UNIVERSITÀ DEGLI STUDI DI PADOVA
CONCORDIA UNIVERSITY

A thesis presented in Partial Fulfilment of the Requirements for the Algant's Master degree in Mathemathics

Modular forms modulo p

Supervisors:

Professor Adrian Iovita
Professor Giovanni Rosso

Candidate:

Paola Mupo

Academic year 2023-2024
12^{th} July 2024

A mamma, papà
e Camilla

Contents

Introduction

Modular forms are classically defined as holomorphic functions on the complex upper half plane $\mathbb{H}$ that satisfy some functional equations with respect to the action of the modular group $SL_2(\mathbb{Z})$ and its subgroups Γ on $\mathbb{H}$. Thanks to properties of periodicity a modular form f of level Γ is naturally endowed with Fourier expansions

$$f = \sum_{n \geq n_0} a_n q^n$$

at the *cusps* of Γ, called *q-expansions*. With these premises the most naive reader may think that modular forms are merely analytic objects that can be studied through means of complex analysis. But they are indeed powerful tools in modern number theory. Historically, the coefficients of their q-expansions were discovered to encrypt beautiful numerical identities and their popularity grew steadily over the past century as modular forms have found their application in several different contexts. To mention one, modularity theorems, which in a certain sense imply that rational elliptic curves *arise* from modular forms, are incarnations of the deep relation between these two objects which becomes explicit when we attach to them L-functions and Galois representations.

Modular forms of a fixed level Γ over the complex numbers also have a *geometric* interpretation as global differentials on the Riemann surface obtained by quotienting the complex upper half plane by the action of the group Γ. This interpretation is of extreme importance. On one hand it makes easier to study the properties of classical modular forms. On the other it paves the way to the definition of modular forms over fields of positive characteristic.

The aim of this work is to define modular forms modulo p and to present a result about them adopting the two perspectives mentioned above. First we will deal with the case of the full modular group and we will see modular forms only through their q-expansions. Then we will focus on their geometric embodiment to generalize their characterization to level N.

Chapter 1 presents the definition of modular forms as complex analytic objects and collects some of the main results in the classical theory of modular forms which will be of central importance to our purpose. In particular, in the first section we introduce modular forms of full level and state a theorem about their structure of a graded $\mathbb{C}$-algebra generated by the Eisenstein series Q and R of weight 4 and 6 respectively. We then generalize the definition of modular forms to arbitrary congruence subgroups of the modular group.

In Chapter 2 we characterize modular forms modulo p of level 1 for $p \geq 5$ following Swinnerton-Dyer's construction in *On l-adic representations and congruences for coefficients of modular forms* [17]. The associated graded algebra $\widetilde{M}$ is the result of the reduction modulo p of the Fourier expansions of modular forms whose coefficients lie in the ring $\mathbb{Z}_{(p)}$. The action of the operator

$$\theta := q\frac{d}{dq}$$

plays a fundamental role in this setting. Moreover elegant congruence relations between the Bernoulli numbers imply that the reduction of the weight $p-1$ Eisenstein series E_{p-1} is 1 and this is enough to describe the whole algebra of modular forms of full level. More precisely, if we denote by $\tilde{A}$ the homogeneous polynomial in Q and R that corresponds to E_{p-1} modulo p then

$$\widetilde{M} = \mathbb{F}_p[Q, R]/(\tilde{A} - 1).$$

Furthermore $\widetilde{M}$ inherits the structure of graded algebra. Its graded pieces are indexed by $\mathbb{Z}/(p-1)\mathbb{Z}$ and multiplication by $\tilde{A}$ naturally yields the notion of a filtration ω for the elements f of $\widetilde{M}$. Such a simple description seems to require nothing more than the few tools we developed in the first Chapter of this work.
The aim of Chapter 3 and 4 is to extend it to the more general case of modular forms of level N, for an integer $N \geq 3$. The complex analytic theory of modular forms ceases to be enough for such an intent and we're forced to use *geometric* means. In Chapter 3 we give another, more intrinsic, definition of modular forms which arises from the geometry of *elliptic curves*. Following the work of Katz they will either be *functions* on classes of elliptic curves with additional data, or *sections* of line bundles over a *universal* curve. In order to do so we also need to extend our notion of an elliptic curve over a field to the more general one of an elliptic curve over a scheme. In this perspective an elliptic curve is a morphism of schemes whose fibers parametrize genus one curves with a section, that is to say a *family* of elliptic curves in the classical sense. After defining *level structures* for elliptic curves, we will reach the notion of a *universal elliptic curve* $\mathbb{E}$ lying over a *modular curve* $Y(N)$, which represents the functor associating to a scheme the set of isomorphism classes of elliptic curves carrying such extra information. As a result elliptic curves with level N-structures can be obtain through pull-back from the universal elliptic curve

$$\begin{array}{c} \mathbb{E} \\ \big\downarrow \\ Y(N). \end{array}$$

An invertible sheaf on the modular curve, denoted by $\underline{\omega}$, naturally emerges from this setting and represents the key to interpret geometric modular forms, as either functions on pairs of elliptic curves over varying base schemes and level N-structures or equivalently as global sections of the powers of $\underline{\omega}$ on the modular curve. As a result we can define modular forms over any ring. In particular the graded algebra of modular forms modulo p, denoted by $R^{\cdot}_N$, simply coincides with the one of modular forms over a field of positive characteristic p and their q-expansions are defined as their evaluation at a particular curve or, equivalently, in terms of the *cusps* of the modular curve.
Chapter 4 follows Katz's argument in *A result on modular forms in characteristic* p [9]. As in the full level case the only modular form whose q-expansion is 1 is the *Hasse invariant*

denoted by A and its geometric description comes from the action of Fobenius on elliptic curves. Again multiplication by A does not affect q-expansions and naturally determines a filtration on the graded algebra of modular forms. As in Chapter 2 we will analyze the behaviour of an operator on the ring of modular forms whose effect upon q-expansions is $q\frac{d}{dq}$. The construction of such an operator, denoted by $A\theta$, represents the core of Chapter 4 and relies on the action of Frobenius on the first relative de Rham cohomology of $\mathbb{E}$ over $Y(N)$. In particular the image of such a map splits the Hodge filtration on the open subset of the modular curve where the Hasse invariant is invertible. Here we can define $A\theta$ exploiting the action of a *connection* on the first relative de Rham cohomology and working locally we extend such a definition to the whole modular curve. The central theorem of this section is followed by some of its corollaries whose flavour recalls the results presented at the end of Chapter 2 in the full level case.

The main body of this thesis is followed by three appendices. They are a collection of several definitions, proofs and examples that the author of this work has found herself useful in the understanding of the results of Chapter 3 and 4. Appendix A develops in full generality some algebraic-geometric tools about *cohomology of sheaves and de Rham cohomology* and includes some examples in the case of our interest. Appendix B presents the *Hodge filtration* and the *conjugate filtration* that appear in Chapter 4. To conclude in Appendix C we define the algebraic *Gauss-Manin connection* following the exposition of Katz and Oda in [11]. This section includes an explicit computation by Katz for the case of the universal elliptic curve and presents as well the definition of the *Kodaira-Spencer morphism*. The two play a primary role in the construction of the θ operator of Chapter 4.

Chapter 1

Classical theory of modular forms over $\mathbb{C}$

In this chapter we present the classical definitions and some of the results of the theory of modular forms over $\mathbb{C}$ which will be useful in the rest of our work.

1.1 Modular forms of level 1

Let $\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$ be the complex upper half plane. We define the modular group as

$$SL_2(\mathbb{Z}) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, \quad det\gamma = 1 \right\}.$$

Definition 1.1. *Let $f : \mathbb{H} \longrightarrow \mathbb{C}$ be an holomorphic function. We say that f is weakly modular of weight $k \in \mathbb{Z}$ if for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and for any $z \in \mathbb{H}$ we have*

$$f(\gamma z) = (cz + d)^k f(z).$$

We will often write $f_{|k,\gamma}$ to denote the weight k action of γ on f i.e.

$$f_{|k,\gamma}(z) = (cz + d)^{-k} f(z).$$

Then asking that f is weakly modular is equivalent to $f_{|k,\gamma} = f$ for all $f \in SL_2(\mathbb{Z})$.

Remark 1.1. *We observe that if $f \neq 0$ is weakly modular of weight k, then k is even. Indeed let $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{Z})$, then $f(\gamma z) = f(z) = (-1)^k f(z)$ for all $z \in \mathbb{H}$. If k is odd $f(z) = -f(z)$ i.e. $f(z) = 0$ for any $z \in \mathbb{H}$ and this is a contradiction.*

If f is weakly modular

$$f(z + 1) = f(Tz) = f(z)$$

where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hence f is periodic of period 1. The maps

$$z \longrightarrow e^{2\pi i z} \qquad q \longrightarrow \frac{\log q}{2\pi i}$$

give us a bijection between the upper half plane and the punctured unit disk. It follows that the function $\widetilde{f}(q) = f\left(\frac{\log q}{2\pi i}\right)$ is periodic of period $2\pi i$ and admits a Fourier expansion

$$\widetilde{f}(q) = \sum_{n\in\mathbb{Z}} a_n q^n.$$

Remark 1.2. *We say that f is meromorphic at ∞ if $\widetilde{f}(q) = \sum_{n\geq -n_0} a_n q^n$ for an $n_0 > 0$. We say that f is holomorphic at ∞ if $\widetilde{f}(q) = \sum_{n\geq 0} a_n q^n$. Moreover we say that f is cuspidal if f is holomorphic at ∞ and $a_0 = 0$.*

Definition 1.2. *Let $f : \mathbb{H} \longrightarrow \mathbb{C}$ be an holomorphic function. We say that f is a modular form of weight k and level 1 if f is a weakly modular form of weight k and it is holomorphic at ∞.*

From now on we will use the same notation for f and its expansion at ∞.
Let $k \geq 0$ be an even integer. We define the weight k Eisenstein series

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^k}.$$

For or $k \geq 4$ G_k is a modular form of weight k and level $SL_2(\mathbb{Z})$, which has Fourier expansion given by:

$$\begin{aligned} G_k(z) &= \frac{\zeta(1-k)}{2} + \sum_{n\geq 1} \sigma_{k-1}(n) q^n \\ &= -\frac{B_k}{2k} + \sum_{n\geq 1} \sigma_{k-1}(n) q^n \end{aligned}$$

where $\sigma_{k-1}(n) = \sum\limits_{d|n} d^{k-1}$.

Definition 1.3. *The normalized Eisenstein series of weight k is*

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

For $k = 2$ the Eisensten series

$$G_2(z) = 2\zeta(2) + \sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2}$$

is not a modular form of weight 2 because it is not weakly modular of weight 2. In particular one can prove that for $\gamma = S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ we have

$$E_2(\gamma z) = E_2(-1/z) = z^2 E_2(z) + \frac{12}{2\pi i} z. \tag{1.1}$$

Remark 1.3. *Let us denote by $M_k(\mathbb{C})$ the set of modular forms of weight k and level $SL_2(\mathbb{Z})$ and let $S_k(\mathbb{C})$ be the subset of cusp forms. They clearly form $\mathbb{C}$-vector spaces. Moreover it is easy to see that if $f \in M_k(\mathbb{C})$ and $g \in M_h(\mathbb{C})$, then $gh \in M_{h+g}(\mathbb{C})$. Then*

$$M(\mathbb{C}) = \bigoplus_{k\geq 1} M_k(\mathbb{C})$$

is a graded algebra and taking Fourier expansion at the cusp gives us an embedding

$$M(\mathbb{C}) \hookrightarrow \mathbb{C}[\![q]\!]$$

We now recall a technical result for weakly modular meromorphic functions.

Theorem 1.1 (The valence formula)**.** *Let f be a non zero meromorphic function on $\mathbb{H}$ which is weakly modular of weight k. Then:*

$$\frac{k}{12} = \mathrm{ord}_\infty f + \frac{1}{2}\mathrm{ord}_i f + \frac{1}{3}\mathrm{ord}_\rho f + \sum_{\omega \in SL_2(\mathbb{Z})\backslash\mathbb{H}} \mathrm{ord}_\omega f. \tag{1.2}$$

Proof. To prove this classical result we integrate f'/f along the fundamental domain. For the explicit computation see [12] Chapter 1, Theorem 2.1. $\square$

Definition 1.4. *The Ramanujan's Δ function is $\Delta = \frac{E_4^3 - E_6^2}{12^3}$.*

The Δ function is a cusp form of weight 12. As an immediate application of the valence formula we have that it never vanishes in $\mathbb{H}$. As a consequence multiplication by Δ

$$\begin{aligned} M_k(\mathbb{C}) &\longrightarrow S_{k+12}(\mathbb{C}) \\ f &\longrightarrow f\Delta \end{aligned}$$

is an isomorphism of vector spaces. The valence formula also allows us to prove the following result.

Corollary 1.1. *The $\mathbb{C}$-vector spaces $M_k(\mathbb{C})$ and $S_k(\mathbb{C})$ are finite dimensional for every k. Moreover $\dim_{\mathbb{C}}(M_k(\mathbb{C})) = 0$ if $k < 0$ or k is odd and*

$$\dim_{\mathbb{C}}(M_k) = \begin{cases} \lfloor k/12 \rfloor & \text{if } k = 2 \mod 12, \\ \lfloor k/12 \rfloor + 1 & \text{otherwise.} \end{cases}$$

Proof. If f is a modular form then f is holomorphic so all the numbers $\mathrm{ord}_z f$ occurring in the formula (1.2) must be positive. So it's immediate that $M_k(\mathbb{C}) = 0$ for $k < 0$. Moreover applying again (1.2) we must have $M_2(\mathbb{C}) = 0 = S_2(\mathbb{C})$. If $M_k(\mathbb{C}) \neq 0$, the linear map

$$\begin{aligned} M_k(\mathbb{C}) &\longrightarrow \mathbb{C} \\ f = \sum_{n=0}^{\infty} a_n q^n &\longrightarrow a_0 \end{aligned}$$

has kernel $S_k(\mathbb{C})$. So $\dim_{\mathbb{C}} M_k(\mathbb{C}) = \dim_{\mathbb{C}} S_k(\mathbb{C}) + 1$ and the isomorphism above reduces us to compute the dimension of $\dim_{\mathbb{C}}(M_k(\mathbb{C})$ for $k \leq 10$. Constant functions are clearly in $M_0(\mathbb{C})$ so it is nonzero and we conclude that $M_0(\mathbb{C}) = \mathbb{C}$. Assume now that $2 < k \leq 10$. If $f \in S_k(\mathbb{C})$, $f \neq 0$, we have $\mathrm{ord}_\infty f = 1$ and $\lfloor k/12 \rfloor = 0$ contradicting (1.2). So we must have $S_k(\mathbb{C}) = 0$ and $M_k(\mathbb{C}) = 1$. To conclude

$$\begin{aligned}\dim_{\mathbb{C}}(M_k(\mathbb{C}) &= \dim_{\mathbb{C}}(S_k(\mathbb{C})) + 1 = \dim_{\mathbb{C}}(M_{k-12}(\mathbb{C})) + 1 \\ &= \dim_{\mathbb{C}}(M_{k-24}(\mathbb{C})) + 2 \\ &= \ldots = \dim_{\mathbb{C}}(M_{k-\lfloor k/12 \rfloor 12}(\mathbb{C})) + \lfloor k/12 \rfloor\end{aligned}$$

and it equals $\lfloor k/12 \rfloor$ if $k - \lfloor k/12 \rfloor 12 = 2$ i.e. $k = 2 \mod 12$, $1 + \lfloor k/12 \rfloor$ otherwise. □

Theorem 1.2. *Any modular form $f \in M_k(\mathbb{C})$ can be written as an isobaric polynomial in E_4 and E_6 i.e. if $f \in M_k(\mathbb{C})$, then*

$$f = \sum_{4i+6j=k} c_{i,j} E_4^i E_6^j$$

for some $c_{i,j} \in \mathbb{C}$. As a consequence we have the equality of graded algebras

$$M(\mathbb{C}) = \mathbb{C}\left[E_4, E_6\right].$$

Proof. We prove that $\{E_4^i E_6^j, 4i + 6j = k\}$ is a set of generators for $M_k(\mathbb{C})$. If $k \leq 12$, the $\mathbb{C}$-vector space $M_k(\mathbb{C})$ has dimension 1. Then for $k = 4$ and $k = 6$ we must have that E_4 and E_6 are a basis for $M_4(\mathbb{C})$ and $M_6(\mathbb{C})$ respectively. Moreover E_4^2 and $E_4 E_6$ are non zero modular forms of weight 8 and 10 respectively so they must be a basis for $M_k(\mathbb{C})$ for $k = 8, 10$. Let now $k \geq 12$ and $f \in M_k(\mathbb{C})$. We choose $a, b \geq 0$ such that $4a + 6b = k$. This is always possible. Indeed, $k = 2m$ thus the condition $4a + 6b = k$ equals $2a + 3b = m$ and such a and b can always be found by coprimality of 2 and 3. Moreover from $k \geq 12$ we can assume $a, b \geq 0$. Then $E_4^a E_6^b$ is a modular form of weight k and $f - a_0(f) E_4^a E_6^b$ is a cusp form, namely

$$f - a_0(f) E_4^a E_6^b \in S_k(\mathbb{C}).$$

Moreover

$$\frac{f - a_0(f) E_4^a E_6^b}{\Delta}$$

is a modular form of weight $k - 12$. Using the inductive hypothesis we have

$$\begin{aligned} f &= \Delta \left(\sum_{4i+6j=k-12} c_{i,j} E_4^i E_6^j \right) + a_0(f) E_4^a E_6^b \\ &= \frac{E_4^3 - E_6^2}{12^3} \left(\sum_{4i+6j=k-12} c_{i,j} E_4^i E_6^j \right) + a_0(f) E_4^a E_6^b \end{aligned}$$

and we conclude that f can be written as an isobaric polynomial of degree k in E_4 and E_6. To conclude that we get the whole graded ring of polynomials it suffices to check that

E_4 and E_6 are algebraically independent. It is clear from the homogeneity property that a non trivial relation among elements of distinct weight cannot exists. Hence if E_4 and E_6 verify an algebraic relation, the monomials occurring in it must have the same weight. In such a relation, if a power of E_4 occurs we have

$$E_4^m + E_6 P(E_4, E_6) = 0.$$

But $E_6(i) = 0$ and $E_4(i) \neq 0$ so this cannot happen. Similarly pure powers of E_6 cannot occur. Hence E_4 divides each monomial and cancelling E_4 we obtain a relation of lower degree, so we conclude by induction. $\square$

1.2 Modular forms of arbitrary level

Definition 1.5. *Let $N \geq 1$ be an integer. The principal subgroup of level N is the kernel of the natural map of reduction $SL_2(\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$, namely:*

$$\Gamma(N) := \left\{ \gamma \in SL_2(\mathbb{Z}),\ \gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Definition 1.6. *A subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$ is called a congruence subgroup if there exists an $N > 1$ such that $\Gamma(N) \subseteq \Gamma$.*

The congruence subgroups we're mainly interested into are $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$ where

$$\Gamma_0(N) := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ c = 0 \mod N \right\}$$

and

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

Definition 1.7. *An holomorphic function $f : \mathbb{H} \longrightarrow \mathbb{C}$ is a weakly modular form of weight k and level Γ if*

$$f(\gamma z) = (cz + d)^k f(z)$$

for all $z \in \mathbb{H}$, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Let $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. Then $SL_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q})$ transitively. Indeed by definition

$$\gamma\infty = \lim_{z \to \infty} \frac{az + b}{cz + d} = \frac{a}{c}$$

for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. If we let $\frac{a}{c} \in \mathbb{Q}$ with a and c coprime then there exist $b, -d \in \mathbb{Z}$ such that $ad - bc = 1$. Hence

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $SL_2(\mathbb{Z})$ and $\gamma\infty = \frac{a}{c}$. As a consequence, given $\frac{a}{c}$ and $\frac{a'}{c'}$ in $\mathbb{Q}$, if we choose $\gamma, \gamma' \in SL_2(\mathbb{Z})$ such that $\gamma\infty = \frac{a}{b}$ and $\gamma'\infty = \frac{a'}{b'}$ then

$$(\gamma' \circ \gamma^{-1}) \left(\frac{a}{c}\right) = \frac{a'}{c'}.$$

Moreover the stabilizer of the action of the modular group at ∞ is given by

$$\mathrm{Stab}_{SL_2(\mathbb{Z})}(\infty) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}, \ b \in \mathbb{Z} \right\}.$$

Definition 1.8. *The set of cusps of* Γ *is given by* $\mathrm{Cusps}(\Gamma) := \Gamma\backslash\mathbb{P}^1(\mathbb{Q})$.

Let $\mathfrak{c} = [t]$ be a cusp and let $\mathrm{Stab}_\Gamma(t)$ be the stabilizer of $t \in \mathbb{Q}$ through the action of Γ. If we also have $\mathfrak{c} = [t']$, i.e. $t' = \gamma t$ for some $\gamma \in \Gamma$, then $\mathrm{Stab}_\Gamma(t') = \gamma \mathrm{Stab}_\Gamma(t)\gamma^{-1}$. Moreover if $t = \gamma_t\infty$ for some $\gamma_t \in SL_2(\mathbb{Z})$ we have $\mathrm{Stab}_\Gamma(t) = \Gamma \cap \gamma_t \mathrm{Stab}_{SL_2(\mathbb{Z})}(\infty)\gamma_t^{-1}$. Hence it makes sense to define

$$H_\mathfrak{c} := \mathrm{Stab}_{SL_2(\mathbb{Z})}(\infty) \cap \gamma_t^{-1}\Gamma\gamma_t.$$

Remark 1.4. *Let* $\mathfrak{c} = [t]$ *be a cusp, then* $H_\mathfrak{c}$ *is either the cyclic subgroup generated by* $\begin{pmatrix} 1 & h_\mathfrak{c} \\ 0 & 1 \end{pmatrix}$*, or the one generated by* $\begin{pmatrix} -1 & h_\mathfrak{c} \\ 0 & -1 \end{pmatrix}$*, in which case we say that the cusp is irregular, or the subgroup* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ *generated by* $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ *and* $\begin{pmatrix} 1 & h_\mathfrak{c} \\ 0 & 1 \end{pmatrix}$*. Moreover* $h_\mathfrak{c}$ *is the index of* $H_\mathfrak{c}$ *in* $\mathrm{Stab}_{SL_2(\mathbb{Z})}(\infty)$.

Definition 1.9. *Let* $\mathfrak{c} \in \mathrm{Cusps}(\Gamma)$*, we call* $h_\mathfrak{c}$ *the width of the cusp.*

We give the following proposition.

Proposition 1.1. *Let* Γ *be a congruence subgroup of* $SL_2(\mathbb{Z})$ *and* $\overline{\Gamma}$ *its image in* $PSL_2(\mathbb{Z})$*. Then*

$$\sum_{\mathfrak{c} \in \mathrm{Cusps}(\Gamma)} h_\mathfrak{c} = [PSL_2(\mathbb{Z}) : \overline{\Gamma}] = [SL_2(\mathbb{Z}) : \{\pm\Gamma\}]$$

Moreover if $\overline{\Gamma} \triangleleft PSL_2(\mathbb{Z})$ *then* $h_\mathfrak{c} = h_{\mathfrak{c}'}$ *for all* $h_\mathfrak{c}, h_{\mathfrak{c}'} \in \mathrm{Cusps}(\Gamma)$.

Proof. The proof of this proposition is a consequence of the following lemma:

Lemma 1.1. *Let* G *be a group acting transitively on a set* X *and* $H \leq G$ *a subgroup of finite index. Let* R *be a set of representatives for* $H\backslash X$*, then*

$$\sum_{x \in R} [\mathrm{Stab}_G(x) : \mathrm{Stab}_H(x)] = [G : H].$$

Proof. We start noticing that we have an injection

$$\mathrm{Stab}_H(x)\backslash\mathrm{Stab}_G(x) \hookrightarrow H\backslash G$$

with image $H\backslash \mathrm{Stab}_G(x)H$. Moreover, fixed x_0 in X, we have a surjective map

$$\begin{aligned} H\backslash G &\twoheadrightarrow H\backslash X \\ Hg &\longrightarrow Hgx_0 \end{aligned}$$

whose fibers have cardinality $[\mathrm{Stab}_G(x) : \mathrm{Stab}_H(x)]$. Indeed since G acts transitively on X, for any $x \in X$ we can find $g_x \in G$ such that $g_x x_0 = x$ and this gives surjectivity. Furthermore, denoting by T_{Hx} the fiber of Hx in $H\backslash X$ we have

$$\begin{aligned} T_{Hx} &= \{Hg \in H\backslash G \ : \ Hgx_0 = Hx\} \\ &= \{Hg' \in H\backslash G \ : \ Hg'g_x x_0 = Hx\} \\ &= \{Hg' \in H\backslash G \ : \ Hg'x = Hx\} \\ &= H\backslash H\mathrm{Stab}_G(x) = \mathrm{Stab}_H(x)\backslash \mathrm{Stab}_G(x) \end{aligned}$$

To conclude, taking a set of representatives R we have

$$[G:H] = \sum_{x\in R} |T_{Hx}| = \sum_{x \in R} [\mathrm{Stab}_G(x) : \mathrm{Stab}_H(x)].$$

□

We apply the lemma with $X = \mathbb{P}^1(\mathbb{Q})$, $G = PSL_2(\mathbb{Z})$ and $H = \overline{\Gamma}$. The last statement is straight forward from the definition of $H_{\mathfrak{c}}$. □

Remark 1.5. *If $\Gamma = \Gamma(N)$, for any cusp $\mathfrak{c}$ we have $h_{\mathfrak{c}} = N$ and applying proposition 1.1. we obtain that*

$$N|\mathrm{Cusps}(\Gamma(N))| = [PSL_2(\mathbb{Z}) : \overline{\Gamma(N)}] = \frac{1}{2}|SL_2(\mathbb{Z}/N\mathbb{Z})|$$

hence

$$|\mathrm{Cusps}(\Gamma(N))| = \frac{N^2}{2}\prod_{p|N}\left(1 - \frac{1}{p^2}\right).$$

Now let f be weakly modular of weight k and level Γ. Let $\mathfrak{c} = [t]$ be a cusp and let $t = \gamma_t\infty$. Then $f_{\mathfrak{c}} = f_{|k,\gamma_t}$ is invariant under the weight k action of $H_{\mathfrak{c}}$. Hence if we let

$$\mathfrak{h}_{\mathfrak{c}} = \begin{cases} h_{\mathfrak{c}} \text{ if } \mathfrak{c} \text{ is regular,} \\ 2h_{\mathfrak{c}} \text{ if } \mathfrak{c} \text{ is irregular,} \end{cases}$$

the group $H_{\mathfrak{c}}$ contains $\begin{pmatrix} 1 & \mathfrak{h}_{\mathfrak{c}} \\ 0 & 1 \end{pmatrix}$ thus $f_{\mathfrak{c}}$ is periodic of period $\mathfrak{h}_{\mathfrak{c}}$. As before we consider the function on the punctured disk $\tilde{f}_{\mathfrak{c}}(q_{\mathfrak{c}})$ obtained after the change of variable

$$q_{\mathfrak{c}} = e^{\frac{2\pi i z}{\mathfrak{h}_{\mathfrak{c}}}}.$$

If $\tilde{f}_{\mathfrak{c}}$ admits a meromorphic extension at zero we say that the function f is meromorphic at the cusp $\mathfrak{c}$ and in this case $\tilde{f}_{\mathfrak{c}}$ admits a Laurent expansion

$$\tilde{f}_{\mathfrak{c}} = \sum_{n\in\mathbb{Z}} a_{\mathfrak{c},n} q_{\mathfrak{c}}^n.$$

If $\tilde{f}_{\mathfrak{c}}$ is holomorphic (respectively vanishes) at zero we say that f is holomorphic (respectively vanishes) at $\mathfrak{c}$.

Definition 1.10. *A modular form of weight k and level Γ is a holomorphic function $f : \mathbb{H} \longrightarrow \mathbb{C}$ such that f is weakly modular of weight k and level Γ and holomorphic at all cusps of Γ. Moreover we say that f is a cusp form if f vanishes at all cusps.*

Chapter 2

Algebraic structure of modular forms modulo *p* of level *1*

In this chapter we will give an algebraic representation of modular forms modulo p of level 1 following [17]. The reader may acknowledge that such a description is effective but *naive* and requires nothing more than the classical tools we developed in Chapter 1.

2.1 Preliminaries

Following Ramanujan's notaion we set

$$P := E_2 = 1 - 12\sum_{n\geq 1}\sigma_1(n)q^n,$$
$$Q := E_4 = 1 + 240\sum_{n\geq 1}\sigma_3(n)q^n,$$
$$R := E_6 = 1 - 504\sum_{n\geq 1}\sigma_5(n)q^n.$$

We moreover introduce the operator

$$\theta := q\frac{d}{dq} = \frac{1}{2\pi i}\frac{d}{dz}.$$

Proposition 2.1. *Let f be a modular form of weight k, then $\partial f := 12\theta f - kPf$ is a modular form of weight $k+2$.*

Proof. Assume $f \in M_k(\mathbb{C})$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. We want to prove that

$$\partial f(\gamma z) = (cz+d)^{k+2}\partial f(z) \quad \text{i.e.} \quad \partial f_{|_{(k+2)},\gamma}(z) = \partial f(z).$$

We recall that the modular group is generated by the transformations

$$S : z \longrightarrow -1/z$$
$$T : z \longrightarrow z+1$$

and the action above respects composition, namely

$$g_{|k,\gamma|k,\gamma'} = g_{|k,\gamma\gamma'}.$$

So it suffices to prove invariance under the weight $k+2$ action of T and S. Clearly

$$\partial f(z+1) = 12\theta f(z+1) - kP(z+1)f(z+1) = \partial f(z)$$

since $\theta f(z+1) = \frac{1}{2\pi i}\frac{d}{dz}f(z+1)$ and $f(z+1) = f(z)$. From (1.1) we have

$$P(-1/z) = z^2 P(z) + \frac{12}{2\pi i}z.$$

Moreover

$$\frac{d}{dz}f(-1/z) = \left(\frac{d}{dz}f(-1/z)\right)\frac{1}{z^2}.$$

And $f(-1/z) = z^k f(z)$ yields

$$\frac{d}{dz}f(-1/z) = kz^{k-1}f(z) + \frac{d}{dz}f(z)z^k.$$

Hence

$$\theta f(-1/z) = \frac{1}{2\pi i}z^2\left(kz^{k-1}f(z) + \frac{d}{dz}f(z)z^k\right).$$

Then

$$\begin{aligned}
\partial f(-1/z) &= 12\theta f(-1/z) - kP(-1/z)f(-1/z) \\
&= \frac{12}{2\pi i}z^2\left(kz^{k-1}f(z) + \frac{d}{dz}f(z)z^k\right) - k\left(z^2P(z) + \frac{12}{2\pi i}z\right)f(z)z^k \\
&= z^{k+2}\left(\theta f(z) + \frac{12kf(z)}{2\pi iz} - kf(z)P(z) - \frac{12kf(z)}{2\pi iz}\right) \\
&= z^{k+2}(\theta f - kPf)(z).
\end{aligned}$$

□

Similarly one can prove that

$$12\theta P - P^2 = -Q.$$

As a consequence

Proposition 2.2. *We have*

$$\begin{aligned}
\partial Q &= -4R, \\
\partial R &= -6Q^2.
\end{aligned}$$

Proof. By Proposition 2.1. we have that $\partial Q \in M_6(\mathbb{C})$ and the latter is a $\mathbb{C}$-vector space of dimension 1. So there exist $\lambda \in \mathbb{C}$ such that $\partial Q = \lambda R$ and

$$\begin{aligned}\partial Q &= 12\theta Q - 4PQ \\ &= 12q\frac{d}{dq}\left(1 + 240\sum_{n\geq 1}\sigma_3(n)q^n\right) - 4\left(1 - 12\sum_{n\geq 1}\sigma_1(n)q^n\right)\left(1 + 240\sum_{n\geq 1}\sigma_3(n)q^n\right) \\ &= -4 + 2016q + ... = \lambda(1 - 504q + ...)\end{aligned}$$

yields $\lambda = -4$. Similarly $\partial R \in M_4(\mathbb{C})$ and the latter is a one dimensional vector space over $\mathbb{C}$ generated by Q^2, namely $\partial R = \lambda Q^2$. Then

$$\begin{aligned}\partial R &= 12\theta R - 4PR \\ &= 12q\frac{d}{dq}\left(1 - 504\sum_{n\geq 1}\sigma_5(n)q^n\right) - 6\left(1 - 12\sum_{n\geq 1}\sigma_1(n)q^n\right)\left(1 - 504\sum_{n\geq 1}\sigma_5(n)q^n\right) \\ &= -6 - 2880q + ... = \lambda(1 + 240q + ...)^2\end{aligned}$$

which yields $\lambda = -6$. □

2.2 Modular forms modulo p

From now on we assume $p \geq 5$. Let

$$\mathcal{O} = \mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q} = \{a/b \in \mathbb{Q} \ : \ p \nmid b\}.$$

We denote by $M_k(\mathcal{O})$ the $\mathcal{O}$-module of modular forms of weight k whose Fourier expansions have coefficients in $\mathcal{O}$, namely

$$M_k(\mathcal{O}) = \left\{ f \in M_k(\mathbb{C}) \ : \ f = \sum_n a_n q^n, \ a_n \in \mathcal{O} \right\}$$

and set $M(\mathcal{O}) = \bigoplus_{k\geq 0} M_k(\mathcal{O})$. We notice that $Q, R \in M(\mathcal{O})$ and in this way we have a diagram:

$$\begin{tikzcd} M(\mathbb{C}) \arrow[r, equal] & \mathbb{C}[Q,R] \\ M(\mathcal{O}) \arrow[u, hook] & \mathcal{O}[Q,R]. \arrow[l, hook'] \arrow[u, hook] \end{tikzcd}$$

Proposition 2.3. *We have that $M(\mathcal{O}) = \mathcal{O}[Q,R]$.*

Proof. Let $f \in M(\mathcal{O})$, i.e. $f \in M_k(\mathbb{C})$ such that $f = \sum_n a_n q^n$ with $a_n \in \mathcal{O}$. Let $\phi(Q,R) \in \mathbb{C}[Q,R]$ such that $\phi(Q,R) = f$. In the same style of Theorem 1.2. we prove that $\phi(Q,R) \in \mathcal{O}[Q,R]$ by induction on k. If $k \leq 12$, the vector space $M_k(\mathbb{C})$ has dimension 1. Indeed if $k = 4$, Q is a basis and $f = \lambda Q$ for some $\lambda \in \mathbb{C}$. Hence f has Fourier coefficients in $\mathcal{O}$ if and only if λQ has Fourier coefficients in $\mathcal{O}$, if and only if $\lambda \in \mathcal{O}$, i.e. $\phi(Q,R) = \lambda Q \in \mathcal{O}[Q,R]$. Similarly for $k = 6, 8, 10$ we have $f = \lambda R$,

$f = \lambda Q^2$, $f = \lambda QR$ respectively and we must have $\lambda \in \mathcal{O}$. Assume that $k \geq 12$ and $f = \sum_n a_n q^n \in M_k(\mathcal{O})$. Then $f - a_0 Q^i R^j$ with $4i + 6j = k$ is a cusp form. Since $a_0 \in \mathcal{O}$ we have $f - a_0 Q^i R^j \in S_k(\mathcal{O})$. We recall that we have an isomorpshism

$$\begin{aligned} M_k(\mathbb{C}) &\longrightarrow S_{k+12}(\mathbb{C}) \\ f &\longrightarrow \Delta f \end{aligned}$$

induced by Δ. Notice that $\Delta = \frac{Q^3 - R^2}{12^3} \in \mathcal{O}[Q, R]$. Hence $\frac{f - a_0 Q^i R^j}{\Delta} \in M_{k-12}(\mathcal{O})$. But then by the inductive hypothesis $\frac{f - a_0 Q^i R^j}{\Delta} = \psi(Q, R) \in \mathcal{O}[Q, R]$ which implies

$$f = \left(\psi(Q, R) + a_0 Q^i R^j\right) \Delta$$

and the latter belongs to $\mathcal{O}[Q, R]$. $\square$

We now define modular forms modulo p as follows.

Definition 2.1. *Let $\widetilde{M_k} \subseteq \mathbb{F}_p[\![q]\!]$ be the $\mathbb{F}_p$-vector space obtained by reducing modulo p the coefficients of the modular forms in $M(\mathcal{O})$, namely*

$$\widetilde{M_k} := \{\widetilde{f} = \sum_n \widetilde{a_n} q^n, \ f \in M_k(\mathcal{O})\}.$$

We define the $\mathbb{F}_p$-algebra of modular forms modulo p to be

$$\widetilde{M} = \sum_{k \geq 0} \widetilde{M}_k.$$

We want to characterize the algebraic structure of $\widetilde{M}$. We have a diagram

$$\begin{tikzcd} M(\mathcal{O}) \arrow[r, equal] \arrow[d, two heads] & \mathcal{O}[Q, R] \arrow[d, two heads] \\ \widetilde{M} & \mathbb{F}_p[Q, R]. \arrow[l, two heads, "\psi"'] \end{tikzcd}$$

Where the maps are induced by the reduction modulo p. The map ψ is clearly surjective but it may not be injective: two modular forms in $\mathcal{O}[Q, R]$ may have the same q expansion modulo p. Our aim is then to determine $\ker \psi$.
To proceed with our argument we introduce the following notation. Let $f \in M(\mathcal{O})$ be a modular form such that (in terms of polynomials in Q and R) $f = \phi(Q, R) \in \mathcal{O}[Q.R]$. We denote by $\widetilde{f}$ the function obtained by reducing modulo p its Fourier coefficients. Moreover we denote by $\widetilde{\phi}(Q, R) \in \mathbb{F}_p[Q, R]$ the corresponding isobaric polynomial modulo p. Then

$$\widetilde{f} = \psi(\widetilde{\phi}(Q, R)) =: \widetilde{\phi}(\widetilde{Q}, \widetilde{R}).$$

We state the following results about congruences between the Bernoulli numbers.

Theorem 2.1 (Von Staudt-Clausen)**.** *Let p be a prime. For all $n > 0$, we have*

$$pB_{2n} = \begin{cases} 0 \mod p & \text{if } (p-1) \nmid 2n, \\ -1 \mod p & \text{if } (p-1) | \ 2n. \end{cases}$$

Corollary 2.1 (Kummer's congruence)**.** *Suppose $k \geq 1$ and $(p-1)$ does not divide $2k$. The class of $\frac{B_{2k}}{2k}$ modulo p only depends on $2k \mod (p-1)$, i.e. if*

$$2k = 2k' \mod (p-1)$$

then

$$\frac{B_{2k}}{2k} = \frac{B_{2k'}}{2k'} \mod p.$$

Proof. For a proof of these classical results see [12] Chapter 10, sections 1 and 2. □

Let us now consider the polynomials $A, B \in \mathbb{C}[Q,R]$ such that $A(Q,R) = E_{p-1}$ and $B(Q,R) = E_{p+1}$. Then $A, B \in \mathcal{O}[Q,R]$. Indeed

$$E_{p-1} = 1 - \frac{2(p-1)}{B_{p-1}} \sum_{n\geq 1} \sigma_{p-2}(n) q^n \qquad E_{p+1} = 1 + \frac{2(p+1)}{B_{p+1}} \sum_{n\geq 1} \sigma_p(n) q^n$$

From Corollary 2.1. we have that

$$\frac{p+1}{B_{p+1}} = \frac{2}{B_2}$$

so $\frac{2(p+1)}{B_{p+1}} \in \mathcal{O}$. This shows that $E_{p+1} \in M(\mathcal{O})$ and $B(Q,R) \in \mathcal{O}[Q,R]$. Similarly $pB_{p-1} = -1 \mod p$ yields $\mathrm{ord}_p(B_{p-1}) = -1$ and

$$\mathrm{ord}_p\left(\frac{p-1}{B_{p-1}}\right) = 1.$$

Then $\frac{2(p-1)}{B_{p-1}} \in \mathcal{O}$ and $A(Q,R) \in \mathcal{O}[Q,R]$.

Remark 2.1. *The observation above yields in particular that*

$$\widetilde{E}_{p-1} = \widetilde{A}(\widetilde{Q}, \widetilde{R}) = 1.$$

As a consequence $(\widetilde{A} - 1) \subseteq \ker \psi$. This is enough to describe $\widetilde{M}$, indeed the following theorem holds:

Theorem 2.2.

$$\widetilde{M} \cong \mathbb{F}_p[Q,R]/(\widetilde{A} - 1).$$

In order to prove it we need a lemma.

Lemma 2.1. *i) $\widetilde{A}(\widetilde{Q}, \widetilde{R}) = 1$ and $\widetilde{B}(\widetilde{Q}, \widetilde{R}) = \widetilde{P}$.*

ii) $\partial \widetilde{A}(Q,R) = \widetilde{B}(Q,R)$ and $\partial \widetilde{B}(Q,R) = QA(Q,R)$.

iii) $\widetilde{A}(Q,R)$ has no repeated factor and $\widetilde{A}$ and $\widetilde{B}$ are coprime.

Proof. i) From the observation above $\widetilde{A}(\widetilde{Q},\widetilde{R}) = \widetilde{E}_{p-1} = 1$. Moreover by Kummer's congruence

$$\frac{B_{p+1}}{2(p+1)} = \frac{B_2}{4} = -\frac{1}{12} \mod p$$

and the fact that $a^p = a \mod p$ yields $\sigma_p(n) = \sigma_1(n)$ for all $n \geq 1$. We conclude that

$$\widetilde{E}_{p+1} = \left(1 - 12\sum_{n\geq 1}\sigma(n)q^n\right) \mod p = \widetilde{P}.$$

ii) We have $\theta\widetilde{A}(\widetilde{Q},\widetilde{R}) = 0$ then $\partial\widetilde{A}(\widetilde{Q},\widetilde{R}) = \widetilde{P}\widetilde{A}(\widetilde{Q},\widetilde{R}) = \widetilde{B}(\widetilde{Q},\widetilde{R})$ i.e.

$$\partial\widetilde{A}(\widetilde{Q},\widetilde{R}) - \widetilde{B}(\widetilde{Q},\widetilde{R}) = 0$$

in $\widetilde{M}_{p+1}$. Then $\partial A(Q,R) - B(Q,R) \in M_{p+1}(\mathcal{O})$ and all its coefficients are congruent to zero modulo p. So we must have $\partial A(Q,R) - B(Q,R) \in p\mathcal{O}[Q,R]$ and thus $\partial\widetilde{A} - \widetilde{B} = 0$ in $\mathbb{F}_p[Q,R]$. Similarly

$$\partial\widetilde{B}(\widetilde{Q},\widetilde{R}) = \partial\widetilde{P} = 12\theta\widetilde{P} - \widetilde{P}^2 = \widetilde{Q} = \widetilde{Q}\widetilde{A}(\widetilde{Q},\widetilde{R})$$

that yields $\partial\widetilde{B}(\widetilde{Q},\widetilde{R}) - \widetilde{Q}\widetilde{A}(\widetilde{Q},\widetilde{R}) = 0$ in $\widetilde{M}$. The modular form $\partial B(Q,R) - A(Q,R)$ has all its Fourier coefficients divisible by p, namely $\partial B(Q,R) - A(Q,R) \in p\mathcal{O}[Q,R]$ so $\partial\widetilde{B}(Q,R) - \widetilde{A}(Q,R) = 0$ in $\mathbb{F}_p[Q,R]$.

iii) The irreducible elements of $\overline{\mathbb{F}_p}[Q,R]$ are of the form Q, R and $Q^3 - \alpha R^2$. Assume that $Q^3 - \alpha R^2$ is an irreducible factor of $\widetilde{A}(Q,R)$, namely

$$(Q^3 - \alpha R^2)^n | \widetilde{A}(Q,R)$$

for some $\alpha \in \overline{\mathbb{F}_p}$. Assume that $n > 1$. We must have $\alpha \neq 1$ since $Q^3 - R^2$ has zero constant factor in the Fourier expansion but $A(Q,R) = E_{p-1}$ has not. Then

$$\partial(Q^3 - \alpha R^2) = 3Q^2(-4R) - 2\alpha R(-6Q^2) = -12Q^2R(1-\alpha) \neq 0.$$

We now assume that n is the exact power of $(Q^3 - \alpha R^2)$ dividing $\widetilde{A}(Q,R)$. Then $\partial\widetilde{A}(Q,R) = \widetilde{B}(Q,R)$ is divided exactly by $(Q^3 - \alpha R^2)^{n-1}$ since $(Q^3 - \alpha R^2)$ and $\partial(Q^3 - \alpha R^2)$ are coprime. But then $\partial\widetilde{B}(Q,R) = Q\widetilde{A}(Q,R)$ is divided exactly by $(Q^3 - \alpha R^2)^{n-2}$ i.e. $(Q^3 - \alpha R^2)^{n-2}$ divides exactly $\widetilde{A}(Q,R)$ and this is a contradiction. Similarly if $\widetilde{A}(Q,R)$ is divisible by Q^n, we have $\partial Q = -4R$ and it is coprime with Q. Then $\partial\widetilde{A} = \widetilde{B}$ is divided exactly by Q^{n-1} and $\partial\widetilde{B} = Q\widetilde{A}$ is divided exactly by Q^{n-2} and this is again a contradiction. The case with R^n uses the same argument. We conclude that $\widetilde{A}$ has no repeated factors. In particular all its factors appear with multiplicity $n = 1$ so that they appear with multiplicity $n = 0$ in $\partial\widetilde{A} = \widetilde{B}$.

□

Now we can prove the theorem.

Proof. Let $\mathfrak{a}$ be the kernel of ψ. Point i) of the lemma above shows that $(\widetilde{A}-1) \subseteq \mathfrak{a}$. We notice that $\mathfrak{a}$ must be prime since $\widetilde{M} \subseteq \mathbb{F}_p[\![q]\!]$ is an integral domain. Moreover we cannot have that $\mathfrak{a}$ is maximal. We would have otherwise that $\mathbb{F}_p[Q,R]/\mathfrak{a}$ is a field and a finitely generated $\mathbb{F}_p$-algebra. By Hilbert's Nullstellensatz the extension $\mathbb{F}_p \subseteq \mathbb{F}_p[Q,R]/\mathfrak{a}$ would be finite and $\widetilde{Q}$ and $\widetilde{R}$ algebraic over $\mathbb{F}_p$ hence constant. But we notice that $Q = 1 + 240\sum_{n\geq 1}\sigma_3(n)q^n$ and $R = 1 - 504\sum_{n\geq 1}\sigma_5(n)q^n$ so if $p \neq 2,3$ at least one of them has coefficient of q non zero modulo p. To conclude it is then enough to prove that $(\widetilde{A}-1)$ is prime or, equivalently, irreducible. Indeed we recall that $\mathbb{F}_p[Q,R]$ has Krull dimension equal to 2 and the fact that $\mathfrak{a}$ is not maximal implies the existence of $\mathfrak{m} \subseteq \mathbb{F}_p[Q,R]$ maximal such that $\mathfrak{a} \subset \mathfrak{m}$. Assuming $(\widetilde{A}-1)$ irreducible we have a inclusion of prime ideals

$$0 \subset (\widetilde{A}-1) \subseteq \mathfrak{a} \subset \mathfrak{m} \subset \mathbb{F}_p[Q,R]$$

which yields $(\widetilde{A}-1) = \mathfrak{a}$.
To prove then that $(\widetilde{A}-1)$ is irreducible we let $\widetilde{\phi}(Q,R) \in \mathbb{F}_p[Q,R]$ be an irreducible proper factor of $\widetilde{A}-1$ in $\mathbb{F}_p[Q,R]$. Then we can write

$$\widetilde{\phi}(Q,R) = 1 + \widetilde{\phi}_1(Q,R) + ... + \widetilde{\phi}_n(Q,R)$$

where each of the $\widetilde{\phi}_i(Q,R)$ is isobaric of degree i and $n < p-1$. Let ζ be a primitive $(p-1)$-th root of unity. We notice that $\widetilde{A}(\zeta^4 Q, \zeta^6 R) = \widetilde{A}(Q,R)$ since $\widetilde{A}$ is homogeneous of degree $p-1$. Then $\widetilde{\phi}(\zeta^4 Q, \zeta^6 R)$ is also a divisor of $\widetilde{A}(Q,R)-1$ and it is different from $\widetilde{\phi}(Q,R)$, hence coprime with it. So $\widetilde{\phi}(Q,R)\widetilde{\phi}(\zeta^4 Q,\zeta^6 R)$ divides $\widetilde{A}(Q,R)-1$. Then considering the isobaric terms of highest degree we must have that $\widetilde{\phi}_n(Q,R)\widetilde{\phi}_n(\zeta^4 Q,\zeta^6 R) = \zeta^n\widetilde{\phi}_n(Q,R)^2$ divides $\widetilde{A}(Q,R)$ but this contradicts Lemma 2.1 □

Remark 2.2. *We recall that the multiplication by E_{p-1}*

$$f \longrightarrow fE_{p-1}$$

gives us a chain of maps among the subspaces

$$M_k(\mathbb{C}) \longrightarrow M_{k+p-1}(\mathbb{C}) \longrightarrow M_{k+2(p-1)}(\mathbb{C}) \cdots \longrightarrow M_{k+n(p-1)}(\mathbb{C}) \cdots .$$

Since $\widetilde{f}\widetilde{A}(\widetilde{Q},\widetilde{R}) = \widetilde{f}$ the corresponding maps on $\widetilde{M}_k$ are injective. Hence we have an induced filtration

$$\widetilde{M}_k \subseteq \widetilde{M}_{k+p-1} \subseteq \widetilde{M}_{k+2(p-1)} \cdots \subseteq \widetilde{M}_{k+n(p-1)} \cdots .$$

We conclude that the structure of $M_k(\mathbb{C})$ of a graded algebra induces a grading on $\widetilde{M}$ with values in $\mathbb{Z}/(p-1)\mathbb{Z}$, namely:

$$\widetilde{M} = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} \sum_{k=\alpha \mod p} \widetilde{M}_k.$$

Remark 2.3. *We remark that $\widetilde{P}$ is by definition a modular form modulo p, namely $\widetilde{B}(\widetilde{Q},\widetilde{R}) = \widetilde{P}$.*

We now let $\widetilde{f}$ be a graded element in $\widetilde{M}$, i.e.

$$\widetilde{f} \in \sum_{k=\alpha \mod p} \widetilde{M}_k$$

for some $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$. By multiplying each summand by suitable powers of $\widetilde{A}(\widetilde{Q},\widetilde{R})$ we can assume that $\widetilde{f} \in \widetilde{M}_k$ for some k.

Definition 2.2. *We define $\omega(\widetilde{f}) = k$ to be the filtration of $\widetilde{f}$.*

In other words $\omega(\widetilde{f})$ is the smallest integer k such that there exists a $g \in M_k$ such that $\widetilde{g} = \widetilde{f}$.

Proposition 2.4. *i) Let $k \in \mathbb{Z}$ a positive integer and $f \in M_k(\mathcal{O})$ with $f = \phi(Q,R)$ for some $\phi(Q,R) \in \mathcal{O}[Q,R]$. Assume $\widetilde{f} \neq 0$. Then $\omega(\widetilde{f}) < k$ if and only if $\widetilde{A}(Q,R)$ divides $\widetilde{\phi}(Q,R)$.*

ii) Let $\widetilde{f}$ be a graded element, then $\omega(\theta\widetilde{f}) \leq \omega(\widetilde{f}) + p + 1$ and equality holds if and only if $\omega(\widetilde{f}) = 0 \mod p$.

Proof. i) One implication is clear. Assume that $\widetilde{A}(Q,R)$ divides $\widetilde{\phi}(Q,R)$, namely $\widetilde{\phi}(Q,R) = \widetilde{A}(Q,R)^n\widetilde{\psi}(Q,R)$, then

$$\widetilde{f} = \widetilde{\phi}(\widetilde{Q},\widetilde{R}) = \widetilde{A}(\widetilde{Q},\widetilde{R})^n\widetilde{\psi}(\widetilde{Q},\widetilde{R}) = \widetilde{\psi}(\widetilde{Q},\widetilde{R}) = \widetilde{g}$$

where $g = \psi(Q,R) \in \mathcal{O}[Q,R]$ is an isobaric polynomial of degree $k' = k - n(p-1)$, that is $\omega(f) = k'$. Conversely assume $\omega(f) = k' < k$ for some $k' = k \mod (p-1)$, i.e. $k = k' + n(p-1)$. Then $\widetilde{f} = \widetilde{g}$ for $g \in M_{k'}$. Let $g = \psi(Q,R)$ as an isobaric polynomial in Q and R, then

$$\widetilde{\phi}(\widetilde{Q},\widetilde{R}) = \widetilde{\psi}(\widetilde{Q},\widetilde{R}) = \widetilde{\psi}(\widetilde{Q},\widetilde{R})\widetilde{A}(\widetilde{Q},\widetilde{R})^n$$

in $\widetilde{M}_k$. Consider $\widetilde{\phi} - \widetilde{\psi}\widetilde{A}^n \in \mathbb{F}_p[Q,R]$. We have that $\phi(Q,R) - \psi(Q,R)A(Q,R)^n$ is in $M_k(\mathcal{O})$ and it's congruent to zero modulo p. So it must have all its coefficients in $p\mathcal{O}$. Hence $\widetilde{\phi}(Q,R) - \widetilde{\psi}(Q,R)\widetilde{A}(Q,R)^n = 0$ in $\mathbb{F}_p[Q,R]$ and this allows us to conclude.

ii) Assume that $\omega(\widetilde{f}) = k$, i.e. $\widetilde{f} \in \widetilde{M}_k$ and let $f = \phi(Q,R) \in M(\mathcal{O})$ be a modular form of weight k that lifts it. We can write $12\theta\widetilde{f} = \widetilde{A}(\widetilde{Q},\widetilde{R})\partial\widetilde{f} + k\widetilde{B}(\widetilde{Q},\widetilde{R})\widetilde{f}$ and it is in $\widetilde{M}_{k+p+1}$. Then we have $\omega(\theta f) \leq k + p + 1$ and strict inequality holds if and only if $\widetilde{A}$ divides $\widetilde{A}\partial\widetilde{\phi} + \bar{k}\widetilde{B}\widetilde{\phi}$ in $\mathbb{F}_p[Q,R]$ by the point above. But we recall that $\widetilde{A}$ and $\widetilde{B}$ are coprime and the assumption $\omega(\widetilde{f}) = k$ implies that $\widetilde{A}(Q,R)$ does not divide $\widetilde{\phi}(Q,R)$. Hence $\widetilde{A}$ divides $\widetilde{A}\partial\widetilde{\phi} + \bar{k}\widetilde{B}\widetilde{\phi}$ if and only if $\bar{k} = k \mod p = 0$.

□

We conclude stating the following result for modular forms in characteristic p.

Proposition 2.5. *Let $\widetilde{f},\widetilde{g} \in \widetilde{M}_k$. Then $\widetilde{f} = \widetilde{g}$ if and only if for each $n \leq \lfloor k/12 \rfloor$ the coefficients of q^n of $\widetilde{f}$ and $\widetilde{g}$ are equal.*

Proof. To prove the proposition we recall the following algorithm for the construction of a basis for S_k.

Lemma 2.2. *The space $S_k(\mathbb{C})$ has a basis $g_1, g_2, ..., g_d$ where $d = \dim_{\mathbb{C}}(S_k(\mathbb{C}))$ such that the g_j's lie in $\mathbb{Z}[\![q]\!]$ and $a_i(g_j) = 0$ for $i < j$ and $a_j(g_j) = 1$.*

Proof. We notice that if $a, b \geq 0$, the modular forms $g_j = \Delta^j R^{2(d-j)+a} Q^b$ for $j = 1, ..., d$ are in $\mathbb{Z}[\![q]\!]$ since Δ, R and Q lie in $\mathbb{Z}[\![q]\!]$. We recall that

$$d = \begin{cases} \lfloor k/12 \rfloor - 1 & \text{if } k = 2 \mod 12, \\ \lfloor k/12 \rfloor & \text{if } k \neq 2 \mod 12. \end{cases}$$

We notice that the g_j's are cusp forms and we can choose a, b such that $g_j \in S_k(\mathbb{C})$. Indeed, if $k = 0 \mod 12$, then $d = \lfloor k/12 \rfloor$ with $k = 12d$, then we set $a = b = 0$ and $g_j = \Delta^j R^{2(d-j)} \in S_k(\mathbb{C})$. Now let $k = c + n12$ with $0 < c < 12$. If $c = 2$ then $d = n-1$ and we choose $4a+6b = 14$ and for any j we have $12j+6(2(d-j))+6a+4b = 12n-12+14 = k$, i.e. $g_j \in S_k(\mathbb{C})$. Similarly for the remaining cases we have $d = n$ and we choose $a, b \geq 0$ such that $4a + 6b = c$ (namely $a = 1, b = 0$ if $c = 4$, $a = 0, b = 1$ if $c = 6$, $a = 2, b = 0$ if $c = 8$ and $a = 1 = b$ if $c = 10$) and obtain that $g_j \in S_k(\mathbb{C})$. Furthermore we clearly have $a_i(g_j) = 0$ for $i < j$ and $a_j(g_j) = 1$. This also proves thar they're linearly independent over $\mathbb{C}$ and thus form a basis for $S_k(\mathbb{C})$. $\square$

As a consequence if $f \in S_k(\mathbb{C})$, then we can write $f = \lambda_1 g_1 + ... + \lambda_d g_d$ with $\lambda_i \in \mathbb{C}$. Then $a_i(f) = \lambda_i$ for $i = 1, ..., d$ i.e. f can be written as linear combination of the g_i's and the coefficients are given by the first d Fourier coefficients of f.
We can now prove the proposition. Let $\widetilde{f}, \widetilde{g} \in \widetilde{M}_k$ and assume that the coefficients of q^n of the two coincide for each $n \leq \lfloor k/12 \rfloor$. Then the first $\lfloor k/12 \rfloor$ coefficients of $\widetilde{f} - \widetilde{g}$ are 0. We take lifts for $f, g \in M_k(\mathcal{O})$ and it's not restricting to assume $f - g \in S_k(\mathcal{O})$. Then $a_i(f-g) \in p\mathcal{O}$ for $i \leq \lfloor k/12 \rfloor$ and notice that $d = \dim_{\mathbb{C}}(S_k(\mathbb{C})) \leq \lfloor k/12 \rfloor$. From the lemma above we have $f - g = a_1(f-g)g_1 + ... + a_d(f-g)g_d$ and taking the reduction modulo p we conclude $\widetilde{f} - \widetilde{g} = 0$. $\square$

Chapter 3

Katz's modular forms

Our aim is to extend the definition of modular forms modulo p for arbitrary level N. The classical theory of modular forms is no longer enough and we're forced to approach geometric tools. From now on modular forms will either be *rules* which associate to a class of elliptic curves over a ring with an additional *level structure* an element of the base ring or equivalently sections of a line bundle over the *modular* curve.

3.1 Modular curves and some motivations

Why to bother about a universal curve?
We have a natural action of $\mathbb{Z}^2$ on $\mathbb{H} \times \mathbb{C}$ as follows:

$$\begin{aligned}(\mathbb{H} \times \mathbb{C}) \times \mathbb{Z}^2 &\longrightarrow \mathbb{H} \times \mathbb{C} \\ ((\tau, z), (n, m)) &\longrightarrow (\tau, (z + m\tau + n)).\end{aligned}$$

Let

$$\pi : (\mathbb{H} \times \mathbb{C})/\mathbb{Z}^2 \longrightarrow \mathbb{H}$$

be the natural projection. Then the fiber of a point $\tau \in \mathbb{H}$ is given by the class of pairs (τ, z) such that two pairs (τ, z) and (τ, z') are equal if and only if $z = z' \mod (\mathbb{Z} + \tau\mathbb{Z})$, Hence

$$\pi^{-1}(\tau) \cong \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}.$$

We denote $\Lambda_\tau := \mathbb{Z} + \tau\mathbb{Z}$. The complex torus $\mathbb{C}/\Lambda_\tau$ is complex analytically equivalent to an elliptic curve E_τ over $\mathbb{C}$ of equation[1]

$$Y^2 = X^3 - g_2(\tau)X + g_3(\tau)$$

where

$$\begin{aligned}12(2\pi i)^{-4} g_2(\tau) &= E_4(\tau) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n, \\ 216(2\pi i)^{-6} g_4(\tau) &= E_6(\tau) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n.\end{aligned}$$

[1] See [16] Chapter 6 for a complete argument.

Letting the modular group $SL_2(\mathbb{Z})$ act on $\widetilde{\mathbb{E}} := (\mathbb{H} \times \mathbb{C})/\mathbb{Z}^2$ through the classical action on $\mathbb{H}$ we obtain

$$\pi : SL_2(\mathbb{Z})\backslash\widetilde{\mathbb{E}} \longrightarrow SL_2(\mathbb{Z})\backslash\mathbb{H}.$$

Recalling that two elliptic curves E_τ and $E_{\tau'}$ are isomorphic if and only if $\tau' = \gamma\tau$ for some $\gamma \in SL_2(\mathbb{Z})$, we have that the fiber of a point $SL_2(\mathbb{Z})\tau$ corresponds to the isomorphism class of the corresponding elliptic curve E_τ. Hence the map above parametrizes elliptic curves over $\mathbb{C}$ up to isomorphism.
We can repeat the same argument with any subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$ of Chapter 1 and obtain

$$\pi : \Gamma\backslash\widetilde{\mathbb{E}} \longrightarrow \Gamma\backslash\mathbb{H}.$$

It turns out that π parametrizes elliptic curves with *additional structure*. In the case $\Gamma = \Gamma(N)$, we obtain classes of isomorphism of elliptic curves equipped with certain level N-structures. If E_τ is a complex elliptic curve we consider the subgroup of N-torsion points $E_\tau[N]$ given by

$$0 \longrightarrow \frac{1}{N}\Lambda_\tau/\Lambda_\tau \longrightarrow E_\tau \xrightarrow{[N]} E_\tau.$$

A level N structure is an isomorphism

$$\alpha_N : (\mathbb{Z}/N\mathbb{Z})^2 \longrightarrow E_\tau[N]$$

and corresponds to the choice of a basis $\alpha_N(1,0) = P$, $\alpha_N(0,1) = Q$ for $E_\tau[N]$. There is a pairing [2]

$$e_N : E_\tau[N] \times E_\tau[N] \longrightarrow \mu_N$$

which can be computed as follows. We fix a basis for $E_\tau[N]$, for istance $\omega_1 = \frac{1}{N} + \Gamma_\tau$ and $\omega_2 = \frac{\tau}{N} + \Gamma_\tau$ and we let $\gamma \in M_2(\mathbb{Z}/N\mathbb{Z})$ be such that $\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$. We have

$$e_N(P,Q) = e^{2\pi i \det\gamma/N}.$$

One can see that this does not depend on the choice of the basis and if P, Q are generators of $E_\tau[N]$ we have $\gamma \in GL_2(\mathbb{Z}/N\mathbb{Z})$ hence $e_N(P,Q)$ is a primitive root of unity.
We then consider classes of isomorphism of elliptic curves E_τ with level N structure determined by the N-torsion points P, Q of determinant $e_N(P,Q) = e^{2\pi i/N}$ i.e. pairs of the form $(E_\tau, (\frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda\tau))$ for $\tau \in \mathbb{H}$. One can easily check that two such classes $[(E_\tau, (\frac{1}{N} + \Lambda\tau, \frac{\tau}{N} + \Lambda\tau))]$ and $[(E_{\tau'}, (\frac{1}{N} + \Lambda\tau', \frac{\tau'}{N} + \Lambda\tau'))]$ are equal if and only if

$$\Gamma(N)\tau' = \Gamma(N)\tau.$$

The group $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ can be seen as an Hausdorff topological space with the classical quotient topology from $\mathbb{C}$. It can be equipped with complex charts and thus inherits the structure of a Riemann Surface [3]. We define

$$X(\Gamma) = \Gamma\backslash\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = Y(\Gamma) \cup \mathrm{Cusps}(\Gamma).$$

[2]See [16] Chapter III.8 for the characterization of the Weil Pairing on elliptic curves over arbitrary fields k and [10] Chapter 2.8 for a more general definition.

[3]See [3] Chapter 2.

It is an Hausdorff, connected and compact Riemann Surface and thus corresponds to an algebraic projective curve. Let

$$p : \mathbb{H} \longrightarrow Y(\Gamma) \hookrightarrow X(\Gamma)$$

be the natural map and let us denote by $\Omega^1_{X(\Gamma)}$ the sheaf of $\mathbb{C}$-linear (holomorphic) differentials on the modular curve $X(\Gamma)$. *We have a correspondence between modular forms of weight $2k$ and global sections of* ${\Omega^1_{X(\Gamma)}}^{\otimes k}$. In particular if we let

$$\omega \in H^0\left(X(\Gamma), {\Omega^1_{X(\Gamma)}}^{\otimes k}\right),$$

then the pull-back $p^*\omega$ defines a modular form of weight $2k$ and level Γ. Indeed let $x = \tau\Gamma = p(\tau) \in Y(\Gamma)$, then for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ we have $(p \circ \gamma)(\tau) = p(\tau)$. Hence $\gamma^* p^* \omega = p^*\omega$ must hold. If $p^*\omega = f(\tau)(d\tau)^k$ then:

$$\begin{aligned}
\gamma^* p^* \omega &= f(\gamma\tau)(d\gamma(\tau))^k \\
&= f(\gamma\tau)\left(\frac{1}{(cz+d)^2}\right)^k (d\tau)^k \\
&= p^*\omega = f(\tau)(d\tau)^k.
\end{aligned}$$

which yields $f(\gamma\tau) = (cz+d)^{2k} f(\tau)$, i.e. f is weakly modular of weight $2k$ and level Γ. Moreover the local charts around the cusps $\mathfrak{c} = [t] \in \Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ are disjoint open neighbourhoods which are homeomorphic to the unit disk through $z \longrightarrow q_{\mathfrak{c}}$. If $p^*\omega$ is locally $g(q_{\mathfrak{c}})d(q_{\mathfrak{c}})$, we can recover from $g(q_{\mathfrak{c}})$ the q-expansion of f at the cusp $\mathfrak{c}$ exactly how we defined it in Chapter 1.

Coversely, repeating the argument backwards, for any modular form $f : \mathbb{H} \longrightarrow \mathbb{C}$, the position

$$p^*\omega := f(\tau)(d\tau)^k$$

defines a global section of ${\Omega^1_{X(\Gamma)}}^{\otimes k}$. Then we can identify modular forms of level N and weight $2k$ with $H^0\left(X(\Gamma), {\Omega^1_{X(\Gamma)}}^{\otimes k}\right)$.

To conclude our argument, we fix $\Gamma = \Gamma(N)$ and we let $\mathbb{E} := \Gamma(N)\backslash\widetilde{\mathbb{E}}$, $Y(N) := Y(\Gamma(N))$. We consider

$$\begin{array}{c} \mathbb{E} \\ \downarrow{\scriptstyle \pi} \\ Y(N). \end{array}$$

The discussion above suggests us to *extend* our definition of an elliptic curve over a certain field k to a notion of elliptic curve over a scheme. It will be a morphism of schemes whose *fibers* are elliptic curves in the classical sense. Then $\mathbb{E}/Y(N)$ is going to be an elliptic curve and its fibers elliptic curves with level N structure. In a *naive* way modular forms of weight $2k$, not necessarily holomorphic at the cusps, are elements of

$$H^0\left(Y(N), {\Omega^1_{Y(N)}}^{\otimes k}\right)$$

and holomorphic modular forms of weight $2k$ are sections in $H^0\left(X(N), {\Omega^1_{X(N)}}^{\otimes k}\right)$. Finally let $\underline{\omega}_{\mathbb{E}/Y(N)} = \pi_* \Omega^1_{\mathbb{E}/Y(N)}$. The Kodaira-Spencer isomorphism (Appendix C.3) tells us that

$$ {\Omega^1_{Y(N)}}^{\otimes k} \cong \omega^{\otimes 2k}_{\mathbb{E}/Y(N)}. $$

All in all, it makes then sense to define modular forms of weight $2k$ and level N as

$$ H^0\left(Y(N), \underline{\omega}^{\otimes 2k}_{\mathbb{E}/Y(N)}\right). $$

Our aim is to generalize the argument above to a scheme $Y(N)$ over $\mathbb{Z}[1/N]$. To do so we will translate our problem in the formalism of moduli spaces.

3.2 Arithmetic moduli of elliptic curves: an overview

The results of the following section are in [10]. Many of them are presented without a proof. Indeed, the above mentioned topic constitutes an entire branch unto itself and going into details would make us stray from our purpose. We give the definition of an N-structure and state a representability theorem in the category Ell. At the end of it we will have the notion of a universal curve in the sense that any elliptic curve with level N structure can be seen as a pullback of it.

In this section we will denote by S a scheme and by E/S an elliptic curve over S as follows.

Definition 3.1. *An elliptic curve is a proper, smooth morphism of schemes together with a section which we denote O*

$$ \begin{tikzcd} E \arrow[d, shift right] \\ S \arrow[u, bend right] \end{tikzcd} $$

whose fibers are connected curves of genus one.

This means that for any $s \in S$, if we denote by $k(s) = \mathcal{O}_{S,s}/\mathfrak{m}_{S,s}$ the residue field at s and by E_s the curve obtained by pullback

$$ \begin{tikzcd} E_s \arrow[r] \arrow[d] & E \arrow[d, "p"] \\ \mathrm{Spec}(k(s)) \arrow[r] & S \end{tikzcd} $$

then $E_s/k(s)$ is an elliptic curve in the usual sense.

Remark 3.1. *The scheme E/S has a unique structure of a commutative group scheme. In [10] Theorem 2.1.2 Katz and Mazur give a detailed proof of this fact reducing to the well known case of an elliptic curve over a field k. Moreover, as in the case of elliptic curves over a field, one can define the map $[N]$ of multiplication by N over a group scheme (see [15] Remark 3.4).*

It is important to recall the following crucial fact about the N-torsion of an elliptic curve.

Theorem 3.1. *Let $N \geq 1$ be an integer. Let S be a scheme over $\mathbb{Z}[1/N]$, i.e. N is invertible in S. Let $E[N]$ be the kernel of the multiplication by N morphism:*

$$[N] : E \longrightarrow E.$$

Then $E[N]$ is a finite étale subgroup scheme over S which is locally on S isomorphic to the constant group scheme $(\mathbb{Z}/N\mathbb{Z})^2_S$.

Proof. A whole detailed proof can be found in [10] Chapter 2.3. We will sketch the main steps here, since they are an interesting reduction to the case of elliptic curves over an algebraically closed field. In the latter situation the statement above is a classical result, whose proof can be found in [16] Chapter III. Zariski locally on S, E is given by a smooth Weirstrass cubic in $\mathbb{P}^2_S$ with origin $(0, 0, 1)$ (see [10] section 2.2). So we may suppose that S is the open set in

$$\mathrm{Spec}(\mathbb{Z}[a_1, a_2, a_3, a_4, a_6])$$

over which the generalised Weirstrass cubic

$$X^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

is smooth. Then S is regular and E, being smooth over S, is regular. We check that $[N]$ is finite flat and fiber by fiber étale and this yields that $[N]$ is finite étale . Finite morphisms of regular schemes of the same dimension are automatically flat, so to prove that $[N]$ is finite and flat it suffices to prove that it is finite. Since E is proper over S, any S-morphism of E is proper so it is enough to check it has finite fibers and this can be checked geometric fiber by geometric fiber. We're reduced to show that $[N] : E \longrightarrow E$ is finite when E is an elliptic curve over an algebraically closed field k. But any morphism between proper smooth connected curves over k is either constant or finite. In particular the map induced by $[N]$ on differentials is multiplication by N so $[N]$ is non constant thus finite and étale. This shows that $[N]$ is finite étale over S. To conclude that $E[N]$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2_S$, since with our reduction S is normal and connected, it is enough to check it at a geometric point and it is again the case of an elliptic curve over an algebraically closed field. $\square$

Definition 3.2. *Let S be a scheme and E/S an elliptic curve. A (naive) $\Gamma(N)$-structure on E is a group schemes isomorphism*

$$\alpha : (\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z})_S \xrightarrow{\sim} E[N].$$

We now define the category of elliptic curves in the sense of Definition 3.1.

Definition 3.3 (The category Ell)**.** *The category of elliptic curves is given by the following data.*
Objects are elliptic curves over variable base schemes

$$\begin{array}{c} E \\ \big\downarrow{\scriptstyle p} \\ S. \end{array}$$

Morphisms are commutative squares of the form

$$\begin{tikzcd} E' \arrow[r] \arrow[d, "p'"] & E \arrow[d, "p"] \\ S' \arrow[r, "f"] & S \end{tikzcd}$$

where the induced morphism $E' \longrightarrow E \times_S S'$ is an isomorphism of elliptic curves.

If we consider only schemes over $\operatorname{Spec}(\mathbb{Z}[1/N])$ we will denote the corresponding subcategory by $\mathrm{Ell}_{\mathbb{Z}[1/N]}$.

Definition 3.4 (Moduli problem)**.** *A contravariant functor $\mathcal{P} : \mathrm{Ell} \longrightarrow \mathrm{Set}$ is a moduli problem for elliptic cuves. Given $E/S \in \mathrm{Ell}$ an element of $\mathcal{P}(E/S)$ is called a level $\mathcal{P}$ structure over S.*

The reader might guess that we're interested in the following moduli problem:

Definition 3.5. *For $N \geq 3$ the level N moduli problem is*

$$\begin{aligned} \Gamma(N) : \mathrm{Ell}_{\mathbb{Z}[1/N]} &\longrightarrow \mathrm{Set} \\ E/S &\longrightarrow \{\textit{level } N \textit{ structures } E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2_S\}. \end{aligned}$$

The moduli problem $\mathcal{P}$ is said to be representable if it is representable as a functor from Ell. This means that there exists an elliptic curve over a scheme

$$\begin{tikzcd} \mathbb{E} \arrow[d] \\ \mathcal{M}(\mathcal{P}) \end{tikzcd}$$

and a functorial isomorphism

$$\mathrm{Hom}_{\mathrm{Ell}}(E/S, \mathbb{E}/\mathcal{M}(\mathcal{P})) \cong \mathcal{P}(E/S).$$

Remark 3.2. *If the moduli problem $\mathcal{P}$ is representable, the scheme $\mathcal{M}(\mathcal{P})$ represents the functor on the category of schemes* Sch *which associate to a scheme S the set of isomorphism classes of pairs $(E/S, \alpha)$ with E an elliptic curve over S and $\alpha \in \mathcal{P}(E/S)$ a level $\mathcal{P}$-structure.*

We give now some definitions.

Definition 3.6 (Relative representabe moduli problem)**.** *The moduli problem $\mathcal{P}$ is said to be relatively representable over* Ell *if for every $E/S \in \mathrm{Ell}$ the functor*

$$\begin{aligned} \mathrm{Sch}/S &\longrightarrow \mathrm{Set} \\ T &\longrightarrow \mathcal{P}(E_T/T) \end{aligned}$$

is representable by a scheme $\mathcal{P}_{E/S}$.

Definition 3.7 (Rigid moduli problem). *A moduli problem $\mathcal{P}$ is called rigid if for any elliptic curve E/S and any level $\mathcal{P}$ structure $\alpha \in \mathcal{P}(E/S)$ on E/S the pair $(E/S, \alpha)$ has no non trivial automorphism.*

Definition 3.8. *Let P be a property of morphisms of schemes. A moduli problem $\mathcal{P}$ is said to be of type P over* Ell *if it is relatively representable and for any E/S the morphism of schemes*

$$\begin{array}{c} \mathcal{P}_{E/S} \\ \Big\downarrow \\ S \end{array}$$

has property P.

Remark 3.3. *The level N moduli problem is relatively representable and étale over* Ell *(see [10] Theorem 3.6.0). More generally Katz and Mazur show that if C/S is a smooth commutative group scheme of relative dimension* 1 *and A is a fixed finite abelian group, then the functor on* Sch/S *which sends any scheme T over S to* $\mathrm{Hom}_{gr}(A, C(T))$ *is representable by an S-scheme of finite presentatiom. It follows that the sub-functor that sends a scheme T over S to the set of A-structures on C_T/T is representable by a closed subscheme of such a scheme. For more details about this see [10] 1.6.*

It turns out that the level N moduli problem is also rigid.

Proposition 3.1 (Rigidity of level N structures). *Let $f : E \longrightarrow E$ be an automorphism of an elliptic curve E over a connected scheme S. Let $N \geq 3$ and $E[N]$ the kernel of the multiplication by N map. If f induces the identity on $E[N]$ then $f = 1$.*

Proof. We recall [4] that for any $f \in \mathrm{End}(E)$ we have its dual isogeny $\hat{f} \in \mathrm{End}(E)$. They satisfy

$$f \circ \hat{f} = \hat{f} \circ f = [\deg f].$$

The trace of f is defined as the integer $\mathrm{tr}(f) = f + \hat{f}$. We need an auxiliary lemma.

Lemma 3.1. *If $f : E \longrightarrow E$ is an S-morphism of an elliptic curve, then*

i) Inside the ring $\mathrm{End}(E)$, *f is a root of the $\mathbb{Z}$-polynomial:*

$$X^2 - \mathrm{tr}(f)X + \deg f.$$

ii) We have the inequality

$$\mathrm{tr}(f)^2 \leq 4 \deg f.$$

Proof. The first statement is clear from

$$f^2 - (f + \hat{f})f + \hat{f}f = 0.$$

The second holds if and only if

$$\mathrm{tr}(f)^2 - 4 \deg f \leq 0$$

[4]See [16] Chapter III.

if and only if the polynomial

$$X^2 - \mathrm{tr}(f)X + \deg f$$

takes only positive values for real values of X. This is equivalent to having

$$n^2 - \mathrm{tr}(f)n + \deg f \geq 0$$

for $n \in \mathbb{Z} \subseteq \mathrm{End}(E)$ that is $\deg(n - f) \geq 0$ which allows us to conclude. $\square$

Back to our case, assume that f fixes $E[N]$. Then $f - 1$ kills $E[N]$ so it factors through N, namely $f = 1 + g[N]$ for some $g \in \mathrm{End}(E)$. Hence $\mathrm{tr}(f) = 2 + N\mathrm{tr}(g)$ and $\deg(f) = 1 + \mathrm{tr}(g)N + \deg(g)N^2$. But $f \in \mathrm{Aut}(E)$ so $\deg f = 1$ and $N\mathrm{tr}(g) = -N^2 \deg g$. From part ii) of the lemma we have $\mathrm{tr}(g)^2 \leq 4$ and thus $|N \deg g| \leq 2$, which yields for $N \geq 3$ that $\deg g < 1$. So we must have $\deg g = 0$ and $f = 1$. $\square$

Rigidity of the level N problem will play a primary role in our discussion. It is indeed the key to representability.

Theorem 3.2. *A relatively representable moduli problem $\mathcal{P}$ which is also affine over* Ell *is representable if and only if it's rigid. If moreover it is étale over* Ell *then it is represented by a smooth affine curve over $\mathbb{Z}$.*

Proof. This result is non trivial. See [10] Chapter 4.7. $\square$

From now on we will consider schemes S over $\mathbb{Z}[1/N]$. We can finally state our main result:

Proposition 3.2. *For $N \geq 3$ the level N moduli problem*

$$\begin{aligned} \Gamma(N) : \mathrm{Ell}_{\mathbb{Z}[1/N]} &\longrightarrow \mathrm{Set} \\ E/S &\longrightarrow \{\textit{level } N \textit{ structures } E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2\} \end{aligned}$$

is representable. In particular the associated functor on $\mathrm{Sch}_{\mathbb{Z}[1/N]}$ is represented by a smooth affine curve Y_N over $\mathbb{Z}[1/N]$.

Proof. The proposition follows from Theorem 3.2., Remark 3.3. and Proposition 3.1. $\square$

Remark 3.4. *If we consider elliptic curves over $S = \mathrm{Spec}(\mathbb{C})$ we recover the classical definition of modular curve. Following the argument of Section 3.1, elliptic curves over $\mathbb{C}$ with level N-structure are parametrized by*

$$Y_N := \bigsqcup_{\gamma \in SL_2(\mathbb{Z}/N\mathbb{Z}) \backslash GL_2(\mathbb{Z}/N\mathbb{Z})} \Gamma(N)\backslash\mathbb{H}.$$

Here each connected component $Y(N) := \Gamma(N)\backslash\mathbb{H}$ represents the moduli problem over $\mathrm{Ell}_{\mathbb{C}}$ of isomorphism classes of pairs $(E_\tau, (P, Q))$ where E_τ is an elliptic curve and (P, Q) is a level N-structure of determinant ζ i.e. a basis for the N-th torsion subgroup of pairing $e_N(P, Q) = \zeta$ for ζ a primitive root of 1.

Let ζ_N vary between the primitive N-th roots of 1. Let us consider Y_N as a curve over $\mathbb{Z}[1/N, \zeta_N]$ under base extension. Since the setting in the complex case of Remark 3.1. is obtained by base change $\mathbb{Z}[1/N] \longrightarrow \mathbb{C}$ it's not surprising that the curve Y_N turns out to be disjoint union of $\phi(N)$ affine irreducible (all isomorphic) curves over $\mathbb{Z}[1/N, \zeta_N]$. We denote each irreducible component by $Y(N)$. We have then a universal pair

$$(\mathbb{E}/Y(N), \alpha_{univ})$$

that represents the moduli problem in $\mathrm{Ell}_{\mathbb{Z}[1/N,\zeta_N]}$ of level N-structures of pairing ζ_N. In particular $Y(N)$ represents the functor on $\mathrm{Sch}/\mathbb{Z}[1/N, \zeta_N]$ which associates to each scheme S the set of pairs $(E/S, \alpha_N)$ of elliptic curves over S with level N-structures of pairing ζ_N.

Remark 3.5. *We will work over an algebraically closed field K of positive characteristic p and with an integer $N \geq 3$ coprime with p. We will consider only affine schemes over the base field K. Fixed a primitive N-th root of unity ζ_N, the $\Gamma(N)$ moduli problem of determinant ζ_N is representable in the category Ell_K by a pair $(\mathbb{E}_K/Y(N)_K, \alpha_{univ})$. Such an object is simply obtained after base extension from the pair $(\mathbb{E}/Y(N), \alpha_{univ})$ in the category* $\mathrm{Ell}_{\mathbb{Z}[1/N,\zeta_N]}$.

Definition 3.9. *We refer to the object* $\begin{array}{c}(\mathbb{E}, \alpha_{univ}) \\ \downarrow \pi \\ Y(N)\end{array}$ *as the universal elliptic curve.*

3.3 Katz's modular forms

We are now ready to give the definition of modular forms. We recall again the definition of an elliptic curve over a scheme.

Definition 3.10. *Let S be a scheme. An elliptic curve E over S is a smooth proper morphism $p : E \longrightarrow S$ whose geometric fibers are connected curves of genus 1 with a section $e : S \longrightarrow E$.*

We denote by $\underline{\omega}_{E/S}$ the sheaf $p_*\Omega^1_{E/S} = R^0 p_* \Omega^1_{E/S}$. Such a sheaf is a line bundle and its formation is compatible with base change, i.e. if we have a pullback square:

$$\begin{array}{ccc} E_{S'} & \longrightarrow & E \\ \downarrow & & \downarrow p \\ S' & \xrightarrow{g} & S \end{array}$$

then $\underline{\omega}_{E_{S'}/S'} = g^* \underline{\omega}_{E/S}$.

Definition 3.11 (Modular forms of level 1)**.** *A modular form of weight $k \in \mathbb{Z}$ and level 1 is a rule f which assigns to each elliptic curve E over any scheme S a section $f(E/S)$ of $(\underline{\omega}_{E/S})^{\otimes k}$ over S such that:*

i) $f(E/S)$ depends only on the S-isomorphism class of the elliptic curve E.

ii) The formation of $f(E/S)$ commutes with arbitrary base change. Hence if we have $g : S' \longrightarrow S$ and

$$\begin{array}{ccc} E_{S'} & \longrightarrow & E \\ \downarrow & & \downarrow p \\ S' & \xrightarrow{g} & S \end{array}$$

then $f(E_{S'}/S') = g^*(f(E/S))$.

We denote by $M(\mathbb{Z}, 1, k)$ the $\mathbb{Z}$-module of such modular forms of weight k. If we consider elliptic curves defined over a ring R it makes sense to give the following equivalent definition:

Definition 3.12. *A modular form f of weight k is a rule which assigns to each pair $(E/R, \omega_{E/R})$ consisting of an elliptic curve E over a ring R, together with a basis $\omega_{E/R}$ of $H^0(\mathrm{Spec}(R), \underline{\omega}_{E/R})$, i.e. a nowhere vanishing section of $\Omega^1_{E/R}$, an element $f(E/R, \omega_{E/R})$ of R such that*

i) $f(E/R, \omega_{E/R})$ depends only on the isomorphism class of the pair $(E, \omega_{E/R})$.

ii) f is homogeneous of degree $-k$ in the second variable, namely for any $\lambda \in R^*$ we have $f(E/R, \lambda\omega_{E/R}) = \lambda^{-k} f(E/R, \omega_{E/R})$.

iii) The formation of E/R commutes with arbitrary extension of scalars $u : R \longrightarrow R'$, namely $f(E_{R'}/R', \omega_{E_{R'}/R'}) = u(f(E/R, \omega_{E/R}))$.

The correspondence between the two definitions is given by the formula

$$f(E/\mathrm{Spec}(R)) = f(E/R, \omega_{E/R})\omega^{\otimes k}_{E/R}.$$

Remark 3.6. *The position above makes sense. Let $S = \mathrm{Spec}(R)$ and let ω be a nowhere vanishing differential for E/R i.e. a global basis for $\Omega^1_{E/S}$. We have $p_*\Omega^1_{E/S} = \Gamma(\widetilde{E, \Omega^1_{E/S}})$ and thus $\underline{\omega}^{\otimes k}_{E/S} = (p_*\Omega^1_{E/S})^{\otimes k} = (\Gamma(\widetilde{E, \Omega^1_{E/S}}))^{\otimes k} =$ [5] $\Gamma(\widetilde{E, \Omega^1_{E/S}})^{\otimes k}$ hence*

$$H^0(S, \underline{\omega}^{\otimes k}_{E/S}) = (p_*\Omega^1{}_{E/S})^{\otimes k}(S) = (\Omega^1{}_{E/S}(E))^{\otimes k} = R\omega^{\otimes k}.$$

Remark 3.7. *If in the definition above we consider only schemes S or rings R lying over R_0 and only change of base given by R_0-morphisms, we obtain the notion of modular forms of weight k and level 1 defined over R_0, whose R_0-module we denote by $M(R_0, 1, k)$.*

Remark 3.8. *If we consider $R_0 = \mathbb{C}$ then any elliptic curve over $\mathbb{C}$ is of the form $E(\Lambda) = \mathbb{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}$ and we have a correspondence*

$$SL_2(\mathbb{Z})\backslash\mathbb{H} \longleftrightarrow \{\Lambda \subseteq \mathbb{C}\}/\mathbb{C}^*.$$

[5] Here we use that on a scheme $X = \mathrm{Spec}(R)$ if we have coherent $\mathcal{O}_X$ modules $\widetilde{M}$ and $\widetilde{N}$, then $\widetilde{M} \otimes_{\mathcal{O}_X} \widetilde{N} \cong M \widetilde{\otimes_{\mathcal{O}_X}} N$.

It's an easy exercise to check that we recover the classical notion of modular forms of weight k and level $SL_2(\mathbb{Z})$. Indeed, let $\Lambda_{\tau_1} = \mathbb{Z} + \tau_1\mathbb{Z}$ and $\Lambda_{\tau_2} = \mathbb{Z} + \tau_2\mathbb{Z}$. We recall that maps between complex tori are of the form

$$\begin{aligned} \mathbb{C}/\Lambda_{\tau_2} &\longrightarrow \mathbb{C}/\Lambda_{\tau_1} \\ z &\longrightarrow \alpha z \end{aligned}$$

form some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_{\tau_2} \subseteq \Lambda_{\tau_1}$. In particular the elliptic curves $\mathbb{C}/\Lambda_{\tau_1}$ and $\mathbb{C}/\Lambda_{\tau_2}$ are isomorphic if and only if there exists $\alpha \in \mathbb{C}^*$ such that

$$\Lambda_{\tau_1} = \alpha\Lambda_{\tau_2}$$

or equivalently if and only if, from the correspondence above, we have

$$\tau_2 = \gamma\tau_1$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\alpha = c\tau_1 + d$.
Let $\omega_2 = dz$ be the canonical invariant differential on $\mathbb{C}/\Lambda_{\tau_2}$ then $\omega_1 = d(\alpha z) = \alpha dz$ is an invariant differential on $\mathbb{C}/\Lambda_{\tau_1}$. Let f be a modular form in the sense of Definition 3.12. Regarding f as a function of τ i.e. $f(\tau) = f(\mathbb{C}/\Lambda_\tau, \omega)$, we have

$$\begin{aligned} f(\gamma\tau_1) = f(\tau_2) = f(\mathbb{C}/\Lambda_{\tau_2}, \omega_2) &= f(\mathbb{C}/\Lambda_{\tau_1}, \alpha^{-1}\omega_1) \\ &= \alpha^k f(\mathbb{C}/\Lambda_{\tau_1}, \omega_1) = (cz+d)^k f(\tau_1). \end{aligned}$$

Remark 3.9 (The Tate curve)**.** *In the classical theory of modular forms we require a modular form $f(\tau)$ to be holomorphic at ∞. This means that the Laurent series around zero of $\tilde{f}(q) = f(\log q/2\pi i)$, $0 < |q| < 1$, lies in $\mathbb{C}[\![q]\!]$. Our aim is to interpret the q-expansion of f in the perspective above as the value of such a rule f at a particular elliptic curve. To do so we will follow Katz's exposition in [8] Appendix 1.2. In particular, let $\tau \in \mathbb{H}$ and consider the associated elliptic curve $E_\tau = \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$. Taking the exponential gives us a complex analytic isomorphism*

$$\begin{aligned} \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z} &\longrightarrow \mathbb{C}^*/q^{\mathbb{Z}} \\ z &\longrightarrow t = e^{2\pi i z} \end{aligned}$$

where $q = e^{2\pi i \tau}$ and $q^{\mathbb{Z}}$ is the multiplicative subgroup of $\mathbb{C}^*$ generated by q. In particular the canonical differential dz is sent to $2\pi i \frac{dt}{t}$. So asking that the q-expansion of f lies in $\mathbb{C}[\![q]\!]$ is equivalent to asking that

$$f(\mathbb{C}^*/q^{\mathbb{Z}}, dt/t) \in \mathbb{C}[\![q]\!].$$

Let us find an equation for the curve above. The elliptic curve $E_\tau = \mathbb{C}/\Lambda_\tau$ given by the lattice $\mathbb{Z} + \tau\mathbb{Z}$ with differential dz is described by the Weirstrass equation

$$Y^2 = X^3 - g_2(\tau)X + g_3(\tau) \tag{3.1}$$

where

$$12(2\pi i)^{-4}g_2(\tau) = E_4(\tau) = 1 + 240\sum_{n\geq 1}\sigma_3(n)q^n,$$
$$216(2\pi i)^{-6}g_3(\tau) = E_6(\tau) = 1 - 504\sum_{n\geq 1}\sigma_5(n)q^n.$$

The canonical differential corresponds to $\frac{dX}{Y}$*. The isomorphism is as usual given by the Weirstrass* $\wp$*-function*

$$\begin{aligned}\mathbb{C}/\Lambda_\tau &\longrightarrow E_\tau\\ z+\Lambda_\tau &\longrightarrow (\wp(z,\tau),\wp'(z,\tau))\\ \Lambda_\tau &\longrightarrow O.\end{aligned}$$

Through the change of variable $q = e^{2\pi i\tau}$ *we may see the coefficients of (3.1) as lying in* $\mathbb{C}((q))$*. In particular the equation above defines an elliptic curve over* $\mathbb{Z}[1/6]((q))$*. To get rid of the denominators in (3.1) we make the change of variables*

$$\begin{aligned}\frac{1}{(2\pi i)^2}x &\longrightarrow x + \frac{1}{12}\\ \frac{1}{(2\pi i)^3}y &\longrightarrow x + 2y\end{aligned}$$

Then we get the equation

$$Y^2 + XY = X^3 + a_4(q)X + a_6(q) \tag{3.2}$$

where

$$a_4(q) = -5\sum_{n\geq 1}\sigma_3(n)q^n,$$
$$a_6(q) = \sum_{n\geq 1}\frac{-5\sigma_3(n) - 7\sigma_5(n)}{12}q^n.$$

One can easily see that $a_4(q)$ *and* $a_6(q)$ *lie in* $\mathbb{Z}((q))$*. Hence this last equation defines an elliptic curve with coefficients in* $\mathbb{Z}((q))$ *whose canonical differential is* $\omega_{can} = \frac{dX}{2Y+X}$*. The Tate curve* $\mathrm{Tate}(q)$ *is the curve over* $\mathbb{Z}((q))$ *defined by (3.2) whose restriction to* $\mathbb{Z}[1/6]((q))$ *is given by* (3.1)*. Doing a little algebra and summing up we have the following result.*

Proposition 3.3. *We have a complex analytic isomorphism*

$$\begin{aligned}\mathbb{C}^*/q^{\mathbb{Z}} &\longrightarrow \mathrm{Tate}(q)\\ t &\longrightarrow (X(t,q),Y(t,q))\end{aligned}$$

where

$$\begin{aligned}X(t,q) &= \sum_{n\in\mathbb{Z}}\frac{q^n t}{(1-q^n t)^2} - 2\sum_{n\geq 1}\frac{q^n}{1-q^n}\\ Y(t,q) &= \sum_{n\in\mathbb{Z}}\frac{(q^n t)^2}{(1-q^n t)^3} + \sum_{n\geq 1}\frac{q^n}{1-q^n}\end{aligned} \tag{3.3}$$

Moreover the discriminant and j-invariant of the Tate curve are given by the formulas

$$\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24} \in \mathbb{Z}[\![q]\!]$$
$$j(q) = \frac{1}{q} + 744 + 196884q + \dots$$

Proof. See Theorem 1.1 of [15] Chapter 5. □

Let us now fix a base ring R_0. The pair $(\mathrm{Tate}(q), \omega_{can})$ can be seen through base change as an elliptic curve over $\mathbb{Z}(\!(q)\!) \otimes_{\mathbb{Z}} R_0$ i.e

$$\begin{tikzcd}
\mathrm{Tate}(q)_{R_0} \arrow[r] \arrow[d] & \mathrm{Tate}(q) \arrow[d] \\
\mathrm{Spec}(\mathbb{Z}(\!(q)\!) \otimes_{\mathbb{Z}} R_0) \arrow[r] \arrow[d] & \mathrm{Spec}(\mathbb{Z}(\!(q)\!)) \arrow[d] \\
\mathrm{Spec}(R_0) \arrow[r] & \mathrm{Spec}(\mathbb{Z})
\end{tikzcd}$$

and we can evaluate any modular form of weight k and level 1 defined over R_0 at it in order to define:

Definition 3.13. *The q-expansion of a modular form f of level 1 is the finite-tailed Laurent series*

$$f(\mathrm{Tate}(q)_{R_0}, \omega_{can}) \in \mathbb{Z}(\!(q)\!) \otimes_{\mathbb{Z}} R_0.$$

Definition 3.14. *We say that f is holomorphic at ∞ if its q-expansion lies in $\mathbb{Z}[\![q]\!] \otimes_{\mathbb{Z}} R_0$.*

3.4 Modular forms of level N

Definition 3.15. *A modular form of weight k and level N is a rule f which assigns to each pair $(E/S, \alpha_N)$ where E is an elliptic curve over S and α_N a level N structure a section $f(E/S, \alpha_N)$ of $\underline{\omega}_{E/S}^{\otimes k}$ such that*

i) $f(E/S, \alpha_N)$ depends only on the isomorphism class of $(E/S, \alpha_N)$.

ii) The formation of f commutes with arbitrary base change, i.e. if $g : S' \longrightarrow S$ is a morphism of schemes and $E_{S'}/S'$ is the elliptic curve obtained by pullback

$$\begin{tikzcd}
E_{S'} \arrow[r] \arrow[d] & E \arrow[d, "p"] \\
S' \arrow[r, "g"] & S
\end{tikzcd}$$

then $f(E_{S'}/S', \alpha'_N) = g^*(f(E/S, \alpha_N))$.

If we consider elliptic curves over affine schemes, we have the equivalent definition:

Definition 3.16. *A modular form of weight k and level N is a rule f which assigns to each triple $(E/R, \omega_{E/R}, \alpha_N)$, consisting of an elliptic curve over a ring R together with a base $\omega_{E/R}$ of $H^0(\mathrm{Spec}(R), \underline{\omega}_{E/R})$ and a level N structure α_N, an element $f(E/R, \omega_{E/R}, \alpha_N) \in R$ such that:*

i) $f(E/R, \omega_{E/R}, \alpha_N)$ *depends only on the isomorphism class of* $(E/R, \omega_{E/R}, \alpha_N)$.

ii) The formation of f commutes with arbitrary base change, i.e. for any $g : R \longrightarrow R'$ we have $f(E_{R'}/R', \omega_{E_{R'}/R'}, {\alpha_N}') = g(f(E/R, \omega_{E/R}, \alpha_N))$.

ii) f is homogenous of degree $-k$ in the second variable, namely for any $\lambda \in R^*$, $f(E/R, \lambda\omega_{E/R}, \alpha_N) = \lambda^{-k} f(E/R, \omega_{E/R}, \alpha_N)$

Similarly if we consider only schemes or rings lying over a fixed ring R_0, we obtain modular forms of weight k and level N defined over a ring R_0. The R_0-module of all such is denoted by $M(R_0, N, k)$.
We now assume that N is invertible in R_0 and that R_0 contains a primitive N-th root of 1, ζ_N. We consider the pair $(\mathrm{Tate}(q), \omega_{can})$ consisting of the Tate curve over $\mathbb{Z}(\!(q)\!)$ and its canonical differential. Then a level N-structure is given by the choice of a basis for the N-torsion subgroup. Through the isomorphism $\mathrm{Tate}(q) \cong \mathbb{C}^*/q^{\mathbb{Z}}$ the points in $\mathrm{Tate}(q)[N]$ are given by

$$ {\zeta_N}^i q^{j/N} \qquad 0 \leq i, j \leq N-1. $$

Plugging the values for t in (3.3) we see that they have coordinates in $\mathbb{Z}[\![q^{1/N}]\!] \otimes_{\mathbb{Z}} \mathbb{Z}\left[\frac{1}{N}, \zeta_N\right]$ and the non constant q-coefficients of their coordinates lie in $\mathbb{Z}[\zeta_N]$. Hence for any level N structure α_N of the Tate curve, i.e. any choice of a basis for $\mathrm{Tate}(q)[N]$, we may consider the triple

$$ (\mathrm{Tate}(q^{1/N}), \omega_{can}, \alpha_N) $$

over $\mathbb{Z}(\!(q^{1/N})\!) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N, \zeta_N]$. Let us denote by $(\mathrm{Tate}(q^{1/N})_{R_0}, \omega_{can}, \alpha_N)$ the Tate curve over $\mathbb{Z}(\!(q^{1/N})\!) \otimes_{\mathbb{Z}} R_0$ obtained by base change equipped with its canonical differential and the level N structure above. We give the following definition:

Definition 3.17. *The q-expansions of a modular form f of level N over R_0 are the finitely many, finite-tailed, Laurent series:*

$$ f(\mathrm{Tate}(q^{1/N})_{R_0}, \omega_{can}, \alpha_N) \in \mathbb{Z}(\!(q^{1/N})\!) \otimes_{\mathbb{Z}} R_0 $$

for α_N varying among all level N structures.

Definition 3.18. *A modular form of level N defined over a ring R_0 is said to be holomorphic if it has all its q-expansions in $\mathbb{Z}[\![q^{1/N}]\!] \otimes_{\mathbb{Z}} R_0[1/N, \zeta_N]$. If R_0 itself contains $1/N$ and ζ_N this is equivalent to asking that all its q-expansions lie in $\mathbb{Z}[\![q^{1/N}]\!] \otimes_{\mathbb{Z}} R_0$.*

Now we consider a base ring R_0 which contains $1/N$ and ζ_N a primitive N-th root of unity. Our aim is indeed to work over the algebraically closed field K of positive characteristic of Remark 3.5. We want to give a description of the ring $M(R_0, N, k)$ of modular forms of weight k over R_0 in terms of the universal elliptic curve with level N-structure $\mathbb{E}_{R_0}/Y(N)_{R_0}$. For the sake of simplicity we will forget about the ground ring and we will denote by $\mathbb{E}/Y(N)$ the universal elliptic curve and $\underline{\omega}_{\mathbb{E}/Y(N)} = \pi_* \Omega^1_{\mathbb{E}/Y(N)}$ the associated line bundle on $Y(N)$ over any base ring (keeping in mind that everything works well under base change) . The scheme $Y(N)$ is a smooth affine curve over R_0 and represents the functor

$$\begin{aligned} \mathrm{Sch}/R_0 &\longrightarrow \mathrm{Set} \\ S &\longrightarrow \{(E/S, \alpha_N),\ \alpha_N \text{ a level } N\text{-structure of pairing } \zeta_N\}. \end{aligned}$$

Hence any elliptic curve $(E/S, \alpha)$ over the base ring R_0 with level structure α of determinant ζ_N is determined by base a change $g : S \longrightarrow Y(N)$ through the pullback

$$\begin{tikzcd} (E, \alpha) \arrow[r] \arrow[d] & (\mathbb{E}, \alpha_{univ}) \arrow[d, "\pi"] \\ S \arrow[r, "g"] & Y(N). \end{tikzcd}$$

For any modular form f its value $f(E/S, \alpha)$ in $H^0(S, \underline{\omega}^{\otimes k}_{E/S})$ is uniquely determined by

$$f(E/S, \alpha) = g^* f(\mathbb{E}/Y(N), \alpha_{univ})$$

by definition. Then it is natural to give the following equivalent definition.

Definition 3.19. *A modular form of weight k and level N over R_0 is a section in*

$$H^0(Y(N), \underline{\omega}^{\otimes k}_{\mathbb{E}/Y(N)}).$$

In our argument of Section 3.1. we arrived to the definition of holomorphic modular forms as sections of differentials on the *compactified* modular curve $X(N)$. To conclude this section we want to present a curve which will do the same job in the general case following sections 1.4 and 1.5 of [8]. As usual, many of the statements won't be proved here as they're beyond the scope of this work. First we give a remark.

Remark 3.10. *If we let $N = 1$ we consider the moduli problem in* Ell *that sends any elliptic curve E/S to its isomorphism class. It's not surprising that such a moduli problem is not representable. Indeed, it's clearly not rigid and Theorem 3.2. does not apply. So our setting over $\mathbb{C}$*

$$\begin{tikzcd} (\mathbb{H} \times \mathbb{C})/\mathbb{Z}^2 \arrow[d] \\ SL_2(\mathbb{Z})\backslash\mathbb{H} \end{tikzcd}$$

where the modular curve $Y(1) := SL_2(\mathbb{Z})\backslash\mathbb{H}$ parametrizes elliptic curves up to isomorphism does not give us an elliptic curve over $\mathbb{C}$. Anyway let us consider the j-function

$$j(\tau) = \frac{1278 g_2(\tau)^3}{\Delta(\tau)} = \frac{1278 g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}$$

which is a weakly modular function of weight zero, meromorphic at ∞. In terms of Katz's modular forms, it is the rule which sends any elliptic curve E_τ over $\mathbb{C}$ to its j-invariant.

It's an easy application of the valence formula to check that it is surjective (indeed the surjectivity of j hides behind the reason why any elliptic curve over $\mathbb{C}$ is of the form E_τ, see [3] or [16]). Hence it gives us a complex analytic isomorphism

$$Y(1) \xrightarrow{j} \mathbb{C} \cong \mathbb{A}^1_{\mathbb{C}}.$$

We have then morphisms of Riemann surfaces (thus of schemes over $\mathbb{C}$)

$$\Gamma(N)\backslash\mathbb{H} \twoheadrightarrow SL_2(\mathbb{Z})\backslash\mathbb{H} = \mathbb{A}^1_{\mathbb{C}} \hookrightarrow \mathbb{P}^1_{\mathbb{C}}.$$

And the compactified modular curve $X(N) := \Gamma(N)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$ was build ad hoc to fit in the commutative diagram

$$\begin{tikzcd} Y(N) \arrow[r, hook] \arrow[d, two heads] & X(N) \arrow[d, two heads] \\ Y(1) \cong \mathbb{A}^1_{\mathbb{C}} \arrow[r, hook] & \mathbb{P}^1_{\mathbb{C}}. \end{tikzcd}$$

Now we go back to the general case of $\mathrm{Sch}_{\mathbb{Z}[1/N,\zeta_N]}$ and consider the smooth affine curve $Y(N)$. As in the complex case, there is a finite and flat morphism of schemes $Y(N) \longrightarrow \mathbb{A}^1_{\mathbb{Z}[1/N,\zeta_N]}$ and the last one embeds naturally into $\mathbb{P}^1_{\mathbb{Z}[1/N,\zeta_N]}$.

Definition 3.20. *The modular curve $X(N)$ over $\mathbb{Z}[1/N,\zeta_N]$ is the normalization of the projective line $\mathbb{P}^1_{\mathbb{Z}[1/N,\zeta_N]}$ in $Y(N)$.*

Then $X(N)$ comes equipped with a natural factorization of

$$Y(N) \to \mathbb{A}^1_{\mathbb{Z}[1/N,\zeta_N]} \hookrightarrow \mathbb{P}^1_{\mathbb{Z}[1/N,\zeta_N]}$$

trough $Y(N) \hookrightarrow X(N)$. Moreover the modular curve $X(N)$ is a smooth proper curve over $\mathbb{Z}[1/N,\zeta_N]$ and the set

$$X(N) \setminus Y(N)$$

is (not surprisingly) a disjoint union of sections. We call such sections the cusps of $X(N)$, which we will keep denoting by $\mathrm{Cusps}(\Gamma(N))$ or equivalently $\mathrm{Cusps}(N)$.

Remark 3.11. *The cusps of $X(N)$ are in correspondence with the set of isomorphism classes of the level N-structures of the Tate curve. This means the following fact. The completion of $X(N)$ along each cusp is isomorphic to $\mathrm{Spec}\mathbb{Z}[1/N][\zeta_N]((q))$. If we consider in this context the universal elliptic curve*

$$\begin{tikzcd} (\mathbb{E}, \alpha_{univ}) \arrow[d, "\pi"] & \\ Y(N) \arrow[r, hook] & X(N) \end{tikzcd}$$

then the inverse image of $(\mathbb{E}, \alpha_{univ})$ over (the spectrum of) $\mathbb{Z}[1/N][\zeta_N]((q))$ (viewed as a punctured disc around the cusp) is isomorphic to the inverse image over $\mathbb{Z}[1/N][\zeta_N]((q))$ of the Tate curve with a level N structure that will correspond to that cusp. For a complete discussion of the topic see [10] Chapter 8.

Furthermore

Remark 3.12. *There is a canonical way to extend $\underline{\omega}_{\mathbb{E}/Y(N)}$ to a unique invertible sheaf $\underline{\omega}$ on $X(N)$ whose restriction to $Y(N)$ is $\underline{\omega}_{\mathbb{E}/Y(N)}$. Such a sheaf is of formation compatible with base change and its sections over the completion $\mathbb{Z}[1/N][\zeta_N]((q))$ at each cusp are precisely the $\mathbb{Z}[1/N][\zeta_N]((q))$ multiples of the canonical differential of the Tate curve. For the explicit construction see [10] Chapter 10.13.*

Back to the setting of our base ring R_0 which contains $1/N$ and ζ_N, we can characterize holomorphy of modular forms as follows. A modular form $f \in H^0(Y(N)_{R_0}, \underline{\omega}_{\mathbb{E}/Y(N)})$ is holomorphic at ∞ if it extends to a global section of $\underline{\omega}$. All in all, holomorphic modular forms of weight k and level N are sections in

$$H^0\left(X(N)_{R_0}, \underline{\omega}\right).$$

3.5 The Hasse Invariant and the action of Frobenius

From now on we will work in positive characteristic p.

Definition 3.21. *Let S be a scheme over $\mathbb{F}_p$. The absolute Frobenius is the morphism of schemes F_{abs} on S which corresponds to the identity on topological spaces ad whose map on structure rings $F_{abs}^{\#} : \mathcal{O}_S \longrightarrow \mathcal{O}_S$ is induced by the Frobenius endomorphism i.e. $F_{abs}^{\#}(x) = x^p$ for every section of $\mathcal{O}_S$ on an open of S.*

Let $\pi : X \longrightarrow S$ be a smooth morphism of schemes, S a smooth scheme over $\mathbb{F}_p$. The absolute Frobenius yields a commutative diagram

$$\begin{tikzcd} X \arrow[r, "F_{abs}"] \arrow[d, "\pi"] & X \arrow[d, "\pi"] \\ S \arrow[r, "F_{abs}"] & S. \end{tikzcd}$$

Clearly $F_{abs} : X \longrightarrow X$ is not a morphism of S-schemes. We define $X^{(p)}$ to be the smooth scheme over S obtained by taking the fiber product in the diagram

$$\begin{tikzcd} X^{(p)} \arrow[r, "\sigma"] \arrow[d, "\pi^{(p)}"] & X \arrow[d, "\pi"] \\ S \arrow[r, "F_{abs}"] & S. \end{tikzcd}$$

More concretely, we assume that π is finite and $S = \mathrm{Spec}(R)$ for an $\mathbb{F}_p$-algebra R. Then X is locally the spectrum of a finitely generated R-algebra $A = R[\underline{X}]/(f_i, i \in I)$. As a consequence $X^{(p)}$ is locally $\mathrm{Spec}A^{(p)}$ with $A^{(p)} = A \otimes_{F_{abs}} R = R[\underline{X}]/(f_i^{(p)}, i \in I)$ where if $f = \sum_I a_I \underline{X}^I$ then $f^{(p)} = \sum_I a_I^p \underline{X}^I$. The natural morphism σ is the map on structure sheaves $\mathcal{O}_X \longrightarrow \mathcal{O}_{X^{(p)}}$ induced by $A \longrightarrow A^{(p)}, f \longrightarrow f^{(p)}$.

By the universal property of the fiber product $X^{(p)}$ fits in a commutative diagram

$$\begin{tikzcd} X \arrow[r, "Fr"] \arrow[rr, bend left, "F_{abs}"] \arrow[dr, "\pi"'] & X^{(p)} \arrow[r, "\sigma"] \arrow[d, "\pi^{(p)}"] & X \arrow[d, "\pi"] \\ & S \arrow[r, "F_{abs}"] & S \end{tikzcd}$$

where $\sigma \circ Fr = F_{abs}$ is the absolute Frobenius.

Definition 3.22. *The map $Fr : X \longrightarrow X^{(p)}$ is called the relative Frobenius.*

The relative Frobenius is a morphism of ringed spaces $(Fr, Fr^{\#})$ with map on structure sheaves $Fr^{\#} : \mathcal{O}_{X^{(p)}} \longrightarrow Fr_*\mathcal{O}_X$. In the setting above the relative Frobenius is the map induced by $Fr^{\#}_{\mathrm{Spec}(A)} : A^{(p)} \longrightarrow A$ that sends $f \otimes 1 = f^{(p)} \in A \otimes_{F_{abs}} R$ in f^p, i.e.

$$\begin{aligned} R[\underline{X}]/(f_i^{(p)}, i \in I) &\longrightarrow R[\underline{X}]/(f_i, i \in I) \\ \underline{X} &\longrightarrow \underline{X}^p. \end{aligned}$$

The Frobenius maps allow us to define an important invariant for elliptic curves which turns out to be a modular form in the sense of Katz.

Let E/R be an elliptic curve over a $\mathbb{F}_p$-algebra R. The absolute Frobenius

$$\begin{tikzcd} E \arrow[r, "F_{abs}"] \arrow[d, "\pi"] & E \arrow[d, "\pi"] \\ \mathrm{Spec}(R) \arrow[r, "F_{abs}"] & \mathrm{Spec}(R) \end{tikzcd}$$

induces a map on cohomologies:

$$F_{abs}^* := R^1\pi_* F_{abs}^{\#} : R^1\pi_*\mathcal{O}_E \longrightarrow R^1\pi_*\mathcal{O}_E.$$

In other words, if $[f] \neq 0$ spans $H^1(E, \mathcal{O}_E)$ as an R-module, the Frobenius map induces a well defined map $H^1(E, \mathcal{O}_E) \longrightarrow H^1(E, \mathcal{O}_E)$, $[f] \longrightarrow [f^p]$ and taking the associated sheaves we conclude

$$R^1\pi_*\mathcal{O}_E = \widetilde{H^1(E, \mathcal{O}_E)} \longrightarrow R^1\pi_*\mathcal{O}_E = \widetilde{H^1(E, \mathcal{O}_E)}.$$

We let now η be a generator of $H^1(E, \mathcal{O}_E)$ as an R-module, dual to the nowhere vanishing differential $\omega \in \Omega^1_{E/R}(E)$. Then $F^*_{abs}(\eta) = A(E/R, \omega)\eta$ for some $A(E/R, \omega) \in R$.

We define:

Definition 3.23. *The Hasse invariant A is the rule which associates to $(E/R, \omega)$ the value $A(E/R, \omega)$ such that $F^*_{abs}(\eta) = A(E/R, \omega)\eta$.*

An equivalent description comes from the relative Frobenius

$$\begin{tikzcd} E \arrow[r, "Fr"] \arrow[dr, "\pi"'] \arrow[rr, bend left, "F_{abs}"] & E^{(p)} \arrow[r, "\sigma"] \arrow[d, "\pi^{(p)}"] & E \arrow[d, "\pi"] \\ & \mathrm{Spec}(R) \arrow[r, "F_{abs}"] & \mathrm{Spec}(R). \end{tikzcd}$$

We pick a basis η for $R^1\pi_*\mathcal{O}_E$ that is a section in $H^1(E, \mathcal{O}_E)$, dual to the nowhere vanishing differential ω and we denote by $\eta^{(p)}$ the corresponding basis of $R^1\pi_*\mathcal{O}_{E^{(p)}}$, obtained by base change through F_{abs}. In terms of global sections we pick the basis of $H^1(E^{(p)}, \mathcal{O}_{E^{(p)}}) = H^1(E, \mathcal{O}_E)^{(p)}$ given by $\eta^{(p)} = \sigma^*(\eta)$. Let Fr^* be the map induced by the relative Frobenius on cohomologies, then $F^*_{abs}(\eta) = Fr^*(\eta^{(p)}) = A(E/R, \omega)\eta$.

Proposition 3.4. *The Hasse invariant is a modular form over $\mathbb{F}_p$ of weight $p-1$.*

Proof. It sufficies to check that $A(E/R, \lambda\omega) = \lambda^{-(p-1)}A(E/R, \omega)$ for $\lambda \in R^*$. The dual of $\lambda\omega$ is $\lambda^{-1}\eta$. Hence $F^*_{abs}(\lambda^{-1}\eta) = A(E/R, \lambda\omega)\lambda^{-1}\eta$. Thus

$$A(E/R, \lambda\omega)\lambda^{-1}\eta = F^*_{abs}(\lambda^{-1}\eta) = \lambda^{-p}F^*_{abs}(\eta) = \lambda^{-p}A(E/R, \omega)\eta.$$

□

Proposition 3.5. *The Hasse invariant has q-expansions equal to* 1 *i.e. if we consider the pair* $(\mathrm{Tate}(q)_{\mathbb{F}_p}, \omega_{can})$ *of the Tate curve over* $\mathbb{F}_p((q))$ *with its canonical differential, then*

$$A(\mathrm{Tate}(q)_{\mathbb{F}_p}, \omega_{can}) = 1.$$

Proof. We would like to prove that, fixed a basis η for $H^1(\mathrm{Tate}(q)_{\mathbb{F}_p}, \mathcal{O}_{\mathrm{Tate}(q)_{\mathbb{F}_p}})$ we have

$$F^*_{abs}(\eta) = \eta.$$

By Serre's duality $H^1(\mathrm{Tate}(q)_{\mathbb{F}_p}, \mathcal{O}_{\mathrm{Tate}(q)_{\mathbb{F}_p}})$ is dual to the $\mathbb{F}_p((q))$-vector space

$$H^0\left(\mathrm{Tate}(q)_{\mathbb{F}_p}, \Omega^1_{\mathrm{Tate}(q)_{\mathbb{F}_p}/\mathbb{F}_p((q))}\right).$$

The sheaf of differentials $\Omega^1_{\mathrm{Tate}(q)_{\mathbb{F}_p}/\mathbb{F}_p((q))}$ is in turn dual to the $\mathbb{F}_p((q))$-linear derivations $\mathrm{Der}_{\mathbb{F}_p((q))}(\mathcal{O}_{\mathrm{Tate}(q)_{\mathbb{F}_p}})$. So we may take as basis η of $H^1(\mathrm{Tate}(q)_{\mathbb{F}_p}, \mathcal{O}_{\mathrm{Tate}(q)_{\mathbb{F}_p}})$ the dual basis to ω_{can}, the no-where vanishing invariant differential for $\mathrm{Tate}(q)_{\mathbb{F}_p}$. We denote by

$$D : \mathcal{O}_{\mathrm{Tate}(q)_{\mathbb{F}_p}} \longrightarrow \mathcal{O}_{\mathrm{Tate}(q)_{\mathbb{F}_p}}$$

the dual derivation to ω_{can}, then the action induced by Frobenius is

$$D \xrightarrow{Fr^*} D^p = {}^6 D \circ D \circ \ldots \circ D.$$

We consider the formal completion of the Tate curve along the identity section and we compute the action of the Frobenius restricting to $\widehat{\mathrm{Tate}(q)}_{\mathbb{F}_p}$, recalling that we have an isomorphism $\widehat{\mathrm{Tate}(q)} = \widehat{\mathbb{G}}_m$. We complete the multiplicative scheme along the identity section i.e. along the closed subscheme of ideal $(t-1)$ and we denote by $X = t-1$ the local parameter at it. Then the invariant (with respect to the formal group law) differential is given by $\frac{dX}{X+1}$. Hence the dual derivation to it is $D = (X+1)\frac{d}{dX}$. To conclude it suffices to check that $D^p = D$. But one easily sees that $D(X) = X+1$, $D^2(X) = D(X+1) = X+1$ and iterating $D^p(X) = X+1 = D(X)$ hence $D^p = D$. □

Remark 3.13. *Notice that by definition A is a modular form of full level. Hence given a triple $(E/R, \omega_{E/R}, \alpha)$ of an elliptic curve E/R over $\mathbb{F}_p$ with differential $\omega_{E/R}$ and level N structure, we can forget about the last one, i.e. $A(E/R, \omega_{E/R}, \alpha) = A(E/R, \omega_{E/R})$. Then Proposition 3.5. yields that for any level N-structure α_N of the Tate curve* $\mathrm{Tate}(q^{1/N})$ *over $\mathbb{F}((q^{1/N}))$ we have*

$$A(\mathrm{Tate}(q^{1/N})_{\mathbb{F}_p}, \omega_{can}, \alpha_N) = 1.$$

[6] Notice that since $\mathrm{char} K = p$ the map D^p is actually a derivation.

It's important to mention that another description of the Hasse invariant comes from the dual isogeny of the relative Frobenius. We sketch it in the next remark.

Remark 3.14. *Let E/R be an elliptic curve over an $\mathbb{F}_p$-algebra R and let $Fr : E \longrightarrow E^{(p)}$ be the relative Frobenius. We denote by*

$$V : E^{(p)} \longrightarrow E$$

its dual, the Verschiebung map. We recall the following fact about elliptic curves over a field E/k where k is algebraically closed of positive characteristic p. A proof can be found in [16] Chapter 4. If we denote by $[p^n] : E \longrightarrow E$ the multiplication by p^n map, then only one of the following cases can occur:

1. *For all $n > 0$ the n-th iterate Verschiebung map V^n is inseparable and its kernel is trivial. As a consequence $[p^n]$ is bijective for any n and $E[p^n]$ is trivial. In this case we say that E/k is supersingular.*
2. *For all $n > 0$ the n-th iterate Verschiebung map V^n is separable and its kernel is not trivial, in particular $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$. We say that E/k is ordinary.*

Moreover we say that an elliptic curve E/R over the field K of characteristic p is ordinary if each of its fiber is. Then we conclude that E/R is ordinary if and only if the Verschiebung $V : E^{(p)} \longrightarrow E$ is étale or equivalently if and only if the map induced on tangent spaces $tg(V)$ is an isomorphism, since any of these property holds if and only if it holds fiberwise. By Serre's duality $H^1(E, \mathcal{O}_E)$ is dual to $H^0(E, \Omega_{E/R})$ thus it can be identified with $\mathrm{Hom}_{\mathcal{O}_E}(\Omega^1_{E/S}, \mathcal{O}_E)$. The action of Verschiebung on the latter corresponds to the one of Frobenius on $H^1(E, \mathcal{O}_E)$. In particular E/R is ordinary if and only if the Hasse invariant $A(E/R, \omega)$ is non zero in R.

We now fix an algebraically closed field K of characteristic p, and an integer $N \geq 3$ such that $(N, p) = 1$. We return to the description of A as a global section on the modular scheme $Y(N)_K = Y(N)$ in order to give an important result about the zeroes of the Hasse invariant.

Remark 3.15. *Assume $p > 2$. Deuring computes the Hasse invariant for an elliptic curve in Legendre form*

$$Y^2 = X(X-1)(X-\lambda) \qquad \lambda \neq 0, 1$$

over an algebraically closed field of characteristic p. It corresponds to the polynomial

$$A(\lambda) = \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i$$

where $m = (p-1)/2$. Such a description turns out to be very useful. Igusa in [5] uses it to count the number of supersingular elliptic curves over a given field of positive characteristic. In particular he shows that $A(\lambda)$ satisfies a certain differential equation hence it must have simple zeroes. A detailed argument can be found in Theorem 4.1 in [16].

Proposition 3.6. *The zeroes of A are simple.*

Proof. All the q-expansions of A are equal to 1, so zeroes of A are (closed) points in $Y(N)$. Let $\mathbb{E}/Y(N)$ be the universal elliptic curve over K. Let $x \in Y(N)$ be a zero of A.
We will give two proofs of the fact that x is a simple zero. The first one is for $p > 2$ and uses Remark 3.15. In particular it relies on the fact that every elliptic curve over a scheme where 2 is invertible admits locally a Legendre form (see [10] section 2.2). We may restrict to an affine open neighborhood of x and assume that $Y(N)$ is the spectrum of a ring R and $\mathbb{E}$ is locally the curve

$$Y^2 = X(X-1)(X-\lambda)$$

for $\lambda \in R$, $\lambda \neq 0, 1$. Since $Y(N)$ is a smooth curve over K, we may assume that R is the coordinate ring of a smooth affine curve over K and it's thus a local K-algebra, in particular a DVR with residue field K. Moreover the Hasse invariant is the section $A(\lambda) \in R$ given by the polynomial of Remark 3.15. The assumption $\lambda \neq 0$ implies that λ never vanishes on the curve. If we denote by $\lambda(x) \in K$ the image of λ in the residue field at x, then $\lambda - \lambda(x)$ has order exactly one at x, so it's a uniformizer at x . If $\mathrm{ord}_x(A) \geq 2$ we would have that $(\lambda - \lambda(x))^2$ divides $A(\lambda)$ and this contradict the fact that the Deuring polynomial has simple zeroes.
The second proof works more generally and exploits the universal property of the modular curve. Let us denote by $\mathcal{O}_{Y(N),x}$ the local ring at x and $\mathfrak{m}_{Y(N),x}$ its maximal ideal. We are under the assumption that A vanishes at x. This means that if

$$A(\mathbb{E}/Y(N)) = A(\mathbb{E}/Y(N), \omega)\omega^{p-1}$$

is the global section on $Y(N)$ corresponding to the Hasse invariant then

$$A(\mathbb{E}/Y(N), \omega)_x \in \mathfrak{m}_{Y(N),x}$$

where $B := A(\mathbb{E}/Y(N), \omega)_x$ is the image of $A(\mathbb{E}/Y(N), \omega)$ in $\mathcal{O}_{Y(N),x}$. We want to prove that $B \notin \mathfrak{m}^2_{Y(N),x}$. Let $E := \mathbb{E} \times_{Y(N)} S$ where $S = \mathrm{Spec}\left(\mathcal{O}_{Y(N),x}\right)$ and assume that $B \in \mathfrak{m}_x^2$. Let $R = \mathcal{O}_{Y(N),x}/\mathfrak{m}^2_{Y(N),x}$, then R is a local K-algebra with residue field K. Moreover let $E_R = E \otimes_{\mathcal{O}_{Y(N),x}} R$ the elliptic curve obtained by base change $\mathcal{O}_{Y(N),x} \twoheadrightarrow R$

$$\begin{tikzcd}
E_R \arrow[r] \arrow[d] & E \arrow[r] \arrow[d] & \mathbb{E} \arrow[d] \\
\mathrm{Spec}(R) \arrow[r] & S \arrow[r] & Y(N).
\end{tikzcd}$$

As $B \in \mathfrak{m}_{Y(N),x}$ the curve $E_0 = E_R \otimes_R K = E \otimes_{\mathcal{O}_{Y(N),x}} K$ is supersingular and E_R is obtained by base change $K \hookrightarrow R$ from E_0 i.e. $E_R = E_0 \otimes_K R$

$$\begin{tikzcd}
E_R \arrow[r] \arrow[d] & E_0 \arrow[d] \\
\mathrm{Spec}(R) \arrow[r] & \mathrm{Spec}(K).
\end{tikzcd}$$

We obtain two morphisms defining E_R through pullback from $\mathbb{E}$. The first is determined by the base change $\mathcal{O}_{Y(N),x} \twoheadrightarrow R$ and the second by

$$\mathcal{O}_{Y(N),x} \twoheadrightarrow R \twoheadrightarrow K \hookrightarrow R.$$

These two are different because R is not a field, so they correspond to level structures α_1 and α_2 on E_R respectively . We call $\varphi : R \twoheadrightarrow K \hookrightarrow R$. We have then a cartesian diagram

$$\begin{array}{ccc} (E_R, \alpha_2) & \longrightarrow & (E_R, \alpha_1) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(R) & \xrightarrow{\mathrm{Spec}\varphi} & \mathrm{Spec}(R). \end{array}$$

We may iteratively define α_3, α_4,..., α_n by pulling back

$$\begin{array}{c} (E_2, \alpha_2) \\ \downarrow \\ \mathrm{Spec}(R) \end{array}$$

by $\mathrm{Spec}(\varphi)$. Indeed, we observe that $\varphi \circ \varphi = \varphi$ and on the top row we keep obtaining E_R, but the level structures must be different since φ is not the identity. The isomorphism $E_R \cong E_R$ of the top row permutes the level structures, so for n large enough we must get $\alpha_n = \alpha_1$. But this contradicts the universal property of $\mathbb{E}/Y(N)$, since the maps from $\mathrm{Spec}(R)$ to $Y(N)$ are different. $\square$

We conclude this section computing the action of Frobenius on the first relative de Rham cohomology of the Tate curve $\mathrm{Tate}(q)_K$ over $K(\!(q)\!)$.

Remark 3.16. *Since the formation of cohomology and of Frobenius commutes with base change, we can work with* $\mathrm{Tate}(q)_{\mathbb{F}_p}$ *over* $\mathbb{F}_p(\!(q)\!)$. *The natural map of reduction modulo* p

$$\mathbb{Z}_p(\!(q)\!) \twoheadrightarrow \mathbb{F}_p(\!(q)\!)$$

allows us to obtain $\mathrm{Tate}(q)_{\mathbb{F}_p}$ *by base change from* $\mathrm{Tate}(q)_{\mathbb{Z}_p}$. *This means that we have a pullback diagram*

$$\begin{array}{ccc} \mathrm{Tate}(q)_{\mathbb{F}_p} & \longrightarrow & \mathrm{Tate}(q)_{\mathbb{Z}_p} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{F}_p(\!(q)\!)) & \longrightarrow & \mathrm{Spec}(\mathbb{Z}_p(\!(q)\!)). \end{array}$$

We may write $\mathrm{Tate}(q)_{\mathbb{F}_p} = \mathrm{Tate}(q)_{\mathbb{Z}_p} \otimes \mathbb{F}_p(\!(q)\!)$. *Moreover by functoriality of cohomology*

$$H^1_{dR}(\mathrm{Tate}(q)_{\mathbb{F}_p}/\mathbb{F}_p(\!(q)\!)) \cong H^1_{dR}(\mathrm{Tate}(q)_{\mathbb{Z}_p}/\mathbb{Z}_p(\!(q)\!)) \otimes \mathbb{F}_p(\!(q)\!).$$

There exists a lift of the relative Frobenius in characteristic zero

$$F : \mathrm{Tate}(q)_{\mathbb{Z}_p} \longrightarrow \mathrm{Tate}(q)'_{\mathbb{Z}_p}.$$

More precisely the following lemma holds.

Lemma 3.2. *Let R_0 be a discrete valuation ring of residue field K of characteristic p and generic characteristic zero, R an R_0-algebra and E/R an elliptic curve. Let $E \otimes R/pR$ denote the elliptic curve over the K-algebra R/pR obtained by base change through the canonical map of reduction. Let $Fr : E \otimes R/pR \longrightarrow (E \otimes R/pR)^{(p)}$ be the Frobenius isogeny. Assume $E \otimes R/pR$ is ordinary. Then we can lift Fr to an isogeny $F : E \longrightarrow E'$ such that*

$$\begin{tikzcd} E \arrow[r, "F"] & E' \\ E \otimes R/pR \arrow[u] \arrow[r, "Fr"] & (E \otimes R/pR)^{(p)} \arrow[u] \end{tikzcd}$$

commutes.

Proof. This lemma is a consequence of a more general result about the canonical subgroup of an elliptic curve by Lubin and Katz. We will sketch a proof in the case of our interest, for a detailed argument see [8] Chapter 3. Under our assumption the Verschiebung isogeny

$$V : (E \otimes R/pR)^{(p)} \longrightarrow E \otimes R/pR$$

is seperable and its kernel is a finite flat subgroup scheme, étale over R/pR. By Hensel's lemma we can lift it to a subgroup scheme of E, say H_1 such that $H_1 \otimes R/pR = \ker V$. Taking its Cartier dual we obtain a subgroup scheme H of E and we consider the unique isogeny of kernel H

$$E \xrightarrow{F} E' = E/H.$$

Then $H \otimes R/pR$ is the kernel of Frobenius and we conclude. $\square$

We work in characteristic zero. Such F induces a morphism on cohomologies

$$\begin{tikzcd} H^1_{dR}(Tate'(q)_{\mathbb{Z}_p}/\mathbb{Z}_p(\!(q)\!)) \arrow[r, "F^*"] \arrow[d] & H^1_{dR}(Tate(q)_{\mathbb{Z}_p}/\mathbb{Z}_p(\!(q)\!)) \arrow[d] \\ \left(H^1_{dR}(Tate(q)_{\mathbb{Z}_p}/\mathbb{Z}_p(\!(q)\!)) \otimes \mathbb{F}_p(\!(q)\!)\right)^{(p)} \arrow[r, "Fr^*"] & H^1_{dR}(Tate(q)_{\mathbb{Z}_p}/\mathbb{Z}_p(\!(q)\!)) \otimes \mathbb{F}_p(\!(q)\!). \end{tikzcd}$$

We use now functoriality of the Gauss-Manin connection. If we denote by φ the map on differentials induced by Frobenius we have

$$\begin{tikzcd} H^1_{dR}(E'/R) \arrow[r, "\nabla"] \arrow[d, "F^*"] & H^1_{dR}(E'/R) \otimes \Omega^1_R \arrow[d, "F^* \otimes \varphi"] \\ H^1_{dR}(E/R) \arrow[r, "\nabla"] & H^1_{dR}(E/R) \otimes \Omega^1_R. \end{tikzcd}$$

Let us fix the basis $\{\omega_{can}, \eta_{can}\}$ of $H^1_{dR}(\mathrm{Tate}(q)_{\mathbb{Z}_p}/\mathbb{Z}_p(\!(q)\!))$ where $\eta_{can} = \nabla(\frac{d}{dq})(\omega_{can})$. We remark that such a choice gives us a basis compatible with the Hodge filtration (see Appendix C). Let $\{\omega^{(p)}_{can}, \eta^{(p)}_{can}\}$ be the basis of

$$H^1_{dR}(\mathrm{Tate}(q)^{(p)}_{\mathbb{F}_p}/\mathbb{F}_p(\!(q)\!)) = H^1_{dR}(\mathrm{Tate}(q)_{\mathbb{F}_p}/\mathbb{F}_p(\!(q)\!))^{(p)}$$

obtained by base change through the reduction modulo p and F_{abs}. Moreover we fix the basis $\{\omega'_{can}, \eta'_{can}\}$ in characteristic zero corresponding to $\omega^{(p)}_{can}$ and $\eta^{(p)}_{can}$. Then

$$\nabla(\omega_{can}) = \nabla\left(\frac{d}{dq}\right)(\omega_{can}) \otimes \frac{dq}{q} = \eta_{can} \otimes \frac{dq}{q}.$$

We have

$$F^*(\omega'_{can}) = p\omega_{can}.$$

And

$$\nabla(F^*(\omega'_{can})) = \nabla(p\omega_{can}) = p\nabla(\omega_{can}) = p\left(\eta_{can} \otimes \frac{dq}{q}\right).$$

On the other hand

$$(F^* \otimes \varphi)(\nabla(\omega'_{can})) = F^*(\eta'_{can}) \otimes \frac{dq^p}{q^p} = F^*(\eta'_{can}) \otimes p\frac{dq}{q}.$$

By functoriality $\nabla \circ F^* = (F^* \otimes \varphi) \circ \nabla$ and thus

$$p\eta_{can} \otimes \frac{dq}{q} = F^*(\eta'_{can}) \otimes p\frac{dq}{q}$$

which implies $F^*(\eta'_{can}) = \eta_{can}$. By base change we conclude

$$Fr^*(\omega^{(p)}_{can}) = 0,$$
$$Fr^*(\eta^{(p)}_{can}) = \eta_{can}.$$

Chapter 4

A result on modular forms in characteristic p

In this chapter we will prove a result on modular forms for level N in positive characteristic p following Katz [9]. As in the full level case the Hasse invariant A is the only modular form whose q-expansion equals 1 and the multiplication by A does not affect q-expansions. On the wave of Chapter 2 we will define the *filtration* of a modular form of level N and we will build an operator $A\theta$ acting on modular forms whose effect on q-expansion is $q\frac{d}{dq}$, in order to get a statement analogous to Proposition 2.4. for modular forms of level N.

4.1 The general setting

Throughout all this chapter we fix an algebraically closed field K of prime characteristic p and an integer $N \geq 3$ prime to p. Let ζ be a primitive N-th root of unity. The moduli problem in Ell_K which associates to each elliptic curve E/B where B is a K-algebra the set of level N-structures of determinant ζ is representable. Let

$$\begin{tikzcd} (\mathbb{E}, \alpha_{univ}) \arrow[d, "\pi"] \\ Y(N) \end{tikzcd}$$

be the object in Ell_K representing it. Then $Y(N)$ is a smooth affine irreducible curve over K. Let us set

$$\underline{\omega} := \underline{\omega}_{\mathbb{E}/Y(N)} = \pi_* \Omega^1_{\mathbb{E}/Y(N)}.$$

The graded ring of (not necessarily holomorphic at the cusps) modular forms is

$$R_N^{\bullet} = \bigoplus_{k \in \mathbb{Z}} H^0\left(Y(N), \underline{\omega}^{\otimes k}\right).$$

Let B be any K-algebra. Let f be a modular form of weight k, i.e.

$$f = f(\mathbb{E}/Y(N), \alpha_{univ})\omega^{\otimes k}.$$

For any triple $(E/B, \omega_{E/B}, \alpha)$ of an elliptic curve E over B, a basis $\omega_{E/B}$ for $\underline{\omega}_{E/B}$ and a level N structure α on E/B we denote by

$$f(E/B, \omega_{E/B}, \alpha) \in B$$

its value at it. Moreover we can consider the Tate curve over $B = K(\!(q^{1/N})\!)$, which we will denote by $\mathrm{Tate}(q)$ to have a lighter notation, with its canonical differential ω_{can}. By evaluating f at the level N structure α_0 of determinant ζ we obtain the q-expansion at the corresponding cusp which we denote

$$f_{\alpha_0}(q) := f(\mathrm{Tate}(q), \omega_{can}, \alpha_0).$$

Let $A \in R_N^{p-1}$ be the Hasse invariant of Chapter 3.5. Then

Proposition 4.1. *All the q-expansions of the Hasse invariant are identically* 1.

Proof. It has been proved in Proposition 3.5 $\square$

Furthermore

Proposition 4.2. *Taking q-expansions at each cusp determines ring homomorphisms:*

$$R_N^\bullet \longrightarrow K(\!(q^{1/N})\!)$$
$$R_{N,holo}^\bullet \longrightarrow K[\![q^{1/N}]\!]$$

whose kernel is exactly $(A-1)$.

Before proving the claim we give an auxiliary lemma.

Lemma 4.1. *Let X be a proper, smooth, irreducible curve over K. Let $\mathcal{L}$ be an ample line bundle on X. Let*

$$S = \bigoplus_{n \geq 0} H^0(X, \mathcal{L}^{\otimes n}).$$

Let s be a section in $\Gamma(X, \mathcal{L}^{\otimes k})$ for some k, coprime with $\mathrm{char}K$. *If s has at least one simple zero, then $s-1$ generates a prime ideal in S.*

Remark 4.1. *We recall that $\mathcal{L}$ ample yields that X is quasi-compact and the opens $X_{s'}$ where s' trivializes $\mathcal{L}$ for s' homogeneous in S such that $X_{s'}$ is affine form a basis for the topology on X. Moreover the natural map $X \longrightarrow$* $\mathrm{Proj}(S)$ *is an open immersion with dense image. Since X is proper we obtain an isomorphism*

$$X \cong \mathrm{Proj}(S).$$

Proof. We recall the following lemma in Hartshorne 5.14 [4]:

Lemma 4.2 (Harthshorne 5.14)**.** *Let X be a scheme, $\mathcal{L}$ an invertible sheaf on X and $\mathcal{F}$ a quasi coherent sheaf on X. Let $f \in \Gamma(X, \mathcal{L})$ and X_f the open set of points where $f_x \notin \mathfrak{m}_x \mathcal{L}_x$. Suppose furthermore that X has a finite covering by affine subsets U_i such that $\mathcal{L}_{|U_i}$ is free for each i and such that $U_i \cap U_j$ is quasi compact for each i, j. For every section $t \in \Gamma(X_f, \mathcal{F})$ there exists $n > 0$ such that the section $f^n_{|X_s} t \in \Gamma(X_f, \mathcal{F} \otimes \mathcal{L}^{\otimes n})$ extends to a global section of $\mathcal{F} \otimes \mathcal{L}^{\otimes n}$.*

We recall that s trivializes $\mathcal{L}^{\otimes k}$ on X_s i.e. $\mathcal{L}^{\otimes k}_{|X_s} \cong \mathcal{O}_{X|X_s} s_{|X_s}$, thus $\mathcal{L}^{\otimes n}$ is trivial on X_s for every n. Restriction gives maps $\Gamma(X, \mathcal{L}^{\otimes n}) \longrightarrow \Gamma(X_s, \mathcal{L}^{\otimes n})$. Moreover sending $s^{-n} \in S_s$ to $s^{\otimes -n}_{|X_s}$ we have a natural ring homomorphism

$$S_s \longrightarrow \bigoplus_{n \in \mathbb{Z}} \Gamma(X_s, \mathcal{L}^{\otimes n}).$$

Choosing the basis of Remark 4.1. above we are under the assumption of Lemma 4.2. (indeed $X_s \cap X_{s'} = X_{ss'}$ for global sections s and s', which is affine) and we may apply it with $\mathcal{F} = \mathcal{O}_X$ and conclude that the map above is an isomorphism.
We want to prove that $s-1$ generates a prime ideal in S, checking that the subset $Z = V(s-1) \subseteq \operatorname{Spec}(S)$ is irreducible. We notice that $V(s-1)$ can be seen in the spectrum of $S[1/s] = S_s$ since $x \in V(s-1)$ holds if and only if $(s-1) \in x$ and in particular we must have $s \notin x$ i.e. the image of x is a prime in the localization S_s. We may then see Z as a closed subset of $\operatorname{Spec}\left(\bigoplus_{n \in \mathbb{Z}} \Gamma(X_s, \mathcal{L}^{\otimes n})\right)$ through the isomorphism above. We fix an affine open subset $U = \operatorname{Spec} A \subseteq X_s$. Then $\mathcal{L}$ is trivial on U i.e. $\mathcal{L}_{|U}$ is free generated by some $T \in \mathcal{L}(U)$ and since $\mathcal{L}^{\otimes k}_{|U} \cong \mathcal{O}_{X_s} s_{|X_s}$ we must have $s_{|X_s} = uT^k$ for some $u \in A^\times$. Then

$$\bigoplus_{n \in \mathbb{Z}} \Gamma(U, \mathcal{L}^{\otimes n}_{|U}) = \bigoplus_{n \in \mathbb{Z}} AT^n = A[T, T^{-1}].$$

And Z corresponds to $V(T^k u - 1) = V \subseteq \operatorname{Spec}(A[T, T^{-1}])$ i.e.

$$V = \operatorname{Spec}\left(A[T, T^{-1}]/(uT^k - 1)\right).$$

Notice that since k is invertible in K we obtain that Z is étale over $U = \operatorname{Spec}(A)$, hence over X_s. Moreover X is normal, hence X_s is normal and Z is normal. We would like to prove that Z is connected since for normal schemes it's equivalent to being irreducible. The open $X_s \subseteq X$ is irreducible so covering it by affines U of the form above they must have non empty intersection. As a consequence the corresponding affine opens of Z above them must have non empty intersection. So it suffices to prove that $\operatorname{Spec}\left(A[T, T^{-1}]/(uT^k - 1)\right)$ is connected, in particular we only have to check that the generic fiber is connected. Indeed if $Z \xrightarrow{f} X$ is an étale morphism, assume $f^{-1}(\eta)$ is connected where η is the generic point of X. If Z is not connected i.e. $Z = U_1 \cup U_2$ with U_i disjoint opens, then, since $f^{-1}(\eta)$ is connected, we must have $f^{-1}(\eta) \subseteq U_1$ or $f^{-1}(\eta) \subseteq U_2$. Assume $f^{-1}(\eta) \subseteq U_1$ and $U_2 \neq \emptyset$, then $\{\eta\} \cap f(U_2) = \emptyset$ and $f(U_2)$ is a non empty open since étale maps are open, contradicting the fact that $\{\eta\}$ is dense in X.
Let $F = \operatorname{Frac} A = \mathcal{O}_{X,\eta}$ be the local ring at the generic point, we check that

$$\operatorname{Spec}\left(F[T, T^{-1}]/(uT^k - 1)\right) \cong \operatorname{Spec}\left(F[z]/(z^k - u)\right)$$

is irreducible, proving that $z^k - u$ is irreducible in $F[z]$. Let $x \in X$ be a simple zero of s. Let $\mathcal{O}_{X,x}$ be the local ring at x, with maximal ideal $\mathfrak{m}_{X,x}$, then under our assumption $O_{X,x}$ is a DVR and we can see F as the field of fractions of $O_{X.x}$. Then $s_x \in \mathfrak{m}_{X,x} \setminus \mathfrak{m}^2_{X,x}$ and under the isomorphisms above u is a uniformizer. We conclude that the polynomial $z^k - u$ is irreducible by Eisenstein's criterion. $\square$

We can now prove Proposition 4.2.

Proof. We keep denoting by $\underline{\omega}$ the natural extension to $X(N)$ of the invertible sheaf $\underline{\omega}$ on $Y(N)$. Such a sheaf is an ample line bundle on $X(N)$, since the associated divisor has positive degree. Indeed the Kodaira-Spencer mapping extends to an isomorphism

$$\underline{\omega}^{\otimes 2} \cong \Omega^1_{X(N)}\langle \mathrm{Cusps}(N)\rangle.$$

Hence

$$\deg(\underline{\omega}^{\otimes 2}) = \deg(\Omega^1_{X(N)}\langle \mathrm{Cusps}(N)\rangle) = 2g-2+|\mathrm{Cusps}(N)| = 2g-2+\frac{N^2}{2}\prod_{p|N}\left(1-\frac{1}{p^2}\right).$$

Where g is the genus of the curve $X(N)$ and the number of cusps follows from Remark 1.5. Since $g \geq 0$ and $N \geq 3$ the quantity above is always positive, so $\underline{\omega}^{\otimes 2}$ is ample hence $\underline{\omega}$ is ample.
Thanks to Remark 4.1. we have

$$X(N) \cong \mathrm{Proj}\left(\bigoplus_{n\geq 0} H^0(X(N),\underline{\omega}^{\otimes n})\right).$$

Moreover if $n < 0$ we have $\deg(\underline{\omega}^{\otimes n}) = n\deg\underline{\omega} < 0$ i.e. the divisor of $\underline{\omega}$ has negative degree hence $H^0(X(N),\underline{\omega}^{\otimes n}) = 0$. As a consequence we may write

$$\bigoplus_{n\geq 0} H^0\left(X(N),\underline{\omega}^{\otimes n}\right) = \bigoplus_{n\in\mathbb{Z}} H^0\left(X(N),\underline{\omega}^{\otimes n}\right) = R^{\bullet}_{N,holo}.$$

Then the ring $R^{\bullet}_{N,holo}$ has Krull dimension 2, since $X(N)$ is a projective curve. Let us fix any level N structure α_0 of the Tate curve. We denote by ψ the morphism

$$\begin{aligned} R^{\bullet}_{N,holo} &\longrightarrow K[\![q^{1/N}]\!] \\ f &\longrightarrow f(\mathrm{Tate}(q),\omega_{can},\alpha_0) \end{aligned}$$

obtained taking q-expansions at α_0 of homogeneous elements $f \in R^{\bullet}_{N,holo}$. Then $\ker\psi$ is a prime ideal since the image of ψ embeds in an integral domain. Moreover $\ker\psi$ cannot be maximal. Indeed, let Δ be the modular discriminant, then

$$\psi(\Delta) = \Delta(\mathrm{Tate}(q),\omega_{can},\alpha_0) = q^{1/N} + \dots$$

hence $q^{1/N}K[\![q^{1/N}]\!] \subseteq \mathrm{im}\psi \subseteq K[\![q^{1/N}]\!]$ has dimension al least one and $\ker\psi$ has codimension at least 1. We deduce that there exists $\mathfrak{m}$ maximal such that $\ker\psi \subseteq \mathfrak{m}$. Clearly $\ker\psi$ contains $(A-1)$ and since the zeroes of A are simple, we apply Lemma 4.1. and conclude that $(A-1)$ is prime. We have a chain of prime ideals:

$$0 \subset (A-1) \subseteq \ker\psi \subset \mathfrak{m} \subset R^{\bullet}_{N,holo}$$

and we conclude that the equality $(A-1) = \ker\psi$ must hold.
To conclude, also the map

$$R^{\bullet}_N \xrightarrow{\psi} K(\!(q)\!)$$

induced by taking q-expansions at α_0 of non necessarily holomorphic modular forms has kernel exactly $(A-1)$. Indeed, such a kernel clearly contains $(A-1)$. Let $f \in R_N^\bullet$ and assume that $\psi(f) = 0$. Up to multiplying each homogeneous term of f by powers of A we may assume that f is homogeneous i.e. $f \in H^0(Y(N), \underline{\omega}^{\otimes k})$ for some k. Then $\psi(f) = f_{\alpha_0}(q)$. If f is not holomorphic at all cusps, then f must have poles at them of finite order. Assume that r is the maximum of them, then $f\Delta^r$ is an holomorphic modular form and, taking q-expansion at α_0, $(f\Delta^r)(\mathrm{Tate}(q), \omega, \alpha_0) = f_{\alpha_0}(q)\Delta_{\alpha_0}(q) = 0$. It follows that $A-1$ divides $\Delta^r f$ in $R_{N,holo}^\bullet$ i.e. $\Delta^r f = (A-1)g$. Since Δ never vanishes on $Y(N)$ hence it's invertible in $R_N^\bullet$ we conclude $f = (A-1)g\Delta^{-r} \in (A-1)$. $\square$

Remark 4.2. *In the conclusion of the proof above we used the fact that the modular discriminant Δ is a cusp form, in particular it has a simple zero at each cusp. Indeed, let E/B be any elliptic curve over K. Then E admits locally a Weirstrass form. If $p \geq 2$ we have for example*

$$Y^2 = 4X^3 - g_4(E/B,\omega)X + g_6(E/B,\omega)$$

where X,Y are sections in $\mathcal{O}_E$ such that $\omega = \frac{dX}{Y}$. Note that we must have

$$\begin{aligned} X(E/B,\lambda\omega) &= \lambda^{-2}X(E/B,\omega), \\ Y(E/B,\lambda\omega) &= \lambda^{-3}Y(E/B,\omega), \\ g_4(E/B,\lambda\omega) &= \lambda^{-4}g_4(E/B,\omega), \\ g_6(E/B,\lambda\omega) &= \lambda^{-6}g_6(E/B,\omega). \end{aligned}$$

The discriminant of an elliptic curve is invariant under isomorphism and non zero. In the case above it can be defined as

$$\Delta(E/B,\omega) = \frac{g_4(E/B,\omega)^3 - g_6(E/B,\omega)^2}{12}$$

Then it's clear that it is homogeneous of degree -12 in ω. We can define Δ to be the rule which associates to $(E/B,\omega)$ such a discriminant and we obtain a modular form of weight 12. Moreover by Remark 3.6 we have

$$\Delta(\mathrm{Tate}(q), \omega_{can}, \alpha_0) = q^{1/N} \prod_{n\geq 1} \left(1 - q^{n/N}\right)^{24}.$$

for any level N structure α_0 of the Tate curve, i.e. Δ is a cusp form.

As a consequence, as in the level 1 case, multiplication by A does not effect q-expansions. We give the following definition:

Definition 4.1. *A form $f \in R_N^k$ is said to be of exact filtration k if it is not divisible by A in $R_N^\bullet$, or equivalently, if there is no form $f' \in R_N^{k'}$ of weight $k' < k$ which, at some cusp, has the same q-expansion of f.*

4.2 The main theorem and its corollaries

Theorem 4.1. *1. There exists a derivation $A\theta : R_N^\bullet \longrightarrow R_N^{\bullet+p+1}$ which increases degrees by $p+1$ and whose effect upon each q-expansion is $q\frac{d}{dq}$, namely*

$$(A\theta f)_{a_0}(q) = q\frac{d}{dq}(f_{a_0}(q))$$

for any $f \in R_N^\bullet$, a_0 a level N structure.

2. If $f \in R_N^k$ has exact filtration k and p does not divide k, then $A\theta f$ has exact filtration $k+p+1$ and in particular $A\theta f \neq 0$.

3. If $f \in R_N^{pk}$ and $A\theta f = 0$ then $f = g^p$ for a unique $g \in R_N^k$.

Before proving the theorem we list and prove its corollaries.

Corollary 4.1. *(1) The operator $A\theta$ maps the subring of holomorphic forms to the ideal of cusp forms.*

(2) If f is non zero and holomorphic of weight $1 \leq k \leq p-2$ then f has exact filtration k.

(3) If $1 \leq k \leq p-2$ the map $A\theta : R_{N,holo}^k \longrightarrow R_{N,holo}^{k+p+1}$ is injective.

(4) If f is non-zero and holomorphic of weight $p-1$ and vanishes at some cusp, then f has exact filtration $p-1$.

(5) (Determination of $\ker(A\theta)$). If $f \in R_N^k$ has $A\theta f = 0$ we can uniquely write $f = A^r g^p$ with $0 \leq r \leq p-1$, $r+k = 0 \mod p$ and $g \in R_N^l$ with $pl + r(p-1) = k$.

(6) In (5) above, if f is holomorphic (respectively a cusp form) so is g.

Proof. (1) It is clear looking at q-expansions.

(2) Assume f has not exact filtration k, then $f = Ag$ for some g holomorphic of weight $k-(p-1) < 0$. Then g is holomorphic of negative weight, hence $g = 0$.

(3) Assume $f \in R_N^k$ is non zero with $1 \leq k \leq p-2$. By point (2) f has exact filtration k. By part 2. of the theorem we must have $A\theta f \neq 0$.

(4) Let $f \in R_{N,holo}^{p-1}$, $f \neq 0$ and f vanishes at some cusp. Assume f has not filtration $p-1$, hence $f = gA$ for some form g of weight $k' = k-(p-1) = (p-1)-(p-1) = 0$. Hence g is holomorphic of weight zero, i.e. g is a section in $H^0(X(N), \mathcal{O}_{X(N)}) = K$. But then g is constant. Moreover f vanishes at some cusp and the q-expasion of A at all cusps is 1, so we must have $g = 0$ hence $f = 0$ and this is a contradiction.

(5) If $k = 0 \mod p$ i.e. $r = 0$ we're in case 3. of Theorem 4.1. To prove the statement we use induction on r. Assume $r > 1$, then $k \neq 0 \mod p$. But $A\theta f = 0$ so by part 2. of the main theorem f has not exact filtration k, i.e. there exists $h \in R_N^{k-p+1}$ such that $f = Ah$. Moreover $k+r = 0 \mod p$ yields $(k-p+1)+(r-1) = 0 \mod p$

and since f and h must have the same q-expansion we have $A\theta(h) = 0$. So we may apply the inductive hypothesis to h and get $h = A^{r-1}g^p$ for some $g \in R_N^l$ such that $lp + (r-1)(p-1) = k + 1 - p$. Hence $f = Ah = A^r g^p$ with $pl + r(p-1) = k$.

(6) It is clear looking at q-expansions.

$\square$

4.3 A derivation for the ring of modular forms

We begin the construction of the operator θ. We consider the relative Frobenius

$$\begin{tikzcd} \mathbb{E} \arrow[r, "Fr"] \arrow[rr, bend left, "F_{abs}"] \arrow[dr, "\pi"'] & \mathbb{E}^{(p)} \arrow[r, "\sigma"] \arrow[d, "\pi^{(p)}"] & \mathbb{E} \arrow[d, "\pi"] \\ & Y(N) \arrow[r, "F_{abs}"] & Y(N). \end{tikzcd}$$

It induces a morphism on the first de Rham cohomology:

$$Fr^* : H^1_{dR}(\mathbb{E}^{(p)}/Y(N)) \longrightarrow H^1_{dR}(\mathbb{E}/Y(N))$$

as follows. The associated map on structure sheaves $Fr^{\#} : \mathcal{O}_{\mathbb{E}^{(p)}} \longrightarrow Fr_*\mathcal{O}_{\mathbb{E}}$ extends to

$$Fr^{\#} : \Omega^{\bullet}_{\mathbb{E}^{(p)}/Y(N)} \longrightarrow Fr_*\Omega^{\bullet}_{\mathbb{E}/Y(N)}$$

and taking the functor $\mathbb{R}^1\pi_*^{(p)}$ we get

$$\mathbb{R}^1\pi_*^{(p)}Fr^{\#} : \mathbb{R}^1\pi_*^{(p)}\Omega^{\bullet}_{\mathbb{E}^{(p)}/Y(N)} \longrightarrow \mathbb{R}^1\pi_*^{(p)}Fr_*\Omega^{\bullet}_{\mathbb{E}/Y(N)} = \mathbb{R}^1\pi_*\Omega^{\bullet}_{\mathbb{E}/Y(N)}.$$

Let $\mathcal{U}$ be its image as a sheaf on $Y(N)$.

Lemma 4.3. *$\mathcal{U}$ and $H^1_{dR}(\mathbb{E}/Y(N))/\mathcal{U}$ are locally free $\mathcal{O}_{Y(N)}$-modules of rank* 1.

Proof. We have the Hodge filtration (Appendix B.2)

$$0 \longrightarrow \pi_*^{(p)}\Omega^1_{\mathbb{E}^{(p)}/Y(N)} \longrightarrow H^1_{dR}(\mathbb{E}^{(p)}/Y(N)) \longrightarrow R^1\pi_*^{(p)}\mathcal{O}_{\mathbb{E}^{(p)}} \longrightarrow 0.$$

We can then see $\pi_*^{(p)}\Omega^1_{\mathbb{E}^{(p)}/Y(N)} = \underline{\omega}_{E^{(p)}/Y(N)}$ as a subsheaf of $H^1_{dR}(\mathbb{E}^{(p)}/Y(N))$. In particular the restriction of Frobenius to it is zero. Let us check it locally. Assume that $Y(N)$ is Spec(B), for a K-algebra B. Then $\mathbb{E}$ is locally Spec(A) with

$$A = B[X,Y]/(f(X,Y))$$

a finitely generated B-algebra. It follows that $\mathbb{E}^{(p)}$ is locally Spec$(A^{(p)})$ where

$$A^{(p)} = A \otimes_{F_{abs}} B \cong B[X,Y]/(f^{(p)}(X,Y)).$$

The relative Frobenius on the structure sheaves $Fr^{\#} : \mathcal{O}_{E^{(p)}} \longrightarrow Fr_*\mathcal{O}_{\mathbb{E}}$ acts locally as

$$A^{(p)} \xrightarrow{Fr^{\#}} A$$
$$a \otimes_{F_{abs}} 1 \longrightarrow a^p.$$

We also have that $\pi_*\Omega^1_{\mathbb{E}/Y(N)}$ is locally $\Omega^1_{A/B}$ as a B-module. Hence $\pi_*^{(p)}\Omega^1_{\mathbb{E}^{(p)}/Y(N)}$ corresponds to $\Omega^1_{A^{(p)}/B} = \Omega^1_{A/B} \otimes_{F_{abs}} B$ as a B-module. As a consequence the Frobenius acts locally as $\Omega^1_{A^{(p)}/B} \xrightarrow{Fr^*} \Omega^1_{A/B}$ sending $da \otimes 1$ to $da^p = pa^{p-1}da = 0$.
Then Fr^* kills $\pi_*^{(p)}\Omega^1_{\mathbb{E}^{(p)}/Y(N)}$ and factors through the quotient

$$H^1_{dR}(\mathbb{E}^{(p)}/Y(N))/\pi_*^{(p)}\Omega^1_{\mathbb{E}^{(p)}/Y(N)} \cong R^1\pi_*^{(p)}\mathcal{O}_{\mathbb{E}^{(p)}}.$$

Here it induces the inclusion map in the conjugate filtration (Appendix B.3)

$$0 \longrightarrow R^1\pi_*^{(p)}\mathcal{O}_{\mathbb{E}^{(p)}} \longrightarrow H^1_{dR}(\mathbb{E}/Y(N)) \longrightarrow \pi_*^{(p)}\Omega^1_{\mathbb{E}^{(p)}/Y(N)} \longrightarrow 0.$$

Hence $\mathcal{U} \cong R^1\pi_*^{(p)}\mathcal{O}_{\mathbb{E}^{(p)}}$ and $H^1_{dR}(\mathbb{E}/Y(N))/\mathcal{U} \cong \pi_*^{(p)}\Omega^1_{\mathbb{E}^{(p)}/Y(N)}$ and we conclude since both are locally free sheaves of rank 1. □

Lemma 4.4. *The open subset $Y(N)^{Hasse} \subseteq Y(N)$ where the Hasse invariant is invertible is the largest open set where $\mathcal{U}$ splits the Hodge filtration i.e.*

$$H^1_{dR}(\mathbb{E}/Y(N)) \cong \underline{\omega} \oplus \mathcal{U}.$$

Proof. Let us work locally on $Y(N)$. Let $U \subseteq Y(N)$ be an open such that both $\underline{\omega}$, $R^1\pi_*\mathcal{O}_{\mathbb{E}}$ and $\mathcal{U}$ are free of rank 1. We pick a local basis $\{\omega,\eta\}$ of $H^1_{dR}(\mathbb{E}/Y(N))$ compatible with the Hodge filtration. This means that ω is a local basis for $\underline{\omega}$ and η projects to the dual basis $\overline{\eta}$ to ω of $R^1\pi_*\mathcal{O}_{\mathbb{E}}$. Similarly we choose by base change through the absolute Frobenius the local basis $\{\omega^{(p)},\eta^{(p)}\}$ for $H^1_{dR}(\mathbb{E}^{(p)}/Y(N))$. Then $Fr^*(\omega^{(p)}) = 0$ and

$$Fr^*(\eta^{(p)}) = B\omega + A\eta.$$

Moreover $Fr^*(\eta^{(p)}) = F^*_{abs}(\eta)$ [1]. Projecting to $R^1\pi_*\mathcal{O}_{\mathbb{E}}$, we have that by definition $F^*_{abs}(\eta)$ is sent to $A(\pi^{-1}(U)/U,\omega)\overline{\eta}$ and in the notation above $Fr^*(\eta^{(p)})$ projects to $A\overline{\eta}$ in $R^1\pi_*\mathcal{O}_{\mathbb{E}}$. Hence the coefficient A is exactly the Hasse invariant $A = A(\pi^{-1}(U)/U,\omega)$. A matrix for Fr^* on U is given by

$$\begin{pmatrix} 0 & B \\ 0 & A \end{pmatrix}$$

and $\mathcal{U}$ is locally generated by $B\omega+A\eta$. Then ω and $B\omega+A\eta$ span the whole $H^1_{dR}(\mathbb{E}/Y(N))$ on U if and only if A is invertible, i.e. $U \subseteq Y(N)^{Hasse}$. □

Remark 4.3. *Notice that since $\mathcal{U}$ is locally free of rank 1 and we chose an open U such that $\mathcal{U}$ is free isomorphic to $\mathcal{O}_{Y(N)}$, we must have that A and B in the proof above don't vanish at the same points, i.e. B does not vanish at the zeroes of A.*

[1] Here we denote by F^*_{abs} the map induced by the absolute Frobenius on the relative de Rham cohomology.

We can now begin the construction of θ. We have the splitting

$$\underline{\omega} \oplus \mathcal{U} = H^1_{dR}(\mathbb{E}/Y(N)).$$

Taking symmetric powers

$$\mathrm{Sym}^k H^1_{dR}(\mathbb{E}/Y(N)) = \underline{\omega}^{\otimes k} \oplus \left(\mathcal{U} \otimes \underline{\omega}^{\otimes(k-1)}\right) \oplus \cdots \oplus \mathcal{U}^{\otimes k}.$$

The Gauss-Manin connection (Appendix C) extends to a connection

$$\nabla : \mathrm{Sym}^k H^1_{dR}(\mathbb{E}/Y(N)) \longrightarrow \mathrm{Sym}^k H^1_{dR}(\mathbb{E}/Y(N)) \otimes \Omega^1_{Y(N)}.$$

We consider the composition of maps:

$$\begin{tikzcd}
\underline{\omega}^{\otimes k} \arrow[r, hook] \arrow[rrddd, dotted, bend right] & \mathrm{Sym}^{\mathrm{k}} H^1_{dR}(\mathbb{E}/Y(N)) \arrow[d, "\nabla"] & \\
& \mathrm{Sym}^{\mathrm{k}} H^1_{dR}(\mathbb{E}/Y(N)) \otimes \Omega^1_{Y(N)} \arrow[d, "KS"] & \\
& \mathrm{Sym}^{\mathrm{k}} H^1_{dR}(\mathbb{E}/Y(N)) \otimes \underline{\omega}^{\otimes 2} \arrow[r, equal] & \underline{\omega}^{\otimes(k+2)} \oplus \cdots \arrow[d, two heads] \\
& & \underline{\omega}^{\otimes k+2}
\end{tikzcd}$$

where the third arrow is the Kodaira-Spencer isomorphism in Appendix C.4. Taking global sections we get

$$\theta : H^0(Y(N)^{Hasse}, \underline{\omega}^{\otimes k}) \longrightarrow H^0(Y(N)^{Hasse}, \underline{\omega}^{\otimes k+2}).$$

Proposition 4.3. *The effect of θ on q-expansions is $q\frac{d}{dq}$.*

Proof. Let $f \in R^k_N$ and consider the triple $(\mathrm{Tate}(q), \omega_{can}, \alpha_0)$, where α_0 is a level N-structure on $\mathrm{Tate}(q)/K(\!(q^{1/N})\!)$. The q-expansion of f at the corresponding cusp is

$$f_{\alpha_0}(q) = f(\mathrm{Tate}(q), \omega_{can}, \alpha_0) \in K(\!(q^{1/N})\!).$$

Let $f_{\alpha_0}(q)\omega_{can}^{\otimes k}$ be the corresponding section in $H^0(K(\!(q^{1/N})\!), \underline{\omega}_{can}^{\otimes k})$. Since all the arrows above commute with base change, to conclude it suffices to check that $\theta(f_{\alpha_0}(q)\omega_{can}^{\otimes k})$ corresponds to $(q\frac{d}{dq}f_{\alpha_0}(q))\omega_{can}^{\otimes k+2}$. We fix a basis of $H^1_{dR}(\mathrm{Tate}(q)/K(\!(q^{1/N})\!))$ compatible withe the Hodge filtration i.e. $\{\omega_{can}, \eta_{can}\}$ such that the projection of η_{can} to $\underline{\omega}_{can}^{-1}$ is a dual basis to ω_{can}. Thanks to Lemma C.2 we can set $\eta_{can} = \nabla(q\frac{d}{dq})(\omega_{can})$. By Remark C.2. we can compute

$$\nabla(f_{\alpha_0}(q)\omega_{can}^{\otimes k}) = \nabla\left(q\frac{d}{dq}\right)(f_{\alpha_0}(q)\omega_{can}^{\otimes k}) \otimes \frac{dq}{q}$$
$$= \left(q\frac{d}{dq}f_{\alpha_0}(q)\omega_{can}^{\otimes k} + kf_{\alpha_0}(q)\omega_{can}^{\otimes k-1}\nabla\left(q\frac{d}{dq}\right)(\omega_{can})\right) \otimes \frac{dq}{q}.$$

With the choices above the image of the relative Frobenius $\mathcal{U}$ is spanned by $\nabla\left(q\frac{d}{dq}\right)(\omega_{can})$. Indeed by Remark 3.15. Fr^* kills $\omega_{can}^{(p)}$ and $Fr^*(\eta_{can}^{(p)}) = \eta_{can}$. Hence applying the Kodaira-Spencer morphism and projecting modulo $\mathcal{U}$ we obtain

$$\theta(f_{\alpha_0}(q)\omega_{can}^{\otimes k}) = q\frac{d}{dq}f_{\alpha_0}(q)\omega_{can}^{\otimes k} \otimes \omega_{can}^{\otimes 2} = q\frac{d}{dq}f_{\alpha_0}(q)\omega_{can}^{\otimes k+2}.$$

□

To conclude part 1) of the main theorem we state the following proposition:

Proposition 4.4. *There exists an operator $A\theta : R_N^k \longrightarrow R_N^{k+p+1}$ such that*

$$\begin{tikzcd}
H^0(Y(N)^{Hasse}, \underline{\omega}^{\otimes k}) \arrow[r, "\theta"] & H^0(Y(N)^{Hasse}, \underline{\omega}^{\otimes k+2}) \arrow[r, "A"] & H^0(Y(N)^{Hasse}, \underline{\omega}^{\otimes k+p+1}) \\
H^0(Y(N), \underline{\omega}^{\otimes k}) \arrow[u, hook] \arrow[rr, "A\theta"] & & H^0(Y(N), \underline{\omega}^{\otimes k+p+1}). \arrow[u, hook]
\end{tikzcd}$$

Proof. We compute a local expression for $A\theta$ on $Y(N)^{Hasse}$ and we prove that it can be extended to $Y(N)$. As above we work locally and restrict to an open $U \subseteq Y(N)^{Hasse}$ such that $\underline{\omega}$, $R^1\pi_*\mathcal{O}_{\mathbb{E}}$ and $\mathcal{U}$ are free of rank 1. We fix a basis ω for $\underline{\omega}$. Let ξ be the corresponding local basis of $\Omega^1_{Y(N)}$ through the Kodaira-Spencer isomorphism. Let $D \in \mathrm{Der}_k(\mathcal{O}_{Y(N)})$ be the dual derivation to ξ. Define $\omega' = \nabla(D)(\omega)$. Then $\{\omega, \omega'\}$ is a local basis of $H^1_{dR}(\mathbb{E}/Y(N))$ compatible with the Hodge filtration[2] i.e. the projection of ω' on $\underline{\omega}^{\otimes -1}$ is a basis of $R^1\pi_*\mathcal{O}_{\mathbb{E}}$ dual to ω. As in the proof of Lemma 4.4. after these choices, $\mathcal{U}$ is generated by

$$A\omega^{-1} + B\omega.$$

Moreover we fix a basis u of $\mathcal{U}$ such that the projection of u on $\underline{\omega}^{\otimes -1}$ is dual to ω. Hence $u = \lambda(A\omega' + B\omega)$ such that $\lambda A\omega'$ is dual to ω. This yields $\lambda = A^{-1}$ and

$$u = \omega' + \frac{B}{A}\omega.$$

Let $f \in H^0(Y(N)^{Hasse}, \underline{\omega}^{\otimes k})$. Assume that locally $f = f_1\omega^{\otimes k}$. We find a local expression for $\theta(f)$ computing $\theta(f_1\omega^{\otimes k})$.

$$\nabla(f_1\omega^{\otimes k}) = \nabla(D)(f_1\omega^{\otimes k}) \otimes \xi$$
$$= D(f_1)\omega^{\otimes k} \otimes \xi + kf_1\omega^{\otimes k-1}\nabla(D)(\omega) \otimes \xi.$$

[2]Let us denote by ω^{-1} the dual basis of $\underline{\omega}^{-1}$ to ω. We have $\nabla(\omega) = \nabla(D)(\omega) \otimes \xi$ and the composition of arrows defining the Kodaira-Spencer map gives us $\omega \to \nabla(D)(\omega) \otimes \xi \twoheadrightarrow \omega^{-1} \otimes \xi$. Projecting $\nabla(D)(\omega)$ is sent to ω^{-1}.

Applying the Kodaira-Spencer isomorphism we get:

$$D(f_1)\omega^{\otimes k+2} + kf_1\omega^{\otimes k+1} \otimes \nabla(D)(\omega) = D(f_1)\omega^{\otimes k+2} + kf_1\omega^{\otimes k+1} \otimes \left(-\frac{B}{A}\omega + u\right).$$

And projecting modulo $\mathcal{U}$

$$\theta(f_1\omega^{\otimes k}) = D(f_1)\omega^{\otimes k+2} - k\frac{B}{A}f_1\omega^{\otimes k+2}.$$

Hence multiplying by $A\omega^{\otimes p-1}$ we obtain

$$A\theta(f) = (AD(f_1) - kBf_1)\omega^{\otimes k+p+1}.$$

The local definition of $A\theta$ works everywhere and we may extend it to $Y(N)$. $\square$

We observe that we have defined $A\theta$ for $H^0(Y(N), \underline{\omega}^{\otimes k})$ for $k \geq 0$. To conclude, we extend the definition to R_N^k for negative k. Let $f \in H^0(Y(N), \underline{\omega}^{\otimes k})$ for $k < 0$. By Remark 4.2. we define

$$A\theta(f) := \frac{A\theta(f\Delta^{pr})}{\Delta^{pr}} \quad \text{for } r >> 0.$$

4.4 Conclusion

We now prove part 2. and 3. of the main theorem.

Proof.

1. Assume that $f \in R_N^k$ has exact filtration k. Then f is not divisible by A, hence for some zero $x \in Y(N)$ of A, the order of f at x is strictly smaller than the vanishing order of A at x. Fix an open neighbourhood of x as in the proof of Proposition 4.4. Then we can write locally $f = f_1\omega^{\otimes k}$ and

   $$A\theta f = (AD(f_1) - kf_1B)\omega^{\otimes k+p+1}.$$

   Under our assumption f_1 is not divisible by A and by Remark 4.3. B does not vanish at x. Hence if p does not divide k

   $$\mathrm{ord}_x(AD(f_1) - kf_1B) = \mathrm{ord}_x(f) < \mathrm{ord}_x(A)$$

   which yields that A does not divide $A\theta(f)$ i.e. $A\theta(f)$ has exact filtration $k+p+1$.

2. Let $f \in R_N^{pk}$ such that $A\theta f = 0$. We fix an open subset of U as above and write $f = f_1\omega^{pk}$. Then

   $$A\theta f = AD(f_1)\omega^{p+k+1} = 0.$$

   And this can happen if and only if $D(f_1) = 0$ where we chose D to be a local basis for $\mathrm{Der}_k(Y(N))$. We recall that $Y(N)$ is an affine smooth curve over K, which is algebraically closed, hence perfect. Hence $\mathcal{O}_{Y(N)}(U)$ is locally a finitely generated K-algebra of Krull dimension 1, that is, of the form $K[X,Y]/(g(X,Y))$ and the derivation D kills f_1. Hence $D(f_1) = 0$ yields that $f_1 = g_1^p$ for a unique $g_1 \in \mathcal{O}_{Y(N)}(U)$. Hence locally

   $$f = g_1^p\omega^{\otimes pk} = (g_1\omega^{\otimes k})^p.$$

We may cover $Y(N)$ by open subsets U of this form. By uniqueness the sections $(g_1\omega^{\otimes k})^p$ must coincide on intersections. As a consequence they glue to a unique $g \in H^0(Y(N), \underline{\omega}^{\otimes k})$ which verifies $f = g^p$.

$\square$

Appendix A

Cohomology of sheaves and de Rham Cohomology

A.1 Cohomology of sheaves

We introduce cohomology for a sheaf on a topological space X.

Proposition A.1. *Let $(X, \mathcal{O}_X)$ be a ringed space. The category $\mathrm{Mod}_{\mathcal{O}_X}$ of sheaves of $\mathcal{O}_X$-modules has enough injectives.*

Proof. Let $\mathcal{F}$ be an $\mathcal{O}_X$ module. The stalk $\mathcal{F}_x$ is a $\mathcal{O}_{X,x}$-module. The category of modules over a ring has enough injectives, so for any x we have an embedding $\mathcal{F}_x \longrightarrow \mathcal{I}_x$ with $\mathcal{I}_x$ an injective $\mathcal{O}_{X,x}$-module. Consider the one point ringed space $\{x\}$ with sheaf $\mathcal{I}_x$ and $j : \{x\} \longrightarrow X$ the inclusion. Then we define

$$\mathcal{I} = \prod_{x \in X} j_* \mathcal{I}_x$$

where j_* is the direct image functor, namely $j_*\mathcal{I}_x(U) = \mathcal{I}_x$ if $x \in U$, $j_*\mathcal{I}_x(U) = 0$ otherwise, for any $U \subseteq X$. For any sheaf of $\mathcal{O}_X$-modules we have

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{G}, j_*\mathcal{I}_x) \cong \mathrm{Hom}_{\mathcal{O}_{X.x}}(\mathcal{G}_x, \mathcal{I}_x).$$

Indeed to any morphism of sheaves ϕ we can associate the induced morphism on the stalks at x. Conversely, given an $\mathcal{O}_{X,x}$-linear map $f_x : \mathcal{G}_x \longrightarrow \mathcal{I}_x$, we define the morphism $f = (f_U)_{U \subseteq X}$ where $f_U : \mathcal{G}(U) \longrightarrow j_*\mathcal{I}_x(U)$ is such that: $f_U(s) = f_x(s_x)$ if $x \in U$ for a section s in $\mathcal{G}(U)$, $f_U : \mathcal{G}(U) \longrightarrow 0$ otherwise. The two are clearly inverse to each other. Hence

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{I}) \cong \prod_{x \in X} \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F}, j_*\mathcal{I}_x) \cong \prod_{x \in X} \mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{F}_x, \mathcal{I}_x).$$

Then the embeddings $\mathcal{F}_x \longrightarrow \mathcal{I}_x$ give us a morphism $\mathcal{F} \longrightarrow \mathcal{I}$ which is clearly injective. To conclude $\mathcal{I}$ is injective, indeed

$$\mathrm{Hom}_{\mathcal{O}_X}(-, \mathcal{I}) \cong \prod_{x \in X} \mathrm{Hom}_{\mathcal{O}_{X,x}}(-, \mathcal{I}_x)$$

is exact since $\mathrm{Hom}_{\mathcal{O}_{X,x}}(-, \mathcal{I}_x)$ is exact. $\square$

Corollary A.1. *Let X be a topological space. The category of abelian sheaves $\mathfrak{Ab}(X)$ has enough injectives.*

Proof. We consider the ringed space $(X, \mathcal{O}_X)$ where $\mathcal{O}_X$ is the constant sheaf associated to $\mathbb{Z}$, then $\mathrm{Mod}_{\mathcal{O}_X} = \mathfrak{Ab}(X)$. $\square$

Now it makes sense to give the following definition.

Definition A.1. *Let X be a topological space and $\Gamma(X, -) : \mathfrak{Ab}(X) \longrightarrow \mathfrak{Ab}$ the global section functor. The cohomology functors $H^i(X, -)$ are defined as the right derived functors of $\Gamma(X, -)$, namely $H^i(X, -) := R^i\Gamma(X, -)$. For any abelian sheaf $\mathcal{F}$, $H^i(X, \mathcal{F})$ are the cohomology groups of F.*

Cohomology of a sheaf $\mathcal{F}$ can be computed using flasque resolutions.

Lemma A.1. *Let $(X, \mathcal{O}_X)$ be a ringed space. Any injective $\mathcal{O}_X$-module is flasque.*

Proof. Let $V \subseteq U$ be open subsets of X. We have an inclusion of $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{O}_{X|_V} \longrightarrow \mathcal{O}_{X|_U}$$

where $\mathcal{O}_{X|_U}$ is the sheaf of rings on an open U obtained by the restriction of $\mathcal{O}_X$ at U, extended to zero outside U. Applying $\mathrm{Hom}_{\mathcal{O}_X}(-, \mathcal{I})$, we have an exact sequence

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_{X|_U}, \mathcal{I}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_{X|_V}, \mathcal{I}) \longrightarrow 0.$$

To conclude we have $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_{X|_U}, \mathcal{I}) \cong \mathcal{I}(U)$. Indeed to any section $s \in \mathcal{I}(U)$ we associate the morphism $\mathcal{O}_{X|_U} \longrightarrow \mathcal{I}$ defined as follows. For any W open in U, the map $\mathcal{O}_X(W) \longrightarrow \mathcal{I}(W)$ is the unique $\mathcal{O}_X(W)$-linear map sending 1 to $s_{|_W}$. Conversely, any morphism $\mathcal{O}_{X|_U} \longrightarrow \mathcal{I}$, gives a $\mathcal{O}_X(U)$-linear map to $\mathcal{I}(U)$, uniquely determined by a section in $\mathcal{I}(U)$. Hence we have that $\mathcal{I}(U) \longrightarrow \mathcal{I}(V) \longrightarrow 0$. $\square$

Proposition A.2. *Let $\mathcal{F}$ be a flasque sheaf on X, then $H^i(X, \mathcal{F}) = 0$ for all $i \geq 1$.*

Proof. We prove it by induction on i. Let $\mathcal{I}$ be an injective object such that $\mathcal{F}$ embeds into $\mathcal{I}$. Then we have a short exact sequence $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I} \longrightarrow \mathcal{G} \longrightarrow 0$ where the sheaf $\mathcal{G}$ is flasque. Moreover we have the exact sequence of global sections

$$0 \longrightarrow \Gamma(X, \mathcal{F}) \longrightarrow \Gamma(X, \mathcal{I}) \longrightarrow \Gamma(X, \mathcal{G}) \longrightarrow 0$$

which proves the statement for $i = 0$. The long exact sequence of cohomology together with the fact that $H^i(X, \mathcal{I}) = 0$ for $i > 0$ yields

$$\cdots \longrightarrow 0 \longrightarrow H^i(X, \mathcal{G}) \longrightarrow H^{i+1}(X, \mathcal{F}) \longrightarrow 0 \cdots$$

Using the inductive hypotesis we have $H^i(X, \mathcal{G}) = 0$ and we conclude $H^{i+1}(X, \mathcal{F}) = 0$. $\square$

Remark A.1. *This proves that any flasque sheaf is acyclic hence we can compute cohomology using flasque resolutions.*

A.2 Čech cohomology

Let X be a topological space and let $\mathcal{U} = \{U_i\}_{i \in I}$ be an open covering of X. For any finite indexes $i_0 \dots i_p \in I$ we denote $U_{i_0} \cap \cdots \cap U_{i_p} = U_{i_0 \dots i_p}$. Let $\mathcal{F}$ be an abelian sheaf on X. We build the Čech complex as follows: for each $p \geq 0$

$$C^p(\mathcal{U}, \mathcal{F}) = \prod_{i_0 < \cdots < i_p} \mathcal{F}(U_{i_0 \dots i_p})$$

$$d^p : C^p(\mathcal{U}, \mathcal{F}) \longrightarrow C^{p+1}(\mathcal{U}, \mathcal{F})$$

$$\alpha \longrightarrow d^p(\alpha)$$

where

$$(d^p(\alpha))_{i_0 \dots i_{p+1}} = \sum_{k=0}^{p+1} (-1)^k \alpha_{i_0 \dots \hat{i_k} \dots i_{p+1}|_{U_{i_0 \cdots i_{p+1}}}}.$$

Here the hat on the index means that we cancel it from the string.

Definition A.2. *Let X be a topological space and $\mathcal{U}$ be an open covering of X. We define the p-th Čech cohomology group*

$$\check{H}^p(\mathcal{U}, \mathcal{F}) = H^p(C^\bullet(\mathcal{F}, \mathcal{U})).$$

Lemma A.2. *For any X, $\mathcal{U}, \mathcal{F}$ as above $\check{H}^0(\mathcal{U}, \mathcal{F}) = \Gamma(X, F)$.*

Proof. Let

$$d^0 : C^0(\mathcal{U}, \mathcal{F}) = \prod_{i \in I} F(U_i) \longrightarrow C^1(\mathcal{U}, \mathcal{F}) = \prod_{i,j} \mathcal{F}(U_i \cap U_j)$$

$$(x_i)_{i \in I} \longrightarrow (x_{j|_{U_{ij}}} - x_{i|_{U_{ij}}})_{i,j}.$$

Then $\check{H}^0(\mathcal{U}, \mathcal{F}) = H^0(C^\bullet(\mathcal{U}, \mathcal{F})) = \ker d^0$ and by the properties of sheaves

$$0 \longrightarrow F(X) \longrightarrow \prod_{i \in I} F(U_i) \longrightarrow \prod_{i,j} \mathcal{F}(U_i \cap U_j)$$

is exact hence $F(X) = \Gamma(X, \mathcal{F}) = \ker d^0$. □

Definition A.3. *Let X be a topological space. For any open $U \subseteq X$ we let $f : U \longrightarrow X$ be the inclusion map. We construct a complex of sheaves $\mathcal{C}^\bullet(\mathcal{U}, \mathcal{F})$ on X as follows: we fix an open covering $\mathcal{U}$ of X and for each $p \geq 0$ we let*

$$\mathcal{C}^p(\mathcal{U}, \mathcal{F}) = \prod_{i_0 < \cdots < i_p} f_*(\mathcal{F}_{|_{U_{i_0 \cdots i_p}}}) \quad \text{and} \quad d : \mathcal{C}^p(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{C}^{p+1}(\mathcal{U}, \mathcal{F})$$

where d acts on sections as described above. Then clearly $\Gamma(X, \mathcal{C}^p(\mathcal{U}, \mathcal{F})) = C^p(\mathcal{U}, \mathcal{F})$

Lemma A.3. *For any sheaf of abelian groups $\mathcal{F}$ on X, the complex $\mathcal{C}^\bullet(\mathcal{U}, \mathcal{F})$ is a resolution of $\mathcal{F}$ i.e. we have natural maps such that*

$$0 \longrightarrow \mathcal{F} \xrightarrow{\varepsilon} \mathcal{C}^0(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{C}^1(\mathcal{U}, \mathcal{F}) \longrightarrow \dots \tag{A.1}$$

is exact.

Proof. We build $\varepsilon : \mathcal{F} \longrightarrow \prod_{i\in I} f_*(\mathcal{F}_{|U_i})$ considering $\mathcal{F} \longrightarrow f_*\mathcal{F}_{|U_i}$ for any i and taking the direct product. The exactess of the first step follows from the sheaf axioms for $\mathcal{F}$. Indeed for any $V \subseteq X$ we have that

$$0 \longrightarrow \mathcal{F}(V) \longrightarrow \prod_{i\in I} f_*\mathcal{F}_{|U_i}(V) = \prod_{i\in I} \mathcal{F}(V\cap U_i) \longrightarrow \prod_{i,j\in I} f_*\mathcal{F}_{|U_i\cap U_j}(V) = \prod_{i,j\in I} \mathcal{F}(V\cap U_i\cap U_j)$$

is exact since $V \cap U_i$ is an open cover for V. To show the exactness of the complex we check it on stalks. Let $x \in X$, $x \in U_j$ for some j. For each $p \geq 1$ we build

$$k_x^p : \mathcal{C}^p(\mathcal{U}, \mathcal{F})_x \longrightarrow \mathcal{C}^{p-1}(\mathcal{U}, \mathcal{F})_x$$

as follows. Any $\alpha_x \in \mathcal{C}^p(\mathcal{U}, \mathcal{F})_x$ is the class of an element $\alpha \in \mathcal{C}^p(\mathcal{U}, \mathcal{F})(V)$ for an open $x \in V$. We may assume $V \subseteq U_j$. We let $(k^p(\alpha))_{i_0\ldots i_{p-1}} = \alpha_{ji_0\ldots i_{p-1}}$. Notice that it makes sense since $\alpha \in \prod_{|I|=p} \mathcal{F}(U_I \cap V)$ and $U_{i_0\ldots i_{p-1}} \cap V = U_{i_0\ldots i_{p-1}} \cap U_j \cap V = U_{ji_0\ldots i_{p-1}} \cap V$. One has $\alpha_x = k_x^{p+1} d_x^p \alpha_x + d_x^{p-1} k_x^p \alpha_x$. Indeed

$$(k^{p+1}d^p\alpha)_{i_0\ldots i_p} = (d^p\alpha)_{ji_0\ldots i_p} = \alpha_{i_0\ldots i_p|_{U_{i_0\ldots i_p}}} + \sum_{l=0}^{p} (-1)^{l+1} \alpha_{ji_0\ldots\hat{i_l}\ldots i_p|_{U_{i_0\ldots i_p}}},$$

$$(d^{p-1}k^p\alpha)_{i_0\ldots i_p} = \sum_{l=0}^{p} (-1)^l (k^p(\alpha))_{i_0\ldots\hat{i_l}\ldots i_p|_{U_{i_0\ldots i_p}}} = \sum_{l=0}^{p} (-1)^l \alpha_{ji_0\ldots\hat{i_l}\ldots i_p|_{U_{i_0\ldots i_p}}}.$$

Summing the two and restricting to $U_{i_0\ldots i_p} \cap V$ we obtain α. As a consequence we get equality on stalks. The complex of stalks is nullhomotopic and we conclude that it has zero cohomology groups i.e. it is exact. □

Proposition A.3. *Let X be a topological space and $\mathcal{F}$ a flasque sheaf on X, $\mathcal{U}$ an open covering of F. Then $\check{H}^p(\mathcal{U}, \mathcal{F}) = 0$ for $p > 0$.*

Proof. Let us consider the resolution above $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{C}^0(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{C}^1(\mathcal{U}, \mathcal{F}) \longrightarrow \ldots$ then $\mathcal{C}^i(\mathcal{U}, \mathcal{F}) = \prod_{U_I} f_*\mathcal{F}_{|U_I}$ is flasque ($\mathcal{F}_{|U_I}$ is flasque, f_* preserves flasque sheaves and product of flasque is flasque). So we can compute the usual cohomology groups using this resolution. We know $H^i(X, \mathcal{F}) = 0$ for $i > 0$ since $\mathcal{F}$ is flasque. Taking global sections we obtain the Čech complex

$$0 \longrightarrow F(X) \longrightarrow \Gamma(X, \mathcal{C}^0(\mathcal{U}, \mathcal{F})) \longrightarrow \Gamma(X, \mathcal{C}^1(\mathcal{U}, \mathcal{F})) \longrightarrow \ldots$$

and taking cohomologies we recover $\check{H}^i(\mathcal{U}, \mathcal{F})$. But

$$H^i(\Gamma(X, \mathcal{C}^\bullet(\mathcal{U}, \mathcal{F}))) = R^i\Gamma(X, \mathcal{F}) = H^i(X, \mathcal{F}) = 0$$

for $i > 0$ then $\check{H}^i(\mathcal{U}, \mathcal{F}) = 0$. □

Proposition A.4. *Let X be a topological space and $\mathcal{F}$ a sheaf on X, $\mathcal{U}$ an open covering of X. For every $p \geq 0$ we have a natural map:*

$$\check{H}^p(\mathcal{U}, \mathcal{F}) \longrightarrow H^p(X, \mathcal{F}).$$

Proof. Let $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I}^\bullet$ be an injective resolution for $\mathcal{F}$ and $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{C}^\bullet(X, \mathcal{F})$ the resolution above. Using injectivity we build a morphism of complexes

$$\phi^\bullet : \mathcal{C}^\bullet(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{I}^\bullet$$

as follows. Since $\mathcal{I}^0$ is injective we have the existence of ϕ^0 such that

$$\begin{tikzcd} \mathcal{F} \arrow[r, hook] \arrow[d] & \mathcal{C}^0(\mathcal{U}, \mathcal{F}) \arrow[dl, dotted, "\phi^0"] \\ \mathcal{I}^0 & \end{tikzcd}$$

commutes. Similarly let

$$K^0 = \ker\left(\mathcal{C}^1(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{C}^2(\mathcal{U}, \mathcal{F})\right) \cong \operatorname{im}\left(\mathcal{C}^0(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{C}^1(\mathcal{U}, \mathcal{F})\right).$$

Applying the universal property of cokernels we obtain $\widetilde{\phi}^1$ such that

$$\begin{tikzcd} \mathcal{F} \arrow[r, hook] \arrow[dr] & \mathcal{C}^0(\mathcal{U}, \mathcal{F}) \arrow[r] \arrow[d, "\phi^0"] & K^0 \arrow[d, "\widetilde{\phi^1}"] \\ & \mathcal{I}^0 \arrow[r] & \mathcal{I}^1. \end{tikzcd}$$

Moreover injectivity of $\mathcal{I}^1$ yields the existence of $\widetilde{\phi}^1$ such that

$$\begin{tikzcd} K^0 \arrow[r, hook] \arrow[d, "\widetilde{\phi^1}"] & \mathcal{C}^1(\mathcal{U}, \mathcal{F}) \arrow[dl, dotted, "\phi^1"] \\ \mathcal{I}^1 & \end{tikzcd} .$$

commutes. Applying iteratively the argument above we build $\phi^i : \mathcal{C}^i(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{I}^i$. Taking global sections and cohomology we conclude

$$H^i(\Gamma(X, \mathcal{C}^\bullet(\mathcal{U}, \mathcal{F}))) = \check{H}^i(\mathcal{U}, \mathcal{F}) \overset{H^i(\Gamma(X,\phi^\bullet))}{\longrightarrow} H^i(\Gamma(X, \mathcal{I}^\bullet)) = H^i(X, \mathcal{F}).$$

□

Theorem A.1. *Let X be a noetherian, separated scheme. Let $\mathcal{U}$ be a finite affine cover of X and $\mathcal{F}$ a quasi coherent sheaf on X. Then for any $p \geq 0$*

$$\check{H}^p(\mathcal{U}, \mathcal{F}) \cong H^p(X, \mathcal{F}).$$

Proof. For $p = 0$ we have $\check{H}^0(\mathcal{U}, \mathcal{F}) = \Gamma(X, \mathcal{F}) = H^0(X, \mathcal{F})$. For the general case, we embed $\mathcal{F}$ into a flasque sheaf $\mathcal{G}$ and get a short exact sequence of quasi-coherent sheaves

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{R} \longrightarrow 0.$$

Since $\mathcal{F}$ is quasi-coherent and $U_{i_0 \dots i_p}$ is affine we obtain for any index $I = i_0 \dots i_p$ that

$$0 \longrightarrow \mathcal{F}(U_I) \longrightarrow \mathcal{G}(U_I) \longrightarrow \mathcal{R}(U_I) \longrightarrow 0.$$

is exact. As a consequence we have a short exact sequence of complexes

$$0 \longrightarrow C^\bullet(\mathcal{U}, \mathcal{F}) \longrightarrow C^\bullet(\mathcal{U}, \mathcal{G}) \longrightarrow C^\bullet(\mathcal{U}, \mathcal{R}) \longrightarrow 0.$$

Taking cohomologies, recalling that $\mathcal{G}$ flasque implies $\check{H}^p(\mathcal{U}, \mathcal{G}) = 0$ for $p \geq 1$, we have

$$0 \longrightarrow \check{H}^0(\mathcal{U}, \mathcal{F}) \longrightarrow \check{H}^0(\mathcal{U}, \mathcal{G}) \longrightarrow \check{H}^0(\mathcal{U}, \mathcal{R}) \longrightarrow \check{H}^1(\mathcal{U}, \mathcal{F}) \longrightarrow 0$$

and

$$\check{H}^{p-1}(\mathcal{U}, \mathcal{R}) \cong \check{H}^p(\mathcal{U}, \mathcal{F}).$$

Hence

$$\begin{tikzcd}
0 \arrow[r] & \check{H}^0(\mathcal{U}, \mathcal{F}) \arrow[r] \arrow[d, equal] & \check{H}^0(\mathcal{U}, \mathcal{G}) \arrow[r] \arrow[d, equal] & \check{H}^0(\mathcal{U}, \mathcal{R}) \arrow[r] \arrow[d, equal] & \check{H}^1(\mathcal{U}, \mathcal{F}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^0(\mathcal{U}, \mathcal{F}) \arrow[r] & H^0(\mathcal{U}, \mathcal{G}) \arrow[r] & H^0(\mathcal{U}, \mathcal{R}) \arrow[r] & H^1(\mathcal{U}, \mathcal{F}) \arrow[r] & 0
\end{tikzcd}$$

which yields

$$\check{H}^1(\mathcal{U}, \mathcal{F}) \cong H^1(\mathcal{U}, \mathcal{F}).$$

We conclude by induction on p, using that $\check{H}^{p-1}(\mathcal{U}, \mathcal{R}) \cong \check{H}^p(\mathcal{U}, \mathcal{F})$ and the fact that $\mathcal{R}$ is quasi-coherent. □

Remark A.2. *If X is affine we easily conclude thanks to Theorem A.1 that for any quasi coherent $\mathcal{O}_X$-module $\mathcal{F}$ on X*

$$H^i(X, \mathcal{F}) = 0$$

since we may compute Čech cohomology choosing as affine cover $\mathcal{U} = \{X\}$. Hence any quasi coherent sheaf on an affine scheme is acyclic.
Moreover let X be any noetherian, separated scheme. For any affine open U_i we denote by $f : U_i \hookrightarrow X$ the corresponding immersion. It is an affine morphism so f_* is exact. Then $\mathcal{F}_{|U_i}$ is quasi coherent on an affine scheme and hence acyclic. We conclude that also $f_*\mathcal{F}_{|U_i}$ is acyclic on X. Then $\prod_I f_*\mathcal{F}_{|U_I}$ is acyclic and (A.1) is an acyclic resolution of $\mathcal{F}$.

A.3 An explicit computation for elliptic curves

Sheaf cohomology for quasi-coherent sheaves over quasi-compact and separated schemes can be computed using Čech cohomology. We will give an explicit example in the case of an elliptic curve over a field.
Let k be a field. For simplicity we assume $k = \overline{k}$ and char$k \neq 2, 3$. Let E/k be an elliptic curve. Then we may assume

$$E = \mathrm{Proj}\left(k[X, Y, Z]/(Y^2Z - X^3 - aXZ^2 - bZ^3)\right).$$

We recall that ${\Omega^1}_{E/k}$ is a locally free sheaf of rank 1. In the affine open $\{Z \neq 0\}$ E is locally

$$\mathrm{Spec}\left(k[X, Y]/(Y^2 - X^3 - aX - b)\right)$$

and a basis is given by $\omega = \frac{dX}{Y}$. We notice that $Y^2 = X^3 + aX + b$ yields

$$2Y dY = dX(3X^2 + a)$$

hence:

$$\frac{dX}{Y} = \frac{2dY}{3X^2 + a}$$

and $3X^2 + a \neq 0$ if $Y = 0$ since $X^3 + aX + b$ has no multiple roots. Hence we may write

$$H^0(E, \Omega^1{}_{E/k}) = \frac{dX}{Y} k.$$

Moreover we recall that $H^0(E, \mathcal{O}_E) = \mathcal{O}_E(E) = k$. Let us fix $P \neq Q \in E$ distinct points. If we set $U = E \setminus \{P\}$ and $V = E \setminus \{Q\}$ then $\mathcal{U} = \{U, V\}$ is an affine cover for the elliptic curve. The associated Čech complex is

$$\begin{aligned} \mathcal{O}_E(U) \oplus \mathcal{O}_E(V) &\xrightarrow{d^0} \mathcal{O}_E(U \cap V) \\ (f_U, f_V) &\longrightarrow f_{V|_{U\cap V}} - f_{U|_{U\cap V}}. \end{aligned}$$

Then it is clear that $H^n(E, \mathcal{O}_E) = 0$ for all $n \geq 2$. So we're only left to determine

$$H^1(E, \mathcal{O}_E) = \frac{\mathcal{O}_E(U \cap V)}{\mathrm{im} d^0}$$

where $\mathrm{im} d^0 = \{f_{UV} \in \mathcal{O}_E(U \cap V),\ f_{UV} = f_{V|_{U\cap V}} - f_{U|_{U\cap V}}\}$. We recall the following result.

Theorem A.2 (Riemann-Roch). *Let $D = \sum_P n_P P$ be a divisor on E and for any open $U \subseteq E$ let*

$$\mathcal{L}_D(U) = \{f \in k(E) \ : \mathrm{ord}_P(f) \geq -n_P,\ P \in U\}$$

and let $l(D) = \dim_k(H^0(E, \mathcal{L}_D))$. If $D > 0$

$$l(D) = \mathrm{deg} D.$$

Proof. For a proof and a more general statement see [4] Chapter 4. □

Now we notice that if $D = (P)$ then $l(D) = 1$ and since $1 \in \mathcal{L}_D(E)$ we must have $\mathcal{L}_{(P)}(E) = k$ i.e. there are no regular functions on E with only one pole.
Moreover let us consider $D = (P) + (Q)$. If $f \in \mathcal{L}_D(E)$ then $\mathrm{ord}_P(f) \geq 1$, $\mathrm{ord}_Q(f) \geq 1$ and $\mathrm{ord}_R(f) \geq 0$ for $R \neq P, Q$. But $l(D) = 2$ yields the existence of $f \in \mathcal{L}_D(E) \setminus k$. So f has at least one pole and we conclude by the observation above that $\mathrm{ord}_P f = \mathrm{ord}_Q f = -1$. Then $\mathcal{L}_D(E) = k \oplus fk$ and moreover $1, f \in \mathcal{O}_E(U \cap V)$.

Proposition A.5. *We have that*

$$H^1(E, \mathcal{O}_E) = [f]k.$$

In particular $H^1(E, \mathcal{O}_E)$ is a one dimensional k-vector space.

Proof. By definition $H^1(E,\mathcal{O}_E) = \frac{\mathcal{O}_E(U\cap V)}{\{f_{U_{|U\cap V}} - f_{V_{|U\cap V}}\}}$. We claim that $[1]=0$ and $[f]\neq 0$. Indeed, $1_{|U\cap V} \in \mathcal{O}_E(U\cap V)$ and $1_{|U\cap V} = (1_{|V})_{|U\cap V} - (0_{|U})_{|U\cap V}$ so it is clearly in $\mathrm{im}d^0$. Moreover $[f]\neq 0$. Assume $f = f_{U_{|U\cap V}} - f_{V_{|U\cap V}}$ for $f_U \in \mathcal{O}_E(U)$ and $f_V \in \mathcal{O}_E(V)$. Notice $\mathrm{ord}_Q(f_U)\geq 0$ and $\mathrm{ord}_P(f_V)\geq 0$. Hence

$$-1 = \mathrm{ord}_P(f) = \mathrm{ord}_P(f_{U_{|U\cap V}} - f_{V_{|U\cap V}}) = \mathrm{ord}_P(f_U)$$

and f_U is a regular function on $E\setminus\{P\}$ which has a simple pole at P and we conclude that it must then be constant. Similarly

$$-1 = \mathrm{ord}_Q(f) = \mathrm{ord}_Q(f_{U_{|U\cap V}} - f_{V_{|U\cap V}}) = \mathrm{ord}_Q(f_V)$$

hence f_V is regular on $E\setminus\{Q\}$ and has a simple pole at Q, then it must be constant. So f is constant and this is a contradiction. Thus we have $[f]k \subseteq H^1(E,\mathcal{O}_E)$. To conclude we check that equality holds. We consider multiple cases:

i) Let $[g]\in H^1(E,\mathcal{O}_E)$, $g\in\mathcal{O}_E(U\cap V)$. Suppose $\mathrm{ord}_P g = -1 = \mathrm{ord}_Q g$. Then $g\in\mathcal{L}_D(E)$ hence $g = 1\cdot a + f\cdot b$. We conclude that

$$[g] = [1]a + [f]b = [f]b \in [f]k.$$

ii) Let $g\in\mathcal{O}_E(U\cap V)$. Suppose $\mathrm{ord}_P g\leq -2$ and $\mathrm{ord}_Q g\geq 0$. Then we claim that $[g]=0$. Indeed since g is holomorphic at Q we have that g is regular on $U = E\setminus\{P\}$. Hence $g = (g_{|U})_{|U\cap V} - (0_{|V})_{|U\cap V} \in \mathrm{im}d^0$ i.e. $[g]=0$.

iii) Let $g\in\mathcal{O}_E(U\cap V)$. Suppose $\mathrm{ord}_p g = -2$ and $\mathrm{ord}_Q g = -1$. Let T be a uniformizer at P. Then

$$g_P = \frac{a}{T^2} + \frac{b}{T} + \dots$$

for some $a,b\in k$. Let $D' = 2(P)$. By Theorem A.2.

$$\dim_k(H^0(E,\mathcal{L}_{\mathcal{D}'})) = \deg D' = 2.$$

So there exists a non constant $h\in H^0(E,\mathcal{L}_{D'})$, namely $\mathrm{ord}_P h\geq -2$ and $\mathrm{ord}_R h\geq 0$ for $R\neq P$. Moreover we must have $\mathrm{ord}_P h = -2$ otherwise h would be constant. Hence

$$h_P = \frac{c}{T^2} + \frac{d}{T} + \dots$$

with $c\neq 0$. We also have that h is regular on U i.e. $h_{|U}\in\mathcal{O}_E(U)$. We set $g_1 = g + \left(\frac{-a}{c}\right) h_{|U\cap V}$ then $g_1 = g + \left(\frac{-a}{c}\right) h_{|U\cap V} - 0 = g + \left(\frac{-a}{c}\right) h_{|U\cap V} - 0_{|V_{|U\cap V}}$ i.e. $[g_1] = [g]$. Furthermore

$$g_{1P} = g_P + \left(\frac{-a}{c}\right) h_P = \frac{a}{T^2} + \frac{b}{T} + \dots - \frac{a}{c}\frac{c}{T^2} - \frac{a}{c}\frac{d}{T} + \dots$$

namely $\mathrm{ord}_P(g_1)\geq -1$ and $\mathrm{ord}_Q(g_1) = -1$ since g has a pole of order 1 at Q and h is regular at Q. This yields $g_1\in H^0(E,\mathcal{L}_D)$ and $g_1 = \alpha\cdot 1 + \beta\cdot f$. We conclude $[g_1] = [g] = \beta[f]\in[f]k$ for $\beta\in k$.

iv) Let $g \in \mathcal{O}_E(U \cap V)$ and suppose $\mathrm{ord}_P g = -n$ and $\mathrm{ord}_Q g = -1$. We use induction on n. The case $n = 2$ has been proved above. Assume $n > 2$ and consider the divisor $n(P)$. Then $\dim_k(H^0(E, \mathcal{L}_{n(P)})) = n$. Notice that $\dim_k H^0(E, \mathcal{L}_{(n-1)(P)})) = n - 1$ and $\mathcal{L}_{(n-1)(P)} \subset \mathcal{L}_{n(P)}$ hence there exists $h \in \mathcal{L}_{n(P)} \setminus \mathcal{L}_{(n-1)(P)}$. Then we must have $\mathrm{ord}_P h = -n$ and $\mathrm{ord}_R h \geq 0$ for $R \neq P$. Let

$$h_P = \frac{c}{T^n} + \frac{d}{T^{n-1}} + \dots$$

for $c \neq 0$ in k and

$$g_P = \frac{a}{T^n} + \frac{b}{T^{n-1}} + \dots$$

Notice that h is regular on $E \setminus \{P\} = U$. We set

$$g_1 = g - \frac{a}{c} h_{|U \cap V}.$$

Then $g_1 = g - \frac{a}{c} h_{|U \cap V} - (0_{|V})_{|U \cap V}$ namely $[g_1] = [g]$. Moreover

$$g_{1P} = \frac{a}{T^n} + \frac{b}{T^{n-1}} + \dots - \frac{a}{c} \frac{c}{T^n} + \dots$$

i.e. $\mathrm{ord}_P g_1 \geq -(n-1)$ and $\mathrm{ord}_Q g_1 = ord_Q g = -1$ since h is holomorphic at Q. By the inductive hypothesis $[g] = [g_1] \in [f]k$.

v) Finally let $\mathrm{ord}_P g = -n$ and $\mathrm{ord}_Q g = -m$. We use induction on m. If $m = 1$ it's the case above. Assume $m > 1$. As above we consider $m(Q)$ and apply Riemann-Roch Theorem to it. We find $h \in H^0(E, \mathcal{L}_{m(Q)}) \setminus H^0(E, \mathcal{L}_{(m-1)(Q)})$ and we must have that $\mathrm{ord}_Q h = -m$ and h is regular elsewhere, namely $h \in \mathcal{O}_E(V)$. We fix a uniformizer at Q and we write

$$h_Q = \frac{c}{T^m} + \frac{d}{T^{m-1}} + \dots$$

and

$$g_Q = \frac{a}{T^m} + \frac{b}{T^{m-1}} + \dots$$

and we set $g_1 = g - \frac{a}{c} h_{|U \cap V} - (0_{|U})_{|U \cap V}$. Then $[g] = [g_1]$ and g_1 has a pole of order $-n$ at P since h is holomorphic in V and g has a pole of order $-n$ at P. Moreover $\mathrm{ord}_Q g_1 \geq -(m-1)$. We use the inductive hypothesis to conclude $[g] = [g_1] \in [f]k$.

□

Remark A.3. *Through our computation we found that*

$$\dim_k H^1(E, \mathcal{O}_E) = 1 = \dim_k H^0(E, \Omega^1_{E/k}).$$

Indeed the two are dual by Serre's duality.

A.4 Higher direct image

We go back to our more general setting and give the following definition.

Definition A.4. *Let $f : X \longrightarrow Y$ be a continuous map of topological spaces. The higher direct image functor $R^i f_* : \mathfrak{Ab}(X) \longrightarrow \mathfrak{Ab}(Y)$ is defined as the right derived functor of the direct image functor $f_* : \mathfrak{Ab}(X) \longrightarrow \mathfrak{Ab}(Y)$.*

Proposition A.6. *For each $i \geq 0$ and each $\mathcal{F} \in \mathfrak{Ab}(X)$, $R^i f_*(\mathcal{F})$ is the sheaf associated to the pre-sheaf*

$$V \longrightarrow H^i(f^{-1}(V), \mathcal{F}_{|_{f^{-1}(V)}})$$

on Y.

Proof. Let us denote by $\mathcal{H}^i(X, \mathcal{F})$ such a sheaf. Then

$$\mathcal{H}^i(X, -) : \mathfrak{Ab}(X) \longrightarrow \mathfrak{Ab}(Y)$$

form a δ-functor. For $i = 0$ we have

$$\mathcal{H}^0(X, \mathcal{F})(V) = H^0(f^{-1}(V), \mathcal{F}_{|_{f^{-1}(V)}}) = f_*\mathcal{F}(V)$$

for any V i.e. $\mathcal{H}^0(X, -) = f_*$ by definition. Moreover the $R^i f_*$'s are the right derived functors of f_*. Let $\mathcal{I} \in \mathfrak{Ab}(X)$ be injective . For any open V, we have that $\mathcal{I}_{|_{f^{-1}(V)}}$ is injective in $\mathfrak{Ab}(f^{-1}(V))$ so $H^i(f^{-1}(V), \mathcal{I}_{|_{f^{-1}(V)}}) = \mathcal{H}^i(X, \mathcal{I})(V) = 0$ for $i \geq 1$. Hence $\mathcal{H}^i(X, \mathcal{I}) = 0$. Then $\mathcal{H}^i(X, -)$ is a universal δ-functor such that $\mathcal{H}^0(X, -) \cong f_*$. We conclude that $\mathcal{H}^i(X, -) = R^i f_*$ must hold. □

Proposition A.7. *Let X be a Noetherian scheme, $f : X \longrightarrow Y$ a morphism of schemes, $Y = \operatorname{Spec}(A)$ affine. Let $\mathcal{F}$ be a quasi coherent $\mathcal{O}_X$-module on X, then*

$$R^i f_* \mathcal{F} = \widetilde{H^i(X, \mathcal{F})}.$$

Proof. Under our assumption $f_*\mathcal{F}$ is quasi-coherent, in particular since Y is affine we must have $f_*\mathcal{F} = \widetilde{\Gamma(Y, f_*\mathcal{F})} = \widetilde{\Gamma(X, \mathcal{F})}$ so the claim is true for $i = 0$. Moreover the $\widetilde{H^i(X, -)}$'s form a δ-functor. Any quasi coherent sheaf embeds into a flasque, quasi coherent sheaf and cohomology vanishes for it. Then the right hand side is an effeceable δ-functor, thus it is universal and we must have $R^i f_* \mathcal{F} = \widetilde{H^i(X, \mathcal{F})}$. □

To conclude this section we state the following result.

Proposition A.8 (Projection formula)**.** *Let $f : X \longrightarrow Y$ be a morphism of ringed spaces. Let $\mathcal{F}$ be an $\mathcal{O}_X$ module and let ε be a locally free $\mathcal{O}_Y$-module of finite rank. Then*

$$R^i f_* \left(\mathcal{F} \otimes_{\mathcal{O}_X} f^*\varepsilon\right) \cong R^i f_* \left(\mathcal{F}\right) \otimes_{\mathcal{O}_Y} \varepsilon.$$

Proof. For $i = 0$ we recover the projection formula for the direct image functor f_* and locally free modules (see [4] Chapter 5). For the general case, we use the fact that ε and $f^*\varepsilon$ are locally free hence flat so the associated tensor functors $- \otimes_{\mathcal{O}_Y} \varepsilon$ and $- \otimes_{\mathcal{O}_X} f^*\varepsilon$ are exact and thus commute with cohomology. Given an injective resolution $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I}^\bullet$ for $\mathcal{F}$, we have that $0 \longrightarrow \mathcal{F} \otimes_{\mathcal{O}_X} f^*\varepsilon \longrightarrow \mathcal{I}^\bullet \otimes_{\mathcal{O}_X} f^*\varepsilon$ is an injective resolution for $\mathcal{F} \otimes_{\mathcal{O}_X} f^*\varepsilon$. Applying f_* and taking cohomology

$$R^i f_*(\mathcal{F} \otimes_{\mathcal{O}_X} f^*\varepsilon) = H^i(f_*(\mathcal{I}^\bullet \otimes_{\mathcal{O}_X} f^*\varepsilon)).$$

The projection formula for f_* yields

$$H^i(f_*(\mathcal{I}^\bullet \otimes_{\mathcal{O}_X} f^*\varepsilon)) = H^i(f_*\mathcal{I}^\bullet \otimes_{\mathcal{O}_Y} \varepsilon) = H^i(f_*\mathcal{I}^\bullet) \otimes_{\mathcal{O}_Y} \varepsilon = R^i f_*(\mathcal{F}) \otimes_{\mathcal{O}_Y} \varepsilon.$$

□

A.5 Hypercohomology and de Rham cohomology

In this section we define hypercohomology and give a way to compute it. We start with a general definition.

Definition A.5. *Le $\mathcal{A}$ be an abelian category that has enough injectives. A right Cartan-Eilenberg resolution $I^{\bullet,\bullet}$ of a cochain complex $A^\bullet$ is an upper half plane double complex of injective objects $I^{p,q}$ with an augmentation map $\epsilon : A^\bullet \longrightarrow I^{\bullet,0}$*

$$\begin{array}{ccccccccccc}
\vdots & & \vdots & & & & \vdots & & \vdots & & \\
\uparrow & & \uparrow & & & & \uparrow & & \uparrow & & \\
I^{0,1} & \xrightarrow{\delta^{0,1}} & I^{1,1} & \xrightarrow{\delta^{1,1}} & \dots & & I^{p,1} & \longrightarrow & I^{p+1,1} & \longrightarrow & \dots \\
\uparrow & & \uparrow & & & & \uparrow & & \uparrow & & \\
I^{0,0} & \xrightarrow{\delta^{0,0}} & I^{1,0} & \xrightarrow{\delta^{1,0}} & \dots & & I^{p,0} & \xrightarrow{\delta^{p,0}} & I^{p+1,0} & \xrightarrow{\delta^{p+1,0}} & \dots \\
\epsilon^0\uparrow & & \epsilon^1\uparrow & & & & \epsilon^p\uparrow & & \epsilon^{p+1}\uparrow & & \\
A^0 & \xrightarrow{\delta_A^0} & A^1 & \longrightarrow & \dots & & A^p & \xrightarrow{\delta_A^p} & A^{p+1} & \longrightarrow & \dots
\end{array}$$

such that

1. *If $A^p = 0$ then $I^{p,\bullet} = 0$.*

2. *The maps on coboundary and cohomology*

$$B^p(\epsilon) : B^p(A^\bullet) \longrightarrow B^p(I^\bullet, \delta^\bullet)$$
$$H^p(\epsilon) : H^p(A^\bullet) \longrightarrow H^p(I^\bullet, \delta^\bullet)$$

are injective resolutions for $B^p(A^\bullet)$ and $H^p(A^\bullet)$.

Remark A.4. *Here by $B^p(I^\bullet, \delta^\bullet)$ we mean the cochain complex where the q-th term is $B^p(I^{\bullet,q}) = \operatorname{im}\left(\delta^{p-1,q} : I^{p-1,q} \longrightarrow I^{p,q}\right)$. We denote by $Z^p(I^\bullet, \delta^\bullet)$ the cochain complex where the q-th term is $Z^p(I^{\bullet,q}) = \ker\left(\delta^{p,q} : I^{p,q} \longrightarrow I^{p+1,q}\right)$. Hence $H^p(I^\bullet, \delta^\bullet)$ is the complex whose q-th term is $H^p(I^\bullet, \delta^q) = Z^p(I^{\bullet,q})/B^p(I^{\bullet,q})$. Under these assumptions*

$$\varepsilon^p : A^p \longrightarrow I^{p,\bullet}$$

is an injective resolution.

Definition A.6. *Let $F : \mathcal{A} \longrightarrow \mathcal{B}$ be a left exact functor and assume that $\mathcal{A}$ has enough injectives. If $A^\bullet$ is a cochain complex in $\mathcal{A}$ and $A^\bullet \longrightarrow I^{\bullet,\bullet}$ a Cartan-Eilenberg resolution. We define*

$$\mathbb{R}^i F(A^\bullet) = H^i(Tot^{\oplus}(F(I^{\bullet,\bullet}))$$

where $Tot^{\oplus}(F(I^{\bullet,\bullet}))$ is the total complex associated to $F(I^{\bullet,\bullet})$. Then

$$\mathbb{R}^i F : \mathrm{Ch}(\mathcal{A}) \longrightarrow \mathcal{B}$$

are the right-hyperderived functors of F.

In the case of sheaves we give the following definition.

Definition A.7. *Let X be a topological space and let $\mathcal{F}^\bullet$ be a complex of sheaves on X. The hypercohomology $\mathbb{H}^i(X, \mathcal{F}^\bullet)$ is defined as*

$$\mathbb{R}^i\Gamma(X, \mathcal{F}^\bullet).$$

This generalizes sheaf cohomology to complexes of sheaves. If $\mathcal{I}^\bullet$ is a bounded below complex of injective sheaves then $\mathbb{H}^i(X, \mathcal{I}^\bullet) = H^i(\Gamma(X, \mathcal{I}^\bullet))$.

We now give a construction using Čech cohomology. Let X be a quasi-compact and separated scheme over a field k. Assume that we have a complex of quasi coherent $\mathcal{O}_X$-modules:

$$\mathcal{S}^\bullet : \mathcal{S}^0 \xrightarrow{d^0} \mathcal{S}^1 \xrightarrow{d^1} \mathcal{S}^2 \xrightarrow{d^2} \cdots$$

We choose a finite affine cover $\mathcal{U} = \{U_i\}_{i=0,\ldots,n}$ of X. For any i we have the Čech complex

$$\mathcal{C}^\bullet(\mathcal{U}, \mathcal{S}^i) : \mathcal{C}^0(\mathcal{U}, \mathcal{S}^i) \xrightarrow{d^0} \mathcal{C}^1(\mathcal{U}, \mathcal{S}^i) \xrightarrow{d^1} \cdots.$$

By Remark A.2. it is an acyclic resolution for $\mathcal{S}^i$.
Moreover $d^i : \mathcal{S}^i \longrightarrow \mathcal{S}^{i+1}$ induces maps:

$$C^j(\mathcal{U}, \mathcal{S}^i) = \prod_{I \subseteq \{0,\ldots,n\}\ |I|=j+1} \mathcal{S}^i(U_I) \xrightarrow{\prod_I d^i_{U_I}} C^j(\mathcal{U}, \mathcal{S}^{i+1}) = \prod_{I \subseteq \{0,\ldots,n\}\ |I|=j+1} \mathcal{S}^{i+1}(U_I)$$

which we will keep denoting by d^i for simplicity. Taking sections we obtain the double complex

$$\begin{tikzcd}
\vdots & \vdots & & \vdots & \vdots & \\
C^2(\mathcal{U},\mathcal{S}^0) \arrow[r, "d^0"] \arrow[u, "\delta^2"] & C^2(\mathcal{U},\mathcal{S}^1) \arrow[r, "d^1"] \arrow[u, "\delta^2"] & \cdots & C^2(\mathcal{U},\mathcal{S}^i) \arrow[r, "d^i"] \arrow[u, "\delta^2"] & C^2(\mathcal{U},\mathcal{S}^{i+1}) \arrow[r, "d^{i+1}"] \arrow[u, "\delta^2"] & \cdots \\
C^1(\mathcal{U},\mathcal{S}^0) \arrow[r, "d^0"] \arrow[u, "\delta^1"] & C^1(\mathcal{U},\mathcal{S}^1) \arrow[r, "d^1"] \arrow[u, "\delta^1"] & \cdots & C^1(\mathcal{U},\mathcal{S}^i) \arrow[r, "d^i"] \arrow[u, "\delta^1"] & C^1(\mathcal{U},\mathcal{S}^{i+1}) \arrow[r, "d^{i+1}"] \arrow[u, "\delta^1"] & \cdots \\
C^0(\mathcal{U},\mathcal{S}^0) \arrow[r, "d^0"] \arrow[u, "\delta^0"] & C^0(\mathcal{U},\mathcal{S}^1) \arrow[r, "d^1"] \arrow[u, "\delta^0"] & \cdots & C^0(\mathcal{U},\mathcal{S}^i) \arrow[r, "d^i"] \arrow[u, "\delta^0"] & C^0(\mathcal{U},\mathcal{S}^{i+1}) \arrow[r, "d^{i+1}"] \arrow[u, "\delta^0"] & \cdots
\end{tikzcd}$$

where each square

$$\begin{array}{ccc} C^{j+1}(\mathcal{U}, \mathcal{S}^i) & \xrightarrow{d^i} & C^{j+1}(\mathcal{U}, \mathcal{S}^{i+1}) \\ \delta^j \Big\uparrow & & \delta^j \Big\uparrow \\ C^j(\mathcal{U}, \mathcal{S}^i) & \xrightarrow{d^i} & C^j(\mathcal{U}, \mathcal{S}^{i+1}) \end{array}$$

commutes. We denote such a double complex by $C^\bullet(\mathcal{U}, \mathcal{S}^\bullet)$. Taking the total complex associated to it we have

$$T^n(\mathcal{U}, \mathcal{S}^\bullet) = \bigoplus_{p+q=n} C^p(\mathcal{U}, \mathcal{S}^q) \xrightarrow{D^n} T^{n+1}(\mathcal{U}, \mathcal{S}^\bullet) = \bigoplus_{p+q=n+1} C^p(\mathcal{U}, \mathcal{S}^q)$$

where

$$(D^n(c))^{\alpha,\beta} = d^{\beta-1}c^{\alpha,\beta-1} + (-1)^{\alpha-1}\delta^{\alpha-1}c^{\alpha-1,\beta}.$$

The i-th hypercohomology is

$$\mathbb{H}^i(\mathcal{U}, \mathcal{S}^\bullet) = \ker D^i / \mathrm{im} D^{i-1}.$$

Definition A.8. *Let X be a quasi-compact, separated, smooth scheme over k. The De Rham complex $\Omega^\bullet_{X/k}$ is the complex:*

$$\mathcal{O}_X \xrightarrow{d} \Omega^1_{X/k} \xrightarrow{d} \Omega^2_{X/k} \longrightarrow \cdots$$

where $\Omega^i_{X/k} = \bigwedge^i \Omega^1_{X/k}$.

Definition A.9. *The de Rham i-th cohomology of X is defined as the i-th hypercohomolgy of the de Rham complex i.e.*

$$H^i_{dR}(X) = \mathbb{H}^i(X, \Omega^\bullet{}_{X/k}).$$

Now we see another explicit computation in the case of an elliptic curve following the construction above. Let E/k be an elliptic curve. As in the previuos section we fix points $P \neq Q \in E$ and affine open subsets $U = E \setminus \{P\}$ and $V = E \setminus \{Q\}$ such that $\mathcal{U} = \{U, V\}$. The associated de Rham complex is

$$\mathcal{O}_E \xrightarrow{d} \Omega^1_{E/k}.$$

Indeed $\Omega^i_{E/k} = 0$ for $i \geq 2$ because the sheaf of differentials is locally free of rank 1. The double complex is given by

$$\begin{array}{ccc} C^1(\mathcal{U}, \mathcal{O}_E) = \mathcal{O}_E(U \cap V) & \xrightarrow{\quad d \quad} & C^1(\mathcal{U}, \Omega^1_{E/k}) = \Omega^1_{E/k}(U \cap V) \\ \delta^0 \Big\uparrow & & \delta^0 \Big\uparrow \\ C^0(\mathcal{U}, \mathcal{O}_E) = \mathcal{O}_E(U) \oplus \mathcal{O}_E(V) & \xrightarrow{d} & C^0(\mathcal{U}, \Omega^1_{E/k}) = \Omega^1_{E/k}(U) \oplus \Omega^1_{E/k}(V). \end{array}$$

And the total complex is

$$T^0(E, \Omega^\bullet_{E/k}) \xrightarrow{D^0} T^1(E, \Omega^\bullet_{E/k}) \xrightarrow{D^1} T^2(E, \Omega^\bullet_{E/k})$$

where

$$\begin{aligned}
T^0(E, \Omega^\bullet_{E/k}) &= \mathcal{O}_E(U) \oplus \mathcal{O}_E(V),\\
T^1(E, \Omega^\bullet_{E/k}) &= \mathcal{O}_E(U \cap V) \oplus \left(\Omega^1_{E/k}(U) \oplus \Omega^1_{E/k}(V)\right),\\
T^2(E, \Omega^\bullet_{E/k}) &= \Omega^1_{E/k}(U \cap V).
\end{aligned}$$

The maps are defined as

$$\begin{aligned}
D^0(f_U, f_V) &= (f_{V|_{U\cap V}} - f_{U|_{U\cap V}}, df_U, df_V),\\
D^1(f_{UV}, \omega_U, \omega_V) &= df_{UV} + \omega_{V|_{U\cap V}} - \omega_{U|_{U\cap V}}.
\end{aligned}$$

Hence

$$\begin{aligned}
H^0_{dR}(E) &= \ker D^0\\
&= \{(f_U, f_V) \in \mathcal{O}_E(U) \oplus \mathcal{O}_E(V) \ : f_{U|_{U\cap V}} = f_{V|_{U\cap V}},\ df_U = df_V = 0\}\\
&= \mathcal{O}_E(E)\\
&= k
\end{aligned}$$

and $H^1_{dR}(E) = \ker D^1/\mathrm{im} D^0$ where

$$\begin{aligned}
\ker D^1 &= \{(f_{UV}, \omega_U, \omega_V) \ : df_{UV} = \omega_{U|_{U\cap V}} - \omega_{V|_{U\cap V}}\},\\
\mathrm{im} D^0 &= \{(f_{V|_{U\cap V}} - f_{U|_{U\cap V}}, df_U, df_V),\ (f_U, f_V) \in \mathcal{O}_E(U) \oplus \mathcal{O}_E(V)\}.
\end{aligned}$$

Lemma A.4. *We have a k-linear injective map*

$$\begin{aligned}
\phi : H^0(E, \Omega^1_{E/k}) &\longrightarrow H^1_{dR}(E)\\
\omega &\longrightarrow [(0, \omega_{|_U}, \omega_{|_V})].
\end{aligned}$$

.

Proof. To begin $(0, \omega_{|_U}, \omega_{|_V})$ is a cocycle since $(\omega_{|_U})_{|_{U\cap V}} - (\omega_{|_V})_{|_{U\cap V}} = 0$. Assume that $\phi(\omega) = 0$. Then $\omega_{|_U} = df_U$ and $\omega_{|_V} = df_V$ for some $f_U \in \mathcal{O}_E(U)$ and $f_V \in \mathcal{O}_E(V)$ such that $f_{V|_{U\cap V}} - f_{U|_{U\cap V}} = 0$. Then f_U and f_V glue to an $f \in \mathcal{O}_E(E) = k$. The fact that $\omega = df = 0$ allows us to conclude. □

Proposition A.9. *We have a short exact sequence*

$$0 \longrightarrow H^0(E, \Omega^1_{E/k}) \xrightarrow{\phi} H^1_{dR}(E) \xrightarrow{\psi} H^1(E, \mathcal{O}_E) \longrightarrow 0$$

where $\psi([(f_{UV}, \omega_U, \omega_V)]) = [f_{UV}]$.

Proof. We have already checked that ϕ is injective. Now we check that ψ is well defined. Let $((f_U)_{|_{U\cap V}} - (f_V)_{|_{U\cap V}}, df_U, df_V)$ be in $\mathrm{im} D^0$ i.e. its class in the de Rham cohomology is trivial. Then it is sent to the class of $(f_U)_{|_{U\cap V}} - (f_V)_{|_{U\cap V}}$ in $H^1(E, \mathcal{O}_E)$ which is clearly zero.
Moreover $\psi(\phi(\omega)) = ([0, \omega_{|_U}, \omega_{|_V}]) = 0$ so it's immediate that $\psi \circ \phi = 0$. On the other hand let $[(f_{UV}, \omega_U, \omega_V)]$ in $H^1_{dR}(E)$ be such that $f_{UV} = (f_V)_{|_{U\cap V}} - (f_U)_{|_{U\cap V}}$ for $f_V \in \mathcal{O}_E(V)$

and $f_U \in \mathcal{O}_E(U)$. Then $[(f_{UV}, \omega_U, \omega_V) - (f_{UV}, df_U, df_V)] = [(0, \omega_U - df_U, \omega_V - df_V)] = \alpha$. We clearly have $[(f_{UV}, \omega_U, \omega_V)] = \alpha$ and

$$\begin{aligned}(\omega_U - df_U)_{|U\cap V} - (\omega_V - df_V)_{|U\cap V} &= (\omega_U)_{|U\cap V} - (\omega_V)_{|U\cap V} + (df_V)_{|U\cap V} - (df_U)_{|U\cap V} \\ &= (\omega_U)_{|U\cap V} - (\omega_V)_{|U\cap V} + df_{UV} = 0\end{aligned}$$

since $(f_{UV}, \omega_U, \omega_V)$ is a cocycle.
To conclude we prove that ψ is surjective. We first assume that $P = O$ the origin point of the elliptic curve. Assume that E is locally given by

$$Y^2 = X^3 + aX + b$$

and that $\omega = \frac{dX}{Y}$ is the nowhere vanishing differential. Let $\eta = X\frac{dX}{Y}$. We notice that η has order -2 at P and no residue. Moreover let $f \in \mathcal{O}_E(U \cap V)$ such that $[f] \neq 0$ in $H^1(E, \mathcal{O}_E)$, namely $\mathrm{ord}_P f = \mathrm{ord}_Q f = -1$. Then

$$f_P = \frac{\gamma}{T} + \ldots$$

with $\gamma \neq 0$. We let $\eta_1 = \eta + \frac{1}{\gamma} df$. Then η_1 is regular at P, hence on $E \setminus \{Q\}$ i.e. $\eta_1 \in \Omega^1_{E/k}(V)$. We set $\omega_U = \eta_{|U} \in \Omega^1{}_{E/k}(U)$ and $\omega_V = \eta_{1|V} \in \Omega^1_{E/k}(V)$ and $f_{UV} = \frac{1}{\gamma} f_{|U\cap V}$. Then $(\omega_U)_{|U\cap V} - (\omega_V)_{|U\cap V} = \frac{1}{\gamma} df_{|U\cap V} = df_{UV}$. This proves that $(f_{UV}, \omega_U, \omega_V)$ is a cocycle and we may call $\delta = [(f_{UV}, \omega_U, \omega_V)] \in H^1_{dR}(E)$. Then $\psi(\delta) = [f_{UV}]$ is a generator for $H^1(E, \mathcal{O}_E)$ and we conclude that ψ is surjective.
If $P \neq O$ we use Riemann-Roch theorem. We let $[f] \in H^1(E, \mathcal{O}_E)$ non zero, namely $\mathrm{ord}_P f = -1 = \mathrm{ord}_Q f$. We have $l(2(P)) = 2 = l(2(Q))$ so we find $f_U \in H^0(E, \mathcal{L}_{2(P)}) \setminus k$ and $f_V \in H^0(E, \mathcal{L}_{2(Q)}) \setminus k$. We must have $\mathrm{ord}_P f_U = -2 = \mathrm{ord}_Q f_V$ otherwise they would be constant and $f_U \in \mathcal{O}_E(U)$ and $f_V \in \mathcal{O}_E(V)$. Let ω be the canonical nowhere vanishing differential, we set $\omega_U = f_U \omega_{|U} \in \Omega^1{}_{E/k}(U)$ and $\omega_V = f_V \omega_{|V} \in \Omega^1_{E/k}(V)$. Then $\alpha = (f_U \omega_{|U})_{|U\cap V} - (f_V \omega_{|V})_{|U\cap V} \in \Omega^1_{E/k}(U \cap V)$. Moreover $df \in \Omega^1{}_{E/k}(U \cap V)$ has a double pole at P and Q and $\Omega^1{}_{E/k}(U \cap V)$ is a $\mathcal{O}_E(U \cap V)$-module of rank 1. Hence $\alpha = gdf$ for some $g \in \mathcal{O}_E(U \cap V)$. Taking orders at P and Q, we must have $\mathrm{ord}_P g = 0 = \mathrm{ord}_Q g$. Hence g is holomorphic on E and thus must be constant. It cannot be zero otherwise α would be zero. Then $d(gf) = gdf = \alpha = \omega_{U|U\cap V} - \omega_{V|U\cap V}$ is a cocycle. Hence $\psi([(gf, \omega_U, \omega_V)]) = [gf] = g[f]$ a generator for $H^1(E, \mathcal{O}_E)$. We conclude that ψ is surjective. □

Corollary A.2. *$\dim_k(H^1_{dR}(E)) = 2$ and $[\omega]$,$[\delta]$ above are generators.*

Remark A.5. *The exact sequence above is called the Hodge filtration. We proved that it holds in the case of an elliptic curve over a field k. In the next section we will see how it appears from a more general setting. In particular we will analyze the case of curves over a field of positive characteristic.*

In [8] $A1.2.3$ Katz shows that the first de Rham cohomology of an elliptic curve E/R is nothing other than the module of differentials on E/R having at worst double poles at the identity section ∞. In our case the argument goes as follows.

Remark A.6. *Let E/k be an elliptic curve over a field k and assume $\mathrm{char}(k) \neq 2, 3$. Let $\mathcal{O}_E(\infty) := \mathcal{L}_{(\infty)}$ be the sheaf of holomorphic functions with at worst one simple pole at ∞. Let $\Omega^1_E(2\infty) = \Omega^1_E \otimes_k \mathcal{L}_{(2\infty)}$[1]. The inclusion of complexes*

$$\begin{array}{ccc} \mathcal{O}_E(\infty) & \longrightarrow & \Omega^1_E(2\infty) \\ \uparrow & & \uparrow \\ \mathcal{O}_E & \longrightarrow & \Omega^1_E \end{array}$$

is a quasi-isomorphism. Taking hypercohomology one finds that

$$H^1_{dR}(E/k) = \mathbb{H}^1(E, \Omega^\bullet_E) = \mathbb{H}^1(E, \Omega^\bullet_E(2\infty)).$$

Using Čech cohomology one easily sees that $H^1(E, \mathcal{O}_E(\infty)) = 0 = H^1(E, \Omega^1_E(2\infty))$ and also

$$\mathbb{H}^1(E, \Omega^\bullet_E(2\infty)) = \mathrm{coker}\left(\mathcal{O}_E(\infty)(E) \xrightarrow{d} \Omega^1_E(2\infty)(E)\right).$$

By Riemann-Roch Theorem $\mathcal{O}_E(\infty)(E) = H^0(E, \mathcal{L}_{(\infty)}) = k$ hence d is the zero map. We conclude

$$H^1_{dR}(E/k) \cong H^0(E, \Omega^1_E(2\infty)).$$

Again by Riemann-Roch $H^0(E, \Omega^1_E(2\infty))$ has dimension 2. Clearly the holomorphic differential $\frac{dX}{Y}$ is in $H^0(E, \Omega^1_E(2\infty))$. Moreover $X\frac{dX}{Y}$ is a section in $\Omega^1_E(2\infty)$ and has exactly a double pole at ∞. The two must be a basis.

Remark A.7. *The pair*

$$\omega := \frac{dX}{Y} \qquad \eta := X\frac{dX}{Y}$$

is a basis for $H^1_{dR}(E/k)$ through the identification of $H^1_{dR}(E/k)$ with global differentials having at worst double pole at ∞. [2]

To conclude we go back to the general case and give the definition of the sheaf of relative de Rham cohomology .

Definition A.10. *Let $\pi : X \longrightarrow S$ be a smooth k-morphism of smooth k-schemes. The relative de Rham cohomology of X/S is the sheaf on S*

$$H^i_{dR}(X/S) = \mathbb{R}^i\pi_*(\Omega^\bullet_{X/S}).$$

[1] Notice that for any $f \in \mathcal{O}_E(\infty)$ the differential df has a double pole at ∞ hence is in $\Omega^1_E(2\infty)$.

[2] Notice that such a characterization could have been easily deduced by the explicit computation above.

Appendix B

The Hodge filtration and the conjugate filtration

The aim of this section is to introduce the Hodge filtration and the conjugate filtration for a smooth curve X/S over a field of positive characteristic K. This is the setting of Lemma 4.3 in Chapter 4.

B.1 Some results about spectral sequences

We first recall some general facts about spectral sequences.

Definition B.1. *Let $\mathcal{A}$ be an abelian category. A spectral sequence starting at page a is a collection of objects $\{E_r^{p,q}\}_{r\geq a,\ p,q\in\mathbb{Z}}$ and morphisms $d_r^{p,q} : E_r^{p,q} \longrightarrow E_r^{p+r,q-r+1}$ such that*

1. $d_r^{p+r,q-r+1} \circ d_r^{p,q} = 0$.
2. $E_{r+1}^{p,q} \cong \ker d_r^{p,q} / \mathrm{im} d_r^{p-r,q+r-1}$

We denote by $\{E_r^{p,q},\ d_r^{p,q}\}_{p,q\in\mathbb{Z}}$ the r-th page of the spectral sequence.

A spectral sequence is bounded if for each n and r there are only finitely many nonzero terms of total degree n in $E_r^{\bullet,\bullet}$. If this is the case, for any fixed p, q the sequence $\{E_r^{p,q}\}_{r\geq a}$ stabilizes. We denote $E_\infty^{p,q} = E_r^{p,q}$ for $r >> 0$. Moreover if r_0 is such that

$$E_{r_0}^{p,q} = E_{r+1}^{p,q} = \cdots = E_\infty^{p,q}$$

for all p, q we say that the spectral sequence degenerates at page r_0.

Definition B.2. *We say that a bounded spectral sequence $\{E_r^{p,q}\}_{r\geq a,\ p,q\in\mathbb{Z}}$ converges to a complex $H^\bullet = \{H^n\}_{n\in\mathbb{Z}}$ if there exists a filtration $F^\bullet H^\bullet$ of $H^\bullet$, i.e. for any q*

$$F^\bullet H^q : \cdots \subseteq F^{p+1} H^q \subseteq F^p H^q \subseteq \ldots$$

such that $F^p H^{p+q} / F^{p+1} H^{p+q} \cong E_\infty^{p,q}$. We denote $E_r^{p,q} \implies H^{p+q}$.

Let now $(C^\bullet, d^\bullet)$ be a cochain complex in $\mathcal{A}$ with bounded filtration $F^\bullet C^\bullet$ that is

$$0 \subseteq \cdots \subseteq F^{p+1}C^q \subseteq F^pC^q \subseteq \cdots \subseteq F^0C^q = C^q$$

such that $d^q : F^pC^q \longrightarrow F^pC^{q+1}$ for all p, q. We denote by $\mathrm{gr}^p(C^\bullet)$ the complex of *graded pieces*

$$\mathrm{gr}^p(C^i) = F^pC^i/F^{p+1}C^i$$

Remark B.1. *The fitration on $C^\bullet$ naturally induces a filtration on cohomology $F^\bullet H^q(C^\bullet)$ namely*

$$F^pH^q(C^\bullet) = \mathrm{im}\left(H^q(F^pC^\bullet) \longrightarrow H^q(C^\bullet)\right).$$

Moreover if the filtration on $C^\bullet$ is bounded also the filtration $F^\bullet H^q(C^\bullet)$ is bounded since $F^pC^\bullet = 0$ implies $F^pH^q(C^\bullet) = 0$ by definition for all q.

Theorem B.1 (Covergence)**.** *Let $F^\bullet C^\bullet$ be a bounded filtration of a cochain complex $C^\bullet$. Then it naturally determines a spectral sequence with*

$$\begin{aligned} E_0^{p,q} &:= F^pC^{p+q}/F^{p+1}C^{p+q}, \\ E_1^{p,q} &:= H^{p+q}(\mathrm{gr}^pC^\bullet), \\ E_\infty^{p,q} &:= \mathrm{gr}^pH^{p+q}(C^\bullet). \end{aligned}$$

We write

$$E_1^{p,q} := H^{p+q}(\mathrm{gr}^pC^\bullet) \implies H^{p+q}(C^\bullet).$$

Moreover page 1 maps

$$d_1^{p,q} : H^{p+q}(\mathrm{gr}^p) \longrightarrow H^{p+q+1}(\mathrm{gr}^{p+1}(C^\bullet))$$

are the connecting maps on cohomology rising from

$$0 \longrightarrow \mathrm{gr}^{p+1}C^\bullet \longrightarrow F^pC^\bullet/F^{p+2}C^\bullet \longrightarrow \mathrm{gr}^pC^\bullet \longrightarrow 0.$$

Proof. See Theorem 5.4.1 and Theorem 5.5.1 of [18]. □

Remark B.2. *Let $\mathcal{A}$ be an abelian category with enough injectives and $A \in \mathcal{A}$ an object of finite filtration $F^\bullet A$. We can construct from below a filtered injective resolution $A \longrightarrow I^\bullet$ such that $F^\bullet A \longrightarrow F^\bullet I^\bullet$ is an injective resolution.*

Proposition B.1. *Let $A \in \mathcal{A}$ and $F^\bullet A$ as above. Let $T : \mathcal{A} \longrightarrow \mathcal{B}$ be an additive left exact functor. There is a convergent spectral sequence such that*

$$E_1^{p,q} = R^{p+q}T(\mathrm{gr}^pA) \implies R^{p+q}T(A)$$

with page one maps

$$d_1^{p,q} : R^{p+q}T(\mathrm{gr}^pA) \longrightarrow R^{p+q+1}T(\mathrm{gr}^{p+1}A)$$

being the connecting maps of the functors $R^{p+q}T$ for the exact sequence

$$0 \longrightarrow \mathrm{gr}^{p+1}A \longrightarrow F^pA/F^{p+2}A \longrightarrow \mathrm{gr}^pA \longrightarrow 0.$$

Proof. Thanks to Remark B.2. we may fix a filtered injective resolution $A \longrightarrow I^\bullet$ such that $F^pI^\bullet$ is an injective resolution of F^pA for any p. Applying T and recalling that it is left exact we get

$$\begin{tikzcd}
0 \arrow[r] & TA \arrow[r] & TI^0 \arrow[r] & TI^1 \arrow[r] & \cdots \\
0 \arrow[r] & TF^1A \arrow[r] \arrow[u, hook] & TF^1I^0 \arrow[r] \arrow[u, hook] & TF^1I^1 \arrow[r] \arrow[u, hook] & \cdots \\
0 \arrow[r] & TF^2A \arrow[r] \arrow[u, hook] & TF^2I^0 \arrow[r] \arrow[u, hook] & TF^2I^1 \arrow[r] \arrow[u, hook] & \cdots \\
& \vdots \arrow[u, hook] & \vdots \arrow[u, hook] & \vdots \arrow[u, hook] &
\end{tikzcd}$$

Hence $TF^\bullet I^\bullet$ is a bounded filtration of $TI^\bullet$. We apply the convergence theorem with $C^\bullet := TI^\bullet$ and $F^pC^\bullet := TF^pI^\bullet$. We obtain

$$E_1^{p,q} = H^{p+q}(\mathrm{gr}^p TI^\bullet) \implies H^{p+q}(TI^\bullet) = R^{p+q}TA.$$

Moreover we have short exact sequences:

$$0 \longrightarrow F^{p+1}I^q \longrightarrow F^pI^q \longrightarrow gr^pI^q \longrightarrow 0$$

which split since $F^{p+1}I^q$ is injective, hence gr^pI^q is injective for any q since direct summand of an injective object. Then

$$\mathrm{gr}^pA \longrightarrow \mathrm{gr}^pI^\bullet$$

is an injective resolution for gr^pA. We conclude

$$R^{p+q}T(\mathrm{gr}^pA) = H^{p+q}(T\mathrm{gr}^pI^\bullet) = H^{p+q}(\mathrm{gr}^pTI^\bullet).$$

□

Remark B.3. *We will deal with the case of a cochain complex $C^\bullet$ in $\mathrm{Ch}^{\geq 0}(\mathcal{A})$ and the functor $\mathbb{R}^0T : \mathrm{Ch}^{\geq 0}(\mathcal{A}) \longrightarrow B$. Recalling that $\mathbb{R}^iT$ are the left derived functors of $\mathbb{R}^0T$, the proposition above yields a spectral sequence:*

$$E_1^{p,q} = \mathbb{R}^{p+q}T(\mathrm{gr}^pC^\bullet) \implies \mathbb{R}^{p+q}T(C^\bullet)$$

B.2 The Hodge filtration for the de Rham complex

We will follow Katz's argument in [7]. Given a complex $C^\bullet$ in an abelian variety $\mathcal{A}$ there is a natural way to define a filtration on it.

We construct the Hodge filtration $F^\bullet C^\bullet$:

$$F^p(C^q) = \begin{cases} 0 \text{ if } q < p, \\ C^q \text{ if } q \geq p. \end{cases}$$

We have that $\mathrm{gr}^p C^\bullet = F^p(C^\bullet)/F^{p+1}(C^\bullet) = C^p[-p]$ is the complex consisting in the object C^p in degree p and zero elsewhere. Then $\mathbb{R}^{p+q}T(\mathrm{gr}^p C^\bullet) = R^q T(C^p)$ and convergence yields a spectral sequence:

$$E_1{}^{p,q} := R^q T(C^p) \implies \mathbb{R}^{p+q}T(C^\bullet).$$

Let now $X \xrightarrow{\pi} S$ be a smooth scheme over a field k. We denote by $\Omega^\bullet_X$ the de Rham complex of X and $\Omega^\bullet_{X/S}$ the de Rham complex of relative differentials. We apply the construction above to $\Omega^\bullet_X$ with $T = \Gamma(X, -)$ and we get

$$E_1{}^{p,q} := R^q\Gamma(X, \Omega^p_X) = H^q(X, \Omega^p_X) \implies \mathbb{R}^{p+q}\Gamma(X, \Omega^\bullet_X) = H^{p+q}_{dR}(X).$$

Applying the construction above to $\Omega^\bullet_{X/S}$ and $T = \pi_*$ we have

$$E_1^{p,q} := R^q\pi_*(\Omega^p_{X/S}) \implies \mathbb{R}^{p+q}\pi_*(\Omega^\bullet_{X/S}) = H^{p+q}_{dR}(X/S). \tag{B.1}$$

Definition B.3. *We call (B.1) the Hogde-de Rham spectral sequence.*

Let now X/S be a smooth curve over a field k. By an argument of Deligne and Illusie in [2] we have that (B.1) degenerates at page 1. Convergence tells us that we have a filtration on the relative de Rham cohomology $F^\bullet H^q_{dR}(X/S)$ such that

$$\mathrm{gr}^p H^{p+q}_{dR}(X/S) = E_1{}^{p,q}.$$

Remark B.4. *Let $p + q = 1$. The first two terms of the above filtration appear in the exact sequence*

$$0 \longrightarrow F^1 H^1_{dR}(X/S) \longrightarrow F^0 H^1_{dR}(X/S) \longrightarrow \mathrm{gr}^0 H^1_{dR}(X/S) \longrightarrow 0.$$

For a curve we have $\Omega^2_{X/S} = 0$ hence

$$F^2\Omega^\bullet_{X/S} = 0.$$

By Remark B.1. we also have

$$F^2 H^1_{dR}(X/S) = F^2\mathbb{R}\pi_*(\Omega^\bullet_{X/S}) = 0$$

hence

$$F^1 H^1_{dR}(X/S) = \mathrm{gr}^1 H^1_{dR}(X/S)$$

Rewriting the sequence above we get the Hodge-de Rham short exact sequence:

$$0 \longrightarrow R^0\pi_*(\Omega^1_{X/S}) \longrightarrow H^1_{dR}(X/S) \longrightarrow R^1\pi_*(\mathcal{O}_X) \longrightarrow 0.$$

Furthermore we have another natural ascending filtration on a complex $C^\bullet$. The canonical filtration (see 2.2.2 [7]) is defined as

$$\tau_{\le p} C^q = \begin{cases} C^q & \text{if } q < p, \\ \ker(d^q : C^q \longrightarrow C^{q+1}) & \text{if } q = p, \\ 0 & \text{if } q > p. \end{cases}$$

To obtain a descending filtration we set $F^pC^\bullet = \tau_{\leq -p}C^\bullet$. The graded pieces of F are $\mathrm{gr}^pC^\bullet = H^{-p}(C^\bullet)[p]$ and convergence yields

$$E_1{}^{p,q} := \mathbb{R}^{p+q}T(H^{-p}(C^\bullet)[p]) = R^{2p+q}T(H^{-p}(C^\bullet)) \implies \mathbb{R}^{p+q}T(C^\bullet)$$

with page 1 maps $R^{2p+q}T(H^{-p}(C^\bullet)) \longrightarrow R^{2p+2+q}T(H^{-p-1}(C^\bullet))$. Replacing (p,q) by $(-q, p+2q)$ we obtain a spectral sequence starting at page 2

$$E_2{}^{p,q} := R^pT(H^q(C^\bullet)) \implies \mathbb{R}^{p+q}T(C^\bullet).$$

Again we consider X/S smooth schemes over a field k. We apply the construction above to the relative de Rham complex $\Omega^\bullet_{X/S}$ in order to get:

$$E_2{}^{p,q} := R^p\pi_*(H^q(\Omega^\bullet_{X/S})) \implies H^{p+q}_{dR}(X/S). \tag{B.2}$$

B.3 The conjugate filtration

Let $\pi : X \longrightarrow S$ be a smooth morphism of schemes, S a smooth scheme over a field k. Moreover we assume that k has positive characteristic p. The absolute Frobenius $F_{abs} : S \longrightarrow S$, which on sections corresponds to raising to the p-th power, and the relative Frobenius $X \longrightarrow X^{(p)}$ fit in a commutative diagram

$$\begin{tikzcd}
X \arrow[r, "Fr"] \arrow[rr, bend left, "F_{abs}"] \arrow[dr, "\pi"'] & X^{(p)} \arrow[r, "\sigma"] \arrow[d, "\pi^{(p)}"] & X \arrow[d, "\pi"] \\
& S \arrow[r, "F_{abs}"] & S
\end{tikzcd}$$

where $\sigma \circ Fr = F_{abs}$ is the absolute Frobenius on X (see Chapter 3.5).

The following theorem holds:

Theorem B.2 (Cartier)**.** *Let X/S be smooth morphisms over a field of positive characteristic p. There exists a unique morphism of $\mathcal{O}_{X^{(p)}}$-algebras*

$$\mathcal{C}^{-1} : \bigoplus_i \Omega^i_{X^{(p)}/S} \longrightarrow \bigoplus_i H^i(Fr_*\Omega^\bullet_{X/S})$$

such that

$$\mathcal{C}^{-1} : \Omega^1_{X^{(p)}/S} \longrightarrow H^1(Fr_*\Omega^\bullet_{X/S})$$

sends a section $x \otimes 1$ of $\Omega^1_{X^{(p)}/S}$ on an open of $X^{(p)}$ to $[x^{p-1}dx]$. Moreover $\mathcal{C}^{-1}$ is an isomorphism.

Proof. See [6] Theorem 7.2. □

The Cartier isomorphism induces isomorphisms:

$$\Omega^i_{X^{(p)}/S} \cong H^i(Fr_*\Omega^\bullet_{X/S}).$$

We can rewrite the terms of the spectral sequence at $(B.2)$ noticing that $\pi_* = \pi_*^{(p)} Fr_*$:

$$R^a\pi_*(H^b(\Omega^\bullet_{X/S})) = R^a\pi_*^{(p)} Fr_*(H^b(\Omega^\bullet_{X/S})) = {}^1R^a\pi_*^{(p)}(H^b(Fr_*\Omega^\bullet_{X/S})) \cong R^a\pi_*^{(p)}(\Omega^b_{X^{(p)}/S}).$$

And we obtain

$$E_2^{a,b} = R^a\pi_*^{(p)}(\Omega^b_{X^{(p)}/S}) \implies H^{a+b}_{dR}(X/S). \tag{B.3}$$

Definition B.4. *We call (B.3) the conjugate spectral sequence.*

Moreover by a proof of Katz (see [7](2.3.2.3)) the spectral sequence (B.3) degenerates at page 2. To conclude, we may use the same kind of argument of the previous section to get a filtration on the relative de Rham cohomology. We obtain the *conjugate* short exact sequence:

$$0 \longrightarrow R^1\pi_*^{(p)}(\mathcal{O}_{X^{(p)}/S}) \longrightarrow H^1_{dR}(X/S) \longrightarrow R^0\pi_*^{(p)}(\Omega^1_{X^{(p)}/S}) \longrightarrow 0.$$

[1] Here we used the fact that Fr_* commutes with cohomology since the direct image functor of an affine morphism is an exact functor in the category of quasi coherent sheaves.

Appendix C

The Gauss-Manin connection

C.1 Connections

Let S be a smooth scheme over a field k and let ε be a quasi coherent sheaf of $\mathcal{O}_S$-modules.

Definition C.1. *A connection on ε is an homomorphism ρ of abelian sheaves:*

$$\rho : \varepsilon \longrightarrow \Omega^1_{S/k} \otimes_{\mathcal{O}_S} \varepsilon$$

such that $\rho(fe) = df \otimes e + f\rho(e)$ for any section f and e of $\mathcal{O}_S$ and ε respectively on an open of S.

Remark C.1. *A connection gives rise to homomorphisms of abelian sheaves*

$$\rho_i : \Omega^i_{S/k} \otimes_{\mathcal{O}_S} \varepsilon \longrightarrow \Omega^{i+1}_{S/k} \otimes_{\mathcal{O}_S} \varepsilon$$
$$\rho_i(\omega \otimes e) = d\omega \otimes e + (-1)^i \omega \wedge \rho(e)$$

where $\omega \wedge \rho(e)$ denotes the image of $\omega \otimes \rho(e)$ under the canonical map

$$\Omega^i_{S/k} \otimes_{\mathcal{O}_S} \Omega^1_{S/k} \otimes_{\mathcal{O}_S} \varepsilon \longrightarrow \Omega^{i+1}_{S/k} \otimes_{\mathcal{O}_S} \varepsilon$$
$$\omega \otimes \tau \otimes e \longrightarrow \omega \wedge \tau \otimes e.$$

Definition C.2. *The curvature K of the connection ρ is the $\mathcal{O}_S$-linear map*

$$K = \rho_1 \circ \rho : \varepsilon \longrightarrow \Omega^2_{S/k} \otimes_{\mathcal{O}_S} \varepsilon.$$

We notice that

$$(\rho_{i+1} \circ \rho_i)(\omega \otimes e) = \omega \wedge K(e)$$

holds for any section ω of $\Omega^i_{S/k}$ and e of ε on an open subset of S.

Definition C.3. *The connection ρ is called integrable if $K = 0$ or, equivalently, if ρ gives rise to a complex $\Omega^\bullet_{S/k} \otimes_{\mathcal{O}_S} \varepsilon$*

$$\varepsilon \longrightarrow \Omega^1_{S/k} \otimes_{\mathcal{O}_S} \varepsilon \longrightarrow \Omega^2_{S/k} \otimes_{\mathcal{O}_S} \varepsilon \longrightarrow \dots$$

called the de Rham complex of ρ.

Remark C.2. *A connection ρ on ε yields an $\mathcal{O}_S$-linear mapping:*

$$\mathrm{Der}_k(\mathcal{O}_S) \longrightarrow \mathrm{End}_k(\varepsilon)$$

which sends any k-linear derivation D of $\mathcal{O}_S$ to

$$\rho(D) : \varepsilon \xrightarrow{\rho} \Omega^1_{S/k} \otimes_{\mathcal{O}_S} \xrightarrow{D\otimes 1} \mathcal{O}_S \otimes_{\mathcal{O}_S} \varepsilon \cong \varepsilon$$

where we identify D with the associated morphism $\psi_D : \Omega^1_{S/k} \longrightarrow \mathcal{O}_S$ through the correspondence

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_S}(\Omega^1_{S/k}, \mathcal{O}_S) &\cong \mathrm{Der}_k(\mathcal{O}_S) \\ \psi_D &\longrightarrow D = \psi_D \circ d. \end{aligned}$$

Then one easily verifies that

$$\rho(D)(fe) = D(f)e + f\rho(D)(e).$$

C.2 Another filtration on the de Rham complex

Let S be a smooth affine scheme over a field k and let $\pi : X \longrightarrow S$ be a smooth morphism of schemes. We have an exact sequence:

$$0 \longrightarrow \pi^*\Omega^p_{S/k} \longrightarrow \Omega^p_{X/k} \longrightarrow \Omega^p_{X/S} \longrightarrow 0$$

which is split exact since all of them are locally free $\mathcal{O}_X$-modules. Then we may see $\pi^*\Omega^p_{S/k} \hookrightarrow \Omega^p_{X/k}$ and consider the natural map

$$\pi^*\Omega^p_{S/k} \otimes_{\mathcal{O}_X} \Omega^{q-p}_{X/k} \longrightarrow \Omega^q_X$$

coming from $\Omega^p_{X/k} \otimes_{\mathcal{O}_X} \Omega^{q-p}_{X/k} \longrightarrow \Omega^q_{X/k}$.

Definition C.4. *We define the Koszul filtration $F^\bullet\Omega^\bullet_X$*

$$F^p\Omega^q_{X/k} := \mathrm{im}\left(\pi^*\Omega^p_{S/k} \otimes_{\mathcal{O}_X} \Omega^{q-p}_{X/k} \longrightarrow \Omega^q_{X/k}\right) \tag{C.1}$$

where $\Omega^i_{X/k} = 0$ for $i < 0$.

The graded pieces of the filtration are

$$\mathrm{gr}^p\Omega^\bullet_{X/k} = \pi^*\Omega^p_{S/k} \otimes_{\mathcal{O}_X} \Omega^{\bullet-p}_{X/S}.$$

We consider the functor

$$T := \mathbb{R}^0\pi_* : \mathrm{Ch}^{\geq 0}(\mathrm{Sh}/X) \longrightarrow \mathrm{Sh}/S$$

and apply Proposition B.1 to T with $A = \Omega^\bullet_X$ and $F^iA = F^i\Omega^\bullet_X$ in order to have

$$E_1^{p,q} = \mathbb{R}^{p+q}\pi_*(\pi^*\Omega^p_{S/k} \otimes_{\mathcal{O}_X} \Omega^{\bullet-p}_{X/S}) \implies \mathbb{R}^{p+q}\pi_*\Omega^\bullet_X.$$

Using the projection formula:

$$\begin{aligned}\mathbb{R}^{p+q}\pi_*(\pi^*\Omega^p_{S/k}\otimes_{\mathcal{O}_X}\Omega^{\bullet-p}_{X/S}) &= \Omega^p_{S/k}\otimes_{\mathcal{O}_S}\mathbb{R}^{p+q}\pi_*(\Omega^{\bullet-p}_{X/S})\\ &= \Omega^p_{S/k}\otimes_{\mathcal{O}_S}\mathbb{R}^{q}\pi_*(\Omega^{\bullet}_{X/S})\\ &= \Omega^p_{S/k}\otimes_{\mathcal{O}_S} H^q_{dR}(X/S).\end{aligned}$$

We get the complex:

$$H^q_{dR}(X/S)\xrightarrow{d_1^{0,q}}\Omega^1_{S/k}\otimes_{\mathcal{O}_S}H^q_{dR}(X/S)\longrightarrow\Omega^2_{S/k}\otimes_{\mathcal{O}_S}H^q_{dR}(X/S)\longrightarrow\dots$$

It looks like the de Rham complex of a connection, in particular if $d_1^{0,q}$ is a connection we get integrability for free.

Remark C.3. *Back to our general setting of spectral sequences, we give the following construction. Suppose that for page $r = a$ we are given a bigraded product:*

$$E_r^{p,q}\times E_r^{p',q'}\longrightarrow E_r^{p+p',q+q'} \tag{C.2}$$

such that the differential d_r satisfies the Leibnitz relation:

$$d_r^{p+p',q+q'}(xx') = d_r^{p,q}(x)x' + (-1)^p x d_r^{p'q'}(x') \tag{C.3}$$

for any $x\in E_a^{p,q}, x'\in E_a^{p',q'}$. Then the product of two cocycles (respectively coboundaries) is again a cocycle (respectively a coboundary). We can extend the product to cohomology and by induction we have a product as in (C.2) such that (C.3) holds for every $r\geq a$. We shall call this a multiplicative structure on the spectral sequence.
Now let $(C^\bullet, d^\bullet)$ be a complex equipped with a bigraded product, namely

$$C^p\times C^q\longrightarrow C^{p+q}$$

such that the differentials satisfy Leibnitz rule. Assume that $C^\bullet$ is endowed with a bounded filtration $F^\bullet C^\bullet$ which is multiplicative i.e.

$$F^pC^q\times F^{p'}C^{q'}\longrightarrow F^{p+p'}C^{q+q'}.$$

Then $E_0^{p,q} = F^pC^q/F^{p+1}C^q$ inherits the product structure

$$E_0^{p,q}\times E_0^{p',q'}\longrightarrow E_0^{p+p',q+q'}$$

and the spectral sequence has a multiplicative structure.

The de Rham complex is equipped with the exterior product

$$\begin{aligned}\Omega^p_{S/k}\otimes\Omega^q_{S/k}&\longrightarrow\Omega^{p+q}_{S/k}\\ \omega\otimes\tau&\longrightarrow\omega\wedge\tau\end{aligned}$$

and the canonical differential maps $d_{S/k}:\Omega^{p+q}_{S/k}\longrightarrow\Omega^{p+q+1}_{S/k}$ satisfy

$$d_{S/k}(\omega\wedge\tau) = d_{S/k}(\omega)\wedge\tau + (-1)^p\omega\wedge d_{S/k}(\tau).$$

The filtration (C.1) is multiplicative. By Remark C.3. the spectral sequence $E_r^{p,q}$ has multiplicative structure and the page 1 maps satisfy Leibnitz rule. For $q = 0$ we have that $E_1^{\bullet,0}$ is the complex $\Omega^{\bullet}_{S/k} \otimes H^0_{dR}(X/S)$ with differential maps $d_{S/k} \otimes 1$ and we may see the de Rham complex as a subcomplex of it. We have the product $E_1^{i,0} \times E_1^{0,q} \longrightarrow E_1^{i,q}$. Then for any section ω and e of $\Omega^i_{S/k}$ and $H^q_{dR}(X/S)$ respectively on an open of S

$$d_1^{i,q}(\omega \cdot e) = d_1^{i,0}(\omega) \cdot e + (-1)^i \omega \cdot d_1^{0,q}(e) = d_{S/k}(\omega) \otimes 1 \cdot e + (-1)^i \omega \cdot d_1^{0,q}(e).$$

We conclude that $d_1^{0,q} : H^q_{dR}(X/S) \longrightarrow \Omega^1_{S/k} \otimes H^q_{dR}(X/S)$ is a connection on the sheaf of relative de Rham cohomology.

Definition C.5. *We call*

$$\nabla := d_1^{0,q} : H^q_{dR}(X/S) \longrightarrow \Omega^1_{S/k} \otimes H^q_{dR}(X/S)$$

the Gauss-Manin connection.

Moreover for $p = 0$ we have the induced product $E_1^{0,q} \times E_1^{0,q'} \longrightarrow E_1^{q+q'}$ i.e.

$$H^q_{dR}(X/S) \times H^{q'}_{dR}(X/S) \longrightarrow H^{q+q'}_{dR}(X/S)$$

and the map $d_1^{0,q}$ verifies

$$d_1^{0,q+q'}(e \cdot e') = d_1^{0,q}(e) \cdot e' + (-1)^q e \cdot d_1^{0,q'}(e')$$

for any $e \in H^q_{dR}(X/S)$ and $e' \in H^{q'}_{dR}(X/S)$. We say that the Gauss-Manin connection is compatible with the cup product.

Remark C.4. *As explained above the Gauss-Manin connection gives a map from* $\mathrm{Der}_k(\mathcal{O}_S)$ *to* $\mathrm{End}_k(H^q_{dR}(X/S))$ *that sends a k-linear derivation D of $\mathcal{O}_S$ to $\nabla(D)$ where*

$$\nabla(D) : H^q_{dR}(X/S) \longrightarrow \Omega^1_{S/k} \otimes_{\mathcal{O}_S} H^q_{dR}(X/S) \xrightarrow{D\otimes 1} \mathcal{O}_s \otimes_{\mathcal{O}_S} H^q_{dR}(X/S) \cong H^q_{dR}(X/S).$$

By the observation above we have

$$\nabla(D)(e \cdot e') = \nabla(D)(e)e' + e\nabla(D)(e')$$
$$\nabla(D)(f) = D(f)$$

for any section e, e' and f of $H^q_{dR}(X/S)$, $H^{q'}_{dR}(X/S)$ and $\mathcal{O}_S$ respectively. This shows that $\nabla(D)$ extends the k-derivation D to the sheaf $H^q_{dR}(E/S)$.

C.3 A computation for the universal elliptic curve

In this section we compute the Gauss-Manin connection for $\mathbb{E}/Y(N)$ over the complex numbers $\mathbb{C}$ following [8] A.1.3.

First we need to recall some preliminary facts about integrable connections over $\mathbb{C}$. Let $X \xrightarrow{f} S$ be a smooth proper family of connected varieties over $\mathbb{C}$. We identify X with X^{an} and we may restrict to the case of S affine.

Remark C.5. *We have a well defined functor from the category of quasi coherent locally free $\mathcal{O}_S$-modules endowed with an integrable connection and the category of local systems of finite dimensional vector spaces on S^{an}. Such a functor sends any pair (ε, ∇) of a quasi-coherent locally free sheaf and a connection ∇ to the germs of horizontal sections ε^{∇} of the connection. It is an equivalence of categories. Indeed in the other direction we have the functor which sends any local system (locally constant sheaf) $\mathcal{L}$ to the pair $(\mathcal{L} \otimes_{\mathbb{C}} \mathcal{O}_S, 1 \otimes d)$.*

We recall that we have an *analytic* connection on S defined as follows. For every $s \in S$ the fiber X_s is a connected complex variety. By Poincaré lemma the sequence

$$0 \longrightarrow \mathbb{C} \longrightarrow \Omega^1_{X_s} \longrightarrow \Omega^2_{X_s} \longrightarrow \dots$$

is exact, i.e. $\Omega^\bullet_{X_s}$ is a resolution for the costant sheaf $\mathbb{C}$. Hence we have a quasi-isomorphism of complexes

$$\begin{array}{ccccc} \Omega^1_{X_s} & \longrightarrow & \Omega^2_{X_s} & \longrightarrow & \cdots \\ \uparrow & & \uparrow & & \\ \mathbb{C} & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

and taking hypercohomology

$$\mathbb{H}^i(X_s, \Omega^\bullet_X) \cong H^i(X_s, \mathbb{C}).$$

So we can compute the first de Rham cohomology as

$$H^1_{dR}(X_s/\mathbb{C}) = H^1(X_s, \mathbb{C}). \tag{C.4}$$

Letting s vary in S the complex vector spaces $H^1_{dR}(X_s/\mathbb{C})$ describe the relative the Rham cohomology $H^1_{dR}(X/S)$ and the $H^1(X_s, \mathbb{C})$'s determine a locally constant $\mathcal{O}_S$-module $R^1 f_* \mathbb{C}$. The isomorphism (C.4) on fibers yields an isomorphims of $\mathcal{O}_S$-modules

$$H^1_{dR}(X/S) = R^1 f_* \mathbb{C} \otimes_{\mathbb{C}} \mathcal{O}_S.$$

Hence we may see the natural connection $1 \otimes d$ that arises from the local system $R^1 f_* \mathbb{C}$ as a connection on the relative de Rham cohomology. Such a connection coincides exactly with the Gauss-Manin connection defined algebraically in the previous section. Indeed:

Proposition C.1. *The canonical morphism of sheaves*

$$R^q f_* \mathbb{C} = \mathbb{R}^1 f_* \Omega^\bullet_X \longrightarrow \mathbb{R}^1 f_* \Omega^\bullet_{X/S}$$

is an isomorphism between the source and the germs of horizontal sections for the Gauss-Manin connection $(\mathbb{R}^1 f_* \Omega^\bullet_{X/S})^{\nabla}$.

Proof. As in the section above, we consider the Koszul filtration of Ω^1_X and the corresponding spectral sequence

$$E_1^{p,q} = \Omega^p_S \otimes_{\mathcal{O}_S} \mathbb{R}^q f_* \Omega^\bullet_{X/S} \Longrightarrow \mathbb{R}^{p+q} f_* \Omega^\bullet_X.$$

The Gauss-Manin connection is defined as $\nabla = d_1^{0,q}$. Since $\mathbb{R}^q f_* \Omega^\bullet_{X/S}$ is quasi coherent and locally free we must have by Remark C.5.

$$\mathbb{R}^q f_* \Omega^\bullet_{X/S} \cong (\mathbb{R}^q f_* \Omega^\bullet_{X/S})^\nabla \otimes_{\mathbb{C}} \mathcal{O}_S.$$

So we may rewrite

$$E_1^{p,q} = \Omega^p_S \otimes_{\mathbb{C}} (\mathbb{R}^q f_* \Omega^\bullet_{X/S})^\nabla$$

and $d_1^{0,q} = 1 \otimes d$. Furthermore, since $(\mathbb{R}^q f_* \Omega^\bullet_{X/S})^\nabla$ is locally constant, hence flat, we may write the page two of the spectral sequence as

$$E_2^{p.q} = H^p(\Omega^\bullet_S) \otimes_{\mathbb{C}} (\mathbb{R}^q f_* \Omega^\bullet_{X/S})^\nabla.$$

Moreover by Poincaré Lemma we have

$$H^p(\Omega^\bullet_S) = R^p(\Gamma(X, \mathbb{C})) = \begin{cases} \mathbb{C} \text{ if p=0,} \\ 0 \text{ otherwise.} \end{cases}$$

Hence

$$E_2^{p.q} = \begin{cases} (\mathbb{R}^q f_* \Omega^\bullet_{X/S})^\nabla \text{ if p=0,} \\ 0 \text{ otherwise.} \end{cases}$$

This shows that the spectral sequence degenerates at page 2 and allows us to conclude that

$$\mathbb{R}^q f_* \Omega^\bullet_X = E_\infty^{0,q} = E_2^{0,q} = (\mathbb{R}^q f_* \Omega^\bullet_{X/S})^\nabla.$$

□

We can now begin the computation of the Gauss-Manin connection for $\mathbb{E}/Y(N)$ over $\mathbb{C}$. We recall that the modular curve $Y(N) = \Gamma(N)\backslash\mathbb{H}$ parametrizes classes of isomorphism of elliptic curves E_τ for $\tau \in Y(N)$ where $E_\tau = \mathbb{C}/\Lambda_\tau$, $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$. More concretely we may see $\mathbb{E}$ as the family of elliptic curves described locally affine by

$$Y^2 = 4X^3 - g_2(\tau)X - g_3(\tau) \quad \tau \in Y(N)$$

hence as an elliptic curve over R where R is the ring of holomorphic functions of $\Gamma(N)\backslash\mathbb{H}$. The global differentials on $Y(N)$ are just given by $Rd\tau$. Our aim is to compute the action of $\nabla(\frac{d}{d\tau})$ on the first de Rham cohomology. We work on fibers to choose a basis for the first de Rham cohomology. For any τ we choose a basis for $H^1_{dR}(E_\tau/\mathbb{C}) = H^1(E_\tau, \mathbb{C})$ as follows. We have a perfect pairing

$$\begin{aligned} H^1(E_\tau, \mathbb{C}) \times H_1(E_\tau, \mathbb{C}) &\longrightarrow \mathbb{C} \\ (\omega, \gamma) &\longrightarrow \int_\gamma \omega \end{aligned}$$

which allows us to identify $H^1_{dR}(E_\tau/\mathbb{C})$ with the dual of $H_1(E_\tau, \mathbb{C})$ which is the $\mathbb{C}$-vector space generated by the paths

$$\gamma_1(\tau) := [0, \tau],$$
$$\gamma_2(\tau) := [0, 1].$$

Moreover we have an alternate perfect pairing

$$H^1_{dR}(E_\tau/\mathbb{C}) \times H^1_{dR}(E_\tau/\mathbb{C}) \longrightarrow \mathbb{C}$$

which realizes

$$H^1_{dR}(E_\tau/\mathbb{C}) = H^1_{dR}(E_\tau/\mathbb{C})^\vee \cong H_1(E_\tau, \mathbb{C}).$$

Hence we choose a basis for $H^1_{dR}(E_\tau/\mathbb{C})$ which we keep denoting for simplicity $\gamma_1(\tau), \gamma_2(\tau)$ such that $\int_{\gamma_i(\tau)} \xi = \langle \gamma_i(\tau), \xi \rangle$ for every $\xi \in H^1_{dR}(E_\tau/\mathbb{C})$.
On the other hand we fix the canonical basis (see Remark A.7.) given by

$$\omega(\tau) = \frac{dX}{Y} = dz$$
$$\eta(\tau) = X\frac{dX}{Y} = \wp(z,\tau)dz$$

We want to express it in terms of $\gamma_1(\tau)$ and $\gamma_2(\tau)$. We denote the associated periods by $\omega_i(\tau) = \int_{\gamma_i(\tau)} \omega(\tau)$ and $\eta_i(\tau) = \int_{\gamma_i(\tau)} \eta(\tau)$ respectively. Then we must have

$$\omega(\tau) = \omega_1(\tau)\gamma_2(\tau) - \omega_2(\tau)\gamma_1(\tau)$$
$$\eta(\tau) = \eta_1(\tau)\gamma_2(\tau) - \eta_2(\tau)\gamma_1(\tau).$$

As τ varies in $\Gamma(N)\backslash\mathbb{H}$, $H^1(E_\tau, \mathbb{C})$ determines the local system $H^1_{dR}(\mathbb{E}/Y(N))^\nabla$, so the sections γ_1 and γ_2 obtained by the varying of τ are horizontal for the Gauss-Manin connection. Varying τ we also obtain the basis ω,η in $H^1_{dR}(\mathbb{E}/R)$. Such a basis is compatible with the Hodge filtration i.e. the choice of ω and η determines an isomorphism

$$H^1_{dR}(\mathbb{E}/R) \longrightarrow \underline{\omega}_{\mathbb{E}/R} \otimes \underline{\omega}^{-1}_{\mathbb{E}/R}$$

and η projects to a basis of $\underline{\omega}^{-1}_{\mathbb{E}/Y(N)}$ dual to ω [1]. Expressing it in terms of γ_1, γ_2 we have

$$\omega = \omega_1\gamma_2 - \omega_2\gamma_1,$$
$$\eta = \eta_1\gamma_2 - \eta_2\gamma_1.$$

Inverting the relation using the period relation of Legendre [2]

$$\eta_1\omega_1 - \eta_2\omega_1 = 2\pi i$$

we obtain

$$2\pi i \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} -\eta_2 & \omega_2 \\ -\eta_1 & \omega_1 \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix}.$$

Now we apply $\nabla\left(\frac{d}{d\tau}\right)$, recalling that it annihilates γ_1 and γ_2. Denoting $\frac{d}{d\tau}$ by $'$ we get

$$0 = \begin{pmatrix} -\eta_2' & \omega_2' \\ -\eta_1' & \omega_1' \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix} + \begin{pmatrix} -\eta_2 & \omega_2 \\ -\eta_1 & \omega_1 \end{pmatrix} \begin{pmatrix} \nabla\left(\frac{d}{d\tau}\right)(\omega) \\ \nabla\left(\frac{d}{d\tau}\right)(\eta) \end{pmatrix}$$

[1] See [8] A1.2.5.
[2] Wait for Remark C.6. for a proof.

and inverting again

$$\begin{pmatrix} \nabla\left(\frac{d}{d\tau}\right)(\omega) \\ \nabla\left(\frac{d}{d\tau}\right)(\eta) \end{pmatrix} = -\frac{1}{2\pi i}\begin{pmatrix} \omega_1 & -\omega_2 \\ \eta_1 & -\eta_2 \end{pmatrix}\begin{pmatrix} -\eta_2' & \omega_2' \\ -\eta_1' & \omega_1' \end{pmatrix}\begin{pmatrix} \omega \\ \eta \end{pmatrix}$$

$$= -\frac{1}{2\pi i}\begin{pmatrix} \omega_2\eta_1' - \omega_1\eta_2' & \omega_1\omega_2' - \omega_2\omega_1' \\ \eta_1'\eta_2 - \eta_1\eta_2' & \omega_2'\eta_1 - \eta_2\omega_1' \end{pmatrix}\begin{pmatrix} \omega \\ \eta \end{pmatrix}.$$

We may explicitly compute $\omega_1(\tau) = \tau$ and $\omega_2(\tau) = 1$ and Legendre's relation becomes $\eta_1 - \tau\eta_2 = 2\pi i$ which implies $\eta_1' - \tau\eta_2' = \eta_2$ and $\eta_1'\eta_2 - \eta_1\eta_2' = \eta_2^2 - 2\pi i\eta_2$. All in all, we can write

$$\begin{pmatrix} \nabla\left(\frac{d}{d\tau}\right)(\omega) \\ \nabla\left(\frac{d}{d\tau}\right)(\eta) \end{pmatrix} = -\frac{1}{2\pi i}\begin{pmatrix} \eta_2 & -1 \\ \eta_2^2 - 2\pi i\eta_2 & -\eta_2 \end{pmatrix}\begin{pmatrix} \omega \\ \eta \end{pmatrix}.$$

Lemma C.1.

$$\eta_2(\tau) = -\sum_{(n,m)\neq(0,0)} \frac{1}{(m\tau+n)^2} = -\frac{\pi}{3}E_2(\tau)$$

Proof. We recall that $\eta_2(\tau) = \wp(z,\tau)dz$. The Weirstrass $\wp$ function satisfies $-\wp(z,\tau) = \zeta'(z,\tau)$ where $\zeta(z,\tau)$ is the Weistrass ζ function defined as

$$\zeta(z) = \frac{1}{z} + \sum_{(m,n)\neq(0,0)} \frac{1}{z - m\tau - n} + \frac{1}{m\tau+n} + \frac{z}{(m\tau+n)^2}$$

which is an absolutely convergent sum so we can change the order of summation. With a direct computation we have

$$\eta_2(\tau) = \int_{\gamma_2(\tau)} \wp(z,\tau)dz = \int_0^1 -\zeta'(z,\tau)dz = \int_z^{z+1} -\zeta'(z,\tau)dz = \zeta(\tau,z) - \zeta(\tau,z+1)$$

And rearranging the terms in the sum we get the desired result [3]. □

Remark C.6. *In the style of the proof above one also sees that*

$$\eta_1 = -\sum_{(n,m)\neq(0,0)} \frac{\tau}{(m\tau+n)^2}$$

hence $\eta_2(-1/\tau) = \tau\eta_1(\tau)$. *With this in mind Legendre's relation is equivalent to*

$$\eta_2(-1/\tau) = \tau^2\eta_2(\tau) + 2\pi i\tau$$

that is nothing more than (1.1)

$$E_2(-1/\tau) = \tau^2 E_2(\tau) - \frac{6i\tau}{\pi}.$$

To conclude

$$\begin{pmatrix} \nabla\left(\frac{d}{d\tau}\right)(\omega) \\ \nabla\left(\frac{d}{d\tau}\right)(\eta) \end{pmatrix} = \frac{1}{2\pi i}\begin{pmatrix} \frac{\pi^2}{3}E_2(\tau) & 1 \\ \frac{\pi^4}{9}E_2(\tau) - \frac{12}{2\pi i}E_2'(\tau) & -\frac{\pi}{3}E_2(\tau) \end{pmatrix}.$$

[3] See [8] A.1.33.

Finally, through the change of variable $q = e^{2\pi i\tau}$ we obtain the Tate curve over $\mathbb{C}((q))$. We choose the canonical basis for $H^1_{dR}(\mathrm{Tate}(q)/\mathbb{C}((q)))$ determined by $\omega_{can} = \frac{dt}{t} = 2\pi i z = 2\pi i\omega$. Then the dual η_{can} is going to be $\frac{1}{2\pi i}\eta$. We have

$$\nabla(\theta)\begin{pmatrix}\omega\\ \eta\end{pmatrix} = \frac{1}{2\pi i}\begin{pmatrix}\nabla_\tau(\omega)\\ \nabla_\tau(\eta)\end{pmatrix} = \begin{pmatrix}\frac{-P}{12} & \frac{-1}{4\pi^2}\\ \frac{\pi^2}{36}(P^2-12\theta P) & \frac{P}{12}\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix}$$

and in terms of ω_{can} and η_{can}

$$\nabla(\theta)\begin{pmatrix}\omega_{can}\\ \eta_{can}\end{pmatrix} = \begin{pmatrix}\frac{-P}{12} & 1\\ \frac{P^2-12\theta P}{144} & \frac{P}{12}\end{pmatrix}\begin{pmatrix}\omega_{can}\\ \eta_{can}\end{pmatrix}. \tag{C.5}$$

C.4 The Kodaira-Spencer morphism

In our discussion we let K be a field and E an elliptic curve over a smooth affine scheme S over K. Let us denote $\underline{\omega}_{E/S} = \pi_*(\Omega^1_{E/S})$.
By Serre's duality the invertible sheaves $R^0\pi_*(\Omega^1_{E/S})$ and $R^1\pi_*(\mathcal{O}_E)$ are dual to each other. We denote the further by $\underline{\omega}^{\otimes -1}_{E/S}$ and we rewrite the Hodge filtration on the relative the Rham cohomology as

$$0 \longrightarrow \underline{\omega}_{E/S} \longrightarrow H^1_{dR}(E/S) \longrightarrow \underline{\omega}^{\otimes -1}_{E/S} \longrightarrow 0.$$

The Gauss Manin connection induces a mapping

$$\underline{\omega}_{E/S} \hookrightarrow H^1_{dR}(E/S) \xrightarrow{\nabla} \Omega^1_S \otimes_{\mathcal{O}_S} H^1_{dR}(E/S) \twoheadrightarrow \Omega^1_S \otimes_{\mathcal{O}_S} \underline{\omega}^{\otimes -1}_{E/S}$$

where the last arrow is the projection modulo $\underline{\omega}_{\mathbb{E}/Y(N)}$.

Remark C.7. *The above map $\phi : \underline{\omega}_{E/S} \longrightarrow \Omega^1_S \otimes_{\mathcal{O}_S} \underline{\omega}^{\otimes -1}_{E/S}$ is $\mathcal{O}_S$- linear. Indeed for any section ω and a of $\underline{\omega}_{E/S}$ and $\mathcal{O}_S$ respectively on an open of S we have*

$$\phi(a\omega) = [\nabla(a\omega)] = [da \otimes \omega + a\nabla(\omega)] = a[\nabla(\omega)] = \phi(\omega)$$

where by the square bracket we denote the image of sections through the projection modulo $\Omega^1_S \otimes_{\mathcal{O}_S} \underline{\omega}_{E/S}$.

Definition C.6. *The map ϕ induces an $\mathcal{O}_S$-linear morphism*

$$KS : \underline{\omega}^{\otimes 2}_{E/S} \longrightarrow \Omega^1_S$$

which we call the Kodaira-Spencer morphism.

Let us fix $N \geq 3$ an integer. Let $\mathrm{Tate}(q)$ be the Tate curve over $K((q^{1/N}))$ and let ω_{can} be its canonical differential.

Lemma C.2. *The image of $\omega^{\otimes 2}_{can}$ under the Kodaira-Spencer morphism is $\frac{dq}{q}$.*

Proof. The Kodaira-Spencer morphism $\underline{\omega}_{can}^{\otimes 2} \longrightarrow \Omega^1_{K(\!(q^{1/N})\!)}$ is induced by the mapping

$$\begin{tikzcd}
\underline{\omega}_{can} \arrow[r, hook] \arrow[rrd, bend left] & H^1_{dR}(\mathrm{Tate}(q)/K(\!(q^{1/N})\!)) \arrow[d, "\nabla"] & \\
& H^1_{dR}(\mathrm{Tate}(q)/K(\!(q^{1/N})\!)) \otimes \Omega^1_{K(\!(q^{1/N})\!)} \arrow[r, two heads] & \underline{\omega}_{can}^{\otimes -1} \otimes \Omega_{K(\!(q^{1/N})\!)}.
\end{tikzcd}$$

Let ω_{can}, η_{can} be a basis of $H^1_{dR}(\mathrm{Tate}(q)/K(\!(q^{1/N})\!))$ such that η_{can} projects to the dual basis to ω_{can} of $\underline{\omega}_{can}^{\otimes -1}$ i.e.

$$\eta_{can} \mod \underline{\omega}_{can} = \omega_{can}^{-1}.$$

To conclude it is sufficient to show that the composition of arrows above sends ω_{can} to $\omega_{can}^{-1} \otimes \frac{dq}{q}$. Let $q\frac{d}{dq}$ be the derivation dual to $\frac{dq}{q}$. Then we can recover $\nabla(\omega)$ from $\nabla\left(q\frac{d}{dq}\right)$ (Remark C.4) by $\nabla(\omega) = \nabla\left(q\frac{d}{dq}\right)(\omega) \otimes \frac{dq}{q}$. By the computation of section 3 of this appendix we have $\nabla\left(q\frac{d}{dq}\right)(\omega) = \eta_{can} - \frac{P}{12}\omega_{can}$. Hence

$$\nabla(\omega) = \nabla\left(q\frac{d}{dq}\right)(\omega) \otimes \frac{dq}{q} = \left(\eta_{can} - \frac{P}{12}\omega_{can}\right) \otimes \frac{dq}{q}$$

and projecting on $R^1\pi_*\mathcal{O}_{\mathrm{Tate}(q)}$ we obtain that ω_{can} is sent to $\omega_{can}^{-1} \otimes \frac{dq}{q}$. Hence we conclude that $KS(\omega_{can}^{\otimes 2}) = \frac{dq}{q}$. $\square$

Remark C.8. *The computation above shows that the Kodaira-Spencer map sends a basis of $\underline{\omega}_{can}^{\otimes 2}$ to a generator of $\Omega^1_{K(\!(q^{1/N})\!)}$. In particular KS is an isomorphism. Indeed all the maps in the definition of KS commute with base change and any elliptic curve E/S over the base field K (with level N-structure) can be obtained through pullback from the universal elliptic curve $\mathbb{E}/Y(N)$. This allows us to conclude that the Kodaira-Spencer morphism is an isomorphism for elliptic curves.*

Bibliography

[1] Bryden Cais. Serre's conjectures. In *Expository notes for a seminar*. Citeseer, 2009.

[2] Pierre Deligne and Luc Illusie. Relèvements modulo p et décomposition du complexe de de rham. *Inventiones mathematicae*, 89:247–270, 1987.

[3] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[4] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[5] Jun-ichi Igusa. Class number of a definite quaternion with prim discriminant. *Proceedings of the National Academy of Sciences*, 44(4):312–314, 1958.

[6] Nicholas M Katz. Nilpotent connections and the monodromy theorem: Applications of a result of turrittin. *Publications mathématiques de l'IHES*, 39:175–232, 1970.

[7] Nicholas M Katz. Algebraic solutions of differential equations (p-curvature and the hodge filtration). *Inventiones mathematicae*, 18(1):1–118, 1972.

[8] Nicholas M Katz. p-adic properties of modular schemes and modular forms. In *Modular Functions of One Variable III: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*, pages 69–190. Springer, 1973.

[9] Nicholas M Katz. A result on modular forms in characteristic p. In *Modular Functions of one Variable V: Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik July 2–14, 1976*, pages 53–61. Springer, 2006.

[10] Nicholas M Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108. Princeton University Press, 1985.

[11] Nicholas M Katz and Tadao Oda. On the differentiation of de rham cohomology classes with respect to parameters. *Journal of Mathematics of Kyoto University*, 8(2):199–213, 1968.

[12] Serge Lang. *Introduction to modular forms*, volume 222. Springer Science & Business Media, 2012.

[13] Jean-Pierre Serre. Formes modulaires et fonctions zêta p-adiques. In *Modular Functions of One Variable III: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*, pages 191–268. Springer, 1973.

[14] Jean-Pierre Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.

[15] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[16] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[17] Henry Peter Francis Swinnerton-Dyer. On l-adic representations and congruences for coefficients of modular forms. In *Modular Functions of One Variable III: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*, pages 1–55. Springer, 1973.

[18] Charles A Weibel. *An introduction to homological algebra*, volume 38. Cambridge university press, 1994.