manuscripta math. 99, 55 – 72 (1999)

Bartolomé López

A special integral basis for a plane model of the Drinfeld modular curve $X_1(\mathfrak{n})$ mod T

Received: 23 October 1998

Abstract. In this work we get some properties of the plane model $C_1(\mathfrak{n})$ (Section 3) of the reduction mod T of the Drinfeld modular curve $X_1(\mathfrak{n})$. The main result is the explicit presentation of a special integral basis for this model (Theorem 4.5). This integral basis is close to be minimal.

Introduction

It is known that the classical modular curve $X_1(n)$ has an explicit plane model (cf. [18]). In the frame of Coding Theory, a similar plane model of the reduction mod T of the Drinfeld modular curve $X_1(\mathfrak{n})$ was introduced in [16] ($\mathfrak{n}$ denotes a prime ideal in $\mathbb{F}_q[T]$). This plane model, that we denote in this work by $C_1(\mathfrak{n})$, is smooth in the affine part and has two singular points on the line at infinity. Let $P(x, y) \in \mathbb{F}_q[x, y]$ be the polynomial which defines $C_1(\mathfrak{n})$; put $n = \deg_y(P)$. Then the set $\{1, y, \ldots, y^{n-1}\}$ is an integral basis for the extension $\overline{\mathbb{F}}_q[x] \subset \overline{\mathbb{F}}_q(C_1(\mathfrak{n}))$. Nevertheless, it is not a minimal basis (see section 2 for the definition of minimal basis). We found an integral basis for this extension which is close to be minimal. We have calculated (cf. [15]) the complexity of constructing a minimal basis from that special integral basis by means of Coates' algorithm. This complexity is relatively low compared with the complexity of constructing a minimal basis from the basis $\{1, y, \ldots, y^{n-1}\}$: the estimate is $O(n^{6.5}(\log_q n)^7)$ in the first case; in the second case, the estimate is $O(n^{11.5})$.

We see this result as a non-trivial example on integral bases for plane curves which deserves further understanding. We think that a deeper comprehension of this example would help to obtain results on integral bases for more general families of plane curves.

We organize the contents of this paper as follows.

In Sect. 1, we first present Drinfeld modular curves analytically (over $\mathbf{C}$). These curves have canonical models defined over finite extensions of

B. López: Departamento de Matemáticas, Universidad de Cádiz, E-11510 Puerto Real (Cádiz), Spain. e-mail: bartolome.lopez@uca.es

Mathematics Subject Classification (1991): 11G09, 11R58, 11G20

$\mathbb{F}_q(T)$. Then we present Drinfeld modular curves as moduli varieties of Drinfeld modules. This allows us to study the reduction modulo a prime of those canonical models.

In Sect. 2, we recall some facts concerning the integral closure of $\overline{\mathbb{F}}_q[x] \subset \overline{\mathbb{F}}_q(C)$, where C is the plane curve defined by an absolutely irreducible polynomial $P(x, y) \in \mathbb{F}_q[x, y]$.

In Sect. 3, we present the plane model $C_1(\mathfrak{n})$ for the fiber $\overline{M}_1^2(\mathfrak{n})_{\mathfrak{p}}$; the symbol $\overline{M}_1^2(\mathfrak{n})$ denotes the scheme over Spec$((\mathbb{F}_q[T])[\mathfrak{n}^{-1}])$ defined at the end of section 1 and $\mathfrak{p}$ is a prime ideal in $(\mathbb{F}_q[T])[\mathfrak{n}^{-1}]$. The expansion of the functions $s_1 e_{(0,1/f)}^{q-1}$ and $s_2 e_{(0,1/f)}^{q^2-1}$ in the local parameter $t_{\mathfrak{n},\mathfrak{p}}$ at the cusps is also introduced in this section (the functions $s_1 e_{(0,1/f)}^{q-1}$ and $s_2 e_{(0,1/f)}^{q^2-1}$ are introduced in Remark 1.3, and $t_{\mathfrak{n},\mathfrak{p}}$ is introduced in Remark 3.5). This expansion is the tool to prove the Lemmas of Sect. 4.

Section 4 is the central part of the work. We present here a special integral basis for the plane model $C_1(\mathfrak{n})$ of the fiber $\overline{M}_1^2(\mathfrak{n})_{(T)}$ (Theorem 4.5). It is derived from Lemmas 4.1, 4.3 and 4.4.

1. Preliminaries

We will introduce some facts on Drinfeld modules; a reference for this is [13]. We also recall some definitions and results on Drinfeld modular curves which can be found in [19], [20] (Lecture 8) and [4].

Let $A := \mathbb{F}_q[T]$. Consider a field k such that there exists a morphism $\mathfrak{i} : A \to k$. Let $k\{\tau\}$ be the ring of non-commutative polynomials over k, where τ is the Frobenius endomorphism: if B is a k-algebra, then $\tau(\beta) = \beta^q$, $\beta \in B$. The product in $k\{\tau\}$ satisfies the rule $\tau\alpha = \alpha^q\tau$, where $\alpha \in k$. The ring $k\{\tau\}$ can be identified with the ring of q-additive polynomials $\sum_{i=0}^{l} \alpha_i Z^{q^i}$, where the product is given by substitution. A Drinfeld module of rank d over k is an $\mathbb{F}_q$-homomorphism $\phi : A \to k\{\tau\}$ defined by

$$\phi(T) = \mathfrak{i}(T)\tau^0 + \sum_{i=1}^{d} \alpha_i \tau^i ,$$

where $\alpha_i \in k$ and $\alpha_d \neq 0$. Two Drinfeld modules ϕ, ϕ' are isomorphic if there exists an element $u \in k^*$ such that $u \cdot \phi(a) = \phi'(a) \cdot u$ for any $a \in A$.

Let us now denote by $K = \mathbb{F}_q(T)$ the field of rational functions in an indeterminate T. We define on $\mathbb{F}_q(T)$ a valuation by $|a/b| = q^{\deg a - \deg b}$. The completion of K with respect to $|\ |$ is $K_\infty = \mathbb{F}_q((1/T))$. There exists a unique extension of the valuation $|\ |$ to the algebraic closure $\overline{K}_\infty$ of K_∞. The completion $\mathbf{C}$ of $\overline{K}_\infty$ is an algebraically closed field.

An A-lattice in $\mathbf{C}$ of rank d is a discrete, finitely generated A-module $\Lambda \subset \mathbf{C}$ such that $\dim_K K\Lambda = d$. We can associate to Λ the exponential function

$$e_\Lambda(z) = z \prod_{\beta \in \Lambda - \{0\}} (1 - z/\beta) \ .$$

Through the function e_Λ, we can construct a Drinfeld module of rank d. This construction establishes a bijection between lattices and Drinfeld modules. Homothetic lattices correspond to isomorphic Drinfeld modules. We will deal with Drinfeld modules of ranks one and two.

An important example of Drinfeld module is the *Carlitz* module of rank one, defined by

$$\rho(T) = T\tau^0 + \tau \ .$$

Let $L = \overline{\pi}A$ be the lattice corresponding to ρ. The element $\overline{\pi}$ is well-defined up to an element of $\mathbb{F}_q^*$. We define the functions

$$\mathbf{t}(z) = e_L(\overline{\pi}z)^{-1}, \quad t(z) = \mathbf{t}(z)^{q-1} \ . \tag{1}$$

The function $t(z)$ is the analogue to the classical function $e^{2\pi i z}$.

Any Drinfeld module of rank two over $\mathbf{C}$ is isomorphic to one given by

$$\phi_z(T) = T\tau^0 + g(z)\tau + \Delta(z)\tau^2 \ , \tag{2}$$

where $z \in \Omega = \mathbf{C} - K_\infty$, and $g(z)$ and $\Delta(z)$ are functions on Ω (cf. [6], subsection 5.1, p. 679). The group $\Gamma(1) := GL(2, A)$ acts on Ω in the following way: if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ and $z \in \Omega$, then

$$\gamma(z) = \frac{az + b}{cz + d} \ .$$

Two Drinfeld modules ϕ_z, $\phi_{z'}$ are isomorphic if and only if z and z' are equivalent by $\Gamma(1)$.

The space Ω has the structure of a rigid analytic space over $\mathbf{C}$. A meromorphic function h on Ω is said to be a *modular function of weight k* for a group Γ of finite index in $\Gamma(1)$ if

$$h\left(\frac{az + b}{cz + d}\right) = (cz + d)^k h(z) \ ,$$

for every $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. A modular function h is called *meromorphic at the cusp* ∞ if h has an expansion in the function $\mathbf{t}(z)$ of the form $\sum_{n \geq n_0} a_n \, \mathbf{t}(z)^n$. A modular function h is said to be a *modular form* if h is holomorphic on Ω and has an expansion of the form $\sum_{n \geq 0} a_n \, \mathbf{t}(z)^n$. The functions $g(z)$ and $\Delta(z)$ are examples of modular forms for the full group $\Gamma(1)$ of weights $q-1$ and q^2-1, respectively (cf. [12], p. 27). The function $j(z) = g(z)^{q+1}/\Delta(z)$ is a meromorphic modular function of weight 0 for $\Gamma(1)$. The modular forms $g(z)$ and $\Delta(z)$ have expansions in $t(z)$. More precisely, the power series in $t(z)$, $(\overline{\pi})^{1-q}g(z) = 1 + \ldots$ and $(\overline{\pi})^{1-q^2}\Delta(z) = -t(z) + \ldots$ have coefficients in A. Hence, the power series in t,

$$j(z) = -t(z)^{-1} + \ldots \tag{3}$$

has coefficients in A.

Let now $\mathfrak{n}$ be an ideal in A. The principal congruence subgroup $\Gamma(\mathfrak{n})$ of level $\mathfrak{n}$ in $\Gamma(1)$ is the group of matrices $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ such that $a, d \equiv 1 \bmod \mathfrak{n}$, $b, c \equiv 0 \bmod \mathfrak{n}$. A congruence subgroup of level $\mathfrak{n}$ is a group Γ which contains $\Gamma(\mathfrak{n})$. Distinguished examples of congruence subgroups (apart from $\Gamma(\mathfrak{n})$ itself) are

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : c \equiv 0 \bmod \mathfrak{n} \right\},$$

$$\Gamma_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : a \equiv 1 \bmod \mathfrak{n},\ c \equiv 0 \bmod \mathfrak{n} \right\}.$$

The quotient $Y = \Gamma\backslash\Omega$ has the structure of a rigid analytic space. The canonical smooth compactification of Y is the space $X = \Gamma\backslash\Omega^*$, supplied with a convenient topology, where $\Omega^* = \Omega \cup \mathbb{P}^1(K)$ (cf. [20], Lecture 8). The points of $\Gamma\backslash\mathbb{P}^1(K)$ are the cusps of X. We will denote by $X(\mathfrak{n})$, $X_0(\mathfrak{n})$ and $X_1(\mathfrak{n})$ the spaces $\Gamma(\mathfrak{n})\backslash\Omega^*$, $\Gamma_0(\mathfrak{n})\backslash\Omega^*$ and $\Gamma_1(\mathfrak{n})\backslash\Omega^*$, respectively.

Let us now consider a congruence subgroup Γ' such that $\Gamma' \subset \Gamma$. There is a natural projection $\lambda : \Gamma'\backslash\Omega^* \to \Gamma\backslash\Omega^*$. The ramification of λ can be obtained from the stabilizers of the points of Ω^* for the action of the groups Γ and Γ' as follows. Let $\varphi : \Omega^* \to \Gamma\backslash\Omega^*$ and $\varphi' : \Omega^* \to \Gamma'\backslash\Omega^*$ be the natural projections. For each point $z \in \Omega^*$, we consider the subgroups $\Gamma_z = \{\gamma \in \Gamma : \gamma(z) = z\}$ and $\Gamma'_z = \{\gamma' \in \Gamma' : \gamma'(z) = z\}$. Let $w \in \Gamma\backslash\Omega^*$ and $\lambda^{-1}(w) = \{p_1, \ldots, p_r\}$. We now consider points $z, z_1, \ldots, z_r \in \Omega^*$ such that $\varphi(z) = w$ and $\varphi'(z_i) = p_i$. Then, the ramification index of λ at p_i is $[\Gamma_{z_i} Z(\mathbb{F}_q) : \Gamma'_{z_i} Z(\mathbb{F}_q)]$, where $Z(\mathbb{F}_q)$ is the center of $\Gamma(1)$ (observe that the action of $Z(\mathbb{F}_q)$ on Ω^* is trivial). Furthermore, the points of $\lambda^{-1}(w)$ correspond to the double cosets of $\Gamma' Z(\mathbb{F}_q)\backslash\Gamma Z(\mathbb{F}_q)/\Gamma_z Z(\mathbb{F}_q)$ (compare with Proposition 1.37 of [22]).

In the sequel, $\mathfrak{n}$ will denote a *prime* ideal in A generated by a *monic* polynomial f:

$$f = T^m + a_{m-1}T^{m-1} + \ldots + a_0. \tag{4}$$

We now determine the ramification indices at the cusps of the projections $X_1(\mathfrak{n}) \to X_0(\mathfrak{n})$ and $X_0(\mathfrak{n}) \to \Gamma(1)\backslash\Omega^*$.

Proposition 1.1. *The cusps of* $X_0(\mathfrak{n})$ *are represented by* $0 = (1:0)$ *and* $\infty = (0:1)$. *The cusp* ∞ *of* $X_0(\mathfrak{n})$ *is unramified above* $X(1) = \Gamma(1)\backslash\Omega^*$, *and the cusp* 0 *is ramified with ramification index* q^m. *The curve* $X_1(\mathfrak{n})$ *has* $\frac{q^m-1}{q-1}$ *cusps above each cusp of* $X_0(\mathfrak{n})$.

Proof. The cusps of $X_0(\mathfrak{n})$ correspond to the double cosets of $\Gamma_0(\mathfrak{n})\backslash\Gamma(1)/\Gamma(1)_\infty$. A set of representatives of $\Gamma_0(\mathfrak{n})\backslash\Gamma(1)$ is

$$\left\{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} : \deg c < m\right\} \bigcup \left\{\begin{pmatrix} 0 & 1 \\ 1 & f \end{pmatrix}\right\}.$$

Hence, there are two double cosets in $\Gamma_0(\mathfrak{n})\backslash\Gamma(1)/\Gamma(1)_\infty$ which correspond to the matrices

$$\mathrm{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma_f = \begin{pmatrix} 0 & 1 \\ 1 & f \end{pmatrix}.$$

Thus, the cusps of $X_0(\mathfrak{n})$ are represented by ∞ and $\gamma_f(\infty) = 0$.

The claim on the ramification indices of the map $X_0(\mathfrak{n}) \to X(1)$ at ∞ and 0 follows from the fact that $\Gamma_0(\mathfrak{n})_\infty = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \in \mathbb{F}_q^*, b \in A\}$ and $\Gamma_0(\mathfrak{n})_0 = \{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, d \in \mathbb{F}_q^*, c \in \mathfrak{n}\}$.

Let $\lambda : X_1(\mathfrak{n}) \to X_0(\mathfrak{n})$ be the natural projection. We claim that λ is unramified at each cusp of $X_1(\mathfrak{n})$. We prove this for the cusps above ∞; the claim for the cusps above 0 follows from a similar argument. The set of matrices

$$G = \left\{\gamma_a = \begin{pmatrix} a & b \\ f & d \end{pmatrix} : a \text{ monic}, \deg a < m, \deg d < m, ad - bf = 1\right\}$$

is a set of representatives of $\Gamma_0(\mathfrak{n})/\Gamma_1(\mathfrak{n})Z(\mathbb{F}_q)$. Hence, the number of double cosets of $\Gamma_1(\mathfrak{n})Z(\mathbb{F}_q)\backslash\Gamma_0(\mathfrak{n})/\Gamma_0(\mathfrak{n})_\infty$ equals the cardinality of the quotient set $G/\sim$, where $\sim$ is the equivalence relation in G defined as follows:

$$\gamma_{a'} \sim \gamma_a \Leftrightarrow \text{there exists } \sigma \in \Gamma_0(\mathfrak{n})_\infty \text{ such that } \gamma_{a'} = \gamma_a\,\sigma.$$

From this definition, it is easy to check that if $\gamma_{a'} \sim \gamma_a$, then $\gamma_{a'} = \gamma_a$. This proves the claim. □

The space $X = \Gamma\backslash\Omega^*$ has the structure of a smooth projective curve over $\mathbf{C}$. The function field $\mathcal{M}(X)$ of X is the field of meromorphic functions on Ω which are invariant under the action of Γ. For instance, in the case of the full group $\Gamma(1)$, we have that $\mathcal{M}(X(1)) = \mathbf{C}(j(z))$. It is also possible to present explicit models of the function fields of $X_0(\mathfrak{n})$ and $X_1(\mathfrak{n})$. The function field of $X_0(\mathfrak{n})$ is $\mathbf{C}(j(z), j(fz))$. To introduce the function field of $X_1(\mathfrak{n})$ we define some modular forms for the group $\Gamma(\mathfrak{n})$.

Let us consider $\mathfrak{n} = (f)$, and $u = (u_1/f, u_2/f)$ such that $\deg u_i < \deg f$. Let ϕ_z be the Drinfeld module defined in equation (2) and Λ_z its corresponding lattice. For each u, we define the function

$$e_u(z) = e_{\Lambda_z}((u_1 z + u_2)/f)$$

on Ω. This function has an expansion in $\mathfrak{t}(z/f)$ (cf. equation (1)), which can be explicitly given as follows. Let

$$h_u(z) := \rho(u_1)(\mathfrak{t}(z/f)^{-1}) + e_L(\overline{\pi} u_2/f),$$

where ρ is the Carlitz module and L is the lattice corresponding to ρ. Then,

$$\overline{\pi} e_u(z) = h_u(z) \prod_{c \in A-\{0\}} \left(1 - \frac{h_u(z)}{\rho(c)(1/\mathfrak{t}(z))}\right) \tag{5}$$

(cf. [4], pp. 61-62). Now, the function field of $X_1(\mathfrak{n})$ is

$$\mathbf{C}\left(g(z)e_{(0,1/f)}(z)^{q-1}, \Delta(z)e_{(0,1/f)}(z)^{q^2-1}\right).$$

The curves $X_0(\mathfrak{n})$ and $X_1(\mathfrak{n})$ have canonical models defined over K that we will denote by $X_0(\mathfrak{n})/K$ and $X_1(\mathfrak{n})/K$, respectively. The function fields of $X_0(\mathfrak{n})/K$ and $X_1(\mathfrak{n})/K$ are:

$$\begin{aligned} &\mathcal{M}(X_0(\mathfrak{n})/K) = K(j(z), j(fz)), \\ &\mathcal{M}(X_1(\mathfrak{n})/K) = K\left(g(z)e_{(0,1/f)}(z)^{q-1}, \Delta(z)e_{(0,1/f)}(z)^{q^2-1}\right). \end{aligned} \tag{6}$$

The curves $X_0(\mathfrak{n})/K$ and $X_1(\mathfrak{n})/K$ have good reduction mod $\mathfrak{p}$, $\mathfrak{p} \in \mathrm{Spec}(A[\mathfrak{n}^{-1}])$. In order to introduce this result, we consider these curves as moduli varieties of Drinfeld modules. Details of the facts that we present here are in [17], [21] and [20]. We will deal with the case of $X_1(\mathfrak{n})$; the case of the curve $X_0(\mathfrak{n})$ is analogous.

Let $\mathfrak{n} = (f)$ be a prime ideal of A and let S be a scheme over $A[\mathfrak{n}^{-1}]$ with canonical morphism $\mathfrak{i} : A[\mathfrak{n}^{-1}] \to H^0(S, \mathcal{O}_S)$. A pair (E, ϕ), where E is a group scheme over S and $\phi : A[\mathfrak{n}^{-1}] \to \mathrm{End}_S(E)$ is a morphism from $A[\mathfrak{n}^{-1}]$ to the endomorphism ring of E as group scheme, is a Drinfeld module of rank d over S if there exists a covering of S by affine open subschemes $U = \mathrm{Spec}(R)$ such that $E_U \simeq \mathrm{Spec}(R[x])$ and

$$\phi(T)|_{\mathrm{Spec}(R)} = \mathfrak{i}(T)\tau^0 + \sum_{i=1}^{d} \alpha_i \tau^i ,$$

where τ is the q-power Frobenius endomorphism, $\alpha_i \in R$ and α_d is a unit in R.

Let (E, ϕ) be a Drinfeld module over S. We consider the subscheme of E of $\mathfrak{n}$-division points, $E_{\mathfrak{n}} = \ker \phi(f)$. A level $\mathfrak{n}$ structure on ϕ is an isomorphism

$$\alpha : (\mathfrak{n}^{-1}/A)^d \times_A S \simeq E_{\mathfrak{n}}$$

as group schemes over S.

Remark 1.2. The group scheme E, or more precisely, its sheaf of sections, is an invertible sheaf over S. There exist sections $s_i \in H^0(S, E^{1-q^i})$ such that $s_i|_{\mathrm{Spec}(R)} = \alpha_i$. Furthermore, if α is a level $\mathfrak{n}$ structure and $u \in (\mathfrak{n}^{-1}/A)^d$, then $\alpha(u)$ defines a section $e_u \in H^0(S, E)$.

The functor

$$\mathfrak{M}^d(\mathfrak{n})(S) = \left\{ \begin{array}{l} \text{Set of isomorphism classes of Drinfeld modules} \\ \text{over } S \text{ of rank } d \text{ with level } \mathfrak{n} \text{ structure} \end{array} \right\}$$

is representable by an affine scheme $M^d(\mathfrak{n})$ smooth over $A[\mathfrak{n}^{-1}]$. For $d = 2$, the fibers of the morphism $M^2(\mathfrak{n}) \to \mathrm{Spec}(A[\mathfrak{n}^{-1}])$ are affine curves.

From now on, we will assume $d = 2$. Let $\phi_{\mathfrak{n}}$ be the universal module of rank 2 over the scheme $M^2(\mathfrak{n})$ with level $\mathfrak{n}$ structure $\alpha : (\mathfrak{n}^{-1}/A)^2 \to E_{\mathfrak{n}}$, where E is the line bundle on $M^2(\mathfrak{n})$ associated with $\phi_{\mathfrak{n}}$. The sections s_1, s_2, e_u considered in Remark 1.2 satisfy

$$s_1^{q+1}/s_2,\, s_1 e_u^{q-1},\, s_2 e_u^{q^2-1} \in H^0(M^2(\mathfrak{n}), \mathcal{O}_{M^2(\mathfrak{n})}).$$

The group $GL(2, A/\mathfrak{n})/Z(\mathbb{F}_q)$ acts as a group of automorphisms on the scheme $M^2(\mathfrak{n})$ and the quotient by this action is $\mathbb{A}^1_{A[\mathfrak{n}^{-1}]}$. The natural projection $M^2(\mathfrak{n}) \to \mathbb{A}^1_{A[\mathfrak{n}^{-1}]}$ is given by the section $j = s_1^{q+1}/s_2$ on $M^2(\mathfrak{n})$. The action of $GL(2, A/\mathfrak{n})/Z(\mathbb{F}_q)$ on the sections $s_1 e_u^{q-1}$ and $s_2 e_u^{q^2-1}$ is the following: if $\gamma \in GL(2, A/\mathfrak{n})$, then

$$(s_1 e_u^{q-1})^\gamma = s_1 e_{u\gamma}^{q-1} \quad \text{and} \quad (s_2 e_u^{q^2-1})^\gamma = s_2 e_{u\gamma}^{q^2-1} .$$

Remark 1.3. The global sections s_1, s_2, j, $s_1 e_u^{q-1}$ and $s_2 e_u^{q^2-1}$ on $M^2(\mathfrak{n})$ define functions on each fiber $M^2(\mathfrak{n})_{\mathfrak{p}}$ of the morphism

$$M^2(\mathfrak{n}) \to \operatorname{Spec}(A[\mathfrak{n}^{-1}])$$

We denote both, sections on $M^2(\mathfrak{n})$ and functions on $M^2(\mathfrak{n})_{\mathfrak{p}}$, with the same symbol, if there is no risk of confusion.

The scheme $M^2(\mathfrak{n})$ has a canonical compactification $\overline{M}^2(\mathfrak{n})$ smooth and proper over $A[\mathfrak{n}^{-1}]$ (cf. [20], Lecture 9). The group $GL(2, A/\mathfrak{n})/Z(\mathbb{F}_q)$ acts on $\overline{M}^2(\mathfrak{n})$ and the quotient of this action is $\mathbb{P}^1_{A[\mathfrak{n}^{-1}]}$.

Let us now consider the subgroup $H_1(\mathfrak{n})$ of $GL(2, A/\mathfrak{n})$, where

$$H_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, A/\mathfrak{n}) : a = 1, c = 0 \right\} . \tag{7}$$

We denote by $\overline{H_1(\mathfrak{n})}$ the image of $H_1(\mathfrak{n})$ in $GL(2, A/\mathfrak{n})/(Z(\mathbb{F}_q))$. The scheme $\overline{M}_1^2(\mathfrak{n}) = \overline{H_1(\mathfrak{n})} \backslash \overline{M}^2(\mathfrak{n})$ is smooth and proper over $A[\mathfrak{n}^{-1}]$. The fibers of the morphism $\overline{M}_1^2(\mathfrak{n}) \to \operatorname{Spec}(A[\mathfrak{n}^{-1}])$ are absolutely irreducible curves. We will explain this last claim.

Let $M^2(\mathfrak{n})_{(0)}$ be the generic fiber of the morphism

$$M^2(\mathfrak{n}) \to \operatorname{Spec}(A[\mathfrak{n}^{-1}]).$$

Then,

$$M^2(\mathfrak{n})_{(0)} \times_K \mathbf{C} \simeq (\Gamma(\mathfrak{n}) \backslash \Omega) \times \Xi ,$$

where $\Xi = GL(A^2) \backslash GL(\mathfrak{n}^{-1} A^2 / A^2)$ (cf. [20], Lecture 8, Proposition 2.1 and Theorem 2.2). There is a natural bijection between Ξ and $GL(2, A) \backslash GL(2, A/\mathfrak{n})$. The map $\det : GL(2, A) \backslash GL(2, A/\mathfrak{n}) \to (A/\mathfrak{n})^* / \mathbb{F}_q^*$ is a bijection. The group $GL(2, A/\mathfrak{n})$ acts on $(\Gamma(\mathfrak{n}) \backslash \Omega) \times ((A/\mathfrak{n})^* / \mathbb{F}_q^*)$ as follows. Each matrix $\gamma \in GL(2, A/\mathfrak{n})$ can be written as a product of two matrices μ and α in $GL(2, A/\mathfrak{n})$, $\gamma = \mu\,\alpha$, such that $\det \mu \in \mathbb{F}_q^*$ and $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ with $d \in (A/\mathfrak{n})^*$. For each $\xi \in (A/\mathfrak{n})^*$, we consider a matrix $\sigma \in GL(2, A)$ such that its image $\overline{\sigma}$ in $GL(2, A/\mathfrak{n})$ equals $\begin{pmatrix} 1 & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mu^{\mathrm{t}} \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$. Now, if $([z], [\xi]) \in (\Gamma(\mathfrak{n}) \backslash \Omega) \times ((A/\mathfrak{n})^* / \mathbb{F}_q^*)$, then

$$\gamma\ ([z], [\xi]) = ([\sigma(z)], [d\,\xi]) .$$

The map $\det : H_1(\mathfrak{n}) \to (A/\mathfrak{n})^*$ is surjective. Hence, if $M_1^2(\mathfrak{n}) = \overline{H_1(\mathfrak{n})} \backslash M^2(\mathfrak{n})$ and $M_1^2(\mathfrak{n})_{(0)}$ is the generic fiber of the morphism $M_1^2(\mathfrak{n}) \to \operatorname{Spec}(A[\mathfrak{n}^{-1}])$, then

$$M_1^2(\mathfrak{n})_{(0)} \times_K \mathbf{C} \simeq \overline{H_1(\mathfrak{n})} \backslash \left(M^2(\mathfrak{n})_{(0)} \times_K \mathbf{C} \right) \simeq \Gamma_1'(\mathfrak{n}) \backslash \Omega ,$$

where $\Gamma_1'(\mathfrak{n}) = \{\gamma^{\mathrm{t}} \in GL(2, A) : \gamma \in \Gamma_1(\mathfrak{n})\}$. Thus, the fiber $M_1^2(\mathfrak{n})_{(0)}$ is connected. Hence, the generic fiber $\overline{M}_1^2(\mathfrak{n})_{(0)}$ of the morphism $\overline{M}_1^2(\mathfrak{n}) \to \mathrm{Spec}(A[\mathfrak{n}^{-1}])$ is connected; this implies that all the fibers of this morphism are connected (cf. Corollary 11.5 of [14], p. 280). Being smooth, they are irreducible.

Remark 1.4. The automorphism of Ω given by $z \mapsto 1/z$ induces an isomorphism $\Gamma_1'(\mathfrak{n})\backslash\Omega \simeq \Gamma_1(\mathfrak{n})\backslash\Omega$. Hence, $M_1^2(\mathfrak{n})_{(0)} \times_K \mathbf{C} \simeq \Gamma_1(\mathfrak{n})\backslash\Omega$ and $\overline{M}_1^2(\mathfrak{n})_{(0)} \times_K \mathbf{C} \simeq X_1(\mathfrak{n})$.

2. Minimal bases for plane curves

Let $P(x, y) \in \mathbb{F}_q[x, y]$ be an absolutely irreducible polynomial; $P(x, y)$ defines a projective plane curve that we denote by C. The places $\mathbf{q}$ of C over the algebraic closure of $\mathbb{F}_q$ can be represented by irreducible parametrizations $(x_{\mathbf{q}}(t), y_{\mathbf{q}}(t))$ of $P(x, y)$, where $x_{\mathbf{q}}(t), y_{\mathbf{q}}(t) \in \overline{\mathbb{F}}_q((t))$. The valuation associated to $\mathbf{q}$ is denoted by $v_{\mathbf{q}}$.

In the sequel, we will assume that $P(x, y)$ is *monic* and *separable* in y. Let now R be the integral closure of $\overline{\mathbb{F}}_q[x]$ in $\overline{\mathbb{F}}_q(C)$, where $\overline{\mathbb{F}}_q(C)$ is the function field of C. The ring R is a free $\overline{\mathbb{F}}_q[x]$-module of rank $\deg_y(P)$. An integral basis for R is a basis as free $\overline{\mathbb{F}}_q[x]$-module.

Let λ be the projection

$$\begin{tikzcd} C \arrow[r, "\lambda"] & \mathbb{P}^1 \\ (x, y) \arrow[r, mapsto] & x \end{tikzcd} .$$

The symbols $e_{\mathbf{q}}$ and $m_{\mathbf{q}}$ will denote the ramification index and the differential exponent of λ at $\mathbf{q}$, respectively. If $\mathbf{q}$ is a place of C such that $x_{\mathbf{q}}(t) \in \overline{\mathbb{F}}_q[[t]]$, then $e_{\mathbf{q}} = \mathrm{ord}(x_{\mathbf{q}}(t) - x_{\mathbf{q}}(0))$ and $m_{\mathbf{q}} = \mathrm{ord}(x_{\mathbf{q}}'(t))$. If $\mathbf{q}$ is a place of C such that $x_{\mathbf{q}}(t) \notin \overline{\mathbb{F}}_q[[t]]$, then $e_{\mathbf{q}} = \mathrm{ord}(1/x_{\mathbf{q}}(t))$ and $m_{\mathbf{q}} = \mathrm{ord}((1/x_{\mathbf{q}}(t))')$. We will denote by $\mathcal{A}$ the set of places $\mathbf{q}$ of C such that $x_{\mathbf{q}}(t) \in \overline{\mathbb{F}}_q[[t]]$; for each $\alpha \in \overline{\mathbb{F}}_q$, we will denote by $\mathcal{A}_\alpha$ the set of places $\mathbf{q}$ of $\mathcal{A}$ such that $x_{\mathbf{q}}(0) = \alpha$. Finally, $\mathcal{A}_\infty$ will denote the set of places $\mathbf{q}$ such that $x_{\mathbf{q}}(t) \notin \overline{\mathbb{F}}_q[[t]]$.

Next, we recall some facts concerning integral bases. For characteristic zero, these results are in [3]; we will sketch the proofs (they are also valid for characteristic p).

Let $n := \deg_y(P)$. Let $\{h_1, \ldots, h_n\}$ be a basis for $\overline{\mathbb{F}}_q(C)$ over $\overline{\mathbb{F}}_q(x)$. One can associate to $\mathcal{B} = \{h_1, \ldots, h_n\}$ the rational function

$$\mathcal{D}(h_1, \ldots, h_n) = \det\left(\mathrm{Tr}_{\overline{\mathbb{F}}_q(C)/\overline{\mathbb{F}}_q(x)}(h_i h_j)\right),$$

which is called the *discriminant* of $\mathcal{B}$. A classical result says that, if $\{h_1, \dots, h_n\}$ is an integral basis for R over $\overline{\mathbb{F}}_q[x]$, then

$$\mathcal{D}(h_1, \dots, h_n) = \zeta \prod_{\alpha \in \overline{\mathbb{F}}_q} (x - \alpha)^{\sum_{\mathfrak{q} \in \mathcal{A}_\alpha} m_\mathfrak{q}} , \tag{8}$$

for some $\zeta \in \overline{\mathbb{F}}_q^*$.

Let now $h \in R$. We define

$$\nu(h) = \min_{\mathfrak{q} \in \mathcal{A}_\infty} \left[\frac{v_\mathfrak{q}(h)}{e_\mathfrak{q}} \right].$$

Let $\{h_1, \dots, h_n\}$ be an integral basis for R. Since $v_\mathfrak{q}(x^{\nu(h_i)} h_i) \geq 0$ for each $\mathfrak{q} \in \mathcal{A}_\infty$, we have that

$$\operatorname{ord}_\infty \mathcal{D}\left(x^{\nu(h_1)} h_1, \dots, x^{\nu(h_n)} h_n\right) \geq \sum_{\mathfrak{q} \in \mathcal{A}_\infty} m_\mathfrak{q},$$

where $\operatorname{ord}_\infty$ denotes the order of the expansion in $1/x$ of an element in $\overline{\mathbb{F}}_q(x)$ (as a formal Laurent series). On the other hand, it follows from equation (8) that

$$\begin{aligned}\operatorname{ord}_\infty \mathcal{D}&\left(x^{\nu(h_1)} h_1, \dots, x^{\nu(h_n)} h_n\right) \\ &= -2(\nu(h_1) + \dots + \nu(h_n)) - \sum_{\mathfrak{q} \in \mathcal{A}} m_\mathfrak{q}.\end{aligned}$$

Hence, if $\{h_1, \dots, h_n\}$ is an integral basis for R, then

$$\nu(h_1) + \dots + \nu(h_n) \leq -1/2 \sum_{\mathfrak{q} \in C} m_\mathfrak{q}.$$

Definition 2.1. *An integral basis $\{h_1, \dots, h_n\}$ for R is a minimal basis if*

$$\nu(h_1) + \dots + \nu(h_n) = -1/2 \sum_{\mathfrak{q} \in C} m_\mathfrak{q}.$$

It is always possible to construct a minimal basis for R as it follows. We will use Coates' algorithm; a detailed description of this algorithm can be found in [3].

Let $\{h_1, \dots, h_n\}$ be an integral basis. We assume that the h_i's have been permuted in such a way that $\nu(h_1) \geq \nu(h_2) \geq \dots \geq \nu(h_n)$. For each h_i, $i = 1, \dots, n$, and for each $\mathfrak{q} \in \mathcal{A}_\infty$, we consider the expansion

$$x_\mathfrak{q}(t)^{\nu(h_i)}\, h_i(x_\mathfrak{q}(t), y_\mathfrak{q}(t)) = \sum_{s \geq 0} b_{(i,\mathfrak{q},s)}\, t^s .$$

Let $\mathcal{A}_\infty = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$. We now consider the $n \times n$ matrix

$$B = \begin{pmatrix} b_{(1,\mathfrak{q}_1,0)} & \cdots & b_{(1,\mathfrak{q}_1,e_{\mathfrak{q}_1}-1)} & \cdots & b_{(1,\mathfrak{q}_r,0)} & \cdots & b_{(1,\mathfrak{q}_r,e_{\mathfrak{q}_r}-1)} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{(n,\mathfrak{q}_1,0)} & \cdots & b_{(n,\mathfrak{q}_1,e_{\mathfrak{q}_1}-1)} & \cdots & b_{(n,\mathfrak{q}_r,0)} & \cdots & b_{(n,\mathfrak{q}_r,e_{\mathfrak{q}_r}-1)} \end{pmatrix}.$$

If $\det B \neq 0$, then $\{h_1, \ldots, h_n\}$ is a minimal basis; this follows from the properties of the discriminant defined above. If $\det B = 0$, then there exist $\beta_1, \ldots, \beta_n \in \overline{\mathbb{F}}_q$ which satisfy the following: if $i_0 = \max\{i : \beta_i \neq 0\}$, then

$$\nu\left(\beta_1 x^{\nu(h_1)-\nu(h_{i_0})} h_1 + \ldots + \beta_{i_0} h_{i_0}\right) \geq \nu(h_{i_0}) + 1.$$

We can replace the basis $\{h_1, \ldots, h_n\}$ by the basis $\{\tilde{h}_1, \ldots, \tilde{h}_n\}$, where $\tilde{h}_i = h_i$ if $i \neq i_0$, and $\tilde{h}_{i_0} = \beta_1 x^{\nu(h_1)-\nu(h_{i_0})} h_1 + \ldots + \beta_{i_0} h_{i_0}$. Then,

$$\nu(\tilde{h}_1) + \ldots + \nu(\tilde{h}_n) \geq \nu(h_1) + \ldots + \nu(h_n) + 1.$$

If $\{\tilde{h}_1, \ldots, \tilde{h}_n\}$ is a minimal basis, we stop. Otherwise, we repeat the previous argument. We find a minimal basis after a finite number of steps.

3. The plane model $C_1(\mathfrak{n})$

Let $\mathfrak{p} \in \operatorname{Spec}(A[\mathfrak{n}^{-1}])$. Let $\overline{M}_1^2(\mathfrak{n})_\mathfrak{p}$ be the fiber corresponding to $\mathfrak{p}$ of the morphism $\overline{M}_1^2(\mathfrak{n}) \to \operatorname{Spec}(A[\mathfrak{n}^{-1}])$. Let $s_1 e_u^{q-1}$ and $s_2 e_u^{q^2-1}$ be the functions on $\overline{M}^2(\mathfrak{n})_\mathfrak{p}$ considered in Remark 1.3.

Proposition 3.1. *The function field of $\overline{M}_1^2(\mathfrak{n})_\mathfrak{p}$ is*

$$k(\mathfrak{p})\left(s_1 e_{(0,1/f)}^{q-1}, s_2 e_{(0,1/f)}^{q^2-1}\right),$$

where $k(\mathfrak{p})$ is the residue field of $\mathfrak{p}$.

Proof. First, we recall that $\overline{H_1(\mathfrak{n})}$ denotes the image of $H_1(\mathfrak{n})$ (cf. equation (7)) in $GL(2, A/\mathfrak{n})/Z(\mathbb{F}_q)$.

Since $s_1 e_{(0,1/f)}^{q-1}$ and $s_2 e_{(0,1/f)}^{q^2-1}$ are invariant under the fiberwise action of $H_1(\mathfrak{n})$, the field $k(\mathfrak{p})(s_1 e_{(0,1/f)}^{q-1}, s_2 e_{(0,1/f)}^{q^2-1})$ is contained in the function field of $\overline{M}_1^2(\mathfrak{n})_\mathfrak{p}$.

Conversely, let $\gamma \in GL(2, A/\mathfrak{n})/Z(\mathbb{F}_q)$ be such that $h^\gamma = h$ for any function h on $\overline{M}_1^2(\mathfrak{n})_\mathfrak{p}$. Then,

$$(s_1 e_{(0,1/f)}^{q-1})^\gamma = s_1 e_{(0,1/f)}^{q-1}.$$

This implies that $\gamma \in \overline{H_1(\mathfrak{n})}$. Hence, the function field of $\overline{M}_1^2(\mathfrak{n})_\mathfrak{p}$ is contained in $k(\mathfrak{p})(s_1 e_{(0,1/f)}^{q-1}, s_2 e_{(0,1/f)}^{q^2-1})$. □

Let us now describe the cusps of $X_1(\mathfrak{n})$ above the cusp of $X_0(\mathfrak{n})$ represented by 0 (cf. Proposition 1.1). It is possible to present explicit local parameters at these cusps.

Let G be the set of representatives of $\Gamma_0(\mathfrak{n})/\Gamma_1(\mathfrak{n})Z(\mathbb{F}_q)$ defined in the proof of Proposition 1.1. We have that

$$U = \left\{ b/d : \gamma_a = \begin{pmatrix} a & b \\ f & d \end{pmatrix} \in G \right\} \tag{9}$$

is a set of representatives of the cusps of $X_1(\mathfrak{n})$ above the cusp 0 of $X_0(\mathfrak{n})$. Furthermore, $\{d : \gamma_a \in G\}$ is a set of representatives of $(A/\mathfrak{n})^*/\mathbb{F}_q^*$. Let $w = b/d \in U$ and let $\mu \in \Gamma(1)$ be such that $\mu(w) = \infty$. Then, $t(\mu(z)/f)$ is a local parameter at the cusp w (cf. [9], pp. 294-296 or [4], pp. 45-46). We choose

$$\mu = \begin{pmatrix} f & -a \\ d & -b \end{pmatrix}.$$

Proposition 3.2. *Let $w = b/d$ be a representative of a cusp of $X_1(\mathfrak{n})$ above the cusp* 0 *of $X_0(\mathfrak{n})$ and let $t_\mathfrak{n} = t(\mu(z)/f)$ be as above. The coefficients of the expansion in $t_\mathfrak{n}$ of the functions $g(z)e_{(0,1/f)}(z)^{q-1}$ and $\Delta(z)e_{(0,1/f)}(z)^{q^2-1}$ belong to A.*

Proof. Let $\omega = \mu(z)$ and let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. Then,

$$(e_u(z))^\gamma = (cz+d)^{-1} e_{u\gamma}(z).$$

By substituting $z = \mu^{-1}(\omega)$ in equation (5), we obtain the formula

$$\begin{aligned} &\overline{\pi}(-d\omega + f)e_{(0,1/f)}(z) \\ &\quad = \rho(-d)(\mathbf{t}(\omega/f)^{-1}) \prod_{c \in A-\{0\}} \left(1 - \frac{\rho(-d)(\mathbf{t}(\omega/f)^{-1})}{\rho(c)(\mathbf{t}(\omega)^{-1})}\right). \end{aligned} \tag{10}$$

The $(q-1)$-th power of the right side in equation (10) is a power series in $t(\omega/f) = t_\mathfrak{n}$.

On the other hand, $g(\gamma(z)) = (cz+d)^{q-1}g(z)$ and $\Delta(\gamma(z)) = (cz+d)^{q^2-1}\Delta(z)$. Hence, the coefficients of the expansion in $t(\omega)$ of the functions $(\overline{\pi})^{1-q}(-d\omega + f)^{1-q}g(z)$ and $(\overline{\pi})^{1-q^2}(-d\omega + f)^{1-q^2}\Delta(z)$ belong to A. □

The fiber $\overline{M}_1^2(\mathfrak{n})_\mathfrak{p}$ has a simple plane model. To introduce this model, we first define the polynomials $P_i(x, y) \in k(\mathfrak{p})[x, y]$ recursively:

$$P_0 = 1, \;\; P_{i+1} = \mathfrak{i}(T)P_i + xP_i^q + yP_i^{q^2}, \tag{11}$$

where $\mathfrak{i} : A \to k(\mathfrak{p})$ is the natural morphism. Now, let

$$P(x, y) = P_m + a_{m-1}P_{m-1} + \ldots + a_0 \;,$$

where the $a_i \in \mathbb{F}_q$ are the coefficients of the polynomial f (cf. equation (4)). The polynomial $P(x, y)$ defines a plane curve that we denote by $C_1(\mathfrak{n})$.

Proposition 3.3. *The functions* $s_1 e_{(0,1/f)}^{q-1}$ *and* $s_2 e_{(0,1/f)}^{q^2-1}$ *on* $M_1^2(\mathfrak{n})_{\mathfrak{p}}$ *satisfy the equation*

$$P(s_1 e_{(0,1/f)}^{q-1}, s_2 e_{(0,1/f)}^{q^2-1}) = 0.$$

Proof. This follows from the equation $\phi_{\mathfrak{n}}(e_{(0,1/f)}) = 0$, where $\phi_{\mathfrak{n}}$ is the Drinfeld module on $M^2(\mathfrak{n})_{\mathfrak{p}}$ defined by $\phi_{\mathfrak{n}}(T) = \mathfrak{i}(T)\tau^0 + s_1\tau + s_2\tau^2$. □

From now to the end of Proposition 3.4, we will assume that $\mathfrak{p} = (0)$; we recall that the polynomial $P(x, y)$ and the curve $C_1(\mathfrak{n})$ have been defined for each $\mathfrak{p} \in \operatorname{Spec}(A[\mathfrak{n}^{-1}])$.

The functions $g(z)e_{(0,1/f)}(z)^{q-1}$ and $\Delta(z)e_{(0,1/f)}(z)^{q^2-1}$ on the curve $X_1(\mathfrak{n})$ satisfy the equation

$$P(g(z)e_{(0,1/f)}(z)^{q-1}, \Delta(z)e_{(0,1/f)}(z)^{q^2-1}) = 0.$$

This implies that the curve $C_1(\mathfrak{n})$ has as a component a plane model of $X_1(\mathfrak{n})$. Indeed, $C_1(\mathfrak{n})$ is a plane model of $X_1(\mathfrak{n})/K$:

Proposition 3.4. *The curve* $C_1(\mathfrak{n})$ *is absolutely irreducible.*

Proof. Let $w = b/d \in U$ (see equation (9)). Assume that $\deg d = l < m$. By equation (10),

$$\overline{\pi}(-d\omega + f)e_{(0,1/f)}(z) = \zeta\,\mathbf{t}(\omega/f)^{-q^l} + \dots,$$

where $\zeta \in \mathbb{F}_q^*$. Since $(\overline{\pi})^{1-q}g(z) = 1 + \dots$, we have that

$$g(z)e_{(0,1/f)}(z)^{q-1} = t(\omega/f)^{-q^l} + \dots \tag{12}$$

Hence, the place of $C_1(\mathfrak{n})$ corresponding to w is on the line at infinity. To simplify matters, we identify w with the corresponding place of $C_1(\mathfrak{n})$.

Let $Q \in \mathbf{C}[x, y]$ be an irreducible polynomial such that

$$Q(g(z)e_{(0,1/f)}(z)^{q-1}, \Delta(z)e_{(0,1/f)}(z)^{q^2-1}) = 0.$$

The polynomial Q defines a projective plane curve Z which is a component of $C_1(\mathfrak{n})$ and a plane model of $X_1(\mathfrak{n})$.

Let us now consider the projection

$$\begin{tikzcd} C_1(\mathfrak{n}) \arrow[r, "\lambda"] & \mathbb{P}^1 \\ (x, y) \arrow[r, mapsto] & x \end{tikzcd}.$$

From equation (12), we get that the ramification index e_w of λ at w is q^l. Hence, $\sum_{w\in U} e_w = \frac{q^{2m}-1}{q^2-1} = \deg_y(P)$. Since $\sum_{w\in U} e_w \leq \deg_y(Q)$, we have that $Z = C_1(\mathfrak{n})$. □

Let us now consider the scheme $\overline{M}_1^2(\mathfrak{n})$. We know that the group $GL(2, A/\mathfrak{n})/Z(\mathbb{F}_q)$ acts on $\overline{M}^2(\mathfrak{n})$ and the quotient by this action is $\mathbb{P}^1_{A[\mathfrak{n}^{-1}]}$ (cf. [20], Theorem 5.3, p.163). Hence, there is a natural projection $\overline{M}_1^2(\mathfrak{n}) \to \mathbb{P}^1_{A[\mathfrak{n}^{-1}]}$. By Proposition 3.2, the cusps of $X_1(\mathfrak{n})/K$ above the cusp 0 of $X_0(\mathfrak{n})$ are defined over K; we recall that these cusps are represented by the elements of the set U defined in equation (9). Because of the isomorphism $\overline{M}_1^2(\mathfrak{n})_{(0)} \simeq X_1(\mathfrak{n})/K$, these cusps correspond to closed subschemes of $\overline{M}_1^2(\mathfrak{n})$ isomorphic to $\mathrm{Spec}(A[\mathfrak{n}^{-1}])$; these subschemes lie above the infinite section of $\mathbb{P}^1_{A[\mathfrak{n}^{-1}]}$. Hence, for each fiber $\overline{M}_1^2(\mathfrak{n})_{\mathfrak{p}}$, the elements of the set U correspond to $\frac{q^m-1}{q-1}$ $k(\mathfrak{p})$-rational points on $\overline{M}_1^2(\mathfrak{n})_{\mathfrak{p}}$. For each $w \in U$, we will denote by $w_{\mathfrak{p}}$ the corresponding point on $\overline{M}_1^2(\mathfrak{n})_{\mathfrak{p}}$.

Remark 3.5. Let us denote by $\sum b_i t_{\mathfrak{n}}^i$ and $\sum c_i t_{\mathfrak{n}}^i$ the expansions at a cusp $w \in U$ (determined by the choice of the matrix μ, see Proposition 3.2) of $g(z)e_{(0,1/f)}(z)^{q-1}$ and $\Delta(z)e_{(0,1/f)}(z)^{q^2-1}$, respectively. For each $\mathfrak{p} \in \mathrm{Spec}(A[\mathfrak{n}^{-1}])$, let $\mathfrak{i} : A \to k(\mathfrak{p})$ be the natural morphism. The formal Laurent series $\sum \mathfrak{i}(b_i)t_{\mathfrak{n},\mathfrak{p}}^i$ and $\sum \mathfrak{i}(c_i)t_{\mathfrak{n},\mathfrak{p}}^i$ are the expansions in a local parameter $t_{\mathfrak{n},\mathfrak{p}}$ at $w_{\mathfrak{p}}$ of the functions $s_1 e_{(0,1/f)}^{q-1}$ and $s_2 e_{(0,1/f)}^{q^2-1}$, respectively.

4. Valuations at the places of $C_1(\mathfrak{n})$ at infinity

From now on, we assume that $\mathfrak{p} = (T)$; this hypothesis is needed in the proof of Lemma 4.4. Nevertheless, Lemmas 4.1 and 4.3, and Corollary 4.2 are valid for any $\mathfrak{p} \in \mathrm{Spec}(A[\mathfrak{n}^{-1}])$.

Let us denote by $U_{\mathfrak{p}}$ the set of places of $C_1(\mathfrak{n})$ which correspond to the cusps of $X_1(\mathfrak{n})$ above the cusp 0 of $X_0(\mathfrak{n})$. The places of $U_{\mathfrak{p}}$ are on the line at infinity of $C_1(\mathfrak{n})$. The ramification of the projection

$$\begin{array}{rcl} C_1(\mathfrak{n}) & \xrightarrow{\lambda} & \mathbb{P}^1 \\ (x, y) & \longmapsto & x \end{array}$$

at these places is determined in the following Lemma.

Lemma 4.1. *The ramification index of λ is q^i at exactly q^i places of $U_{\mathfrak{p}}$, for $i = 0, 1, \ldots, m-1$.*

Proof. This follows from the proof of Proposition 3.4 and Remark 3.5. □

Corollary 4.2. *The curve $C_1(\mathfrak{n})$ is absolutely irreducible.*

Since $C_1(\mathfrak{n})$ is the curve which corresponds to the model $k(\mathfrak{p})(s_1 e_{(0,1/f)}^{q-1}, s_2 e_{(0,1/f)}^{q^2-1})$ of the function field $k(\mathfrak{p})(\overline{M}_1^2(\mathfrak{n})_{\mathfrak{p}})$, in the sequel we will put $x = s_1 e_{(0,1/f)}^{q-1}$ and $y = s_2 e_{(0,1/f)}^{q^2-1}$.

Lemma 4.3. *Let $\mathfrak{q} \in U_{\mathfrak{p}}$. Let $v_{\mathfrak{q}}$ be the valuation associated to $\mathfrak{q}$. If $v_{\mathfrak{q}}(x) = -q^l$, then $v_{\mathfrak{q}}(y) = q^m - q^l(q+1)$.*

Proof. We have that

$$j(z) = \frac{g(z)^{q+1}}{\Delta(z)} = \frac{(g(z)e_{(0,1/f)}(z)^{q-1})^{q+1}}{\Delta(z)e_{(0,1/f)}(z)^{q^2-1}}.$$

By equation (3), $j(z) = -t(z)^{-1} + \dots$ Hence, $v_{\mathfrak{q}}(x^{q+1}/y) = -q^m$. □

Lemma 4.4. *Let $P_i(x, y)$ be the polynomials defined in equation (11). Let $\mathfrak{q}$ and $v_{\mathfrak{q}}$ be as in* Lemma 4.3. *We have that:*

(a) if $v_{\mathfrak{q}}(x) = -q^l, l \leq m-2$, then $v_{\mathfrak{q}}(P_i) \geq -(q^l + q^{l+1} + \dots + q^{m-2})$, for $i = 1, 2, \dots, m-1$;

(b) if $v_{\mathfrak{q}}(x) = -q^{m-1}$, then $v_{\mathfrak{q}}(P_i) \geq 0$, for $i = 1, 2, \dots, m-1$.

Proof. To simplify matters, the local parameter $t_{\mathfrak{n},\mathfrak{p}}$ at $w_{\mathfrak{p}}$ in Remark 3.5 will be denoted by t, and the point $w_{\mathfrak{p}}$ will be identified with the corresponding place $\mathfrak{q} \in U_{\mathfrak{p}}$. The coefficients of the formal Laurent series in t that we will consider in this proof will be denoted by the symbol $*$; these coefficients belong to $\mathbb{F}_q$.

The first terms of the expansion of x in t depend only on the factor $\rho(-d)(\mathfrak{t}(\omega/f)^{-1})$ of $\overline{\pi}(-d\omega + f)e_{(0,1/f)}(z)$ in equation (10). If $v_{\mathfrak{q}}(x) = -q^l$, then

$$x = t^{-q^l} + *t^{-q^l+q^{l-1}} + \dots + *t^{-q^l+q^{l-1}+\dots+q+1} + \dots$$

Assume that $l \leq m-2$. Let $j = x^{q+1}/y$. Then, for $i \leq m-(l+2)$, we have that

$$x^{1+\dots+q^i} \equiv P_{i+1} \bmod (1),$$

i.e., considered as formal Laurent series, $x^{1+\dots+q^i}$ and P_{i+1} coincide modulo an element in $\mathbb{F}_q[[t]]$.

Let now $i > m-(l+1)$. We claim that

$$x^{1+\dots+q^{m-(l+2)}}\left(* + *t^{q^{m-2}} + \dots + *t^{q^{m-2}+\dots+1} + \dots\right) \equiv P_i \bmod (1).$$

We first prove the case $i = m-l$. The expansion of j^{-1} is

$$j^{-1} = -t^{q^m} + *t^{q^m+q^{m-1}} + \dots + *t^{q^m+\dots+q+1} + \dots$$

Hence,

$$x^{q^{m-l}} j^{-1} = -1 + *t^{q^{m-1}} + \dots + *t^{q^{m-1}+\dots+q+1} + \dots$$

Now, since $P_{m-l} = xP^{q}_{m-(l+1)} + yP^{q^2}_{m-(l+1)}$, we have that

$$x^{1+\ldots+q^{m-(l+1)}}\left(*t^{q^{m-1}}+\ldots+*t^{q^{m-1}+\ldots+1}+\ldots\right)\equiv P_{m-l} \bmod (1).$$

Finally,

$$\begin{aligned} & x^{q^{m-(l+1)}}(*t^{q^{m-1}}+\ldots+*t^{q^{m-1}+\ldots+1}+\ldots) \\ & \qquad = *+*t^{q^{m-2}}+\ldots+*t^{q^{m-2}+\ldots+1}+\ldots \end{aligned}$$

For $i > m-l$, the claim is proved by induction, using the same argument.

For the case $l = m-1$, it follows that

$$*+*t^{q^{m-2}}+\ldots+*t^{q^{m-2}+\ldots+q+1}+\ldots = P_i,$$

for $i \geq 1$. □

Let us state the main result. We use here the notations of section 2. Let R be the integral closure of $\overline{\mathbb{F}}_q[x]$ in $\overline{\mathbb{F}}_q(C_1(\mathfrak{n}))$. Since $C_1(\mathfrak{n})$ is smooth in the affine part (cf. [16], Lemma 2, p. 2627), we have that $R = \overline{\mathbb{F}}_q[x, y]$. Hence, the set $\mathcal{B} = \{1, y, \ldots, y^{n-1}\}$, where $n = \deg_y(P) = \frac{q^{2m}-1}{q^2-1}$, is an integral basis for R.

Theorem 4.5. *Let R be the integral closure of $\overline{\mathbb{F}}_q[x]$ in $\overline{\mathbb{F}}_q(C_1(\mathfrak{n}))$. There exists an integral basis $\{h_1, \ldots, h_n\}$ for R, where*

$$h_l = y^{l_0}P_1^{l_1}\cdots P_{m-1}^{l_{m-1}},$$

and the exponents $l_0, l_1, \ldots, l_{m-1}$ satisfy:

(a) $\deg_y(h_l) = l-1$, *$l_i < q^2$ for $i \geq 1$ and $l_0 - 1 \leq \frac{l_1+\ldots+l_{m-1}}{q^2-q} \leq l_0$;*

(b) $\nu(h_l) \geq -l_0$.

Proof. Property (b) follows from property (a) and Lemmas 4.3 and 4.4: let $\mathfrak{q} \in U_{\mathfrak{p}}$ be such that $v_{\mathfrak{q}}(x) = -q^s$. If $s = m-1$, then $v_{\mathfrak{q}}(h_l) \geq -l_0q^{m-1}$. If $s < m-1$, then

$$v_{\mathfrak{q}}(h_l) \geq l_0(q^m - q^{s+1} - q^s) - (q^s + \ldots + q^{m-2})(l_1 + \ldots + l_{m-1}).$$

By property (a), $l_1 + \ldots + l_{m-1} \leq (q^2-q)l_0$. Hence, $v_{\mathfrak{q}}(h_l) \geq -l_0q^s$.

Let us now obtain for fixed l, $0 < l < n$, exponents $l_0, l_1, \ldots, l_{m-1}$ which satisfy property (a). Let $\delta_i := \deg_y(P_i)$; note that $\delta_{i+1} = q^2\delta_i + 1$, for $i = 1, 2, \ldots, m-1$. We consider $l_{m-1}, \epsilon_{m-1} \in \mathbb{N}$ such that

$$l = l_{m-1}\delta_{m-1} + \epsilon_{m-1},$$

with $\frac{l_{m-1}}{q^2-q} \leq \epsilon_{m-1} \leq \frac{l_{m-1}}{q^2-q} + \delta_{m-1}$. If $\epsilon_{m-1} - 1 \leq \frac{l_{m-1}}{q^2-q}$, then the exponents $l_0 = \epsilon_{m-1}, 0, \dots, 0, l_{m-1}$ satisfy property (a). If $\frac{l_{m-1}}{q^2-q} < \epsilon_{m-1} - 1$, then we consider l_{m-2} and ϵ_{m-2} such that

$$\epsilon_{m-1} = l_{m-2}\delta_{m-2} + \epsilon_{m-2},$$

with $\frac{l_{m-1}+l_{m-2}}{q^2-q} \leq \epsilon_{m-2} \leq \frac{l_{m-1}+l_{m-2}}{q^2-q} + \delta_{m-2}$. If $\epsilon_{m-2} - 1 \leq \frac{l_{m-1}+l_{m-2}}{q^2-q}$, then the exponents $l_0 = \epsilon_{m-2}, 0, \dots, 0, l_{m-2}, l_{m-1}$ satisfy property (a). Otherwise, using the previous argument, from ϵ_{m-2} and δ_{m-3}, we get l_{m-3} and ϵ_{m-3}. This process finishes after a finite number of steps (at most m). □

Example 4.6. Let $q = 3$ and $m = 3$. The numbers $\sum_l \nu(h_l)$ corresponding to the basis $\mathcal{B} = \{1, y, \dots, y^{n-1}\}$, the basis of Theorem 4.5 and a minimal basis are

$$-4095, \ -164 \quad \text{and} \quad -117,$$

respectively.

In general, the numbers $\sum_l \nu(h_l)$ corresponding to the basis $\mathcal{B}$ and a minimal basis are

$$-\frac{n(n-1)}{2} \quad \text{and} \quad -\frac{q^2(q^m-1)(q^{m-1}-1)}{(q^2-1)(q-1)},$$

respectively. For the basis of Theorem 4.5, we have the inequality

$$\sum_l \nu(h_l) \geq -(1 + 1/q)mn.$$

Acknowledgements. This work is part of my Ph. D. Thesis; I would like to express my gratitude to my advisor Ignacio Luengo for his guidance and support during the last years. I wish to thank also Ernst-Ulrich Gekeler for helpful conversations and valuable suggestions on Drinfeld modules. I would like to thank also DGICYT (projects PB94-291 and PB97-0284-C02-C01) for financial support.

References

[1] Deligne, P., Husemöller, D.: Survey of Drinfeld Modules. Contemp. Math. **67**, 25–91 (1987)

[2] Drinfeld, V.: Elliptic Modules, Math. USSR-Sb. **23**, 561–592 (1976)

[3] Duval, D.: Diverses questions relatives au calcul formel avec des nombres algébriques. Thèse, Univ. de Grenoble, 1987

[4] Gekeler, E.-U.: *Drinfeld Modular Curves*. Lecture Notes in Math. Vol. **1231**, Berlin: Springer, 1986

[5] Gekeler, E.-U.: Über Drinfeld'sche Modulkurven vom Hecke-Typ. Compositio Math. **57**, 219–236 (1986)

[6] Gekeler, E.-U.: On the coefficients of Drinfeld modular forms. Invent. Math. **93**, 667–700 (1988)

[7] Gekeler, E.-U.: Modulare Einheiten für Funktionenkörper. J. Reine Angew. Math. **348**, 94–115 (1984)

[8] Gekeler, E.-U.: Moduli for Drinfeld Modules. In: *The Arithmetic of Function Fields*. (D. Goss, D. Hayes and M. Rosen Eds.), Berlin–New York: de Gruyter, 1992, pp. 153–170

[9] Gerritzen, L., van der Put, M.: *Schottky Groups and Mumford Curves*. Lecture Notes in Math. Vol. **817**, Berlin: Springer, 1980

[10] Goss, D.: The Algebraist's Upper Half-Plane. Bull. Amer. Math. Soc. **2**, 391–415 (1980)

[11] Goss, D.: π-adic Eisenstein Series for Functions Fields. Compositio Math. **41**, 3–38 (1980)

[12] Goss, D.: Modular forms for $\mathbb{F}_r[T]$. J. Reine Angew. Math. **317**, 16–39 (1980)

[13] Goss, D.: *Basic structures of function field arithmetic*. Berlin–Heidelberg–New York: Springer, 1996

[14] Hartshorne, R.: *Algebraic Geometry*. Graduate Texts in Math. Vol. **52**, New York: Springer, 1977

[15] López, B.: Plane Models of Drinfeld Modular Curves. Tesis, Univ. Complutense de Madrid, 1996

[16] Manin, Y., Vladut, S.: Linear Codes and Modular Curves. J. Soviet Math. **30**, 2611–2643 (1985)

[17] Matzat, B.-H.: Introduction to Drinfeld Modules. In: *Drinfeld Modules, Modular Schemes and Applications*, (E.-U. Gekeler, M. van der Put, M. Reversat and J. van Geel Eds.), Singapore: World Scientific, 1997, pp. 3–16

[18] Mestre, J.: Corps euclidiens, unités exceptionelles et courbes elliptiques. J. Number Theory **13**, 123–137 (1981)

[19] van der Put, M.: The structure of Ω and its quotients $\Gamma\backslash\Omega$. In: *Drinfeld Modules, Modular Schemes and Applications*, (E.-U. Gekeler, M. van der Put, M. Reversat and J. Van Geel Eds.), Singapore: World Scientific, 1997, pp. 103/112

[20] van der Put, M., Top, J.: Analytic compactification and modular forms (*Lecture 8*); Algebraic compactification and modular interpretation (*Lecture 9*). In: *Drinfeld Modules, Modular Schemes and Applications*, (E.-U. Gekeler, M. van der Put, M. Reversat and J. Van Geel Eds.), Singapore: World Scientific, 1997, pp. 113–166

[21] Saïdi, M.: Moduli schemes of Drinfeld modules. In: *Drinfeld Modules, Modular Schemes and Applications*, (E.-U. Gekeler, M. van der Put, M. Reversat and J. Van Geel Eds.), Singapore: World Scientific, 1997, pp. 17–31

[22] Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten Publ. and Princeton Univ. Press, 1971