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 $|a_p| \le 2\sqrt{p}$. 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

$$\begin{tikzcd} \pi : \overline{E} \arrow[r] & \overline{E} \\ (x,y) \arrow[r, mapsto] & (x^p, y^p) \end{tikzcd}$$

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 $(t_n) = (\mathrm{Tr}(\pi^n))$.

The interprettation in terms of fixed points follows from $(x^{p^n}, y^{p^n}) = (x,y)$ if and only if $x,y \in \mathbb{F}_{p^r}$, after which the equality $\overline{E}(\mathbb{F}_{p^n}) = \ker(\pi^n - 1)$ holds. Since the norm $\mathrm{N}(\pi^n - 1)$ agrees with the degree of the morphism $\pi^n - 1$, and since $\pi^n - 1$ is separable, we have the equality $N_E(p^r) = \mathrm{N}(\pi^r - 1)$. Moreover,

$$\mathrm{N}(\pi^n - 1) = (\pi^r - 1)(\hat{\pi}^r - 1) = p^r - \mathrm{Tr}(\pi^r) + 1.$$

A recursion for $(t_n) = (\mathrm{Tr}(\pi^n))$ follows from the identity

$$\mathrm{Tr}(\pi^{n+1}) - t_1\,\mathrm{Tr}(\pi^n) + p\,\mathrm{Tr}(pi^{n-1}) = \mathrm{Tr}((\pi^2 - t_1\,\pi + p)\pi^{n-1}) = 0$$

which gives the recurrence relation $t_{n+1} - t_1 t_n + p\,t_{n-1} = 0$.

We can construct the first terms of the sequence, as polynomials in $t = t_1$ in Sage.

```
FF.<t,p> = PolynomialRing(ZZ,2)
tr = [2,t]
for i in range(8):
    tr.append(t*tr[i+1] - p*tr[i])
print(tr)
```

which gives the following initial list of Frobenius traces in terms of $t = \mathrm{Tr}(\pi) = a_p$.

```
[2,
 t,
 t^2 - 2*p,
 t^3 - 3*t*p,
 t^4 - 4*t^2*p + 2*p^2,
 t^5 - 5*t^3*p + 5*t*p^2,
 t^6 - 6*t^4*p + 9*t^2*p^2 - 2*p^3,
 t^7 - 7*t^5*p + 14*t^3*p^2 - 7*t*p^3,
 t^8 - 8*t^6*p + 20*t^4*p^2 - 16*t^2*p^3 + 2*p^4,
 t^9 - 9*t^7*p + 27*t^5*p^2 - 30*t^3*p^3 + 9*t*p^4]
```

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 $\mathscr{P}_N \subset \mathscr{P}$:

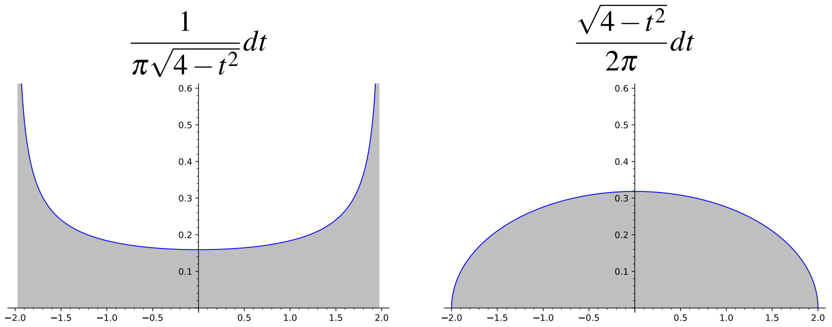
$$\mathbb{E}(\psi) = \lim_{N \to \infty} \frac{1}{N} \sum_{p \in \mathscr{P}_N} \psi(p).$$

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.



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

SO(2) 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:

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

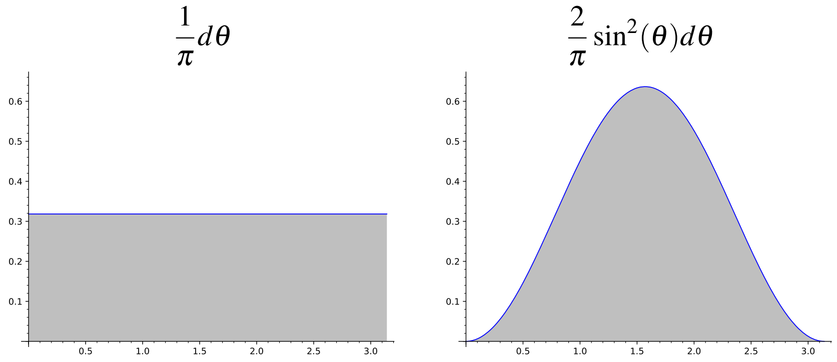
Naturally $\mu(t)$ being a probability distribution implies that $\int_{-2}^{2} \mu(t) = 1$.

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

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

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

The probability distribution functions in the Frobenius angle space are as follows:



$\frac{1}{\pi}d\theta$ $\frac{2}{\pi}\sin^2(\theta)d\theta$

SO(2) SU(2)

In particular, in the CM case, the Frobenius elements $\phi_p = \sqrt{p}e^{i\theta} \in K \subset \mathbb{C}$, have uniformly distributed arguments θ, while for a generic curve $E/\mathbb{Q}$ the Frobenius angles follow a $\sin(\theta)^2$ distribution.

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 $\tilde{a}_p = 0$.

It suffices to compute the density of primes such that $\psi_E(p) = \tilde{a}_p = 0$ (if and only if $\xi(p) = -1$ on $\mathrm{N}(\mathrm{U}(1))$ or, for $\mathrm{SU}(2)$, if the reduction is supersingular):

$$\mathbb{E}(\xi) = \lim_{N \to \infty} \frac{1}{N} \Bigg(\sum_{\substack{p \in \mathscr{P}_N \\ a_p \neq 0}} 1 - \sum_{\substack{p \in \mathscr{P}_N \\ a_p = 0}} 1 \Bigg) = \begin{cases} 1 \text{ if } \xi = 1, \\ 0 \text{ if } \xi \neq 1. \end{cases}$$

This sum converges to 1 for the generic Sato-Tate group $\mathrm{SU}(2)$, for which $\xi = 1$, or 0 for the CM case, Sato-Tate group $\mathrm{N}(\mathrm{U}(1))$. In order to compute these values experimentally, we create the curve in `Sage`.

```
E0 = EllipticCurve([1,-1,0,-2,-1])
E1 = EllipticCurve([0,-1,1,-10,-20])
```

Then we define a function which computes the mean value of $\xi(p)$ over the first primes.

```
def xi_trace_zero_expectation(E,max_prime):
   D = ZZ(E.discriminant())
   N,e = (0,0)
   for p in primes(max_prime):
       if D.mod(p) == 0: continue
       Ep = E.base_extend(FiniteField(p))
       ap = Ep.trace_of_frobenius()
       if ap != 0: e += 1
       if ap == 0: e -= 1
       N += 1
   return RR(e)/N
```

We obtain the following approximations to multiplicative character values for $a_p = 0$:

```
sage: xi_trace_zero_expectation(E0,2^12)
-0.0195381882770870
sage: xi_trace_zero_expectation(E1,2^12)
0.960923623445826
```

We note that the value for the generic curve E_1 is not exactly 1 because at certain primes p (of lower order of magnitude) give supersingular reduction.

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.

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 SU(2) and their recurrence relations.

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

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

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

$$\chi : \mathrm{SO}(2) \xrightarrow{\cong} \mathrm{U}(1) \subset \mathbb{C}^*,$$

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \longmapsto \cos(\theta) + i\sin(\theta)$$

embedding 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 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 SU(2), holds for the sequence (τ_n) on SO(2), begining with the initialization $\tau_0 = 2$ and $\tau_1 = \tau$.

N(U(1)). The rotation group SO(2) can be diagonalized over $\mathbb{C}$ by conjugation in 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 SO(2) as conjugate to the skew diagonal embedding of the unitary group $\mathrm{U}(1) = \{\mu \mid \mu\overline{\mu} = 1\}$ in 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 U(1) for this image in SU(2) and N(U(1)) for its normalizer. The normalizers of U(1) and 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 N(U(1)) $\cong$ N(SO(2) as the extension of $\{\pm 1\}$ by 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 N(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.

Remark. The relation of N(U(1)) to the orthogonal group O(2) is not formally needed, but we include additional details here as a remark. The inclusion SO$(2) \subset$ O(2) gives a restriction map

$$\mathfrak{R}(\mathrm{O}(2)) \longrightarrow \mathfrak{R}(\mathrm{SO}(2)),$$

whose image is the subring of real-valued characters $\mathbb{Z}[\tau] \subset \mathbb{Z}[\chi, \overline{\chi}]$, where $\tau = \chi + \overline{\chi}$ is the degree-2 real character obtained from the embedding in $\mathrm{GL}_2(\mathbb{R})$. Denote ω the trace character of $\mathrm{O}(2) \subset \mathrm{GL}_2(\mathbb{R})$ and let $\xi = \det : \mathrm{O}(2) \longmapsto \{\pm 1\}$ the the determinant character on $\mathrm{O}(2)$ with kernel $\mathrm{SO}(2)$. This gives the ring structure:

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

The restriction map $\mathrm{Res} : \mathfrak{R}(\mathrm{O}(2)) \longrightarrow \mathfrak{R}(\mathrm{SO}(2))$ has kernel ideal $(\xi - 1)$ and $\mathrm{Res}(\omega) = \tau = \chi + \overline{\chi}$ (coming from $\mathrm{SO}(2) \subset \mathrm{O}(2) \subset \mathrm{GL}_2(\mathbb{R})$).

N.B. The character ω is uniformly zero on the coset $\mathrm{O}(2) \backslash \mathrm{SO}(2)$, since the trace of a reflection is 0. As a ring, $\mathfrak{R}(\mathrm{O}(2))$ is generated by ω and ξ. As a module it is generated by irreducible characters 1, ξ and ω_n for $n \geq 1$:

$$\mathfrak{R}(\mathrm{O}(2)) = \mathbb{Z}[\omega] \oplus \mathbb{Z}\xi = \mathbb{Z} \oplus \mathbb{Z}\xi \oplus \bigoplus_{n=1}^{\infty} \mathbb{Z}\omega_n,$$

where $\omega_n = \mathrm{Ind}(\chi^n)$ are the characters on $\mathrm{O}(2)$ induced by χ^n on $\mathrm{SO}(2)$, whose restrictions are the real-valued characters $\mathrm{Res}(\omega_n) = \tau_n = \chi^n + \overline{\chi}^n$ on $\mathrm{SO}(2)$. For $n = 0$, the character $\omega_0 = 1 + \xi$ is reducible, and for even n, the characters ω_n are not in the subring $\mathbb{Z}[\omega]$.

We can now identify the $\mathrm{O}(2)$ as the quotient by the double cover $\pi : \mathrm{N}(\mathrm{U}(1)) \to \mathrm{O}(2)$, determined as a factor of the restriction of the symmetric square $S^2 : \mathrm{SU}(2) \to \mathrm{SO}(3)$, with kernel $\{\pm 1\}$.

$$\begin{tikzcd}
1 \arrow[r] & \{\pm 1\} \arrow[r] & \mathrm{SU}(2) \arrow[r, "S^2"] & \mathrm{SO}(3) \arrow[r] & 1 \\
1 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[u, equal] & \mathrm{N}(\mathrm{U}(1)) \arrow[r, "\pi"] \arrow[u, hook] & \mathrm{O}(2) \arrow[r] \arrow[u, hook, "\mathrm{id} \oplus \xi"'] & 1 \\
1 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[u, equal] & \mathrm{SO}(2) \arrow[r, "{[2]}"] \arrow[u, hook] & \mathrm{SO}(2) \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

In particular, the restriction of π to $\mathrm{SO}(2)$ gives the squaring morphism $[2] : \mathrm{SO}(2) \to \mathrm{SO}(2)$, such that $[2]^*(\tau_n) = \tau_{2n}$ for all $n \geq 1$. Moreover, $\pi^*(\xi) = \xi$ and $\pi^*(\omega_n) = \sigma_{2n}$ for all $n \geq 1$.

We note that the recurrence relation

$$\sigma \sigma_n = \sigma_{n+1} + \sigma_{n-1} \in \mathfrak{R}(\mathrm{N}(\mathrm{U}(1))),$$

together with the relation $\sigma_0 \sigma_n = 2\sigma_n$ (which follows from the identity $\xi \sigma_n = \sigma_n$), implies that

$$\sigma_2 \sigma_{2n} = \sigma_{2(n+1)} + \sigma_{2(n-1)}.$$

This in turn implies the recurrence relation

$$\omega \omega_n = \omega_{n+1} + \omega_{n-1} \in \mathfrak{R}(\mathrm{O}(2)).$$

It follows that the morphism π^* gives an isomorphism with the subring:

$$\mathfrak{R}(\mathrm{O}(2)) = \frac{\mathbb{Z}[\omega, \xi]}{(\xi^2 - 1, (\xi - 1)\omega)} \xrightarrow{\cong} \frac{\mathbb{Z}[\sigma_2, \xi]}{(\xi^2 - 1, (\xi - 1)\sigma_2)} \subset \mathfrak{R}(\mathrm{N}(\mathrm{U}(1))).$$

---

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 $\{e_1 e_2\}$ 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 $\sigma_n \not\in \mathbb{Z}[\sigma] = \mathbb{Z}[\sigma_1]$. 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 $(1, \tau_1, \dots, \tau_n)$ for $\mathfrak{R}(\mathrm{SO}(2))$.

A simple Sage function provides the recursive construction of the sequence of irreducible characters.

```
def symmetric_power_recursion(psi0,psi1,n):
    chars = [psi0,psi1]
    for i in range(1,n):
        chars.append(psi1*chars[i]-chars[i-1])
    return chars
```

The recursion gives polynomial expression for the initial irreducible characters in terms of $x = \psi$. Setting $x = 2$, the value of $\psi(1)$, we obtain the sequence $(\psi_n(1)) = (1, 2, 3, 4, \dots)$ of degrees of the symmetric power representations (beginning with $n = 0$).

```
sage: PZ.<x> = ZZ[x]
sage: chars = symmetric_power_recursion(PZ(1),x,6); chars
[1, x, x^2 - 1, x^3 - 2*x, x^4 - 3*x^2 + 1, x^5 - 4*x^3 + 3*x]
sage: [chi(x=2) for chi in chars]
[1, 2, 3, 4, 5, 6]
```

The same recurrence beginning with $(2, x)$ gives the polynomial expressions for the irreducible characters on $\mathrm{N}(\mathrm{U}(1))$, which are all of degree 2.

```
sage: PZ.<x> = ZZ[x]
sage: chars = symmetric_power_recursion(PZ(2),x,6); chars
[2, x, x^2 - 2, x^3 - 3*x, x^4 - 4*x^2 + 2, x^5 - 5*x^3 + 5*x]
sage: [chi(x=2) for chi in chars]
[2, 2, 2, 2, 2, 2]
```

From the initial conditions $U_1(x) = T_1(x)$ and $U_2(x) = T_2(x) + 1$, we deduce the equalities:

$$U_{2n+1}(x) = T_{2n+1}(x) + \cdots + T_3(x) + T_1(x) \text{ and } U_{2n}(x) = T_{2n}(x) + \cdots + T_2(x) + 1.$$

This implies that $\mathrm{Res}(\psi_{2n+1}) = \tau_{2n+1} + \cdots + \tau_1$ and $\mathrm{Res}(\psi_{2n}) = \tau_{2n} + \cdots + \tau_2 + 1$

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.

First we initialize the elliptic curves E_0 and E_1.

```
E0 = EllipticCurve([1,-1,0,-2,-1])
E1 = EllipticCurve([0,-1,1,-10,-20])
```

Then we code the inner product matrix of orthogonal characters on an elliptic curve as an expectation (to given precision and number of primes).

```
def elliptic_chars_matrix(E,num_chars,SatoTate="SU2",max_prime=2^12,prec=32):
    # Given an elliptic curve E/Q, and a number n = num_chars of irreducible
    # characters, compute the nxn inner product matrix with respect to the
    # first n irreducible characters for the Sato-Tate group "SU2" or "NU1".
    RR = RealField(prec); n = num_chars
    MatRR = MatrixSpace(RR,n,n); A = MatRR(0)
    D = E.discriminant(); bad_primes = D.numerator() * D.denominator()
    # Initialize psi0 for recursion:
    match SatoTate:
        case "SU(2)":
            psi0 = 1
        case "NU(1)":
            psi0 = 2
        case _:
          assert False, "SatoTate must SU(2) or NU(1)"
    num = 0
    for p in primes(max_prime):
        if bad_primes.mod(p) == 0: continue
        Ep = E.base_extend(GF(p))
        ap = Ep.trace_of_frobenius()
        if SatoTate == "NU(1)":
           if ap != 0:
               # U(1):
               chars = symmetric_power_recursion(psi0,ap/RR(p).sqrt(),n-1)
               chars = [1,1] + chars[1:]
           else:
               # N(U(1))\U(1):
               chars = [1,-1] + [0 for i in range(n-2)]
        else:
           chars = symmetric_power_recursion(psi0,ap/RR(p).sqrt(),n)
        A += MatRR([[chars[i]*chars[j] for j in range(n)] for i in range(n)])
        num += 1
    return 1/num*A
```

We verify that the expectation for the inner product matrix of characters on $\mathrm{SU}(2)$ is a close approximation of the identity for the elliptic curve E_1:

```
# E1: Generic elliptic curve of conductor 11:
A1 = elliptic_chars_matrix(E1,5)
print("Inner product matrix of SU(2) irreducible characters for E1:\n%s" % A1)
print("Approximating:")
print(matrix([ [ round(A0[i,j]) for j in range(5) ] for i in range(5) ]))
```

```
Inner product matrix of SU(2) irreducible characters for E1:
[   1.00000000 0.00480343155 -0.0331592300 0.00885968073 -0.0205551784]
[0.00480343155   0.966840769  0.0136631124 -0.0537144082  0.0205506508]
[-0.0331592300  0.0136631124   0.946285593  0.0253540824 -0.0257573944]
[0.00885968073 -0.0537144082  0.0253540824   0.974242606 -0.0336468926]
[-0.0205551784  0.0205506508 -0.0257573944 -0.0336468926    1.00271966]
Approximating:
[1 0 0 0 0]
[0 1 0 0 0]
[0 0 1 0 0]
[0 0 0 1 0]
[0 0 0 0 1]
```

This suggestss that the Sato-Tate group is indeed $\mathrm{SU}(2)$. A similar computation for the elliptic curve E_0, with respect to the irreducible characters for the group $N(U(1))$:

```
# E0: CM elliptic curve of discriminant -7 and conductor 49
A0 = elliptic_chars_matrix(E0,5,SatoTate="NU(1)")
print("Inner product matrix of N(U(1)) irreducible characters for E0:\n%s" % A0)
print("Approximating:")
print(matrix([ [ round(A0[i,j]) for j in range(5) ] for i in range(5) ]))
```

closely approximates the identity:

```
Inner product matrix of N(U(1)) irreducible characters for E0:
[   1.00000000 -0.0195381883  0.0182177321 -0.0246144382 -0.0375056680]
[-0.0195381883    1.00000000  0.0182177321 -0.0246144382 -0.0375056680]
[ 0.0182177321  0.0182177321   0.955847373 -0.0192879360 -0.0331171787]
[-0.0246144382 -0.0246144382 -0.0192879360   0.971959071  0.0136752048]
[-0.0375056680 -0.0375056680 -0.0331171787  0.0136752048   0.960608465]
Approximating:
[1 0 0 0 0]
[0 1 0 0 0]
[0 0 1 0 0]
[0 0 0 1 0]
[0 0 0 0 1]
```

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.

Under the hypothesis that the Sato-Tate group of E_0 is $\mathrm{SU}(2)$, we would use the symmetric power characters ψ_n on $\mathrm{SU}(2)$ (as hypothetically irreducible characters):

```
# E0: CM elliptic curve of discriminant -7 and conductor 49
B0 = elliptic_chars_matrix(E0,5)
print("Inner product matrix of SU(2) irreducible characters for E0:\n%s" % B0)
print("Approximating:")
print(matrix([ [ round(B0[i,j]) for j in range(5) ] for i in range(5) ]))
```

which gives the resulting matrix:

```
Inner product matrix of SU(2) irreducible characters for E0:
[    1.00000000   0.0182177321  -0.0441526265  -0.0192879360    0.966882823]
[  0.0182177321    0.955847373 -0.00107020386    0.922730194  -0.0431183992]
[ -0.0441526265 -0.00107020386     1.92273019  -0.0249006672    0.850221481]
[ -0.0192879360    0.922730194  -0.0249006672     1.85022148  -0.0995085278]
[   0.966882823  -0.0431183992    0.850221481  -0.0995085278     2.77947989]
Approximating:
[1 0 0 0 1]
[0 1 0 1 0]
[0 0 2 0 1]
[0 1 0 2 0]
[1 0 1 0 3]
```

approximating the integer matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 & 3 \end{pmatrix}.$$

We can express the restriction of the characters ψ_n on $\mathrm{SU}(2)$ to $\mathrm{N}(\mathrm{U}(1))$ and subsequently to its connected component $\mathrm{U}(1) \cong \mathrm{SO}(2)$ and to its coset $\mathrm{N}(\mathrm{U}(1))\backslash\mathrm{U}(1)$, via the evaluation $\sigma = 0$.

$\mathrm{SU}(2)$	$\mathrm{N}(\mathrm{U}(1))$	$\mathrm{SO}(2)$	$\mathrm{N}(\mathrm{U}(1))\backslash\mathrm{U}(1)$
ψ_0	1	1	1
ψ_1	$\sigma = \sigma_1$	τ_1	0
ψ_2	$\sigma^2 - 1 = \sigma_2 + \xi$	$\tau_2 + 1$	-1
ψ_3	$\sigma_3 + \sigma_1$	$\tau_3 + \tau_1$	0
ψ_4	$\sigma_4 + \sigma_2 + 1$	$\tau_4 + \tau_2 + 1$	1

Given the inner products $\langle \tau_i, \tau_j \rangle = 2\delta_{ij}$, on $\mathrm{SO}(2)$, we can express the inner product matrix on $\mathrm{N}(\mathrm{U}(1))$ as the mean of the inner product matrices on each of the two cosets $\mathrm{U}(1) \cong \mathrm{SO}(2)$ and $\mathrm{N}(\mathrm{U}(1))\backslash\mathrm{U}(1)$:

$$\frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 3 & 0 & 3 \\ 0 & 2 & 0 & 4 & 0 \\ 1 & 0 & 3 & 0 & 5 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 \end{pmatrix}.$$

This average over the two cosets explains the empirically computed matrix above.

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:

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

    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 $2^4\,7^2$:

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

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

We define a Sage function for the inner product of characters:

```
def elliptic_inner_product(E0,E1,F=None,max_prime=2^12,prec=32):
    # Given elliptic curves E0/Q and E1/Q, and F = F(x), compute
    # the expectation of F(psi_E0)*F(psi_E1), over primes up to
    # the bound max_prime.
    RR = RealField(prec)
    D0 = E0.discriminant(); bad_primes0 = D0.numerator() * D0.denominator()
    D1 = E1.discriminant(); bad_primes1 = D1.numerator() * D1.denominator()
    if F is None: F = var(’x’)
    S,num = (0,0)
    for p in primes(max_prime):
        if bad_primes0.mod(p) == 0: continue
        if bad_primes1.mod(p) == 0: continue
        FF = FiniteField(p)
        Ep0 = E0.base_extend(FF)
        ap0 = E0p.trace_of_frobenius()/RR(p).sqrt()
        Ep1 = E1.base_extend(FF)
        ap1 = E1p.trace_of_frobenius()/RR(p).sqrt()
        S += RR(F(x=ap0)*F(x=ap1))
        num += 1
    return S/num
```

And use this to compute the inner product matrix of a sequence of elliptic curves:

```
def elliptic_inner_product_matrix(EE,max_prime=2^12,prec=32):
    n = len(EE)
    C = MatrixSpace(RealField(prec),n,n)(0)
    for i in range(n):
        C[i,i] = elliptic_inner_product(EE[i],EE[i])
        for j in range(i+1,n):
            C[i,j] = elliptic_inner_product(EE[i],EE[j]); C[j,i] = C[i,j]
    return C
```

We now compute the inner product matrix for the two Frobenius trace characters:

```
EE = [E0,E1]
C0 = elliptic_inner_product_matrix(EE)
print("Inner product matrix of Frobenius trace characters for E0 and E1:\n%s" % C0)
```

This gives an approximation to the identity matrix:

```
Inner product matrix of Frobenius trace characters for E0 and E1:
[   0.955847373 -0.0709614164]
[-0.0709614164    0.966840769]
```

showing that ψ_{E_0} and ψ_{E_1} are orthogonal (hence not isogenous).

We set up the sequence of elliptic curves $(E_1,\ldots,E_5)$:

```
E2,E3,E4,E5 = [
    EllipticCurve([ 1, 1, 1, -30, -76 ]),
    EllipticCurve([ 0, -1, 1, -7, 10 ]),
    EllipticCurve([ 1, 1, 0, -2, -7 ]),
    EllipticCurve([ 0, -1, 1, -40, -221 ]) ]
EE = [E1,E2,E3,E4,E5]
```

The inner product matrix for ψ_E on elliptic curves $(E_1,E_2,\ldots,E_5)$

```
C1 = elliptic_inner_product_matrix(EE)
print("Inner product matrix of Frobenius trace characters for curves E_1,...,E_5:\n%s" % C
```

is (empirically) the identity matrix:

```
Inner product matrix of Frobenius trace characters for curves E_1,...,E_5:
[   0.966840769 -0.0219430888 -0.0233377450 -0.0306092552 -0.0343138510]
[-0.0219430888    0.977411554 -0.0132096764 -0.0495865242 -0.0306092552]
[-0.0233377450 -0.0132096764    0.956891850 -0.0132096764 -0.0233377450]
[-0.0306092552 -0.0495865242 -0.0132096764    0.977411554 -0.0219430888]
[-0.0343138510 -0.0306092552 -0.0233377450 -0.0219430888    0.966840769]
```

which suggests they are not isogenous over $\mathbb{Q}$. However, with respect to the character $\psi_E^2 - 1$:

```
C2 = elliptic_inner_product_matrix(EE,x^2-1)
print("Inner product matrix of character psi_2 = psi^2 - 1 on curves E_1,...,E_5:\n%s" % C
```

we find the inner product matrix:

```
Inner product matrix of character psi_2 = psi^2 - 1 on curves E_1,...,E_5:
[   0.946285593  0.0158882574 -0.0431622908  0.0158882574    0.946285593]
[ 0.0158882574    0.977365384 -0.0670398756    0.977365384  0.0158882574]
[-0.0431622908 -0.0670398756     1.92212554 -0.0670398756 -0.0431622908]
[ 0.0158882574    0.977365384 -0.0670398756    0.977365384  0.0158882574]
[   0.946285593  0.0158882574 -0.0431622908  0.0158882574    0.946285593]
```

which approximates the matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

This suggests that the pairs (E_1,E_5) and (E_2,E_4) are isogenous over some quadratic extension (potentially different for each pair), and, since $\psi_{E_3}^2 - 1$ is reducible, that E_3 is a CM curve.

Setting up the list of elliptic curves $(E_0,E_6,\ldots,E_{15})$:

```
EE = [E0] + [
    EllipticCurve([ 0, 1, 0, -16, -29 ]),
    EllipticCurve([ 0, 0, 0, -343, 2401 ]),
    EllipticCurve([ 0, 0, 0, 49, 686 ]),
    EllipticCurve([ 0, -1, 0, -800, 8359 ]),
    EllipticCurve([ 0, -1, 0, -16, -1392 ]),
    EllipticCurve([ 0, 0, 0, -7, -7 ]),
    EllipticCurve([ 0, -1, 0, -114, 127 ]),
    EllipticCurve([ 0, 0, 0, -35, 98 ]),
    EllipticCurve([ 0, 1, 0, -2, -1 ]),
    EllipticCurve([ 0, 1, 0, -408, 6292 ]) ]
```

we find that the curves are pairwise non isogenous (orthogonal ψ_{E_i}):

```
C3 = elliptic_inner_product_matrix(EE)
assert matrix([[round(C3[i,j]) for j in range(11)] for i in range(11)]) == 1
```

but the inner product matrix for $\psi_{E_i}^2 - 1$:

```
C4 = elliptic_inner_product_matrix(EE,x^2-1)
matrix([[round(C4[i,j]) for j in range(11)] for i in range(11)])
```

reveals certain geometrically isogenous pairs:

$$\begin{pmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$