Classical Modular forms and Galois representations

Tobias Schmidt

April 13, 2010

Abstract

These notes are based on two lectures which were given by the author at the Workshop on Arithmetic Algebraic Geometry, I.I.T. Guwhati, India, fall 2008. They were intended to give a quick survey on classical complex modular forms and their l-adic Galois representations. Accordingly, the focus is rather on results and examples whereas proofs are mainly sketched or omitted. Nothing in these notes is new or original and most of the exposed material can be found in any standard textbook on the subject (such as [4], [6], [7]). Where this is not the case we have indicated precise references.

1 Classical modular forms

1.1 Definitions and notations

Throughout these notes we fix two integers $k, N \geq 1$. The symbol p will always denote a prime number. Let $\Gamma(N)$ be the kernel of the reduction map

$$SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}).$$

By a *congruence subgroup* we mean a subgroup of $SL_2(\mathbb{Z})$ containing $\Gamma(N)$ for suitable N. Prominent examples are given by the congruence subgroups *of Hecke type*

$$SL_2(\mathbb{Z}) \supseteq \Gamma_0(N) \supseteq \Gamma_1(N) \supseteq \Gamma(N)$$

where a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ lies in $\Gamma_0(N)$ (resp. $\Gamma_1(N)$) iff $c \equiv 0\ (N)$ (resp. $c \equiv 0\ (N),\ a \equiv d \equiv 1\ (N)$). Let $GL_2^+(\mathbb{R})$ be the subgroup of $GL_2(\mathbb{R})$ consisting of matrices with positive determinant. Let $\mathbb{H}$ be the complex upper half plane endowed with its natural $GL_2^+(\mathbb{R})$-action by linear fractional transformations: $\gamma.z := \frac{az+b}{cz+d}$ where a, b, c, d are the entries of γ as above and $z \in \mathbb{H}$. If f is any $\mathbb{C}$-valued function on $\mathbb{H}$ we put

$$(f\ |_k\ \gamma)(z) := \det(\gamma)^{k/2}(cz+d)^{-k} f(\gamma.z).$$

This defines a $GL_2^+(\mathbb{R})$-action on the vector space of such functions, the so-called *weight k action*. Let Γ be a fixed congruence subgroup containing $\Gamma(N)$. A *modular form of weight k on* Γ is a complex-valued function on $\mathbb{H}$ satisfying

(a) $f|_k\gamma = f$ for all $\gamma \in \Gamma$,

(b) f is holomorphic on $\mathbb{H}$,

(c) $f|_k\alpha$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

To illustrate the last condition let $SL_2(\mathbb{Z}) = \sqcup_j \Gamma\gamma_j SL_2(\mathbb{Z})_\infty$ be a double coset decomposition where $SL_2(\mathbb{Z})_\infty$ denotes the stabilizer of ∞ in $SL_2(\mathbb{Z})$. Assume condition (b) holds. Then (c) is tantamount to requiring that the finitely many functions $f|_k\gamma_j$ admit power series expansions around ∞ as $\sum_{n\geq 0} a_n q^{n/N}$ with $q = \exp(2\pi i z)$.

Each γ_j as above will take the point ∞ to a point in $\mathbb{Q} \cup \infty$ which is called a *cusp* of Γ. Since Γ has finite index in $SL_2(\mathbb{Z})$ there are *only finitely many cusps.* If f vanishes at all cusps or equivalently if $a_0 = 0$ for the Fourier expansion of f around every $\gamma_j(\infty)$ we call f a *cusp form.* We denote the complex vector spaces of modular forms (resp. cusp forms) of weight k on Γ by $M_k(\Gamma)$ (resp. $S_k(\Gamma)$). Clearly $S_k(\Gamma) \subseteq M_k(\Gamma)$ and if $-1 \in \Gamma$ then (a) implies that $M_k(\Gamma) = 0$ for odd k.

1.2 Modular curves

Fix a congruence subgroup Γ. Recall the natural $GL_2(\mathbb{C})$-action on $\mathbb{P}^1(\mathbb{C})$ via

$$\gamma.[x, y] := [ax + by, cx + dy]$$

where $[x, y]$ are homogeneous coordinates. The map

$$\mathbb{H} \longrightarrow \mathbb{P}^1(\mathbb{C}),\ z \mapsto [z, 1]$$

is a $GL_2^+(\mathbb{R})$-equivariant embedding and we put $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Clearly Γ stabilizes $\mathbb{H}^*$ and we may define the *modular curves*

$$Y(\Gamma) := \Gamma\backslash\mathbb{H}, \qquad X(\Gamma) := \Gamma\backslash\mathbb{H}^*.$$

Mapping $\alpha \mapsto \alpha(\infty)$ induces a bijection

$$\Gamma\backslash SL_2(\mathbb{Z})/SL_2(\mathbb{Z})_\infty \xrightarrow{\cong} X(\Gamma) - Y(\Gamma).$$

Thus, adding the cusps of Γ to $Y(\Gamma)$ yields $X(\Gamma)$ which in fact is compact. The space $X(\Gamma)$ can be endowed with the structure of a complex Riemann surface where suitable charts are given (around most points) via the natural projection $\mathbb{H} \to X(\Gamma)$. Applying the Riemann-Roch theorem to $X(\Gamma)$ yields precise formulas (except for $k = 1$) for the dimensions of $M_k(\Gamma)$ and $S_k(\Gamma)$. In particular,

Theorem 1.1 $\dim_{\mathbb{C}} M_k(\Gamma) < \infty$.

Following common usage we write $X(N), X_0(N), X_1(N)$ instead of $X(\Gamma)$ in case of $\Gamma = \Gamma(N), \Gamma_0(N), \Gamma_1(N)$ respectively.

1.3 Example: Level 1

A fundamental domain for the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ is given by

$$\{z \in \mathbb{H} : |z| \geq 1 \text{ and } -1/2 \leq Re(z) \leq 1/2\}.$$

Hence, $SL_2(\mathbb{Z})$ has only one cusp namely ∞. In fact, it can be shown that there is a complex analytic isomorphism $X(1) \xrightarrow{\cong} \mathbb{P}^1(\mathbb{C})$ from which one may deduce

Theorem 1.2 *Denoting by $\lfloor . \rfloor$ the function "greatest integer" one has*

$$\dim_{\mathbb{C}} M_k(SL_2(\mathbb{Z})) = \begin{cases} 0 & k = 2 \\ \lfloor k/12 \rfloor & k \equiv 2 \ (12), k > 2 \\ \lfloor k/12 \rfloor + 1 & else. \end{cases}$$

Since $f \in M_k(SL_2(\mathbb{Z}))$ is a cusp form iff it vanishes at infinity there is an exact sequence for even $k \geq 4$

$$0 \longrightarrow S_k(SL_2(\mathbb{Z})) \longrightarrow M_k(SL_2(\mathbb{Z})) \longrightarrow \mathbb{C} \longrightarrow 0$$

induced by the map $\sum_{n \geq 0} a_n q^n \to a_0$. It follows that in this case there is a unique normalized modular form

$$E_k := 1 + a_1 q + a_2 q^2 + ...$$

inside $M_k(SL_2(\mathbb{Z}))$, the classical *Eisenstein series of weight* k on $SL_2(\mathbb{Z})$. Its very existence is due to complex lattice theory which we will sketch in the next section.

1.4 Complex lattices and elliptic curves

There is a close relation between modular forms and elliptic curves. To illustrate this, we will briefly talk about modular forms of level 1 and elliptic curves with complex coefficients. By a *lattice* in $\mathbb{C}$ we mean a discrete subgroup of the form $\mathbb{Z}w_1 + \mathbb{Z}w_2$ where the $w_i \in \mathbb{C}$ are linearly independent over $\mathbb{R}$ and $w_1/w_2 \in \mathbb{H}$. Let $\mathcal{L}$ be the set of all lattices in $\mathbb{C}$. There is then a $\mathbb{C}$-linear isomorphism between

$$\begin{aligned} M_1'(SL_2(\mathbb{Z})) \quad &:= \{f : \mathbb{H} \to \mathbb{C},\ f|_k\gamma = f \text{ for all } \gamma \in SL_2(\mathbb{Z})\}, \\ L_1'(SL_2(\mathbb{Z})) \quad &:= \{F : \mathcal{L} \to \mathbb{C},\ F(\lambda L) = \lambda^{-k} F(L) \text{ for all } \lambda \in \mathbb{C}^\times\} \end{aligned}$$

given by

$$f \mapsto F_f(\mathbb{Z}w_1 + \mathbb{Z}w_2) := w_2^{-k} f(w_1/w_2).$$

Denoting by ζ the Riemann ζ-function the series

$$E_k(z) := \frac{1}{2}\,\zeta(1-k)^{-1} \sum_{w \in \mathbb{Z}z + \mathbb{Z}, w \neq 0} w^{-k}$$

for $k \geq 4$ and $z \in \mathbb{H}$ is easily seen to be absolutely and locally uniformly convergent. It therefore defines a holomorphic function of z on $\mathbb{H}$. Clearly, $E_k =$

0 if k is odd and from the above isomorphism we see that $E_k \in M_1'(SL_2(\mathbb{Z}))$. Computing the Fourier expansion of E_k around ∞, one obtains

$$E_k(q) = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

where B_k is the kth Bernoulli number and $\sigma_{k-1}(n) := \sum_{0<d|n} d^{k-1}$. Hence $E_k, k \geq 4$ is the Eisenstein series referred to above.

Given a lattice $L \in \mathcal{L}$ the quotient $\mathbb{C}/L$ is a complex torus which gives rise to an elliptic curve over $\mathbb{C}$ as follows. If $\wp$ denotes the Weierstrass $\wp$-function associated to L, there is an isomorphism (of complex Lie groups)

$$\mathbb{C}/L \longrightarrow E_L(\mathbb{C}), \ z \mapsto [\wp(z), \wp'(z), 1]$$

onto the $\mathbb{C}$-points of an elliptic curve $E_L/\mathbb{C}$ given as a cubic in $\mathbb{P}^2(\mathbb{C})$ by a Weierstrass equation of the form

$$E_L : y^2 = 4x^3 - g_2 x - g_3$$

with constants $g_i = g_i(L)$. Under this isomorphism the holomorphic and nowhere vanishing invariant differential dz is mapped to dx/y. This sets up a bijection

$$\mathcal{L} \cong \{(E, \omega) : E/\mathbb{C} \text{ and } \omega \in \Omega_E \text{ holomorphic nonvanishing}\}$$

given by $L \mapsto (E_L, dx/y)$. This is the well known uniformization for complex elliptic curves. In this way a modular form $f \in M_k(SL_2(\mathbb{Z}))$ may be regarded as a "rule" $\mathbb{F}$ assigning each pair (E, ω) as above an element $F_f(L(E, \omega)) \in \mathbb{C}$ in a "holomorphic" way and with the property that $\mathbb{F}((E, \lambda\omega)) = \lambda^{-k}\mathbb{F}((E, \omega))$ for all $\lambda \in \mathbb{C}^\times$. Along these lines the theory of analytic modular forms generalizes vastly to so-called "geometric modular forms", a theory for which we refer to [5].

1.5 The Petersson inner product

Let Γ be a congruence subgroup. The differential

$$dv := \frac{dx \wedge dy}{y^2}$$

on $\mathbb{H}$ is easily seen to be $SL_2(\mathbb{Z})$-invariant and therefore extends to $Y(\Gamma)$. Let $f, g \in M_k(\Gamma)$ and let one of them be a cusp form. The function on $\mathbb{H}$

$$\delta(f, g)(z) := f(z)\overline{g(z)}\mathrm{Im}(z)^k$$

is Γ-invariant in the sense

$$\delta(f(\gamma.z), g(\gamma.z)) = \delta(f, g)(z)$$

for $\gamma \in \Gamma, z \in \mathbb{H}$. Here, we denote by $\mathrm{Im}(z)$ the imaginary part of z and use $\mathrm{Im}(\gamma.z) = \mathrm{Im}(z)/|cz + d|^2$. Since $(fg)(\infty) = 0$, the absolute value $|\delta(f, g)|$ is bounded on $\mathbb{H}$. From this it is not hard to see that the integral

$$(f, g) := v(Y(\Gamma))^{-1} \int_{Y(\Gamma)} \delta(f, g)\, dv$$

is well-defined and gives an hermitian inner product on $S_k(\Gamma)$. One verifies immediately that if $\Gamma' \subseteq \Gamma$ is another congruence subgroup then $(f,g)_\Gamma = (f,g)_{\Gamma'}$. It is therefore not ambiguous to omit the level from the notation. Furthermore if $\gamma \in SL_2(\mathbb{Z})$ then one may deduce that

$$(f|_k\gamma, g|_k\gamma) = v(Y(\Gamma))^{-1} \int_{Y(\Gamma)} \delta(f,g) \circ \gamma \; dv = (f,g).$$

Summing up:

Theorem 1.3 $(.,.)$ *is an $SL_2(\mathbb{Z})$-invariant hermitian inner product on $S_k(\Gamma)$.*

The orthogonal complement $N_k(\Gamma) := S_k(\Gamma)^\perp$ inside $M_k(\Gamma)$ is called the *space of Eisenstein series of level* Γ. The name is justified by the following construction. For simplicity we let $\Gamma := \Gamma(N)$ and $k \geq 3$. For integers $0 \leq \mu, \nu < N$ put

$$E_k(z,\mu,\nu,N) := \sum_{m,n} (mz+n)^{-k}$$

where the summation runs over $m \equiv \mu \ (N)$ and $n \equiv \nu \ (N)$ omitting the point $(0,0)$ in case $\mu = \nu = 0$. Clearly, $E_k(z,0,0,1) = E_k$ whence $E_k(z,\mu,\nu,N)$ enjoys the same convergence properties as E_k and is therefore holomorphic on $\mathbb{H}$. Each $E_k(z,\mu,\nu,N)$ is even a modular form: condition (a) is a short computation with congruences and condition (b) follows from the two facts: (i) the $\mathbb{C}$-span

$$\sum_{0 \leq \nu,\mu < N} \mathbb{C}\, E_k(z,\mu,\nu,N)$$

is $SL_2(\mathbb{Z})$-stable and (ii) each element in it is holomorphic at ∞. The latter follows, as in the case of E_k, by explicitly computing q-expansions. The elements $E_k(z,\mu,\nu,N)$ are called *Eisenstein series of higher level.*

Theorem 1.4 *One has*

$$N_k(\Gamma(N)) = \sum_{0 \leq \nu,\mu < N} \mathbb{C}\, E_k(z,\mu,\nu,N).$$

1.6 Diamond operators and Nebentypus

We start with some preliminaries on the level. Let Γ be a congruence subgroup. Since $\Gamma \supseteq \Gamma(N)$, some N, we have $M_k(\Gamma) \subseteq M_k(\Gamma(N))$. Furthermore, letting

$$\delta_N := \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in GL_2^+(\mathbb{R})$$

one has $\delta_N^{-1}\Gamma(N)\delta_N \supseteq \Gamma_1(N^2)$. Hence, given $f \in M_k(\Gamma(N))$ we obtain

$$f(Nz) = f(\delta_n.z) = N^{-k/2}(f|_k\delta_N) \in M_k(\delta_N^{-1}\Gamma(N)\delta_N) \subseteq M_k(\Gamma_1(N^2)).$$

If furthermore $f = \sum_n a_n q^{n/N}$ equals the Fourier expansion of f then $f(Nz) = \sum_n a_n q^n$. Hence, by "conjugation" we may view f as having level $\Gamma_1(N^2)$ without changing its Fourier coefficients. This is why we will restrict to level $\Gamma_1(N)$ in the following. Note also that $f \in M_k(\Gamma(N))$ actually lies in $M_k(\Gamma_1(N))$

iff $f(z) = f(z+1)$. We will reduce our analysis of the space $M_k(\Gamma_1(N))$ even one step further. There is a group isomorphism

$$\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\cong} (\mathbb{Z}/N)^\times, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d.$$

We may therefore unambiguously define for given $d \in (\mathbb{Z}/N)^\times, f \in M_k(\Gamma_1(N))$

$$f|\langle d\rangle := f|_k\gamma$$

where $\gamma \in \Gamma_0(N)$ is any matrix having d in its lower right corner. We call $\langle d\rangle$ the *diamond operator* associated with $d \in (\mathbb{Z}/N)^\times$. It preserves the subspace of cusp forms. Given a *Dirichlet character mod* N i.e. a homomorphism

$$\varepsilon : (\mathbb{Z}/N)^\times \longrightarrow \mathbb{C}^\times$$

define

$$M_k(N,\varepsilon) := \{f \in M_k(\Gamma_1(N)),\ f|\langle d\rangle = \varepsilon(d)f \text{ for all } d \in (\mathbb{Z}/N)^\times\}$$

and $S_k(N,\varepsilon) := M_k(N,\varepsilon) \cap S_k(\Gamma_1(N))$. Elements in these spaces are said to have *Nebentypus* ε. Note that if ε has not the same parity as k (i.e. $\varepsilon(-1) \neq (-1)^k$) then $-1 \in \Gamma_0(N)$ implies $M_k(N,\varepsilon) = 0$. By semisimplicity we now have

$$M_k(\Gamma_1(N)) = \oplus_\varepsilon\ M_k(N,\varepsilon)$$

and similarly for $S_k(N,\varepsilon)$ where ε runs through all Dirichlet characters mod N. This decomposition is orthogonal with respect to the Petersson inner product.

Proposition 1.5 *If* $\varepsilon_1 \neq \varepsilon_2$ *then* $(f_1, f_2) = 0$ *for* $f_i \in M_k(N,\varepsilon_i)$.

Indeed, pick $\gamma \in \Gamma_0(N)$ such that $\varepsilon_1(\gamma) \neq \varepsilon_2(\gamma)$. Then

$$\varepsilon_1(\gamma)(f_1,f_2) = (f_1|_k\gamma, f_2) = (f_1, f_2|_k\gamma^{-1}) = \varepsilon_2(\gamma)(f_1,f_2)$$

by the $SL_2(\mathbb{Z})$-invariance of $(.,.)$.

We will henceforth restrict to a fixed Nebentypus ε.

1.7 Hecke operators

The theory of modular forms is enriched by the presence of Hecke operators. We first give an ad-hoc definition and relate it afterwards to the usual double coset formalism.

Let $n \geq 1$ and define for $f \in M_k(N,\varepsilon), z \in \mathbb{H}$

$$(f|T_n)(z) := n^{k-1} \sum_{ad=n} \sum_{b=0}^{d-1} \varepsilon(a) d^{-k} f(\frac{az+b}{d})$$

with $\varepsilon(a) := 0$ if $(a,N) \neq 1$.

Theorem 1.6 *Each* T_n *defines an operator on* $M_k(N,\varepsilon)$ *stabilizing* $S_k(N,\varepsilon)$.

T_n is called the n-th *Hecke operator* on $M_k(N,\varepsilon)$. Define the *Hecke algebra* $\mathcal{H}(N,k,\varepsilon)$ for $M_k(N,\varepsilon)$ to be the $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(M_k(N,\varepsilon))$ generated by the elements $T_p, \langle p\rangle$ for $p \nmid N$ and by $U_p := T_p$ for $p \mid N$. It has finite dimension over $\mathbb{C}$. The U_p-operators are sometimes called *Atkin-Lehner operators* due to their significance in Atkin-Lehner theory (cf. [1]).

Theorem 1.7 *$\mathcal{H}(N,k,\varepsilon)$ is commutative and contains all $T_n, n \geq 1$.*

The commutativity follows from a general double coset formalism which we will sketch below together with the presence of certain anti-involutions on representatives of these double cosets. The fact that $\mathcal{H}(N,k,\varepsilon)$ contains in fact all $T_n, n \geq 1$ follows from certain recursion formulas. For example, one has

$$T_p\, T_{p^e} = \begin{cases} T_{p^{e+1}} + p^{k-1}\langle p\rangle T_{p^{e-1}} & p \nmid N \\ T_{p^{e+1}} & p \mid N \end{cases}$$

and similarly $T_n T_m = T_{nm}$ if $(n,m) = 1$.

Theorem 1.8 *Given $f \in M_k(N,\varepsilon)$ with q-expansion $\sum_n a_n q^n$ one has*

$$\begin{aligned} (f|T_p)(q) &= \textstyle\sum_n a_{pn} q^n + \varepsilon(p) p^{k-1} \sum_n a_n q^{pn}, \\ (f|U_p)(q) &= \textstyle\sum_n a_{pn} q^n \end{aligned}$$

Note that the first formula implies the second since $\varepsilon(p) = 0$ if $(p,N) \neq 1$.

Remark: Invoking the modular curve $X_1(N)$ the Hecke operators $T_n, n \geq 1$ can be given an interpretation as algebraic correspondances on the smooth algebraic curve associated via GAGA to the compact Riemann surface $X_1(N)$. As such they induce endomorphisms of the Jacobian variety of $X_1(N)$. We will not pursue this point of view any further (e.g. [7], §2.8).

Recall that $(.,.)$ makes $S_k(N,\varepsilon)$ a unitary space whence each $T_n, n \geq 1$ has an adjoint. For primes outside the level the latter are easy to determine.

Theorem 1.9 *Let $(p,N) = 1$. Then $T_p^* = \bar{\varepsilon} T_p$ and $\langle p\rangle^* = \langle p\rangle^{-1}$. In particular, $S_k(N,\varepsilon)$ has a basis consisting of simultaneous eigenvectors for all these operators.*

Proof: The first identity follows from the $SL_2(\mathbb{Z})$-invariance of $(.,.)$ and the second is immediate. Hence all these operators are normal whence the last statement follows since $\mathcal{H}(N,k,\varepsilon)$ is commutative. □

A cusp form $f = \sum_{n\geq 1} a_n q^n \in S_k(N,\varepsilon)$ is called a *normalized eigenform* if $T_n(f) = \lambda_n f$ with $\lambda_n \in \mathbb{C}$ for all $n \geq 1$ and $a_1 = 1$. In this case, $\lambda_n = a_n$ and the subfield $K_f = \mathbb{Q}(a_n, n \geq 1) \subseteq \mathbb{C}$ is called the *Hecke field* of f. It is a finite extension of $\mathbb{Q}$ containing the values $\varepsilon(p)$ for $p \nmid N$.

We conclude with the important fact that the formal Dirichlet series associated to the $T_n, n \geq 1$ has an Euler product. Let us make this precise. Let A be any commutative ring and form the formal power series ring $\tilde{A} := A[[u_p : p \text{ prime}]]$ in the infinitely many variables u_p. Elements of $\tilde{A}$ are called *formal Dirichlet series* over A. Writing $n^{-s} := \prod_p u_p^{e_p}$ if $n = \prod_p p^{e_p} \geq 2$ and $1^{-s} := 1$ we see that any element in $\tilde{A}$ has a unique expression as $\sum_{n\geq 1} a_n n^{-s}$ with a sequence $\{a_n\}$ in A. Let $\phi_p(s) \in A[[u_p]]$ be given for all primes p. Suppose

$\phi_p(s) \in 1+u_p\, A[[u_p]]$ for almost all p. The product $\prod_p \phi_p(s)$ is then meaningful in $\tilde{A}$. If an arbitrary element ϕ in $\tilde{A}$ can be expressed as such a product we will say that ϕ has a *formal Euler product.*

Applying this to the commutative ring $\mathcal{H}(N,k,\varepsilon)$ one may prove the

Theorem 1.10 *The formal Dirichlet series $\sum_n T_n n^{-s}$ has the formal Euler product*

$$\prod_{p|N}(1-T_p p^{-s})^{-1} \times \prod_{p\nmid N}(1-T_p p^{-1}+p^{k-1}\langle p\rangle p^{-2s})^{-1}.$$

1.8 Interlude: Double coset formalism

To introduce Hecke algebras in a general automorphic setting one usually invokes a certain double coset formalism. We sketch it here in our case of interest. Let

$$\Delta_0(N) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}), c \equiv 0\ (N), (a,N)=1, ad-bc>0 \Big\}.$$

It is a semi-group containing $\Gamma_0(N)$. Abbreviate

$$[\alpha] := \Gamma_0(N)\alpha\Gamma_0(N)$$

for the double coset of $\alpha \in \Delta_0(N)$ inside $\Gamma_0(N)\backslash GL_2^+(\mathbb{R})/\Gamma_0(N)$. Let $R(N)$ be the free $\mathbb{Z}$-module on symbols $[\alpha], \alpha \in \Delta_0(N)$ endowed with the following multiplication: let $[\alpha],[\beta]$ be given. By our choice of $\Delta_0(N)$ there are decompositions into left cosets

$$[\alpha] = \bigsqcup_i \Gamma_0(N)\alpha_i, \qquad [\beta] = \bigsqcup_j \Gamma_0(N)\beta_j$$

with *finitely* many $\alpha_i, \beta_j \in \Delta_0(N)$ (note that $[\Gamma_0(N) : \Gamma_0(N) \cap \alpha^{-1}\Gamma_0(N)\alpha] < \infty$, cf. [7], Lem. 2.7.1). Then we put

$$[\alpha]\cdot[\beta] := \sum_\gamma c_\gamma[\gamma]$$

where the summation runs through all double cosets $[\gamma] \subseteq \Delta_0(N)$ and $c_\gamma := \#\{(i,j) : \Gamma_0(N)\alpha_i\beta_j = \Gamma_0(N)\gamma\}$. It is clear that $c_\gamma = 0$ for almost all γ whence extending this definition linearly gives an associative unital $\mathbb{Z}$-algebra structure on $R(N)$. Crucial is the following

Lemma 1.11 *Any $\alpha \in \Delta_0(N)$ determines uniquely positive integers $l,m \geq 1$ such that $l|m, (l,N)=1$ and*

$$[\alpha] = \Gamma_0(N)\begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix}\Gamma_0(N)$$

as double cosets inside $\Gamma_0(N)\backslash GL_2^+(\mathbb{R})/\Gamma_0(N)$.

Define

$$T(l,m) := [\begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix}]$$

for all such (l,m) and $T(n) := \sum_{lm=n} T(l,m)$ for all $n \geq 1$.

Theorem 1.12 *The algebra $R(N)$ equals the polynomial ring over $\mathbb{Z}$ in the variables $T(p),\ T(p,p),\ p \nmid N$ and $T(q),\ q \mid N$ where q, p are prime numbers.*

To connect this approach to the former we define an $R(N)$-action on $M_k(N, \varepsilon)$ as follows. The character ε extends from $\Gamma_0(N)$ to $\Delta_0(N)$ via

$$\varepsilon(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) := \bar{\varepsilon}(a)$$

(note that if $\gamma \in \Gamma_0(N)$ then $ad \equiv 1\ (N)$ implies $\bar{\varepsilon}(a) = \varepsilon(d)$). Let $\alpha \in \Delta_0(N)$ and write $[\alpha] = \sqcup_i \Gamma_0(N)\alpha_i$ with finitely many $\alpha_i \in \Delta_0(N)$. Then if $f \in M_k(N, \varepsilon)$ define

$$f|[\alpha] := \det(\alpha)^{k/2-1} \sum_i \bar{\varepsilon}(\alpha_i)(f|_k \alpha_i).$$

We obtain well defined operators on $M_k(N, \varepsilon)$ that stabilize $S_k(N, \varepsilon)$.

Theorem 1.13 *The ring homomorphism $R(N) \longrightarrow \mathrm{End}_{\mathbb{C}}(M_k(N, \varepsilon))$ satisfies $T(p) \mapsto T_p, T(p,p) \mapsto p^{k-2}\langle p\rangle$ and $T(q) \mapsto U_q$.*

1.9 L-series attached to modular forms

Let $f = \sum_{n\geq 1} a_n q^n \in S_k(N, \varepsilon),\ q = \exp(2\pi i z)$. By standard Fourier theory

$$a_n = \int_0^1 \exp(-2\pi i n(x+iy)) f(x+iy) dx$$

for any $y \in \mathbb{R}$. Since $f(\infty) = 0$, it is easy to see that $y^{k/2}|f|$ is bounded on $\mathbb{H}$ whence we obtain

$$|a_n| << y^{-k/2} \exp(2\pi n y) << n^{k/2}$$

by putting $y := 1/n$. It follows that the Dirichlet series

$$L(s, f) := \sum_{n\geq 1} a_n n^{-s},\ \ s \in \mathbb{C}$$

converges absolutely and locally uniformly in the strip $Re(s) > k/2 + 1$ and defines a holomorphic function. Recall that the complex Γ-function $\Gamma(s)$ is a meromorphic function on $\mathbb{C}$ with no zeroes whose poles are at the non-positive integers and simple. For $Re(s) > 0$ it admits the explicit description

$$\Gamma(s) = \int_0^\infty t^{s-1} \exp(-t)\, dt.$$

Theorem 1.14 *The function $\Lambda_N(s, f) := (2\pi/\sqrt{N})^{-s}\Gamma(s)L(s, f)$ has analytic continuation to $\mathbb{C}$ and satisfies the functional equation*

$$\Lambda_N(s, f) = i^k \Lambda_N(k - s, f|_k\, \omega_N)$$

where $\omega_N := \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$.

It follows that $L(s, f)$ is an *entire* function on $\mathbb{C}$ with simple zeroes at the non-positive integers. When has it an Euler product?

Theorem 1.15 *Let $f \in S_k(N,\varepsilon)$ be nonzero. The following conditions are equivalent:*

1. *f is an eigenform for all $T_n, n \geq 1$.*
2. *$a_1 \neq 0$ and $L(s,f) = a_1 \prod_p (1 - t(p)p^{-s} + \varepsilon(p)p^{k-1-2s})^{-1}$.*

In this case $f|T_n = t(n)f$ with $t(n) = a_n/a_1$.

Proof: This follows from the formal Euler product over $\mathcal{H}(N,k,\varepsilon)$ appearing in Thm. 1.10. □

Example: let $N = 1, k = 12$ and recall *Ramanujan's Δ-function*

$$\Delta := (E_4^3 - E_3^4)/12^3 \in S_{12}(SL_2(\mathbb{Z})).$$

Since $\dim_{\mathbb{C}} S_{12}(SL_2(\mathbb{Z})) = 1$ by Thm. 1.2 the function Δ has to be an eigenform for all T_n. We denote (for historical reasons) its q-expansion by $\sum_{n\geq 1} \tau_n q^n$. Since $\tau_1 = 1$ we obtain from the theorem

$$L(s,\Delta) = \prod_p (1 - \tau_p p^{-s} + p^{11-2s})^{-1}.$$

In this situation it is interesting to know that $|\tau_p| \leq 2p^{11/2}$ since this used to be the famous *Ramanujan conjecture* (proved by Deligne). Furthermore, all coefficients $\tau_n, n \geq 1$ are in $\mathbb{Z}$ and Ramanujan proved many astonishing arithmetic properties about them e.g. $\tau_n \equiv \sigma_{11}(n)$ (691).

1.10 Newforms

We have seen that $S_k(N,\varepsilon)$ has a basis consisting of eigenforms f for all T_p where p is prime to the level. However, the corresponding L-series $L(s,f)$ admit usually no Euler product due to the missing factors in the level (cf. Thm. 1.15). The idea to remedy this asymmetry is to restrict to a subspace of $S_k(N,\varepsilon)$ (obtained essentially by exluding all cusp forms coming from a lower level) over which the *whole* Hecke algebra is diagonalizable. To make this precise let $l \geq 1$ be an integer and put $\delta_l := \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}$ as before. If $f \in M_k(N,\varepsilon)$ then

$$f(lz) = l^{-k/2}(f|_k\delta_l)(z) \in M_k(Nl, \varepsilon|_{\Gamma_0(Nl)})$$

(see above) and similarly for $S_k(N,\varepsilon)$. Let m_ε be the conductor of ε. Let (M,l) be positive integers such that $m_\varepsilon|M|N$ with $M \neq N$ and $l|(N/M)$. Given $f \in S_k(M,\varepsilon)$ we have $f(lz) \in S_k(Ml,\varepsilon) \subseteq S_k(N,\varepsilon)$ where the latter holds since $Ml|N$ and therefore $\Gamma_0(N) \subseteq \Gamma_0(Ml)$. It makes therefore sense to define the *space of old forms*

$$S_k^1(N,\varepsilon)$$

to be the $\mathbb{C}$-span generated inside $S_k(N,\varepsilon)$ by the set

$$\bigcup_M \bigcup_l \{f(lz), f(z) \in S_k(M,\varepsilon)\}$$

where (M, l) runs through the positive integers satisfying the conditions above. The *space of newforms*

$$S_k^0(N, \varepsilon) := S_k^1(N, \varepsilon)^\perp$$

is the orthogonal complement with respect to the Petersson inner product. Of course, it might very well be zero. However, if ε is primitive (i.e. $m_\varepsilon = N$) then clearly $S_k^0(N, \varepsilon) = S_k(N, \varepsilon)$.

Theorem 1.16 *Both spaces $S_k^1(N, \varepsilon)$ and $S_k^0(N, \varepsilon)$ are stable under the induced actions of $T_n, (n, N) = 1$.*

Proof: $S_k^1(N, \varepsilon)$ is stable since the $T_n, (n, N) = 1$ essentially commute with the δ_l where l is as above. Using the formulas for the adjoints (Thm. 1.9) one deduces stability of $S_k^1(N, \varepsilon)^\perp = S_k^0(N, \varepsilon)$. □

Theorem 1.17 *("multiplicity one") Assume $f \in S_k(N, \varepsilon)$ and $g \in S_k^0(N, \varepsilon)$. Suppose that for each $(n, N) = 1$ the functions f, g are eigenforms of T_n with the same eigenvalue. Then $g \in \mathbb{C} f$.*

The theorem implies that Hecke characters appearing in the eigenspace decomposition of $S_k^0(N, \varepsilon)$ with respect to the $T_n, (n, N) = 1$ have multiplicity one.

An element $f = \sum_n a_n q^n \in S_k^0(N, \varepsilon)$ is called *primitive of conductor N* if it is an eigenform for all $T_n, (n, N) = 1$ and if it is normalized (i.e. $a_1 = 1$).

Theorem 1.18 *Primitive forms are eigenforms for the whole Hecke algebra $\mathcal{H}(N, k, \varepsilon)$. $S_k^0(N, \varepsilon)$ has a basis consisting of primitive forms.*

Proof: Let $f \in S_k^0(N, \varepsilon)$ be primitive and $T \in \mathcal{H}(N, k, \varepsilon)$. Since $\mathcal{H}(N, k, \varepsilon)$ is commutative we may apply the multiplicity one theorem to f and $f|T$ which yields $f|T \in \mathbb{C} f$. The second statement is clear since $S_k(N, \varepsilon)$ has such a basis according to Thm. 1.9. □

2 Galois representations

2.1 l-adic representations

We briefly recall some background from l-adic representation theory. For more details we refer to the lucid exposition in [8]. Let K be a field, K_s its separable closure and $G_K := Gal(K_s/K)$. Let l be a prime and V a finite dimensional $\mathbb{Q}_l$-vector space. An *l-adic representation* of G_K is a continuous homomorphism

$$G_K \longrightarrow Aut_{\mathbb{Q}_l}(V).$$

Examples:

1. *Roots of unity.* Let $l \neq char\ K$ and μ_n the group of l^n-th roots of unity in K_s, $T_l(\mu) := \varprojlim_n \mu_n$ the l-adic Tate module and $V_l(\mu) = T_l(\mu) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. The natural continuous action of G_K on μ_n induces an l-adic representation

$$\chi_l : G_K \longrightarrow Aut(V_l(\mu)).$$

This is of course nothing else than the l-adic cyclotomic character.

2. *Elliptic curves.* Let $l \neq char\ K, E$ be an elliptic curve over K and E_n the group of l^n-torsion points of E. Let $T_l(E) := \varprojlim_n E_n$ be the l-adic Tate module and $V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. The natural continuous action of G_K on E_n induces an l-adic representation
$$\pi_l : G_K \longrightarrow Aut(V_l(E)).$$
The image of π_l is a closed subgroup isomorphic to $GL_2(\mathbb{Z}_l)$, i.e. an l-adic Lie group. Duality of abelian varieties induces a canonical isomorphism $\wedge^2 V_l(E) \cong V_l(\mu)$ whence $\det(\pi_l) = \chi_l$.

Remark: Replacing l and $\mathbb{Q}_l$ by a finite place λ of a number field $L/\mathbb{Q}$ and the completion L_λ one defines λ-*adic representations* in an analogous manner.

From now on K will be a number field. Let $\rho : G_K \to Aut(V)$ be a λ-adic representation and v a finite place of K. ρ is said to be *unramified* at v if $\rho(I_w) = 1$ for the inertia subgroup $I_w \subseteq G_K$ of every extension w of v to K_s. Let D_w be the decomposition group and $F_w \in D_w/I_w$ a Frobenius element at $w|v$. If ρ is unramified at v its restriction $\rho|_{D_w}$ factors through D_w/I_w whence $\rho(F_w)$ is well defined. Since decomposition group and inertia are unique up to conjugation the conjugacy class of this element in $Aut(V)$ depends only on v and we denote it by $\rho(Frob_v)$. For example, in the above examples χ_l is unramified outside l and π_l is unramified outside l and places of bad reduction of E.

We record for future reference the following simple application of the *Čebotarev density theorem* (cf. [8], I.§2 Cor. 2).

Proposition 2.1 *Let L/K be a Galois extension (finite or not) of the number field K, unramified outside a finite set of places S. The elements $F_w, w|v, v \notin S$ form a dense subset of $Gal(L/K)$.*

2.2 Modular forms and λ-adic representations

Let as above $k, N \geq 1$ and ε a Dirichlet character mod N with $\varepsilon(-1) = (-1)^k$. Primitive forms give rise to adic Galois representations in the following sense.

Theorem 2.2 *(Deligne-Eichler-Serre-Shimura) Let*
$$f = \sum_n a_n q^n \in S_k^0(N, \varepsilon)$$
be a primitive form of conductor N. Let $K/\mathbb{Q}$ be the Hecke field of f. Let λ be a finite place of K, K_λ the completion and l the characteristic of its residue field. There exists a λ-adic representation
$$\rho_{f,\lambda} : G_{\mathbb{Q}} \longrightarrow GL_2(K_\lambda)$$
with the following properties:

1. *$\rho_{f,\lambda}$ is irreducible,*
2. *$\rho_{f,\lambda}$ is unramified outside Nl,*
3. *if $(p, Nl) = 1$ then $\operatorname{tr}(\rho_{f,\lambda}(Frob_p)) = a_p$ and $\det(\rho_{f,\lambda}(Frob_p)) = \varepsilon(p)\, p^{k-1}$.*

Remarks:

1.The representation $\rho_{f,\lambda}$ is uniquely determined by the given properties 1.-3. Indeed, by irreducibility it is uniquely determined by the characteristic polynomials and by Prop. 2.1 it suffices to look at Frobenius elements.

2. The representation $\rho_{f,\lambda}$ is constructed via the natural Galois representation on the étale l-adic cohomology of certain schemes over $\mathbb{Q}$ base extended to $\bar{\mathbb{Q}}$. We will not present this construction here but refer to [2] for all details.

To illustrate the result we look more closely at the cases of low weight.

2.2.1 Weight 1

Let $k = 1$. In this case, $\rho_{f,\lambda}$ is actually defined over K and, extending linearly to $\mathbb{C}$, we obtain a continuous representation

$$\rho_f : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C}).$$

It has the properties:

1. ρ_f is irreducible with finite image,
2. ρ_f is unramified outside N,
3. if $(p, N) = 1$ then $\mathrm{tr}(\rho_f(Frob_p)) = a_p$ and $\det(\rho_f(Frob_p)) = \varepsilon(p)$.

By Prop. 2.1 the formula for det implies that $\det \rho_f = \varepsilon$ whence ρ_f is *odd*. Since the image is finite ρ_f induces an *Artin representation* of $Gal(L/\mathbb{Q})$ where $Gal(\bar{\mathbb{Q}}/L) := \ker \rho_f$. The following theorem is due to Deligne-Serre (cf. [3], Thm. 4.6).

Theorem 2.3 *The Artin conductor of ρ_f equals N and the Artin L-series $L(s, \rho_f)$ equals $L(s, f)$.*

Recall that the famous *Artin conjecture* says that $L(s, \rho)$ is entire for any irreducible Artin representation $\rho \neq 1$.

Corollary 2.4 *The Artin conjecture holds for ρ_f.*

Proof: By Thm. 1.14 the L-series $L(s, f)$ is entire. □

2.2.2 Weight 2

Let $k = 2$. In this case, the image of $\rho_{f,\lambda}$ inside $GL_2(K_\lambda)$ is a compact subgroup whence an l-adic Lie group. It is not finite. Assume for simplicity $\varepsilon = 1$. To avoid a greater diversion into the theory of abelian varieties we assume that the level satisfies

$$N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}.$$

In this case the modular curve $X_0(N)$ corresponds (via GAGA) to an elliptic curve over $\mathbb{Q}$. The space $S_2(N)$ can be identified with the space of holomorphic differentials on $X_0(N)$ of degree 1 whence $\dim_{\mathbb{C}} S_2(N) = 1$. Hence, there exists a *unique* primitive form $f \in S_2(N)$. It follows that $\rho_{f,\lambda} = \pi_l$ where

$$\pi_l : G_{\mathbb{Q}} \longrightarrow Aut_{\mathbb{Q}_l}(V_l(X_0(N)))$$

as in our previous example ($K = \mathbb{Q},\ \lambda = l$).

For general N one has to pass to the Jacobian variety of $X_0(N)$ to realize the representation $\rho_{f,l}$.

References

[1] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[2] P. Deligne. *Formes modulaires et représentations l-adiques (Sém. Bourb., vol. 1968/69, exp. 355).* Lect. Notes in Math., Vol. 179. Springer-Verlag, Berlin, 1971.

[3] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530, 1974.

[4] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Math.* Springer-Verlag, New York, 2005.

[5] H. Hida. *Geometric modular forms and elliptic curves.* World Sci. Publ. Co. Inc., River Edge, NJ, 2000.

[6] S. Lang. *Introduction to modular forms.* Springer-Verlag, Berlin, 1976. Grundlehren der math. Wiss., No. 222.

[7] T. Miyake. *Modular forms.* Springer-Verlag, Berlin, 1989.

[8] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Math.* A K Peters Ltd., Wellesley, MA, 1998.

Tobias Schmidt
Mathematisches Institut
Westfälische Wilhelms-Universität Münster, Germany
mail: toschmid@math.uni-muenster.de