Modular forms and Galois representations

Ana Caraiani

Problem sets for Arizona Winter School, March 2013

1 Modular curves as moduli of elliptic curves

1.1 No level structure

Exercise 1.1. Let $\mathbb{H}$ be the upper half plane given by $\{\tau \in \mathbb{C} | \text{Im } \tau > 0\}$. Check that we have a bijection between points of $\mathbb{H}/SL_2(\mathbb{Z})$ and lattices $\Lambda \subset \mathbb{C}$ up to homothety.

Exercise 1.2. Let $\Lambda \subset \mathbb{C}$ be a lattice and set $E = \mathbb{C}/\Lambda$. Weierstrass's theorem says that E has the structure of an elliptic curve over $\mathbb{C}$, given by the equation

$$y^2 = 4x^3 - 60G_4x - 140G_6,$$

where

$$G_4 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4}, G_6 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}.$$

Check that scaling the lattice Λ by $\mu \in \mathbb{C}^*$ gives an isomorphic elliptic curve.

Exercise 1.3. Let $p \geq 5$. Let E_{p-1} be given by the formula

$$E_{p-1}(\tau) = \sum_{\substack{(m,n) \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^{p-1}}$$

Prove that it is a modular form of weight $p-1$ and level 1 using Version 1 of the definition in [C].

Exercise 1.4. An orbifold is a Hausdorff space X which is covered by charts (V, G, U, π), where V is an open subset in $\mathbb{R}^n$,U is an open subset of X, G is finite group action on V and preserving linear maps, and $\pi : V \to U$ is a G-invariant map for which the induced map $V/G \to U$ is a homeomorphism.

Check that the only cone points of the orbifold $\mathbb{H}/SL_2(\mathbb{Z})$ are i with angle $\frac{2\pi}{2}$ (i.e. group $G_i = \mathbb{Z}/2\mathbb{Z}$) and $\rho = e^{\frac{2\pi i}{3}}$ with angle $\frac{2\pi}{3}$ (i.e. group $G_\rho = \mathbb{Z}/3\mathbb{Z}$). All other points in $\mathbb{H}/SL_2(\mathbb{Z})$ have neighbourhoods homeomorphic to $\mathbb{R}^2$.

1.2 Level structure $\Gamma_0(N)$, $\Gamma_1(N)$ and $\Gamma(N)$

Let $N \geq 1$ be an integer. Recall that the congruence subgroups $\Gamma_0(N), \Gamma_1(N)$ and $\Gamma(N)$ are defined as follows:

1. $\Gamma_0(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} | \gamma \in SL_2(\mathbb{Z}) \; \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}$

   (a) $\Gamma_1(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} | \gamma \in SL_2(\mathbb{Z}) \; \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}$

   (b) $\Gamma(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} | \gamma \in SL_2(\mathbb{Z}) \; \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}$

Exercise 1.5. These act naturally on $\mathbb{H}$ via the action of $SL_2(\mathbb{Z})$. Prove that we have the following natural bijections between sets:

1. $\mathbb{H}/\Gamma_0(N)$ is naturally in bijection with pairs (Λ, Σ) taken up to homothety, consisting of a lattice Λ together with a cyclic subgroup $\Sigma \subset \mathbb{C}/\Lambda$ of order N.

2. $\mathbb{H}/\Gamma_1(N)$ is naturally in bijection with pairs (Λ, P) taken up to homothety, consisting of a lattice Λ together with a point $P \in \mathbb{C}/\Lambda$ of order N.

(Hint: for the first bijection, define a natural surjective map $\mathbb{H} \to \{(\Lambda, \Sigma)\}/\sim$, where $\sim$ denotes homothety, in such a way that it factors through $\mathbb{H}/\Gamma_0(N)$ and you get a commutative diagram

$$\begin{array}{ccc} \mathbb{H}/\Gamma_0(N) & \longrightarrow & \{(\Lambda, \Sigma)\}/\sim . \\ \downarrow & & \downarrow \\ \mathbb{H}/SL_2(\mathbb{Z}) & \xrightarrow{\sim} & \{\Lambda\}/\sim \end{array}$$

The vertical maps should be easy to analyze.)

Exercise 1.6. (From [S]) Let $E = \mathbb{C}/\Lambda$ be the elliptic curve associated to the lattice $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$. Recall the Weil pairing

$$\wedge : E[N] \times E[N] \to \mu_N,$$

where $\mu_N \subset \mathbb{C}^\times$ is the group of Nth roots of unity. The Weil pairing is bilinear, alternating and non-degenerate. Prove that on $E[N] = \frac{1}{N}\Lambda/\Lambda \subset \mathbb{C}/\Lambda$, the Weil pairing is given by the formula

$$\left(\frac{aw_1 + bw_2}{N}\right) \wedge \left(\frac{cw_1 + dw_2}{N}\right) = e^{2\pi i(ad-bc)/N}.$$

(Hint: first prove it for $e^{2\pi ik(ad-bc)/N}$ for some k prime to N. Then compute $w_1 \wedge w_2$ using the definition of $\wedge$ and Prop 5.5 of [S])

Exercise 1.7. Prove that $\mathbb{H}/\Gamma(N)$ is naturally in bijection with pairs up to homothety consisting of lattices Λ together with a commutative diagram

$$\begin{array}{ccc} E[N] = \frac{1}{N}\Lambda/\Lambda & \xrightarrow{\simeq} & (\mathbb{Z}/N\mathbb{Z})^2 \\ \downarrow \wedge & & \downarrow \wedge \\ \mu_N & \xrightarrow{\simeq} & \mathbb{Z}/N\mathbb{Z} \end{array},$$

where $\wedge$ is the Weil pairing on the left hand side and the symplectic pairing $(a,b) \wedge (c,d) = ad - bc$ on the right hand side.

Exercise 1.8. Check that the image of the map

$$GL_2(\mathbb{Z}) \to GL_2(\mathbb{Z}/N\mathbb{Z})$$

consists of the matrices in $GL_2(\mathbb{Z}/N\mathbb{Z})$ with determinant ± 1.

Exercise 1.9. Understand the argument on pages 7,8 of [C], which shows that if we define $Y/\mathbb{C}$ to be the moduli space of elliptic curves $E/\mathbb{C}$ together with an isomorphism $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ then Y is a disjoint union of $\varphi(N)$ copies of the modular curve $Y(N) = \mathbb{H}/\Gamma(N)$. (Here $\varphi(N)$ is the Euler φ-function.)

Exercise 1.10. The modular curve $X(1)$ has only one cusp, which we call ∞. How many cusps does the modular curve $X_0(p)$ of level $\Gamma_0(p)$ have? What is the degree of ramification of the map $X_0(p) \to X(1)$ at each cusp? (Hint: for the second question, use the moduli interpretation to compute the degree of the map $X_0(p) \to X(1)$, then show that the cusp of $X_0(p)$ in the $\Gamma_0(p)$-orbit of $\infty \in \mathbb{P}^1(\mathbb{Q})$ is unramified.)

Let $f : X \to Y$ be a complex analytic map between Riemann surfaces. Then the Riemann-Hurwitz formula computes the genus g_X of X in terms of the genus g_Y of Y together with some extra information on the map f:

$$2 - 2g_X = (\deg f)(2 - 2g_Y) - \sum_P (e_P - 1),$$

where the sum is over points $P \in X$ where f is ramified with ramification index e_P.

Exercise 1.11. Let $p \geq 5$ be a prime number. Compute the genus of $X_0(p)$ using the Riemann-Hurwitz formula and Exercise 1.10. (Hint: use example 1.2.10 of [C] as a model.)

Exercise 1.12. (From [C]) Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup. The curves $X(\Gamma) = \mathbb{H}^*/\Gamma$ are compact Riemann surfaces and so, they are algebraic curves. Why are compact complex manifolds of dimension one algebraic? Understand why the key point is the existence on X of a meromorphic differential ω. Also understand why the result fails in higher dimensions.

Exercise 1.13. Recall that a modular form of weight 2 and level $\Gamma_1(p)$ over $\mathbb{C}$ can be defined as a global section of the sheaf $\omega_{X_1(p)}^{\otimes 2}$ on $X_1(p)$. Use Example 1.2.10 of [C] to compute the dimension of the space of cusp forms of weight 2 and level $\Gamma_1(p)$ over $\mathbb{C}$.

(Hint: use the Kodaira-Spencer isomorphism to reinterpret modular forms as sections of the sheaf of differentials $\Omega^1_{X_1(p)}(\infty)$. Which sections do cusp forms correspond to?).

Can you compute the dimension of the space of cusp forms of weight 2 and level $\Gamma_0(p)$ in the same way? What is the dimension for level $\Gamma_0(p)$?

2 Tate curves and the q-expansion principle

2.1 Tate curves

Exercise 2.1. Let τ be a point on the upper half plane, which defines an elliptic curve E_τ. Let $q = e^{2\pi i \tau}$ Show that we have a uniformization

$$\mathbb{G}_m(\mathbb{C})/q^{\mathbb{Z}} \simeq E_\tau(\mathbb{C})$$

given by the exponential map.

Recall the definition of the Tate curve $T(q)$, which is an elliptic curve over the ring of Laurent series $\mathbb{Z}((q))$. Its equation is

$$y^2 + xy = x^3 + a_4(q)x + a_6(q),$$

where

$$a_4 = -\sum_{n\geq 1} \frac{n^3 q^n}{1-q^n}, a_6 = -\sum_{n\geq 1} \frac{(5n^3+7n^5)q^n}{12(1-q^n)}$$

Exercise 2.2. (From [C]) In what context does the definition of $G_m/q^{\mathbb{Z}}$ make sense?

Exercise 2.3. Check that the power series

$$x(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}, y(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u^2}{(1-q^n u)^3} + \sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}$$

formally define points on $T(q)$.

Let K be a local field that is complete with respect to a discrete valuation v. Check that $x(u,q), y(u,q)$ converge for $u, q \in K^\times$ whenever $|q|_v < 1$ and $u \notin q^{\mathbb{Z}}$. Conclude that in this case we have a map

$$\mathbb{G}_m(K)/q^{\mathbb{Z}} \to T(q)(K)$$

given by $u \mapsto (x(u,q), y(u,q))$, and sending 1 to the point at infinity. This map is an isomorphism.

Exercise 2.4. Use the map you defined in Exercise 1.5 to see which subgroups of order p in $T(q)[p]$ the different cusps of $\Gamma_0(p)$ correspond to.

2.2 The q-expansion principle

Recall that the q-expansion principle says that if a modular form (on a connected modular curve $X(\Gamma)$) has its q-expansion at one cusp vanish, then that modular form must be identically 0.

Exercise 2.5. Prove Corollary 1.3.2 of [C]. More precisely, let $R \hookrightarrow S$ be an inclusion of rings. Let f be a modular form of weight k and level $\Gamma = \Gamma(N)$ and assume that N is invertible in R. Suppose that f is a modular form over S whose q-expansion at one cusp lies in $R[[q]] \subset S[[q]]$. Prove that f is a modular form with coefficients in R.

(Hint: use one of the equivalent definitions of a modular form to try to come up with an exact sequence that will help you detect whether f is defined over R.)

2.3 Hecke operators

Exercise 2.6. Let $\Gamma = \Gamma(N)$ with $(p, N) = 1$. Let R be a ring in which p is invertible. We've seen two definitions of the Hecke operator T_p on modular forms of weight k, level $\Gamma(N)$, in addition to the classical one involving q-expansions. The first is as a correspondence

$$\begin{array}{ccc} X_0(p) & \xrightarrow{w_p} & X_0(p) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ X & \xrightarrow{C_p} & X \end{array},$$

where w_p is an involution sending the $\Gamma_0(p)$-level structure $\phi : E \to D$ to the one given by the dual isogeny $\widehat{\phi} : E \to D$. This correspondence C_p gives rise to the map

$$pT_p = \pi_*(\pi \circ w_p)^* : H^0(X(\Gamma), \omega^k) \to H^0(X(\Gamma), \omega^k).$$

The second is the "rule" definition

$$T_p(E, \omega, \alpha) = p^{k-1} \sum_{\phi : D \to E} f(D, \phi^*(\omega), \phi^*(\alpha)).$$

Check that these definitions of T_p coincide.

Exercise 2.7. (From [C]) Consider the following alternative definition of T_p:

$$T_p f(E, \omega, \alpha) = p^{k-1} \sum_{\phi : E/P \to E} f(E/P, \phi^*(\omega), \phi^*(\alpha)),$$

where E is an elliptic curve over R (with $p \in R$ invertible) and the sum is over all $p + 1$ etale subgroup schemes P of order p in $E[p]$. Understand why the above definition is sloppy. (Hint: why is $T_p f$ a modular form over R if the maps ϕ or the subgroup schemes P are not necessarily defined over R. Show that everything is OK using the q-expansion principle.

Exercise 2.8. Let f be a modular form of weight k, level $\Gamma = \Gamma(N, p)$ (level $\Gamma_0(p)$ at p) and with coefficients in R, such that $p \in R$ is invertible. Then f is a rule assigning a section of ω_E^k to each triple $(E, \alpha, \phi : D \to E)$, where E/R is an elliptic curve, α is a $\Gamma(N)$-level structure and ϕ is a p-isogeny. The U_p operator is defined as follows:

$$U_p f(E, \omega, \alpha, \phi : D \to E) = p^{k-1} \sum_{\eta : B \to E} f(B, \phi^*(\omega), \phi^*(\alpha)),$$

where the sum is over p-isogenies which are *distinct* from α.

Show that this definition is equivalent to the usual one on q-expansions:

$$U_p f = p^{k-1} \sum_{\substack{n=0 \\ p|n}}^{\infty} a_{n/p} q^n.$$

Exercise 2.9. (From [C]) Recall that $M_k(\Gamma, R, 0)$ is the space of p-adic modular forms, which are functions which are non-zero at all points of ordinary reduction. If $f = \sum a_n q^n \in M_k(\Gamma, R, 0)$, show that

$$V_p f = \sum a_n q^{np} \in M_k(\Gamma, R, 0)$$

and that $U_p V_p$ is the identity. Prove it by defining V_p in the correct way.

3 The Hasse invariant and the ordinary and supersingular locus

Exercise 3.1. (From [C]) Let E/R be an elliptic curve given by the equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

and let ω be the differential

$$\omega = \frac{dx}{2y + a_1 x + a_3} \in H^0(E/R, \Omega^1).$$

Let $S = R/2$. Prove that $a_1 \pmod 2 = A(E_S, \omega_S)$ is the Hasse invariant.

Exercise 3.2. (From [C]) Let E/R be the same elliptic curve as in Exercise 3.1.

1. Let K be the fraction field of R. Compute the 3-adic valuations of the x-coordinates of the 3-torsion points of E over $\bar{K}$, using the same method as for 2-torsion in the begining of Section 3 of [C]. Show that there exists a canonical subgroup of order 3 if the valuation of a_2 is less than $\frac{3}{4}$.

2. Identify $a_2 \pmod 3$ with the Hasse invariant $A(E_S, \omega_S)$, where $S = \frac{R}{3}$.

If we study an elliptic curve E/R in an infinitesimal neighborhood of the origin, the completed local ring is just $R[[x]]$ (since the curve is smooth), the meromorphic differentials are of the form $R[[x]]dx$ and the group law can be written as a power series in two variables $G(x, y) \in R[[x, y]]$. The kind of object we get is a *formal group* over R.

Definition 3.3. A formal group (law) over R is a power series $G(x, y) \in R[[x, y]]$ such that

$$G(x, y) = x + y + \text{higher order terms}$$

and which satisfies the usual properties of addition (commutativity, associativity etc.)

For example, the additive group $\mathbb{G}_a$ is described by the law $G(x, y) = x + y$ and the multiplicative group is described by the law $G(x, y) = x + y + xy$.

Using the addition law, we can define multiplication by any integer. For example, $[p](X) = pX + \text{higher terms}$, which, in the case when G is obtained from E, reflects the fact that the isogeny $[p]$ induces multiplication by p on the tangent space of E.

Exercise 3.4. What is the formula for multiplication by p on $\mathbb{G}_a$ and $\mathbb{G}_m$?

An isogeny $f : E' \to E$ induces a map of formal groups $G_{E'} \to G_{E'}$, which is a power series $f(x) \in R[[x]]$ such that $f(G_{E'}(x, y)) = G_E(f(x), f(y))$.

Exercise 3.5. Let E/R be an elliptic curve with $G(x, y) \in R[[x, y]]$ its associated formal group law. Prove that

$$[p]_G(x) \equiv ax^p + \text{higher terms} \pmod{p}$$

for some $a \in R/p$. (Hint: in characteristic p, the map on the formal group law of E induced by the Frobenius isogeny is $x \mapsto x^p$.)

Exercise 3.6. (Adapted from [S]) Let $E/\bar{\mathbb{F}}_p$ be an elliptic curve. Show that the following are equivalent:

1. $E[p](\bar{\mathbb{F}}_p) = \{0\}$.
2. The isogeny $F^\vee : E^{(p)} \to E$ dual to the relative Frobenius is purely inseparable.
3. The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.
4. In the formal group G of E, the map $[p]_G(x) = ax^p + \text{higher terms}$ has $a = 0$. (Hint: what does the property of being purely inseparable say about the map an isogeny induces on tangent spaces?)

If any of these properties hold, we call the elliptic curve E supersingular. Otherwise, we say E is ordinary.

Exercise 3.7. Let E/R be the same elliptic curve as in Exercise. The differential

$$\omega = \frac{dx}{2y + a_1 x + a_3} \in H^0(E/R, \Omega^1)$$

turns out to be invariant under translation by any point on the elliptic curve (Prop. 5.1 of [S]). As in [C], in the completion of a local ring of E, the differential ω can be identified with $f(x)dx$, for some $f(x) \in R[[x]]$. In this infinitesimal neighborhood, the invariance under the formal group law G translates into $f(G(x,y))d(G(x,y)) = f(x)dx$.

1. For the invariant differential ω, justify the identity $f([p]_G x)d([p]_G(x)) = pf(x)dx$.

2. From Exercise 3.5, we may assume that:

$$[p]_G(x) \equiv ax^p + \text{higher terms} \pmod{p}$$

and we can also set

$$\omega = (1 + a_1 x + \cdots + a_n x^n + \dots)dx.$$

Use the identity above to prove that $a_{p-1} \equiv a \pmod{p}$.

Exercise 3.8. Let E/R be an elliptic curve with invariant differential equal to

$$\omega = (1 + a_1 x + \cdots + a_n x^n + \dots)dx.$$

In the same way as in Exercises 3.1,3.2, prove that $a_{p-1} \equiv A(E, \omega) \pmod{p}$.

Exercise 3.9. Putting together Exercises 3.5.3.6.3.7 and 3.8, conclude that an elliptic curve E over $\bar{\mathbb{F}}_p$ is supersingular if and only if $A(E, \omega) = 0$. Equivalently, E is ordinary if and only if $A(E, \omega)$ is invertible.

3.1 The geometry of $X_0(p)/\bar{\mathbb{F}}_p$ and $X_0^{\text{rig}}(p)$

Exercise 3.10. Which cusp of $X_0^{(\text{rig})}(p)$ does the canonical subgroup of the Tate curve $T(q)$ correspond to?

Exercise 3.11. Let p be a prime. We can defne the modular curve $X_0(p)$ of level $\Gamma_0(p)$ over $\bar{\mathbb{F}}_p$ as a moduli space of elliptic curves $E/\bar{\mathbb{F}}_p$ together with an isogeny $E' \to E$ of degree p. Show that over $\mathbb{Z}[\frac{1}{p}]$, this is equivalent to a considering pairs (E, C) where C is a subgroup of order p of $E[p]$.

1. Why can't we define $X_0(p)/\bar{\mathbb{F}}_p$ as a moduli for pairs (E, C), where $C \subset E[p](\bar{\mathbb{F}}_p)$ is a subgroup of order p?

2. Use the moduli-theoretic interpretation to prove that the modular curve $X_0(p)$ over $\bar{\mathbb{F}}_p$ is a union of two copies of the modular curve $X(1)$ of level 1, which intersect at the supersingular points. (Hint: what the other possible isogenies of degree p in characteristic p, in the ordinary case and in the supersingular case?)

Exercise 3.12. Let $w : X_0(p) \to X_0(p)$ be the involution which sends $(E, \phi : E' \to E)$ to $(E', \phi^\vee : E \to E')$, where $\phi^\vee$ is the dual isogeny to ϕ. We can also think if w as an involution of $X_0^{\mathrm{rig}}(p)$.

Describe the rigid-analytic space $X_0^{\mathrm{rig}}(p)$ with its ordinary and supersingular loci. Does ω preserve the ordinary and supersingular loci in $X_0^{\mathrm{rig}}(p)$? How many connected components does the ordinary locus have? What does the right side of the picture on page 31 of [C] look like?

4 The Langlands correspondence for GL_1

Our goal is to reformulate class field theory, in order to illustrate the $n = 1$ case of the Langlands correspondence, namely the bijection between algebraic grossencharacters of a number field K and characters of the Galois group $Gal(\bar{K}/K)$. The correspondence between modular forms and Galois representations will fit in with the $n = 2$ case.

Definition 4.1. A *grossencharacter* is a continuous character $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$, and it is *algebraic* if for each embedding $\tau : K \hookrightarrow \mathbb{C}$ there exists an integer n_τ such that $\chi(\alpha) = \prod_\tau (\tau(\alpha))^{-n_\tau}$ for every $\alpha \in (K_\infty^\times)^\circ$. (Here $(K_\infty^\times)^\circ$ denotes the connected component of the identity in $K_\infty^\times$.)

Exercise 4.2. Show that a grossencharacter $\mathbb{A}_\mathbb{Q}^\times / \mathbb{Q}^\times \to \mathbb{C}^\times$ which is trivial on $(\mathbb{R}^\times)^\circ = \mathbb{R}_{>0}$ is the same thing as a Dirichlet character. (Hint: show that $\mathbb{A}^\times = \mathbb{Q}^\times \widehat{\mathbb{Z}} \mathbb{R}_{>0}$, where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$.)

Exercise 4.3. Consider the character $\chi : \mathbb{A}_K^\times \to \mathbb{C}^\times$ defined by the product formula:

$$\chi((\alpha_v)_v) = \prod_v |\alpha_v|_v^{n_v},$$

where v runs over places of K and $|\ |_v$ denotes valuation, and $n_v = 2$ if v is complex and $n_v = 1$ otherwise. Show that χ is an algebraic grossencharacter. (Hint: to show that χ is trivial on $K^\times$, first prove the result for $K = \mathbb{Q}$, then relate the product formula for $\alpha \in K^\times$ with the product formula for $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}^\times$.)

Definition 4.4. Let p be a prime number. An *algebraic character* $\chi_0 : \mathbb{A}_K^\times \to \bar{\mathbb{Q}}_p$ is a character with open kernel and such that for each $\tau : K \hookrightarrow \bar{\mathbb{Q}}_p$ there is an integer n_τ such that $\chi_0(\alpha) = \prod_\tau (\tau(\alpha))^{n_\tau}$.

Exercise 4.5. (From [G]) Show that if χ_0 is an algebraic character, then χ_0 takes values in some number field. (Hint: show that $\mathbb{A}_K^\times / (K^\times \ker \chi_0)$ is finite and that $\chi_0(K^\times \ker \chi_0)$ is contained in a number field)

Exercise 4.6. (From [G]) Let $\iota_p : \bar{\mathbb{Q}}_p \xrightarrow{\sim} \mathbb{C}$ be an isomorphism. Prove that ι_p induces a bijection between p-adic algebraic characters of K and algebraic

grossencharacters of K. (Hint: Show that χ_0 maps to χ, defined by

$$\chi(\alpha) = \iota_p \left(\chi_0(\alpha) \prod_{\tau: K \hookrightarrow \bar{\mathbb{Q}}_p} \tau(\alpha_\infty)^{-n_\tau} \right)$$

where $\alpha \in \mathbb{A}_K^\times$.)

Exercise 4.7. (From [G]) Use the Artin reciprocity map

$$Art_K : \mathbb{A}_K^\times / \overline{K^\times (K_\infty^\times)^\circ} \xrightarrow{\sim} Gal(K^{\mathrm{ab}}/K)$$

to show that algebraic characters $\chi_0 : \mathbb{A}_K^\times \to \bar{\mathbb{Q}}_p^\times$ are in bijection with Galois characters $\rho : Gal(\bar{K}/K) \to \bar{\mathbb{Q}}_p^\times$ which are de Rham at all $v|p$. (Hint: Show that χ_0 maps to ρ, defined by

$$(\rho \circ Art_K)(\alpha) = \iota_p \left(\chi_0(\alpha) \prod_{\tau: K \hookrightarrow \bar{\mathbb{Q}}_p} \tau(\alpha_\infty)^{-n_\tau} \right)$$

where $\alpha \in \mathbb{A}_K^\times$.)

Exercise 4.8. Putting together Exercises 4.5,4.6 and 4.7, we get a bijection $\chi \leftrightarrow \rho_\chi$ between algebraic grossencharacters of K and characters of $Gal(\bar{K}/K)$ which are de Rham at p. We'll call this the global Langlands correspondence for $n = 1$.

Let v be a finite place of K. Then $\chi|_{K_v^\times}$ corresponds to the character $\chi \circ (Art_{K_v})^{-1}$ of W_{K_v} via the local reciprocity map $Art_{K_v} : K_v^\times \xrightarrow{\sim} W_{K_v}^{\mathrm{ab}}$. State what the compatibility between local and global Langlands should be for $n = 1$ and check that it holds.

Exercise 4.9. Let $\chi : \mathbb{A}_{\mathbb{Q}}^\times / \mathbb{Q}^\times \to \mathbb{C}^\times$ be the algebraic grossencharacter defined in Exercise 4.3 (taking $K = \mathbb{Q}$). Can you describe the p-adic character ρ_χ of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ corresponding to χ?

5 Modular curves and modular forms from the adelic point of view

The goal of this section is to make explicit the connection between the classical definition of modular forms and modular curves and the adelic definition, in order to motivate the definitions in Chapter 4 of [G]. We will work in the case $F = \mathbb{Q}$, $S(D) = \emptyset$, so that the quaternion algebra D is just $M_2(\mathbb{Q})$. We have one infinite place and so $k_\infty = k$ and set $\eta_\infty = 0$.

The space $S_{D,k,0}$ is defined in Chapter 4 of [G]. It has an action of $G_D(\mathbb{A}^\infty)$ by right-translation.

Exercise 5.1. The group $GL_2(\mathbb{R})^+$ acts on the upper half plane $\mathbb{H}$ via

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \tau \to \frac{a\tau + b}{c\tau + d}.$$

Check that the stabilizer of $i \in \mathbb{H}$ is $\mathbb{R}_{>0}SO(2)$.

Exercise 5.2. Let $GL_2(\mathbb{Q})^+$ consist of matrices in $GL_2(\mathbb{Q})$ with positive determinant. Use strong approximation for SL_2 (essentially the fact that

$$SL_2(\mathbb{A}^\infty) = SL_2(\mathbb{Q})SL_2(\widehat{\mathbb{Z}})$$

to prove that

$$GL_2(\mathbb{A}^\infty) = GL_2(\mathbb{Q})^+ GL_2(\widehat{\mathbb{Z}}).$$

Now also prove that $GL_2(\mathbb{A}) = GL_2(\mathbb{Q})UGL_2(\mathbb{R})^+$ for any open subgroup $U \subset GL_2(\widehat{\mathbb{Z}})$ with $\det U = \widehat{\mathbb{Z}}$. Can the result still hold for a subgroup $U \subset GL_2(\widehat{\mathbb{Z}})$ with $\det U \neq \widehat{\mathbb{Z}}$?

Exercise 5.3. Let $E/\mathbb{C}$ be such an elliptic curve. Then its homology with $\mathbb{Q}$-coefficients, $H := H_1(E, \mathbb{Q})$ is a 2-dimensional vector space over $\mathbb{Q}$ and $H \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^2$ is naturally equipped with a complex structure (this follows from Hodge theory). Show that $\mathbb{H}^\pm := \mathbb{C}\backslash\mathbb{R}$ parametrizes complex structures $h : \mathbb{C} \to \mathbb{R}^2$.

Exercise 5.4. Use its moduli interpretation to show that modular curve $X(N) = \mathbb{H}/\Gamma(N)$ can be identified with the double coset space $GL_2(\mathbb{Q})\backslash\mathbb{H}^\pm \times GL_2(\mathbb{A}^\infty)/U(N)$, where

$$U(N) = \{g \in GL_2(\widehat{\mathbb{Z}}) | g \equiv \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix} \pmod N\}$$

and it acts on the right on $GL_2(\mathbb{A}^\infty)$ and $GL_2(\mathbb{Q})$ acts diagonally on the two factors.

1. First prove that $GL_2(\mathbb{Q})\backslash\mathbb{H}^\pm \times GL_2(\mathbb{A}^\infty)/GL_2(\widehat{\mathbb{Z}})$ parametrizes elliptic curves $E/\mathbb{C}$, in the following two steps.

2. Let $V = \mathbb{Q}^2$. Show that $(\tau, g) \in \mathbb{H}^\pm \times GL_2(\mathbb{A}^\infty)$ determines the following data: an elliptic curve $E_\tau/\mathbb{C}$ together with isomorphisms $\eta : H_1(E, \mathbb{Q}) \simeq V$ and $\eta^\infty : H_1(E, \mathbb{Q}) \otimes \mathbb{A}^\infty \simeq V \otimes \mathbb{A}^\infty$, in such a way that the $GL_2(\mathbb{Q})$-action on (τ, g) sends (E, η, η^∞) to $(E, g \circ \eta, \eta^\infty)$. Conclude that you have a bijection between the points of $GL_2(\mathbb{Q})\backslash\mathbb{H}^\pm \times GL_2(\mathbb{A}^\infty)$ and the pairs (E, η^∞).

3. Now let $\Lambda = \mathbb{Z}^2 \subset \mathbb{Q}^2$. Consider the triples (E, η, η^∞). Use Exercise to ensure that η^∞ sends $H_1(E, \widehat{\mathbb{Z}})$ isomorphically to $\Lambda \otimes \widehat{\mathbb{Z}}$, up to possibly changing η by some element in $GL_2(\mathbb{Q})^+$. Does this depend on the choice of element in $GL_2(\mathbb{Q})^+$? What are the $\widehat{\mathbb{Z}}$-automorphisms of $\Lambda \otimes \widehat{\mathbb{Z}}$? Conclude that $GL_2(\mathbb{Q})\backslash\mathbb{H}^\pm \times GL_2(\mathbb{A}^\infty)/GL_2(\widehat{\mathbb{Z}})$ is a moduli space for elliptic curves E with no extra structure.

4. Now think about $GL_2(\mathbb{Q})\backslash\mathbb{H}^{\pm}\times GL_2(\mathbb{A}^{\infty})/U(N)$. How are $H_1(E,\mathbb{Z}/N\mathbb{Z})$ and $E[N]$ related?

Exercise 5.5. Use Exercise 5.4 to check that the forms $S_{D,0,0}$ which are invariant under $U(N)$ are modular functions on $X(N)$.

Exercise 5.6. (Adapted from [G]) Define

$$U_1(N)=\{g\in GL_2(\widehat{\mathbb{Z}})|q\equiv\begin{pmatrix}*&*\\0&1\end{pmatrix}\pmod N\}$$

1. Let $GL_2(\mathbb{Q})^+$ be the subgroup of $GL_2(\mathbb{Q})$ consisting of matrices with positive determinant. Show that the intersection of $GL_2(\mathbb{Q})^+$ and $U_1(N)$ inside $Gl_2(\mathbb{A}^{\infty})$ is $\Gamma_1(N)$. (Hint: what is $\widehat{\mathbb{Z}}^{\times}\cap\mathbb{Q}^{\times}$?)

2. Show that $S_{D,k,0}^{U_1(N)}$ (the $U_1(N)$-invariants in $S_{D,k,0}$) can be naturally identified with a space of functions

$$\varphi:\Gamma_1(N)\backslash GL_2(\mathbb{R})^+\to\mathbb{C}$$

satisfying

$$\varphi(gu_{\infty})=j(u_{\infty},i)\varphi(g)$$

for all $g\in GL_2(\mathbb{R})^+, u_{\infty}\in\mathbb{R}_{>0}SO(2)$.

3. Deduce that there is a natural isomorphism between $S_{D,k,0}^{U_1(N)}$ and $S_k(\Gamma_1(N))$, which takes a function φ as above to the function $(gi\mapsto j(g,i)^k\varphi(g)), g\in GL_2(\mathbb{R})$. Why is the latter function well-defined?

Exercise 5.7. Spell out what the role of condition (4) in the definition of $S_{D,k,\eta}$ is. Why do we need it only in the case when $S(D)=\emptyset$?

5.1 Hecke operators revisited

Let $K/\mathbb{Q}_p$ be finite, with ring of integers $\mathcal{O}_K$ and uniformizer ϖ_K.

Exercise 5.8. Let $\mathcal{H}$ be the ring generated by comactly supported $\mathbb{C}$-valued functions on $GL_2(\mathcal{O}_K)\backslash GL_2(K)/GL_2(\mathcal{O}_K)$, with multiplication given by convolution. Show that $\mathcal{H}\simeq\mathbb{C}[T_p,S_p^{\pm1}]$, where T_p is the characteristic function of

$$GL_2(\mathcal{O}_K)\begin{pmatrix}\varpi_K&0\\0&1\end{pmatrix}GL_2(\mathcal{O}_K)$$

and S_p is the characteristic function of

$$GL_2(\mathcal{O}_K)\begin{pmatrix}\varpi_K&0\\0&\varpi_K\end{pmatrix}GL_2(\mathcal{O}_K).$$

Exercise 5.9. (From [G]) Show that we have decompositions

$$GL_2(\mathcal{O}_K)\begin{pmatrix} \varpi_K & 0 \\ 0 & \varpi_K \end{pmatrix} GL_2(\mathcal{O}_K) = \begin{pmatrix} \varpi_K & 0 \\ 0 & \varpi_K \end{pmatrix} GL_2(\mathcal{O}_K).$$

and

$$GL_2(\mathcal{O}_K)\begin{pmatrix} \varpi_K & 0 \\ 0 & 1 \end{pmatrix} GL_2(\mathcal{O}_K) =$$

$$= \left(\bigsqcup_{\alpha \in \mathcal{O}_K \pmod{\varpi_K}} \begin{pmatrix} \varpi_K & \alpha \\ 0 & 1 \end{pmatrix} GL_2(\mathcal{O}_K) \right) \bigsqcup \begin{pmatrix} 1 & 0 \\ 0 & \varpi_K \end{pmatrix} GL_2(\mathcal{O}_K).$$

Exercise 5.10. Let $S_k(\Gamma_1(N))$ be the space of cusp forms of weight k and level $\Gamma_1(N)$ with $p \nmid N$. Show that the definition of the Hecke operator T_p as the characteristic function of $GL_2(\mathbb{Z}_p)\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} GL_2(\mathbb{Z}_p)$ acting on $S_k(\Gamma_1(N))$ via its identification with $S^{U_1(N)}_{M_2(\mathbb{Q}),k,0}$ (which has an action of $GL_2(\mathbb{A}^\infty)$ by right-translation) coincides with the rule-based definition

$$T_p f(E, \omega, \alpha) = p^{k-1} \sum_{\phi : E/P \to E} f(E/P, \phi^*(\omega), \phi^*(\alpha))$$

that was introduced in Exercise 2.6.

References

[C] Calegari, F.: Congruences between modular forms - Notes for the Arizona Winter School

[G] Gee. T.: Modularity lifting theorems - Notes for the Arizona Winter School

[S] Silverman, J.: The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer Verlag, New York, 1986. MR 817210 (87g:11070)