3.2 Modular Symbols

Modular symbols provide a "combinatorial" and computable presentation of $\mathrm{H}_1(X_0(N), \mathbb{Z})$ in terms of paths between elements of $\mathbb{P}^1(\mathbb{Q})$.

We denote the *modular symbol* defined by a pair $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$ by $\{\alpha, \beta\}$. 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 $\mathrm{H}_1(X_0(N), \mathbb{Z}; \{\text{cusps}\})$ of $X_0(N)$ *relative to the cusps* is an enlargement of the usual homology group, in that we allow paths with endpoints in the cusps instead of restricting to closed loops.

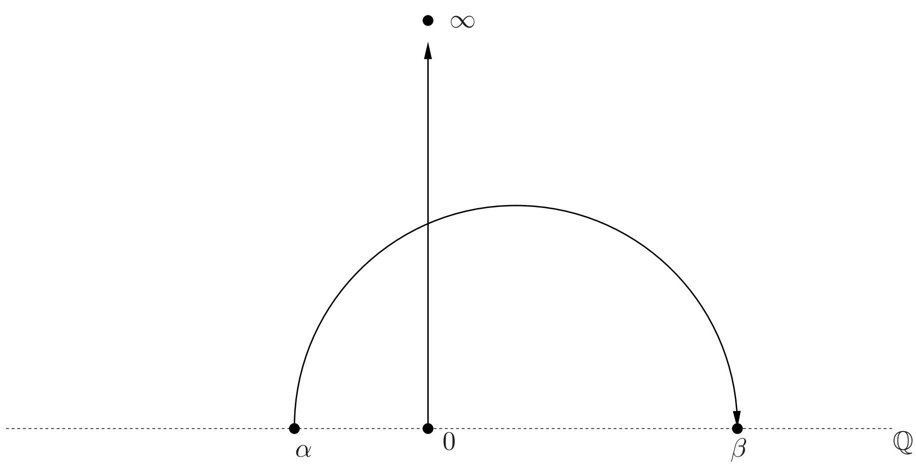

Figure 3.2.1: The modular symbols $\{\alpha, \beta\}$ and $\{0, \infty\}$.

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

$$\{\alpha, \alpha\} = 0 \qquad \text{and} \qquad \{\alpha, \beta\} = -\{\beta, \alpha\}.$$

Let $\mathbb{M}_2$ be the free abelian group with basis the set of symbols $\{\alpha, \beta\}$ modulo the 3-term homology relations above and modulo any torsion. Define a left action of $\mathrm{GL}_2(\mathbb{Q})$ on $\mathbb{M}_2$ by letting $g \in \mathrm{GL}_2(\mathbb{Q})$ act by

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

and g acts on α and β via the corresponding 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 $\Gamma_0(N)$, 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

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

See Exercise 3.2 for a generalization of this observation.

There is a natural homomorphism

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

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 (this is a fairly involved topological argument).

Manin also identified the subspace of $\mathbb{M}_2(\Gamma_0(N))$ that is sent isomorphically onto $\mathrm{H}_1(X_0(N), \mathbb{Z})$. 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. Thus 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 homologous to a $\mathbb{Z}$-linear combination of closed paths.

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

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

For any (commutative) ring R let

$$\mathbb{M}_2(\Gamma_0(N), R) = \mathbb{M}_2(\Gamma_0(N)) \otimes_{\mathbb{Z}} R,$$

and

$$\mathbb{S}_2(\Gamma_0(N), R) = \mathbb{S}_2(\Gamma_0(N)) \otimes_{\mathbb{Z}} R.$$

Example 3.2.3. We illustrate modular symbols in the case when $N = 11$. Using SAGE, which implements the Manin symbols algorithm that we describe below over $\mathbb{Q}$, we find that $\mathbb{M}_2(\Gamma_0(11), \mathbb{Q})$ has basis $\{\infty, 0\}$, $\{-1/8, 0\}$, $\{-1/9, 0\}$:

```
sage: set_modsym_print_mode ('modular')
sage: M = ModularSymbols(11, 2)
sage: 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 $\{-1/8, 0\}$ and $\{-1/9, 0\}$.

```
sage: S = M.cuspidal_submodule()
sage: S.integral_basis()     # basis over ZZ.
({-1/8,0}, {-1/9,0})
```

3.3 Computing with Modular Symbols

3.3.1 Manin's Trick

In this section, we describe a trick of Manin that proves 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 $r_0, r_1, \dots, r_m$ 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

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

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 3.3.1. *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 3.3. □

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 $r_0\{0, \infty\}, \dots r_m\{0, \infty\}$ generate $\mathbb{M}_2(\Gamma_0(N))$.

Proposition 3.3.2 (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 3.3.2. 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 included 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 3.3.2. 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

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

then $b' = (ba' - 1)/a \in \mathbb{Z}$ so the matrix

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

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

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

as elements of $\mathcal{M}_2(\Gamma_0(N))$. By induction $\{0, b'/a'\}$ is a linear combination of symbols of the form $r_k\{0, \infty\}$, which completes the proof. □

Example 3.3.3. 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

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

3.3.2 Manin symbols

As above, fix coset representatives $r_0, \ldots, r_m$ for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Consider formal symbols $[r_i]'$ for $i = 0, \ldots, m$. Let $[r_i]$ be the modular symbol $r_i\{0, \infty\} = \{r_i(0), r_i(\infty)\}$. We equip the symbols $[r_0]', \ldots, [r_m]'$ with a right action of $\mathrm{SL}_2(\mathbb{Z})$, which is given by $[r_i]'.g = [r_j]'$, where $\Gamma_0(N)r_j = \Gamma_0(N)r_i g$. We extend the notation by writing $[\gamma]' = [\Gamma_0(N)\gamma]' = [r_i]'$, where $\gamma \in \Gamma_0(N)r_i$. Then the right action of $\Gamma_0(N)$ is simply $[\gamma]'.g = [\gamma g]'$.

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 Theorem 1.1.2 and $\tau = TS$, so $T = \tau\sigma \in \langle \sigma, \tau \rangle$.

The following theorem provides us with a finite presentation for the space $\mathcal{M}_2(\Gamma_0(N))$ of modular symbols.

Theorem 3.3.4 (Manin)**.** *Consider the quotient M of the free abelian group on Manin symbols $[r_0]', \ldots, [r_m]'$ modulo the subgroup generated by the elements (for all i):*

$$[r_i]' + [r_i]'\sigma \qquad \textit{and} \qquad [r_i]' + [r_i]'\tau + [r_i]'\tau^2,$$

and modulo any torsion. Then there is an isomorphism $\Psi : M \xrightarrow{\sim} \mathbb{M}_2(\Gamma_0(N))$ given by $[r_i]' \mapsto [r_i] = r_i\{0, \infty\}$.

Proof. We will only prove that Ψ is surjective; the proof that Ψ is injective requires much more work and will be omitted from this book (see [Man72, §1.7] for a complete proof). [[**Todo: And reference my book with Ribet, or Wiese's work?**]]

Proposition 3.3.2 implies that Ψ is surjective, assuming that Ψ is well defined. We next verify that Ψ is well defined, i.e. that the listed two and three term relations hold in the image. To see that 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

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

□

Example 3.3.5. By default SAGE computes modular symbols spaces over $\mathbb{Q}$, i.e., $\mathbb{M}_2(\Gamma_0(N);\mathbb{Q}) \cong \mathbb{M}_2(\Gamma_0(N)) \otimes \mathbb{Q}$. SAGE represents (weight 2) Manin symbols as pairs (c,d). Here c,d are integers that satisfy $0 \leq c,d < N$; they define a point $(c:d) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, hence a right coset of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ (see Proposition 3.3.1).

Create $\mathbb{M}_2(\Gamma_0(N);\mathbb{Q})$ in SAGE by typing `ModularSymbols(N, 2)`. We then use the SAGE command `manin_generators` to enumerate a list of generators $[r_0], \ldots, [r_n]$ as in Theorem 3.3.4 for several spaces of modular symbols.

```
sage: M = ModularSymbols(2,2)
sage: M
Full Modular Symbols space for Gamma_0(2) of weight 2 with
sign 0 and dimension 1 over Rational Field
sage: M.manin_generators()
[(0,1), (1,0), (1,1)]

sage: M = ModularSymbols(3,2)
sage: M.manin_generators()
[(0,1), (1,0), (1,1), (1,2)]

sage: M = ModularSymbols(6,2)
sage: M.manin_generators()
[(0,1), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5), (2,1),
 (2,3), (2,5), (3,1), (3,2)]
```

Given `x=(c,d)`, the command `x.lift_to_sl2z(N)` finds an element `[a,b,c',d']` of $\mathrm{SL}_2(\mathbb{Z})$ whose lower two entries are congruent to (c,d) modulo N.

```
sage: M = ModularSymbols(2,2)
sage: [x.lift_to_sl2z(2) for x in M.manin_generators()]
[[1, 0, 0, 1], [0, -1, 1, 0], [0, -1, 1, 1]]
sage: M = ModularSymbols(6,2)
sage: x = M.manin_generators()[9]
sage: x
(2,5)
sage: x.lift_to_sl2z(6)
[1, 2, 2, 5]
```

The manin_basis command returns a list of indices into the Manin generator list such that the corresponding symbols form a basis for the quotient of the $\mathbb{Q}$-vector space spanned by Manin symbols modulo the 2 and 3-term relations of Theorem 3.3.4.

```
sage: M = ModularSymbols(2,2)
sage: M.manin_basis()
[1]
sage: [M.manin_generators()[i] for i in M.manin_basis()]
[(1,0)]
sage: M = ModularSymbols(6,2)
sage: M.manin_basis()
[1, 10, 11]
sage: [M.manin_generators()[i] for i in M.manin_basis()]
[(1,0), (3,1), (3,2)]
```

Thus, e.g., every element of $\mathbb{M}_2(\Gamma_0(6))$ is a $\mathbb{Q}$-linear combination of the symbols $[(1,0)]$, $[(3,1)]$, and $[(3,2)]$. We can write each of these as a modular symbol using the modular_symbol_rep function.

```
sage: M.basis()
((1,0), (3,1), (3,2))
sage: [x.modular_symbol_rep() for x in M.basis()]
[{Infinity,0}, {0,1/3}, {-1/2,-1/3}]
```

The manin_gens_to_basis function returns a matrix whose rows express each Manin symbol generator in terms of the subset of Manin symbols that forms a basis (as returned by manin_basis.

```
sage: M = ModularSymbols(2,2)
sage: M.manin_gens_to_basis()
[-1]
[ 1]
[ 0]
```

Since the basis is $(1,0)$ this means that in $\mathbb{M}_2(\Gamma_0(2);\mathbb{Q})$, we have $[(0,1)] = -[(1,0)]$ and $[(1,1)] = 0$. (Since no denominators are involved, we have in fact computed a presentation of $\mathbb{M}_2(\Gamma_0(2);\mathbb{Z})$.)

Convert a Manin symbol $x = (c,d)$ to an element of a modular symbols space M, use `M(xx)`:

```
sage: M = ModularSymbols(2,2)
sage: x = (1,0); M(x)
(1,0)
sage: M( (3,1) )    # entries are reduced modulo $2$ first
0
sage: M( (10,19) )
-(1,0)
```

Next consider $\mathbb{M}_2(\Gamma_0(6);\mathbb{Q})$:

```
sage: M = ModularSymbols(6,2)
sage: M.manin_gens_to_basis()
[-1  0  0]
[ 1  0  0]
[ 0  0  0]
[ 0 -1  1]
[ 0 -1  0]
[ 0 -1  1]
[ 0  0  0]
[ 0  1 -1]
[ 0  0 -1]
[ 0  1 -1]
[ 0  1  0]
[ 0  0  1]
```

Recalling that our choice of basis for $\mathbb{M}_2(\Gamma_0(6);\mathbb{Q})$ is $[(1,0)], [(3,1)], [(3,2)]$. Thus, e.g., first row of this matrix says that $[(0,1)] = -[(1,0)]$, and the fourth row asserts that $[(1,2)] = -[(3,1)] + [(3,2)]$.

```
sage: M = ModularSymbols(6,2)
sage: M((0,1))
-(1,0)
sage: M((1,2))
-(3,1) + (3,2)
```