Chapter 3

Modular Symbols of Weight Two

We saw in Chapter 2 (especially Section 2.2) that we can compute each space $M_k(\mathrm{SL}_2(\mathbb{Z}))$ explicitly. This involved computing Eisenstein series E_4 and E_6 to some precision, then forming the basis $\{E_4^a E_6^b : 4a + 6b = k, 0 \le a, b \in \mathbb{Z}\}$ for $M_k(\mathrm{SL}_2(\mathbb{Z}))$. In this chapter we instead consider the problem of computing $M_2(\Gamma_0(N))$, for positive integers N. Again we have a decomposition

$$M_2(\Gamma_0(N)) = S_2(\Gamma_0(N)) \oplus \mathrm{Eis}_2(\Gamma_0(N)),$$

where $\mathrm{Eis}_2(\Gamma_0(N))$ is a space spanned by explicit generalized Eisenstein series and $S_2(\Gamma_0(N))$ is the space of cusp forms, i.e., elements of $M_2(\Gamma_0(N))$ that vanish at all cusps.

The space $\mathrm{Eis}_2(\Gamma_0(N))$ can be computed explicitly much like $M_k(\mathrm{SL}_2(\mathbb{Z}))$, as we will see in Chapter 5. On the other hand, general elements of $S_2(\Gamma_0(p))$ can not be written as sums or products of generalized Eisenstein series. In fact, the structure of $M_2(\Gamma_0(N))$ is drastically different than that of $M_k(\mathrm{SL}_2(\mathbb{Z}))$. For example, when p is a prime $\mathrm{Eis}_2(\Gamma_0(p))$ has dimension 1, whereas $S_2(\Gamma_0(p))$ has dimension about $p/12$.

Fortunately an idea of Birch called "modular symbols" provides a powerful method for computing $S_2(\Gamma_0(N))$, and indeed much more. In this chapter, we explain how $S_2(\Gamma_0(N))$ is related to modular symbols, and how to use this relationship to explicitly compute a basis for $S_2(\Gamma_0(N))$. We will discuss much more general modular symbols in Chapter 8, where we will explain how to use them to compute $S_k(\Gamma_1(N))$ for any integers $k \ge 2$ and N.

Section 3.1 contains a brief summary of basic facts about modular forms, Hecke operators, and integral homology. Section 3.2 introduces modular symbols, and describes how to compute with them. Section 3.3 outlines an algorithm for constructing cusp forms using modular symbols in conjunction with Atkin-Lehner theory.

This chapter assumes some familiarity with algebraic curves, Riemann surfaces, and homology groups of compact Riemann surfaces.

3.1 Review of modular forms and Hecke operators

The group $\Gamma_0(N)$ acts on $\mathfrak{h}^*$ by linear fractional transformations, and the quotient $\Gamma_0(N)\backslash\mathfrak{h}^*$ is a Riemann surface, which we denote by $X_0(N)$. Shimura showed in [Shi94, §6.7] that $X_0(N)$ has a canonical structure of algebraic curve over $\mathbb{Q}$.

Recall from Section 1.3 that a cusp form of weight 2 for $\Gamma_0(N)$ is a function f on $\mathfrak{h}$ such that $f(z)dz$ defines a holomorphic differential on $X_0(N)$. Equivalently, a cusp form is a holomorphic function f on $\mathfrak{h}$ such that

(a) the expression $f(z)dz$ is invariant under replacing z by $\gamma(z)$ for each $\gamma \in \Gamma_0(N)$, and

(b) $f(z)$ vanishes at every cusp for $\Gamma_0(N)$.

The space $S_2(\Gamma_0(N))$ of weight 2 cusp forms on $\Gamma_0(N)$ is a finite dimensional complex vector space, of dimension equal to the genus g of $X_0(N)$. Viewed topologically, as a 2-dimensional real manifold, $X_0(N)(\mathbb{C})$ is a g-holed torus (see Figure 3.1.1 on page 32).

Condition (b) in the definition of $f(z)$ means that $f(z)$ has a Fourier expansion about each element of $\mathbb{P}^1(\mathbb{Q})$. Thus, at ∞ we have

$$\begin{aligned} f(z) &= a_1 e^{2\pi i z} + a_2 e^{2\pi i 2z} + a_3 e^{2\pi i 3z} + \cdots \\ &= a_1 q + a_2 q^2 + a_3 q^3 + \cdots, \end{aligned}$$

where, for brevity, we write $q = q(z) = e^{2\pi i z}$.

Example 3.1.1. Let E be the elliptic curve defined by the equation $y^2 + xy = x^3 + x^2 - 4x - 5$. Let $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$, where $\tilde{E}$ is the reduction of E mod p (note that for the bad primes we have $a_3 = -1$, $a_{13} = 1$). For n composite, define a_n using the relations at the end of Section 3.3. Then

$$\begin{aligned} f &= q + a_2 q^2 + a_3 q^3 + a_4 q^4 + a_5 q^5 + \cdots \\ &= q + q^2 - q^3 - q^4 + 2q^5 + \cdots \end{aligned}$$

is the q-expansion of a modular form on $\Gamma_0(39)$. The Shimura-Taniyama conjecture, which is now a theorem (see [BCDT01]) asserts that any q-expansion constructed as above from an elliptic curve over $\mathbb{Q}$ is a modular form.

Just as is the case for level 1 modular forms (see Section 2.4) there is a family of commuting Hecke operators that act on $S_2(\Gamma_0(N))$. To define them conceptually, we introduce an interpretation of $X_0(N)$ as a space whose points *parameterize* elliptic curves with extra structure.

Proposition 3.1.2. *The complex points of the open subcurve $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{h}$ are in natural bijection with pairs (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of $E(\mathbb{C})$ of order N.*

Suppose n and N are coprime positive integers. Keeping in mind Proposition 3.1.2, we see that there are two natural maps π_1 and π_2 from $Y_0(n\cdot N)$ to $Y_0(N)$; the first, π_1, sends a pair (E, C) to (E, C'), where C' is the unique cyclic subgroup of C of order N, and the second, π_2, sends a point $(E, C) \in Y_0(N)(\mathbb{C})$ to $(E/D, C/D)$, where D is the unique cyclic subgroup of C of order n. These maps extend in a unique way to algebraic maps from $X_0(n\cdot N)$ to $X_0(N)$:

$$\begin{tikzcd} & X_0(n\cdot N) \arrow[dl, "\pi_2"'] \arrow[dr, "\pi_1"] & \\ X_0(N) & & X_0(N). \end{tikzcd}$$

The nth *Hecke operator* T_n is $(\pi_1)_* \circ (\pi_2)^*$, where π_2^* and $(\pi_1)_*$ denote pullback and pushforward of differentials respectively. (There is a similar definition of T_n when $\gcd(n, N) \neq 1$.) Using our interpretation of $S_2(\Gamma_0(N))$ as differentials on $X_0(N)$ this gives an action of Hecke operators on $S_2(\Gamma_0(N))$. One can show that these induce the maps of Proposition 2.4.6 on q-expansions.

Example 3.1.3. There is a basis of $S_2(39)$ so that

$$T_2 = \begin{pmatrix} 1 & 1 & 0 \\ -2 & -3 & -2 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad T_5 = \begin{pmatrix} -4 & -2 & -6 \\ 4 & 4 & 4 \\ 0 & 0 & 2 \end{pmatrix}.$$

Notice that these matrices commute, and that 1 is an eigenvalue of T_2, and 2 is an eigenvalue of T_5.

The first homology group $\mathrm{H}_1(X_0(N), \mathbb{Z})$ is the group of closed 1-cycles modulo boundaries of 2 cycles (formal sums of images of 2-simplexes). Recall that topologically $X_0(N)$ is a g-holed torus, where g is the genus of $X_0(N)$. The group $\mathrm{H}_1(X_0(N), \mathbb{Z})$ is thus a free abelian group of rank $2g$ (see, e.g., [GH81, Ex. 19.30]), with two generators corresponding to each hole, as illustrated in the case $N = 39$ in Figure 3.1.1.

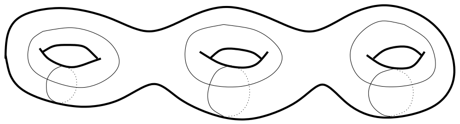
Homology is closely connected to modular forms, since the Hecke operators T_n also act on $\mathrm{H}_1(X_0(N), \mathbb{Z})$. The action is by pullback of homology classes by π_2 followed by taking the image under π_1. Moreover, integration defines a pairing

$$\langle\, ,\, \rangle : S_2(\Gamma_0(N)) \times H_1(X_0(N), \mathbb{Z}) \to \mathbb{C}. \tag{3.1.1}$$

Explicitly, for a path x,

$$\langle f, x\rangle = 2\pi i \int_x f(z)dz,$$

where the integral is locally a complex line integral along preimages of intervals of x in the upper half plane.



$$\mathrm{H}_1(X_0(39), \mathbb{Z}) \cong \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$$

Figure 3.1.1: The homology of $X_0(39)$.

Theorem 3.1.4. *The pairing (3.1.1) is nondegenerate and Hecke equivariant in the sense that for every Hecke operator T_n, we have $\langle fT_n, x\rangle = \langle f, T_n x\rangle$.*

As we will see, modular symbols allow us to make explicit the action of the Hecke operators on $\mathrm{H}_1(X_0(N), \mathbb{Z})$; the above pairing then translates this into a wealth of information about cusp forms.

3.2 Modular symbols

The modular symbols formalism provides a presentation of $\mathrm{H}_1(X_0(N), \mathbb{Z})$ in terms of paths between elements of $\mathbb{P}^1(\mathbb{Q})$. Furthermore, a trick due to Manin gives an explicit finite list of generators and relations for the space of modular symbols.

The *modular symbol* defined by a pair $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$ is denoted $\{\alpha, \beta\}$. As illustrated in Figure 3.2.1, we view this modular symbol as the homology class, relative to the cusps, of a (geodesic) path from α to β in $\mathfrak{h}^*$. The homology group relative to the cusps is a slight enlargement of the usual homology group, in that we allow paths with endpoints in the cusps instead of restricting to closed loops.

Note that modular symbols satisfy the following homology relations: if $\alpha, \beta, \gamma \in \mathbb{Q} \cup \{\infty\}$, then

$$\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0.$$

Furthermore, the space of modular symbols is torsion free, so, e.g., $\{\alpha, \alpha\} = 0$ and $\{\alpha, \beta\} = -\{\beta, \alpha\}$.

Denote by $\mathbb{M}_2$ the free abelian group with basis the set of symbols $\{\alpha, \beta\}$ modulo the three-term homology relations above and modulo any torsion. There is a left action of $\mathrm{GL}_2(\mathbb{Q})$ on $\mathbb{M}_2$, whereby a matrix g acts by

$$g\{\alpha, \beta\} = \{g(\alpha), g(\beta)\},$$

and g acts on α and β by a linear fractional transformation. The space $\mathbb{M}_2(\Gamma_0(N))$ of *modular symbols for* $\Gamma_0(N)$ is the quotient of $\mathbb{M}_2$ by the submodule generated by the infinitely many elements of the form $x - g(x)$, for x in $\mathbb{M}_2$ and g in

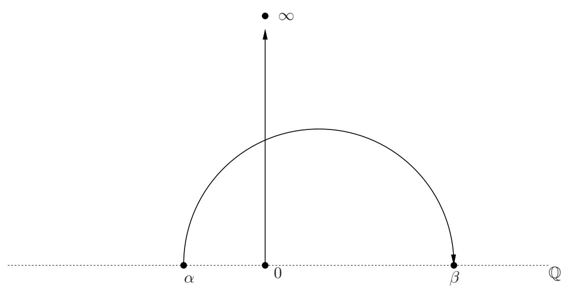


Figure 3.2.1: The modular symbols $\{\alpha, \beta\}$ and $\{0, \infty\}$.

$\Gamma_0(N)$, and modulo any torsion. A *modular symbol for* $\Gamma_0(N)$ is an element of this space. We frequently denote the equivalence class that defines a modular symbol by giving a representative element.

Example 3.2.1. Some modular symbols are 0 no matter what the level N is! For example, since $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, we have

$$\{\infty, 0\} = \{\gamma(\infty), \gamma(0)\} = \{\infty, 1\},$$

so

$$0 = \{\infty, 1\} - \{\infty, 0\} = \{\infty, 1\} + \{0, \infty\} = \{0, \infty\} + \{\infty, 1\} = \{0, 1\}.$$

There is a natural homomorphism

$$\varphi : \mathbb{M}_2(\Gamma_0(N)) \to \mathrm{H}_1(X_0(N), \{\text{cusps}\}, \mathbb{Z}) \qquad (3.2.1)$$

that sends a formal linear combination of geodesic paths in the upper half plane to their image as paths on $X_0(N)$. In [Man72] Manin proved that (3.2.1) is an isomorphism. He also identified the subspace of $\mathbb{M}_2(\Gamma_0(N))$ that is sent isomorphically onto $\mathrm{H}_1(X_0(N), \mathbb{Z})$. This subspace is constructed as follows. Let $\mathbb{B}_2(\Gamma_0(N))$ denote the free abelian group whose basis is the finite set $C(\Gamma_0(N)) = \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$ of cusps for $\Gamma_0(N)$. The *boundary map*

$$\delta : \mathbb{M}_2(\Gamma_0(N)) \to \mathbb{B}_2(\Gamma_0(N))$$

sends $\{\alpha, \beta\}$ to $\{\beta\} - \{\alpha\}$, where $\{\beta\}$ denotes the basis element of $\mathbb{B}_2(\Gamma_0(N))$ corresponding to $\beta \in \mathbb{P}^1(\mathbb{Q})$. The kernel $\mathbb{S}_2(\Gamma_0(N))$ of δ is the subspace of

cuspidal modular symbols. An element of $\mathbb{S}_2(\Gamma_0(N))$ can be thought of as a linear combination of paths in $\mathfrak{h}^*$ whose endpoints are cusps, and whose images in $X_0(N)$ are a linear combination of loops.

Theorem 3.2.2 (Manin)**.** *The map φ given above induces a canonical isomorphism*

$$\mathbb{S}_2(\Gamma_0(N)) \cong \mathrm{H}_1(X_0(N), \mathbb{Z}).$$

Example 3.2.3. We illustrate modular symbols in the case when $N = 11$. Using SAGE we find that $\mathbb{M}_2(11)$ has basis $\{\infty, 0\}$, $\{-1/8, 0\}$, $\{-1/9, 0\}$:

```
sage: M = ModularSymbols(11, 2)
sage: print [b.modular_symbol_rep() for b in M.basis()]
[{Infinity,0}, {-1/8,0}, {-1/9,0}]
```

The integral homology $\mathrm{H}_1(X_0(11), \mathbb{Z})$ corresponds to the abelian subgroup generated by $\{-1/7, 0\}$ and $\{-1/5, 0\}$.

3.2.1 Manin's trick

In this section, we describe a trick of Manin that shows that the space of modular symbols can be computed.

The group $\Gamma_0(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$ (see Exercise 1.6). Let $r_0, r_1, \ldots, r_m$ be distinct right coset representatives for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, so that

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(N)r_0 \cup \Gamma_0(N)r_1 \cup \cdots \cup \Gamma_0(N)r_m,$$

where the union is disjoint. For example, when N is prime, a list of coset representatives is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ N-1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Let

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \{(a : b) \;:\; a, b \in \mathbb{Z}/N\mathbb{Z},\ \gcd(a, b, N) = 1\}/\sim$$

where $(a : b) \sim (a' : b')$ if there is $u \in (\mathbb{Z}/N\mathbb{Z})^*$ such that $a = ua', b = ub'$.

Proposition 3.2.4. *There is a bijection between $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ and the right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, which sends a coset representative $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to the class of $(c : d)$ in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.*

Proof. See Exercise 3.1. □

We now describe an observation of Manin (see [Man72, §1.5]) that is crucial to making $\mathbb{M}_2(\Gamma_0(N))$ computable. It allows us to write any modular symbol $\{\alpha, \beta\}$ as a $\mathbb{Z}$-linear combination of symbols of the form $r_i\{0, \infty\}$, where the $r_i \in \mathrm{SL}_2(\mathbb{Z})$ are coset representatives as above. In particular, the finitely many symbols $r_0\{0, \infty\}, \ldots r_m\{0, \infty\}$ generate $\mathbb{M}_2(\Gamma_0(N))$.

Proposition 3.2.5 (Manin). *Let N be a positive integer and $r_0, \ldots, r_m$ a set of right coset representatives for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Every $\{\alpha, \beta\} \in \mathbb{M}_2(\Gamma_0(N))$ is a $\mathbb{Z}$-linear combination of $r_0\{0,\infty\}, \ldots r_m\{0,\infty\}$.*

We give two proofs of the proposition. The first is useful for actual computation (see [Cre97a, §2.1.6]); the second seems less useful for computation but is easy to understand conceptually (see [MTT86, §2]).

Continued Fractions Proof of Proposition 3.2.5. Because of the relation $\{\alpha, \beta\} = \{0, \beta\} - \{0, \alpha\}$, it suffices to consider modular symbols of the form $\{0, b/a\}$, where the rational number b/a is in lowest terms. Expand b/a as a continued fraction and consider the successive convergents in lowest terms:

$$\frac{b_{-2}}{a_{-2}} = \frac{0}{1}, \quad \frac{b_{-1}}{a_{-1}} = \frac{1}{0}, \quad \frac{b_0}{a_0} = \frac{b_0}{1}, \ldots, \quad \frac{b_{n-1}}{a_{n-1}}, \quad \frac{b_n}{a_n} = \frac{b}{a}$$

where the first two are added formally. Then

$$b_k a_{k-1} - b_{k-1} a_k = (-1)^{k-1},$$

so that

$$g_k = \begin{pmatrix} b_k & (-1)^{k-1} b_{k-1} \\ a_k & (-1)^{k-1} a_{k-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Hence

$$\left\{ \frac{b_{k-1}}{a_{k-1}}, \frac{b_k}{a_k} \right\} = g_k\{0,\infty\} = r_i\{0,\infty\},$$

for some i, is of the required special form. Since

$$\{0, b/a\} = \{0,\infty\} + \{\infty, b_0\} + \left\{ \frac{b_0}{1}, \frac{b_1}{a_1} \right\} + \cdots + \left\{ \frac{b_{n-1}}{a_{n-1}}, \frac{b_n}{a_n} \right\},$$

this completes the proof. □

Inductive Proof of Proposition 3.2.5. As in the first proof it suffices to prove the proposition for any symbol $\{0, b/a\}$, where b/a is in lowest terms. We will induct on $a \in \mathbb{Z}_{\geq 0}$. If $a = 0$ then the symbol is $\{0, \infty\}$, which corresponds to the identity coset, so assume that $a > 0$. Find $a' \in \mathbb{Z}$ such that

$$ba' \equiv 1 \pmod{a},$$

and set $b' = (ba' - 1)/a$. Then the matrix

$$\delta = \begin{pmatrix} b & b' \\ a & a' \end{pmatrix}$$

is an element of $\mathrm{SL}_2(\mathbb{Z})$, so $\delta = \gamma \cdot r_j$ for some right coset representative r_j and $\gamma \in \Gamma_0(N)$. Then

$$\{0, b/a\} - \{0, b'/a'\} = \{b'/a', b/a\} = \begin{pmatrix} b & b' \\ a & a' \end{pmatrix} \cdot \{0,\infty\} = r_j\{0,\infty\}.$$

By induction $\{0, b'/a'\}$ is a linear combination of symbols of the form $r_k\{0,\infty\}$, which completes the proof. □

Example 3.2.6. Let $N = 11$, and consider the modular symbol $\{0, 4/7\}$. We have

$$\frac{4}{7} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}},$$

so the partial convergents are

$$\frac{b_{-2}}{a_{-2}} = \frac{0}{1}, \quad \frac{b_{-1}}{a_{-1}} = \frac{1}{0}, \quad \frac{b_0}{a_0} = \frac{0}{1}, \quad \frac{b_1}{a_1} = \frac{1}{1}, \quad \frac{b_2}{a_2} = \frac{1}{2}, \quad \frac{b_3}{a_3} = \frac{4}{7}.$$

Thus, noting as in Example 3.2.1 that $\{0, 1\} = 0$, we have

$$\begin{aligned} \{0, 4/7\} &= \{0,\infty\} + \{\infty, 0\} + \{0, 1\} + \{1, 1/2\} + \{1/2, 4/7\} \\ &= \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \{0,\infty\} + \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix} \{0,\infty\} \\ &= \begin{pmatrix} 1 & 0 \\ 9 & 1 \end{pmatrix} \{0,\infty\} + \begin{pmatrix} 1 & 0 \\ 9 & 1 \end{pmatrix} \{0,\infty\} \\ &= 2 \cdot \left[\begin{pmatrix} 1 & 0 \\ 9 & 1 \end{pmatrix} \{0,\infty\} \right] \end{aligned}$$

3.2.2 Manin symbols

As above, fix coset representatives $r_0, \ldots, r_m$ for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Denote the modular symbol $r_i\{0,\infty\}$ by $[r_i]$. The symbols $[r_0], \ldots, [r_m]$ are called *Manin symbols*, and they are equipped with a right action of $\mathrm{SL}_2(\mathbb{Z})$, which is given by $[r_i]g = [r_j]$, where $\Gamma_0(N) r_j = \Gamma_0(N) r_i g$. Note that Manin symbols are nothing more than modular symbols of the form $r_i\{0,\infty\}$.

Theorem 1.1.2 implies that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the two matrices $\sigma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Note that $\sigma = S$ from that theorem and $\tau = TS$, so $T = \tau\sigma \in \langle \sigma, \tau \rangle$.

The following theorem provides us with a finite presentation for the space of modular symbols.

Theorem 3.2.7 (Manin). *The Manin symbols $[r_0], \ldots, [r_m]$ satisfy the following relations:*

$$[r_i] + [r_i]\sigma = 0$$
$$[r_i] + [r_i]\tau + [r_i]\tau^2 = 0.$$

Furthermore these are all relations in the following sense: if we consider the free abelian group on formal symbols $[r_i]$ modulo the above relations and modulo any torsion, we obtain $\mathbb{M}_2(\Gamma_0(N))$.

Proof. To see that the the first relation holds, note that

$$\begin{aligned} [r_i] + [r_i]\sigma &= \{r_i(0), r_i(\infty)\} + \{r_i\sigma(0), r_i\sigma(\infty)\} \\ &= \{r_i(0), r_i(\infty)\} + \{r_i(\infty), r_i(0)\} \\ &= 0. \end{aligned}$$

For the second relation we have

$$\begin{aligned}[r_i] + [r_i]\tau + [r_i]\tau^2 &= \{r_i(0), r_i(\infty)\} + \{r_i\tau(0), r_i\tau(\infty)\}\{r_i\tau^2(0), r_i\tau^2(\infty)\}\\ &= \{r_i(0), r_i(\infty)\} + \{r_i(\infty), r_i(1)\}\{r_i(1), r_i(0)\}\\ &= 0\end{aligned}$$

The proof that these general all relations (modulo torsion) is deeper; see [Man72, §1.7]. □

3.2.3 Hecke operators on modular symbols

When p is a prime not dividing N, define

$$T_p\{\alpha,\beta\} = \begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix}\{\alpha,\beta\} + \sum_{r \bmod p} \begin{pmatrix} 1 & r\\ 0 & p\end{pmatrix}\{\alpha,\beta\}.$$

As mentioned before, this definition is compatible with the integration pairing $\langle\, ,\rangle$ of Section 3.1, in the sense that $\langle fT_p, x\rangle = \langle f, T_p x\rangle$. When $p \mid N$, the definition is the same, except that the matrix $\left(\begin{smallmatrix} p & 0\\ 0 & 1\end{smallmatrix}\right)$ is not included in the sum. (There is a similar definition of T_n for n composite; see Section 8.3.1 for the general definition.)

For example, when $N = 11$ we have

$$\begin{aligned} T_2\{0, 1/5\} &= \{0, 2/5\} + \{0, 1/10\} + \{1/2, 3/5\}\\ &= -2\{0, 1/5\}.\end{aligned}$$

In [Mer94], L. Merel gives a description of the action of T_p directly on Manin symbols $[r_i]$ (see Section 8.3.2 for details). For example, when $p = 2$ and N is odd, we have

$$T_2([r_i]) = [r_i]\begin{pmatrix} 1 & 0\\ 0 & 2\end{pmatrix} + [r_i]\begin{pmatrix} 2 & 0\\ 0 & 1\end{pmatrix} + [r_i]\begin{pmatrix} 2 & 1\\ 0 & 1\end{pmatrix} + [r_i]\begin{pmatrix} 1 & 0\\ 1 & 2\end{pmatrix}. \qquad (3.2.2)$$

3.3 Computing the space of modular forms

In this section we describe how to use modular symbols to construct a basis of $S_2(\Gamma_0(N))$ consisting of modular forms that are eigenvectors for every element of the ring $\mathbb{T}'$ generated by the Hecke operator T_p, with $p \nmid N$. Such eigenvectors are called *eigenforms*.

Suppose M is a positive integer that divides N. As explained in [Lan95, VIII.1–2], for each divisor d of N/M there is a natural *degeneracy map* $\beta_{M,d}$: $S_2(M) \to S_2(\Gamma_0(N))$ given by $\beta_{M,d}(f(q)) = f(q^d)$. The *new subspace* of $S_2(\Gamma_0(N))$, denoted $S_2(\Gamma_0(N))^{\mathrm{new}}$, is the complementary $\mathbb{T}$-submodule of the $\mathbb{T}$-module generated by the images of all maps $\beta_{M,d}$, with M and d as above. (It is a nontrivial fact that this complement is well defined; one possible proof uses the Petersson inner product.)

The theory of Atkin and Lehner [AL70] (see Section 6.1.1) asserts that, as a $\mathbb{T}'$-module, $S_2(\Gamma_0(N))$ decomposes as follows:

$$S_2(\Gamma_0(N)) \quad = \bigoplus_{M\mid N,\ d\mid N/M} \beta_{M,d}(S_2(M)^{\mathrm{new}}).$$

To compute $S_2(\Gamma_0(N))$ it thus suffices to compute $S_2(M)^{\mathrm{new}}$ for each positive divisor M of N.

We now turn to the problem of computing $S_2(\Gamma_0(N))^{\mathrm{new}}$. Atkin and Lehner [AL70] also proved that $S_2(\Gamma_0(N))^{\mathrm{new}}$ is spanned by eigenforms, each of which occurs with multiplicity one in $S_2(\Gamma_0(N))^{\mathrm{new}}$. Moreover, if $f \in S_2(\Gamma_0(N))^{\mathrm{new}}$ is an eigenform then the coefficient of q in the q-expansion of f is nonzero, so it is possible to normalize f so that coefficient of q is 1. With f so normalized, if $T_p(f) = a_p f$, then the pth Fourier coefficient of f is a_p. If $f = \sum_{n=1}^\infty a_n q^n$ is a normalized eigenvector for all T_p, then the a_n, with n composite, are determined by the a_p, with p prime, by the following formulas: $a_{nm} = a_n a_m$ when n and m are relatively prime, and $a_{p^r} = a_{p^{r-1}} a_p - p a_{p^{r-2}}$ for $p \nmid N$ prime. When $p \mid N$, $a_{p^r} = a_p^r$. We conclude that in order to compute $S_2(\Gamma_0(N))^{\mathrm{new}}$, it suffices to compute all systems of eigenvalues $\{a_2, a_3, a_5, \ldots\}$ of the Hecke operators $T_2, T_3, T_5, \ldots$ acting on $S_2(\Gamma_0(N))^{\mathrm{new}}$. Given a system of eigenvalues, the corresponding eigenform is $f = \sum_{n=1}^\infty a_n q^n$, where the a_n, for n composite, are determined by the recurrence given above.

In light of the pairing $\langle\, ,\rangle$ introduced in Section 3.1, computing the above systems of eigenvalues $\{a_2, a_3, a_5, \ldots\}$ amounts to computing the systems of eigenvalues of the Hecke operators T_p on the subspace V of $\mathbb{S}_2(\Gamma_0(N))$ that corresponds to the new subspace of $S_2(\Gamma_0(N))$. For each proper divisor M of N and each divisor d of N/M, let $\phi_{M,d} : \mathbb{S}_2(\Gamma_0(N)) \to \mathbb{S}_2(\Gamma_0(M))$ be the map sending x to $\left(\begin{smallmatrix} d & 0\\ 0 & 1\end{smallmatrix}\right)x$. Then V is the intersection of the kernels of all maps $\phi_{M,d}$.

The computation of the systems of eigenvalues of a collection of commuting diagonalizable endomorphisms involves standard linear algebra techniques, such as computation of characteristic polynomials and kernels of matrices. There are, however, several tricks that greatly speed up this process, some of which are described in Chapter 7.

Example 3.3.1. All forms in $S_2(\Gamma_0(39))$ are new. Up to Galois conjugacy, the eigenvalues of the Hecke operators T_2, T_3, T_5, and T_7 on $\mathbb{S}_2(\Gamma_0(39))$ are $\{1, -1, 2, -4\}$ and $\{a, 1, -2a-2, 2a+2\}$, where $a^2 + 2a - 1 = 0$. Each of these eigenvalues occur in $\mathbb{S}_2(\Gamma_0(39))$ with multiplicity two; for example, the characteristic polynomial of T_2 on $\mathbb{S}_2(\Gamma_0(39))$ is $(x-1)^2 \cdot (x^2 + 2x - 1)^2$. Thus $S_2(\Gamma_0(39))$ is spanned by

$$\begin{aligned} f_1 &= q + q^2 - q^3 - q^4 + 2q^5 - q^6 - 4q^7 + \cdots,\\ f_2 &= q + aq^2 + q^3 + (-2a-1)q^4 + (-2a-2)q^5 + aq^6 + (2a+2)q^7 + \cdots,\end{aligned}$$

and the Galois conjugate of f_2.

3.3.1 Summary

To compute the q-expansion, to some precision, of each eigenforms in $S_2(\Gamma_0(N))$, we use the degeneracy maps so that we only have to solve the problem for $S_2(\Gamma_0(N))^{\text{new}}$. Here, using modular symbols, we compute all systems of eigenvalues $\{a_2, a_3, a_5, \ldots\}$, then write down each of the corresponding eigenforms $f = q + a_2q^2 + q_3q^3 + \cdots$.

3.4 Exercises

3.1 Let p be a prime.

(a) List representative elements of $\mathbb{P}^1(\mathbb{Z}/3\mathbb{Z})$.

(b) What is the cardinality of $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ as a function of p?

(c) Prove that there is a bijection between the right cosets of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ and the elements of $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. (As mentioned in this chapter this is also true for composite level; see [Cre97a, §2.2] for complete details.)

3.2 Use the inductive proof of Proposition 3.2.5 to write $\{0, 4/7\}$ in terms of Manin symbols.

3.3 Show that the Hecke operator T_2 acts as multiplication by 3 on the space $\mathbb{M}_2(\Gamma_0(3))$ as follows:

(a) Write down right coset representatives for $\Gamma_0(3)$ in $\mathrm{SL}_2(\mathbb{Z})$.

(b) List all 8 relations coming from 3.2.7.

(c) Find a single Manin symbols $[r_i]$ so that the three other Manin symbols are a nonzero multiple of $[r_i]$ modulo the relations found in the previous step.

(d) Use formula (3.2.2) to compute the image of your symbol $[r_i]$ under T_2. You will obtain a sum of four symbols. Using the relations above, write this sum as a multiple of $[r_i]$. (The multiple must be 3 or you made a mistake.)