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:

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

All three identities follow from the inclusion $\gamma_i \in [-2\sqrt{p}, 2\sqrt{p}]$. The first of the identities is the discriminant of the polynomial $G_p(x)$, and the second concerns the positivity of $G_p(x)$ outside of $(\gamma_1, \gamma_2) \subseteq (-2\sqrt{p}, 2\sqrt{p})$.

- $0 \le \mathrm{disc}(G_p(x)) = a_1^2 - 4a_2 = (\gamma_1 - \gamma_2)^2 \le 4p$.
- $-2\sqrt{p} - \gamma_i \le 0 \le 2\sqrt{p} + \gamma_i$, from which we obtain the two bounds:

$$\begin{aligned} G_p(+2\sqrt{p}) &= (+2\sqrt{p} - \gamma_1)(+2\sqrt{p} - \gamma_2) = 4p - 2a_1\sqrt{p} + a_2 \ge 0, \\ G_p(-2\sqrt{p}) &= (-2\sqrt{p} - \gamma_1)(-2\sqrt{p} - \gamma_2) = 4p + 2a_1\sqrt{p} + a_2 \ge 0. \end{aligned}$$

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 $(N_J(p^n))$.

We can create the formal ring $\mathbb{Z}[a_1,a_2,p][\pi]$ in Sage:

```
PP.<a1,a2,p> = PolynomialRing(ZZ,3)
PX.<x> = PolynomialRing(PP)
f = x^4 - a1*x^3 + (a2+2*p)*x^2 - a1*p*x + p^2
QX.<pi> = PX.quotient_ring(f)
```

and determine the sequence of generic traces:

```
sage: [ (pi^n).trace() for n in range(1,6) ]
[a1,
 a1^2 - 2*a2 - 4*p,
 a1^3 - 3*a1*a2 - 3*a1*p,
 a1^4 - 4*a1^2*a2 - 4*a1^2*p + 2*a2^2 + 8*a2*p + 4*p^2,
 a1^5 - 5*a1^3*a2 - 5*a1^3*p + 5*a1*a2^2 + 15*a1*a2*p + 5*a1*p^2]
```

and the first terms of of generic norms:

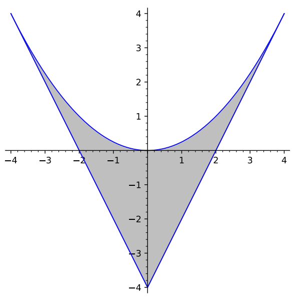
```
sage: [ (pi^n-1).norm() - (p+1)^(2*n) + a1^r*(p+1)^n for n in range(1,3) ]
[a2, 2*a2*p^2 + a2^2 + 4*a2*p + 2*a2]
```

For a particular curve C or Jacobian J, we can compute the sequence of integer values for $N_C(p^n)$ or $N_J(p^n)$.

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

$$\tilde{F}_p(x) = x^4 - \tilde{a}_1 x^3 + (\tilde{a}_2 + 2)x^2 - \tilde{a}_1 x + 1,$$

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

$$\frac{2ds_1ds_2}{\pi^2\sqrt{(s_1^2-4s_2)(4-2s_1+s_2)(4+2s_1+s_2)}}.$$

---

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 $\mathrm{SO}(2)$.

From the inner product matrix for $\mathrm{USp}(4)$ one concludes that $(1, \psi_1, \psi_2 + 1, \psi_1^2 - \psi_2 - 2)$ is a basis of irreducible characters on $\mathrm{USp}(4)$. Similarly, on $\mathrm{SU}(2) \times \mathrm{SU}(2)$ the virtual characters $(1, \psi_1, \psi_2, \psi_1^2 - 2\psi_2 - 2)$ give rise to the inner product matrix:

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

which suggest that $(1, \psi_2)$ are irreducible and $(\psi_1, \psi_1^2 - 2\psi_2 - 2)$ are sums of two distinct irreducible characters. Indeed if (φ_1, φ_2) are the irreducible characters on the first and second factor of $\mathrm{SU}(2) \times \mathrm{SU}(2)$, respectively, we have

$$\psi_1 = \varphi_1 + \varphi_2, \text{ and } \psi_2 = \varphi_1\varphi_2,$$

and

$$\psi_1^2 - 2\psi_2 - 2 = (\varphi_1^2 - 1) + (\varphi_2^2 - 1) = S^2(\varphi_1) + S^2(\varphi_2).$$

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.

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

In Sage we can construct these curves as follows:

```
PQ.<x> = PolynomialRing(QQ)
C0 = HyperellipticCurve(-x^5,x^3 + x + 1)
C1 = HyperellipticCurve(x^4 - 7,x^3 + x)
C2 = HyperellipticCurve(-1,x^3 + x)
C3 = HyperellipticCurve(x^4 + x^2,x^3 + 1)
C4 = HyperellipticCurve(x^5,1)
C5 = HyperellipticCurve(x^6,1)
Crvs = [C0,C1,C2,C3,C4,C5]
```

In order to look up the data in the LMFDB, it is useful to know the discriminant:

```
def discriminant(C):
   return C.igusa_clebsch_invariants()[3]/2^12

for C in Crvs:
   print("C%s: %s" % (Crvs.index(C),discriminant(C).factor()))

C0: 23^2
C1: 2^6 * 7
C2: 2^8 * 7^2
C3: -1 * 2 * 3 * 7^2
C4: 5^5
C5: -1 * 2^4 * 3^6
```

N.B. For each curve, the Sato-Tate groups can be found in the LMFDB. In particular their connected components are as follows:

- $\mathrm{SU}(2) \times \mathrm{SU}(2)$
- $\mathrm{SO}(2) \times \mathrm{SU}(2)$
- $\mathrm{SU}(2) \times \mathrm{SU}(2)$
- $\mathrm{SU}(2) \times \mathrm{SU}(2)$
- $\mathrm{SO}(2) \times \mathrm{SO}(2)$
- $\mathrm{SO}(2)$

with respective components groups:

- $\{1\}$
- C_2
- $\{1\}$
- $\{1\}$
- C_4
- S_3

```
def genus2_inner_product_matrix(C0,C1,chars,max_prime=2^10,prec=32):
    # Given genus-2 curves C0/Q and C1/Q, and a character sequence
    # chars = (chi_i(x,y)), compute the expectation of the matrix
    #     (chi_i(psi_C0,1,psi_C0,2)*chi_j(psi_C1,1psi_C1,j)),
    # over primes up to the bound max_prime.
    RR = RealField(prec)
    D0 = discriminant(C0); bad_primes0 = D0.numerator() * D0.denominator()
    D1 = discriminant(C1); bad_primes1 = D1.numerator() * D1.denominator()
    n = len(chars)
    A = MatrixSpace(RR,n,n)(0)
    num = 0
    for p in primes(max_prime):
        if bad_primes0.mod(p) == 0: continue
        if bad_primes1.mod(p) == 0: continue
        FF = FiniteField(p)
        sqrtp = RR(p).sqrt()
        C0p = C0.base_extend(FF)
        f0p = C0p.frobenius_polynomial()
        (a0_1,a0_2) = (-RR(f0p[3])/sqrtp,RR(f0p[2])/p-2)
        C1p = C1.base_extend(FF)
        f1p = C1p.frobenius_polynomial()
        (a1_1,a1_2) = (-RR(f1p[3])/sqrtp,RR(f1p[2])/p-2)
        for i in range(n):
            for j in range(n):
                (Fi,Fj) = (chars[i],chars[j])
                A[i,j] += RR(Fi(a0_1,a0_2)*Fj(a1_1,a1_2))
        num += 1
    return A*(1/num)
```

The following computation suggests that C_0 and C_1 have independent Galois representations but the character $\psi_2 + 1$ is not irreducible on either curve, suggesting both Sato-Tate groups are proper subgroups of $\mathrm{USp}(4)$.

```
sage: P2.<s1,s2> = PolynomialRing(QQ,2); one = P2(1)
sage: chars = [one,s1,s2+1]
sage: genus2_inner_product_matrix(C0,C1,chars)
[   1.00000000  0.0233165194   0.916698532]
[-0.0191967414 -0.0757464348  -0.130829140]
[  0.979408722 -0.0762762215   0.844596297]
```

On the other hand, the inner product matrix (now with respect to $(1,\psi_1,\psi_2)$) suggest a common irreducible factor of ψ_1 on C_1 and C_3 but no such factor in ψ_2.

```
sage: P2.<s1,s2> = PolynomialRing(QQ,2); one = P2(1)
sage: chars = [one,s1,s2]
sage: genus2_inner_product_matrix(C1,C3,chars)
[   1.00000000  0.0428025942 -0.0633599550]
[ 0.0301490670   0.771475847  0.0329457660]
[-0.0833014680   0.133867857  0.0196059062]
```

This suggests that C_1 and C_3 have a common elliptic factor (up to isogeny).

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.

The inner product with the characters of the elliptic curves and number fields reveals the isogeny factors and characters which factor through the component groups. First we implement the inner product with respect to the respective Frobenius traces.

```
def genus2_elliptic_inner_product(C,E,max_prime=2^10,prec=24):
    # Given a genus-2 curve C/Q and and elliptic curve E/Q,
    # compute the expectation of the matrix the normalized
    # trace products ((a_C * a_E)/p) over primes p up to the
    # bound max_prime.
    RR = RealField(prec)
    D0 = discriminant(C); bad_primes0 = D0.numerator() * D0.denominator()
    D1 = discriminant(E); bad_primes1 = D1.numerator() * D1.denominator()
    S,num = (RR(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)
        Np = C.base_extend(FF).cardinality()
        aC = p+1-Np
        aE = E.base_extend(FF).trace_of_frobenius()
        S += RR(aE*aC)/p
        num += 1
    return A*(1/num)
```

Then the given elliptic curves can be created in Sage as follows:

```
E0 = EllipticCurve([1,0,1,-1,0]) # quotient of C1, C2, C3 (14a)
E1 = EllipticCurve([0,-1,0,0,-4]) # quotient of C2 (56a)
E2 = EllipticCurve([0,0,0,-1,0]) # quotient of C1 (32a)
E3 = EllipticCurve([1,0,0,1,0]) # quotient of C3 (21a)
E4 = EllipticCurve([0,0,0,0,4]) # quotient of C5 (108a)
E5 = EllipticCurve([0,0,1,0,0]) # quotient of C5 (27a)
Ells = [E0,E1,E2,E3,E4,E5]
```

The dependency relation between the Frobenius trace characters on the genus-2 curves and elliptic curves can be represented in a matrix:

```
RR = RealField(24)
A = MatrixSpace(RR,6)(0)
for i in range(len(Ells)):
    for j in range(len(Crvs)):
        A[i,j] = genus2_elliptic_inner_product(Crvs[j],Ells[i])

print("Inner product matrix of genus2 and elliptic traces characters:")
print(A)
print(matrix([[round(A[i,j]) for j in range(6)] for i in range(6)]))
```

This produces the following inner product matrix:

```
Inner product matrix of genus2 and elliptic traces characters:
[   -0.130043     0.876022     0.867462     0.893295   -0.0151389   -0.0858860]
[   -0.133701   -0.0964069     0.832199   -0.0786114   -0.0874424     0.179150]
[   0.0539637     0.877716   -0.0877914    -0.121748   -0.0658112    0.0688629]
[0.0000367416    -0.101803   -0.0578966     0.881226   0.00219613    0.0578194]
[-0.000962213    0.0217028    0.0203094  -0.00743401    0.0858841     0.858093]
[   -0.186443   -0.0383263    0.0729446   -0.0206447    -0.118797     0.837158]
[0 1 1 1 0 0]
[0 0 1 0 0 0]
[0 1 0 0 0 0]
[0 0 0 1 0 0]
[0 0 0 0 0 1]
[0 0 0 0 0 1]
```

Showing that E_0 is a common isogeny factor of C_1, C_2 and C_3, E_1 an isogeny factor of C_2, E_2 an isogeny factor of C_1, and E_3 an isogeny factor of C_3. This gives

$$\mathrm{Jac}(C_1) \sim E_0 \times E_2, \quad \mathrm{Jac}(C_2) \sim E_0 \times E_1, \quad \mathrm{Jac}(C_3) \sim E_0 \times E_3,$$

and finally we have $\mathrm{Jac}(C_5) \sim E_4 \times E_5$. The Jacobians of C_0 and C_4, on the other hand, are simple (indecomposable), and have no such elliptic curve factors.

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 $\chi_1,\dots,\chi_t$ 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?

If the character ψ is independent of (the characters on) $G = \mathrm{Gal}(K/\mathbb{Q})$ then we have the relation:

$$(\langle \psi\chi_i, \psi\chi_j \rangle) = (\langle \psi^2\chi_i, \chi_j \rangle) = (\langle \psi^2\chi_i, \chi_j \rangle) = \langle \psi, \psi \rangle (\langle \chi_i, \chi_j \rangle).$$

In particular, if ψ is irreducible, then the inner product matrices are equal. On the other hand, if the Frobenius representation is not independent of G, due to nontrivial action on the component group, then this can be measured in the inner product matrix of the twists $\psi\chi_i$.

Appendix. We give below some code for the numerical integration, decomposing the region of integration into slices, since Sage doesn't currently have a function for integration over a non rectangular regions.

Each of the following three functions defines an integration over a function f with respect to a probability density funcction $\mu(s_1,s_2)$ on $\mathrm{USp}(4)$, $\mathrm{SU}(2)\times\mathrm{SU}(2)$, or $\mathrm{SO}(2)\times\mathrm{SO}(2)$.

```
Groups=('USp(4)','SU(2)xSU(2)','SO(2)xSO(2)')

def haar_measure(s1,s2,Group="USp(4)"):
    D0 = (s1^2 - 4*s2)
    D1 = (4 - 2*s1 + s2)*(4 + 2*s1 + s2)
    if G=="USp4":
        return sqrt(D0*D1)
    elif G=="SU(2)xSU(2)":
        return sqrt(D1/D0)
    elif G=="SO(2)xSO(2)":
        return sqrt(1/(D0*D1))
    else:
        assert False, "Group must be in %s" % Groups

def haar_integral(f,Group="USp(4)",N=2^10,epsilon=0.1^12):
    s1,s2 = f.parent().gens()
    if f(-s1,s2) == -f(s1,s2):
        return RR(0)
    if f(-s1,s2) == f(s1,s2):
         (B,mult) = (0,2)
    else:
         (B,mult) = (-4*N+1,1)
    # Fix the integration constant, and set bounds away
    # from the boundary to avoid integration at infinity.
    if Group == "USp(4)":
        cc,e1,e2 = (1/(4*RR.pi()^2),0,0)
    elif Group == "SU(2)xSU(2)":
        cc,e1,e2 = (1/(2*RR.pi()^2),0,epsilon)
    elif Group == "SO(2)xSO(2)":
        cc,e1,e2 = (2/RR.pi()^2,epsilon,epsilon)
    else:
        assert False, "Group must be in %s" % Groups
    # Riemann sums of integrals:
    I0 = 0
    s2 = var('s2')
    for i in range(B,4*N):
        s1 = i/N
        (a,b) = (2*abs(s1)-4+e1,s1^2/4-e2)
        mu = haar_measure(s1,s2,Group)
        I0 += mult*numerical_integral(f([s1,s2])*mu,a,b)[0]/N
    return cc*I0
```

Next we define a function for the inner product matrix determined by each of these probability integrals. For a given list of (virtual) characters, the integrals over products $\psi\chi$ gives the inner product $\langle\psi,\chi\rangle$ as expectation.

```
def haar_inner_product_matrix(B,Group="USp(4)"):
    n = len(B)
    A = MatrixSpace(RR,n,n)(0)
    for i in range(n):
        A[i,i] = haar_integral(B[i]^2,Group)
        for j in range(i+1,n):
            A[i,j] = haar_integral(B[i]*B[j],Group)
            A[j,i] = A[i,j]
    return A
```

Finally we can compute the inner product matrices associated to the virtual characters

$$(\psi_{(0,0)}, \psi_{(1,0)}, \psi_{(0,1)}, \psi_{(2,0)}) = (1, \psi_1, \psi_2, \psi_1^2 - \psi_2 - 2).$$

```
P2.<S1,S2> = PolynomialRing(ZZ,2); one = P2(1)
chars = [one,S1,S2,S1^2-(S2+2)]
RR = RealField(32)

A44 = haar_inner_product_matrix(chars,"USp(4)")
print("Numerical integral for USp(4):")
print(A44)
print(matrix(matrix([[round(A44[i,j]) for j in range(4)] for i in range(4)])))

B44 = haar_inner_product_matrix(chars,"SU(2)xSU(2)")
print("Numerical integral for SU(2)^2:")
print(B44)
print(matrix(matrix([[round(B44[i,j]) for j in range(4)] for i in range(4)])))

C44 = haar_inner_product_matrix(chars,"SO(2)xSO(2))
print("Numerical integral for SO(2)^2:")
print(C44)
print(matrix(matrix([[round(C44[i,j]) for j in range(4)] for i in range(4)])))
```

This gives the following inner product for USp(4):

```
Numerical integral for USp(4):
[      1.00042218     0.000000000     -1.00072372 -0.000120619627]
[     0.000000000      1.00000000     0.000000000     0.000000000]
[     -1.00072372     0.000000000      2.00160828 -0.000160827678]
[-0.000120619627     0.000000000 -0.000160827678      1.00040207]
[ 1  0 -1  0]
[ 0  1  0  0]
[-1  0  2  0]
[ 0  0  0  1]
```

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

```
Numerical integral for SU(2)^2:
[      1.00026278     0.000000000 -0.000211950900 -0.000317057902]
[     0.000000000      1.99999655     0.000000000     0.000000000]
[-0.000211950900     0.000000000      1.00036036      1.00005759]
[-0.000317057902     0.000000000      1.00005759      3.00056566]
[1 0 0 0]
[0 2 0 0]
[0 0 1 1]
[0 0 1 3]
```

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

```
Numerical integral for SO(2)^2:
[     1.00235557     0.000000000 -0.00967552672      2.00367177]
[    0.000000000      3.99870738     0.000000000     0.000000000]
[-0.00967552672     0.000000000      4.03559572      3.97860427]
[     2.00367177     0.000000000      3.97860427      12.0011784]
[ 1  0  0  2]
[ 0  4  0  0]
[ 0  0  4  4]
[ 2  0  4 12]
```