Weil pairing and the Drinfeld modular curve

van der Heiden, Gerrit

Chapter 1

Introduction

This thesis deals with the study of Drinfeld modules and Drinfeld modular schemes. The main research questions that led to this thesis find their origin in [56], where an explicit description of the Drinfeld modular scheme which classifies $\mathbb{F}_q[t]$-Drinfeld modules of rank 2 is given. In this description this article addresses the following questions:

(1) What does the compactification of the Drinfeld modular scheme look like?

(2) Which moduli functor is associated to the compactified modular scheme?

These two questions are already answered for classical modular curves. Question (1) is answered in the classical case by Katz and Mazur in their book [33], in which they describe the compactification of the classical modular schemes. Question (2) is answered in the classical case by Deligne and Rapoport in their article [10], where they introduce 'generalized elliptic curves with level n-structure'. This latter concept enables them to describe the moduli functor associated to the compactified modular scheme in case the characteristic does not divide the level n.
The major part of this thesis addresses these two questions in the case of general A-Drinfeld modules. In Chapter 4 the Weil pairing for Drinfeld modules is developed. This pairing serves as a helpful tool in studying question (1) in Chapter 5. In Chapter 6 the first step towards answering question (2) is made. Besides the treatment of both these questions, the reader will find two independent number theoretical problems concerning Drinfeld modules in Chapter 2 and Chapter 3; cf. Section 1.3.

Before doing the technical, algebraic part of questions (1) and (2), I would like to give in this first chapter a proper introduction to the field of Drinfeld modules, and I would like to explain what questions (1) and (2) are about by describing them in the analytic case for both elliptic curves and Drinfeld modules.

The theory of Drinfeld modules is a relatively new area of research in function field arithmetic. Although in the 1930's L. Carlitz introduced an object which is now called an 'analytic Drinfeld module of rank 1', this topic does not appear in mathematics until Vladimir Gershonovich Drinfeld in 1974 introduces *elliptic modules* in his paper [11]. These elliptic modules are nowadays called *Drinfeld modules*. Of course, this latter name honours its inventor, but one could argue that Drinfeld's original terminology is more

appropriate: Drinfeld modules (and especially those of rank 2) are the function field analogue of elliptic curves.

Drinfeld's 1974 paper is quite remarkable; not in the least because Drinfeld was only nineteen years old at the time he wrote it. This paper has had an enormous impact on the development of function field arithmetic in the past three decades. However, Drinfeld seemed not mainly concerned with extending the theory of function field arithmetic. His true goal was to prove the *Langlands' correspondence* for Gl_2 over function fields. Let me give a small indication where this rather technical correspondence can be found in the landscape of mathematics.
In number theory there exists a correspondence which is known as *class field theory*. This correspondence was established in the 1920's by T. Takagi and E. Artin and can be considered as a large generalization of the quadratic reciprocity law introduced by Euler and proven by Gauss.
Let K be a global field, i.e., K is either a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$. In the former case K is called a *number field*, and in the latter case K is called a *function field*. Let K^{s} be a separable closure of K, and let $\mathrm{Gal}(K^{\mathrm{s}}/K)$ be the corresponding Galois group. Let V be an n-dimensional $\mathbb{C}$-vectorspace. An *n-dimensional representation of* $\mathrm{Gal}(K^{\mathrm{s}}/K)$ is a continuous group homomorphism

$$\rho : \mathrm{Gal}(K^{\mathrm{s}}/K) \longrightarrow \mathrm{Gl}(V).$$

Here $\mathrm{Gl}(V)$ denotes the group of all $\mathbb{C}$-automorphisms of V.
Class field theory states a bijection between the set of one-dimensional representations of $\mathrm{Gal}(K^{\mathrm{s}}/K)$ and a certain group called the idèle class group. A different formulation of this bijection describes all finite field extensions L of K with abelian Galois group; cf. Subsection 1.2.3.
In 1967 the Canadian mathematician Robert P. Langlands conjectured in a letter to André Weil a correspondence which is a vast generalization of class field theory to n-dimensional representations. This conjecture has important consequences. E.g., Andrew Wiles' proof of Fermat's last theorem is due to results in this direction for Gl_2 in the case $K = \mathbb{Q}$.

In 1974 little was known about this conjecture for Gl_2 in the function field case. In his paper Drinfeld made a first important contribution: he was able to prove a local version of Langlands' conjecture for Gl_2 and function fields. Three years later in [12], when completing his 'PhD', Drinfeld could give the proof of the global Langlands' correspondence for Gl_2 and function fields.[1]
Drinfeld's papers were much appreciated by the mathematical community and were considered to be of major importance: Drinfeld was awarded with a Fields medal in 1990.
At this occasion, Andrew Jaffe and Barry Mazur depict the mathematician Drinfeld as follows:

> 'His breakthroughs have the magic that one would expect of a revolutionary mathematical discovery: they have seemingly inexhaustible consequences. On

[1] cf. [13] for an overview by Drinfeld of his proof

> the other hand, they seem deeply personal pieces of mathematics: "only Drinfeld could have thought of them!" But contradictorily they seem transparently natural; once understood, "everyone should have thought of them!"' Cf. [21].

Although Drinfeld proved Langlands' conjecture only in the special case of dimension 2, his ideas are an essential turning point in the study of Langlands' conjecture over function fields. Along the lines of the strategy that Drinfeld developed in his articles, Laurent Lafforgue proved in 2000 Langlands' correspondence for function fields in every dimension; cf. [35]. Of course, setting out a basic strategy is not quite the same as actually proving the correspondence. As M. Rapoport writes about Lafforgue's work:

> 'Already Drinfeld's proof is extremely difficult. Lafforgue's proof is a real *tour de force*, taking up as it does several hundred pages of highly condensed reasoning. By his achievement Lafforgue has proved himself a mathematician of remarkable strength and perseverance.' Cf. [16].

Also Lafforgue received a Fields medal for his work on the Langlands' correspondence.
Although the theory of Drinfeld modules and its generalizations are mainly the concern of specialists, it is safe to conclude from this series of events that this theory is one of the important developments in mathematics during the last thirty years.

This short history of Drinfeld modules shows that one of the guiding problems that led to the development of this field has been solved. So what remains to be done?
To answer this question, let me point out another reason why Drinfeld's 1974 paper is remarkable. It is clear that the impact of Drinfeld's results intrigued a lot of mathematicians. However, the history of Drinfeld's article and its success may strike you as somewhat surprising once you start reading his paper. Probably the first thing that comes to mind while trying to cope with the mathematics in this paper, is that Drinfeld has not taken accessibility as his main concern.
If one consults the literature on the theory of Drinfeld modules, one finds that more people must share this experience. A number of mathematicians put a lot of effort in explaining Drinfeld's results and making them comprehensible. Work of Goss and Gekeler, together with proceedings such as [23] and [18] enable a larger audience of number theorists and algebraic geometers to enter the field. Moreover, these books show the major implications of Drinfeld modules for the theory of function fields.

I already mentioned the parts of the theory which I would like to clarify in this thesis. To give a better understanding of the guiding questions, I will proceed in this introduction as follows. I shall first discuss (part of) these problems in the context of elliptic curves over $\mathbb{C}$, the field of complex numbers. This section is only meant as a way of fixing ideas. Therefore, it can be skipped by anyone familiar with the theory of elliptic curves.
In the subsequent section I shall introduce Drinfeld modules and some of their properties. This leads up to a discussion of the problems considered in this thesis.
Finally, for completeness sake, I shall give a brief outline of each chapter in Section 1.3.

1.1 Elliptic curves

Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ such that ω_1 and ω_2 are linearly independent over $\mathbb{R}$, then Λ is a lattice of rank 2. We will assume that $\mathrm{im}(\omega_1/\omega_2) > 0$. An elliptic curve E over $\mathbb{C}$ is defined to be the curve $E := \mathbb{C}/\Lambda$ together with the group law induced on E by the addition of $\mathbb{C}$. Maybe $\mathbb{C}/\Lambda$ does not 'look' much like a curve. However, it turns that there exists an honest curve inside $\mathbb{P}^2_{\mathbb{C}}$ given by an equation

$$y^2 = x^3 - g_2 x - g_3 \tag{1.1}$$

such that there exists an complex analytic isomorphism between $\mathbb{C}/\Lambda$ and the $\mathbb{C}$-valued points of the curve given by (1.1). The constants g_2 and g_3 are determined by the lattice Λ.

Let Λ_1 and Λ_2 be two lattices inside $\mathbb{C}$ such that there exists an element $c \in \mathbb{C}$ with $c\Lambda_1 \subset \Lambda_2$, then c induces a map f_c from $E_1 = \mathbb{C}/\Lambda_1$ to $E_2 = \mathbb{C}/\Lambda_2$ given by $f_c : z \mapsto cz$. The maps f_c are called the *morphisms* from E_1 to E_2. A morphism is an *isomorphism* if $c\Lambda_1 = \Lambda_2$. A morphism from E to itself is called an *endomorphism*. The ring of endomorphisms is denoted $\mathrm{End}(E)$. Clearly, multiplication with $n \in \mathbb{Z}$ is an endomorphism. Hence,

$$\mathbb{Z} \subset \mathrm{End}(E).$$

For any $n \in \mathbb{N}$ we can consider the *group of n-torsion points* $E[n]$. This group is defined as

$$E[n] := \{x \in E \mid n \cdot x = 0\}.$$

Suppose that $z \in \mathbb{C}$, then

$$z + \Lambda \in E[n] \Longleftrightarrow z \in \frac{1}{n}\Lambda.$$

This gives us the following explicit description of the group of n-torsion points:

$$E[n] = \frac{1}{n}\Lambda/\Lambda = \frac{\omega_1}{n}\mathbb{Z}/\omega_1\mathbb{Z} \oplus \frac{\omega_2}{n}\mathbb{Z}/\omega_2\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})^2.$$

1.1.1 The Weil pairing

A tool which plays an important role in this thesis is the function field analogue of the *Weil e_n-pairing*. There is a geometric definition of the Weil pairing which defines this pairing not only for elliptic curves, but more generally for principally polarized abelian varieties. We prefer to give here a more elementary definition. Let

$$\mu_n = \{e^{\frac{2\pi i k}{n}} \mid k \in \{0, \ldots, n-1\}\}$$

denote the group of nth roots of unity for some $n \in \mathbb{N}$. The Weil pairing is a bilinear, non-degenerate, alternating map on the n-torsion:

$$e_n : E[n] \times E[n] \longrightarrow \mu_n.$$

To define e_n, we first recall some facts on functions and divisors. These facts can all be found in Chapter III of [52].
A *divisor* is a finite, formal sum

$$D = \sum_i m_i[D_i], \quad m_i \in \mathbb{Z}, \quad D_i \in E.$$

The *support* of D is the set consisting of those D_i for which $m_i \neq 0$.
Let $\mathbb{C}(E)$ denote the function field of E. This is the field consisting of all elliptic functions on E. An *elliptic function* is a meromorphic function

$$g : E \longrightarrow \mathbb{C} \cup \{\infty\}.$$

We associate a divisor $\mathrm{div}(g)$ to g. Write $\mathrm{div}(g) = \sum_i n_i[D_i]$ with $n_i \in \mathbb{Z}$ and $D_i \in E$, then $\mathrm{div}(g)$ is determined by the following two properties:

(1) The support of $\mathrm{div}(g)$ is equal to the set of all zeroes and poles of g.

(2) If $n_i > 0$, then g has a zero of order n_i in $[D_i]$. If $n_i < 0$, then g has a pole of order $-n_i$ in $[D_i]$.

Two divisors D_1, D_2 are called *linearly equivalent* if their difference $D_1 - D_2$ is the divisor of an elliptic function. We denote this as $D_1 \sim D_2$.
Let $D = \sum_i m_i[D_i]$ be a divisor, and let g be an elliptic function such that the support of D and $\mathrm{div}(g)$ are disjoint, then we write

$$g(D) := \prod_i g(D_i)^{m_i}.$$

Two divisors D_1, D_2 are called *linearly equivalent* if their difference $D_1 - D_2$ is the divisor of an elliptic function. We denote this as $D_1 \sim D_2$.

Consider $P, Q \in E[n]$. We can associate the divisors $[P]-[0]$ and $[Q]-[0]$ to these points. Let $D_P \sim [P] - [0]$ and $D_Q \sim [Q] - [0]$ such that D_P and D_Q have disjoint support.
As P and Q are n-torsion points, the divisors nD_P and nD_Q are the divisors of elliptic functions f_P and f_Q, respectively.

The Weil pairing is defined as

$$e_n(P, Q) := \frac{f_P(D_Q)}{f_Q(D_P)}.$$

Remark 1.1.1. To see that $e_n(P, Q)$ is indeed an nth root of unity, one needs *Weil reciprocity*: for two elliptic functions g_1, g_2 we have

$$g_1(\mathrm{div}(g_2)) = g_2(\mathrm{div}(g_1)).$$

Consequently,

$$e_n(P, Q)^n = \left(\frac{f_P(D_Q)}{f_Q(D_P)}\right)^n = \frac{f_P(\mathrm{div}(f_Q))}{f_Q(\mathrm{div}(f_P))} = 1.$$

Weil reciprocity also explains why the definition of e_n does not depend on the choice of the particular divisor D_P (respectively D_Q) in the linear equivalence class of $[P] - [0]$ (respectively $[Q] - [0]$).

From this definition it is not difficult to see that e_n is both bilinear and alternating. As $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, there exists an obvious action of $\mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$ on $E[n]$. As e_n is alternating and bilinear, the Weil pairing e_n is *equivariant* with respect to this action. This means that for all $\alpha \in \mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$ and for all $P, Q \in E[n]$

$$e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\det(\alpha)}.$$

We shall compute e_n explicitly. Elliptic functions can be described in terms of the *Weierstraß σ-function*. We denote $\Lambda^* := \Lambda \backslash \{0\}$. By definition

$$\sigma(z) := z \prod_{\substack{\alpha \in \Lambda \\ \alpha \neq 0}} \left(1 - \frac{z}{\alpha}\right) e^{-\frac{z}{\alpha} - \frac{1}{2}\left(\frac{z}{\alpha}\right)^2}.$$

We state the following properties of the Weierstraß σ-function; cf. Chapter VI of [52].

(1) For every $\alpha \in \Lambda$ with $\alpha \notin 2\Lambda$

$$\sigma(z + \alpha) = -e^{\eta(\alpha)(z + \frac{\alpha}{2})} \sigma(z). \tag{1.2}$$

Here $\eta(\alpha)$ does not depend on z.

(2) Since $\mathrm{im}(\omega_1/\omega_2) > 0$, the elements $\eta(\omega_1)$ and $\eta(\omega_2)$ satisfy the *Legendre relation*:

$$\omega_2 \eta(\omega_1) - \omega_1 \eta(\omega_2) = 2\pi i. \tag{1.3}$$

(3) Let $D = \sum_i m_i [D_i]$ be a divisor with $D_i \in \mathbb{C}$. Assume that $\sum_i m_i = 0$ and that $\sum_i m_i D_i = \xi \in \Lambda$, then there exists an elliptic function g such that its divisor equals D. If we assume that $\xi = 0$, then we have in fact

$$g = \prod_i \sigma(z - D_i)^{m_i}. \tag{1.4}$$

(4) If $\xi \neq 0$, then we may replace D by $D - [\xi] + [0]$. This is called *normalizing*. As D and $D - [\xi] + [0]$ are the same divisors over E, we see that

$$g = \sigma(z)\sigma(z - \xi)^{-1} \prod_i \left(\sigma(z - D_i)^{m_i}\right).$$

Suppose that $P, Q \in E[n]$. Consider f_P to be the function with divisor nD_P with $D_P = [P] - [0]$. After normalizing we get

$$f_P = \left(\frac{\sigma(z - P)}{\sigma(z)}\right)^n \frac{\sigma(z)}{\sigma(z - nP)}.$$

Similarly, we would like to take for f_Q the function with divisor $n[Q] - n[0]$. However, the definition of the Weil pairing requires that the divisors of f_P and f_Q have disjoint support. So instead we take $D_Q = [T + Q] - [T]$ with $T \in E[n]$ such that both T and

$T+Q$ are distinct from P and 0. The divisor D_Q is linearly equivalent to $[Q]-[0]$. Let f_Q be the function whose divisor is nD_Q. After normalizing we get

$$f_Q = \left(\frac{\sigma(z-(T+Q))}{\sigma(z-T)}\right)^n \frac{\sigma(z)}{\sigma(z-nQ)}.$$

Recall that $E[n]$ is generated by $\frac{\omega_1}{n}$ and $\frac{\omega_2}{n}$. So e_n is determined by $e_n(\frac{\omega_1}{n}, \frac{\omega_2}{n})$. We can compute this latter nth root of unity explicitly. Let $P = \frac{\omega_1}{n}$ and $Q = \frac{\omega_2}{n}$. Using $\sigma(z) = \sigma(-z)$ and the functional equation (1.2), it is a straightforward matter to compute that

$$e_n(P,Q) = e^{\eta(\omega_2)P - \eta(\omega_1)Q}.$$

By the Legendre relation (1.3) we see that $n(\eta(\omega_2)P - \eta(\omega_1)Q) = -2\pi i$. Consequently,

$$e_n(P,Q) = e^{\frac{-2\pi i}{n}} = \zeta_n^{-1}.$$

Remark 1.1.2. In the sequel we often consider lattices of the form $\Lambda = \mathbb{Z} + \mathbb{Z}\omega$ with $\mathrm{im}(\omega) > 0$. In this case, as $\mathrm{im}(\omega/1) > 0$, we see that

$$e_n\left(\frac{1}{n}, \frac{\omega}{n}\right) = \zeta_n.$$

Tate curves

There is also another way of describing elliptic curves. We include this description as well, as it prepares for the description of the Tate elliptic curve. Consider the exponential map

$$e : \mathbb{C} \longrightarrow \mathbb{C}^*, \quad z \mapsto e^{2\pi i z}.$$

Let $\omega \in \mathbb{C}$ with $\mathrm{im}(\omega) > 0$, and set $q := e(\omega)$. The image of $\Lambda_\omega = \mathbb{Z} + \mathbb{Z}\omega$ is

$$e(\Lambda_\omega) = \{q^i \mid i \in \mathbb{Z}\} =: \langle q \rangle.$$

In fact, e gives an isomorphism

$$e : E \xrightarrow{\sim} \mathbb{C}^*/\langle q \rangle.$$

Let $\mathcal{C} = \mathbb{C}^*/\langle q \rangle$. The n-torsion of $\mathcal{C}$ is

$$\mathcal{C}[n] := \{x \in \mathcal{C} \mid x^n = 1\}.$$

By construction $\mathcal{C}[n]$ is the image of $E[n]$ under e. Generators of $\mathcal{C}[n]$ as $\mathbb{Z}$-module are $\zeta_n = e^{\frac{2\pi i}{n}}$ and $\beta = e^{\frac{2\pi i \omega}{n}}$, with $\beta^n = q$. So we can write

$$\mathcal{C}[n] \cong \mu_n \oplus \mathbb{Z}/n\mathbb{Z}.$$

Of course, the Weil pairing yields a map $\mathcal{C}[n] \times \mathcal{C}[n] \longrightarrow \mu_n$.

1.1.2 The moduli problem for elliptic curves

Classifying elliptic curves is an important problem. To classify all isomorphy classes of elliptic curves over $\mathbb{C}$, we look for a curve $Y(1)$ over $\mathbb{C}$ such that every point on this curve corresponds to a unique isomorphy class of elliptic curves over $\mathbb{C}$.
Another important *moduli problem* is classifying pairs (E, λ) over $\mathbb{C}$ where E is an elliptic curve and λ is a so-called *level n-structure*. Equipping an elliptic curve with a level n-structure means fixing an isomorphism

$$\lambda : (\mathbb{Z}/n\mathbb{Z})^2 \xrightarrow{\sim} E[n].$$

The pair (E, λ) is called an *elliptic curve with level n-structure* over $\mathbb{C}$.
It turns out that there indeed exist curves $Y(1)$ and $Y(n)$ which classify isomorphy classes of elliptic curves and isomorphy classes of elliptic curves with level n-structure. We will describe $Y(1)$ and $Y(n)$; cf. [10] and [57].

The curve $Y(1)$.
To classify the isomorphy classes of elliptic curves, we consider the Poincaré upper half plane

$$\mathcal{H} := \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}.$$

The group $\mathrm{Sl}_2(\mathbb{Z})$ acts on $\mathcal{H}$ as follows. For all $\sigma = (\sigma_{i,j}) \in \mathrm{Sl}_2(\mathbb{Z})$ and for all $z \in \mathcal{H}$ we define

$$\sigma(z) := \frac{\sigma_{1,1}z + \sigma_{1,2}}{\sigma_{2,1}z + \sigma_{2,2}} \in \mathcal{H}.$$

Let $\omega \in \mathcal{H}$ and let

$$\Lambda_\omega := \mathbb{Z} + \mathbb{Z}\omega.$$

We write E_ω for the elliptic curve corresponding to Λ_ω. Clearly, every elliptic curve E over $\mathbb{C}$ is isomorphic to some E_ω. However, the isomorphy class of E_ω is not determined by a unique ω. In fact, it is not difficult to see that

$$E_\omega \cong E_{\omega'} \iff \text{ there is an element } \sigma \in \mathrm{Sl}_2(\mathbb{Z}) \text{ such that } \omega' = \sigma(\omega).$$

Namely, the isomorphy $c\Lambda_\omega = \Lambda_{\omega'}$ is given by $c = \sigma_{2,1}\omega' + \sigma_{1,1}$ and an easy computation yields $c\omega = -\sigma_{2,2}\omega' + \sigma_{1,2}$.
We conclude that every point of the quotient space

$$Y(1) = \mathrm{Sl}_2(\mathbb{Z})\backslash\mathcal{H}$$

corresponds to a unique isomorphy class of elliptic curves over $\mathbb{C}$.

Remark 1.1.3. Another important way of classifying the isomorphy classes of elliptic curves is the j-invariant. This j-invariant associates to each lattice Λ a complex number $j(\Lambda) \in \mathbb{C}$, which is called the *$j$-invariant of E*; cf. Chapter VI in [52]. This j-invariant only depends on the isomorphy class, and it gives rise to an isomorphism

$$j : Y(1) = \mathrm{Sl}_2(\mathbb{Z})\backslash\mathcal{H} \longrightarrow \mathbb{A}^1(\mathbb{C}) = \mathbb{C}. \tag{1.5}$$

The curve $Y(n)$.
Something similar can be done for isomorphy classes of elliptic curves with level n-structure (E, λ). The elliptic curve with level n-structure (E_1, λ_1) is called *isomorphic* to (E_2, λ_2) if and only if there exists an element $c \in \mathbb{C}^*$ such that $\Lambda_1 = c\Lambda_2$ and $\lambda_1 = c\lambda_2$.

To classify all elliptic curves with level n-structure, we first classify a special class of pairs (E, λ). Let $\omega \in \mathcal{H}$. The lattice Λ_ω is the image of the $\mathbb{Z}$-module homomorphism

$$f_\omega : \mathbb{Z}^2 \longrightarrow \mathbb{C}, \quad (a, b) \mapsto a\omega + b.$$

The map f_ω can be extended in a natural way to a $\mathbb{Q}$-linear homomorphism

$$f_\omega : \mathbb{Q}^2 \longrightarrow \mathbb{C}.$$

It is not difficult to see that the image of $(n^{-1}\mathbb{Z})^2$ under f_ω consists precisely of those elements in $\mathbb{C}$ which are mapped to $E[n]$ under the map $\mathbb{C} \longrightarrow \mathbb{C}/\Lambda_\omega$. Consequently, f_ω induces a natural map

$$(n^{-1}\mathbb{Z}/\mathbb{Z})^2 \xrightarrow{\sim} E[n], \quad (a, b) \mapsto f_\omega(a, b).$$

The natural isomorphism $(\mathbb{Z}/n\mathbb{Z})^2 \xrightarrow{\sim} (n^{-1}\mathbb{Z}/\mathbb{Z})^2$ gives rise to the canonical level n-structure λ_ω on E_ω

$$\lambda_\omega : (\mathbb{Z}/n\mathbb{Z})^2 \xrightarrow{\sim} E[n].$$

Therefore, we can associate to any $\omega \in \mathcal{H}$ the pair $(E_\omega, \lambda_\omega)$. Again, the isomorphy class of such a pair is not uniquely determined by ω. To see which ω's give rise to the same isomorphy class $(E_\omega, \lambda_\omega)$, we consider the action of $\mathrm{Sl}_2(\mathbb{Z})$ on these pairs.

Let $\sigma = (\sigma_{i,j}) \in \mathrm{Sl}_2(\mathbb{Z})$. We define $\tilde{\sigma}$ to be the image of $-\sigma^{-1}$ under the reduction map

$$\mathrm{Sl}_2(\mathbb{Z}) \longrightarrow \mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z}).$$

The action of $\mathrm{Sl}_2(\mathbb{Z})$ on lattices extends to an action on a pair $(E_\omega, \lambda_\omega)$ as follows:
for all $\sigma \in \mathrm{Sl}_2(\mathbb{Z})$

$$\sigma(E_\omega, \lambda_\omega) := (E_{\sigma(\omega)}, \lambda_{\sigma(\omega)} \circ \tilde{\sigma}).$$

This action is defined in such a way that

$$(E_\omega, \lambda_\omega) \cong \sigma(E_\omega, \lambda_\omega).$$

Let $\Gamma(n)$ be the kernel of the map $\mathrm{Sl}_2(\mathbb{Z}) \longrightarrow \mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})$:

$$\Gamma(n) = \{\sigma \in \mathrm{Sl}_2(\mathbb{Z}) \mid \sigma = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \text{ and } a, b, c, d \equiv 0 \bmod n\}$$

Let $\omega, \omega' \in \mathcal{H}$. We saw above that $E_\omega \cong E_{\omega'}$ if and only if $\omega = \sigma(\omega')$ for some $\sigma \in \mathrm{Sl}_2(\mathbb{Z})$. However, if $\omega = \sigma(\omega')$, then

$$\sigma : (E_\omega, \lambda_\omega) \mapsto (E_{\omega'}, \lambda_{\omega'} \circ \tilde{\sigma}).$$

Note that $\tilde{\sigma}$ is trivial if and only if $\sigma \in \Gamma(n)$. Hence,

$$(E_\omega, \lambda_\omega) \cong (E_{\omega'}, \lambda_{\omega'}) \iff \text{there is an element } \sigma \in \Gamma(n) \text{ with } \omega = \sigma(\omega').$$

Consequently, the quotient space

$$\Gamma(n)\backslash\mathcal{H}$$

classifies the isomorphy classes of pairs of the form $(E_\omega, \lambda_\omega)$.

To classify all pairs (E, λ), note that not every elliptic curve with level n-structure (E, λ) over $\mathbb{C}$ is isomorphic to a pair $(E_\omega, \lambda_\omega)$. This is due to the fact that we can alter the level n-structure by elements of $\mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$. However, for every (E, λ) there does exist a pair $(\omega, \alpha) \in \mathcal{H} \times \mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$ such that

$$(E, \lambda) \cong (E_\omega, \lambda_\omega \circ \alpha).$$

There exists an action of $\mathrm{Sl}_2(\mathbb{Z})$ on pairs $(E_\omega, \lambda_\omega \circ \alpha)$ as follows: for every $\sigma \in \mathrm{Sl}_2(\mathbb{Z})$ define

$$\sigma(E_\omega, \lambda_\omega \circ \alpha) := (E_{\sigma(\omega)}, \lambda_\omega \circ \tilde{\sigma} \circ \alpha).$$

In the sequel we will say that $\sigma \in \mathrm{Sl}_2(\mathbb{Z})$ gives an action on pairs (ω, α) by $\sigma(\omega, \alpha) = (\sigma(\omega), \tilde{\sigma} \circ \alpha)$, and we will say that the pair (ω, α) is isomorphic to (ω', α') if

$$(E_\omega, \lambda_\omega \circ \alpha) \cong (E_{\omega'}, \lambda_{\omega'} \circ \alpha').$$

Consequently,

$$(\omega, \alpha) \cong \sigma(\omega, \alpha).$$

To find all pairs (ω, α) which give rise to the same isomorphy class, we use the Weil pairing. For any pair $(E_\omega, \lambda_\omega)$ we have by earlier computations

$$e_n\left(\lambda_\omega(1,0), \lambda_\omega(0,1)\right) = e_n\left(\frac{1}{n}, \frac{\omega}{n}\right) = \zeta_n.$$

Let $\alpha \in \mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$ and set $\lambda = \lambda_\omega \circ \alpha$, then

$$e_n(\lambda(1,0), \lambda(0,1)) = \zeta_n^{\det(\alpha)}.$$

In this way, the Weil pairing gives rise to a map

$$\mathcal{H} \times \mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mu_n, \quad (\omega, \alpha) \mapsto \zeta_n^{\det(\alpha)}.$$

Lemma 1.1.4. *A pair (E, λ) over $\mathbb{C}$ is isomorphic to $(E_\omega, \lambda_\omega)$ for some $\omega \in \mathcal{H}$ if and only if*

$$e_n(\lambda(1,0), \lambda(0,1)) = \zeta_n.$$

Proof. First note that $(\omega, \alpha) \cong (\omega', 1)$ for some $\omega' \in \mathcal{H}$ if and only if $\det(\alpha) = 1 \bmod N$. Namely, as $\sigma(\omega, \alpha) = (\sigma(\omega), \tilde{\sigma} \circ \alpha))$, there exists an element $\sigma \in \mathrm{Sl}_2(\mathbb{Z})$ with $\tilde{\sigma} \circ \alpha = 1$ if and only if α is in the image of the reduction map $\mathrm{Sl}_2(\mathbb{Z}) \longrightarrow \mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})$, i.e., if and only if $\det(\alpha) = 1$.
Suppose that the lattice of E is given by $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\mathrm{im}(\omega_2/\omega_1) > 0$. The isomorphism given by $c = \frac{1}{\omega_1}$ maps (E, λ) to $(E_\omega, \lambda_\omega \circ \alpha)$ with $\omega = \omega_2/\omega_1$. By our previous computations

$$e_n(\lambda(1,0), \lambda(0,1)) = \zeta_n^{\det(\alpha)}.$$

□

According to this lemma, a pair

$$(\omega, \alpha) \in \mathcal{H} \times \mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$$

is isomorphic to some $(\omega', 1)$ if and only if

$$(\omega, \alpha) \in \mathcal{H} \times \mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z}).$$

The space which classifies all pairs $(\omega', 1)$ is $\Gamma(n)\backslash\mathcal{H}$. As

$$\mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})/\mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*,$$

the space

$$Y(n) := (\Gamma(n)\backslash\mathcal{H}) \times (\mathbb{Z}/n\mathbb{Z})^*$$

classifies all isomorphy classes of elliptic curves with level n-structure over $\mathbb{C}$. This space can be seen as $\#(\mathbb{Z}/n\mathbb{Z})^*$ copies of the Riemann surface $\Gamma(n)\backslash\mathcal{H}$. The action of the Weil pairing on $\mathcal{H} \times \mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$ induces a map

$$e_n : Y(n) \longrightarrow \mu_n, \quad (\omega, \alpha) \mapsto \zeta_n^{\det(\alpha)}.$$

This shows that the Weil pairing labels the connected components of $Y(n)$.

1.1.3 Cusps and the Tate elliptic curve

From now on we will assume that $n \geq 3$. The spaces $Y(1)$ and $Y(n)$ are not compact, but can be compactified by adding some points. In fact, it is well-known that the Riemann surface $Y(1)$ is isomorphic to the projective line over $\mathbb{C}$ minus one point. Consequently, the compactification $X(1)$ of $Y(1)$ is isomorphic to $\mathbb{P}^1_{\mathbb{C}}$. The set of *cusps* of $X(1)$ is by definition $X(1) - Y(1)$. So the curve $X(1)$ has only one cusp. We choose coordinates of $X(1)$ such that this cusp is given by $(1:0)$, called the point at ∞.
The map $\mathcal{H} \longrightarrow \mathrm{Sl}_2(\mathbb{Z})\backslash\mathcal{H}$ can be extended to a map

$$\overline{\mathcal{H}} \longrightarrow X(1)$$

such that also the action of $\mathrm{Sl}_2(\mathbb{Z})$ extends. It turns out that the cusps of $\overline{\mathcal{H}}$ are the points $\mathbb{P}^1(\mathbb{Q})$. The cusps of $\mathcal{H}$ are exactly the points which are identified with $(1:0)$ under the action of $\mathrm{Sl}_2(\mathbb{Z})$.
Let $X(n)$ be the compactification of $Y(n)$. Then $X(n)$ consists of $\#(\mathbb{Z}/n\mathbb{Z})^*$ connected components which are each isomorphic to the compactification of $\Gamma(n)\backslash\mathcal{H}$. The set of cusps of $\Gamma(n)\backslash\mathcal{H}$ must be $\Gamma(n)\backslash\mathbb{P}^1(\mathbb{Q})$. Note that the subgroup

$$\begin{pmatrix} \pm 1 & k \\ 0 & \pm 1 \end{pmatrix} \subset \mathrm{Sl}_2(\mathbb{Z})$$

is the subgroup which acts trivially on $(1:0)$. The image of this subgroup in $\mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})$ has $2n$ elements. As $\Gamma(n)$ is the kernel of $\mathrm{Sl}_2(\mathbb{Z}) \longrightarrow \mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})$, it follows that the number of cusps of $\Gamma(n)\backslash\mathcal{H}$ equals

$$\frac{\#\mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})}{2n}.$$

There are two natural questions concerning the cusps of $X(n)$.

(1) Can we interpret the cusps?

(2) Can we extend the functor represented by $Y(n)$ to a functor represented by $X(n)$?

To indicate an answer to these questions, we will need a stronger property of the curve $Y(n)$. We have seen that every point $\eta \in Y(n)$ corresponds to a pair (ω, α) and to an isomorphy class $(E_\omega, \lambda_\omega \circ \alpha)$ over $\mathbb{C}$. We say that there is a *family of elliptic curves over* $Y(n)$. This family is universal. This implies the following. Let K be a $\mathbb{C}$-field, and let (E, λ) be an elliptic curve E over K with a level n-structure λ. Then there is a unique point $\eta \in Y(n)$ such that the image of the corresponding pair $(E_\omega, \lambda_\omega \circ \alpha)$ under the natural map $\mathbb{C} \longrightarrow K$ is K-isomorphic to (E, λ).

The *Tate elliptic curve* $\mathcal{T}$ is an important curve which describes what happens at the cusps. We describe $\mathcal{T}$ only for the connected component $\Gamma(n)\backslash\mathcal{H}$ of $Y(n)$ consisting of the pairs (E, λ) with

$$e_n(\lambda(1,0), \lambda(0,1)) = \zeta_n.$$

The *Tate elliptic curve* is an elliptic curve defined over the field $\mathbb{C}(\!(t)\!)$ as

$$\mathcal{T} := \mathbb{C}(\!(t)\!)^* / \langle t^{nk} \mid k \in \mathbb{Z} \rangle.$$

The n-torsion is

$$\mathcal{T}[n] = \{x \in \mathcal{T} \mid x^n = 1\} = \mu_n \oplus \mathbb{Z}/n\mathbb{Z}.$$

We equip $\mathcal{T}$ with a level n-structure

$$\lambda_{\mathcal{T}} : (\mathbb{Z}/n\mathbb{Z})^2 \longrightarrow \mathcal{T}[n]$$

which is given by

$$(1,0) \mapsto \zeta_n, \quad (0,1) \mapsto t.$$

A *Tate elliptic curve with level n-structure* is a pair $(\mathcal{T}, \lambda_{\mathcal{T}} \circ \tilde{\sigma})$ with $\sigma \in \mathrm{Sl}_2(\mathbb{Z})$. Note that the automorphism group of $\mathcal{T}$ is generated by the following two automorphisms

$$\begin{array}{ll} [-1]: & \mathcal{T} \longrightarrow \mathcal{T}, \quad c \mapsto \frac{1}{c} \\ \rho: & \mathcal{T} \longrightarrow \mathcal{T}, \quad c \mapsto \zeta_n c. \end{array}$$

It is not difficult to see that

$$[-1] : (\mathcal{T}, \lambda_{\mathcal{T}}) \mapsto (\mathcal{T}, \lambda_{\mathcal{T}} \circ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix})$$

and

$$\rho^k : (\mathcal{T}, \lambda_{\mathcal{T}}) \mapsto (\mathcal{T}, \lambda_{\mathcal{T}} \circ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}).$$

So if we choose representatives $\tilde{\sigma}_i$ of the subgroup

$$N := \begin{pmatrix} \pm 1 & k \\ 0 & \pm 1 \end{pmatrix}$$

in $\mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})$, then the pairs $(\mathcal{T}, \lambda_{\mathcal{T}} \circ \tilde{\sigma}_i)$ are $\frac{\#\mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})}{2n}$ distinct isomorphy classes of Tate elliptic curves with level n-structure.

This Tate elliptic curve helps us in studying the cusps as follows. The curve $\mathcal{T}$ has the following affine equation:

$$y^2 + xy = x^3 + Bx + C, \quad B, C \in q^n\mathbb{C}[\![q^n]\!];$$

cf. [57]. So there is a model of $\mathcal{T}$ inside $\mathbb{P}^2_{\mathbb{C}[\![q]\!]}$. This model of $\mathcal{T}$ defines outside $q = 0$ an elliptic curve, but at $q = 0$ it has bad reduction: its equation at $q = 0$ is

$$y^2 + xy = x^3,$$

and this equation has a double point in $(0, 0)$. Consequently, at $q = 0$ the model of the Tate elliptic curve no longer gives rise to an elliptic curve.

Remark 1.1.5. The map which sends the analytic description of the Tate elliptic curve to the $\mathbb{C}[\![q]\!]$-valued points of the above algebraic model of the Tate elliptic curve maps the analytic torsion point t to a pair (x, y) which is not $\mathbb{C}[\![q]\!]$-rational. The other direct summand μ_n of the n-torsion is $\mathbb{C}[\![q]\!]$-rational.

Let us take a closer look at the model of $\mathcal{T}$. We can consider q as a parameter. Mapping $q \mapsto c \in \mathbb{C}\backslash\{0\}$ maps the pair $(\mathcal{T}, \lambda_{\mathcal{T}})$ to a genuine elliptic curve with level n-structure over $\mathbb{C}$. Therefore, this gives rise to a point of $Y(n)$.
At $q = 0$ the Tate elliptic curve $\mathcal{T}$ does not reduce to an elliptic curve. Therefore, the pair $(\mathcal{T}, \lambda_{\mathcal{T}})$ does not give rise to a point of $Y(n)$ under the map $q \mapsto 0$. However, if we let (q_i) be a sequence with $q_i \in \mathbb{C}\backslash\{0\}$ and $q_i \longrightarrow 0$, we get a sequence of points in $Y(n) \subset X(n)$. As $X(n)$ is compact, this sequence converges in $X(n)$. We conclude the reduction of the pair $(\mathcal{T}, \lambda_{\mathcal{T}})$ at $q = 0$ corresponds to a cusp of $X(n)$.

This more or less indicates how a pair $(\mathcal{T}, \lambda_{\mathcal{T}} \circ \tilde{\sigma}_i)$ gives rise to a unique cusp of $X(n)$. Similarly, every pair $(\mathcal{T}, \lambda_{\mathcal{T}} \circ \tilde{\sigma}_i)$ gives rise to a unique cusp of $X(n)$. Because the number of distinct pairs $(\mathcal{T}, \lambda_{\mathcal{T}} \circ \tilde{\sigma}_i)$ equals the number of cusps of $X(n)$, we see how we can use the Tate elliptic curve with level n-structure to describe the cusps. In fact, from an algebraic point of view, the scheme $\oplus_i \mathbb{C}[\![t]\!]_{\tilde{\sigma}_i}$ together with the pairs $(\mathcal{T}, \lambda_{\mathcal{T}} \circ \tilde{\sigma}_i)$ above $\mathbb{C}[\![t]\!]_{\tilde{\sigma}_i}$ describes what is called *the formal neighbourhood* of the cusps of $X(n)$.

The other question (2) asks whether we can use the pairs $(\mathcal{T}, \lambda_{\mathcal{T}} \circ \tilde{\sigma}_i)$ to extend the universal family $\{(E_\omega, \lambda_\omega \circ \alpha)$ above $Y(n)$ to a family above $X(n)$. There is one major problem which obstructs this: only one direct summand $\mathcal{T}[n]$ is $\mathbb{C}[\![t]\!]$-rational; cf. Remark 1.1.5. Therefore, we cannot extend the level n-structure to a map above the cusps.
The natural way to repair this, is to alter the model of $\mathcal{T}$. This is done by Deligne and Rapoport in [10]. The reduction of the given model of Tate elliptic curve does not have a group structure at $t = 0$. By deleting the double point $(0, 0)$ from this reduction, we get the multiplicative group $\mathbb{G}_m$ over $\mathbb{C}$. However, this group does not have enough n-torsion points to extend the notion of a level n-structure: $\mathbb{G}_m[n] \cong \mu_n$.
To solve this, they replace the model of the Tate elliptic curve by the Néron model whose reduction at $t = 0$ is an n-gon of $\mathbb{P}^1$'s over $\mathbb{C}$.

After deleting the intersection points, we get n copies of $\mathbb{G}_m$. This gives us a group structure which is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{G}_m$ and, therefore, enough n-torsion points; cf. [10] and [56]. This Néron model of the Tate elliptic curve together with its group structure is called a *generalized elliptic curve*. Using this model, Deligne and Rapoport can also define an extension of a level n-structure to $X(n)$ and can describe the moduli functor represented by $X(n)$.

1.2 Drinfeld modules

Let p denote a prime number and let q denote a power of p. By $\mathbb{F}_q$ we denote the finite field with q elements. Throughout this section we will assume $A = \mathbb{F}_q[t]$ unless stated otherwise. From a number theoretic point of view the ring $A = \mathbb{F}_q[t]$ has a lot properties in common with $\mathbb{Z}$, and the rational function field $\mathbb{F}_q(t)$ shares a lot of properties with $\mathbb{Q}$. We can stress this analogy even further by completing both fields along the valuation at ∞. (This valuation is the Archimedean one in the number field case and the one corresponding to $\frac{1}{t}$ in the function field case.) This completion of $\mathbb{Q}$ is $\mathbb{R}$, and this completion of $\mathbb{F}_q(t)$ is the field of Laurent series $\mathbb{F}_q(\!(\frac{1}{t})\!)$. The latter field is denoted by K_∞.
Furthermore, we may take the algebraic closure $\mathbb{C}$ of $\mathbb{R}$. The field of complex numbers $\mathbb{C}$ has the nice property that it is complete again. This is not the case for the algebraic closure of $\mathbb{F}_q(\!(\frac{1}{t})\!)$. However, if we take the completion of the algebraic closure of $\mathbb{F}_q(\!(\frac{1}{t})\!)$, then we end up with a field which is both algebraically closed and complete. This field is the function field analogue of $\mathbb{C}$ and is denoted by $\mathbb{C}_\infty$.

1.2.1 Definition of a Drinfeld module over a field

Let K be an A-field. This means that there exists a ring homomorphism

$$\gamma : A \longrightarrow K.$$

Let $K\{\tau\}$ be the following skew polynomial ring. Its elements are finite sums $\sum_i k_i\tau^i$ with $k_i \in K$. Elements in this skew ring are added in the obvious way. Multiplication is determined by multiplication in K and by the rule $\tau k = k^q\tau$ for all $k \in K$.
We also define a ring homomorphism 'evaluation at 0'

$$\partial_0 : K\{\tau\} \longrightarrow K, \quad \sum_i k_i\tau^i \mapsto k_0.$$

Definition 1.2.1. A *Drinfeld module* over K is an $\mathbb{F}_q$-linear ring homomorphism

$$\varphi : A \longrightarrow K\{\tau\},$$

such that

(1) $\partial_0 \circ \varphi = \gamma$.

(2) There is an $a \in A$ such that $\varphi_a \neq \gamma(a)$.

It is a convention to write φ_a instead of $\varphi(a)$ for $a \in A$. Note that this definition shows how a Drinfeld module equips $K\{\tau\}$ with an A-module structure which by (2) is different from the one that $K\{\tau\}$ naturally inherits from γ.

A Drinfeld module over K has a *rank*. This is an integer $r \geq 1$ such that $\deg_\tau(\varphi_a) = r\deg(a)$ for all $a \in A$.

If we define

$$\tau : K \longrightarrow K, \quad k \mapsto k^q,$$

then φ induces an A-module structure on K, and it makes sense to consider the a-torsion points of K via φ. It turns out that the a-torsion has an interesting structure. In some sense this is remarkable, because if we take $K = \mathbb{F}_q(t)$ and consider the natural A-module structure on K, then the a-torsion is not interesting at all: the only a-torsion point in K is 0 for every $0 \neq a \in A$.
The a-torsion of a Drinfeld module of rank r for some $a \in A$ and $a \notin \ker(\gamma)$ has in fact a similar structure as the n-torsion of an elliptic curve:

$$\varphi[a](K^{\mathrm{s}}) \cong (A/aA)^r$$

as A-module. Here K^{s} denotes a separable closure of K.

A *morphism* between two Drinfeld modules ϕ and ψ over K is given by a skew polynomial $\xi \in K\{\tau\}$ such that

$$\xi\phi_a = \psi_a\xi \quad \text{for all } a \in A.$$

An *isomorphism* is a morphism which has an inverse.

A Drinfeld module is said to be of *general characteristic* if $\ker(\gamma) = 0$, otherwise it is said to have *characteristic* $\ker(\gamma)$.

Example 1.2.2. In case $A = \mathbb{F}_q[t]$, the Drinfeld module φ of rank r over an A-field K is determined by

$$\varphi_t = \gamma(t) + c_1\tau + \cdots + c_r\tau^r,$$

with $c_i \in K$ and $c_r \in K^*$. If $r = 1$ and $K = \overline{K}$ is algebraically closed, then the Drinfeld module φ given by

$$\varphi_t = \gamma(t) + c_1\tau$$

is isomorphic to ψ given by

$$\psi_t = \gamma(t) + \tau$$

via the isomorphism given by $\xi \in K$ with $\xi^{q-1} = \frac{1}{c_1}$. The Drinfeld module ψ is called the *Carlitz module*. This module was introduced by L. Carlitz in the 1930's. The t-torsion points of ψ are the roots of the polynomial

$$(\gamma(t) + \tau)(X) = \gamma(t)X + X^q.$$

It is not difficult to see that these roots are given by $\mathbb{F}_q\zeta$ with $\zeta = \sqrt[q-1]{-\gamma(t)}$.

In the sequel we will restrict ourselves mainly to Drinfeld modules of rank 2.

1.2.2 The analytic construction

The similarity between elliptic curves and Drinfeld modules, can easily be seen from an analytic point of view. Similar to elliptic curves over $\mathbb{C}$, Drinfeld modules can analytically be constructed from lattices in $\mathbb{C}_\infty$. Let L be a finite extension of K_∞ and let L^s be its separable closure inside $\mathbb{C}_\infty$. Let φ be a Drinfeld module of rank 2 over L.
A *lattice* Λ is a discrete A-module of finite rank in L^s such that it is invariant under the Galois group $\mathrm{Gal}(L^s/L)$.
A *morphism* over L between two lattices Λ_1 and Λ_2 is given by an element $c \in L$, such that $c\Lambda_1 \subset \Lambda_2$.
Drinfeld shows in his paper [11] that the following categories are equivalent

$$\left\{ \begin{array}{c} \text{isomorphy classes of} \\ \text{Drinfeld modules of} \\ \text{rank 2 over } L \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{isomorphy classes} \\ \text{of lattices of} \\ \text{rank 2 over } L \end{array} \right\}.$$

This equivalence is defined as follows. To a Drinfeld module of rank 2 one may associate an analytic morphism, the 'exponential map'

$$e : L^s \longrightarrow L^s.$$

The map e commutes with addition and is defined up to a scalar by the property

$$e \circ a = \varphi_a \circ e \quad \text{for all } a \in A. \tag{1.6}$$

The kernel of the exponential map is a lattice of rank 2 over L.

On the other hand, one can also associate to a lattice Λ of rank 2 a Drinfeld module of rank 2. The lattice gives rise to the following exponential map:

$$e : L \longrightarrow L, \quad z \mapsto e(z) = z \prod_{\alpha \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\alpha}\right).$$

For every $a \in A$ there exists a skew polynomial $P_a \in L\{\tau\}$ with $P_a \circ e = e \circ a$. It turns out that these polynomials P_a give rise to a Drinfeld module φ with $\varphi_a = P_a$.

1.2.3 Kronecker's Jugendtraum

> "Es handelt sich um meinen liebsten Jugendtraum, nämlich um den Nachweiß, daß die Abel'schen Gleichungen mit Quadratwurzeln rationaler Zahlen durch die Transformations-Gleichungen elliptischer Funktionen mit singulären Moduln grade so erschöpft werden, wie die ganzzahligen Abel'schen Gleichungen durch die Kreisteilungsgleichungen." [34, Vol. V, p. 455]

The similarity between elliptic curves and Drinfeld modules extends to explicit class field theory. Class field theory has to do with describing the abelian extensions of number fields or function fields. The Kronecker-Weber theorem gives an explicit version of this theory for $\mathbb{Q}$ by constructing the maximal abelian extension of $\mathbb{Q}$. This theorem states that the maximal abelian extension of $\mathbb{Q}$ is given by adjoining to $\mathbb{Q}$ the roots of unity

$e^{\frac{2\pi i}{n}}$ for all $n \in \mathbb{N}$.
To stress the analogy with the function field case, we can also say that we get the maximal abelian extension of $\mathbb{Q}$ by adjoining to $\mathbb{Q}$ all n-torsion points of the algebraic group $\mathbb{G}_{m,\mathbb{Q}}$ for all $n \in \mathbb{N}$.

There does not (yet) exist an explicit description of the maximal abelian extension of an arbitrary number field. But there is an explicit description of the maximal abelian extension of an imaginary quadratic number field K. This is a field of the form $K = \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{N}$ and d a non-square. The description of the maximal abelian extension of these fields is known as *Kronecker's Jugendtraum*; cf. [58].
Let E be an elliptic curve such that $\mathrm{End}(E)$ is isomorphic to the ring of integers of K. Moreover, let

$$\Phi_\Lambda(x) : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}$$

be the *Weber function*; cf. Appendix C in [52]. This Weber function can be given very explicitly in terms of Λ. The maximal abelian extension of K is then given by adjoining to K the j-invariant of E and the values $\Phi_\Lambda(t)$ where t runs through the n-torsion points $E[n]$ for all $n \in \mathbb{N}$.

In the function field case, one has for the function field $K = \mathbb{F}_q(t)$ an explicit description of the maximal abelian extension of K completely split at ∞.
Suppose that ψ is the Carlitz module over K:

$$\psi_t = t + \tau.$$

The maximal abelian extension completely split at ∞ can be constructed as follows. Let $(g) \subset A$ be a proper, non-zero ideal, and let $K(\psi[g])$ be the field obtained by adjoining the g-torsion points of ψ to K. This extension is tamely ramified at ∞. The decomposition group and ramification group of this extension at ∞ are both isomorphic to $\mathbb{F}_q^*$. Let $K^+(\psi[g]) = K(\psi[g])^{\mathbb{F}_q^*}$, i.e., the subfield of $K(\psi[g])$ fixed by the action of this subgroup $\mathbb{F}_q^*$. Hence $K^+(\psi[g])$ is completely split at ∞. The maximal abelian extension of K completely split at ∞ is the compositum of all $K^+(\psi[g])$.

In fact, one has this explicit description of the maximal abelian extension of K completely split at ∞ for every global function field K. So if we choose A arbitrary and let K be its quotient field, then we can say the following.
There exists a Drinfeld module ψ of rank 1 defined over the Hilbert class field H tamely ramified at ∞ of K. This field H is the subfield of $\mathbb{C}_\infty$ generated by K and the coefficients of ψ_a for some non-constant $a \in A$; it does not depend on the choice of a.
Let $I \subset A$ be a proper, non-zero ideal of A. Let $\psi[I] = \cap_{g \in I} \psi[g]$ be the I-torsion group of ψ. Define $H(\psi[I])$ to be the field obtained by adjoining $\psi[I]$ to H. Again, $H(\psi[I])$ is tamely ramified at ∞. Its decomposition group at ∞ is $G = \mathbb{F}_{q^{\deg(\infty)}}^*$. The subfield $H^+(\psi[I]) = H(\psi[I])^G$ is completely split at ∞. The maximal abelian extension of K completely split at ∞ equals the compositum of all $H^+(\psi[I])$'s. This construction is due to David Hayes. A nice description can be found in Chapter 7 of [22].

In his article in 1974 also Drinfeld gives a description of the maximal abelian extension completely split at ∞. He uses moduli schemes. Again, let $I \subset A$ be a proper non-zero

ideal. Let $M^1(I)$ denote the Drinfeld modular scheme of rank 1 and level I - we define what we mean by this later on. It turns out that the quotient field of $M^1(I)$ is isomorphic to the field $H^+(\psi[I])$ (or $K^+(\psi[I])$ if $A = \mathbb{F}_q[t]$). Moreover, the scheme $M^1(I)$ is affine and its corresponding ring is the ring of integers of $H^+(\psi[I])$.
The limit of these schemes

$$M^1 := \varprojlim M^1(I)$$

is an affine scheme whose corresponding ring is given by the integral closure of A inside the maximal abelian extension completely split at ∞ of the function field K.

1.2.4 The Weil pairing

The previous subsection shows that the f-torsion of a Drinfeld module of rank 1 can in some sense be seen as the function field analogue of the nth roots of unity. The analogy goes even further. In the previous chapter we described the Weil pairing for elliptic curves. There is in fact a Weil pairing for Drinfeld modules, as we will show in Chapter 4 of this thesis. In particular, see Section 4.5 for the Weil pairing and its properties.

Let us briefly indicate how we get this pairing. Suppose that a Drinfeld module φ of rank 2 over some A-field K is given, together with an element $f \in A \backslash \mathbb{F}_q$ which is not an element of the characteristic of φ. Write $\varphi[f]$ for the kernel of φ_f. The assumption on f implies that

$$\varphi[f](K^{\mathrm{s}}) \cong (A/fA)^2$$

as A-modules. The question is whether we can associate to φ a Drinfeld module ψ of rank 1 over the same field K such that there exists a natural, non-degenerate, alternating, bilinear map on the f-torsion points:

$$w_f : \varphi[f](K^{\mathrm{s}}) \times \varphi[f](K^{\mathrm{s}}) \longrightarrow \psi[f](K^{\mathrm{s}}).$$

The Weil pairing is defined by using the determinant of a Drinfeld module. However, from the definition of a Drinfeld module it is difficult to see what taking a determinant could mean. Therefore, we use the concept of abelian t-modules and t-motives. These concepts were introduced by Greg Anderson in [1], and they give a very helpful description of Drinfeld modules as a subcategory of an abelian category of t-motives. This enables us to define the the determinant of a Drinfeld module.
Using this determinant, we know which rank 1 Drinfeld module ψ to associate to φ. Moreover, the mod f-reduction of this construction yields the Weil pairing on the f-torsion of ψ.

Example 1.2.3. Suppose that φ is a rank 2 Drinfeld module over K given by

$$\varphi_t = \gamma(t) + c_1\tau + c_2\tau^2.$$

It turns out that the Drinfeld module ψ associated to φ is given by

$$\psi_t = \gamma(t) - c_2\tau.$$

Suppose that the t-torsion of φ is K-rational. The Weil pairing w_t is given as follows:

$$\varphi[t](K) \times \varphi[t](K) \longrightarrow \psi[t](K) \quad \text{by} \quad (x, y) \mapsto xy^q - x^q y.$$

The following easy computation shows that $w_t(x, y) \in \psi[t]$:

$$\psi_t(xy^q - x^q y) = \gamma(t)(xy^q - x^q y) - c_2(x^q y^{q^2} - x^{q^2} y^q) =$$

$$y^q(\gamma(t)x + c_1 x^q + c_2 x^{q^2}) - x^q(\gamma(t)y + c_1 y^q + c_2 y^{q^2}) = x^q \varphi_t(y) - y^q \varphi_t(x) = 0.$$

1.2.5 The analytic moduli problem

In the previous section we classified the isomorphy classes of elliptic curves with level n-structure over $\mathbb{C}$. Similarly, we can classify the isomorphy classes of Drinfeld modules with level f-structure.
Recall that a lattice is an A-module of finite rank which lies discretely in $\mathbb{C}_\infty$. As $A = \mathbb{F}_q[t]$, lattices are free A-modules. We will restrict our description to Drinfeld modules of rank 2. Consequently, the lattices corresponding to the Drinfeld modules are free A-modules of rank 2; cf. Section 2 in [57].

Let $Y = A \oplus A$. Let $\Omega^{(2)}$ denote the rigid analytic space

$$\Omega^{(2)} = \mathbb{P}^1_{\mathbb{C}_\infty} - K_\infty\text{-rational points in } \mathbb{P}^1_{\mathbb{C}_\infty}.$$

This space is the analogue of the space $\mathbb{C}\backslash\mathbb{R}$ in the classical case. If we divide out the space $\mathbb{C}\backslash\mathbb{R}$ by the action of ± 1, then we get the space $\mathcal{H}$ which played an important part in the classification of elliptic curves over $\mathbb{C}$.

To every $(x : 1) \in \Omega^{(2)}$ we associate an A-lattice Λ of rank 2 as follows. Let $g_x : Y \longrightarrow \mathbb{C}_\infty$ be an A-linear map given by

$$(a, b) \mapsto ax + b.$$

Let $\Lambda = g_x(Y)$, then Λ is indeed an A-lattice of rank 2. By extending scalars, g_x extends to a K_∞-linear map

$$g_x : Y \otimes_A K_\infty \longrightarrow \Lambda \otimes_A K_\infty.$$

By the analytic theory every Drinfeld module of rank 2 over $\mathbb{C}_\infty$ corresponds to such a lattice $\Lambda \subset \mathbb{C}_\infty$. Hence the map

$$\mathcal{G}_1 : \Omega^{(2)} \longrightarrow \left\{ \begin{array}{l} \text{isomorphy classes of Drinfeld modules} \\ \text{over } \mathbb{C}_\infty \text{ of rank 2} \end{array} \right\}.$$

given by

$$(x : 1) \mapsto \Lambda = g_x(Y)$$

is surjective.

There exists a natural action of $\mathrm{Gl}_2(A)$ on $\Omega^{(2)}$ given by

$$\sigma = (\sigma_{i,j}) : (x : 1) \mapsto (\sigma_{1,1}x + \sigma_{1,2} : \sigma_{2,1}x + \sigma_{2,2}) \quad \text{for all } \sigma \in \mathrm{Gl}_2(A).$$

Suppose that $(x:1),(y:1) \in \Omega^{(2)}$. The lattices $g_x(Y)$ and $g_y(Y)$ are isomorphic if and only if there exists an element $\sigma \in \mathrm{Gl}_2(A)$ mapping the A-basis $\{x,1\}$ to $\{y,1\}$. Or, equivalently, $(y:1) = \sigma(x:1)$. This shows that the space

$$\mathrm{Gl}_2(A)\backslash\Omega^{(2)}$$

classifies the isomorphy classes of Drinfeld modules of rank 2 over $\mathbb{C}_\infty$. Note the similarity with the classical case.

Let $\Lambda = g_x(Y)$. We equip Λ with a level f-structure for some non-constant $f \in A$. A level f-structure is an isomorphism

$$\lambda : (A/fA)^2 \longrightarrow f^{-1}\Lambda/\Lambda.$$

Let $(A/fA)^2 \xrightarrow{\sim} f^{-1}Y/Y$ be the canonical isomorphism, then the map g_x equips $\Lambda = g_x(Y)$ with a canonical level f-structure λ_x. This level structure is given by

$$\lambda_x(1,0) = \frac{x}{f} + \Lambda, \quad \lambda_x(0,1) = \frac{1}{f} + \Lambda.$$

There exists an action of $\mathrm{Gl}_2(A)$ on pairs $(g_x(Y), \lambda_x)$. For any $\sigma \in \mathrm{Gl}_2(A)$ we let $\tilde{\sigma}$ be the image of $-\sigma^{-1}$ under the reduction map $\mathrm{Gl}_2(A) \longrightarrow \mathrm{Gl}_2(A/fA)$. Then $\mathrm{Gl}_2(A)$ acts on a pair $(g_x(Y), \lambda_x)$ as

$$\sigma(g_x(Y), \lambda_x) = (g_{\sigma(x)}(Y), \lambda_x \circ \tilde{\sigma}).$$

Let

$$\Gamma(f) := \ker(\mathrm{Gl}_2(A) \longrightarrow \mathrm{Gl}_2(A/fA)).$$

By definition of this action

$$\sigma(g_x(Y), \lambda_x) \cong (g_x(Y), \lambda_x).$$

If a pair $(g_x(Y), \lambda_x)$ is isomorphic to $(g_y(Y), \lambda_y)$ then there is a $\sigma \in \mathrm{Gl}_2(A)$ with $\sigma(x) = y$ and then $(g_x(Y), \lambda_x) \cong (g_y(Y), \lambda_y \circ \tilde{\sigma})$. The latter is isomorphic to $(g_y(Y), \lambda_y)$ if and only if $\sigma \in \mathbb{F}_q^* \cdot \Gamma(f)$. This implies that the set of isomorphy classes of pairs $(g_x(Y), \lambda_x)$ is classified by the space

$$\mathbb{F}_q^* \cdot \Gamma(f)\backslash\Omega^{(2)}.$$

Remark 1.2.4. The $\mathbb{F}_q^*$ in this expression is 'new' compared to the elliptic curve case. The classical counterpart to $\Omega^{(2)}$ is not $\mathcal{H}$ but $\mathbb{C}\backslash\mathbb{R}$, and we get $\mathcal{H}$ by dividing out $\mathbb{C}\backslash\mathbb{R}$ by the action of the determinant of $\mathrm{Gl}_2(\mathbb{Z})$, which is ± 1. In the Drinfeld module case we have $\det(\mathrm{Gl}_2(A)) = \mathbb{F}_q^*$.

To classify all pairs $(g_x(Y), \lambda)$, we proceed as in the classical case. The space

$$\Omega^{(2)} \times \mathrm{Gl}_2(A/fA)$$

maps surjectively to the set of all isomorphy classes of pairs $(g_x(Y), \lambda)$. This map is given by

$$(x, \alpha) \mapsto (g_x(Y), \lambda_x \circ \alpha).$$

We say that two pairs (x, α) and (y, β) are isomorphic if and only if

$$(g_x(Y), \lambda_x \circ \alpha) \cong (g_y(Y), \lambda_y \circ \beta).$$

The group $\mathrm{Gl}_2(A)$ acts on these pairs (x, α) as follows:
for $\sigma \in \mathrm{Gl}_2(A)$ define

$$\sigma(x, \alpha) := (\sigma(x), \tilde{\sigma} \circ \alpha).$$

Lemma 1.2.5. *A pair (y, β) is isomorphic to a pair $(x, 1)$ for some x if and only if β is in the image of the reduction map $\mathrm{Gl}_2(A) \longrightarrow \mathrm{Gl}_2(A/fA)$.*

Proof. It is not difficult to see that (y, β) is isomorphic to a pair $(x, 1)$ if and only if there is an element $\sigma \in \mathrm{Gl}_2(A)$ with $\tilde{\sigma} \circ \beta = 1$ if and only if β is an element of the image of

$$\mathrm{Gl}_2(A) \longrightarrow \mathrm{Gl}_2(A/fA).$$

□

Because the reduction map $\mathrm{Sl}_2(A) \longrightarrow \mathrm{Sl}_2(A/fA)$ is surjective, it follows that

$$\mathrm{Gl}_2(A) \backslash \mathrm{Gl}_2(A/fA) \cong (A/fA)^*/\mathbb{F}_q^*.$$

Using the above lemma, it follows that the space

$$M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty} := (\mathbb{F}_q^* \cdot \Gamma(f) \backslash \Omega^{(2)}) \times ((A/fA)^*/\mathbb{F}_q^*)$$

classifies the isomorphy classes of Drinfeld modules of rank 2 with level f-structure over $\mathbb{C}_\infty$. In particular, it follows that the space $M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$ consists of $\#(A/fA)^*/\mathbb{F}_q^*$ connected components.

1.2.6 The Weil pairing and the Drinfeld modular curve

Recall that in the classical case $Y(n)$ does not only classify all isomorphy classes (E, λ) over $\mathbb{C}$, but is also comes equipped with a universal family of pairs (E, λ). Something similar is true for the curve $M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$. Every point of this curve corresponds to a rank 2 Drinfeld module φ equipped with a level f-structure λ.

Consider the space $M^1(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$ which classifies all Drinfeld modules of rank 1 with level f-structure. Geometrically, this latter space consists of $(A/fA)^*/\mathbb{F}_q^*$ points. Above each point there is a pair (ψ, μ) over $\mathbb{C}_\infty$ consisting of a Drinfeld module ψ of rank 1 and a level f-structure

$$\mu : A/fA \xrightarrow{\sim} \psi[f].$$

The group $(A/fA)^*$ acts on an isomorphy class (ψ, μ): for all $\rho \in (A/fA)^*$

$$\rho(\psi, \mu) := (\psi, \mu \circ \rho).$$

Note that $\rho(\psi, \mu) \cong (\psi, \mu \circ \rho)$ if and only if $\rho \in \mathbb{F}_q^*$. Namely, the element ρ gives rise to an automorphism of ψ. Therefore, $\mathbb{F}_q^*$ acts trivially. The action of $(A/fA)^*$ induces a transitive action of $(A/fA)^*$ on $M^1(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$.

This enables us to give a very explicit description of the Drinfeld module of rank 1 with level f-structure that exists above every point of $M^1(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$. Let ψ be the Carlitz module

$$\psi_t = t + \tau$$

and let μ be any level f-structure. The family above $M^1(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$ is given by the isomorphy classes of $(\psi, \mu \circ \rho)$ where ρ runs through $(A/fA)^*$.

We use the Weil pairing to associate to a pair (φ, λ) of rank 2 over $\mathbb{C}_\infty$ a pair (ψ, μ) of rank 1 over $\mathbb{C}_\infty$. The construction of the Weil pairing already associates a ψ to φ (up to an element in $\mathbb{C}^*_\infty$). We use the map

$$w_f : \varphi[f] \times \varphi[f] \longrightarrow \psi[f]$$

to associate μ to λ as follows: define

$$\mu(1) := w_f(\lambda(1,0), \lambda(0,1)).$$

The pair (ψ, μ) gives rise to a unique isomorphy class which does not depend on the choice of ψ.
Using the $\mathrm{Gl}_2(A/fA)$-equivariance of the Weil pairing, we see moreover that

$$\sigma(\varphi, \lambda) = (\varphi, \lambda \circ \sigma) \mapsto (\psi, \mu \circ \det(\sigma)) = \det(\sigma)(\psi, \mu).$$

This construction gives a map from the family of pairs (φ, λ) on $M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$ to the family of pairs (ψ, μ) on $M^1(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$. In fact, this map comes from a morphism

$$w_f : M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty} \longrightarrow M^1(f)^{\mathrm{an}}_{\mathbb{C}_\infty}.$$

By the $\mathrm{Gl}_2(A/fA)$-equivariance of w_f it follows that the Weil pairing labels the connected components of $M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$.

1.2.7 The Tate-Drinfeld module and the cusps

To compactify the Drinfeld modular curve, we construct an analogue of the j-invariant for elliptic curves. Let (φ, λ) be a pair of rank 2 over $\mathbb{C}_\infty$. Because $A = \mathbb{F}_q[t]$, the Drinfeld module φ is determined by $\varphi_t = t + c_1\tau + c_2\tau^2$. The *$j$-invariant* of φ is defined to be

$$j(\varphi) := \frac{c_1^{q+1}}{c_2}.$$

By construction, the j-invariant of two isomorphic Drinfeld modules is the same. Consequently, the j-invariant gives a morphism

$$M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty} \longrightarrow \mathbb{A}^{1,\mathrm{an}}_{\mathbb{C}_\infty}$$

from the Drinfeld modular curve to the affine line over $\mathbb{C}_\infty$.
Let $\overline{M}^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$ denote the compactification of $M^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$. The above map extends to a morphism

$$\overline{M}^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty} \longrightarrow \mathbb{P}^{1,\mathrm{an}}_{\mathbb{C}_\infty}.$$

The cusps of $\overline{M}^2(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$ all lie above the point at ∞ of the projective line.

As in the classical case, we address the two following questions.

(1) Can we interpret the cusps?

(2) Can extend the functor represented by $Y(n)$ to a functor represented by $X(n)$?

We remarked in the previous section on elliptic curves how the formal neighbourhood of the cusps of $X(n)$ can be described by the Tate elliptic curve. Analogous to the Tate elliptic curve, we can define the universal Tate-Drinfeld module; cf. Section 5.7.
The Tate-Drinfeld module is the direct sum of a number of copies of $\mathbb{C}_\infty[\![x]\!]$ equipped with a pair $(\varphi^{\mathrm{td}}, \lambda^{\mathrm{td}})$. The direct sum runs over the set $\mathrm{Gl}_2(A/fA)/N$ where

$$N = \begin{pmatrix} \mathbb{F}_q^* & A/fA \\ 0 & (A/fA)^* \end{pmatrix}.$$

The pair $(\varphi^{\mathrm{td}}, \lambda^{\mathrm{td}})$ has the following properties:

(1) The pair $(\varphi^{\mathrm{td}}, \lambda^{\mathrm{td}})$ is a Drinfeld module of rank 2 with level f-structure over $\oplus\mathbb{C}_\infty(\!(x)\!)$.

(2) The reduction φ^{td} mod (x) is the universal Drinfeld module ψ of rank 1 over $\oplus\mathbb{C}_\infty$.

As in the classical case, we show that the formal neighbourhood of the cusps is isomorphic to the universal Tate-Drinfeld module; cf. Proposition 5.9.1. In particular, it follows from this description that the scheme of cusps is isomorphic to a number of copies of $M^1(f)^{\mathrm{an}}_{\mathbb{C}_\infty}$; cf. Theorem 5.9.2.

The second question that we address, is whether we can describe the moduli functor represented by the compact space $\overline{M}^2(f)_{\mathbb{C}_\infty}$. As in the classical case the problem is to extend the level structure to something sensible above the cusps. To this end, we describe the Néron model of the Tate-Drinfeld module. In the Drinfeld case the reduction of this Néron model is a tree of $\mathbb{P}^1$'s. The open subscheme of this model on which there exists a group structure is isomorphic to a number of copies of affine group schemes $\mathbb{G}_a$. These constructions are the first step to formulating the moduli functor represented by $\overline{M}^2(f)_{\mathbb{C}_\infty}$.

1.3 Outline of this thesis

In this final part of the introduction I shall give an outline of this thesis. As the topics that we discuss in the latter three chapters have been the guiding line of the first part of the introduction, we will point out the contents of these chapters only very briefly and we pay some more attention to chapters 2 and 3.

Factoring polynomials with Drinfeld modules

In Chapter 2 we develop an algorithm to factor a polynomial $N \in \mathbb{F}_q[X]$ by using Drinfeld modules. This chapter is more or less readable for anyone who has done an undergraduate course in finite fields. The idea behind Algorithm 2.3.3 is analogous to the idea behind the so-called Elliptic Curve Method to factor a number $n \in \mathbb{N}$.

Let us give a brief exposition of this idea. By using the preliminary steps of the Cantor-Zassenhaus algorithm we may assume that N is a product of k distinct irreducible polynomials $P_i \in \mathbb{F}_q[X]$ all of the same degree d. The ring $B := \mathbb{F}_q[X]/(N)$ comes equipped with a natural $A = \mathbb{F}_q[X]$-action. By choosing a Drinfeld module

$$\varphi : A \longrightarrow B\{\tau\},$$

we can alter this A-action. The map φ_X acts as an $\mathbb{F}_q$-linear operator on each $B_i := \mathbb{F}_q[X]/(P_i)$. If we denote by f_i the characteristic polynomial, then φ defines an $\mathbb{F}_q[X]/f_i$-module structure on B_i. In general, f_i need not be irreducible of degree d anymore.
This can be used to factor N. In Example 2.3.2 we show in a simple case how the algorithm works. In the latter part of this chapter we also give a complexity analysis of the algorithm and compare it to Cantor-Zassenhaus.
The main idea of this algorithm can also be found in Potemine's unpublished thesis [44, ch. 4]. This chapter is based on [28].

A local-global problem for Drinfeld modules

In the third chapter, we deal with a problem whose classical analogue is known as a special case of the Hasse principle. Let x be some element in $\mathbb{Q}$ and let p be some prime number. Let l be a prime and let $\mathbb{Q}_l$ denote the completion of $\mathbb{Q}$ with respect to the valuation at l. Suppose that x is a p^{th}-power in $\mathbb{Q}_l$ for almost every l, is it then a p^{th}-power in $\mathbb{Q}$? This is in fact the case, as is shown in Theorem 9.1.3.ii in [43].
We can address the same problem for elliptic curves. Suppose that E is an elliptic curve over $\mathbb{Q}$. Let $x \in E(\mathbb{Q})$ be a point such that for (almost) every prime l there exists a $y_l \in E(\mathbb{Q}_l)$ such that $x = py_l$. Is there an element $y \in E(\mathbb{Q})$ such that $x = py$? We prove, using Galois cohomology, that the answer to this question is affirmative. This statement can also be found in [59] and [14].
The corresponding question for Drinfeld modules is the following. Let K be a function field with field of constants $\mathbb{F}_q$, let φ be a Drinfeld module of rank 2 over K, and let $(a) \subset A$ be a principal prime ideal. Let $x \in K$ such that for every place ν of K there exists an element $y_\nu \in K_\nu$ such that $x = \varphi_a(y_\nu)$. Is there an element $y \in K$ such that $x = \varphi_a(y)$? It turns out that there are examples for which this is not the case. We give a fairly complete treatment of what can occur: by using Galois cohomology we show that the local-global principle is true in many cases, and by using some Artin-Schreier theory we are able to construct examples for which the local-global principle does not hold. This chapter is based on [30].

Weil pairing for Drinfeld modules

In the fourth chapter we prove the existence of the Weil pairing over an A-field K. Essential for this construction is Anderson's paper [1], in which he introduces the concept of t-motives. In fact, the construction of the Weil pairing is more or less a corollary once Anderson's results are established. In this chapter we extend Anderson's definitions, which are given only for rational function fields, to arbitrary global function fields. In the final section of this chapter, we give an explicit description of the Weil pairing in case $A = \mathbb{F}_q[t]$ and $r = 2$.
This chapter is based on [29].

Weil pairing and the Drinfeld modular scheme

In the fifth chapter we consider the following four problems concerning the compactification of the Drinfeld modular scheme classifying Drinfeld modules of rank 2 with level f-structure over an A_f-scheme S.
(i) For every r we construct a morphism

$$w_f : M^r(f) \longrightarrow M^1(f)$$

extending the Weil pairing of the previous chapter to the modular scheme.
(ii) For $r = 2$ we define the Tate-Drinfeld module and describe its universal property. In the theory of modular curves, one should consider the Tate-Drinfeld module to be the analogue of the Tate-elliptic curve.
(iii) Using the Tate-Drinfeld module, we can describe the scheme of cusps of the compactification $\overline{M}^2(f)$ of $M^2(f)$.
(iv) Finally, we compute the number of geometric components of $M^2(f)$.
This chapter benefits a lot from the work of Thomas Lehmkuhl in [37] and Gebhard Böckle in [3]. The Weil pairing is an important tool in this chapter, and it enables us to give an alternative description of the compactification of the Drinfeld modular scheme of rank 2.

Drinfeld data on the compactified modular scheme

Finally, in the sixth chapter we describe the Néron model of the Tate-Drinfeld data that we have at the cusps of $\overline{M}^2(f)$. This is the analogue of the construction of the Néron model of the Tate elliptic curve as given by Deligne and Rapoport in [10].
Using this construction we can generalize the notion of a Drinfeld module with level f-structure to Drinfeld data defined over $\overline{M}^2(f)$. This is the first step to formulating the moduli functor represented by $\overline{M}^2(f)$.