\[
M = \begin{bmatrix}
a_0 & a_1 & \cdots & a_m \\
\vdots & \ddots & \ddots & \vdots \\
b_0 & b_1 & \cdots & b_n \\
\vdots & \ddots & \ddots & \vdots \\
b_0 & b_1 & \cdots & b_n \\
\end{bmatrix}
\]

\((n \text{ staggered rows of } a_i\text{'s}, \ m \text{ staggered rows of } b_j\text{'s, all other entries } 0)\). The resultant eliminates \(x\), leaving a polynomial in the coefficients that vanishes if and only if \(f\) and \(g\) share a root. Let \(p(x)\) and \(q(x)\) be monic polynomials in \(\mathbb{Q}[x]\). Consider the resultants
\[
\tilde{q}(t, u) = R(p(s), u - s - t; s), \quad r(u) = R(\tilde{q}(t, u), q(t); t).
\]

Show that if \(\alpha\) and \(\beta\) satisfy the polynomials \(p\) and \(q\) then \(\alpha + \beta\) satisfies the polynomial \(r\). Similarly, find polynomials satisfied by \(\alpha \beta\) and \(1/\alpha\) if \(\alpha \neq 0\). (A hint for this exercise is at the end of the book.)

6.4.2. Use the methods of the section or of Exercise 6.4.1 to find a monic integer polynomial satisfied by \(\sqrt{2} + \mu_3\).

6.4.3. Show that \(\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}\). (A hint for this exercise is at the end of the book.)

6.4.4. Show that every algebraic number takes the form of an algebraic integer divided by a rational integer. (A hint for this exercise is at the end of the book.)

6.4.5. Prove Theorem 6.4.5 and its corollaries.

6.5 Algebraic eigenvalues

Returning to the material of Section 6.3, recall the action of the weight-2 Hecke operators \(T = T_p\) and \(T = \langle d \rangle\) on the dual space as composition from the right,
\[
T : \mathcal{S}_2(\Gamma_1(N))^\wedge \to \mathcal{S}_2(\Gamma_1(N))^\wedge, \quad \varphi \mapsto \varphi \circ T,
\]
and recall that the action descends to the quotient \(J_1(N)\). Thus the operators act as endomorphisms on the kernel \(H_1(X_1(N), \mathbb{Z})\), a finitely generated Abelian group. In particular the characteristic polynomial \(f(x)\) of \(T_p\) acting on \(H_1(X_1(N), \mathbb{Z})\) has integer coefficients, and being a characteristic polynomial it is monic. Since an operator satisfies its characteristic polynomial, \(f(T_p) = 0\) on \(H_1(X_1(N), \mathbb{Z})\). Since \(T_p\) is \(\mathbb{C}\)-linear, also \(f(T_p) = 0\) on \(\mathcal{S}_2(\Gamma_1(N))^\wedge\) and so \(f(T_p) = 0\) on \(\mathcal{S}_2(\Gamma_1(N))\). Therefore the characteristic polynomial of \(T_p\) on \(\mathcal{S}_2(\Gamma_1(N))\) divides \(f(x)\) and the eigenvalues of \(T_p\) satisfy \(f(x)\), making them algebraic integers. Since \(p\) is arbitrary this proves
Theorem 6.5.1. Let \( f \in S_2(\Gamma_1(N)) \) be a normalized eigenform for the Hecke operators \( T_p \). Then the eigenvalues \( a_n(f) \) are algebraic integers.

To refine this result we need to view the Hecke operators as lying within an algebraic structure, not merely as a set.

Definition 6.5.2. The Hecke algebra over \( \mathbb{Z} \) is the algebra of endomorphisms of \( S_2(\Gamma_1(N)) \) generated over \( \mathbb{Z} \) by the Hecke operators, 
\[
T_\mathbb{Z} = \mathbb{Z}\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}.
\]

The Hecke algebra \( T_\mathbb{C} \) over \( \mathbb{C} \) is defined similarly.

Each level has its own Hecke algebra, but \( N \) is omitted from the notation since it is usually written somewhere nearby. Clearly any \( f \in S_2(\Gamma_1(N)) \) is an eigenform for all of \( T_\mathbb{C} \) if and only if \( f \) is an eigenform for all Hecke operators \( T_p \) and \( \langle d \rangle \).

For the remainder of this chapter the methods will shift to working with algebraic structure rather than thinking about objects such as Hecke operators one at a time. In particular modules will figure prominently, and so in this context Abelian groups will often be called \( \mathbb{Z} \)-modules. For example, viewing the \( \mathbb{Z} \)-module \( T_\mathbb{Z} \) as a ring of endomorphisms of the finitely generated free \( \mathbb{Z} \)-module \( H_1(X_1(N), \mathbb{Z}) \) shows that it is finitely generated as well (Exercise 6.5.1). Again letting \( f(\tau) = \sum_{n=1}^\infty a_n(f)q^n \) be a normalized eigenform, the homomorphism
\[
\lambda_f : T_\mathbb{Z} \to \mathbb{C}, \quad T f = \lambda_f(T) f
\]
therefore has as its image a finitely generated \( \mathbb{Z} \)-module. Since the image is \( \mathbb{Z}\{a_n(f) : n \in \mathbb{Z}^+\} \) this shows that even though there are infinitely many eigenvalues \( a_n(f) \), the ring they generate has finite rank as a \( \mathbb{Z} \)-module. More specifically, letting
\[
I_f = \ker(\lambda_f) = \{T \in T_\mathbb{Z} : T f = 0 \}
\]
gives a ring and \( \mathbb{Z} \)-module isomorphism (Exercise 6.5.2)
\[
T_\mathbb{Z}/I_f \sim \to \mathbb{Z}\{a_n(f)\}.
\] (6.12)
The image ring sits inside some finite-degree extension field of \( \mathbb{Q} \), i.e., a number field. The rank of \( T_\mathbb{Z}/I_f \) is the degree of this number field as an extension of \( \mathbb{Q} \).

Definition 6.5.3. Let \( f \in S_2(\Gamma_1(N)) \) be a normalized eigenform, \( f(\tau) = \sum_{n=1}^\infty a_n(f)q^n \). The field \( K_f = \mathbb{Q}(\{a_n\}) \) generated by the Fourier coefficients of \( f \) is called the number field of \( f \).
The reader is referred to William Stein’s web site [Ste] and John Cremona’s tables [Cre97] for examples.

Any embedding $\sigma : K_f \hookrightarrow \mathbb{C}$ conjugates $f$ by acting on its coefficients. That is, if $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$ then notating the action with a superscript,

$$f^\sigma(\tau) = \sum_{n=1}^{\infty} a_n^\sigma q^n.$$ 

In fact this action produces another eigenform.

**Theorem 6.5.4.** Let $f$ be a weight 2 normalized eigenform of the Hecke operators, so that $f \in S_2(N, \chi)$ for some $N$ and $\chi$. Let $K_f$ be its number field. For any embedding $\sigma : K_f \hookrightarrow \mathbb{C}$ the conjugated $f^\sigma$ is also a normalized eigenform in $S_2(N, \chi^\sigma)$ where $\chi^\sigma(n) = \chi(n)^\sigma$. If $f$ is a newform then so is $f^\sigma$.

The proof will require two beginning results from commutative algebra, so these are stated first.

**Proposition 6.5.5 (Nakayama’s Lemma).** Suppose that $A$ is a commutative ring with unit and $J \subset A$ is an ideal contained in every maximal ideal of $A$, and suppose that $M$ is a finitely generated $A$-module such that $JM = M$. Then $M = \{0\}$.

**Proof.** Suppose that $M \neq \{0\}$ and let $m_1, \ldots, m_n$ be a minimal set of generators for $M$ over $A$. Since $JM = M$, in particular $m_n \in JM$, giving it the form $m_n = a_1 m_1 + \cdots + a_n m_n$ with all $a_i \in J$. Thus

$$(1 - a_n)m_n = a_1 m_1 + \cdots + a_{n-1} m_{n-1}.$$

But $1 - a_n$ is invertible in $A$, else it sits in a maximal ideal, which necessarily contains $a_n$ as well and therefore is all of $A$, impossible. Thus $m_1, \ldots, m_{n-1}$ is a smaller generating set, and this contradiction proves the lemma. \qed

Again suppose that $A$ is a commutative ring with unit and $J \subset A$ is an ideal, and suppose that $M$ is an $A$-module and a finite-dimensional vector space over some field $k$. The dual space $M^\wedge = \text{Hom}_k(M,k)$ is an $A$-module in the natural way, $a \varphi = \varphi \circ a$ for $a \in A$ and $\varphi \in M^\wedge$ (i.e., $(a \varphi)(m) = \varphi(am)$ for $m \in M$), and similarly for $(M/JM)^\wedge$. Let $M[J]$ be the elements of $M$ annihilated by $J$, and similarly for $M^\wedge[J]$. Then there exist natural isomorphisms of $A$-modules (Exercise 6.5.3)

$$(M/JM)^\wedge \cong M^\wedge[J], \quad M^\wedge/JM^\wedge \cong M[J]^\wedge.$$ (6.13)

Now we can prove Theorem 6.5.4.

**Proof.** The Fourier coefficients $\{a_n\}$ are a system of eigenvalues for the operators $T_n$ acting on $S_2(\Gamma_1(N))$. We need to show that the conjugated coefficients $\{a_n^\sigma\}$ are again a system of eigenvalues.
As explained at the beginning of the section, the action of $\mathbb{T}_\mathbb{Z}$ on $S_2(\Gamma_1(N))$ transfers to the dual space $S_2(\Gamma_1(N))^\wedge$ as composition on the right and then descends to the Jacobian $J_1(N)$, inducing an action on the homology group $H_1(X_1(N), \mathbb{Z})$. This $\mathbb{Z}$-module is free of rank $2g$ where $g$ is the genus of $X_1(N)$ and the dimension of $S_2(\Gamma_1(N))$. Take a homology basis $\{\varphi_1, \ldots, \varphi_{2g}\} \subset S_2(\Gamma_1(N))^\wedge$, so that

$$H_1(X_1(N), \mathbb{Z}) = \mathbb{Z}\varphi_1 \oplus \cdots \oplus \mathbb{Z}\varphi_{2g}. $$

With respect to this basis, each group element $\sum_{j=1}^{2g} n_j \varphi_j$ is represented as an integral row vector $\vec{v} = [n_j] \in \mathbb{Z}^{2g}$ and each $T \in \mathbb{T}_\mathbb{Z}$ is represented by an integral $2g$-by-$2g$ matrix $[T] \in M_{2g}(\mathbb{Z})$, so that the action of $T$ as composition from the right is multiplication by $[T]$, 

$$ T : \vec{v} \mapsto [T] \vec{v}. $$

(6.14)

This action of $\mathbb{T}_\mathbb{Z}$ extends linearly to the free $\mathbb{C}$-module generated by the set $\{\varphi_1, \ldots, \varphi_{2g}\}$, the $2g$-dimensional complex vector space

$$ V = \mathbb{C}\varphi_1 \oplus \cdots \oplus \mathbb{C}\varphi_{2g}. $$

Each element $(z_1 \varphi_1, \ldots, z_{2g} \varphi_{2g})$ is represented by a complex row vector $\vec{v} = [z_j] \in \mathbb{C}^{2g}$, and the action of each $T$ is still described by (6.14). Suppose $\{\lambda(T) : T \in \mathbb{T}_\mathbb{Z}\}$ is a system of eigenvalues of $\mathbb{T}_\mathbb{Z}$ on $V$, i.e., some nonzero $\vec{v} \in \mathbb{C}^{2g}$ satisfies

$$ \vec{v}[T] = \lambda(T)\vec{v}, \quad T \in \mathbb{T}_\mathbb{Z}. $$

Let $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ be any automorphism extending the given embedding $\sigma : \mathbb{K}_f \hookrightarrow \mathbb{C}$. Then $\sigma$ acts on $\vec{v}$ elementwise and fixes the elements of each matrix $[T]$ since it fixes $\mathbb{Q}$. Thus

$$ \vec{v}[T] = (\vec{v}[T])^\sigma = (\lambda(T)\vec{v})^\sigma = \lambda(T)^\sigma \vec{v}^\sigma, \quad T \in \mathbb{T}_\mathbb{Z}, $$

showing that if $\{\lambda(T) : T \in \mathbb{T}_\mathbb{Z}\}$ is a system of eigenvalues on $V$ then so is $\{\lambda(T)^\sigma : T \in \mathbb{T}_\mathbb{Z}\}$. To prove the theorem, this result needs to be transferred from $V$ to $S_2(\Gamma_1(N))$.  

For convenience, abbreviate $S_2(\Gamma_1(N))$ to $S_2$ for the duration of this proof. The space $S_2$ is isomorphic as a complex vector space to its dual space

$$ S_2^\wedge = \mathbb{C}\varphi_1 \oplus \cdots \oplus \mathbb{C}\varphi_{2g}. $$

The dual space is not $V$ but a $g$-dimensional quotient of $V$ under the map $(z_1 \varphi_1, \ldots, z_{2g} \varphi_{2g}) \mapsto \sum z_j \varphi_j$. The map has a $g$-dimensional kernel because the $\{\varphi_j\}$ are linearly independent over $\mathbb{R}$ but dependent over $\mathbb{C}$. The proof will construct a complementary space $S_2^\perp$ isomorphic to $S_2$ such that $V$ is isomorphic to the direct sum $S_2^\perp \oplus S_2^\vee$ as a $\mathbb{T}_\mathbb{Z}$-module and therefore the desired result transfers to the sum, and then the proof will show that the systems of
eigenvalues on the sum are the systems of eigenvalues on \( S_2 \), transferring the result to \( S_2 \) as necessary.

To construct the complementary space, recall the operator \( w_N = \begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix} \) from Section 5.5, satisfying the relation \( w_N T = T^* w_N \) for all \( T \in \mathbb{T}_Z \) where as usual \( T^* \) is the adjoint of \( T \). For any cusp form \( g \in S_2 \) consider an associated map \( \psi_g \) from cusp forms to scalars,

\[
\psi_g : S_2 \rightarrow \mathbb{C}, \quad \psi_g(h) = \langle w_N g, h \rangle.
\]

Then \( \psi_g(h + \tilde{h}) = \psi_g(h) + \psi_g(\tilde{h}) \) but since the Petersson inner product is conjugate-linear in its second factor,

\[
\psi_g(\bar{z} h) = \bar{z} \psi_g(h), \quad z \in \mathbb{C}.
\]

Thus \( \psi_g \) belongs to the set \( S_2^\perp \) of conjugate-linear functions on \( S_2 \), the complex conjugates of the dual space \( S_2^\perp \) (Exercise 6.5.4). This set forms a complex vector space with the obvious operations. It is immediate that \( \psi_{g + \tilde{g}} = \psi_g + \psi_{\tilde{g}} \) and \( \psi_{z g} = z \psi_g \) for \( g, \tilde{g} \in S_2 \) and \( z \in \mathbb{C} \), and therefore the map

\[
\Psi : S_2 \rightarrow S_2^\perp, \quad g \mapsto \psi_g
\]

is \( \mathbb{C} \)-linear. It has trivial kernel, making it an isomorphism. The vector space \( S_2^\perp \) is a \( \mathbb{T}_Z \)-module with the Hecke operators acting from the right as composition, and the linear isomorphism \( \Psi \) is also \( \mathbb{T}_Z \)-linear since

\[
\psi_{T g}(h) = \langle w_N T g, h \rangle = \langle T^* w_N g, h \rangle = \langle w_N g, T h \rangle = (\psi_g \circ T)(h).
\]

That is, \( S_2 \) and \( S_2^\perp \) are isomorphic as complex vector spaces and as \( \mathbb{T}_Z \)-modules. In particular, every system of eigenvalues \( \{ \lambda(T) : T \in \mathbb{T}_Z \} \) on \( S_2 \) is a system of eigenvalues on \( S_2 \) and conversely.

Also, every system of eigenvalues on \( S_2 \) is a system of eigenvalues on the dual space \( S_2^\perp \) and conversely. To see this, let \( f \in S_2 \) be a normalized eigenform. Similarly to before there is a map

\[
\lambda_f : \mathbb{T}_C \rightarrow \mathbb{C}, \quad T f = \lambda_f(T).
\]

(We need the complex Hecke algebra \( \mathbb{T}_C \) in this paragraph.) Let \( J_f = \ker(\lambda_f) = \{ T \in \mathbb{T}_C : T f = 0 \} \), a prime ideal of \( \mathbb{T}_C \). An application of Nakayama’s Lemma shows that \( J_f S_2 \neq S_2 \) (Exercise 6.5.5), making the quotient \( S_2/J_f S_2 \) nontrivial. It follows that the subspace of the dual space annihilated by \( J_f \),

\[
S_2^\perp[J_f] = \{ \varphi \in S_2^\perp : \varphi \circ T = 0 \text{ for all } T \in J_f \},
\]

is nonzero since it is isomorphic to \( (S_2/J_f S_2)^\perp \) by the first isomorphism in (6.13). Since \( T_1 \) is the identity operator, \( T - \lambda_f(T) T_1 \in J_f \) for any \( T \in \mathbb{T}_C \), and so any nonzero \( \varphi \in S_2^\perp[J_f] \) satisfies
This is also a \( \mathbb{Z} \)-module with trivial kernel since if \( \sum z_j \varphi_j = 0 \) in \( S^2 \) and \( \sum z_j \bar{\varphi}_j = 0 \) in \( \overline{S^2} \) then both \( \sum z_j \varphi_j = 0 \) and \( \sum \bar{z}_j \varphi_j = 0 \) in \( S^2 \), i.e., \( \sum \text{Re}(z_j) \varphi_j = 0 \) and \( \sum \text{Im}(z_j) \varphi_j = 0 \) in \( S^2 \); but the \( \{ \varphi_j \} \) are linearly independent over \( \mathbb{R} \), so this implies \( z_j = 0 \) for all \( j \). Since the domain and codomain have the same dimension the map is a linear isomorphism of \( \mathbb{Z} \)-modules. The result that if \( \{ \lambda(T) : T \in \mathbb{Z} \} \) is a system of eigenvalues then so is \( \{ \lambda(T)^o : T \in \mathbb{Z} \} \) now transfers from \( V \) to \( S^2 \oplus \overline{S^2} \) and then to \( S_2 \). Thus if \( f(\tau) = \sum a_n q^n \) is a normalized eigenform in \( S_2(N, \chi) \) then its conjugate \( f^o(\tau) = \sum a_n^o q^n \) is a normalized eigenform in \( S_2(N, \chi^o) \) as desired.

It remains to prove the last statement of the theorem, that if \( f \) is a newform then so is \( f^o \). By Theorem 5.8.3, \( f^o \) takes the form \( f^o(\tau) = \sum a_i f_i(n_i \tau) \) where each \( f_i \) is a newform at level \( M_i \) with \( n_i M_i \mid N \). (Note that this uses only the part of that theorem that we have proved, that the set of such \( f_i \) spans \( S_2(\Gamma_1(N)) \).) Let \( \tau = \sigma^{-1} : \mathbb{C} \to \mathbb{C} \), an extension of another embedding \( \tau : \mathbb{K}_f \to \mathbb{C} \). Then \( f = (f^o)^\tau = \sum a_i^o f_i(n_i \tau) \). If \( f^o \) is not new then by Exercise 5.8.4 it is old and all \( M_i \) are strictly less than \( N \). Since each \( f_i^\tau \) is also a modular form at level \( M_i \) this shows that \( f \) is old as well. The result follows by contraposition.

Linearly combining the normalized eigenforms gives modular forms with coefficients in \( \mathbb{Z} \).

**Corollary 6.5.6.** The space \( S_2(\Gamma_1(N)) \) has a basis of forms with rational integer coefficients.

**Proof.** Let \( f \) be any newform at level \( M \) where \( M \mid N \). Let \( \mathbb{K} = \mathbb{K}_f \) be the number field of \( f \). Let \( \{ \alpha_1, \ldots, \alpha_d \} \) be a basis of \( \mathcal{O}_\mathbb{K} \) as a \( \mathbb{Z} \)-module and let \( \{ \sigma_1, \ldots, \sigma_d \} \) be the embeddings of \( \mathbb{K} \) into \( \mathbb{C} \). Consider the matrix from the end of the previous section and the vector

\[
A = \begin{bmatrix}
\alpha_1^\sigma_1 & \cdots & \alpha_1^\sigma_d \\
\vdots & \ddots & \vdots \\
\alpha_d^\sigma_1 & \cdots & \alpha_d^\sigma_d
\end{bmatrix}, \quad \bar{f} = \begin{bmatrix} f_{\sigma_1} \\
\vdots \\
\vdots \\
f_{\sigma_d}\end{bmatrix}
\]
6.5 Algebraic eigenvalues

and let \( \vec{g} = A\vec{f} \), i.e.,

\[
g_i = \sum_{j=1}^{d} \alpha_i^{\sigma_j} f^{\sigma_j}, \quad i = 1, \ldots, d.
\]

Then \( \text{span}\{g_1, \ldots, g_d\} = \text{span}\{f^{\sigma_1}, \ldots, f^{\sigma_d}\} \) since \( A \) is invertible. Each \( g_i \) takes the form \( g_i(\tau) = \sum_{n} a_n(g_i)q^n \) with all \( a_n(g_i) \in \mathbb{Z} \). For any automorphism \( \sigma : \mathbb{C} \rightarrow \mathbb{C} \), as \( \sigma_j \) runs through the embeddings of \( K_f \) into \( \mathbb{C} \) so does \( \sigma_j \sigma_j \) (composing left to right), and so

\[
g_i^\sigma = \sum_{j=1}^{d} \alpha_j^{\sigma_j\sigma} f^{\sigma_j\sigma} = g.
\]

That is, each \( a_n(g_i) \) is fixed by all automorphisms of \( \mathbb{C} \), showing that each \( a_n(g_i) \) lies in \( \mathbb{Z} \cap \mathbb{Q} = \mathbb{Z} \). Repeating this argument for each newform \( f \) whose level divides \( N \) gives the result. \( \square \)

Exercises

6.5.1. Let \( M \) be a free \( \mathbb{Z} \)-module of rank \( r \). Show that the ring of endomorphisms of \( M \) is a free \( \mathbb{Z} \)-module of rank \( r^2 \), and so any subring is a free \( \mathbb{Z} \)-module of finite rank.

6.5.2. Let \( f \in S_2(\Gamma_1(N)) \) be a normalized eigenform. Thus \( f \in S_2(N, \chi) \) for some Dirichlet character \( \chi : (\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathbb{C}^* \) and \( \lambda_f(d) = \chi(d) \) for all \( d \in (\mathbb{Z}/N\mathbb{Z})^* \). Show that there is a ring and \( \mathbb{Z} \)-module isomorphism \( T_{\mathbb{Z}/I_f} \cong \mathbb{Z}[\{a_n(f), \chi(d)\}] \). Show that adjoining the \( \chi(d) \) values is redundant, making (6.12) in the text correct. (A hint for this exercise is at the end of the book.)

6.5.3. Prove the isomorphisms (6.13). (A hint for this exercise is at the end of the book.)

6.5.4. Let \( V \) be any complex vector space with dual space \( V^\wedge \). Show that the set \( V^\wedge = \{ \vec{\varphi} : \varphi \in V^\wedge \} \) is the set of functions \( \psi : V \rightarrow \mathbb{C} \) such that \( \psi(v + v') = \psi(v) + \psi(v') \) and \( \psi(zv) = \overline{z}\psi(v) \) for all \( v, v' \in V \) and \( z \in \mathbb{C} \).

6.5.5. Let \( J_f, T_{\mathbb{C}}, \) and \( S_2 \) be as in the proof of Theorem 6.5.4. Show that \( J_f \) is a prime ideal. Define the local ring of \( T_{\mathbb{C}} \) at \( J_f \) as a set of equivalence classes of formal elements

\[
A = \{ T/U : T \in T_{\mathbb{C}}, U \in T_{\mathbb{C}} - J_f \} / \sim
\]

where the equivalence relation is

\[
T/U \sim T'/U' \quad \text{if} \quad V(U'T - UT') = 0 \quad \text{for some nonzero} \quad V \in T_{\mathbb{C}} - J_f.
\]


A First Course in Modular Forms
Diamond, F.; Shurman, J.
2005, XVI, 450 p. 57 illus., Hardcover
ISBN: 978-0-387-23229-4