrix} \;\middle|\; \mu\overline{\mu} = 1 \right\} \text{ and } \mathrm{N}(\mathrm{SO}(2)) \cong \mathrm{N}(\mathrm{U}(1)) = \left\{ \begin{pmatrix} \mu & 0 \\ 0 & \overline{\mu} \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & -\overline{\mu} \\ \mu & 0 \end{pmatrix} \right\}.$$

Under this isomorphism we give preference to the notation $\mathrm{N}(\mathrm{U}(1))$ for the Sato-Tate group.

---

3. Consider the elliptic curves $E_0 : y^2 + xy = x^3 - x^2 - 2x - 1$ and $E_1 : y^2 + y = x^3 - x^2 - 10x - 20$. Use the properties of the character ψ_E to identify the Sato-Tate group, $\mathrm{N}(\mathrm{U}(1))$ or $\mathrm{SU}(2)$, and conclude whether the curves are CM or not. **Hint.** Consider the character ξ and whether or not the Sato-Tate group has a component associated to $\tilde{a}_p = 0$.

Virtual character rings.

The virtual character ring $\mathfrak{R}(G)$ is an invariant ring of a compact Lie group G whose additive group is the free abelian group on irreducible complex-valued characters. A character on G is identified with a formal sum according to its decomposition (as a direct sum) into irreducible characters. Addition in $\mathfrak{R}(G)$ is thus the direct sum, and general elements are formal differences $\psi - \chi$ of characters. A multiplication operation is obtained from the tensor product, which is distributive over direct sums.

$\mathrm{SU}(2)$**.** The virtual character ring $\mathfrak{R}(\mathrm{SU}(2))$ is equal $\mathbb{Z}[\psi]$, generated as a module by the basis (ψ_n), where $\psi_n = S^n(\psi)$ denotes the n-th symmetric power character of degree $n+1$. These characters satisfy the relations

$$\psi\psi_{n-1} = \psi_n + \psi_{n-2}.$$

The recursion $\psi_n = \psi\psi_{n-1} - \psi_{n-2}$ allows one to compute the basis (ψ_n) such that $\mathbb{Z}[\psi] = \bigoplus_{n=0}^{\infty} \mathbb{Z}\psi_n$.

Begining from $\psi_0 = 1$ and $\psi_1 = \psi$, the first level of the recurrence is given by the decomposition

$$\psi^2 = S^2(\psi) \oplus \bigwedge^2(\psi) = \psi_2 + \psi_0.$$

If $\psi(p) = \alpha + \overline{\alpha}$, for normalized Frobenius eigenvalues α and $\overline{\alpha}$, with $\alpha\overline{\alpha} - 1$, the recursion gives

$$\psi_2(p) = \psi(p)^2 - 1 = \alpha^2 + 2\alpha\overline{\alpha} + \overline{\alpha}^2 - 1 = \alpha^2 + 1 + \overline{\alpha}^2.$$

The following exercise relates the (normalized) Frobenius eignenvalues to the irreducible characters on $\mathrm{SU}(2)$ and their recurrence relations.

---

4. Show that if $\psi(p) = \alpha + \overline{\alpha}$ on $\mathrm{SU}(2)$, then the n-th symmetric product $\psi_n = S^n(\psi)$ satisfies

$$\psi_n(p) = \sum_{k=0}^{n} \alpha^{n-k}\overline{\alpha}^k = \alpha^n + \alpha^{n-2} + \cdots + \overline{\alpha}^{n-2} + \overline{\alpha}^n.$$

$\mathrm{SO}(2)$. The character ring of the plane rotation group $\mathrm{SO}(2)$ is the group ring $\mathfrak{R}(\mathrm{SO}(2)) = \mathbb{Z}[\chi, \overline{\chi}]$, where χ is the linear character

$$\chi : \mathrm{SO}(2) \xrightarrow{\quad\cong\quad} \mathrm{U}(1) \subset \mathbb{C}^*,$$
$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \longmapsto \cos(\theta) + i\sin(\theta)$$

embedding $\mathrm{SO}(2)$ as the unit circle in $\mathbb{C}^*$, and $\chi\overline{\chi} = 1$. Being a linear character, χ is both a representation (group homomorphism) and a character. The degree-2, real-valued character $\tau = \chi + \overline{\chi}$ plays a role in the representation theory of elliptic curves, and gives a subring $\mathbb{Z}[\tau] \subset \mathfrak{R}(\mathrm{SO}(2))$ of real-valued characters.

---

5. Show that if $\tau(p) = \alpha + \overline{\alpha}$ on $\mathrm{SO}(2)$, with $\chi(p) = \alpha$, then for all $n > 0$, the sequence of real characters $\tau_n = \chi^n + \overline{\chi}^n$ satisfy
$$\tau_n(p) = \chi^n(p) + \overline{\chi}^n(p) = \alpha^n + \overline{\alpha}^n.$$
Conclude that the recurrence $\tau_n = \tau\tau_{n-1} - \tau_{n-2}$, identical to that of the symmetric sums ψ_n on $\mathrm{SU}(2)$, holds for the sequence (τ_n) on $\mathrm{SO}(2)$, begining with the initialization $\tau_0 = 2$ and $\tau_1 = \tau$.

$\mathrm{N}(\mathrm{U}(1))$. The rotation group $\mathrm{SO}(2)$ can be diagonalized over $\mathbb{C}$ by conjugation in $\mathrm{SU}(2)$:

$$\mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \right\} \cong \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \right\} = \left\{ \begin{pmatrix} \mu & 0 \\ 0 & \overline{\mu} \end{pmatrix} \;\middle|\; \mu\overline{\mu} = 1 \right\}.$$

This realizes $\mathrm{SO}(2)$ as conjugate to the skew diagonal embedding of the unitary group $\mathrm{U}(1) = \{\mu \mid \mu\overline{\mu} = 1\}$ in $\mathrm{SU}(2)$:

$$\mathrm{U}(1) \cong \left\{ \begin{pmatrix} \mu & 0 \\ 0 & \bar{\mu} \end{pmatrix} \;\middle|\; \mu\bar{\mu} = 1 \right\} \subset \mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \;\middle|\; \alpha\overline{\alpha} + \beta\overline{\beta} = 1 \right\}.$$

We write simply $\mathrm{U}(1)$ for this image in $\mathrm{SU}(2)$ and $\mathrm{N}(\mathrm{U}(1))$ for its normalizer. The normalizers of $\mathrm{U}(1)$ and $\mathrm{SO}(2)$ take the form:

$$\mathrm{N}(\mathrm{SO}(2)) = \left\langle \mathrm{SO}(2), \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle \cong \mathrm{N}(\mathrm{U}(1)) = \left\langle \mathrm{U}(1), \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} \mu & 0 \\ 0 & \bar{\mu} \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 0 & -\overline{\mu} \\ \mu & 0 \end{pmatrix} \right\}.$$

This realizes $\mathrm{N}(\mathrm{U}(1)) \cong \mathrm{N}(\mathrm{SO}(2)$ as the extension of $\{\pm 1\}$ by $\mathrm{U}(1)$:

$$1 \longrightarrow \mathrm{U}(1) \longrightarrow \mathrm{N}(\mathrm{U}(1)) \xrightarrow{\xi} \{\pm 1\} \longrightarrow 1.$$

This sequence is nonsplit since any element T of the coset $\mathrm{N}(\mathrm{U}(1))\backslash\mathrm{U}(1)$ satisfies $T^2 = -I \in \mathrm{SO}(2)$, hence T has order 4, so there can be no splitting of $\{\pm 1\}$ back to $\mathrm{N}(\mathrm{U}(1))$.

The character ring $\mathfrak{R}(\mathrm{N}(\mathrm{U}(1)))$ is generated by the restriction σ of ψ from $\mathfrak{R}(\mathrm{SU}(2))$ and the quadratic character ξ:

$$\mathfrak{R}(\mathrm{N}(\mathrm{U}(1))) = \frac{\mathbb{Z}[\sigma,\xi]}{(\xi^2-1,(\xi-1)\sigma)}.$$

Let $\sigma_0 = 1+\xi$, set $\sigma_1 = \sigma$, and define the sequence (σ_n) of virtual characters by the recursion

$$\sigma_n = \sigma\sigma_{n-1} - \sigma_{n-2}.$$

Then we obtain a module decomposition of the ring in terms of the basis $(1,\xi,\sigma_1,\sigma_2,\dots)$:

$$\mathfrak{R}(\mathrm{N}(\mathrm{U}(1))) = \mathbb{Z}[\sigma]\oplus\mathbb{Z}\xi = \mathbb{Z}\oplus\mathbb{Z}\xi\oplus\bigoplus_{n=1}^{\infty}\mathbb{Z}\sigma_n.$$

In the exercises below we explore the properties of this sequence.

---

6. Show that there exists a degree-2 character σ_2 on $\mathrm{N}(\mathrm{U}(1))$ such that $S^2(\sigma) = \sigma_2+\xi$ and $\bigwedge^2(\sigma) = 1$, giving the decomposition
$$\sigma^2 = \sigma_2 + 1 + \xi.$$
In particular, σ_2 is a character for $\mathrm{N}(\mathrm{U}(1))$.

   Hint. Let (e_1,e_2) be the basis of the representation of $\mathrm{N}(\mathrm{U}(1))$ on $\mathbb{C}^2$. The subgroup $\mathrm{U}(1)$ acts by transformations $(e_1,e_2)\longmapsto(\mu e_1,\overline{\mu}e_2)$ and elements on the coset $\mathrm{N}(\mathrm{U}(1))\backslash\mathrm{U}(1)$ give rise to the map
$$(e_1,e_2)\longmapsto(-\overline{\mu}e_2,\mu e_1).$$
Consider the action of $\mathrm{N}(\mathrm{U}(1))$ on the subspaces spanned by $\{e_1^2,e_2^2\}$, and by $\{e_1e_2\}$ in $S^2(\mathbb{C}^2)$, and in terms of the basis $\{e_1\wedge e_2\}$ for $\bigwedge^2(\mathbb{C}^2)$.

7. Show that for each $n\geq 0$, σ_n is a character and not just a virtual character.

   Hint. If σ_n is a virtual character, then there exists an irreducible character φ such that $\langle\sigma_n,\varphi\rangle = m < 0$. Consider the restriction of the characters to $\mathrm{U}(1)$ and to $\mathrm{N}(\mathrm{U}(1))\backslash\mathrm{U}(1)$.

8. Show that the degrees of the characters ψ_n on $\mathrm{SU}(2)$ are $\deg(\psi_n) = n+1$, but $\deg(\sigma_n) = 2$ for all $n\geq 0$. In particular $\mathrm{Res}(\psi_n)\neq\sigma_n$ except for $n=1$. Determine an expression for the restriction $\mathrm{Res}(\psi_n)\in\mathfrak{R}(\mathrm{N}(\mathrm{U}(1)))$ in the basis $(1,\xi,\sigma_n,\dots,\sigma_n)$.

9. Note that the recursion for τ_n is the homomorphic image of that for σ_n under restriction, however the module map $\mathfrak{R}(\mathrm{SO}(2))\to\mathfrak{R}(\mathrm{N}(\mathrm{U}(1)))$ sending the basis $(1,\tau_1,\tau_2,\dots)$ to $(1,\sigma_1,\sigma_2,\dots)$ is not a ring homomorphism since $\tau_n\in\mathbb{Z}[\tau] = \mathbb{Z}[\tau_1]\subset\mathfrak{R}(\mathrm{SO}(2))$ but for n even $\sigma_n\notin\mathbb{Z}[\sigma] = \mathbb{Z}[\sigma_1]$. In particular, show that the evaluation of (σ_n) at $\sigma = 0$ gives the sequence
$$(1+\xi,0,-1-\xi,0,1+\xi,0,-1-\xi,0,\dots),$$
whose restriction to $\mathrm{N}(\mathrm{U}(1)))\backslash\mathrm{U}(1)$ is the trivial sequence $(0,0,\dots)$.

10. Compute the inner product matrix $(\langle\sigma_i\sigma_j\rangle)$ for $0\leq i,j\leq n$, noting that it equals the mean of the inner product matrix $(\langle\tau_i,\tau_j\rangle)$ restricted to $\mathrm{SO}(2)\cong\mathrm{U}(1)$ and the zero matrix on $\mathrm{N}(\mathrm{U}(1))\backslash\mathrm{U}(1)$. Conclude that the inner product matrix with respect to $(1,\xi,\sigma_1,\sigma_2,\dots,\sigma_n)$ is the identity matrix and that the characters σ_n are irreducible for all $n\geq 1$.

Next we compute the polynomials T_n and U_n, which give polynomial expressions in ψ for the charactes ψ_n on the Lie groups $\mathrm{SO}(2)$ and $\mathrm{SU}(2)$, respectively. Up to rescaling to the interval $[-1,1]$, these are the classical Chebyshev polynomials.

---

11. Compute the initial terms of the polynomial sequence $(T_n(x))$ and $(U_n(x))$ in $\mathbb{Z}[x]$, such that the evaluations $T_n(\tau)$ and $U_n(\psi)$ give the characters τ_n on $\mathrm{SO}(2)$ and ψ_n on $\mathrm{SU}(2)$, respectively.

12. Show that the polynomial sequences satisfy the orthogonality relations

$$\int_{-2}^{2} \frac{T_m(t)T_n(t)}{\pi\sqrt{4-t^2}}dt = \begin{cases} 4 \text{ if } m=n=0, \\ 2\delta_{mn} \text{ otherwise} \end{cases} \quad \text{and} \quad \int_{-2}^{2} \frac{U_m(t)U_n(t)}{2\pi}\sqrt{4-t^2}\,dt = \delta_{mn},$$

where $\delta_{mn}=1$ if $m=n$ and $\delta_{mn}=0$ otherwise.

13. Determine an expression for U_n in terms of the basis T_n, and deduce rules for the decomposition of the restriction of ψ_n to $\mathrm{SO}(2) \subset \mathrm{SU}(2)$ in terms of the basis $(1, \tau_1, \ldots, \tau_n)$ for $\mathfrak{R}(\mathrm{SO}(2))$.

We can now relate the character theory for compact Lie groups in $\mathrm{SU}(2)$ to the characters of the Galois representation on elliptic curves.

---

14. Let E_0 be the CM curve $y^2+xy=x^3-x^2-2x-1$ of discriminant -7 and conductor 49. Compute the initial five terms of the sequence $(\tau_n)=(\chi^n+\overline{\chi}^n)$, as polynomials in the degree-2 character $\tau=\chi+\overline{\chi}=\psi_{E_0}$, and verify computationally that they satisfy the orthogonality relations.

15. Let E_1 be the curve $y^2+y=x^3-x^2-10x-20$ of conductor 11. Compute the initial five terms of the sequence $(\psi_n)=(S^n(\psi))$, as polynomials in the degree-2 character $\psi=\psi_{E_1}$, and verify computationally that they satisfy the orthogonality relations.

Conversely, the symmetric power characters $(S^n(\psi_E))$ on an CM curve E are neither irreducible for $n \geq 2$, nor orthogonal, as demonstrated in the next exercise.

---

16. On the curve E_0 compute the inner product matrix with respect to the sequence $(\psi_n)=(S^n(\psi))$ of symmetric power characters of $\psi=\psi_{E_1}$. Verify the consistency of the result with respect to the Sato-Tate group $\mathrm{N}(\mathrm{U}(1))$ and not $\mathrm{SU}(2)$, finding an explicit form for the inner product matrix.

Finally we can compare orthogonality relations between different elliptic curves, that is, of their respective irreducible Galois representations ψ_E. Moreover we can compare the inner products with respect to other characters $F(\psi_E)$ in $\mathbb{Z}[\psi_E]$, with a view to determining whether curves are isogenous to a twist of each other.

---

17. Let ψ_E denote the normalized Frobenius trace character on an elliptic curve E. Verify experimentally the independence of the characters ψ_{E_i} on E_i, namely $\mathbb{E}(\psi_{E_0}\psi_{E_1})=0$.

18. Consider the elliptic curve E_1 together with the curves of conductor 11^2:

$$\begin{aligned} E_2 &: y^2+xy+y=x^3+x^2-30x-76, & E_3 &: y^2+y=x^3-x^2-7x+10, \\ E_4 &: y^2+xy=x^3+x^2-2x-7, & E_5 &: y^2+y=x^3-x^2-40x-221. \end{aligned}$$

Compute the inner product matrices with respect to ψ_{E_i} and $\psi_{E_i}^2-1$, for the curves E_1, E_2, E_3, E_4, E_5. What information does this reveal about the curves?

19. Consider the elliptic curve E_0 together with the curves of conductor $2^4\,7^2$:

$$\begin{aligned} E_6 &: y^2=x^3+x^2-16x-29, & E_7 &: y^2=x^3-343x+2401, \\ E_8 &: y^2=x^3+49x+686, & E_9 &: y^2=x^3-x^2-800x+8359, \\ E_{10} &: y^2=x^3-x^2-16x-1392, & E_{11} &: y^2=x^3-7x-7, \\ E_{12} &: y^2=x^3-x^2-114x+127, & E_{13} &: y^2=x^3-35x+98, \\ E_{14} &: y^2=x^3+x^2-2x-1, & E_{15} &: y^2=x^3+x^2-408x+6292. \end{aligned}$$

Compute the inner product matrices with respect to ψ_{E_i} and $\psi_{E_i}^2-1$, for the curves E_0, and $E_6, \ldots, E_{15}$. What information does this reveal about the curves?
