MODULAR FORMS, ELLIPTIC AND MODULAR CURVES

LECTURES AT KYUSHU UNIVERSITY 2010

ANDREAS LANGER

Preface

These lecture notes are based on a course given at the Graduate School of Mathematics at Kyushu University in Fukuoka in spring 2010. The main goal was to give — within one semester — a compact introduction to the theory of elliptic curves, modular curves and modular forms as well as the relations between them. It was aimed at graduate students with some background in number theory or algebraic curves.

Properties of elliptic curves were given in a rather sketchy way, however more details were presented for elliptic curves over $\mathbb{C}$ and over finite fields as these are needed in later chapters. The sections on modular curves and modular forms contain most of the proofs, for example the construction of $X_0(N)$ as a compact Riemann surface as well as their moduli properties are given in full detail, likewise the actions of the Hecke-algebra on weight 2-cusp forms.

The final result given in the course is the analytic continuation of the L-function $L(E,s)$ of an elliptic curve defined over $\mathbb{Q}$, which follows from Eichler-Shimura's Theorem $L(f,s) = L(E,s)$ and analogous properties of the L-function of the cusp form f associated to E. Modularity of elliptic curves is explained from the various (equivalent) view points 'modular curves', 'modular forms' and 'Galois-representations'.

The last chapter contains some notes based on a talk in the arithmetic geometry study group. P-adic Abel-Jacobi maps and their connections to p-adic integration theory are introduced in the classical cases of abelian varieties and K_2 of curves. Finally a more recent generalization, due to A. Besser, is given in the case of K_1 of surfaces. His formula is likely to play an important role in the construction of integral indecomposables in $K_1^{(2)}$.

First I thank Professor Masanobu Kaneko for inviting me as a visiting professor to Kyushu university. Then I thank the Graduate School of Mathematics for their hospitality and for supporting my stay through the global COE-programme 'Maths for Industry'. I also want to thank all the graduate students who attended my course for their interest in these lectures.

Introduction

The Riemann zeta function

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} = \sum_{n \geq 1} n^{-s}$$

is defined for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. $\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$, and it is analytic for $s \neq 1$.

Let

$$\Gamma(s) = \int_0^\infty e^{-y} y^{s-1} \mathrm{d}y$$

be the Gamma function and let

$$Z(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

Then $Z(s)$ is meromorphic on $\mathbb{C}$, analytic for $s \neq 0, 1$ and there is a functional equation

$$Z(s) = Z(1 - s).$$

More generally, let $K/\mathbb{Q}$ be a number field with $[K : \mathbb{Q}] = n$ and let

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}$$

be the Dedekind zeta function, where the product is taken over all prime ideals $\mathfrak{p}$ of O_K. Likewise, $\zeta_K(s)$ has a meromorphic continuation to $\mathbb{C} \backslash \{1\}$ and there is a functional equation given as follows.

Let

- r_1 be the number of real embeddings $K \hookrightarrow \mathbb{R}$;
- r_2 be the number of pairs of complex conjugate embeddings $K \hookrightarrow \mathbb{C}$ and
- D_K be the discriminant of K.

Let

$$Z_K(s) = 2^{-sr_2} \pi^{-\frac{ns}{2}} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s)$$

be the extended Dedekind zeta function ("extended by Euler factors at infinity").

Then $Z_K(s)$ has a meromorphic continuation to $\mathbb{C}$, is analytic for $s \neq 0, 1$ and we have the following functional equation

$$Z_K(s) = |D_K|^{\frac{1}{2} - s} Z_K(1 - s).$$

Now let X/K be a variety over a number field K. Then we can define (formally):

$$L(X, s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(X, s)$$

where again the product is taken over all prime ideals $\mathfrak{p}$ of O_K and $L_{\mathfrak{p}}(X, s)$ contains information of X mod $\mathfrak{p}$ (and is defined via X mod

$\mathfrak{p}$). $L(X,s)$ is a well-defined function for $\mathrm{Re}(s) \gg 0$. One likes to have both meromorphic continuation and a functional equation.

For example, let X be a curve of genus g.

If $g = 0$ then X is $\mathbb{P}^1$ or a conic. Then $L(X,s)$ is a product of Dedekind zeta functions.

If $g = 1$ then X is an elliptic curve and results exist only for $K = \mathbb{Q}$ or K totally real.

Let $E/\mathbb{Q}$ be an elliptic curve, i.e. a smooth, projective geometrically connected curve with a distinguished $\mathbb{Q}$-rational point $\mathcal{O}$. Alternatively, E is given by a hypersurface

$$Y^2 Z = X^3 + aXZ^2 + bZ^3$$

in $\mathbb{P}^2_{\mathbb{Q}}$ with $\mathcal{O} = [0,1,0]$.

The L-series of E is defined as follows:

$$L(E,s) := \prod_{p \text{ prime}} L_p(E,s)^{-1}$$

where the Euler-factor $L_p(E,s)$ is given as follows:

Let p be a prime for which E has good reduction, let $E_p = E \mod p$ and $a_p := 1 + p - \#E_p(\mathbb{F}_p)$. Then $L_p(E,s) := 1 - a_p p^{-s} + p^{1-2s}$.

It is a fact that $L(E,s)$ is analytic for $\mathrm{Re}(s) > \frac{3}{2}$.

Theorem 1. *$L(E,s)$ has an analytic continuation to $\mathbb{C}$. Let $Z(E,s) = (2\pi)^{-s}\Gamma(s)L(E,s)$. Then $Z(E,s)$ has an analytic continuation to $\mathbb{C}$ and there is a functional equation*

$$Z(E, 2-s) = \epsilon N_E^{s-1} Z(E,s)$$

where N_E is the conductor of E (one has $p|N_E \Leftrightarrow E$ has bad reduction at p) and $\epsilon = \pm 1$.

Let $\mathbb{H} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$ be the upper half plane and $N \geq 1$. Let $\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}), c \equiv 0 \mod N\}$. $\Gamma_0(N)$ then acts on $\mathbb{H}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

$\Gamma_0(N)\backslash\mathbb{H} =: Y_0(N)(\mathbb{C})$ is a (noncompact) Riemann surface.

Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\} = \mathbb{H} \cup \mathbb{P}^1_{\mathbb{Q}}$. $\Gamma_0(N)$ acts on $\mathbb{H}^*$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} r = \frac{ar+b}{cr+d}.$$

$\Gamma_0(N)\backslash\mathbb{H}^* =: X_0(N)(\mathbb{C})$ is a compact Riemann surface. The elements of $\mathbb{P}^1_{\mathbb{Q}}$ and their images in $X_0(N)(\mathbb{C})$ are called cusps.

There exists a smooth projective geometrically connected curve $X_0(N)/\mathbb{Q}$ such that $X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H}^*$ (which is a model over $\mathbb{Q}$).

Definition 0.0.1. Let $E/\mathbb{Q}$ be an elliptic curve. E is called modular if there is an $N \in \mathbb{N}$ (more precisely $N = N_E$) and a non-trivial morphism $X_0(N) \to E$ of curves over $\mathbb{Q}$.

The Shimura-Taniyama conjecture, which is now a theorem, is given as follows:

Theorem 2. *(Wiles, Taylor-Wiles, Breuil-Conrad, Diamond-Taylor) Let $E/\mathbb{Q}$ be an elliptic curve. Then E is modular.*

The goal of this course will be to provide a proof of Theorem 1 for (modular, hence all) elliptic curves over $\mathbb{Q}$.

A proof of Theorem 1 goes along the following lines; using modular forms.

A function $f : \mathbb{H} \to \mathbb{C}$ is called a modular form of level N and weight 2 if:

(i) f is holomorphic on $\mathbb{H}$;
(ii) $f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z) = (cz+d)^2 f(z)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$;
(iii) $f(z)$ is "holomorphic in cusps".

The latter statement means for example at the cusp ∞ that f has a q-expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$ for $q = \exp(2\pi i z)$.

The function f is called a cusp form if $a_0 = 0$. Cusp forms of weight 2 correspond uniquely to holomorphic differential forms on $X_0(N)(\mathbb{C})$.

Now if E is a (modular) elliptic curve, then there exists a unique differential form on E (corresponding to $\pi^*\omega$ where $\pi : X_0(N) \to E$) and thus a unique cusp form $f = \sum_{n=1}^{\infty} a_n q^n$.

The *Eichler-Shimura Theorem* now states:

$$L(E,s) = L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

We will prove a functional equation for $L(f,s)$.

Contents

1. Elliptic curves

1.1. **Elliptic curves over $\mathbb{C}$.** A complex number w is called a period of the meromorphic function f, if for all $z \in \mathbb{C}$

$$f(z+w) = f(z).$$

It is easy to see that the periods form a subgroup of the additional group $\mathbb{C}$. Using the identity theorem from complex function theory it is shown that the group of periods of a non-constant meromorphic function is a discrete subgroup in $\mathbb{C}$. A discrete subgroup $\Omega \subset \mathbb{C}$ of rank 2 is called a lattice. A meromorphic function f is called elliptic function with respect of Ω, if Ω is contained in the group of its periods. For such Ω, there exists two $\mathbb{R}$-linear independent elements w_1, w_2 such that $\Omega = \{n_1 w_1 + n_2 w_2 : n_1, n_2 \in \mathbb{Z}\}$. In the following let Ω be a fixed lattice of periods. Then $K(\Omega) = \{f : f \text{ is elliptic with respect to } \Omega\}$ is a field. If $f \in K(\Omega)$, then $f' \in K(\Omega)$. It follows from the maximum principle that any holomorphic elliptic function is constant.

Proposition 1.1.1. *Let f be an elliptic function, $a_1, \dots, a_k$ the poles of f in the parallelogram $P = \{t_1 w_1 + t_2 w_2 : 0 \leq t_1, t_2 < 1\}$, Then*

$$\sum_{v=1}^{k} \operatorname{res}_{a_v} f = 0.$$

Proof. We first assume that no a_v lies in ∂P. Then we apply the residue theorem and use that

$$\int_{\partial P} f(\zeta) d\zeta = 0.$$

If some a_v lie in ∂P we move the parallelogram P into a parallelogram P' such that no a_v lies in $\partial P'$ and apply the same argument. □

Corollary 1.1.2. *If an elliptic function f has at most a simple pole in P (P as in Proposition 1.1.1). Then f is constant.*

Corollary 1.1.3. *Any non-constant elliptic function attains any value in $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ in P with the same multiplicity.*

Proposition 1.1.4. *The function*

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{w \in \Omega \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

is an elliptic function. It is called Weierstrass $\wp$ function.

Proof. We first show that the series is locally uniformly convergent. Let $|z| \leq R$. For almost all $w \in \Omega$, $|w| \geq 2R$. For those w we have

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| = \frac{|z||2w-z|}{|w|^2|z-w|^2} \leq \frac{R \cdot 3|w|}{|w|^2|w|^2/4} \leq C \frac{1}{|w|^3}.$$

One then shows $\sum_{w\neq 0} 1/|w|^3 < \infty$. This proof is left to the reader. In order to show that $\wp$ is elliptic function we consider the derivation $\wp'(z) = -2\sum_{w\neq 0}\frac{1}{(z-w)^3}$. For $\wp'$ we have

$$\wp'(z+w) = \wp'(z)$$

for all $w \in \Omega$. Let $w_0 \in \Omega$ be fixed. Then

$$\frac{\mathrm{d}}{\mathrm{d}z}(\wp(z+w_0) - \wp(z)) = \wp'(z+w_0) - \wp'(z) = 0.$$

Hence $\wp(z+w_0) - \wp(z) = c$. Choose w_0 such that $w_0/2 \notin \Omega$, let $z = -w_0/2$. Then $\wp(w_0/2) - \wp(-w_0/2) = c$. As $\wp$ is an even function, $c = 0$, Proposition 1.1.4 follows. $\square$

Using that for $w \neq 0$.

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \sum_{v=2}^{\infty} \frac{vz^{v-1}}{w^{v+1}}$$

for $|z| < |w|$, one then derives the Laurent-expansion of $\wp$,

$$\wp(z) = \frac{1}{z^2} + \sum_{v=1}^{\infty} c_{2v}z^{2v}, \text{where } c_{2v} = (2v+1)\sum_{\substack{w\in\Omega\\ w\neq 0}} \frac{1}{w^{2v+2}}.$$

Then

$$\begin{aligned}
\wp(z)^3 &= \frac{1}{z^6} + \frac{3c_2}{z^2} + 3c_4 + \cdots\ ,\\
\wp'(z) &= -\frac{2}{z^3} + 2c_2z + 4c_4z^3 + \cdots\ ,\\
\wp'(z)^2 &= \frac{4}{z^6} - \frac{8c_2}{z^2} - 16c_4 + \cdots\ .
\end{aligned}$$

Consider the elliptic function

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 20c_2\wp(z) + 28c_4.$$

In the parallelogram P the only possible pole of f is the zero point. But $\lim_{z\to 0} f(z) = 0$. So defining $f(0) = 0$ we get a holomorphic elliptic function on P, hence $f \equiv 0$. We have shown the next Proposition.

Proposition 1.1.5. *The $\wp$ function satisfies the differential equation as follows;*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

where

$$g_2 = 60\sum_{\substack{w\in\Omega\\ w\neq 0}} \frac{1}{w^4},\ \ g_3 = 140\sum_{\substack{w\in\Omega\\ w\neq 0}} \frac{1}{w^6}.$$

The zeros of $\wp'$ within P are the points

$$\rho_1 = \frac{w_1}{2},\ \rho_2 = \frac{w_1 + w_2}{2},\ \rho_3 = \frac{w_2}{2}.$$

Let $\wp(\rho_v) = e_v$ $(v = 1, 2, 3)$. Then the e_v are pairwise different and we can write

$$\wp'(z)^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3).$$

Hence the e_v are the zeros of the polynomial

$$4X^3 - g_2 X - g_3$$

whose discriminant $\Delta = g_2^3 - 27g_3^2$ must be nonzero. Then we state without proofs;

Proposition 1.1.6.
(i) *Any elliptic function is a rational function in* $\wp$ *and* $\wp'$.
(ii) $K(\Omega) \cong \mathbb{C}(s)[t]/(t^2 - 4s^3 + g_2 s + g_3)$.

Proposition 1.1.7. *(Addition-Theorem) Let* $z_1, z_2 \in \mathbb{C}\backslash\Omega$ *such that* $\wp(z_1) \neq \wp(z_2)$. *Then*

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right).$$

Let $p_j = \wp(z_j),\ p'_j = \wp'(z_j),\ j = 1, 2$ and $p_3 = \wp(z_1 + z_2),\ p'_3 = \wp'(z_1 + z_2)$. Then

$$p'_j = ap_j + b\ (j = 1, 2), \quad -p'_3 = ap_3 + b$$

where $a = \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}$ and $b \in \mathbb{C}$ is defined such that the elliptic function $f(z) = \wp'(z) - a\wp(z) - b$ vanishes in z_1, z_2 and $-z_1 - z_2$. We see that the points $(p_1, p'_1), (p_2, p'_2), (p_3, p'_3)$ lie on a complex line in $\mathbb{C}^2$ (assuming $p_1 \neq p_2$). Consider the map

$$\begin{aligned} \Phi : \mathbb{C}\backslash\Omega &\longrightarrow \mathbb{C}^2 \\ z &\longmapsto (\wp(z), \wp'(z)). \end{aligned}$$

Then the image of Φ is an affine curve of degree 3. We put

$$E = \{(u, v) \in \mathbb{C}^2 : v^2 = 4u^3 - g_2 u - g_3\},$$

then $\Phi(z) \in E$ follows from the differential equation of the $\wp$-function. We have $\Phi(z_1) = \Phi(z_2)$ if and only if $z_1 - z_2 \in \Omega$. We also define the map Φ in the lattice points by considering the complex projective plane $\mathbb{P}^2_{\mathbb{C}} = \{p = [z_0 : z_1 : z_2] : z_0, z_1, z_2 \in \mathbb{C}, [z_0, z_1, z_2] \neq [0, 0, 0]\}$ with homogeneous coordinates z_i. We identify $\mathbb{C}^2$ with its image in $\mathbb{P}^2_{\mathbb{C}}$ via the embedding $(u, v) \mapsto [1, u, v]$. Then $\mathbb{C}^2$ is the complement of the projective line $\{p \in \mathbb{P}^2_{\mathbb{C}}, z_0(p) = 0\}$. Under this identification E is the set of points with $z_0(p) \neq 0$ whose homogeneous coordinates satisfy the homogeneous cubic equation

$$(*) \qquad z_0 z_2^2 = 4z_1^3 - g_2 z_0^2 z_1 - g_3 z_0^3.$$

This equation is also satisfied if $z_0 = 0, z_1 = 0, z_2 = 1$ and this is the only solution, if $z_0 = 0$. Then the set $\overline{E} \subset \mathbb{P}^2_{\mathbb{C}}$ of points whose coordinates satisfy (*) is called projective cubic (in Weierstrass normal form). It contains the affine curve E and the point $p_0 = [0 : 0 : 1]$. The map $\Phi : \mathbb{C}\backslash\Omega \to E$ has a unique continuous extension to $\mathbb{C} \to E$ by defining $\Phi(w) = p_0$ for $w \in \Omega$. In a neighbourhood of w, $\Phi(z)$ is described by

$$\Phi(z) = [(z-w)^3 : (z-w)^3\wp(z) : (z-w)^3\wp'(z)]$$

where the homogeneous coordinates of $\Phi(z)$ appear as holomorphic functions at z. As

$$\Phi(z_1) = \Phi(z_2) \iff z_1 - z_2 \in \Omega,$$

Φ induces a bijection of the factor group

$$\mathbb{C}/\Omega \xrightarrow{\sim} \overline{E}$$

which is a homeomorphism. Via Φ we transform the group law from $\mathbb{C}/\Omega$ to $\overline{E}$:
If $P, Q \in \overline{E}$. Then

$$P \cdot Q = \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q))$$

defines an abelian group structure on $\overline{E}$ with zero element P_0.

1.2. **Elliptic curves over general fields.** Let k be a perfect field.

Definition 1.2.1. $E = (E, \mathcal{O}_E)$ is called an *elliptic curve*, if E is a non-singular, proper, geometrically connected curve of genus 1 over k and $\mathcal{O}_E$ a k-rational point on E.

Lemma 1.2.2. *Let C be a non-singular (i.e. smooth) hypersurface of degree d in $\mathbb{P}^2_k$. Then the genus $g(C)$ of C is given as follows*

$$g(C) = \frac{(d-1)(d-2)}{2}.$$

Proof. Let $\mathcal{I}_C = \mathcal{L}(-C)$ be the ideal sheaf of C. Then we have an exact sequence

$$0 \longrightarrow \mathcal{I}_C \longrightarrow \mathcal{O}_{\mathbb{P}^2} \longrightarrow \mathcal{O}_C \longrightarrow 0$$

where $\mathcal{O}_C = i_*(\mathcal{O}_C)$, with $i : C \to \mathbb{P}^2$ being a closed immersion. Then $C \sim dH$, where H is a hyperplane in $\mathbb{P}^2_k$ and thus $\mathcal{I}_C \cong \mathcal{L}(-dH) \cong \mathcal{O}_{\mathbb{P}^2}(-d)$.

For the computation of $g = \dim H^1(C, \mathcal{O}_C)$ we use

$$\begin{aligned} H^1(\mathbb{P}^2, \mathcal{O}(n)) &= 0 \text{ for all } n, \\ H^2(\mathbb{P}^2, \mathcal{O}(n)) &= H^0(\mathbb{P}^2, \mathcal{O}(-3-n))^*. \end{aligned}$$

Hence we have an exact sequence

$$0 \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow H^0(\mathbb{P}^2, \mathcal{O}(d-3))^* \longrightarrow H^0(\mathbb{P}^2, \mathcal{O}(-3))$$

where the last entry is zero. Therefore we have

$$g = \dim H^0(\mathbb{P}^2, \mathcal{O}(d-3)) = \dim k[X_0, X_1, X_2]_{\deg = d-3} = \frac{(d-1)(d-2)}{2}.$$

□

It follows that if $C \subseteq \mathbb{P}^2$ is a hypersurface of degree 3 and $P \in C(k)$, then (C, P) is an elliptic curve.

1.2.3. Riemann Roch for curves. (Reminder)

Let X/k be a smooth, proper and geometrically connected curve and $g = g(X)$. Let $D = \sum_i n_i P_i$ be a (Weil-)divisor and $\deg D = \sum_i n_i [k(P_i) : k]$. Let $\mathcal{L}(D)$ be the line bundle defined by $\{f : (f) + D \geq 0\}$ and $l(D) = \dim H^0(X, \mathcal{L}(D))$.

Let K be a canonical divisor, which is equivalent to saying that $\mathcal{L}(K) \cong \Omega_{X/k}$. Then Riemann-Roch says:

$$l(D) = \deg D + 1 - g + l(K - D)$$

for all divisors D. Moreover, $l(K) = g$, $\deg K = 2g - 2$.

In particular, if $X = E$ is an elliptic curve, then $K \sim 0$; hence $l(D) = \deg(D) + l(-D)$. Moreover, if $\deg D > 0$, then $l(D) = \deg(D)$.

Proposition 1.2.4. *Let E/k be an elliptic curve. Then there is a smooth plane curve C of degree 3, a rational point $\mathcal{O}_C \in C$, so that $(E, \mathcal{O}_E)$ is isomorphic to $(C, \mathcal{O}_C)$.*

C is given by an equation in $\mathbb{P}^2_k$ of the form

$$ZY^2 + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3$$

and one can choose $\mathcal{O}_C = [0, 1, 0]$.

Proof. We have $l(m\mathcal{O}_E) = m$ for all $m \geq 1$; hence for all $i \geq 2$ there exists $f_i \in k(E)^*$ with $(f_i)_\infty = i\mathcal{O}_E$ and $f_2, \ldots, f_m$ are a basis of $\Gamma(E, \mathcal{L}(m))$ for all $m \geq 2$.

Let $x, y \in k(E)^*$ such that $(x)_\infty = 2\mathcal{O}_E$, $(y)_\infty = 3\mathcal{O}_E$. Then $f_4 = x^2$, $f_5 = xy$, $f_6 = x^3$ or y^3 and thus

$$y^2 + a_1 xy + a_3 y = a_0 x^3 + a_2 x^2 + a_4 x$$

with $a_0 \neq 0$.

We may assume $a_0 = 1$ (otherwise replace x by $a_0 x$).

Let $F = y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3$. Let $C \subseteq \mathbb{P}^2$ given by $F = 0$. Let $\phi = (x, y) : E - \mathcal{O}_E \to C$, giving rise to $\phi : E \to C$, where $\phi(\mathcal{O}_E) = [0, 1, 0] \in \{z = 0\}$.

It remains to show that ϕ is an isomorphism.

As a reminder, morphisms $E \to \mathbb{P}^n_k$ correspond uniquely to line bundles $\mathcal{L}$ on E together with global sections $s_0, \ldots, s_n$ of $\mathcal{L}$, which generate $\mathcal{L}$ (i.e. for all $p \in E$, there exists an i such that $s_i \notin \mathfrak{m}_p \mathcal{L}_p$). $\mathcal{L}$ and $s_0, \ldots, s_n$ define $\phi : E \to \mathbb{P}^n_k$ as follows:

Let $E = \cup_i E_i$, $\mathbb{P}^n_k = \cup_{i=1}^n \mathcal{U}_i$ where $E_i = \{p \in E : s_i \notin \mathfrak{m}_p \mathcal{L}_p\}$. Then $\phi : E_i \to \mathcal{U}_i$ corresponds to Spec $k\left[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}\right] \to \Gamma(E_i, \mathcal{O}_{E_i})$, $\frac{x_j}{x_i} \mapsto \frac{s_j}{s_i}$.

In our example, $\phi : E \to \mathbb{P}^2_k$ correspond to $\mathcal{L}(3\mathcal{O}_E), 1, x, y$.

Let D be a divisor on E, $P \in E_0$. We then have

$$0 \longrightarrow \Gamma(E, \mathcal{L}(D-P)) \longrightarrow \Gamma(E, \mathcal{L}(D)) \longrightarrow \mathcal{L}(D)_{p/\mathfrak{m}_p} \longrightarrow 0.$$

As $\deg D \geq 2$, there exists $s \in \Gamma(E, \mathcal{L}(D))$, $s \notin \mathfrak{m}_p \mathcal{L}(D)|_p$.

If $n = \deg D \geq 3$, $s_0, \dots, s_{n-1}$ is a basis of $V = \Gamma(E, \mathcal{L}(D))$ and $\phi : E \to \mathbb{P}^{n-1}_k$ is the corresponding morphism, then ϕ is a closed immersion.

Proof: the property is stable under base change, so let $k = \bar{k}$.

It remains to show that

(i) V separates points: for all $P, Q \in E(\bar{k})$, with $P \neq Q$, there exists a $s \in V$ such that $s \in \mathfrak{m}_P \mathcal{L}_P$, $s \notin \mathfrak{m}_Q \mathcal{L}_Q$,

(ii) V separates tangent vectors: for all $P \in E(\bar{k})$, there exists an $s \in V$ such that $s \in \mathfrak{m}_p \mathcal{L}_p \backslash \mathfrak{m}_p^2 \mathcal{L}_p$.

Both properties follow from Riemann-Roch:

(i) $\Gamma(E, \mathcal{L}(D-P-Q)) \subsetneq \Gamma(E, \mathcal{L}(D-P))$;

(ii) $\Gamma(E, \mathcal{L}(D-2P)) \subsetneq \Gamma(E, \mathcal{L}(D-P))$.

Also, $\phi : E \to H \subseteq \mathbb{P}^2_k$, corresponding to $\mathcal{L} = \mathcal{L}(3\mathcal{O}_E)$ is a closed immersion. Suppose H is not irreducible and reduced. Then

$$F = Y^2 Z + a_1 XYZ + \cdots = F_1 \cdot F_2$$

with F_1, F_2 homogeneous. And thus we have $\phi : E \xrightarrow{\cong} H_1$, a hypersurface, corresponding to F_1 and $g(H_1) = g(E) = 1$, which is a contradiction. □

Remark. If $\mathrm{char}(k) \neq 2, 3$, then we can show (by a linear transformation $\mathbb{P}^2 \to \mathbb{P}^2$) that $(E, \mathcal{O}_E) \cong (C, 0)$ where C is given by an equation of the form

$$ZY^2 = X^3 + aXZ^2 + bZ^3,$$

this is called the *Weierstrass form* of E.

Then one can easily show that C is non-singular if and only if $\mathrm{disc}(X^3 + aX + b) := -16(4a^3 + 27b^2) \neq 0$.

1.2.5. Let S be a scheme. A S-group scheme $G \to S$ is a group object in **Sch**$/S$, i.e. one has a quadruple

$$(G, m : G \times G \longrightarrow G, \mathrm{inv} : G \longrightarrow G, \epsilon : S \longrightarrow G)$$

satisfying

- Associativity:

$$\begin{array}{ccc} G \times G \times G = G \times (G \times G) = (G \times G) \times G & \xrightarrow{1 \times m} & G \times G \\ \downarrow{\scriptstyle m \times m} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

commutes.

- Existence of inverse:

$$\begin{tikzcd} G \times G \arrow[r, "\mathrm{inv}\times\mathrm{id}"] & G \times G \arrow[dr, "m"] & \\ G \arrow[u, "\Delta"] \arrow[r] & S \arrow[r, "\epsilon"] & G \end{tikzcd}$$

commutes.

- One element:

$$\begin{tikzcd} \begin{array}{c} G = G \times S \\ = S \times G \end{array} \arrow[r, "\mathrm{id}\times\epsilon"] \arrow[d, "\epsilon\times\mathrm{id}"'] \arrow[dr, "\mathrm{id}"] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"'] & G \end{tikzcd}$$

commutes.

Examples 1.2.6.

a. $\mathbb{G}_m = \mathbb{G}_{m,S} = \text{Spec } \mathbb{Z}[T, T^{-1}] \times_{\text{Spec } \mathbb{Z}} S$.

$\mathbb{G}_m$ represents the functor

$$(X \to S) \longmapsto \Gamma(X, \mathcal{O}_X)^*.$$

Proof:

$$\text{Hom}_S(X, \mathbb{G}_m) = \text{Hom}_{\text{Spec } \mathbb{Z}}(X, \text{Spec } \mathbb{Z}[T, T^{-1}]) = \\ \text{Hom}(\mathbb{Z}[T, T^{-1}], \Gamma(X, \mathcal{O}_X)) = \Gamma(X, \mathcal{O}_X)^*.$$

b. $\mu_n = S \times_{\mathbb{G}} \text{Spec } (\mathbb{Z}[T]/(T^n - 1))$. Proof: $\text{Hom}_S(X, \mu_n) = \{x \in \Gamma(X, \mathcal{O}_X)^*, x^n = 1\}$.

c. Let A be an abelian group, then $A_S = \coprod_{a \in A} S$ is an S-group scheme.

If $X \to S$ is an S-scheme with $X = \cup_{i \in I} X_i$ its decomposition into connected components, then

$$\text{Hom}_S(X, \coprod_{a \in A} S) = \prod_i \text{Hom}(X_i, \coprod_{a \in A} S) = \prod_{i \in I} A.$$

A_S is called the *constant group scheme associated to* A.

Definitions 1.2.7.

a. An *abelian variety* A/k is a geometrically connected, proper, integral k-group scheme.

b. Let S be a base scheme. An S-group scheme $\pi : \mathcal{A} \to S$ is called an *abelian scheme* if π is proper, smooth, with geometrically connected fibers.

Remark. One can show that any abelian variety is smooth and projective, and that the group law is commutative.

Theorem 1.2.8. *Let E be an elliptic curve. Then E is an abelian variety with 1-section $\mathcal{O}_E \in E(k)$. Conversely, any abelian variety of dimension 1 is an elliptic curve.*

1.3. **Isogenies.**

1.3.1. Morphism of curves.

Let $f : X \to Y$ be a non-trivial morphism of (smooth, projective) curves over k. Then

(i) f is finite and flat.
(ii) f maps the generic point of Y to the generic point of X.
(iii) $f_*\mathcal{O}_X$ is a locally free $\mathcal{O}_Y$-module of rank n, where $n = [k(X) : k(Y)] =: \deg f$ is the *degree of* f.
(iv) f induces a homomorpism $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ and we have $\deg f^*\mathcal{L} = \deg(f) \deg \mathcal{L}$.
(v) For all $y \in Y$: $f^{-1}y = \mathrm{Spec}\ k(y) \times_Y X$ is a finite $k(y)$-scheme of dimension n.
(vi) Define $f_* : \mathrm{Div}X \to \mathrm{Div}Y$ by $f_*(\sum_{i=1}^r n_iP_i) = \sum_{i=1}^r n_i[k(P_i) : k(f(P_i))]f(P_i)$. Then $\deg f_*D = \deg D$ and $f_*\mathrm{div}_X(g) = \mathrm{div}_Y N_{k(X)/k(Y)}(g)$.
This induces $f_* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(Y)$, $\mathrm{Pic}(X) \to \mathrm{Pic}(Y)$. One has $f_* \circ f^* = \deg(f)$.
(vii) Let $f : X \to Y$, $g, h : Y \to Z$ be finite with Z/k separated. If $g \circ f = h \circ f$, then $g = h$.

Definition 1.3.2. Let $E_1, E_2/k$ be elliptic curves. A morphism $f : E_1 \to E_2$ with $f(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is called an *isogeny.*

Lemma 1.3.3. *An isogeny $f : E_1 \to E_2$ is a morphism of group schemes.*

Let E_1, E_2 be elliptic curves. Then

$$\begin{aligned} \mathrm{Hom}_k(E_1, E_2) &= \{f : E_1 \to E_2, f \text{ morphism with } f(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}\} \\ &= \{f \text{ isogeny}\} \cup \{0\} \\ &= \{\text{Homomorphisms of group schemes } E_1 \to E_2\}. \end{aligned}$$

$\mathrm{Hom}_k(E_1, E_2)$ is an abelian group: $f + g = \mu_{E_2} \circ (f \times g) \times \Delta$.

$\mathrm{End}(E) = \mathrm{Hom}_k(E, E)$ is an associative ring with $1 = \mathrm{id}_E$ and, because of (vii), without zero-divisors. The map

$$\begin{aligned} [\ ] : \mathbb{Z} &\longrightarrow \mathrm{End}(E) \\ n &\longmapsto [n] = 1 + \cdots + 1 (n \text{ times}) \end{aligned}$$

is a ring homomorphism.

Lemma 1.3.4. $[\ ] : \mathbb{Z} \longrightarrow \mathrm{End}(E)$ *is a monomorphism.*

Let $f : E_1 \to E_2$ be an isogeny and T a smooth k-scheme. Then

$$\begin{aligned} f^* : \mathrm{Pic}^0((E_2), T) &\longrightarrow \mathrm{Pic}^0((E_1)_T, T) \\ \mathcal{L} &\longmapsto f^*\mathcal{L} \end{aligned}$$

is well-defined, hence induces a map

$$f^* : \mathrm{Hom}(\ , E_2) \longrightarrow \mathrm{Hom}(\ , E_1).$$

By the Yoneda lemma there exists a unique $\hat{f} : E_2 \to E_1$ which induces f^*.

For $T \in S_m/k$, let $\phi_T : \mathrm{Hom}(T, E_i) \cong \mathrm{Pic}((E_i)_T/T)$. Then $\phi_T(\hat{f}(P)) = f^*(\phi_T(P))$.

Definition 1.3.5. $\hat{f} : E_2 \to E_1$ is called the *dual isogeny* of f.

Proposition 1.3.6.

a. *If $f : E_1 \to E_2$ and $g : E_2 \to E_3$ are isogenies. Then $\widehat{g \circ f} = \hat{f} \circ \hat{g}$.*
b. *Let $f, g : E_1 \to E_2$ be isogenies. Then $\widehat{f+g} = \hat{f} + \hat{g}$.*
c. *If $f : E_1 \to E_2$ is an isogeny with* $\deg f = m$, *then $f \circ \hat{f} = [m]$ and $\hat{f} \circ f = [m]$.*
d. *$\hat{\hat{f}} = f$, $\widehat{[m]} = [m]$ for all $m \in \mathbb{Z}$.*
e. $\deg[m] = m^2$ *for all $m \in \mathbb{Z}\backslash\{0\}$.*
f. *For an isogeny f we have* $\deg f = \deg \hat{f}$.

Definition 1.3.7. Let X, Y be noetherian schemes. A morphism $f : X \to Y$ of finite type is called *étale* if f is flat and the sheaf of relative differentials vanishes, that is $\Omega_{X/Y} = 0$.

Let X and Y be of finite type over k. Then $f : X \to Y$ is étale if an only if f is smooth of relative dimension 0.

Remark 1.3.8.

a. Open immersions are étale.
b. A composition of étale morphisms is étale.
c. A base change of étale morphisms is étale.

Remark 1.3.9. Let k be a field, A a finite k-algebra. Then the following are equivalent.

(i) A is an étale k-algebra.
(ii) $A \cong \prod_{i=1}^r k_i$ where each k_i is a separable field extension of k.
(iii) $A \otimes_k \bar{k} = \prod_{i=1}^r \bar{k}$.
(iv) $\#\mathrm{Spec}\ (A \otimes_k \bar{k}) = \dim_k A$.

For the proof, see Milne, I, paragraph 3.

Definition 1.3.10. Let X, Y be smooth, proper, geometrically connected curves over k and $f : X \to Y$ a non-trivial (hence finite and flat) morphism. Then f is called *separable* if $k(X)/k(Y)$ is a separable field extension (which is equivalent to f being geometrically étale).

Proposition 1.3.11. *Let $f : E_1 \to E_2$ be an isogeny of elliptic curves. Then the following are equivalent*

a. *f is separable.*

b. f *is étale.*
c. $(\mathrm{d}f)_0 : T_0E_1 \to T_0E_2$ *is a bijection.*

Proof. For b. $\Rightarrow$ a., use

$$\begin{array}{ccc} \operatorname{Spec} k(E_1) & \longrightarrow & E_1 \\ \big\downarrow & & \big\downarrow{\scriptstyle f} \\ \operatorname{Spec} k(E_2) & \longrightarrow & E_2. \end{array}$$

This diagram is cartesian; hence $k(E_1)$ is an étale $k(E_2)$-algebra and thus $k(E_1)/k(E_2)$ is separable.

For a. $\Rightarrow$ b., we know that $\mathcal{U} = \{x \ \in E_1 : \big(\Omega_{E_1/E_2}\big)_x = 0\}$ is open in E_1, the generic point μ is in $\mathcal{U}$, as $\operatorname{Spec} k(E_1) \to \operatorname{Spec} k(E_2)$ is étale $\mathcal{U} \neq \emptyset$.

$$\begin{aligned} E_1 \longrightarrow E_2 \text{ is étale } &\iff \Omega_{E_1/E_2} = 0 \\ &\iff \Omega_{E_1/E_2} \otimes_k \bar{k} = 0 \\ &\iff E_1 \times \bar{k} \longrightarrow E_2 \times \bar{k} \text{ is étale.} \end{aligned}$$

Without loss of generality, we may assume $k = \bar{k}$.

Let $x \in E_1(\bar{k})$, $a \in \mathcal{U}(\bar{k})$. Then $\mathcal{U}_x := \mathcal{U} - a + x = \mathcal{T}_{x-a}(\mathcal{U})$ is an open neighbourhood of x in E_1. Then

$$f|_{\mathcal{U}_x} : \mathcal{U}_x \xrightarrow{\mathcal{T}_{a-x}} \mathcal{U} \xrightarrow{f|_{\mathcal{U}}} E_2 \xrightarrow{\mathcal{T}_{f(x-a)}} E_2$$

is étale and thus f is étale.

For b. $\Rightarrow$ c., there is an exact sequence

$$f^*\Omega_{E_2/k} \longrightarrow \Omega_{E_1/k} \longrightarrow \Omega_{E_1/E_2} \longrightarrow 0.$$

We have

$$\Omega_{E_1/k} \otimes k(\mathcal{O}_{E_1}) = (T_0E_1)^*$$

and

$$f^*\Omega_{E_2/k} \otimes k(\mathcal{O}_{E_2}) = (T_0E_2)^*.$$

Now b. implies $(\mathrm{d}f)^* : (T_0E_2)^* \to (T_0E_1)^*$ is surjective and thus $\mathrm{d}f$ is injective and thus $\mathrm{d}f$ is bijective.

For c. $\Rightarrow$ a., we know $\Omega_{E_1/E_2} \otimes k(\mathcal{O}_{E_1}) = 0$ and thus $(\Omega_{E_1/E_2})_{\mathcal{O}_{E_1}} = 0$ and thus $\mathcal{U} = \{x \in E_1 : (\Omega_{E_1/E_2})_x = 0\}$ is open and non-empty. So $\eta \in \mathcal{U}$ and therefore $k(E_1)/k(E_2)$ is étale and also separable. $\square$

Lemma 1.3.12. *Let $f, g : E_1 \longrightarrow E_2$ be isogenies. Then we have*

$$\mathrm{d}(f + g) = \mathrm{d}f + \mathrm{d}g : T_0E_1 \longrightarrow T_0E_2.$$

1.4. **Elliptic curves over finite fields.** Let $k = \mathbb{F}_q$ where $q = p^n$. Let X be an $\mathbb{F}_q$-scheme.

The Frobenius, $\mathrm{Fr}_X : X \to X$ is then given by $\mathrm{id} : \mathrm{sp}(X) \to \mathrm{sp}(X)$ on the underlying topological spaces and $x \mapsto x^q$ on $\mathcal{O}_X \to \mathcal{O}_X$.

If $f : X \to Y$ is an $\mathbb{F}_q$-morphism, then

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{Fr}_X} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{\mathrm{Fr}_Y} & Y \end{array}$$

commutes.

If $X = \mathrm{Spec}\, A$ is affine, then Fr_X is given by $A \to A$, $a \mapsto a^q$.

Let $E/\mathbb{F}_q$ be an elliptic curve. Then $\mathrm{Fr}_E : E \to E$ is an isogeny because

$$\begin{array}{ccc} \mathrm{Spec}\, \mathbb{F}_q & \xrightarrow{\mathrm{Fr}=\mathrm{id}} & \mathrm{Spec}\, \mathbb{F}_q \\ {\scriptstyle \mathcal{O}_E}\downarrow & & \downarrow{\scriptstyle \mathcal{O}_E} \\ E & \xrightarrow{\mathrm{Fr}_E} & E \end{array}$$

commutes.

1.4.1. Let $X/\mathbb{F}_q$ be a smooth projective curve. Then $\deg(\mathrm{Fr}_X) = q$.

Proof. Let $f : X \longrightarrow \mathbb{P}^1$ e a finite morphism. The commutativity of the diagram

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{Fr}_X} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbb{P}^1 & \xrightarrow{\mathrm{Fr}_{\mathbb{P}^1}} & \mathbb{P}^1 \end{array}$$

implies $\deg(\mathrm{Fr}_X) = \deg(\mathrm{Fr}_{\mathbb{P}^1})$. Hence we may assume $X = \mathbb{P}^1$. Then $\deg(\mathrm{Fr}_{\mathbb{P}^1}) = [k(t) : k(t^q)] = q$. $\square$

Lemma 1.4.2. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then* $\deg(1 - \mathrm{Fr}_E) = \#E(\mathbb{F}_q)$.

Proof. Fr_E is not separable, as $k(E) \to k(E)$, $x \mapsto x^q$ is the induced map on $\eta = \mathrm{Spec}\, k(E)$. Thus, from 1.3.11 it follows that $\mathrm{dFr}_E : TE \to TE$ is the zero map and thus (1.3.12) $\mathrm{d}(1 - \mathrm{Fr}_E) = \mathrm{id} : TE \to TE$ and therefore (1.3.11) $1 - \mathrm{Fr}_E$ is separable and thus étale.

Let $(1 - \mathrm{Fr}_E)^{-1}(0) = \ker(1 - \mathrm{Fr}_E)$ be defined by the cartesian diagram

$$\begin{array}{ccc} \ker(1 - \mathrm{Fr}_E) & \longrightarrow & E \\ \downarrow & & \downarrow{\scriptstyle 1-\mathrm{Fr}_E} \\ \mathcal{O} = \mathrm{Spec}\, \mathbb{F}_q & \xrightarrow{\mathcal{O}_E} & E. \end{array}$$

$\mathrm{Ker}(1 - \mathrm{Fr}_E)$ is a closed subgroup scheme of E.

We have $\ker(1-\mathrm{Fr}_E)(\mathbb{F}_q) = E(\mathbb{F}_q)$ because let $\operatorname{Spec}\mathbb{F}_q \xrightarrow{i} E$ be an $\mathbb{F}_q$-rational point. Then

$$\begin{array}{ccc} \operatorname{Spec}\mathbb{F}_q & \xrightarrow{i} & E \\ \| & & \big\downarrow{\scriptstyle 1-\mathrm{Fr}_E} \\ \operatorname{Spec}\mathbb{F}_q & \xrightarrow{0} & E \end{array}$$

commutes. So i factors $\operatorname{Spec}\mathbb{F}_q \to \ker(1-\mathrm{Fr}_E) \to E$. As $1-\mathrm{Fr}_E$ is étale, $\ker(1-\mathrm{Fr}_E) \cong \prod_{i=1}^r \operatorname{Spec} k_i$ with $k_i/\mathbb{F}_q$ finite, separable with $\dim_{\mathbb{F}_q}(\oplus_{i=1}^r k_i) = \deg(1-\mathrm{Fr}_E)$. But $1 = \mathrm{Fr}_E$ on $\ker(1-\mathrm{Fr}_E)$, so $\mathrm{Fr} = 1$ on $\operatorname{Spec} k_i \to \operatorname{Spec} k_i$ and thus $x^q = x$ for all $x \in k_i$, so that $k_i = \mathbb{F}_q$. Therefore $\ker(1-\mathrm{Fr}_E) = \prod_{i=1}^r \operatorname{Spec}\mathbb{F}_q$ and therefore $\deg(1-\mathrm{Fr}_E) = r = \#\ker(1-\mathrm{Fr}_E)(\mathbb{F}_q) = \#(E(\mathbb{F}_q))$. □

Definition 1.4.3. Let $X/\mathbb{F}_q$ be a smooth, projective, geometrically connected variety of dimension d. The *Zeta-function of* X is defined as follows

$$Z_X(t) = \prod_{x \in X_0} (1 - t^{\deg(x)})^{-1} \in \mathbb{Z}[[t]].$$

Here X_0 is the set of closed points on X and for $x \in X_0$, $\deg(x) = [k(x) : \mathbb{F}_q]$.

One can easily show that $\prod_{x\in X_0}(1-t^{\deg(x)})^{-1}$ converges absolutely in $\mathbb{Z}[[t]]$. The connection to the usual zeta-function,

$$\zeta_X(s) = \prod_{x \in X_0} (1 - N(x)^{-s})^{-1}, \qquad \mathrm{Re}(s) \gg 1$$

with $N(x) = \#k(x)$ is as follows:

$$\zeta_X(s) = Z_X(q^{-s}).$$

Theorem 1.4.4. *(Weil-Conjectures)*

a. $Z_X(t) \in \mathbb{Q}(t)$. *Moreover*

$$Z_X(t) = \frac{P_1(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)}$$

where $P_i(t)$ are polynomials in $\mathbb{Z}[[t]]$. We have $P_0(t) = 1-t$, $P_{2d}(t) = 1 - q^d t$.

b. *There is a functional equation*

$$Z_X\left(\frac{1}{q^d}t\right) = Z_X(t)\cdot\left(\pm\left(q^{\frac{d}{2}}t\right)^{\chi}\right)$$

where $\chi = (\Delta\cdot\Delta)$ is the self-intersection number of the diagonal $\Delta \subseteq X \times X$.

c. *Riemann hypothesis: if*

$$P_i(t) = \prod_j (1 - \alpha_{ij}t), \quad \alpha_{ij} \in \mathbb{C}$$

then $|\alpha_{ij}| = q^{\frac{i}{2}}$ *for all* i, j.

Proof. For $X = E$ an elliptic curve, this has been proven by Hasse. For X a curve or an abelian variety, the proof has been given by Weil himself. For arbitrary X, the theorem has been proven by Deligne. We will prove a) and c) in case of an elliptic curve.

Let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$\begin{aligned} Z_E(t) &= \prod_{x \in E_0} (1 - t^{\deg(x)})^{-1} \\ &= \prod_{x \in E_0} (\sum_{n \geq 0} t^{n \deg x}) \\ &= \sum_{\substack{D \geq 0 \\ \text{Divisor in } E}} t^{\deg D} \\ &= 1 + \sum_{n=1}^{\infty} \sum_{\substack{D \geq 0 \\ \deg D = n}} t^n. \end{aligned}$$

Let $D \geq 0$ be a divisor with $\deg D = n \geq 0$. Then

$$\#\{D' : D' \text{ effective divisor on } E \text{ with } D' \sim D\} = \frac{q^{l(D)} - 1}{q - 1}$$

with $l(D) = \dim H^0(E, \mathcal{L}(D))$, because

$$\begin{array}{ccc} (H^0(E, \mathcal{L}(D)) \backslash \{0\}) / \mathbb{F}_q^* & \longrightarrow & \{D' : D' \geq 0, D' \sim D\} \\ f & \longmapsto & (f) + D \end{array}$$

is a bijection. By Riemann-Roch we have $\dim H^0(E, \mathcal{L}(D)) = \deg D = n$.

Hence we obtain

$$\begin{aligned} Z_E(t) &= 1 + \sum_{n=1}^{\infty} \sum_{\substack{\mathfrak{a} \in \mathrm{Pic}(E) \\ \deg \mathfrak{a} = n}} \sum_{\substack{D \geq 0 \\ D \in \mathfrak{a}}} t^n \\ &= 1 + \sum_{n=1}^{\infty} t^n \frac{q^n - 1}{q - 1} \#\{\mathfrak{a} \in \mathrm{Pic}(E) : \deg \mathfrak{a} = n\} \\ &= 1 + \left(\sum_{n=1}^{\infty} t^n \sum_{i=1}^{n-1} q^i \right) \#\mathrm{Pic}^0(E) \\ &= 1 + \frac{t \cdot \#E(\mathbb{F}_q)}{(1-t)(1-qt)} \\ &= \frac{1 - at + qt^2}{(1-t)(1-qt)} \end{aligned}$$

with $a = 1 + q - \#E(\mathbb{F}_q)$.

Let $L_E(t) := 1 - at + qt^2$, so $L_E(t) = (1-\alpha t)(1-\beta t)$ for some $\alpha, \beta \in \mathbb{C}$. As $\alpha\beta = q$, we need to show — in order to prove c) for E – that $|\alpha| = |\beta|$.

We have $\alpha = \frac{a}{2} + \sqrt{\frac{a^2}{4} - q}$, $\beta = \frac{a}{2} - \sqrt{\frac{a^2}{4} - q}$. So we need to show: $4q \geq a^2$.

Put $A = \mathrm{End}_{\mathbb{F}_q}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.

The involution $f \mapsto \hat{f}$ and the degree map extend to maps

$$\begin{aligned} i &: A \longrightarrow A, \quad a \mapsto \hat{a}, \\ \deg &: A \longrightarrow \mathbb{Q}_{\geq 0}. \end{aligned}$$

We have $\widehat{ab} = \hat{b}\hat{a}$, $\hat{m} = m$ for all $m \in \mathbb{Q} \subseteq A$, $\deg a = a\hat{a} = \hat{a}a$, $\widehat{a+b} = \hat{a} + \hat{b}$.

We show that $\deg : A \to \mathbb{Q}_{\geq 0}$ is a positive definite quadratic form.

$$\beta(a,b) := \frac{1}{2}(q(a+b) - q(a) - q(b))$$

is bilinear, because

$$\beta(a,b) = \frac{1}{2}((a+b)(\widehat{a+b}) - a\hat{a} - b\hat{b}) = \frac{1}{2}(a\hat{b} + b\hat{a})$$

is bilinear.

The Cauchy-Schwartz inequality implies

$$|\beta(a,b)| \leq \sqrt{\deg(a)\deg(b)}$$

for all $a, b \in A$. For $a = \mathrm{Fr}_E$, $b = 1$ we obtain, using 1.4.1

$$|1 + q - \deg(1 - \mathrm{Fr}_E)|^2 \leq 4q.$$

Lemma 1.4.2 yields $|1 + q - \#E(\mathbb{F}_q)|^2 \leq 4q$; hence $a^2 \leq 4q$.

$\square$

Corollary 1.4.5. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$.*

Let G/S be a group scheme, $i : H \hookrightarrow G$ a closed immersion. Then H is called a *subgroup scheme* if $\mathrm{Hom}_S(T, H)$ is a subgroup of $\mathrm{Hom}_S(T, G)$ for all T.

For example, let $f : G_1 \to G_2$ be a homomorphism of group schemes over S. Then $\ker(f) = G_1 \times_{G_2} S$ is a subgroup scheme of G.

Let $m \geq 1$ and $f = [m] : E \to E$. Then $\ker[m]$ is denoted by $E[m]$, the subgroup scheme of m-torsion points of E.

Proposition 1.4.6. *Let E/k be an elliptic curve.*

a. *Let $m \in \mathbb{Z}$, $m \neq 0$, $\gcd(m, \mathrm{char}(k)) = 1$. Then $E[m](\bar{k}) \cong \mathbb{Z}/m \times \mathbb{Z}/m$.*
b. *Let $p = \mathrm{char}(k) > 0$. Then $E[p^r](\bar{k}) \cong \mathbb{Z}/p^r\mathbb{Z}$ or 0.*

Definition 1.4.7. Let E/k be an elliptic curve over k, with $\mathrm{char}(k) = p > 0$. E is called *ordinary* (resp. *supersingular*) if $E[p](\bar{k}) \cong \mathbb{Z}/p\mathbb{Z}$ (resp. $E[p](\bar{k}) = 0$).

Let E be an elliptic curve and l a prime that does not divide $\mathrm{char}(k)$.

Definition 1.4.8. $T_l(E) = \varprojlim E[l^r](\bar{k})(\cong \mathbb{Z}_l \oplus \mathbb{Z}_l)$ is called the *l-adic Tate-module of E*. $T_l(E)$ is a continuous $G_k = \mathrm{Gal}(\bar{k}/k)$-module.

Proposition 1.4.9. *Let E_1, E_2 be elliptic curves. The natural map* $\mathrm{Hom}_k(E_1, E_2) \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_l E_1, T_l E_2)$ *is injective.*

Corollary 1.4.10. $\mathrm{Hom}_k(E_1, E_2)$ *is a free $\mathbb{Z}$-module of rank less than or equal to* 4.

1.4.11. Let E/k be an elliptic curve. Then $\mathrm{End}(E)$ is isomorphic to one of the following rings

(i) $\mathbb{Z}$;
(ii) order in an imaginary quadratic field;
(iii) order in an indefinite quaternion algebra.

1.5. **Elliptic curves over p-adic fields.** Let $K/\mathbb{Q}_p$ be a finite extension with ring of integers R and residue field k. Let v be the discrete valuation on R and $\pi \in R$ be a uniformizing element. We assume $\mathrm{char}(k) \neq 2, 3$. Let E/k be an elliptic curve with affine Weierstrass equation $y^2 = x^3 + Ax + B$ and discriminant $\Delta = -16\ (4A^3 + 27B^3)$. The variable change $x = u^2 x',\ y = u^3 y'$, for some $u \in K^\times$ preserves this form. Then

$$u^4 A' = A,\ u^6 B' = B,\ u^{12}\Delta' = \Delta.$$

As E is nonsingular, we have $\Delta \neq 0$. By a change of variables we can achieve $A, B \in R$. Choose coordinates such that $v(\Delta)$ is minimal. Reduce the equation modulo π to obtain a curve $\widetilde{E}$:

$$\widetilde{E} : y^2 = x^3 + \widetilde{A}x + \widetilde{B}$$

which is possibly singular (if $v(\Delta) > 0$). Let $P \in E(K)$. Choose homogeneous coordinates $P = [x_0, y_0, z_0]$ such that all $x_0, y_0, z_0 \in R$ and at least one coordinate lies in $R^\times$. Then $\widetilde{P} = [\widetilde{x_0}, \widetilde{y_0}, \widetilde{z_0}] \in \widetilde{E}(k)$. The reduction map fits into a commutative diagram

$$\begin{array}{ccc} \mathbb{P}^n(K) & \longrightarrow & \mathbb{P}^n(k) \\ \uparrow\cup & & \uparrow\cup \\ E(K) & \longrightarrow & E(k). \end{array}$$

Definition 1.5.1. Let E be an elliptic curve and $\widetilde{E}$ be the reduced curve for a minimal Weierstrass equation. Then

(i) E has good reduction, if $\widetilde{E}$ is non-singular, hence an elliptic curve over k. This is equivalent to the condition $v(\Delta) = 0$, so $\Delta \in R^{\times}$.
(ii) E has multiplicative reduction if $v(\Delta) > 0$ and $A, B \in R^{\times}$.
(iii) E has additive reduction if $v(A) > 0,\ v(B) > 0$.

In case (ii) $\widetilde{E}$ has a singularity which is a node, in case (iii) $\widetilde{E}$ has a singularity which is a cusp. In case (ii), (iii) are saying that E has bad reduction.

Theorem 1.5.2. *Let F be a number field with ring of integers $\mathcal{O}_F$ and E/F be an elliptic curve. Let $F_{\mathfrak{p}}$ be the completion at some prime $\mathfrak{p}$. Then $E/F_{\mathfrak{p}}$, the elliptic curve obtained by base change $\otimes_F F_{\mathfrak{p}}$, has good reduction for almost all primes $\mathfrak{p} \subset \mathcal{O}_F$.*

2. Modular curves and Modular forms

2.1. **Riemann surfaces.**

Definition 2.1.1. Let M be a 2-dimensional manifold (i.e. M is Hausdorff and every $x \in M$ has an open neighbourhood homeomorphic to $\mathbb{R}^2$). A *complex structure* on M is a family of pairs $\{(\mathcal{U}_i, \phi_i), i \in I\}$ called *charts* with the following properties:

(i) $\phi_i : \mathcal{U}_i \to V_i$ is a homeomorphism where $\mathcal{U}_i \subseteq M$ and $V_i \subseteq \mathbb{C}$ are both open; and
(ii) for all pairs i and j $\phi_j \circ \phi_i^{-1} : \phi_i(\mathcal{U}_i \cap \mathcal{U}_j) \to \phi_j(\mathcal{U}_i \cap \mathcal{U}_j)$ is holomorphic and the union of all $\mathcal{U}_i$'s is M.

A *Riemann surface* is a 2-dimensional manifold together with a complex structure.

Let M be a Riemann surface and $\mathcal{U} \subseteq M$ an open subset. A function $f : \mathcal{U} \to \mathbb{C}$ is called *holomorphic* (resp. *meromorphic*) if $f \circ \phi_i^{-1} : \phi_i(\mathcal{U} \cap \mathcal{U}_i) \to \mathbb{C}$ is holomorphic (resp. meromorphic) for all charts $(\mathcal{U}_i, \phi_i)$ of M.

Example 2.1.2. *Let $X/\mathbb{C}$ be a smooth projective curve. Then $X(\mathbb{C})$ is a compact Riemann manifold.*

Proof. The topology on $X(\mathbb{C})$ is induced via the embedding $X(\mathbb{C}) \hookrightarrow \mathbb{P}^n_{\mathbb{C}}$.

For the complex structure, let $x \in X(\mathbb{C})$, $\mathbb{A}^n \subset \mathbb{P}^n$ affine with $x \in \mathbb{A}^n$. Then $X \cap \mathbb{A}^n = V(\mathfrak{p})$ where $\mathfrak{p} \subseteq \mathbb{C}[T_1, \ldots, T_n]$ is a prime ideal. Without loss of generality we may assume $x = 0$.

$\mathcal{O}_{\mathbb{C}^n,0}$ is a regular local ring with maximal ideal $\mathfrak{m}$. There are generators $F_1, \ldots, F_{n-1}, x_i \in \mathfrak{m}$ with $F_1, \ldots, F_{n-1}$ generators of $\mathfrak{p}\mathcal{O}_{\mathbb{C}^n,0}$. Again without loss of generality we may assume $i = n$.

Then there exist generators $g_1, \ldots, g_r$ of $\mathfrak{p}$ of the form $g_i = \sum_{j=1}^{n-1} \frac{h_{ij}}{k} F_j$ with $h_{ij}, k \in \mathbb{C}[T_1, \ldots, T_n]$ and $k(0) \neq 0$.

Hence in a small neighbourhood $\mathcal{U}$ of 0 in $\mathbb{C}^n$ we have that $z \in X$ if and only if $F_i(z) = 0$ for $i = 1, \ldots, n-1$.

As $(F_1, F_2, \ldots, F_{n-1}, x_n)$ are generators of $\mathfrak{m}$ we have that

$$\det\left(\frac{\partial F_i}{\partial x_j}(0), \frac{\partial x_n}{\partial x_j}(0)\right)_{\substack{1\le i\le n-1\\1\le j\le n}} \neq 0$$

and so

$$\det\left(\frac{\partial F_i}{\partial x_j}(0)\right)_{\substack{1\le i\le n-1\\1\le j\le n-1}} \neq 0.$$

The implicit function theorem yields that there exist an $\epsilon > 0$ and holomorphic functions $g_1(z), \ldots, g_{n-1}(z)$ for $|z| < \epsilon$ such that for $|z_1|, \ldots, |z_n| < \epsilon$ we have $F_i(z_1, \ldots, z_n) = 0$ for $i = 1, \ldots, n-1$ if and only if $z_i = g_i(z_n)$ for $i = 1, \ldots, n-1$.

Now let $D = \{(z_1, \ldots, z_n) \in \mathbb{C}^n : |z_i| < \epsilon\}$. Then

$$\begin{array}{rcl}(X \cap \mathbb{A}^n)(\mathbb{C}) \cap D & \to & \mathbb{C} \\ (z_1, \ldots, z_n) & \mapsto & z_n\end{array}$$

is a chart (choose ϵ small enough such that $k(z) \neq 0$ on D). $\square$

Holomorphic differential forms. Let M be a Riemann surface, $p \in M$. Then by $\mathcal{O}_{M,p} = \mathcal{O}_p$ we denote the germs of holomorphic functions in p and $\mathcal{O}_M$ the structure sheaf of holomorphic functions on M. $T_p(M) = \mathrm{Der}_{\mathcal{O}_p}(\mathcal{O}_p, \mathbb{C})$ is the $\mathbb{C}$-vector space of derivations $D : \mathcal{O}_p \to \mathbb{C}$.

Let $U \subseteq M$ be open. A differential form ω on M is an assignment

$$p \in U \mapsto \omega_p \in (T_p(M))^*.$$

For $f \in \Gamma(U, \mathcal{O})$ the differential form $\mathrm{d}f$ on U is defined by $(\mathrm{d}f)_p(D) = D(f_p)$ for all $D \in \mathrm{Der}(\mathcal{O}_p, \mathbb{C})$. A differential form ω on U is called holomorphic, if it is locally of the form $f\mathrm{d}g$ with f and g holomorphic. The sheaf of holomorphic differential forms is denoted Ω_M.

Definition 2.1.3. The *genus* of M is defined by $\dim_{\mathbb{C}} \Gamma(M, \Omega_M)$ and is denoted by g.

Proposition 2.1.4. *The assignment $X \mapsto X(\mathbb{C})$ defines an equivalence of categories*

$$\{\text{smooth projective curves over } \mathbb{C}\} \xrightarrow{\cong} \{\text{compact Riemann surfaces}\}.$$

We have

$$\begin{array}{rcl}H^i(X, \mathcal{O}_X) & \cong & H^i(X(\mathbb{C}), \mathcal{O}_{X(\mathbb{C})}), \\ H^i(X, \Omega_X) & \cong & H^i(X(\mathbb{C}), \Omega_{X(\mathbb{C})}).\end{array}$$

Proposition 2.1.5. *Let M be a compact Riemann manifold. Then, in singular cohomology, we have*

$$H^1_{\mathrm{sing}}(M, \mathbb{Z}) \cong \mathbb{Z}^{2g}$$

where g is the genus of M.

Proof. We have $H^1_{\text{sing}}(M, \mathbb{Z}) \cong H^1(M, \mathbb{Z})$, the latter denoting sheaf cohomology. We know that $H^1(M, \mathbb{Z})$ is torsion-free and finitely generated. It suffices to show that $H^1(M, \mathbb{C}) = H^1(M, \mathbb{Z}) \otimes \mathbb{C}$ is a $2g$-dimensional $\mathbb{C}$-vector space.

Consider the complex of sheaves

$$0 \longrightarrow \mathbb{C} \longrightarrow \mathcal{O}_M \xrightarrow{\mathrm{d}} \Omega \longrightarrow 0.$$

It is exact, because locally any holomorphic form ω is of the form $\omega = \mathrm{d}F = f\mathrm{d}z$.

We have an exact sequence

$$\begin{aligned} 0 \longrightarrow \mathbb{C} \xrightarrow{\equiv} H^0(M, \mathcal{O}_M) = \mathbb{C} \longrightarrow H^0(M, \Omega_M) \\ \longrightarrow H^1(M, \mathbb{C}) \longrightarrow H^1(M, \mathcal{O}_M) \longrightarrow H^1(M, \Omega_M) \\ \longrightarrow H^2(M, \mathbb{C}) \longrightarrow 0. \end{aligned}$$

By Riemann-Roch we have $\dim H^1(M, \Omega_M) = 1$. Hence we get a short exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(M, \Omega_M) \longrightarrow H^1(M, \mathbb{C}) \longrightarrow H^1(M, \mathcal{O}_M) \cong \\ H^0(M, \Omega_M)^* \longrightarrow 0 \end{aligned}$$

and thus $\dim H^1(M, \mathbb{C}) = \dim H^0(M, \Omega_M) + \dim H^0(M, \Omega_M)^* = 2g$. □

Let V be a finite dimensional complex space. A subgroup $\Gamma \subset V$ is called a *lattice* if Γ is discrete and V/Γ is compact. Equivalently, $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_{2g}$ for a $\mathbb{R}$-basis $(v_1, \ldots v_{2g})$ of V.

Let now Γ be a lattice in $\mathbb{C}$. Then $E_\Gamma = \mathbb{C}/\Gamma$ is a compact Riemann surface in a canonical way. We have $g(E_\Gamma) = 1$ because for the fundamental group one has $\pi_1(E_\Gamma) = \Gamma$ and $\pi_1(E_\Gamma) = H_1(E_\Gamma, \mathbb{Z}) = H^1(E_\Gamma, \mathbb{Z}) = \operatorname{Hom}(\Gamma, \mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Z}$. This implies $g(E_\Gamma) = 1$ by proposition 2.1.5.

Alternatively, $E_\Gamma = \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z} \cong S^1 \times S^1$ (as topological spaces) and thus $H^1(E_\Gamma, \mathbb{Z}) \cong H^1(S^1 \times S^1, \mathbb{Z}) \cong \mathbb{Z}^2$.

It follows that E_Γ together with $0 \mod \Gamma$ is an elliptic curve; the addition law is the canonical one.

The following questions arise: is any elliptic curve of the form E_Γ? What are the morphism $E_\Gamma \to E_{\Gamma'}$?

Let <u>Lattices</u> be the category of lattices Γ in $\mathbb{C}$ with $\operatorname{Hom}(\Gamma_1, \Gamma_2)$ defined as those homeomorphisms $f : \Gamma_1 \to \Gamma_2$ for which there exists an $\alpha \in \mathbb{C}$ such that $f(\gamma) = \alpha\gamma$ for all $\gamma \in \Gamma_1$.

Proposition 2.1.6. *We have an equivalence of categories*

$$\underline{\text{Lattices}} \xrightarrow{\cong} \left\{ \begin{array}{c} \text{compact Riemann surfaces of} \\ \text{genus 1 with zero-point} \end{array} \right\} \xrightarrow{\cong} \{\text{elliptic curves}/\mathbb{C}\}.$$

Proof. Let M be a compact Riemann surface with $g(M) = 1$ with $0 \in M$. We need to show that there exists a Γ such that $E_\Gamma \cong M$.

There exists an exact sequence of sheaves

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_M \xrightarrow{\exp(2\pi i)} \mathcal{O}_M^* \longrightarrow 0$$

which yields the exact sequence

$$\begin{array}{cccccccc} & H^0(M,\mathcal{O}_M) & \xrightarrow{\exp(2\pi i)} & H^0(M,\mathcal{O}_M^*) & \longrightarrow & H^1(M,\mathbb{Z}) & \\ & (\cong \mathbb{C}) & & (\cong \mathbb{C}^*) & & =: \Gamma & \\ \longrightarrow & H^1(M,\mathcal{O}_M) & \longrightarrow & \mathrm{Pic}(M) & \xrightarrow{\deg} & H^2(M,\mathbb{Z}) & \longrightarrow 0 \\ & (\cong \mathbb{C}) & & (= H^1(M,\mathcal{O}_M^*)) & & (\cong Z) & \end{array}$$

and thus $M = \mathrm{Pic}^0(M) \cong \mathbb{C}/\Gamma$.

It remains to show that $\mathrm{Hom}(E_{\Gamma_1}, E_{\Gamma_2}) \cong \mathrm{Hom}(\Gamma_1, \Gamma_2)$.

Let f be a homomorphism and g be a holomorphic function such that the square

$$\begin{tikzcd} \mathbb{C} \arrow[r, "g"] \arrow[d] & \mathbb{C} \arrow[d] \\ E_{\Gamma_1} \arrow[r, "f"] & E_{\Gamma_2} \end{tikzcd}$$

commutes.

For all $\gamma \in \Gamma_1$ the function $z \mapsto g(z+\gamma) - g(z)$ is discrete; hence it is constant. So for all $z, \gamma \in \Gamma_1$ we have that $g'(z+\gamma) = g'(z)$ and thus $g'(z)$ is holomorphic on $\mathbb{C}/\Gamma$; hence it is also constant. Thus g is of the form $\alpha z + \beta$ for some $\beta \in \Gamma_2$ and without loss of generality we may assume that $g(z) = \alpha z$. $\square$

2.2. **Modular curves as Riemann surfaces.** Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be the complex upper half plane and $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1_{\mathbb{Q}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

The elements of $\mathbb{P}^1_{\mathbb{Q}} \subset \mathbb{H}^*$ are called *cusps*. $\mathbb{H}^*$ is equipped with an action of $SL_2(\mathbb{Z})$: for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}), z \in \mathbb{H}$, αz is defined to be $\frac{az+b}{cz+d}$, while if $z = (x : y) \in \mathbb{P}^1_{\mathbb{Q}}$, then $\alpha z = \frac{ax+by}{cx+dy}$.

We set $j(\alpha, z) = cz + d$ for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $z \in \mathbb{H}$. We then have

$$j(\alpha\beta, z) = j(\alpha, \beta z) j(\beta, z)$$

and

$$\mathrm{Im}(\alpha z) = \mathrm{Im}\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) = \frac{\mathrm{Im}(z)}{|j(\alpha,z)|^2}.$$

Let $\Gamma \subset SL_2(\mathbb{Z})$ be a fixed subgroup of finite index. For $z \in \mathbb{H}^*$ let $\Gamma_z = \{\gamma \in \Gamma : \gamma z = z\}$, the stabilizer group of z.

Remark 2.2.1.

a. $SL_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1_{\mathbb{Q}}$;
b. $\Gamma_\infty = \Gamma \cap \left\{\left(\begin{smallmatrix} \pm 1 & m \\ 0 & \pm 1 \end{smallmatrix}\right) : m \in \mathbb{Z}\right\}$.

Proof.

a. Let $r = \frac{a}{b} \in \mathbb{Q}$, with $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$. Then there exist $c, d \in \mathbb{Z}$ such that $ad - bc = 1$ and thus $r = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)\infty$.
b. Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\infty$. Then $(a : c) = (1 : 0)$ and thus $c = 0$, so that $ad = 1$ and therefore $a = d = \pm 1$.

$\square$

We define $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$ and $Y(\Gamma) = \Gamma\backslash\mathbb{H}$. The images of $\mathbb{Q} \cup \infty$ under the projection $\mathbb{H}^* \to X(\Gamma)$ are called cusps. We want to show that $X(\Gamma)$ is a compact Riemann surface.

Definition 2.2.2. We define a topology on $\mathbb{H}^*$ as follows:

On $\mathbb{H}$ we choose the natural topology induced by $\mathbb{C}$. For a cusp $s \in \mathbb{Q}$, the sets $\{s\} \cup \{z \in \mathbb{H} : |z - (s + ir)| < r\}$ for $r \in \mathbb{R}_+^*$ form a basis of neighbourhoods of s.

For the cusp $s = \infty$, we define $\{\infty\} \cup \{z \in \mathbb{H} : \mathrm{Im}(z) > r\}$ for $r \in \mathbb{R}_+^*$ as a basis of neighbourhoods.

We remark that $\alpha \in \Gamma$ maps the basis of neighbourhoods of the cusp to the basis of neighbourhoods of the cusp $\alpha(s)$. Consequently, Γ acts continuously on $\mathbb{H}^*$.

Lemma 2.2.3.

a. *Let $A, B \subseteq \mathbb{H}$ be compact subsets. Then $\{\gamma \in \Gamma : \gamma A \cap B \neq \emptyset\}$ is finite;*
b. *let $A \subseteq \mathbb{H}$ be compact and $s \in \mathbb{H}^*$ a cusp. Then there exists a neighbourhood U of s such that $\{\gamma \in \Gamma : U \cap \gamma A \neq \emptyset\}$ is finite.*

Proof.

a. Without loss of generality, we may assume $A = B$. There exist $r, R > 0$ such that $r \leq \mathrm{Im}(z) \leq R$ for all $z \in A$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ with $\gamma A \cap A \neq \emptyset$.

   Then for $z \in \gamma A \cap A$ we have $r \leq \mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)}{|j(\gamma,z)|^2} \leq \frac{R}{|j(\gamma,z)|^2}$. Thus $|j(\gamma,z)|^2 \leq \frac{R}{r}$ and thus $c^2\mathrm{Im}(z)^2 \leq |cz+d|^2 \leq \frac{R}{r}$ so that $c^2r^2 \leq \frac{R}{r}$ and therefore $c \leq \sqrt{\frac{R}{r^3}}$ so that c and z are bounded and thus d is bounded too.

   As $\gamma A \cap A \neq \emptyset$ implies $\gamma^{-1} A \cap A \neq \emptyset$ and using $\gamma^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, it follows that a is bounded too. Since both az and $cz + d$ are bounded, b is also bounded.
b. Without loss of generality, we may assume that $s = \infty$. There exist $r, R > 0$ such that $r \leq \mathrm{Im}(z) \leq R$ for all $z \in A$. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma\backslash\Gamma_\infty$ (so $c \neq 0$) we have $\mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)}{|cz+d|^2} \leq \frac{\mathrm{Im}(z)}{(c\mathrm{Im}(z))^2} \leq \frac{1}{\mathrm{Im}(z)} \leq \frac{1}{r}$ for all $z \in A$.

   For $\gamma \in \Gamma_\infty, z \in A$ we have $\mathrm{Im}(\gamma z) = \mathrm{Im}(z) \leq R$, so $\gamma A \cap \{z | \mathrm{Im}(z) > \max(\frac{1}{r}, R)\} = \emptyset$ for all $\gamma \in \Gamma$, hence b. follows.

□

We endow the quotient topology on $X(\Gamma)$ with respect to the projection $\pi : \mathbb{H}^* \to X(\Gamma)$.

Proposition 2.2.4. *$X(\Gamma)$ is a Hausdorff space.*

Proof. As π is open, we need to show the following claim: for $x, y \in \mathbb{H}^*$ with $\gamma x \neq y$ for all $\gamma \in \Gamma$ there are neighbourhoods U, V of x resp. y with $\gamma U \cap V = \emptyset$ for all $\gamma \in \Gamma$.

Case 1: $x, y \in \mathbb{H}$. There exists a compact neighbourhood U of x with $y \notin \gamma U$ for all $\gamma \in \Gamma$, because $\{\gamma \in \Gamma : \gamma U' \cap \{y\} \neq \emptyset\}$ is finite for any compact neighbourhood U' of x; we take U such that $U \subseteq U' \backslash \cup_{\gamma \in \Gamma} \gamma y$.

Let V' be a compact neighbourhood of y. Then $V' \backslash \cup_{\gamma\in\Gamma} \gamma U$ is a neighbourhood of y. Choose V to be a neighbourhood of y with $V \subseteq V' \backslash \cup_{\gamma\in\Gamma} \gamma U$.

Case 2: $x \in \mathbb{H}$, $y \in \mathbb{P}^1_{\mathbb{Q}}$. This is clear by the second part of Lemma 2.2.3.

Case 3: x and y are both cusps. Without loss of generality we may assume $y = \infty$. Put $L = \{z : \mathrm{Im}(z) = 1\}$ and $K = \{z : \mathrm{Im}(z) = 1, 0 \leq \mathrm{Re}(z) \ \leq h\}$ a section of L, such that $\cup_{\gamma\in\Gamma_\infty} \gamma K = L$.

By the second part of Lemma 2.2.3, there exists a neighbourhood V of $y = \infty$ with $V \cap \gamma K = \emptyset$ and a neighbourhood U of x with $U \cap \gamma K = \emptyset$ for all $\gamma \in \Gamma$. So $\gamma U \cap L = \emptyset$ and $\gamma V \cap L = \emptyset$ for all $\gamma \in \Gamma$; hence $U \cap \gamma V = \emptyset$ for all $\gamma \in \Gamma$. □

Proposition 2.2.5. *$X(\Gamma)$ is compact.*

We first show the following

Lemma 2.2.6. *Let $\mathcal{F} = \{z \in \mathbb{H} : |z| \geq 1, -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}\}$. Then $\mathcal{F} \to SL_2(\mathbb{Z})\backslash\mathbb{H}$ is surjective. More precisely, $\mathcal{F}$ is a fundamental domain, i.e. $\cup_{\gamma\in SL_2(\mathbb{Z})} \gamma\mathcal{F} = \mathbb{H}$ and $\gamma\mathcal{F}^\circ \cap \mathcal{F}^\circ = \emptyset$ for all $\gamma \in \Gamma$, $\gamma \neq 1$.*

Proof. For $z \in \mathbb{H}$, $\{\mathrm{Im}(\gamma z) : \gamma \in \Gamma\}$ is bounded from above (2.2.3, b), hence attains its maximum. Let, without loss of generality, z be such that $\mathrm{Im}(z) = \max\{\mathrm{Im}(\gamma z) : \gamma \in \Gamma\}$. After translation, we may assume that $-\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}$.

Assume $z \notin \mathcal{F}$, so that $|z| < 1$. For $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ we have $\mathrm{Im}(Sz) = \mathrm{Im}(-\frac{1}{z}) = \frac{\mathrm{Im}(z)}{|z|^2} > \mathrm{Im}(z)$. This contradicts the choice of z; hence $z \in \mathcal{F}$.

It is an easy exercise to show that the subgroup of $SL_2(\mathbb{Z})$ generated by S and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ coincides with $SL_2(\mathbb{Z})$. From this the Lemma follows. □

Proof (of 2.2.5). Consider the case $\Gamma = SL_2(\mathbb{Z})$. Let $\{U_i\}_{i\in I}$ be an open covering of $X(\Gamma)$. Assume $i_0 \in I$ such that $\pi^{-1}(U_{i_0})$ is a neighbourhood of ∞. Then $\{\pi^{-1}(U_i)\}_{i\in I\backslash i_0}$ is an open covering of the compact set $\mathcal{F}\backslash\pi^{-1}(U_{i_0})$, hence it has a finite sub-covering. The same then holds for $\{U_i\}$ and thus $X(\Gamma)$ is compact for $\Gamma = SL_2(\mathbb{Z})$.

If $\Gamma \subseteq SL_2(\mathbb{Z})$ is a subgroup of finite index, then $SL_2(\mathbb{Z}) = \cup_{i=1}^r \Gamma\alpha_i$, so $\cup_{i=1}^r \alpha_i (\mathcal{F} \cup \{\infty\}) \subset \mathbb{H}^*$ is compact and

$$\cup_{i=1}^r \alpha_i (\mathcal{F} \cup \{\infty\}) \longrightarrow \mathbb{H}^* \longrightarrow X(\Gamma)$$

is surjective; hence $X(\Gamma)$ is compact. □

The complex structure on $\Gamma\backslash\mathbb{H}^*$.

Lemma 2.2.7.

a. *Let P_0 be a cusp. Then there exists a unique natural number $h > 0$ such that for $\rho \in SL_2(\mathbb{Z})$ with $\rho(P_0) = \infty$ we have*

$$\Gamma_{P_0} = \rho^{-1} \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m : m \in \mathbb{Z} \right\} \rho.$$

b. *Let $P \in \mathbb{H}$. Then Γ_P is a finite cyclic group.*

Proof.

a. Using 2.2.1 we have $\Gamma_{P_0} = \rho^{-1} (\rho\Gamma\rho^{-1})_\infty \rho$ and, for some $h \in \mathbb{N}$, $h > 0$, $(\rho\Gamma\rho^{-1})_\infty = \left\{ \pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)^m : m \in \mathbb{Z} \right\}$. It remains to show that h does not depend on the choice of ρ.

If $\rho P_0 = \infty = \rho' P_0$, then $\rho' = \gamma\rho$ with $\gamma = \pm \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for some $n \in \mathbb{Z}$, so $(\rho'\Gamma\rho'^{-1})_\infty = (\gamma\rho\Gamma\rho^{-1}\gamma^{-1})_\infty = \gamma(\rho\Gamma\rho^{-1})_\infty\gamma^{-1} = (\rho\Gamma\rho^{-1})_\infty$.

b. by 2.2.3 a, Γ_P is finite. Let $\alpha \in SL_2(\mathbb{R})$ such that $\alpha i = P$. Then $\alpha^{-1}\Gamma_p\alpha$ is a finite subgroup of $\{\beta \in SL_2(\mathbb{R}) : \beta i = i\} = \left\{ \left(\begin{smallmatrix} \sin z & \cos z \\ -\cos z & \sin z \end{smallmatrix}\right) : z \in \mathbb{R} \right\} \cong \left\{ \xi \in \mathbb{C} : \xi\bar{\xi} = 1 \right\}$. So $\alpha^{-1}\Gamma_p\alpha$ is cyclic and then so is Γ_P.

□

Lemma 2.2.8. *Let $P \in \mathbb{H}^*$. Then there exists a neighbourhood U of P with the following properties:*

(i) *if $\gamma U \cap U \neq \emptyset$ then $\gamma \in \Gamma_P$;*
(ii) *$\gamma U = U$ for all $\gamma \in \Gamma_P$.*

Proof. First case: let P be a cusp; without loss of generality we may assume $P = \infty$. We choose $U = \{z \in \mathbb{H} : \mathrm{Im}(z) > 1\}$. For $\gamma \in \Gamma\backslash\Gamma_\infty$ we have, writing $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \neq 0$:

$$\mathrm{Im}\,(\gamma z) = \frac{\mathrm{Im}(z)}{|j(\gamma, z)|^2} \leq \frac{\mathrm{Im}(z)}{c^2 \mathrm{Im}(z)^2} \leq \frac{1}{\mathrm{Im}(z)} < 1$$

for $z \in U$, so $\gamma U \cap U = \emptyset$. For $\gamma \in \Gamma_\infty$ we have $\gamma U = U$.

Second case: $P \in \mathbb{H}$. There exists a compact neighbourhood U' of P with $\Gamma' := \{\gamma : \gamma U' \cap U' \neq \emptyset\}$ is finite. Then there exists an $U_0 \subseteq U' \backslash \cup_{\gamma \in \Gamma' \backslash \Gamma_P} \gamma U'$, an open neighbourhood of P such that $\gamma U_0 \cap U_0 \neq \emptyset$ implies $\gamma \in \Gamma_P$.

Finally define $U := \cap_{\gamma \in \Gamma_P} \gamma U_0$. □

For $P \in \mathbb{H}$ define the order e_P of P as follows: $e_P = \frac{1}{2}\#(\Gamma_P)$. (Note that $\{\pm 1\} \subseteq \Gamma_P$.) P is called an elliptic point if $e_P > 1$.

Let $\lambda : \mathbb{H} \to \mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ be a biholomorphic map with $\lambda(P) = 0$ (for example $\lambda(z) = \frac{z-P}{z-\bar{P}}$). Let $\gamma \in \Gamma_P$ be a generator of Γ_P. Let $\bar{\gamma} = \lambda \circ \gamma \circ \lambda^{-1} : \mathbb{D} \to \mathbb{D}$. Then $\bar{\gamma}$ is an isomorphism with $\bar{\gamma}(0) = 0$ and $\bar{\gamma}^{e_P} = \mathrm{id}$, so $\bar{\gamma}(z) = \xi z$ for all $z \in \mathbb{D}$, where ξ is a primitive e_P-th root of unity (Schwarz' Lemma).

Lemma 2.2.9. *The map $\mathbb{D} \to \mathbb{D}$, $z \mapsto z^{e_P}$ induces a homeomorphism $\mathbb{D}/\langle\bar{\gamma}\rangle \xrightarrow{\cong} \mathbb{D}$.*

Let U be as in lemma 2.2.8. Then the map

$$\begin{array}{cccccccc} \lambda_P : & \Gamma_P\backslash U & \xrightarrow{\lambda} & \langle\bar{\gamma}\rangle\backslash\mathbb{D} & \longrightarrow & \mathbb{D} & \subseteq \mathbb{C} \\ & \subset \Gamma_P\backslash\mathbb{H}^* & & z & \longmapsto & z^{e_P} & \end{array}$$

is a homeomorphism onto an open subset of $\mathbb{C}$.

Lemma 2.2.10. *The map*

$$\begin{array}{rcl} U_\infty = \{z \in \mathbb{H} : \mathrm{Im}(z) > 1\} \cup \infty & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \begin{cases} \exp\left(\frac{2\pi i z}{h}\right) & \text{if } z \in \mathbb{H} \\ 0 & \text{if } z = \infty \end{cases} \end{array}$$

induces a homeomorphism

$$\lambda_\infty : \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m : m \in \mathbb{Z} \right\} \backslash U_\infty \longrightarrow V \subseteq \mathbb{C}$$

onto an open disc V around 0.

For the cusp P we obtain, by using 2.2.7, a homeomorphism

$$\begin{array}{lll} \lambda_P : & \Gamma_P\backslash\rho^{-1}(U_\infty) & \xrightarrow{\rho} \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m : m \in \mathbb{Z} \right\} \backslash U_\infty \to V \subseteq \mathbb{C}. \\ & \subseteq \Gamma\backslash\mathbb{H}^* & \end{array}$$

The λ_P, for $P \in \mathbb{H}^*$ defined as above, define the complex structure on $X(\Gamma)$.

2.3. **Moduli properties of modular curves.** Let $N \geq 1$ be a natural number. We define

$$\begin{array}{rcl} \Gamma_0(N) & = & \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \mod N \right\}, \\ X_0(N) & = & X(\Gamma_0(N)) = \Gamma_0(N)\backslash\mathbb{H}^*, \\ Y_0(N) & = & Y(\Gamma_0(N)) = \Gamma_0(N)\backslash\mathbb{H}. \end{array}$$

In the following we discuss the modular curves $X_0(N)$ (resp. $Y_0(N)$) as moduli spaces of elliptic curves with Level structure.

Proposition 2.3.1. *There is a canonical bijection of the set $\mathcal{ELL}_0(N)(\mathbb{C})$ of isomorphism classes of pairs (E, C), where E as an elliptic curve over $\mathbb{C}$ and C a cyclic subgroup of $E(\mathbb{C})$ of order N, and the set $Y_0(N)$:*

$$\varphi : \mathcal{ELL}_0(N)(\mathbb{C}) \to Y_0(N).$$

Proof. Case 1: Let $N = 1$. For $z \in \mathbb{H}$ we consider the lattice $\Lambda_z = \mathbb{Z} \oplus \mathbb{Z}z$ and define $E_z = \mathbb{C}/\Lambda$. For $z, z' \in \mathbb{H}$ we have

$$E_z \cong E_{z'} \iff \gamma z = z' \quad \text{for some } \gamma \in SL_2(\mathbb{Z}).$$

" $\Leftarrow$ ": Let $E_z \cong E_{z'}$. Then there exists $\lambda \in \mathbb{C}^\times : \lambda\Lambda_{z'} = \Lambda_z$. So $\lambda_{z'} = az + b, \lambda = cz + d$ with $a, b, c, d \in \mathbb{Z}$. We have moreover $\lambda^{-1}z = a'z' + b', \lambda^{-1} = c'z' + d'$, as $\lambda^{-1}\Lambda_z = \Lambda_{z'}$, hence $\gamma z = z'$ with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
We have $\mathbb{R}$-linear maps

$$\begin{aligned} f &: \mathbb{C} \longrightarrow \mathbb{C},\, u \longmapsto \lambda u, \\ g &: \mathbb{C} \longrightarrow \mathbb{C},\, u \longmapsto \lambda^{-1} u. \end{aligned}$$

The matrix of f with respect to basis $(1, z), (1, z')$ is $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the matrix of g with respect to basis $(1, z'), (1, z)$ is $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$,
hence $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$. Then

$$0 < \mathrm{Im} z' = \mathrm{Im}\frac{az + b}{cz + d} = \frac{\det\gamma \cdot \mathrm{Im} z}{|cz + d|^2} \Rightarrow \det\gamma = 1.$$

" $\Rightarrow$ " : Define $\lambda = cz + d$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$\lambda z' = \lambda\gamma z = az + b, \lambda = cz + d \;\Rightarrow \lambda\Lambda_{z'} \subseteqq \Lambda_z.$$

For $\gamma^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ we have $\gamma^{-1}z' = z$, so $(-cz' + a)\Lambda_z \subseteqq \Lambda_{z'}$ and

$$-cz' + a = j(\gamma^{-1}, \gamma z) = j(1, z)j(\gamma, z)^{-1} = \lambda^{-1} \Rightarrow \lambda\Lambda_{z'} \subseteqq \Lambda_z,$$

hence we have $E_z \cong E_{z'}$.
Let Λ be an arbitrary lattice on $\mathbb{C}$ and w_1, w_2 a $\mathbb{R}$-basis without loss of generality $\mathrm{Im}(w_1/w_2) > 0$. Define $z := w_1/w_2 \in \mathbb{H}$. Then $\Lambda = w_2\Lambda_z$, i.e. $\mathbb{C}/\Lambda \cong E_z$. Hence the map

$$\begin{aligned} SL_2(\mathbb{Z})\backslash\mathbb{H} &\longrightarrow \text{Isomorphism classes of elliptic curves} \\ z &\longmapsto E_z \end{aligned}$$

is a bijection.
Case 2: $N > 1$. Define $C_z = \dfrac{1}{N}\mathbb{Z} + z\mathbb{Z}/\Lambda_z \subseteqq E_z$, then $(E_z, C_z) \cong$

$(E_{z'}, C_{z'}) \iff$ there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $\gamma z = z'$ and for $\lambda = cz + d$ we have

$$(*) \qquad \lambda(\frac{1}{N}\mathbb{Z} + \mathbb{Z}z') = \frac{1}{N}\mathbb{Z} + \mathbb{Z}z.$$

Consider the diagram

$$\begin{array}{ccccl} \mathbb{Z}^2 & \xrightarrow{\Psi} & \Lambda_{z'} & & e_1 \mapsto z', e_2 \mapsto 1, \\ {\scriptstyle \begin{pmatrix} a & b \\ c & d \end{pmatrix}} \downarrow & & \downarrow {\scriptstyle f} & & \\ \mathbb{Z}^2 & \longrightarrow & \Lambda_z & & e_1 \mapsto z, e_2 \mapsto 1. \end{array}$$

Then (*) implies;

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} e_2 = me_2 \text{ modulo } N \text{ for some } m \in \mathbb{Z} \Leftrightarrow c \equiv 0 \text{ modulo } N.$$

So $(E_z, C_z) \cong (E_{z'}, C_{z'})$ is equivalent that there exists $\gamma \in \Gamma_0(N)$ such that $\gamma z = z'$. It remains to show; for all (E, C) there exists an isomorphism $z : (E, C) \cong (E_z, C_z)$. Choosing $z' \in \mathbb{H}$ such that $E_{z'} \cong E$, then $(E, C) \cong (E_{z'}, C_{z'})$ with $C' = \Lambda'/\Lambda_{z'}$. Choose $\gamma \in SL_2(\mathbb{Z})$ with $\gamma^t \circ \Psi^{-1}(N\Lambda') = Ne_1\mathbb{Z} + e_2\mathbb{Z}$. Then $(E, C) \cong (E_z, C_z)$ with $z = \gamma^{-1}z'$. □

Let S be a noetherian scheme, $\mathcal{F} : \mathbf{Sch}/S \to$ Sets, a contravariant functor from the category $\mathbf{Sch}/S$ of noetherian S-schemes to the category of sets.

Definition 2.3.2. A (noetherian) S-scheme M is called fine moduli space for $\mathcal{F}$, if M represents the functor $\mathcal{F}$, i.e. if there is an isomorphism of functor

$$\mathcal{F} \longrightarrow \mathrm{Hom}_{\mathbf{Sch}/S}(\ , M).$$

Let $N \geq 1$. We consider the following functor

$$\begin{array}{rcl} \mathcal{ELL}_0(N) : \mathbf{Sch}/\mathrm{Spec}\ \mathbb{Z}[\frac{1}{N}] & \longrightarrow & \text{Sets} \\ S & \longrightarrow & \left\{ \begin{array}{c} \text{Isomorphism classes of pairs } (E, C) \\ \text{where } E/S \text{ is an elliptic curve and} \\ C \text{ a cyclic subgroup of order } N \end{array} \right\}. \end{array}$$

Remark. Note that "$E \xrightarrow{\pi} S$ is an elliptic curve" means that E/S is on abelian scheme of relative dimension 1. (This implies that all fibers are elliptic curves). A cyclic subgroup C on E of order N is a closed subgroup scheme of E, such that $\pi : C \to E \to S$ is finite, flat and $\pi_* O_C$ a locally free O_S-module of rank N. Moreover if Spec $\Omega \to S$ is a geometric point, then $C(\Omega) \cong \mathbb{Z}/N\mathbb{Z}$.

Lemma 2.3.3. $\mathcal{ELL}_0(N)$ *does not have a fine moduli space.*

Proof. Assume it does have a fine moduli space that we denote by M. Let k'/k be an extension of fields with $(\mathrm{char}(k), N) = 1$ or $\mathrm{char}(k) = 0$. Then $M(k) \to M(k')$ is injective, hence $\mathcal{ELL}_0(N)(k) \to \mathcal{ELL}_0(N)(k')$ is injective. Let $(E, C) \in \mathcal{ELL}_0(N)(k)$. Choose k with $k^\times/(k^\times)^2 \neq 1$, $(\mathrm{char}(k), 2N) = 1$. Then $\{\pm\mathrm{id}\} \cong \mathbb{Z}/2\mathbb{Z} \subsetneqq \mathrm{Aut}(E, C)$. Let $\varphi : G_k \to \{\pm\mathrm{id}\} \subsetneqq \mathrm{Aut}(E, C)$ a nontrivial homomorphism (ex. because $H^1(k, \mu_2) \cong k^\times/(k^\times)^2$). Let $k' = \bar{k}^{\ker\varphi}$, so

$$\varphi : G_k \to \mathrm{Gal}(k'/k) \xrightarrow{\bar{\varphi}} \{\pm\mathrm{id}\}.$$

The pair $(E \times_k k', C \times_k k')$ with the $\mathrm{Gal}(k'/k)$-action $\bar{\varphi}(\sigma) \times \sigma, \sigma \in \mathrm{Gal}(k'/k)$ comes via base change k'/k from a pair $(E', C') \in \mathcal{ELL}_0(N)(k)$. We have $(E', C') \times_k k' \cong (E, C) \times_k k'$ but $(E, C) \ncong (E', C')$.
This finishes the proof of the Lemma. □

Definition 2.3.4. A S-scheme M is called coarse moduli space for $F : \mathbf{Sch}/S \to \mathrm{Sets}$ if there exists a morphism

$$\varphi : F \longrightarrow \mathrm{Hom}(\ , M)$$

such that

a. If $\mathrm{Spec}\ \bar{k} \to S$ is a geometric point, then φ induces an isomorphism
$$F(\bar{k}) \longrightarrow \mathrm{Hom}(\mathrm{Spec}\ \bar{k}, M),$$
b. φ is universal with respect to morphisms $F \to \mathrm{Hom}(\ , M)$, i.e.
$$\mathrm{Hom}(F, \mathrm{Hom}(\ , N)) \cong \mathrm{Hom}_{\mathbf{Sch}/S}(M, N)$$
for any S-scheme N.

If a coarse moduli space exists, then it is uniquely determined by b. (up to isomorphism).

Proposition 2.3.5. $\mathcal{ELL}_0(N)$ *has a coarse moduli space denoted by* $Y_0(N) \to \mathrm{Spec}\ \mathbb{Z}[\frac{1}{N}]$. $Y_0(N)$ *is smooth and quasi-projective over* $\mathbb{Z}[\frac{1}{N}]$ *of relative dimension* 1.

Finally we briefly discuss the moduli problem for $X_0(N)$.

Definition 2.3.6. A generalized elliptic curve over S is a stable curve $\pi : \mathcal{C} \to S$ of genus 1, i.e. π is proper flat, all geometric fibers $\mathcal{C}_{\bar{s}}$ for $\bar{s} \in S$ are reduced, connected and 1-dimensional and satisfy the following conditions;

a. $\mathcal{C}_{\bar{s}}$ has only ordinary double points as singularities.
b. $\dim_{k(\bar{s})} H^1(\mathcal{C}_{\bar{s}}, O_{\mathcal{C}_{\bar{s}}}) = 1$

together with a morphism

$$\text{“}+\text{”} : \mathcal{C}^{\mathrm{reg}} \times_S \mathcal{C} \longrightarrow \mathcal{C}$$

(where $\mathcal{C}^{\mathrm{reg}}$ is the open subscheme of $\mathcal{C}$ where π is smooth) such that,

(i) the restriction of “ + ” to $\mathcal{C}^{\mathrm{reg}}$ induces a commutative group scheme structure on $\mathcal{C}^{\mathrm{reg}}/S$,

(ii) " + " : $\mathcal{C}^{\text{reg}} \times \mathcal{C} \to \mathcal{C}$ defines an action of $\mathcal{C}^{\text{reg}}$ on $\mathcal{C}$,

(iii) If $\bar{s}$ is a geometric point of S then $\mathcal{C}_{\bar{s}}$ is either smooth over space $k(\bar{s})$ (hence an elliptic curve) or of type a.

In the latter case, we require that $\mathcal{C}_{\bar{s}}^{\text{reg}}$ acts by rotation on the graph $\Gamma(\mathcal{C}_{\bar{s}})$. Let $\overline{\mathcal{ELL}_0}(N)(S)$ be isomorphism classes of pairs $(\mathcal{C}, C)$ where $\mathcal{C}$ is a generalized elliptic curve over S, C a subgroup scheme of $\mathcal{C}^{\text{reg}}$ with $C_{\bar{s}} \cong \mathbb{Z}/N\mathbb{Z}$ for all $\bar{s} \to s$ such that $C_{\bar{s}}$ meets all components of $\mathcal{C}_{\bar{s}}$.

Theorem 2.3.7. *$\overline{\mathcal{ELL}_0}(N)$ has a coarse moduli space denoted by $X_0(N)$. $X_0(N)$ is smooth projective geometrically connected of relative dimension* 1 *over* Spec $\mathbb{Z}[\frac{1}{N}]$. *The morphism $\mathcal{ELL}_0(N) \hookrightarrow \overline{\mathcal{ELL}_0}(N)$ induces an open immersion*

$$Y_0(N) \longrightarrow X_0(N).$$

Proposition 2.3.5 and Theorem 2.3.7 imply that there exists smooth curve $Y_0(N)$ over $\mathbb{Q}$ and $X_0(N)$ defined over $\mathbb{Q}$ such that

$$Y_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathbb{H} \hookrightarrow \Gamma_0(N)\backslash\mathbb{H}^* = X_0(N)(\mathbb{C}).$$

3. Modular forms

3.1. Let $k \geq 0$ be an integer, $\alpha \in GL_2^+(\mathbb{R}) := \left\{\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{R}) : \det\alpha > 0\right\}$.
Consider a function $f : \mathbb{H} \to \mathbb{C}$ and define

$$f|_\alpha(z) := j(\alpha, z)^{-2k} \det(\alpha)^k f(\alpha z)$$

where $\alpha z = \frac{az+b}{cz+d}$. We have $f|_{\alpha\beta} = (f|_\alpha)|_\beta$.

Definition 3.1.1. Let $\Gamma \in SL_2(\mathbb{Z})$ with $-1 \in \Gamma$ be a subgroup of finite index and $k \geq 0$. A meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is called *modular function for* Γ *of weight* $2k$ if the following properties hold

(i) $f|_\gamma = f$ for all $\gamma \in \Gamma$, i.e. $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, $z \in \mathbb{H}$;

(ii) f is meromorphic in the cusps.

This second condition means the following: let s be a cusp and $\rho \in SL_2(\mathbb{Z})$ with $\rho(s) = \infty$. Let $h \geq 1$ be as in Lemma 2.2.6 a. So $\rho^{-1}\left\{\left(\begin{smallmatrix} \pm 1 & mh \\ 0 & \pm 1 \end{smallmatrix}\right) : m \in \mathbb{Z}\right\}\rho = \Gamma_s$. Let $U_\infty = \{z : \operatorname{Im}(z) > 1\}$. Then

$$f|_{\rho^{-1}}(z+h) = \left(f|_{\rho^{-1}\circ\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)}\right)(z) = f|_{\rho^{-1}}(z)$$

so $f|_{\rho^{-1}}(z) = \tilde{f}(q_h)$ where $\tilde{f}$ is meromorphic on $\mathbb{D}\backslash\{0\}$ and $q_h = \exp\left(\frac{2\pi i}{h}z\right)$, thus $\tilde{f}(q_h) = \sum_{n=-\infty}^{\infty} a_n q_h^n$ in a Laurent-expansion. We then have

$$\begin{aligned} f \text{ meromorphic in } s \quad &\Longleftrightarrow \quad a_n = 0 \text{ for all } n \ll 0, \\ f \text{ holomorphic in } s \quad &\Longleftrightarrow \quad a_n = 0 \text{ for all } n < 0, \end{aligned}$$

and $\operatorname{ord}_s(f) = \min\{n : a_n \neq 0\}$.

Definition 3.1.2. A modular function f is called modular form (for Γ of weight $2k$) if f is holomorphic in the cusps. f is called a cusp form if $\mathrm{ord}_s(f) > 0$ for all cusps s.

Define $M_{2k}(\Gamma)$ to be $\{f : \mathbb{H} \to \mathbb{C} : f \text{ a modular form for } \Gamma \text{ of weight } 2k\}$ and $S_{2k}(\Gamma)$ to be $\{f : \mathbb{H} \to \mathbb{C} : f \text{ a cusp form for } \Gamma \text{ of weight } 2k\}$.

Proposition 3.1.3 (Eisenstein series)**.** *Let k be an integer which is at least 2 and let $z \in \mathbb{H}$. The function*

$$G_{2k}(z) := \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^{2k}}$$

is a nonzero modular form of weight $2k$ for $SL_2(\mathbb{Z})$.

Proof. Convergence and holomorphy on $\mathbb{H}$ follow from the following well-known

Lemma 3.1.4. *Let Ω be a lattice in $\mathbb{C}$. The series*

$$L := \sum_{0\neq\rho\in\Omega} \frac{1}{|\rho|^t}$$

is absolutely convergent for $t > 2$.

To show that $G_{2k}(z)$ is finite at ∞, we will show that $G_{2k}(z)$ approaches an explicit finite limit as $z \to i\infty$. The terms of $G_{2k}(z)$ are of the form $1/(mz+n)^{2k}$; those which have $m \neq 0$ will contribute 0 to the sum, while those which have $m = 0$ will each contribute $1/n^{2k}$. Therefore we have

$$\lim_{z\to i\infty} G_{2k}(z) = \sum_{0\neq n\in\mathbb{Z}} \frac{1}{n^{2k}} = 2\zeta(2k),$$

which is finite (and nonzero).

To show that $G_{2k}(z)$ is modular for $SL_2(\mathbb{Z})$, it will suffice to show that it transforms correctly under the matrices S and T; it can be seen that $G_{2k}(z) = G_{2k}(z+1)$ by substituting $z+1$ for z; we have already shown that $G_{2k}(z)$ is uniformly and absolutely convergent so we can rearrange the terms as necessary. We now show that $G_{2k}(z)$ transforms correctly under S by rearranging;

$$\begin{aligned} z^{-2k} \cdot G_{2k}(-1/z) &= \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{z^{-2k}}{(-m/z+n)^{2k}} \\ &= \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(-m+nz)^{2k}} = G_{2k}(z), \end{aligned}$$

as required (again, we are using the fact that $G_{2k}(z)$ is uniformly and absolutely convergent on $\mathbb{H}$), and so therefore $G_{2k}(z)$ is a modular form of weight $2k$, which is what we wanted to prove. $\square$

We see from the proof that $G_{2k}(z)$ does not vanish at ∞, so we have an example of a nonzero form of nonzero weight which is not a cusp form. We will now exhibit the Fourier expansion of $G_{2k}(z)$.

Proposition 3.1.5. *Let $k \geq 2$ be an integer, and let $z \in \mathbb{H}$. The modular form $G_{2k}(z)$ has Fourier expansion*

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n,$$

where we define $\sigma_{2k-1}(n)$ to be the function

$$\sigma_{2k-1}(n) := \sum_{0<m|n} m^{2k-1}.$$

There is a formula for the cotangent function;

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right),$$

and we also have the identity

$$\pi \cot(\pi z) = \pi \frac{\cos(\pi z)}{\sin(\pi z)} = i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi \sum_{n=0}^{\infty} q^n,$$

where $q := e^{2\pi i z}$. By equating these identities, we see that

$$\frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right) = \pi - 2i\pi \sum_{n=0}^{\infty} q^n. \tag{3.1.6}$$

We differentiate both sides of (3.1.6) $2k-1$ times with respect to z to obtain the formula

$$\sum_{m \in \mathbb{Z}} \frac{1}{(m+z)^{2k}} = \frac{(-2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} n^{2k-1} q^n, \tag{3.1.7}$$

which is valid for $k \geq 2$. We note that the left hand side of this looks very like a component of G_{2k}, whereas the right hand side looks much like a component of the Fourier expansion given in the theorem.

We will now use (3.1.7) to write $G_{2k}(z)$ as a Fourier expansion. Because $k \geq 2$, we have absolute convergence of our series, so the following rearrangements are valid;

$$\begin{aligned}
G_{2k}(z) &= \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^{2k}}\\
&= \sum_{0\neq n\in\mathbb{Z}} \frac{1}{n^{2k}} + 2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^{2k}}\\
&= 2\zeta(2k) + 2\frac{(-2\pi i)^{2k}}{(2k-1)!}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{2k-1}q^{mn}\\
&= 2\zeta(2k) + 2\frac{(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n.
\end{aligned}$$

A standard notation for Eisenstein series is to write

$$E_{2k}(z) := \frac{G_{2k}}{2\zeta(2k)},$$

which is called the normalized Eisenstein series of weight $2k$ (of level 1). For these modular forms, the following series identity holds;

$$E_{2k}(z) = 1 - \frac{4k}{B_{2k}}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n,$$

where the B_{2k} are the Bernoulli numbers, which are defined by

$$\frac{t}{e^t-1} = \sum_{m=0}^{\infty} B_m \cdot \frac{t^m}{m!}.$$

We will now construct our first example of a cusp form. We define the Δ function and the Ramanujan τ function in the following;

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

$\Delta(z)$ is an example of a nonzero cusp form (of weight 12). The Fourier coefficients of $\Delta(z)$ are all integers, and they are also multiplicative; that is, $\tau(mn) = \tau(m)\tau(n)$ if $(m,n)=1$. They also satisfy recurrence; if p is a prime, then

$$\tau(p^n) = \tau(p)\tau(p^{n-1}) - p^{11}\tau(p^{n-2}), \text{ for } n\geq 2.$$

Proposition 3.1.8. *There is a canonical isomorphism*

$$\begin{aligned}
S_2(\Gamma) &\longrightarrow H^0(X(\Gamma),\Omega^{\mathrm{hol}})\\
f &\longmapsto \omega_f.
\end{aligned}$$

Proof. We only define the construction of the differential form ω_f associated to $f\in S_2(\Gamma)$.

We know that $f(z)\mathrm{d}z$ is a holomorphic differential form on $\mathbb{H}$. For $\gamma = \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in\Gamma$ we have $f(\gamma z)\mathrm{d}\gamma z = f(\gamma z)(cz+2)^{-2}\mathrm{d}z = f(z)\mathrm{d}z$.

1. For $z \in \mathbb{H}$, ω_f is defined as follows: there exists an open neighbourhood as in Lemma 2.2.7 such that we have

$$\begin{array}{ccccc} U_z & \xrightarrow{\lambda} & V \subseteq \mathbb{D} & & \omega \\ \downarrow{\scriptstyle\pi} & & \downarrow & & \downarrow \\ \Gamma_z\backslash U_z & \xrightarrow{g_z} & V' \subseteq \mathbb{D} & & w^e \end{array}$$

where $e = e_z = \frac{1}{2}\#\Gamma(z)$. Then $\lambda_*(f(z)\mathrm{d}z) = F(\omega)\mathrm{d}\omega$ is a differential form on V and $\mathrm{ord}_0(F) = \mathrm{ord}_z(f)$.

Let ξ be a primitive e-th root of unity. Let $\mathbb{R}\omega = \xi\omega$ on V. Then $\lambda^{-1} \circ R\lambda$ is a generator of Γ_z, so $F(\omega)\mathrm{d}\omega = F(\xi\omega)\mathrm{d}(\xi\omega) = \xi F(\xi\omega)\mathrm{d}\omega$ and thus there exists a holomorphic function F_1 with $F_1(\omega^e) = \omega \cdot F(\omega)$ (because $\omega F(\omega) = \xi\omega F(\xi\omega)$ is invariant under Γ_z). So $\frac{1}{e}\frac{1}{\omega^e}F_1(\omega^e)\mathrm{d}(\omega^e) = \frac{1}{\omega}(\omega F(\omega)\mathrm{d}\omega) = F(\omega)\mathrm{d}\omega$ and thus $w_f|_{U_z}$, which is defined as $(g_z)^{-1}\left(\frac{1}{e}\frac{1}{\omega}F_z(\omega)\mathrm{d}\omega\right)$ is meromorphic on U_z (so $\pi^{-1}(\omega_f) = f(z)\mathrm{d}z$).

Now $e \cdot \mathrm{ord}_0(F_1) = \mathrm{ord}(F) + 1$, so $\mathrm{ord}_0(F_1) > 0$ and thus is $\frac{1}{e}\frac{1}{\omega}F_1(\omega)\mathrm{d}\omega$ holomorphic on V' and thus is also $\omega_f|_{U_z}$ holomorphic.

2. To define ω_f on a cusp, we may assume without loss of generality that $s = \infty$. Then $U_\infty = \{\tau : \mathrm{Im}(\tau) > 1\}$. Consider the map

$$\begin{array}{rcl} \left\{\begin{pmatrix} \pm1 & m \\ 0 & \pm1 \end{pmatrix} : m \in \mathbb{Z}\right\}\backslash U_\infty & \xrightarrow{g_\infty} & \mathbb{D}\backslash\{0\} \\ z & \longmapsto & q = \exp(2\pi i z). \end{array}$$

Then $f(z)\mathrm{d}z = \tilde{f}(q)(\frac{\mathrm{d}q}{\mathrm{d}z})^{-1}\mathrm{d}q = \frac{1}{2\pi i q}\tilde{f}(q)\mathrm{d}q$ and we define $\omega_f|_{U_{\pi(\infty)}} = g_\infty^{-1}\left(\frac{1}{2\pi i q}\tilde{f}(q)\mathrm{d}q\right)$, then ω_f is holomorphic because $\mathrm{ord}(\frac{1}{q}\tilde{f}(q)) = -1 + \mathrm{ord}_\infty(f) \geq 0$.

$\square$

Now let $f(z) \in S_{2k}(\Gamma)$ and $f(z) = \sum_{n=1}^{\infty} a_n q^n$ the q-expansion of $f(z)$.

Lemma 3.1.9. *$a_n = O(n^k)$, so $\left|\frac{a_n}{n^k}\right|$ is bounded for $n \geq 1$.*

Proof (only for $\Gamma = SL_2(\mathbb{Z})$). Because $f(z) = q\left(\sum_{n\geq1} a_n q^{n-1}\right)$ we have $|f(z)| = O(|q|) = O(e^{-2\pi y})$ where $y = \mathrm{Im}(z)$.

Let $\phi(z) = |f(z)|y^k$. Then $\phi(\gamma z) = |f(\gamma z)|\mathrm{Im}(\gamma z)^k = |f(\gamma z)|j(\gamma, z)^{-2k}\mathrm{Im}(z)^k = \phi(z)$.

As $\phi(z) = O(e^{-2\pi y}y^k) = O(1)$, we have that ϕ is bounded on $\mathcal{F} = \{z \in \mathbb{C} : |z| \geq 1, -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}\}$, so ϕ is bounded, so $|f(z)| \leq My^{-k}$ for all $z \in \mathbb{H}$.

Now let $y > 0$ be fixed, $q = \exp(2\pi i)(x + iy)$ where $0 \leq x \leq 1$. Then $a_n = \frac{1}{2\pi i}\int_0^1 f(x + iy)q^{-n}\mathrm{d}x$ so $|a_n| \leq My^{-k}e^{-2n\pi y}$ for all y.

For $y = \frac{1}{n}$ we have $|a_n| \leq Mn^k$. This completes the proof for $\Gamma = SL_2(\mathbb{Z})$. $\square$

3.2. Hecke operators. Let G be a group, with Γ and Γ' subgroups. We say that Γ and Γ' are *commensurable* (notation $\Gamma \sim \Gamma'$) if $\Gamma \cap \Gamma'$ has finite index in both Γ and Γ'.

Let Γ be a subgroup of G, $\tilde{\Gamma} = \{\alpha \in G : \Gamma \sim \alpha\Gamma\alpha^{-1}\}$. Then $\tilde{\Gamma} \subseteq G$ is a subgroup and $\tilde{\Gamma} \supseteq \Gamma$.

Lemma 3.2.1. a. *Let $\alpha \in \tilde{\Gamma}$. Then*

$$\Gamma\backslash(\Gamma\alpha\Gamma) \cong (\Gamma \cap \alpha^{-1}\Gamma\alpha)\backslash\Gamma$$

and

$$(\Gamma\alpha\Gamma)/\Gamma \cong \Gamma/(\Gamma \cap \alpha\Gamma\alpha^{-1}).$$

b. *If $\#(\Gamma\backslash\Gamma\alpha\Gamma) = \#(\Gamma\alpha\Gamma/\Gamma)$, then $\Gamma\alpha\Gamma/\Gamma$ and $\Gamma\backslash\Gamma\alpha\Gamma$ have a common system of representatives.*

Proof. a. $\Gamma \longrightarrow \Gamma\backslash\Gamma\alpha\Gamma$, $\gamma \mapsto \Gamma\alpha\gamma$ induces $\Gamma \cap \alpha^{-1}\Gamma\alpha\backslash\Gamma \longrightarrow \Gamma\backslash\Gamma\alpha\Gamma$.

b. Exercise.

$\square$

Let $\Gamma \subseteq G$ be a subgroup, $\Delta \subseteq \tilde{\Gamma}$ a monoid with $\Gamma \subseteq \Delta$. Let $R[\Gamma, \Delta]$ be the free $\mathbb{Z}$-module with basis $[\Gamma\alpha\Gamma]$, $\alpha \in \Delta$. Let $\alpha, \beta \in \Delta$, $\Gamma\alpha\Gamma = \dot{\bigcup_i} \Gamma\alpha_i$, $\Gamma\beta\Gamma = \dot{\bigcup_j} \Gamma\beta_j$. Then

$$[\Gamma\alpha\Gamma][\Gamma\beta\Gamma] = \sum m_{\Gamma\gamma\Gamma}[\Gamma\gamma\Gamma]$$

with

$$\begin{aligned} m_{\Gamma\gamma\Gamma} &= \#\{(i,j)|\Gamma\alpha_i\beta_j = \Gamma\gamma\} \\ &= \frac{\#\{(i,j)|\Gamma\alpha_i\beta_j\Gamma = \Gamma\gamma\Gamma\}}{\#(\Gamma\backslash\Gamma\gamma\Gamma)}. \end{aligned}$$

One shows: $m_{\Gamma\gamma\Gamma}$ is independent from the choice of representatives α_i, β_j, γ.

Proposition 3.2.2. *$R[\Gamma, \Delta]$ is an associative ring with unit $[\Gamma]$. $R(\Gamma, \Delta)$ is called a* Hecke algebra.

Lemma 3.2.3. *Let Γ, Δ be as above and we assume that there is a map $\iota : \Delta \longrightarrow \Delta$ with*

(i) *$\iota(\alpha\beta) = \iota(\beta)\iota(\alpha)$ and $\iota(\iota(\alpha)) = \alpha$ for all $\alpha, \beta \in \Delta$;*
(ii) *$\iota(\Gamma) = \Gamma$;*
(iii) *$\iota(\Gamma\alpha\Gamma) = \Gamma\alpha\Gamma$, i.e. $\Gamma\iota(\alpha)\Gamma = \Gamma\alpha\Gamma$.*

Then, for each $\alpha \in \Delta$, $\Gamma\backslash\Gamma\alpha\Gamma$ and $\Gamma\alpha\Gamma/\Gamma$ have a common system of representatives and $R[\Gamma, \Delta]$ is commutative.

Proof. $\Gamma\alpha\Gamma = \cup_i \Gamma\alpha_i$, so $\Gamma\alpha\Gamma = \Gamma\iota(\alpha)\Gamma = \cup_i \iota(\alpha_i)\Gamma$, and thus $\#(\Gamma\backslash\Gamma\alpha\Gamma) = \#(\Gamma\alpha\Gamma/\Gamma)$. This implies the first claim, by 3.2.1.

Now we show that $R[\Gamma, \Delta]$ is commutative.

Consider

$$\begin{aligned} \Gamma\alpha\Gamma = & \bigcup \Gamma\alpha_i & = \bigcup \alpha_i\Gamma, \\ \Gamma\beta\Gamma = & \bigcup \Gamma\beta_i & = \bigcup \beta_i\Gamma, \end{aligned}$$

so

$$\begin{aligned} \Gamma\alpha\Gamma &= \bigcup \Gamma\iota(\alpha_i), \\ \Gamma\beta\Gamma &= \bigcup \Gamma\iota(\beta_i), \\ [\Gamma\alpha\Gamma][\Gamma\beta\Gamma] &= \sum_\gamma m_\gamma [\Gamma\gamma\Gamma], \end{aligned}$$

where

$$\begin{aligned} m_\gamma &= \#\left\{(i,j) : \Gamma\alpha_i\beta_j\Gamma = \Gamma\gamma\Gamma\right\}/\#(\Gamma\backslash\Gamma\gamma\Gamma) \\ &= \#\left\{(i,j) : \Gamma\iota(\beta_i)\iota(\alpha_i)\Gamma = \Gamma\iota(\gamma)\Gamma\right\}/\#(\Gamma\backslash\Gamma\beta\Gamma) \\ &= \text{coefficient of } [\Gamma\gamma\Gamma] \text{ in } [\Gamma\beta\Gamma][\Gamma\alpha\Gamma]. \end{aligned}$$

□

Let $n \geq 1$. Now we consider the Hecke algebra for $\Gamma_0(N)$.

Lemma 3.2.4. *Let* $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ *with* $\det\alpha \neq 0$. *Then* $\alpha \in \widetilde{\Gamma_0(N)}$.

Proof. Without loss of generality we may assume $\det\alpha = m \geq 1$. It suffices to consider the case $N = 1$.

Let

$$\Gamma(m) = \left\{ \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod m \right\}.$$

For $\gamma \in \Gamma(m)$ we have $m\alpha^{-1}\gamma\alpha \equiv m\alpha^{-1}\alpha = \left(\begin{smallmatrix} m & 0 \\ 0 & m \end{smallmatrix}\right) \mod m$ (where $m\alpha^{-1} \in SL_2(\mathbb{Z})$) and thus $\alpha^{-1}\gamma\alpha \in SL_2(\mathbb{Z})$ such that $SL_2(\mathbb{Z}) \cap \alpha SL_2(\mathbb{Z})\alpha^{-1} \supseteq \Gamma(m)$ and therefore $\alpha \in \widetilde{SL_2(\mathbb{Z})}$. □

Let

$$\Delta_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \mod N, \gcd(a, N) = 1, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} > 0 \right\}.$$

$\Delta_0(N)$ is a monoid with $\Gamma_0(N) \subseteq \Delta_0(N) \subseteq \widetilde{\Gamma_0(N)}$ and $R(\Gamma_0(N), \Delta_0(N)) = R(N)$ is the Hecke algebra.

Lemma 3.2.5.

(i) *Let* $\alpha \in \Delta_0(N)$. *Then there is a diagonal matrix* $\widetilde{\alpha} \in \Delta_0(N)$ *such that*

$$\Gamma_0(N)\alpha\Gamma_0(N) = \Gamma_0(N)\widetilde{\alpha}\Gamma_0(N).$$

(ii) *For all primes* l *we have*

$$\Gamma_0(N)\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N) = \Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\Gamma_0(N).$$

(iii) *For all primes* $l \nmid N$ *and* $p|N$ *we have*

$$\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\Gamma_0(N) = \bigcup_{j=1}^{l-1}\Gamma_0(N)\begin{pmatrix} 1 & j \\ 0 & l \end{pmatrix}\bigcup\Gamma_0(N)\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix},$$

$$\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_0(N) = \bigcup_{j=0}^{p-1}\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ j & p \end{pmatrix}.$$

Proof. The proof of Lemma 3.2.5 is straight forward. We only show part (i). Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta_0(N)$ where $(a, N) = 1$ and $c = k'N$ for some $k' \in \mathbb{Z}$. We construct a matrix $\beta = \left(\begin{smallmatrix} X & Y \\ kN & z \end{smallmatrix}\right)$ such that $\beta\alpha$ is upper triangular and $\beta \in \Gamma_0(N)$, as follows;
Case 1: If $(a, k'N) = 1$ then we define $z = a$, $k = -k'$ and choose $X, Y \in \mathbb{Z}$ such that $aX + k'NY = 1$. Thus we define $\beta = \left(\begin{smallmatrix} X & Y \\ kN & z \end{smallmatrix}\right)$.
Case 2 : Let $\varepsilon = (a, k')$. Since $(a, N) = 1$, we have $(\varepsilon, N) = 1$. Define $k = -k'/\varepsilon$, $z = a/\varepsilon$. Then $(z, kN) = 1$. Find $X, Y \in \mathbb{Z}$ with $zX - kNY = 1$ and define $\beta = \left(\begin{smallmatrix} X & Y \\ kN & z \end{smallmatrix}\right)$.
Then $\beta\alpha = \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in \Delta_0(N)$. We put $\delta = (a', d')$. Then

$$\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & \frac{d'}{\delta} \end{pmatrix}.$$

Now let $\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in \Delta_0(N)$ with $(a', d') = 1$. Find $X, Y \in \mathbb{Z}$ with $a'X + d'Y = -b'$. Then

$$\begin{pmatrix} 1 & Y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}\begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a' & 0 \\ 0 & d' \end{pmatrix}.$$

This finishes the proof of (i). □

Proposition 3.2.6. $R(N)$ *is commutative and for any* $\alpha \in \Delta_0(N)$, $\Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N)$ *and* $\Gamma_0(N)\alpha\Gamma_0(N)/\Gamma_0(N)$ *have a common system of representatives.*

Proof. Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta_0(N)$ and $\iota(\alpha) := \left(\begin{smallmatrix} a & \frac{c}{N} \\ Nb & d \end{smallmatrix}\right)$. Then $\iota : \Delta_0(N) \longrightarrow \Delta_0(N)$ satisfies (i) to (iii) in 3.2.3 (the third property follows from Lemma 3.2.5). □

Proposition 3.2.7. *$S_2(\Gamma_0(N))$ is in a natural way a $R(N)$-right-module.*
For $\alpha \in \Delta_0(N)$ and $f \in S_2(\Gamma_0(N))$ we define the action $f|_{[\Gamma\alpha\Gamma]}$ by

$$f|_{[\Gamma\alpha\Gamma]} = \sum_i f|_{\alpha_i}$$

where

$$\Gamma\alpha\Gamma = \bigcup_i \Gamma\alpha_i.$$

Proof. For $\gamma \in \Gamma_0(N)$ we have $(\sum_i f|_{\alpha_i})|_\gamma = \sum_i f|_{\alpha_i\gamma}$. As $\alpha_i\gamma$ is a system of representatives of $\Gamma\backslash\Gamma\alpha\Gamma$, we have that $\sum_i f|_{\alpha_i}$ is Γ-invariant.

Write $f|_{\alpha_i} = \sum_{n=1}^\infty a_n^{(i)} q_{h_i}^n$. Then $\sum f|_{\alpha_i} = \sum_{n\geq 1} a_n q_h^n$ for some h. But $\sum f|_{\alpha_i}$ is $\Gamma_0(N)$-invariant and thus $h = 1$. $\square$

Let l be a prime with $l \nmid N$. Define

$$T_l := \sum_{\substack{\det\alpha = l \\ [\Gamma_0(N)\alpha\Gamma_0(N)]}} [\Gamma_0(N)\alpha\Gamma_0(N)] = [\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\Gamma_0(N)].$$

For a prime p with $p|N$, let

$$U_p := \sum_{\substack{\det\alpha = p \\ [\Gamma_0(N)\alpha\Gamma_0(N)]}} [\Gamma_0(N)\alpha\Gamma_0(N)] = [\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_0(N)].$$

By 3.2.5 (c) we have

$$\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\Gamma_0(N) = \bigcup_{j=1}^{l-1}\Gamma_0(N)\begin{pmatrix} 1 & j \\ 0 & l \end{pmatrix}\bigcup\Gamma_0(N)\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}$$

and for $p|N$:

$$\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_0(N) = \bigcup_{j=0}^{p-1}\Gamma_0(N)\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}.$$

For $f(z) = \sum_{n\geq 1} a(n)q^n \in S_2(\Gamma_0(N))$ we have

$$\begin{aligned}
f|_{T_l} &= \sum_{n\geq 1} a(n)\sum_{j=0}^{l-1}\frac{1}{l}\exp\left(2\pi i\frac{z+j}{l}\right) + l\sum_{n\geq 1} a(n)q^{nl} \\
&= \sum_{n=1}^\infty a(nl) + la\left(\frac{n}{l}\right)q^n \\
&\quad\ \text{with } a\left(\frac{n}{l}\right) = 0 \text{ for } \frac{n}{l} \notin \mathbb{Z}, \\
f|_{U_p} &= \sum_{n=1}^\infty a(np)q^n.
\end{aligned}$$

f is called an *eigenform* iff f is an eigenvector for T_l, U_p for all $l \nmid N$ and $p|N$. If f is an eigenform, then $U_p f = \lambda(p)f$, $T_l f = \lambda(l)f$.

Lemma 3.2.8. *Let $f(z) \in S_2(\Gamma_0(N))$ be an eigenform. Then the L-series associated to f, $L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$ has a representation as Euler-product:*

$$L(f,s) = a_1 \prod_{p|N} \left(1 - \lambda(p)p^{-s}\right) \prod_{l \nmid N} \left(1 - \lambda(l)l^{-s} + l^{1-2s}\right).$$

f is called normalized *if $a_1 = 1$. In this case, we have $\lambda(p) = a_p$, $\lambda(l) = a_l$.*

Proof.

$$\begin{aligned} \left(1 - \lambda(l)l^{-s} + l^{1-2s}\right) L(f,s) &= \sum_{n=1}^{\infty} \left(a_n - \lambda(l) a_{\frac{n}{l}} + l a_{\frac{n}{l^2}}\right) n^{-s} \\ &= \sum_{\substack{n=1 \\ \gcd(n,l)=1}}^{\infty} a_n n^{-s}. \end{aligned}$$

$\square$

In general, $S_2(\Gamma_0(N))$ does not have a basis consisting of eigenforms. To study the existence of eigenforms in $S_2(\Gamma_0(N))$ we introduce a hermitian inner product on $S_2(\Gamma_0(N))$.

$v = \frac{\mathrm{d}x\mathrm{d}y}{y^2}$ defines a measure on $\mathbb{H}$ (where $z = x + iy$). We show that v is $GL_2^+(\mathbb{R})$-invariant:

Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2^+(\mathbb{R})$.

Then

$$\begin{aligned} \frac{\mathrm{d}(\alpha z)}{\mathrm{d}z} &= \frac{\det(\alpha)}{j(\alpha,z)^2}, \\ \frac{\mathrm{d}(\overline{\alpha z})}{\mathrm{d}\bar{z}} &= \frac{\det(\alpha)}{j(\alpha,\bar{z})^2}, \\ \frac{1}{y^2}\mathrm{d}x \wedge \mathrm{d}y &= \frac{1}{y^2}\frac{i}{2}\mathrm{d}z \wedge \mathrm{d}\bar{z}, \end{aligned}$$

and

$$\begin{aligned} \frac{i}{2}\frac{1}{\mathrm{Im}(\alpha z)^2}\mathrm{d}(\alpha z) \wedge \mathrm{d}\overline{\alpha z} &= \frac{i}{2}\frac{1}{\mathrm{Im}(z)^2}\frac{|j(\alpha,z)|^4}{(\det\alpha)^2}\left(\frac{\mathrm{d}\alpha z}{fz}\right)^2\left(\frac{\mathrm{d}\overline{\alpha z}}{\mathrm{d}\bar{z}}\right)\mathrm{d}z \wedge \mathrm{d}\bar{z} \\ &= \frac{i}{2}\frac{1}{\mathrm{Im}(z)^2}\mathrm{d}z \wedge \mathrm{d}\bar{z}. \end{aligned}$$

Let $\mathcal{F} := \{z \in \mathbb{H} : |z| > 1, -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}\}$ be a fundamental domain for $SL_2(\mathbb{Z})\backslash\mathbb{H}$. If $\dot{\bigcup_i} \Gamma_0(N)\alpha_i = SL_2(\mathbb{Z})$, then $\mathcal{D} = \cup_i \alpha_i \mathcal{F}$ is a fundamental domain for $\Gamma_0(N)\backslash\mathbb{H}$.

Definition 3.2.9. Let $f, g \in S_2(\Gamma_0(N))$. Then

$$\langle f, g\rangle = \int_{\mathcal{D}} f(z)\overline{g(z)}\mathrm{d}x\mathrm{d}y$$

is called the *Peterson scalar product* on $S_2(\Gamma_0(N))$.

Indeed, we have

(i) $|\langle f,g\rangle| < \infty$.
It suffices to show $\int_{\mathcal{F}} |f(z)\overline{g(z)}|\mathrm{d}x\mathrm{d}y < \infty$. As $|f(z)|, |g(z)| = O(e^{-2\pi y})$ we have

$$\int_{\mathcal{F}} |f(z)\overline{g(z)}|\mathrm{d}x\mathrm{d}y \leq C\int_{\frac{1}{2}}^{\infty} e^{-4\pi y}\mathrm{d}y < \infty.$$

(ii) Independence from the choice of representatives α_i.
For $\alpha \in GL_2^+(\mathbb{R})$, we have

$$\begin{aligned}\int_{\alpha\mathcal{F}} f(z)\overline{g(z)}\mathrm{d}x\mathrm{d}y &= \int_{\mathcal{F}} f(\alpha z)\overline{g(\alpha z)}\mathrm{Im}(\alpha z)^2 y^{-2}\mathrm{d}x\mathrm{d}y \\ &= \int_{\mathcal{F}} (f|_\alpha)(z)\overline{(g|_\alpha)(z)}\mathrm{d}x\mathrm{d}y.\end{aligned}$$

Proposition 3.2.10. *The Hecke operators T_l, for $l \nmid N$, are Hermitian with respect to $\langle,\rangle$. Hence $S_2(\Gamma_0(N))$ has a basis of eigenforms of T_l, $l \nmid N$.*

Proof. If $\Gamma \subseteq SL_2(\mathbb{Z})$ has finite index, then define

$$\int_{\Gamma\backslash\mathbb{H}} f(z)\overline{g(z)}v(\mathrm{d}z) := \int_{\mathcal{D}} f(z)\overline{g(z)}v(\mathrm{d}z)$$

with $\mathcal{D}$ a fundamental domain for Γ, $f, g \in S_2(\Gamma)$. Define

$$(f,g) := \frac{1}{[SL_2(\mathbb{Z}):\Gamma]}\int_{\Gamma\backslash\mathbb{H}} f(z)\overline{g(z)}v(\mathrm{d}z)$$

which is independent from Γ.

Choose a common system of representatives of right- and left-cosets of $\Gamma_0(N)\left(\begin{smallmatrix}1&0\\0&l\end{smallmatrix}\right)\Gamma_0(N)$:

$$\Gamma_0(N)\begin{pmatrix}1&0\\0&l\end{pmatrix}\Gamma_0(N) = \bigcup_i \Gamma_0(N)\alpha_i = \bigcup_i \alpha_i\Gamma_0(N).$$

For $\alpha \in M_2(\mathbb{Z})$ with $\det(\alpha) \neq 0$, put $\alpha' = \det(\alpha) \cdot \alpha^{-1}$. Then α_i' is a system of representatives of $\Gamma_0(N)\backslash\Gamma_0(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & l \end{smallmatrix}\right) \Gamma_0(N)$. We have

$$\begin{aligned}
\langle T_l f, g\rangle &= [SL_2(\mathbb{Z}) : \Gamma_0(N)]\,(T_l f, g) \\
&= \left(\sum_\iota (f|_{\alpha_i}, g)\right)[SL_2(\mathbb{Z}) : \Gamma_0(N)] \\
&= \frac{[SL_2(\mathbb{Z}) : \Gamma_0(N)]}{\left[SL_2(\mathbb{Z}) : \Gamma_0(N) \cap \alpha_i^{-1}\Gamma_0(N)\alpha_i\right]} \int_{\Gamma_0(N)\backslash\mathbb{H}} (f|_{\alpha_i})(z)\overline{g(z)}v(\mathrm{d}z) \\
&= \sum_i \#\left(\Gamma_0(N)\backslash\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\Gamma_0(N)\right) \int_{\Gamma_0(N)\backslash\mathbb{H}} (f|_{\alpha_i})(z)\overline{g(z)}v(\mathrm{d}z) \\
&= \sum_i \#\left(\Gamma_0(N)\begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\Gamma_0(N)/\Gamma_0(N)\right) \int_{\Gamma_0(N)\backslash\mathbb{H}} f(z)\overline{(g|_{\alpha_i})(z)}v(\mathrm{d}z) \\
&= \langle f, T_l g\rangle .
\end{aligned}$$

$\square$

Definition 3.2.11.

$$\begin{aligned}
\mathrm{Im}\left(\oplus_{p|N} S_2(\Gamma_0(\frac{N}{p}))\right) &\rightrightarrows S_2(\Gamma_0(N)) \\
f &\longmapsto f(z) \text{ or } f(pz)
\end{aligned}$$

is called the space of *old forms*, denoted by $S_2(\Gamma_0(N))^{\mathrm{old}}$. Then $S_2(\Gamma_0(N))^{\mathrm{new}} = \left(S_2(\Gamma_0(N))^{\mathrm{old}}\right)^{\perp}$ is called the space of *new forms.*

Proposition 3.2.12. *$S_2(\Gamma_0(N))^{\mathrm{new}}$ is invariant under U_p, T_l for all $p|N$, $l \nmid N$ and has a basis of eigenforms.*

Let $W_N := \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. For $\left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Delta_0(N)$ we have $W_N \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) W_N^{-1} = \left(\begin{smallmatrix} d & -c \\ -bN & a \end{smallmatrix}\right)$. Therefore W_N is in the normalizer of $\Gamma_0(N)$ and for $f \in S_2(\Gamma_0(N))$, we have $f|_{W_N} \in S_2(\Gamma_0(N))$.

Definition 3.2.13. The map

$$\begin{aligned}
w_N : S_2(\Gamma_0(N)) &\longrightarrow S_2(\Gamma_0(N)) \\
f &\longmapsto f|_{W_N}
\end{aligned}$$

is called Atkin-Lehner involution.

Note: $W_N W_N = \left(\begin{smallmatrix} -N & 0 \\ 0 & -N \end{smallmatrix}\right)$ acts as identity on $S_2(\Gamma_0(N))$; hence w_N is really an involution.

Proposition 3.2.14.

a. *w_N commutes with all Hecke operators for $l \nmid N$.*
b. *w_N leaves $S_2(\Gamma(N))^{\mathrm{new}}$ invariant. More precisely: if f is a new form then $w_N(f) = \pm f$.*

Proposition 3.2.15. *Let $f \in S_2(\Gamma_0(N))$ and define $\Lambda(f,s) := (2\pi)^{-s}\Gamma(s)L(f,s)$. Then $\Lambda(f,s)$ has an analytic continuation to $\mathbb{C}$. If $w_N(f) = \pm f$, then $\Lambda(f,s)$ satisfies the functional equation $\Lambda(f,2-s) = \mp N^{s-1}\Lambda(f,s)$.*

Proof. Without loss of generality, we may assume $w_N(f) = \pm f$, $f(z) = \sum_{n=1}^{\infty} a_n q^n$ with $q = \exp(2\pi i z)$, $a_1 = 1$, $a_n = O(n)$ (following Lemma 3.1.9). Then:

$$\begin{aligned} N^{\frac{s}{2}}\Lambda(f,s) &= \sum_{n=1}^{\infty} a_n \left(\frac{2\pi n}{\sqrt{N}}\right)^{-s} \int_0^{\infty} e^{-t} t^s \frac{\mathrm{d}t}{t} \\ &= \sum_{n=1}^{\infty} \int_0^{\infty} a_n e^{-\frac{2\pi n t}{\sqrt{N}}} t^s \frac{\mathrm{d}t}{t} \end{aligned}$$

as $\sum_{n=1}^{\infty} \int_0^{\infty} |a_n| e^{-\frac{2\pi n t}{\sqrt{N}}} t^{\sigma} \frac{\mathrm{d}t}{t}$ converges for $\sigma > 2$.

For $\mathrm{Re}(s) > 2$ we have

$$\begin{aligned} N^{\frac{s}{2}}\Lambda(f,s) &= \int_0^{\infty} t^s \left(\sum_{n=1}^{\infty} a_n e^{-\frac{2\pi n t}{\sqrt{N}}}\right) \frac{\mathrm{d}t}{t} \\ &= \int_0^{\infty} t^s f\left(\frac{it}{\sqrt{N}}\right) \frac{\mathrm{d}t}{t} \\ &= \int_1^{\infty} t^s f\left(\frac{it}{\sqrt{N}}\right) \frac{\mathrm{d}t}{t} + \int_0^{1} t^s f\left(\frac{it}{\sqrt{N}}\right) \frac{\mathrm{d}t}{t} \end{aligned}$$

and $f(it) = O(e^{-2\pi t})$ for $t \geq \frac{1}{2}$. Hence both integrals are uniformly absolutely convergent on any vertical section. Thus we have

$$\begin{aligned} N^{\frac{s}{2}}\Lambda(f,s) &= \int_1^{\infty} t^s f\left(\frac{it}{\sqrt{N}}\right) \frac{\mathrm{d}t}{t} \pm \int_1^{\infty} t^{-s} f\left(\frac{i}{\sqrt{N}t}\right) \frac{\mathrm{d}t}{t} \\ &= \int_1^{\infty} t^s f\left(\frac{it}{\sqrt{N}}\right) \frac{\mathrm{d}t}{t} \pm \int_1^{\infty} t^{-s} \left(f|_{W_N}\right) \left(\frac{it}{\sqrt{N}}\right) \left(\frac{it}{\sqrt{N}}\right)^2 N \frac{\mathrm{d}t}{t} \\ &= \int_1^{\infty} t^s f\left(\frac{it}{\sqrt{N}}\right) \frac{\mathrm{d}t}{t} \mp \int_1^{\infty} t^{2-s} \left(f|_{W_N}\right) \left(\frac{it}{\sqrt{N}}\right) \frac{\mathrm{d}t}{t}, \end{aligned}$$

and thus $N^{\frac{s}{2}}\Lambda(f,s) = \mp N^{1-\frac{s}{2}}\Lambda(f,2-s)$. We have used that $f\left(\frac{i}{t\sqrt{N}}\right) = f|_{W_N}\left(\frac{it}{\sqrt{N}}\right)(it)^2$.

∎

One can also consider modular forms and cusp forms for the modular group

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0(N), a \equiv d \equiv 1(N) \right\}.$$

In this case we denote the spaces $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$. Furthermore, given a character χ of $(\mathbb{Z}/N\mathbb{Z})^{\times}$ we let $M_k(N,\chi)$ and $S_k(N,\chi)$

be the subspaces of $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$ consisting of f such that

$$f|_k\gamma = \chi(d)f$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Gamma_0(N)$. (Implicit in the notation $\chi(d)$ is the usual identification of characters of $(\mathbb{Z}/N\mathbb{Z})^\times$ with Dirichlet characters modulo N.) Another way to describe the subspaces $M_k(N,\chi)$ and $S_k(N,\chi)$ is to say that they are the χ-eigenspaces for the "diamond operator" $f \mapsto f|_k\langle d\rangle$. In this approach d denotes an element of $(\mathbb{Z}/N\mathbb{Z})^\times$, and the operator $\langle d\rangle$ is defined by setting

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

for any $\gamma \in \Gamma_0(N)$ which reduces modulo N to a matrix with d as lower right-hand entry. In view of the isomorphism

$$\begin{aligned} \Gamma_0(N)/\Gamma_1(N) &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \\ \text{coset of } \begin{pmatrix} a & b \\ cN & d \end{pmatrix} &\longmapsto d \mod N, \end{aligned}$$

the diamond operators give a well-defined action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$, and consequently we have eigenspace decompositions

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

and

$$S_k(\Gamma_1(N)) = \oplus_\chi S_k(N,\chi)$$

where χ runs over Dirichlet characters modulo N. Note that if χ is the trivial character then $M_k(N,\chi)$ and $S_k(N,\chi)$ coincide with $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N))$ respectively.

It is possible to extend Proposition 3.2.15 (analytic continuation of L-function) for cusp forms in $S_k(\Gamma_1(N))$.

4. Modular elliptic curves

4.1.

Definition 4.1.1. Let E be an elliptic curve defined over $\mathbb{Q}$. Then E is called modular if there is a non-constant morphism

$$\pi : X_0(N) \to E$$

of algebraic curves defined over $\mathbb{Q}$, where N is the conductor of E.

We formulate equivalent conditions for the modularity of E.

As $\dim H^0(E,\Omega) = 1$, there is an invariant differential form $\omega \in H^0(E,\Omega)$ which is unique up to constants. Over $\mathbb{C}$, we have

$$\pi^*\omega = cf(z)\mathrm{d}z, \quad c \in \mathbb{C},\ c \neq 0$$

where f is a normalized cusp form. Let $J_0(N)$ be the Jacobian variety of $X_0(N)$. For a construction of Jacobians over $\mathbb{C}$, see the beginning of chapter 5. By the universal property of Jacobian varieties, there exists a non-trivial morphism

$$J_0(N) \to E$$

such that the diagram of morphisms

$$\begin{tikzcd} X_0(N) \arrow[r] \arrow[dr, "\pi"'] & J_0(N) \arrow[d] \\ & E \end{tikzcd} \tag{4.1.1}$$

commutes.

Let k be a field, $\mathrm{Ab}^0(k)$ be the category of abelian varieties up to isogeny.

$$\mathrm{Ob}(\mathrm{Ab}^0(k)) = \mathrm{Ob}(\mathrm{Ab}(k)) = \text{ abelian varieties}$$

$$\mathrm{Hom}^0(A,B) = \mathrm{Hom}_{\mathrm{Ab}^0(k)}(A,B) = \mathrm{Hom}_k(A,B) \otimes \mathbb{Q}$$

Lemma 4.1.2. $\mathrm{Ab}^0(k)$ *is a semisimple* $\mathbb{Q}$*-linear abelian category. For* $A \in \mathrm{Ob}(\mathrm{Ab}^0(k))$*,* $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ *is a finite-dimensional semisimple* $\mathbb{Q}$*-algebra.*

The Hecke operators T_l, $l \nmid N$ define correspondences in $X_0(N)$, resp. $J_0(N)$ which are compatible with the action of T_l on $S_2(\Gamma_0(N))$, in the sense of the following

Lemma 4.1.3. *The diagram (use Proposition 3.1.8)*

$$\begin{tikzcd} J_0(N)(\mathbb{C}) \arrow[d, "(T_l)_*"] & S_2(\Gamma_0(N))^*/H_1(X_0(N)(\mathbb{C}),\mathbb{Z}) \arrow[l, "\cong"'] \arrow[d, "T_l^\vee"] \\ J_0(N)(\mathbb{C}) & S_2(\Gamma_0(N))^*/H_1(X_0(N)(\mathbb{C}),\mathbb{Z}) \arrow[l, "\cong"'] \end{tikzcd}$$

is commutative.

Let Π_N be the subalgebra of $\mathrm{End}^0(J_0(N))$ which is generated by Hecke correspondences $(T_l)_*$. Then Π_N is a commutative semisimple $\mathbb{Q}$-algebra. Now we consider the set $\mathrm{Sub}J_0(N)$ of abelian subvarieties of $J_0(N)$ (which are direct summands of $J_0(N)$ by Lemma 4.1.2). For $A \in \mathrm{Sub}J_0(N)$, let $\rho(A) = \{t \in \Pi_N : \mathrm{Im}(t) \subset A\}$. Then $\rho(A)$ is an ideal. Conversely, let for an ideal $I \subset \Pi_N$,

$$\varphi(I) := \mathrm{Im}(I) \in \mathrm{Sub}J_0(N).$$

We have $\rho(\varphi(I)) \supset I$ and $\varphi(\rho(A)) \subset A$. If $\mathfrak{p} \in \mathrm{Spec}\ \Pi_N$ is a prime ideal, we have $\rho(\varphi(\mathfrak{p})) = \mathfrak{p}$. Define $A_{\mathfrak{p}} := J_0(N)/\varphi(\mathfrak{p})$. As $\mathfrak{p}$ is an ideal, the Π_N-action on $J_0(N)$ induces a homomorphism $\Pi_N \to \mathrm{End}(A_{\mathfrak{p}})$.

Proposition 4.1.4. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then E is modular if and only if there exists $N \in \mathbb{N}$ (the conductor of E) and $\mathfrak{p} \in \mathrm{Spec}\ \Pi_N$ with $E \cong A_{\mathfrak{p}}$.*

It is obvious that the existence of an isomorphism $E \cong A_{\mathfrak{p}}$ implies the modularity of E, using diagram (4.1.1).

Let now E be modular, $E \cong A_{\mathfrak{p}}$ for some $\mathfrak{p} \in \operatorname{Spec} \Pi_N$. Let $E(\mathfrak{p}) = \Pi_N/\mathfrak{p}$. As $H^0(E,\Omega)$ is $\mathbb{Q}$-vector-space of dimension 1 and also a $E(\mathfrak{p})$-module, we have $E(\mathfrak{p}) = \mathbb{Q}$. Let $a : \Pi_N \to \mathbb{Q}$ be the corresponding ring homomorphism, i.e. $a(T_l) = T_l \bmod \mathfrak{p}$. Let $\omega \in H^0(E,\Omega)$ be a generator such that $\pi^*\omega = cf(z)\mathrm{d}z = c\omega_f$, for a normalized cusp form f, then we have

$$a(l)f(z) = f|T_l,$$

i.e. f is an eigenform under all Hecke operators T_l for $l \nmid N$ with eigenvalue $a(l) := a(T_l)$.

There exists a model of E over $\operatorname{Spec} \mathbb{Z}[1/N]$, i.e. an elliptic curve $\mathcal{E}$ over $\operatorname{Spec} \mathbb{Z}[1/N]$, with $\mathcal{E}_\eta \cong E$ ($\eta = \operatorname{Spec} \mathbb{Q}$). $\mathcal{E}$ is uniquely determined. We define the L-function of E

$$\begin{aligned} L(E,s) &= \prod_{l\nmid N} L(E_{\mathbb{F}_l}, l^{-s})^{-1} \\ &= \prod_{l\nmid N} (1 - a_l l^{-s} + l^{1-2s})^{-1} \end{aligned}$$

with $a_l = 1 + l - \sharp E_l(\mathbb{F}_l)$ ($E_l := \mathcal{E} \times \mathbb{F}_l$). We have seen in Chapter I, that $|a_l| \le 2\sqrt{l}$. Using this fact it can be shown that $L(E,s)$ converges absolutely and uniformly for $\operatorname{Re}(s) > 3/2$.

Proposition 4.1.5. *Let E be a modular elliptic curve over $\mathbb{Q}$, $E \cong A_{\mathfrak{p}}$ for $\mathfrak{p} \in \operatorname{Spec} \Pi_N$, and f the corresponding eigenform. Then E has a model over $\operatorname{Spec} \mathbb{Z}[1/N]$ and we have*

$$L(E,s) = L(f,s)$$

up to finitely many Euler-factors. Hence $L(E,s)$ has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation with respect to $s \to 2 - s$ (see Theorem 1 in the introduction).

Finally we can describe modularity purely in terms of Galois representations. To E, we can associate a canonical Galois representation on its Tate-module $T_p(E)$ for any prime p. Let $T_p(E) := \varprojlim E_{p^n}(\overline{\mathbb{Q}}) \cong \mathbb{Z}_p^2$. The $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $E(\overline{\mathbb{Q}})$ induces a p-adic Galois representation

$$\rho_{p,E} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}(T_p(E)) = \operatorname{GL}_2(\mathbb{Z}_p).$$

It has the following properties:

- $\det\rho_{p,E} = \chi_p$ (the cyclotomic character).
- $\rho_{p,E}$ is unramified outside pN, i.e. for all primes $l \nmid pN$, the inertia group I_l satisfies $I_l \subset \operatorname{Ker}(\rho_{p,E}|_{G_{\mathbb{Q}_l}})$.

Likewise, by the theory of Eichler and Shimura, one can associate to a normalized newform f in $S_2(\Gamma_0(N))$ a Galois representation

$$\rho_f : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(O_f),$$

where O_f is the ring of integers in a p-adic field K_f obtained by the completion (at a prime above p) of a number field generated by the Fourier coefficients a_n ($n \geq 1$) of f, such that for all primes $l \nmid pN$, ρ_f is unramified at l and satisfies the two conditions

- $\mathrm{Trace}(\rho_f(\mathrm{Frob}_l)) = a_l$,
- $\det(\rho_f(\mathrm{Frob}_l)) = l$.

Definition 4.1.6. A Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(O_K)$$

(where O_K is the ring of integers in a p-adic field K) is called modular, if there exists a cusp form $f \in S_2(\Gamma_0(N))$ such that

$$\rho_f = \rho.$$

Proposition 4.1.7. *The Galois representation $\rho_{p,E}$ associated to a modular elliptic curve E over $\mathbb{Q}$ is modular for all primes p.*

One shows that the characteristic polynomial $\chi_{\rho_{p,E}}(\mathrm{Fr}_l)$ of the l-Frobenius, acting on $T_p(E) \otimes \mathbb{Q}_p$, satisfies

$$\begin{aligned} \chi_{\rho_{p,E}}(\mathrm{Fr}_l) &:= \det(XI - \rho_{p,E}(\mathrm{Fr}_l)) \\ &= X^2 - a_l X + l, \end{aligned}$$

where $a_l = a_l(f)$ is the Fourier coefficient of the eigenform f associated to E. This follows from Eichler-Shimura Theory ([2] and [3]).

Final remark. The modularity conditions given in Definition 4.1.1, Proposition 4.1.4, Proposition 4.1.5 and Proposition 4.1.7 are all equivalent.

References

[1] G. Cornell, J. H. Silverman, G. Stevens, Modular Forms and Fermat's Last Theorem, chapter 3, Springer-Verlag, 1997.

[2] P. Deligne, M. Rapoport, Les schemas de modules de courbes elliptiques, in: Modular Functions in one variable II, Springer Lecture Notes in Mathematics 349, 1973, 193–316.

[3] F. Diamond, J. Shurman, A First Course in Modular Forms, Springer, 2005.

[4] W. Fulton, Algebraic Curves, Math. Lecture Note Series, W.A.Benjamin, 1969.

[5] R. Hartshorne, Algebraic Geometry, Graduate Texts in Math. Springer, 1977.

[6] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Princeton University Press, 1985.

[7] A. W. Knapp, Elliptic Curves, chapters IX to XI, Princeton University Press, 1992.

[8] J. Milne, Étale Cohomology, Princeton University Press, 1980.

[9] D. Mumford, Algebraic Geometry I, Complex Projective Varieties, Grundlehren, Springer, 1976.

[10] T. Saito, Fermat Conjecture (in Japanese), Iwanami Shoten, 2009.

[11] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Princeton University Press, 1971.

[12] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer, 1986.

5. p-adic Regulators and p-adic integration theory (Special lecture)

5.1. Review of classical Abel-Jacobi maps. Let X be a compact Riemann surface of genus g and base point $0 \in X$. Let $x_i \in X$, $i = 1, \dots, N$. We consider a formal linear combination

$$\alpha = \sum_{i=1}^{N} n_i \left([x_i] - [0] \right), \quad n_i \in \mathbb{Z}$$

which we call a zero-cycle of degree 0 on X.

A classical problem in complex function theory which was studied by Abel is to decide when there exists a meromorphic function $f \in \mathbb{C}(X)^*$ with $\mathrm{div}(f) = \alpha$, i.e. when α is a principal divisor.

Let $\mathrm{Div}(X)$ be the divisor group of X and let $C_1(X)$ be the abelian group generated by continuous maps $\gamma : [0,1] \to X$.

Let $\delta : C_1(X) \to \mathrm{Div}(X)$ be the map defined by $\delta(\gamma) = \gamma(1) - \gamma(0)$ and $Z_1(X) = \mathrm{Ker}\delta$ be the group of 1-cycles (closed paths) which has the first homology group $H_1(X, \mathbb{Z})$ as a factor group. For $\gamma \in C_1(X)$ and $\omega \in H^0(X, \Omega^1)$ the integral $\int_\gamma \omega$ is well-defined.

Now let $\gamma \in Z_1(X)$. As global holomophic 1-forms are closed, Stokes' Theorem implies that $\int_\gamma \omega$ only depends on the homology class of γ in $H_1(X, \mathbb{Z})$. Hence one gets a linear, injective map

$$H_1(X, \mathbb{Z}) \longrightarrow H^0(X, \Omega^1)^*.$$

As $H_1(X, \mathbb{Z})$ has rank $2g$, its image defines a lattice in the g-dimensional $\mathbb{C}$-vector space $H^0(X, \Omega^1)^*$, hence the quotient $H^0(X, \Omega^1)^* / H_1(X, \mathbb{Z})$ is a complex torus.

For a zero-cycle α of degree 0, $\alpha = \sum_{i=1}^N n_i([x_i] - [0])$ choose paths γ_i from 0 to x_i. Then the image of $\sum n_i \int_{\gamma_i}$ in $H^0(X, \Omega^1)^* / H_1(X, \mathbb{Z})$ only depends on the zero-cycle α.

Let $Z_0(X)$ be the abelian group of zero-cycles of degree 0. Then the map

$$\begin{array}{rlcl} \rho_X : & Z_0(X) & \longrightarrow & J(X) = \frac{H^0(X,\Omega^1)^*}{H_1(X,\mathbb{Z})} \\ & \sum n_i \left([x_i] - [0] \right) & \longmapsto & \left(\omega \mapsto \sum n_i \int_0^{x_i} \omega \right) \end{array}$$

is well-defined.

The Theorems of Abel and Jacobi describe the properties of ρ_X.

Theorem 5.1.1.

a. *(Abel)* $\mathrm{Ker}\rho_X$ *equals the set of principal divisors, so* ρ_X *induces an injection*

$$A_0(X) = Z_0(X)/\text{principal divisors} \hookrightarrow J(X).$$

b. *(Jacobi)* ρ_X *is an isomorphism.*

Moreover, the quotient J(X) has the structure of an abelian variety, called the Jacobian variety of X*. It has dimension* g*.*

More generally, let $X/\mathbb{C}$ be a smooth proper variety with $\dim X = d$ such that $X(\mathbb{C})$ is a compact complex manifold. Again we can consider the Abel-Jacobi map

$$\rho_X : A_0(X) \longrightarrow \frac{H^0(X,\Omega^1)^*}{H_1(X,\mathbb{Z})} = \mathrm{Alb}_X(X)$$

defined in the same way, with values in the Albanese variety of X, which is an abelian variety associated to X in a canonical way and satisfies a universal property.

The analogue of the Abel-Jacobi theorem does not hold in general as was noticed by Mumford.

Theorem 5.1.2. *If $H^2(X,\mathcal{O}_X) \neq 0$, then* $\mathrm{Ker}\rho_X$ *is large (contains a ∞-dimensional $\mathbb{Q}$-vector space).*

Conjecture 5.1.3. *If $H^2(X,\mathcal{O}_X) = 0$, then ρ_X is an isomorphism.*

One can also consider Abel-Jacobi maps in other codimensions. Let $\mathrm{Ch}^i(X)$ be the Chow group of codimension i-cycles modulo rational equivalence. One has a cycle class map with values in Betti cohomology

$$\mathrm{cl}_B : \mathrm{Ch}^i(X) \longrightarrow H^{2i}_B(X(\mathbb{C}),\mathbb{Z}).$$

Let $\mathrm{Ch}^i(X)_0 = \mathrm{Ker}\mathrm{cl}_B$.

In analogy to

$$\mathrm{Alb}(\mathbb{C}) = \frac{H^{2d-1}(X(\mathbb{C}),\mathbb{C})}{(H^{2d-1}(X(\mathbb{C}),\mathbb{Z}(d)) + \mathrm{Fil}^d)}$$

one can consider the so called intermediate Jacobians

$$\mathrm{Jac}^i_X(\mathbb{C}) = \frac{H^{2i-1}(X(\mathbb{C}),\mathbb{C})}{H^{2i-1}(X(\mathbb{C}),\mathbb{Z}(i)) + \mathrm{Fil}^i}$$

which are no longer abelian varieties in general. (Note that $\mathbb{Z}(i) = \mathbb{Z}(2\pi\sqrt{-1})^{\otimes i}$ for $i \in \mathbb{N}$ and Fil^i denotes the Hodge-filtration.) Let $j \in \mathbb{N}$ be such that $i + j = d$.

By duality between cohomology and homology one has an isomorphism

$$\mathrm{Jac}^i_X(\mathbb{C}) \cong \frac{F^{j+1}H^{2j+1}(X(\mathbb{C}),\mathbb{C})^*}{H_{2j+1}(X(\mathbb{C}),\mathbb{Z})}.$$

The generalized Abel-Jacobi map

$$\rho^{(i)} : \mathrm{Ch}^i(X)_0 \longrightarrow \mathrm{Jac}^i_X(\mathbb{C})$$

can be described via integration as follows.

Let Z be a codimension i-cycle in $\mathrm{Ch}^i(X)_0$ and Γ a topological chain with boundary Z.

Then $\rho^{(i)}_X(\mathbb{Z})(\omega) = \int_\Gamma \omega$ for any holomorphic $j+1$-form ω.

In the following we describe p-adic analogues of these maps, so called p-adic Abel-Jacobi maps which often occur as syntomic regulator maps by using p-adic integration theory.

5.2. Abelian varieties over p-adic fields. Let A/K be an abelian variety over a p-adic field K with good reduction. Consider the Kummer-sequence on $\bar{K}$-valued points

$$0 \longrightarrow A(\bar{K})_{p^n} \longrightarrow A(\bar{K}) \xrightarrow{p^n} A(\bar{K}) \longrightarrow 0.$$

The long exact Galois cohomology sequence induces a map

$$A(K) \otimes \mathbb{Q}_p \xrightarrow{\partial} H^1(K, V_p(A_{\bar{K}}))$$

where $V_p(A_{\bar{K}})$ is the p-adic Tate-module of A $(\otimes\mathbb{Q}_p)$. The image of ∂ is the Bloch-Kato group $H^1_f(K, V_p(A_{\bar{K}}))$, defined in (B-K). As $A(K)$ is a p-adic Lie group one has an exponential map

$$\mathrm{Lie}(A(K)) \xrightarrow{\exp} A(K) \otimes \mathbb{Q}$$

on the Lie algebra $\mathrm{Lie}(A(K))$ which can be canonically defined with $H^1(\hat{A}, \mathcal{O}_{\hat{A}}) \cong H^1_{\mathrm{dR}}(\hat{A})/\mathrm{Fil}^1$ where $\hat{A}$ is the dual abelian variety. This quotient can be identified with $H^{2d-1}_{\mathrm{dR}}(A)/\mathrm{Fil}^d$ which — by Poincaré duality — is isomorphic to $(\mathrm{Fil}^1 H^1_{\mathrm{dR}}(A))^*$.

The map $\partial \circ \exp : H^{2d-1}_{\mathrm{dR}}(A)/\mathrm{Fil}^d \xrightarrow{\cong} H^1_f(K, V_p(A_{\bar{K}}))$ is the Bloch-Kato exponential map (B-K), denoted here by Exp and is defined for any (de Rham) p-adic Galois-representation. Let $x \in A(K)$. Then $\mathrm{Exp}^{-1}(\partial(x))(\omega)$ for $\omega \in H^0(A, \Omega^1)$ can be described using p-adic integrals:

One has (for Log being a local inverse of Exp)

$$\begin{aligned} \mathrm{Exp}^{-1}(\partial(x))(\omega) &= \mathrm{Log}(x)(\omega) \\ &= F_\omega(x) \end{aligned}$$

where F_ω is a Coleman integral of ω satisfying $F_\omega(0) = 0$. The theory of Coleman integrals is reviewed in the next sections. For $\omega \in H^0(A, \Omega^1)$ one way to define F_ω is via the formula

$$F_\omega(x) := \mathrm{Log}(x)(\omega).$$

5.2.1. We will need some elementary definitions and properties in Milnor K-theory.

For a field F, let $K_0(F) = \mathbb{Z}$, $K_1(F) = F^*$,
$K_2(F) = F^* \otimes_{\mathbb{Z}} F^*/\langle a \otimes (1-a), a \neq 0, 1\rangle$.

The image of $a \otimes b$ in $K_2(F)$ is call the Steinberg symbol and denoted by $\{a, b\}$. The relation $\{a, 1-a\} = 0$ in $K_2(F)$ is called Steinberg-relation. Now let F be a discretely valued field with valuation v and residue field k

The map

$$\begin{aligned} T_v : K_2(F) &\longrightarrow K_1(k^*) = k^* \\ \langle a, b\rangle &\longmapsto (-1)^{v(a)v(b)} \overline{\frac{a^{v(b)}}{b^{v(a)}}} \end{aligned}$$

is called the tame symbol.

Let, for a smooth scheme Z over a Dedekind ring R, K_2 be the Zariski sheaf associated to the presheaf

$$K_2(U) = \frac{\mathcal{O}(U)^* \otimes \mathcal{O}(U)^*}{\langle a \otimes (1-a), a, 1-a \in \mathcal{O}(U)^* \rangle}.$$

Then one has the following.

Theorem 5.2.2 (Bloch-Gersten-Quillen). *The complex*

$$\oplus_{x \in Z^0} K_2(k(x)) \xrightarrow{T_y} \oplus_{y \in Z^1} k(y)^* \xrightarrow{\text{div}} \oplus_{z \in Z^2} \mathbb{Z}$$

computes the Zariski-cohomology of the sheaf K_2. Moreover, $H^2_{\text{zar}}(Z, K_2) \cong \mathrm{Ch}^2(Z) := \mathrm{coker}(\text{div})$.

5.3. p-adic integration on curves. Let $C/\mathbb{Z}_p$ be smooth and proper and $U \subset C$ be an affine open such that $Z := C_{\mathbb{F}_p} \backslash U_{\mathbb{F}_p}$ is a finite set of closed points. To U one can associate a basic wide open V in the sense of Coleman ((Col1), (Col2)) which coincides with the affinoid Dagger space $]U_{\mathbb{F}_p}[^{+}_{\hat{C}_{\mathbb{Q}_p}}$ in the rigid analytification $\hat{C}$ of C. Let for $r < 1$, D_r be the disc of radius r. Let V_r be the curve obtained by removing from $\hat{C}$ discs D_r in the tubes of the finitely many points $e \in Z$. Then $V = \varprojlim V_r$. For $e \in Z$ let V_e be the annuli end at e.

Then $A(V_e) = \{f = \sum_{n \geq -\infty} a_n z_e^n, f$ converges for $r < |z_e| < 1$ for some $r > 0\}$. Here z_e is a local parameter at e.

Define $A_{\log}(V_e) = A(V_e)[\log z_e]$ and for $x \in U(\mathbb{F}_p)$, let $\mathcal{U}_x = \{|z_x| < 1\} =]x[_{\hat{C}_{\mathbb{Q}_p}}$ and $A(\mathcal{U}_x) = \{f = \sum_{n \geq 0} a_n z_x^n, f$ converges for $|z_x| < 1\}$.

With the definition $\mathrm{d}\log z_e = \frac{\mathrm{d}z_e}{z_e}$ one sees that any 1-form is locally integrable.

The idea of Coleman-integration is to construct a canonical subspace $A_{\text{Col}}(V) \subset \prod_{x \in U(\mathbb{F}_p)} A(\mathcal{U}_x) \times \prod_{e \in Z} A_{\log}(V_e)$ such that any Coleman 1-form ω, i.e. $\omega \in A_{\text{Col}}(V) \otimes \Omega^1(V) =: \Omega^1_{\text{Col}}(V)$, becomes integrable (globally), unique up to constants, i.e. one obtains an exact sequence

$$0 \longrightarrow \mathbb{C}_p \longrightarrow A_{\text{Col}}(V) \xrightarrow{\mathrm{d}} \Omega^1_{\text{Col}}(V) \longrightarrow 0. \tag{5.3.1}$$

We describe the first step in this construction, namely we associate to $\omega \in \Omega^1(V)$ a unique $F_\omega \in A_{\text{Col},1}(V)$ (unique map up to constants) as follows: consider the class $[\omega] \in H^1_{\text{MW}}(\mathcal{U}_{\mathbb{F}_p}, \mathbb{Q}_p)$ in the Monsky-Washnitzer cohomology which is equipped with a cannonical action of Frobenius Φ. It comes from lifting the Frobenius from $\mathcal{U}_{\mathbb{F}_p}$ to the affinoid Dagger-space $]\mathcal{U}_{\mathbb{F}_p}[^{+}$(GK). There exists a polynomial $P \in \bar{\mathbb{Q}}_p[T]$ with roots which are not roots of unity such that $P(\Phi^*)\omega = \mathrm{d}\eta$ for some $\eta \in A(V)$.

Then Coleman shows that there is a unique $F_\omega \in \prod_{x \in U(\mathbb{F}_p)} A(\mathcal{U}_x) \times \prod_{e \in Z} A_{\log}(V_e)$ (unique up to constants) such that $P(\Phi^*)F_\omega = \eta$, hence one obtains an exact sequence

$$\begin{array}{ccc} 0 \longrightarrow \mathbb{C}_p \longrightarrow A_{\mathrm{Col},1}(V) & \overset{\mathrm{d}}{\longrightarrow} & \Omega^1(V) \longrightarrow 0 \\ F_\omega = \displaystyle\int \omega & \longmapsto & \omega. \end{array}$$

The subspace $A_{\mathrm{Col}}(V)$ together with a map $\int : \omega \mapsto F_\omega$ from $A_{\mathrm{Col}}(V) \otimes_{A(V)} \Omega^1(V)$ to $A_{\mathrm{Col}}(V)$ is uniquely determined by the following properties:

1. $\int$ is primitive for the differentials $\mathrm{d} : \mathrm{d}F_\omega = \omega$.
2. Frobenius-equivariance:
$$\int (\Phi^* \omega) = \Phi^* \left(\int \omega \right).$$
3. If $g \in A(V)$, then $F_{\mathrm{d}g} = g + \mathbb{C}_p$.

Lemma 5.3.2. *For $g \in A(V)$ we have $F_{\mathrm{d}\log g} = \log g$.*

Then define $F_{\log g \cdot \omega} = F_{F_{\mathrm{d}\log g} \cdot \omega}$.

Let now $f, g \in \bar{\mathbb{Q}}_p(C)$. Assume $f, g \in \mathcal{O}(U)^*/\mathbb{Z}_p$. Assume $\mathrm{div}(f) \cap \mathrm{div}(g) \neq \emptyset$. Suppose $\mathrm{ord}_{x_0}(g) \neq 0$ for any $\bar{\mathbb{Q}}_p$-rational point x_0. Choose $F_{\log g \cdot \omega}$ and choose F_ω such that $F_\omega(x_0) = 0$ (for $\omega \in H^0(C, \Omega^1)$. Then choose $\int F_\omega \mathrm{d}\log g$ such that the integration by parts formula holds:

$$F_{\log g \omega} + \int F_\omega \mathrm{d}\log g = \log g F_\omega.$$

As the logarithm is bounded on K^* for any discretely valued field K we see that $\lim\limits_{x \to x_0} (\log g F_\omega)(x) = 0$. Then define

$$F_{\log g \omega}(x_0) = \left(- \int F_\omega \mathrm{d}\log g \right)(x_0).$$

Let $\mathrm{div} f = \sum n_i(x_i)$. Define

$$\int_{(f)} \log g \cdot \omega = \sum_i n_i F_{\log g \omega}(x_i).$$

We have seen that $F_{\log g \omega}$ extends to a functions $C(\mathbb{C}_p) \to \mathbb{C}_p$ by continuity.

Define $r_C(\{f, g\})(w) = \int_{(f)} \log g \cdot \omega$.

Theorem 5.3.3 (Coleman-de Shalit)**.** *(Col-dS) $r_C(\{f, g\})$ is bilinear, skew-symmetric and satisfies the following*

a. *r_C factors through $K_2(\bar{\mathbb{Q}}_p(C))$ to give a homomorphism*
$$r_C : K_2(\bar{\mathbb{Q}}_p(C)) \longrightarrow \mathrm{Hom}(H^0(C, \Omega^1_{C/\bar{\mathbb{Q}}_p}), \bar{\mathbb{Q}}_p),$$
b. *depends only on* $\mathrm{div}(f)$, $\mathrm{div}(g)$*,*
c. *is* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$*-equivariant,*

d. *is functorial in C: if $u : C' \to C$ is a finite morphism, then*

$$r_C(u^*f, u^*g) = u^* r_C(f, g).$$

Coleman and de Shalit apply this construction to CM-elliptic curves E and relate the above regulator r_E, evaluated at certain Steinberg-symbols $\{f, g\}$ where f and g are $\mathbb{Q}$-rational functions with divisors supported at torsion points of E to the value of the p-adic L-function $L_p(E, s)$ at $s = 0$.

In a series of papers ((B1) - (B4)) A. Besser studies rigid syntomic regulators with values in certain (modified) syntomic cohomology groups H^i_{ms}. In particular, for $f, g \in \mathcal{O}(U)^*$, where $U \subset C_{\mathbb{Z}_p}$ is as above he defines $r_{\mathrm{syn}}(f), r_{\mathrm{syn}}(g) \in H^1_{\mathrm{ms}}(U, 1)$ and their cup-product $r_{\mathrm{syn}}\{f, g\}) \in H^2_{\mathrm{ms}}(U, 2)$. One of his main results is to relate the Coleman-de Shalit regulator (defined via p-adic integrals) to syntomic regulators. More precisely he shows the following ((B2)):

Theorem 5.3.4. *The following diagram*

$$\begin{array}{ccc}
K_2(C_{\mathbb{Q}_p}) & \xrightarrow{r_{\mathrm{syn}}} & H^2_{\mathrm{syn}}(C, 2) = H^1_{\mathrm{dR}}(C_{\mathbb{Q}_p}) \\
\downarrow & & \downarrow \\
K_2(\bar{\mathbb{Q}}_p(C)) & \longrightarrow & \mathrm{Hom}(H^1_{\mathrm{dR}}(C_{\bar{\mathbb{Q}}_p}), \bar{\mathbb{Q}}_p) \\
\downarrow{\scriptstyle r_{p,C}} & & \downarrow \\
\mathrm{Hom}(H^0(C, \omega^1_{C/\bar{\mathbb{Q}}_p}), \bar{\mathbb{Q}}_p) & = & \mathrm{Hom}(H^0(C, \omega^1_{C/\bar{\mathbb{Q}}_p}), \bar{\mathbb{Q}}_p)
\end{array}$$

is commutative. Here the first right vertical arrow is induced by Poincaré duality.

The proof of this Theorem relies on the one hand on Serre's cup product formula which says that for two 1-forms of the second kind ω,η giving rise to globally defined cohomology classes in $H^1_{\mathrm{dR}}(C)$.

One has

$$\omega \cup \eta = \sum_{x \in C} \mathrm{Res}_x(F_\omega \cdot \eta)$$

and on the following residue formula ((B2)).

Proposition 5.3.5. *Let $f, g \in \bar{\mathbb{Q}}_p(C)$, $\omega \in H^0(C, \Omega^1_{C/\mathbb{Q}_p})$ and $\eta(f, g)$ be the image of $r_{\mathrm{syn}}(\{f, g\})$ under the isomorphism $H^2_{\mathrm{ms}}(U, 2) \cong H^1_{\mathrm{MW}}(\mathcal{U}_{\mathbb{F}_p}, \mathbb{Q}_p) = H^1_{\mathrm{rig}}(\mathcal{U}_{\mathbb{F}_p}, \mathbb{Q}_p)$.*

Then

$$\sum_{\substack{V_e \text{ annuli} \\ \text{end at } e}} \mathrm{Res}_e(F_\omega \cdot \eta(f, g)) = \sum_{x \in C} \log T_x\{f, g\} F_\omega(x) + \int_{(f)} \log g \cdot \omega.$$

Here T_x is the previously defined tame symbol and $\int_{(f)} \log \cdot \omega$ the integral defined via the function $F_{\log g \cdot \omega}$.

As is explained by Besser the left hand side in the above formula is "morally" the cup-product "$\log f d\log g$" $\cup\omega$ which does not have a meaning in the p-adic setting, but is defined in the context of complex regulators, defined by Bloch and Beilinson.

5.4. p-adic regulators on surfaces. Let X be a smooth proper surface over a p-adic field K with good reduction, so there exists a smooth proper model $\mathcal{X}$ over $\mathcal{O}_K$, the ring of integers in K, with generic fiber X and closed fiber Y.

Let $H^i_{\mathrm{zar}}(\mathcal{X},\mathcal{K}_2)$ (resp. $H^i_{\mathrm{zar}}(X,\mathcal{K}_2)$) be the Zariski-$K$-cohomology on $\mathcal{X}$ (resp. X) and $\mathrm{Pic}(Y)$ the Picard group of Y.

Localization in algebraic K-theory yields an exact sequence (Mi):

$$H^1_{\mathrm{zar}}(\mathcal{X},\mathcal{K}_2) \longrightarrow H^1_{\mathrm{zar}}(X,\mathcal{K}_2) \xrightarrow{\partial} \mathrm{Pic}(Y). \tag{5.4.1}$$

Note that an element in $H^1(X,\mathcal{K}_2)$ is represented by a finite formal sum $\sum_{i=1}^n (C_i,f_i)$, where C_i is a curve on X, $f_i\in k(C_i)$ and $\sum_{i=1}^n \mathrm{div}(f_i)=0$. This follows from Theorem 5.2.2. One has a similar description for $H^1_{\mathrm{zar}}(\mathcal{X},K_2)$.

If for an abelian group M, $\hat{M}=\varprojlim_n M/p^n$ denotes its p-adic completion, then 5.4.1 induces an exact sequence

$$0\longrightarrow H^1_{\mathrm{zar}}\widehat{(\mathcal{X},\mathcal{K}_2)}\otimes\mathbb{Q}_p \longrightarrow H^1_{\mathrm{zar}}\widehat{(X,\mathcal{K}_2)}\otimes\mathbb{Q}_p \xrightarrow{\partial} \mathrm{Pic}(Y). \tag{5.4.2}$$

The following lemma follows from Bloch-Ogus theorey and the theorey of Merkurjev-Suslin relating K_2 of a field to its Galois cohomology (see (CT-R)):

Lemma 5.4.3. *There is an isomorphism*

$$H^1_{\mathrm{zar}}(X,\mathcal{K}_2/p^n)\cong \mathrm{Ker}(H^3_{\mathrm{et}}(X,\mathbb{Z}/p^n(2))\longrightarrow H^3_{\mathrm{et}}(k(X),\mathbb{Z}/p^n(2)))$$

where the right hand side is also known as the first coniveau filtration on $H^3_{\mathrm{et}}(X,\mathbb{Z}/p^n(2))$.

Using lemma 5.4.3 one gets the étale p-adic regulator map

$$H^1\widehat{(X,\mathcal{K}_2)}\otimes\mathbb{Q}_p \overset{c_{\mathrm{et}}}{\hookrightarrow} H^3_{\mathrm{et}}(X,\mathbb{Q}_p(2))\cong H^1(\mathrm{Gal}(\bar{K}/K),V) \tag{5.4.4}$$

where $V:=H^2_{\mathrm{et}}(\bar{X},\mathbb{Q}_p(2))$ and the last isomorphism is induced by the Hochschild-Serre spectral sequence and uses a weight-argument from the Weil-conjectures.

Let

$$H^1_f(K,V):=\mathrm{Ker}\left(H^1(\mathrm{Gal}(\bar{K}/K),V)\longrightarrow H^1(\mathrm{Gal}(\bar{K}/K),B_{\mathrm{cris}}\otimes V)\right)$$

where B_{cris} is Fontaine's ring of p-adic periods. Then 5.4.2 – 5.4.4 induce a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1_{\mathrm{zar}}\widehat{(\mathcal{X},\mathcal{K}_2)}\otimes\mathbb{Q}_p & \longrightarrow & H^1_{\mathrm{zar}}\widehat{(X,\mathcal{K}_2)}\otimes\mathbb{Q}_p \\ & & \big\downarrow r_{\mathrm{syn}} & & \big\downarrow c_{\mathrm{et}} \\ 0 & \longrightarrow & H^1_f(K,V) & \longrightarrow & H^1(\mathrm{Gal}(\bar{K}/K),V). \end{array} \tag{5.4.5}$$

Here the vertical maps are injections and we can identify — using a well-known isomorphism between syntomic cohomology and $H^1(K,V)$ and the compatibility of syntomic with étale regulators proven by Niziol (see also (L-S)) — the left vertical map with the syntomic regulator, although the syntomic cohomology $H^3_{\text{syn}}(\mathcal{X}, S_{\mathbb{Q}_p}(2))$ will not occur explicitly in this section.

On $H^1_{\text{zar}}(\mathcal{X}, \mathcal{K}_2)$ one has so-called decomposable elements arising by cup-product from $\operatorname{Pic}(\mathcal{X}) \otimes \mathcal{O}_K^*$.

One has a map

$$\operatorname{Pic}(\mathcal{X}) \otimes \mathcal{O}_K^* \longrightarrow NS(\mathcal{X}) \otimes \mathcal{O}_K^* \longrightarrow H^1_f(K, \mathbb{Q}_p(1) \otimes \operatorname{NS}(\bar{X}))$$

where $\operatorname{NS}(X)$ denotes the Neron-Severi group.

Assume that $\operatorname{NS}(\bar{X}) = \operatorname{NS}(X)$. Then we get the map

$$\operatorname{Pic}(\mathcal{X}) \otimes \mathcal{O}_K^* \longrightarrow \operatorname{NS}(X) \otimes H^1_f(K, \mathbb{Q}_p(1))$$

which fits into a commutative diagram (L)

$$\begin{array}{ccc} \operatorname{Pic}(\mathcal{X}) \otimes \mathcal{O}_K^* & \longrightarrow & H^1_{\text{zar}}(\widehat{\mathcal{X}, \mathcal{K}_2}) \otimes \mathbb{Q}_p \\ \downarrow & & \downarrow r_{\text{syn}} \\ \operatorname{NS}(X) \otimes H^1_f(K, \mathbb{Q}_p(1)) & \hookrightarrow & H^1_f(K, V). \end{array} \tag{5.4.6}$$

The left vertical map comes from a boundary map of the Kummer sequence $K^* \to H^1(K, \mathbb{Q}_p(1))$. The image of the decomposable elements generates $\operatorname{NS}(X) \otimes H^1_f(K, \mathbb{Q}_p(1))$ (L).

As mentioned in section 5.2, the Bloch-Kato exponential map (B-K) is defined for any (de Rham-) Galois-representation. In our situation, Exp induces an isomorphism (using B_{dR}-comparison isomorphism)

$$H^2_{\text{dR}}(X)/\operatorname{Fil}^2 \cong H^1_f(K, V). \tag{5.4.7}$$

By Poincaré duality, $H^2_{\text{dR}}(X)/\operatorname{Fil}^2 \cong (\operatorname{Fil}^1 H^2_{\text{dR}}(X))^*$ so we can interpret a syntomic cohomology class as a linear form on $\operatorname{Fil}^1 H^2_{\text{dR}}(X)$.

Lemma 5.4.8. *r_{syn} maps the decomposable elements (i.e. $\operatorname{Pic}(\mathcal{X}) \otimes \mathcal{O}_K^*$) in $Fil^1 H^2_{\text{dR}}(X)/\operatorname{Fil}^2$ under the isomorphism Exp^{-1} (5.4.7).*

For the proof see (L).

Corollary 5.4.9. *An element $z \in H^1(\mathcal{X}, \mathcal{K}_2)$ is regulator-indecomposable (i.e. $r_{\text{syn}}(z) \notin \operatorname{NS}(X) \otimes H^1_f(K, \mathbb{Q}_p(1))$) if there exists a 2-form $\omega \in H^0(X, \Omega^2) = \operatorname{Fil}^2 H^2_{\text{dR}}(X)$ such that $r_{\text{syn}}(z)(\omega) \neq 0$.*

If $\omega = \eta_1 \cup \eta_2$ where $\eta_1 \in \operatorname{Fil}^1 H^1_{\text{dR}}(X)$, $\eta_2 \in H^1_{\text{dR}}(X)$ (so ω is a cup-product of two 1-forms) and if $z \in H^1(\mathcal{X}, \mathcal{K}_2)$ is represented by a finite formal sum $z = \sum_{i=1}^n (C_i, f_i)$ then Besser (B4) has recently proven a formula for $r_{\text{syn}}(z)(\eta_1 \cup \eta_2)$ using generalized residues (that he calls triple indices, defined in (B-dJ)), involving $\log f_i$ and the Coleman integrals of η_1 and η_2. If η_1 and η_2 are both global holomorphic 1-forms in $H^0(X, \Omega^1)$ one can describe his formula as follows.

Proposition 5.4.10.

$$r_{\mathrm{syn}}(z)(\eta_1 \cup \eta_2) = \sum_{i=1}^{n} \sum_{e} \mathrm{Res}_e \left(\int F_{\pi_i^* \cdot \eta_1} \pi_i^* \eta_2 \right) \mathrm{d} \log f_i .$$

Here $\pi_i : Z_i \to X$ is a normalization of the curve C_i, the functions f_i are invertible on some open affine $\mathcal{U}_i \subset Z_i$ and the residues are taken at annuli ends attached to the basic wide opens V_i associated to $\mathcal{U}_i$. Then $\int F_{\pi_i^* \cdot \eta_1} \pi_i^* \eta_2$ is a Coleman-integral in $A_{\mathrm{Col}}(V_i)$.

Proposition 5.4.10 should be compared with Theorem 5.1.4 and the Abel-Jacobi map for abelian varieties in section 5.2.

An interesting case where this formula can be applied is the case of a self-product of an elliptic curve $\mathcal{E}/\mathbb{Z}_p$.

There are elements in $H^1(\mathcal{E} \times \mathcal{E}, \mathcal{K}_2)$ which turn out to be regulator-decomposable (see (L)) and there are elements constructed by Mildenhall and Flach (see (Mi)) which are candidates for being regulator-indecomposable. In the following we will discuss these elements.

Let E be an elliptic curve defined over $\mathbb{Q}$ and $X_0(N) \xrightarrow{\pi} E$ a modular parameterization, with N being the conductor of E.

We recall the element defined by Flach/Mildenhall in $H^1(X_0(N) \times X_0(N), \mathcal{K}_2)$ (resp. $H^1(E \times E, \mathcal{K}_2)$). Let l be a prime that does not divide N. Then we have the Atkin-Lehner involution

$$W_l : X_0(lN) \longrightarrow X_0(lN)$$

which on $Y_0(lN)$ can be described as follows:

Identify a point $(A, C_{lN}) \in Y_0(lN)$, where A is an elliptic curve and C_{lN} a (cyclic) subgroup of order lN. with a cyclic isogeny of degree l between elliptic curves equipped with a subgroup of order N

$$\lambda_l : (A, C_N) \longrightarrow (A/C_l, C_{lN}/C_l)$$

where C_N, C_l are the unique subgroups of orders N and l in C_{lN}.

W_l sends the isogeny λ_l to its dual λ_l^*. Cusps on $X_0(N)$ are equivalence classes of $\mathbb{P}^1_{\mathbb{Q}}$ under the action of $\Gamma_0(N)$. For each $0 < d|N$ let $t = \gcd(d, \frac{N}{d})$. Then there are $\phi(t)$ cusps $\binom{a}{d}$ with $a \in (\mathbb{Z}/t\mathbb{Z})^*$. $\binom{a}{d}$ is the class of a cusp $\frac{x}{y}$ with $x \equiv a \mod t$, $y \equiv d \mod N$. Notation: $P_d^a := \binom{a}{d}$.

Above each cusp P_d^a of $X_0(N)$ with $d|N$ there are two cusps in $X_0(lN)$, namely P_d^a and P_{ld}^a that are swapped under W_l.

Then we have the map

$$\epsilon : X_0(lN) \longrightarrow X_0(N) \times X_0(N),$$

$\epsilon = (d_1, d_1 \circ W_l)$, where d_1 is the degeneracy map. The image of ϵ is the graph of the l-Hecke operator on $X_0(N) \times X_0(N)$ and is called T_l.

On $X_0(lN)$ we have the modular unit

$$g_{l,N} := \prod_{d||N} \frac{\Delta_d}{\Delta_{ld}} \in \left(\mathcal{O}(\mathcal{Y}(lN))/\mathbb{Z}\left[\frac{1}{lN}\right]\right)^*$$

where for $M \in \mathbb{N}$, $\Delta_M(z)$ is equal to $\Delta(Mz)$ and is a modular form for $\Gamma_0(M)$ induced by the discriminant form Δ; this is a unique cusp form of weight 12 for $SL_2(\mathbb{Z})$. The divisor of Δ_M at the cusp is well-known.

It is shown by Mildenhall and Flach that

$$(*) \qquad \mathrm{ord}_{P_d^a}(g_{l,N}) = -\mathrm{ord}_{P_{ld}^a}(g_{l,N}) \neq 0.$$

This implies that $\epsilon_*(\mathrm{div} g_{l,N}) = 0$; hence $(T_l, g_{l,N})$ defines an element in $H^1(X_0(N) \times X_0(N), \mathcal{K}_2)$ which is integral away from $N \cdot l$. (Its properties at the prime l where they satisfy an Eichler-Shimura identity are crucial in the papers of Mildenhall/Flach, but we don't need them here.)

Let p be a prime not dividing $l \cdot N$. Then $\pi_*(T_l, g_{l,N})$ is an element in the cohomology $H^1(\mathcal{E} \times \mathcal{E}_{\mathbb{Z}_p}, \mathcal{K}_2)$ and we conjecture that for a given prime p there always exists an $l \neq p$, $l \not| N$ such that $r_{\mathrm{syn}}(\pi_*(T_l, g_{l,N}))$ is indecomposable in $H^3_{\mathrm{syn}}(\mathcal{E} \times \mathcal{E}_{\mathbb{Z}_p}, S_{\mathbb{Q}_p}(2))$.

To prove this conjecture, one has to apply Besser's triple index formula (proposition 5.4.10) to compute

$$r_{\mathrm{syn}}(\pi_*(T_l, g_{l,N}))(\omega_1 \cup \omega_2)$$

where ω is an invariant form of E, so $\omega \in H^0(E, \Omega^1)$, $\omega_1 = \pi_1^*\omega$, $\omega_2 = \pi_2^*\omega$ with $\pi_i : E \times E \to E$ the canonical projections.

Remark. We note that, by different methods, indecomposable elements in $H^1(\mathcal{X}_{\mathbb{Z}_p}, \mathcal{K}_2)$ were constructed by Asakura and Sato (A-S), when $\mathcal{X}$ is a model of an elliptic K_3-surface.

References

[A-S] M. Asakura and K. Sato, *Beilinson's Tate conjecture for K_2 and finiteness of torsion zero-cycles on elliptic surfaces*, Preprint (2009).

[B1] A. Besser, *Syntomic regulators and p-adic integration I: rigid syntomic regulators*, Israel Journal of Math. **120** (2000), 291–334.

[B2] A. Besser, *Syntomic regulators and p-adic integration II: K_2 of curves*, Israel Journal of Math. **120** (2000), 335–360.

[B3] A. Besser, *A generalization of Coleman's integration theory*, Inv Math **120** (2) (2000), 397–434.

[B4] A. Besser, *On the syntomic regulator for K_1 of a surface*, Preprint (2007).

[B-dJ] A. Besser and R. de Jeu, *The syntomic regulator for K_4 of curves*, Preprint (2005).

[B-K] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives.* In: Grothendieck Festschrift Vol. I Progress Math. 86, Birkhäuser (1990), 333–400.

[Col-dS] R. Coleman and E. de Shalit, *p-adic regulators on curves and special values of p-adic L-functions*, Invent. Math. **93** (1988) 239–266.

[Col1] R. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), 171–208.

[Col2] R. Coleman, *Torsion points on curves and p-adic abelian integrals*, Annals of Math. **121** (1985), 111–168.

[CT-R] J.-L. Colliot-Thélène and W. Raskind, *K_2-cohomology and the second chow group*, Math. Annalen **270** (1985), 165–199.

[GK] E. Grosse-Kloenne, *Rigid analytic spaces with overconvergent structure sheaf.* Journal Reine Angew. Math. **519** (2000), 73–95.

[L] A. Langer, *On the syntomic regulator for products of elliptic curves*, Preprint (2010).

[L-S] A. Langer and S. Saito, *Torsion zero cycles on the selfproduct of a modular elliptic curve*, Duke Math. J. vol. 85 (1996), 315–357.

[Mi] S. Mildenhall, *Cycles in a product of elliptic curves, and a group analogous to the class group*, Duke Math. J. **67** (1992), 387–406.

Andreas Langer
University of Exeter
Mathematics
Exeter EX4 4QF
Devon, UK