Chapter 9

Computing Newforms

In this chapter we pull together results and algorithms from Chapter 3, 4, 7, and 8 and explain how to compute cusp forms (especially eigenforms) using modular symbols.

We first discuss in Section 9.1 how to decompose $M_k(\Gamma_1(N))$ as a direct sum of subspaces corresponding to Dirichlet characters. Next in Section 9.2 we state the main theorems of Atkin-Lehner-Li theory, which gives a beautiful decomposition of $S_k(\Gamma_1(N))$ into subspaces on which the Hecke operators acts diagonalizable with "multiplicity one". In Section 9.3 we revisit the connection between cusp forms and modular symbols, then describe two algorithms for computing modular forms. One algorithm finds a basis of q-expansions, and the other computes eigenvalues of newforms.

9.1 Decomposing Modular Forms Using Dirichlet Characters

The group $(\mathbb{Z}/N\mathbb{Z})^*$ acts on $M_k(\Gamma_1(N))$ through the *diamond-bracket operators* $\langle d\rangle$, as follows. For $[d] \in (\mathbb{Z}/N\mathbb{Z})^*$, define

$$f|\langle d\rangle = f|[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)]_k,$$

where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ is congruent to $\left(\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right) \pmod N$. Note that the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective (see Exercise 5.2), so the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ exists. To prove that $\langle d\rangle$ preserves $M_k(\Gamma_1(N))$, we prove the more general fact that $\Gamma_1(N)$ is normal in

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N\right\}.$$

This will imply that $\langle d\rangle$ preserves $M_k(\Gamma_1(N))$ since $\left(\begin{smallmatrix} a & b \\ c & d' \end{smallmatrix}\right) \in \Gamma_0(N)$.

Lemma 9.1.1. *The group $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$, and the quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$.*

Proof. See Exercise 9.1. □

The diamond bracket action is simply the action of $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$ on $M_k(\Gamma_1(N))$. Since $M_k(\Gamma_1(N))$ is a finite dimensional vector space over $\mathbb{C}$, the $\langle d\rangle$ action breaks $M_k(\Gamma_1(N))$ up as a direct sum of factors corresponding to the Dirichlet characters $D(N,\mathbb{C})$ of modulus N.

Proposition 9.1.2. *We have*

$$M_k(\Gamma_1(N)) = \bigoplus_{\varepsilon \in D(N,\mathbb{C})} M_k(N,\varepsilon),$$

where

$$M_k(N,\varepsilon) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : f|\langle d\rangle = \varepsilon(d) f \text{ all } d \in (\mathbb{Z}/N\mathbb{Z})^*\}.$$

Proof. The linear transformations $\langle d\rangle$, for the $d \in (\mathbb{Z}/N\mathbb{Z})^*$, all commute, since $\langle d\rangle$ acts through the abelian group $\Gamma_0(N)/\Gamma_1(N)$. Also, if e is the exponent of $(\mathbb{Z}/N\mathbb{Z})^*$, then $\langle d\rangle^e = \langle d^e\rangle = \langle 1\rangle = 1$, so the matrix of $\langle d\rangle$ is diagonalizable. It is a standard fact from linear algebra that any commuting family of diagonalizable linear transformations is simultaneously diagonalizable (see Exercise 5.1), so there is a basis $f_1,\ldots,f_n$ for $M_k(\Gamma_1(N))$ so that all $\langle d\rangle$ act by diagonal matrices. The eigenvalues of the action of $(\mathbb{Z}/N\mathbb{Z})^*$ on a fixed f_i defines a Dirichlet character, i.e., each f_i has the property that $f_i|\langle d\rangle = \varepsilon_i(d)$, for all $d \in (\mathbb{Z}/N\mathbb{Z})^*$ and some Dirichlet character ε_i. The f_i for a given ε then span $M_k(N,\varepsilon)$, and taken together the $M_k(N,\varepsilon)$ must span $M_k(\Gamma_1(N))$. □

Definition 9.1.3 (Character of Modular Form)**.** If $f \in M_k(N,\varepsilon)$, we say that f *has character ε.*

The spaces $M_k(N,\varepsilon)$ are a direct sum of subspaces $S_k(N,\varepsilon)$ and $E_k(N,\varepsilon)$, where $S_k(N,\varepsilon)$ is the subspace of cusp forms, i.e., forms that vanish at *all* cusps (elements of $\mathbb{Q}\cup\{\infty\}$), and $E_k(N,\varepsilon)$ is the subspace of Eisenstein series, which is the unique subspace of $M_k(N,\varepsilon)$ that is invariant under all Hecke operators and is such that $M_k(N,\varepsilon) = S_k(N,\varepsilon) \oplus E_k(N,\varepsilon)$. The space $E_k(N,\varepsilon)$ can also be defined as the space spanned by all Eisenstein series of weight k and level N, as defined in Chapter 5. The space $E_k(N,\varepsilon)$ can also be defined using the Petersson inner product (see, e.g., [Lan95]).

The diamond bracket operators preserve the subspace of cusp forms, so the isomorphism of Proposition 9.1.2 restricts to an isomorphism of the corresponding cuspidal subspaces. We illustrate how to use SAGE to make a table of dimension of $M_k(\Gamma_1(N))$ and $M_k(N,\varepsilon)$ for $N = 13$.

```
sage: G = DirichletGroup(13)
sage: G
Group of Dirichlet characters of modulus 13 over Cyclotomic Field
of order 12 and degree 4
sage: dimension_modular_forms(Gamma1(13),2)
13
sage: [dimension_modular_forms(e,2) for e in G]
[1, 0, 3, 0, 2, 0, 2, 0, 2, 0, 3, 0]
```

Next we do the same for $N = 100$.

```
sage: G = DirichletGroup(100)
sage: G
Group of Dirichlet characters of modulus 100 over Cyclotomic Field
of order 20 and degree 8
sage: dimension_modular_forms(Gamma1(13),2)
370
sage: [dimension_modular_forms(e,2) for e in G]
[24, 0, 0, 17, 18, 0, 0, 17, 18, 0, 0, 21, 18, 0, 0, 17, 18,
  0, 0, 17, 24, 0, 0, 17, 18, 0, 0, 17, 18, 0, 0, 21, 18, 0,
  0, 17, 18, 0, 0, 17]
```

9.2 Atkin-Lehner-Li Theory

Let

$$\alpha_d : S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N))$$

be the *degeneracy map* given by $f(q) \mapsto f(q^d)$. The *new subspace* of $S_k(\Gamma_1(M))$, which we denote by $S_k(\Gamma_1(M))_{\rm new}$, is the largest $\mathbb{T}$-stable complement of the image of all maps α_d from level properly dividing M.

Let $\mathbb{T}'$ be the subring of $\mathbb{T}$ generated by the T_n with $\gcd(n, N) = 1$.

Theorem 9.2.1 (Atkin, Lehner, Li)**.** *We have a decomposition*

$$S_k(\Gamma_1(N)) = \bigoplus_{M|N} \bigoplus_{d|N/M} \alpha_d(S_k(\Gamma_1(M))_{\rm new}). \tag{9.2.1}$$

Moreover, each space $S_k(\Gamma_1(M))_{\rm new}$ is a direct sum of distinct (non-isomorphic) simple $\mathbb{T}'_{\mathbb{C}}$-modules.

Proof. See [Li75]. □

The analogue of Theorem **??** with Γ_1 replaced by Γ_0 is also true (this is what was proved in [AL70]). The analogue for $S_k(N, \varepsilon)$ is also valid, as long as we omit the spaces $S_k(\Gamma_1(M), \varepsilon)$ for which $M \nmid \mathrm{cond}(\varepsilon)$.

Example 9.2.2. If N is prime and $k \leq 11$, then $S_k(\Gamma_1(N))_{\rm new} = S_k(\Gamma_1(N))$, since $S_k(\Gamma_1(1)) = 0$.

One can prove (using the Petersson inner product) that the Hecke operators T_n on $S_k(\Gamma_1(N))$, with $(n, N) = 1$, are diagonalizable. Another result of Atkin-Lehner-Li theory is that the ring of endomorphism of $S_k(\Gamma_1(N))_{\rm new}$ generated by all Hecke operators equals the ring generated by the Hecke operators T_n with $(n, N) = 1$. This statement need *not* be true if we do not restrict to the new subspace, as the following example shows.

Example 9.2.3. We have

$$S_2(\Gamma_0(22)) = S_2(\Gamma_0(11)) \oplus \alpha_2(S_2(\Gamma_0(11))),$$

where each of the spaces $S_2(\Gamma_0(11))$ has dimension 1. Thus $S_2(\Gamma_0(22))_{\rm new} = 0$. The Hecke operator T_2 on $S_2(\Gamma_0(22))$ has characteristic polynomial $x^2 + 2x + 2$, which is irreducible. Since α_2 commutes with all Hecke operators T_n, with $\gcd(n, 2) = 1$, the subring $\mathbb{T}'$ of the Hecke algebra generated by operators T_n with n odd is isomorphic to $\mathbb{Z}$ (the 2×2 scalar matrices). Thus on the full space $S_2(\Gamma_0(22))$, we do not have $\mathbb{T}' = \mathbb{T}$. However, on the new subspace we do have this equality, since the new subspace has dimension 0.

Example 9.2.4. This example is similar to Example 9.2.3, except that there are newforms. We have

$$S_2(\Gamma_0(55)) = S_2(\Gamma_0(11)) \oplus \alpha_5(S_2(\Gamma_0(11))) \oplus S_2(\Gamma_0(55))_{\rm new},$$

where $S_2(\Gamma_0(11))$ has dimension 1 and $S_2(\Gamma_0(55))_{\rm new}$ has dimension 3. The Hecke operator T_5 on $S_2(\Gamma_0(55))_{\rm new}$ acts via the matrix

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

with respect to some basis.[[**Todo: which?**]] This matrix has eigenvalues 1 and -1. Atkin-Lehner theory asserts that T_5 must be a linear combination of Hecke operators T_n, with $\gcd(n, 55) = 1$. Upon computing the matrix for T_2, we find by simple linear algebra that $T_5 = 2T_2 - T_4$.

Before moving on, we pause to say something about how the Atkin-Lehner-Li theorems are proved. A key result is to prove that if $f, g \in S_k(\Gamma_1(N))_{\rm new}$ and $a_n(f) = a_n(g)$ for all n with $\gcd(n, N) = 1$, then $f = g$. First, replace f and g by their difference $h = f - g$, and observe that $a_n(h) = 0$ for $\gcd(n, N) = 1$. Note that such an h "looks like" it is in the image of the maps α_d, for $d \mid N$. In fact it is—one shows that h is in the old subspace $S_k(\Gamma_1(N))_{\rm old}$ (this is the "crucial" Theorem 2 of [Li75]). But h is also new, since it is the difference of two newforms, so $h = 0$, hence $f = g$. The details involve introducing many maps between spaces of modular forms, and computing what they do to q-expansions.

Definition 9.2.5 (Newform)**.** A *newform* is a $\mathbb{T}$-eigenform $f \in S_k(\Gamma_1(N))_{\rm new}$ that is normalized so that the coefficient of q is 1.

We now motivate this definition by explaining why any $\mathbb{T}$-eigenform can be normalized so that the coefficient of q is 1, and how such an eigenform has the convenient properties that its Fourier coefficients are exactly the Hecke eigenvalues.

Proposition 9.2.6. *If $f = \sum_{n=0}^{\infty} a_n q^n \in M_k(N,\varepsilon)$ is an eigenvector for all Hecke operators T_n normalized so that $a_1 = 1$, then $T_n(f) = a_n f$.*

Proof. The Hecke algebra $\mathbb{T}_{\mathbb{Q}}$ on $S_k(\Gamma_1(N))$ contains the diamond bracket operators $\langle d\rangle$, since $T_{p^2} = T_p^2 - \langle p\rangle p^{k-1}$, so any $\mathbb{T}$-eigenform lies in a subspace $S_k(\Gamma_1(N),\varepsilon)$ for some Dirichlet character ε. The Hecke operators T_p, for p prime, act on $S_k(\Gamma_1(N),\varepsilon)$ by

$$T_p\left(\sum_{n=0}^{\infty} a_n q^n\right) = \sum_{n=0}^{\infty}\left(a_{np}q^n + \varepsilon(p)p^{k-1}a_n q^{np}\right),$$

and there is a similar formula for T_m with m composite. If $f = \sum_{n=0}^{\infty} a_n q^n$ is an eigenform for all T_p, with eigenvalues λ_p, then by the above formula

$$\lambda_p f = \lambda_p a_1 q + \lambda_p a_2 q^2 + \cdots = T_p(f) = a_p q + \text{higher terms}. \tag{9.2.2}$$

Equating coefficients of q we see that if $a_1 = 0$, then $a_p = 0$ for all p, hence $a_n = 0$ for all n, because of the multiplicativity of Fourier coefficients and the recurrence

$$a_{p^r} = a_{p^{r-1}}a_p - \varepsilon(p)p^{k-1}a_{p^{r-2}}.$$

This would mean that $f = 0$, a contradiction. Thus $a_1 \neq 0$, and it makes sense to normalize f so that $a_1 = 1$. With this normalization, (9.2.2) implies that $\lambda_p = a_p$, as desired. □

Remark 9.2.7. In fact, $\langle d\rangle \in \mathbb{Z}[\ldots, T_n, \ldots]$. See Exercise 9.2.

9.3 Computing Cuspforms

Let $\mathbb{S}_k(N,\varepsilon;\mathbb{C})$ be cuspidal modular symbols, as in Chapter 8, and let $\mathbb{S}_k(N,\varepsilon;\mathbb{C})^+$ denote the $+1$ quotient as in (8.5.7). It follows from Theorem 8.5.6, and compatibility of the degeneracy maps, that the $\mathbb{T}$-modules $S_k(N,\varepsilon)_{\mathrm{new}}$ and $\mathbb{S}_k(N,\varepsilon,\mathbb{C})^+_{\mathrm{new}}$ are dual as $\mathbb{T}$-modules. Thus finding the systems of $\mathbb{T}$-eigenvalues on cuspforms is the same as finding the systems of $\mathbb{T}$-eigenvalues on cuspidal modular symbols.

Our strategy to compute $S_k(N,\varepsilon)$ is to first compute spaces $S_k(N,\varepsilon)_{\mathrm{new}}$ using the Atkin-Lehner-Li decomposition (9.2.1). To compute $S_k(N,\varepsilon)_{\mathrm{new}}$ to a given precision, we compute the systems of eigenvalues of the Hecke operators T_p on $V = \mathbb{S}_k(N,\varepsilon,\mathbb{C})^+_{\mathrm{new}}$. Using Proposition 9.2.6, we then recover a basis of q-expansions for newforms. Note that we only need to compute Hecke eigenvalues T_p, for p prime, not the T_n for n composite, since the a_n can be quickly recovered in terms of the a_p using multiplicativity and the recurrence.

The some problems, e.g., construction of models for modular curves, where just having a basis is enough, and knowing the newforms is not so important. For other problems, e.g., enumeration of modular abelian varieties or motives, one is really interested in the newforms, not just any basis for $S_k(N,\varepsilon)$. We next discuss algorithms aimed at each of these problems.

9.3.1 A Basis of q-Expansions

Merel's paper [Mer94] culminates with the following algorithm to compute $S_k(\Gamma_1(N),\varepsilon)$ without finding any eigenspaces:

Algorithm 9.3.1 (Merel's Algorithm for Computing a Basis)**.** *1. [Compute Modular Symbols] Using Algorithm 8.8.1, compute a presentation for $V = \mathbb{S}_k(\Gamma_1(N),\varepsilon)^+ \otimes \mathbb{Q}(\varepsilon)$, viewed as a $K = \mathbb{Q}(\varepsilon)$ vector space, along with an action of Hecke operators T_n.*

2. [Basis for Linear Dual] Write down a basis for $V^* = \mathrm{Hom}(V,\mathbb{Q}(\varepsilon))$. E.g., if we identify V with K^n viewed as column vectors, then V^* is the space of row vectors of length n, and the pairing is the row $\times$ column product.

3. [Find Generator] Find $x \in V$ such that $\mathbb{T}x = V$ by choosing random x until we find one that generates. The set of x that fail to generate lie in a union of a finite number of proper subspace.

4. [Compute Basis] The set of power series

$$f_i = \sum_{n=1}^{m} \psi_i(T_n(x))q^n + O(q^{m+1})$$

form a basis for $S_k(\Gamma_1(N),\varepsilon)$ to precision m.

In practice my experience is that my implementations of Algorithm 9.3.1 are significantly slower than the eigenspace algorithm that we will describe in the rest of this chapter. The theoretical complexity of Algorithm 9.3.1 *may* be better, because it is not necessary to factor any polynomials. Polynomial factorization is difficult from the analysis-of-complexity point of view, though usually fairly fast in practice. The eigenvalue algorithm only requires computing a few images $T_p(x)$ for p prime and x a Manin symbol on which T_p can easily be computed. The Merel algorithm involves computing $T_n(x)$ for all n, and a fairly easy x, which is potentially more work.

Remark 9.3.2. By "easy x", I mean that computing $T_n(x)$ is easier on x than on a completely random element of $\mathbb{S}_k(\Gamma_1(N),\varepsilon)^+$, e.g., x could be a Manin symbol.

9.3.2 Newforms: Systems of Eigenvalues

In this section we describe an algorithm for computing the system of Hecke eigenvalues associated to a simple subspace of a space of modular symbols. This algorithm is better than doing linear algebra directly over the number field generated by the eigenvalues. It only involves linear algebra over the base field, and also yields a compact representation for the answer, which is better than writing the eigenvalues in terms of a power basis for a number field.

Fix N and a Dirichlet character ε modulo N and set

$$V = \mathbb{S}_k(N,\varepsilon)^+_{\mathrm{new}}.$$

Algorithm 9.3.3 (System of Eigenvalues)**.** *Given a $\mathbb{T}$-simple subspace $W \subset V$ of modular symbols, this algoritm outputs maps ψ and e, where $\psi : \mathbb{T}_K \to W$ is a K-linear map and $e : W \cong L$ is an isomorphism of W with a number field L, such that $a_n = e(\psi(T_n))$ is the eigenvalue of the nth Hecke operator acting on a fixed $\mathbb{T}$-eigenvector in $W \otimes \overline{\mathbb{Q}}$. (Thus $f = \sum_{n=1}^{\infty} i(\psi(T_n))q^n$ is a cuspidal modular eigenform.)*

1. [Compute Projection] Let $\varphi : V \to W'$ be any surjective linear map such that $\ker(\varphi)$ equals the kernel of the $\mathbb{T}$-invariant projection onto W. For example, compute φ by finding a simple submodule of $V^* = \mathrm{Hom}(V,K)$ that is isomorphic to W, e.g., by applying Algorithm 7.5.9 to V^* with T replaced by the transpose of T.
2. [Choose v] Choose a nonzero element $v \in V$ such that $\pi(v) \neq 0$ and computation of $T_n(v)$ is "easy", e.g., choose v to be a Manin symbol.
3. [Map From Hecke Ring] Let ψ be the map $\mathbb{T} \to W'$, given by $\psi(t) = \pi(tv)$. Note that computation of ψ is relatively easy, because v was chosen so that tv is relatively easy to compute. In particular, if $t = T_p$, we do not need to compute the full matrix of T_p on V; instead we just compute $T_p(v)$.
4. [Find Generator] Find a random $T \in \mathbb{T}$ such that the iterates

   $$\psi(T^0), \quad \psi(T), \quad \psi(T^2), \quad \ldots, \quad \psi(T^{d-1})$$

   are a basis for W', where W has dimension d.
5. [Characteristic Polynomial] Compute the characteristic polynomial f of $T|_W$, and let $L = K[x]/(f)$. Because of how we chose T in Step 4, the minimal and characteristic polynomials of $T|_W$ are equal, and both are irreducible, so L is an extension of K of degree $d = \dim(W)$.
6. [Field Structure] In this step we endow W' with a field structure. Let $e : W' \to L$ be the unique K-linear isomorphism such that

   $$e(\psi(T^i)) \equiv x^i \pmod{f}$$

   for $i = 0, 1, 2, ..., \deg(f) - 1$. The map e is uniquely determined since the $\psi(T^i)$ are a basis for W'. To compute e, we compute the change of basis matrix from the standard basis for W' to the basis $\{\psi(T^i)\}$. This change of basis matrix is the inverse of the matrix whose rows are the $\psi(T^i)$ for $i = 0, ..., \deg(f) - 1$.
7. [Hecke Eigenvalues] Finally for each integer $n \geq 1$, we have

   $$a_n = e(\psi(T_n)) = e(\pi(T_n(v))),$$

   where a_n is the eigenvalue of T_n. Output the maps ψ and e and terminate.

One reason we separate ψ and e is that when $\dim(W)$ is large, the values $\psi(T_n)$ tend to take too much space to store and are easier to compute, whereas each one of the values $e(\psi(n))$ are huge.[1] The function e typically involves large numbers if $\dim(W)$ is large, since e is got from the iterates of a single vector. For many applications, e.g., databases, it is better to store a matrix that defines e and the images under ψ of many T_n.

Example 9.3.4. The space $S_2(\Gamma_0(23))$ of cusp forms has dimension 2, and is spanned by two $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate newforms, one of which is

$$f = \sum q + aq^2 + (-2a-1)q^3 + (-a-1)q^4 + 2aq^5 + \cdots,$$

where $a = (-1+\sqrt{5})/2$. We will use Algorithm 9.3.3 to compute a few of these coefficients.

The space $\mathbb{M}_2(\Gamma_0(23))^+$ of modular symbols has dimension 3. It has as basis the following basis of Manin symbols:

$$[(0,0)], \quad [(1,0)], \quad [(0,1)],$$

where we use square brackets to differentiate Manin symbols from vectors. The Hecke operator

$$T_2 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 2 \\ -1 & 1/2 & -1 \end{pmatrix}$$

has characteristic polynomial $(x-3)(x^2+x-1)$. The kernel of T_2-3 corresponds to the span of the Eisenstein series of level 23 and weight 2, and the kernel V of $T_2^2 + T_2 - 1$ corresponds to $S_2(\Gamma_0(23))$. (We could also have computed V as the kernel of the boundary map $\mathbb{M}_2(\Gamma_0(23))^+ \to \mathbb{B}_2(\Gamma_0(23))^+$.) Each of the following steps corresponds to the same step of Algorithm 9.3.3.

1. [Compute Projection] Using the Algorithm **??**, we compute projection onto V. The matrix whose first two columns are the echelon basis for V and whose last column is the echelon basis for the Eisenstein subspace is

   $$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -2/11 \\ 0 & 1 & -3/11 \end{pmatrix}$$

[1] John Cremona initially suggested to me the idea of separating these two maps.

and

$$B^{-1} = \begin{pmatrix} 2/11 & 1 & 0 \\ 3/11 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

so projection onto V is given by the first two rows:

$$\pi = \begin{pmatrix} 2/11 & 1 & 0 \\ 3/11 & 0 & 1 \end{pmatrix}.$$

2. [Choose v] Let $v = (0,1,0)^t$. Notice that $\pi(v) = (1,0)^t \neq 0$, and $v = [(1,0)]$ is a sum of only one Manin symbol.

3. [Map From Hecke Ring] This step is purely conceptual, since no actual work needs to be done. We illustrate it by computing $\psi(T_1)$ and $\psi(T_2)$. We have

$$\psi(T_1) = \pi(v) = (1,0)^t,$$

and

$$\psi(T_2) = \pi(T_2(v)) = \pi((0,0,1/2)^t) = (0,1/2)^t.$$

4. [Find Generator] We have

$$\psi(T_2^0) = \psi(T_1) = (1,0)^t,$$

which is clearly independent from $\psi(T_2) = (0,1/2)^t$. Thus we find that the image of the powers of $T = T_2$ generate V.

5. [Characteristic Polynomial] It is easy to compute the characteristic polynomial of a 2×2 matrix. The matrix of $T_2|_V$ is $\left(\begin{smallmatrix} 0 & 2 \\ 1/2 & -1 \end{smallmatrix}\right)$, which has characteristic polynomial $f = x^2 + x - 1$. Of course, we already knew this because we computed V as the kernel of $T_2^2 + T_2 - 1$.

6. [Field Structure] We have

$$\psi(T_2^0) = \pi(v) = (1,0)^t \text{ and } \psi(T_2) = (0,1/2).$$

The matrix with rows the $\psi(T_2^i)$ is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/2 \end{smallmatrix}\right)$, which has inverse $e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$. The matrix e defines an isomorphism between V and the field

$$L = \mathbb{Q}[x]/(f) = \mathbb{Q}((-1+\sqrt{5})/2).$$

For example, $e((1,0)) = 1$ and $e((0,1)) = 2x$, where $x = (-1+\sqrt{5})/2$.

7. [Hecke Eigenvalues] We have $a_n = e(\Psi(T_n))$. For example,

$$\begin{aligned}
a_1 &= e(\Psi(T_1)) = e((1,0)) = 1 \\
a_2 &= e(\Psi(T_2)) = e((0,1/2)) = x \\
a_3 &= e(\Psi(T_3)) = e(\pi(T_3(v))) = e(\pi((0,-1,-1)^t)) = e((-1,-1)^t) = -1-2x \\
a_4 &= e(\Psi(T_4)) = e(\pi((0,-1,-1/2)^t)) = e((-1,-1/2)^t) = -1-x \\
a_5 &= e(\Psi(T_5)) = e(\pi((0,0,1)^t)) = e((0,1)^t) = 2x \\
a_{23} &= e(\Psi(T_{23})) = e(\pi((0,1,0)^t)) = e((1,0)^t) = 1 \\
a_{97} &= e(\Psi(T_{23})) = e(\pi((0,14,3)^t)) = e((14,3)^t) = 14+6x
\end{aligned}$$

It is difficult to appreciate this algorithm without seeing how big the coefficients of the power series expansion of a newform typically are, when the newform is defined over a large field. For such examples, please browse [Ste04].

9.4 Exercises

9.1 Prove that the group $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$, and the quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$.

9.2 Prove that the operators $\langle d\rangle$ are elements of $\mathbb{Z}[\ldots, T_n, \ldots]$. [Hint: Use Dirichlet's theorem on primes in arithmetic progression.]