Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

Subseries: Mathematisches Institut der Universität und
Max-Planck-Institut für Mathematik, Bonn – vol. 8

Adviser: F. Hirzebruch

1231

Ernst-Ulrich Gekeler

Drinfeld Modular Curves

Springer-Verlag

Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

Subseries: Mathematisches Institut der Universität und
Max-Planck-Institut für Mathematik, Bonn – vol. 8

Adviser: F. Hirzebruch

1231

Ernst-Ulrich Gekeler

Drinfeld Modular Curves

Springer-Verlag

Introduction

The analogy of the arithmetic of number fields with that of "function fields" (i.e. function fields in one variable over a finite field of constants) has been known for a long time. This analogy starts with elementary things (structure of rings of integers, ramification theory, product formula...), but reaches into such deep fields like for example

- (abelian and non-abelian) class field theory;
- Iwasawa theory;
- special values of L-functions (conjectures of Birch and Swinnerton-Dyer and of Stark, relations with K-theory);
- diophantine geometry (conjecture of Taniyama-Weil).

Many problems in number theory have parallels for function fields; conversely, it is often possible to transfer techniques and geometric considerations from the theory of function fields to the case of number fields.

Within the classical theory of modular forms on the complex upper half-plane and the various generalizations of that theory, one can distinguish between two different points of view:

a) Langlands' philosophy. Here one looks for general reciprocity laws that relate l-adic Galois representations with representations of adele-valued reductive groups.

b) The classical function theoretic approach. Here one is interested in properties of single modular forms (Fourier coefficients, algebraicity, integrality, congruence properties, associated L-series...).

Needless to say that it is neither possible nor reasonable to strictly separate these approaches.

While the main tools of a) come from representation theory and functional analysis, in b) methods of function theory and algebraic geometry are dominating.
As is well known, the representation theoretic approach in its adelic formulation may be transferred to function fields (see e.g. [32,34,40]). In the important paper [11], Drinfeld has shown how to transfer b) as well, i.e. how to obtain a modular theory in the function field case.

Let now K be a function field over the finite field $\mathbb{F}_q$ with q elements, "∞" a fixed place of K of degree $\delta \geq 1$, A the ring of functions in K with poles at most at ∞, K_∞ the completion at ∞, $C = \hat{K}_\infty$ the completion of an algebraic closure of K_∞.

The group $\Gamma = GL(2,A)$ operates by fractional linear transformations on the "upper half-plane" $\Omega = C - K_\infty$, and the set of similarity classes of two-dimensional free discrete A-lattices in C is naturally parametrized by $\Gamma\backslash\Omega$. To each such lattice Λ, one associates an entire function $e_\Lambda : C \to C$ which will play simultaneously the part of the classical lattice functions σ, ζ, $\wp$ of Weierstraß. By means of e_Λ, one constructs an algebraic object over C (later on called a Drinfeld module over C of rank two) whose definition makes sense over arbitrary A-schemes. Proceeding this way, one obtains on $\Gamma\backslash\Omega$ (and, more generally, on $\Gamma'\backslash\Omega$ for each congruence subgroup Γ' of Γ) an algebraic structure as a modular scheme which, roughly speaking, has all the properties of a classical modular curve. $\Gamma'\backslash\Omega$ carries different structures. It is

a) a rigid analytic variety of dimension one over C;

b) the set of C-valued points of an affine algebraic curve M_Γ, which is defined over a finite extension of K;

c) "fibred over $\Gamma'\backslash\mathfrak{T}$", where $\mathfrak{T}$ denotes the Bruhat-Tits tree of $PGL(2,K_\infty)$.

In considering c), Drinfeld gives (Thm.2 in [11]) an interpretation of the first l-adic cohomology module of M_Γ, as a space of automorphic forms in the sense of [40]. (One should note that this theory has been generalized by introducing a level structure "at infinity" (see [12]), but this aspect, leading far away from the classical case, will not be pursued further in this work.)
In contrast to the situation over number fields, there exist r-dimensional A-lattices in C for arbitrary natural numbers r (instead of $r = 2$ only). Correspondingly, we have Drinfeld modules of rank r, denoted for short by "r-D-modules".

Let us first consider the case $r = 1$. A 1-D-module has a similar meaning for the arithmetic of K as the multiplicative group scheme G_m for the field $\mathbb{Q}$ of rationals. Drinfeld shows [11, Thm.1]: The modular scheme M^1 for 1-D-modules with level structure is $Spec(B)$,

where B is the ring of integers in the maximal abelian extension of K which is totally split at the place ∞. This represents a simultaneous analogue for both the theorem of Kronecker-Weber and the main theorem of complex multiplication.

For an arbitrary r, a r-D-module behaves, roughly speaking, like an "irreducible abelian variety of dimension $r/2$ over $\mathbb{C}$". For example, the A-module of a-division points (where a is a non-constant element of A) is free of rank r over A/a. By deformation arguments, Drinfeld obtains the nonsingularity of the modular scheme for the module problem

"r-D-modules + a sufficiently rigid structure of level".

The critical step in Drinfeld's proof of his Thm.2 is to construct a "compactification" $\bar{M}^2$ of the modular scheme M^2 for 2-D-modules. Although this is done by ad-hoc glueing a certain one-dimensional scheme to M^2 (and not by generalizing the module problem as in [8]), the resulting $\bar{M}^2$ still has a weak modular property with respect to degenerate 2-D-modules. One can give a different construction for $\bar{M}^2 \times C$ which has the advantage of being applicable to the higher ranks $r \geq 2$. For this "Satake-type" compactification, as well as for generalizations of the expansions around cusps given in VI, see [73].

Let us now restrict to the case $r = 2$.

Until recently, not very much was known about the geometry and arithmetic of the curves M_Γ, ($\Gamma' \subset \Gamma = GL(2,A)$ a congruence subgroup), with the exception of the case $A = \mathbb{F}_q[T]$, the polynomial ring in one indeterminate T. In this latter case, the modular scheme $M^2(1) \times C$ for 2-D-modules without structure of level has the curve $M_\Gamma = \Gamma\backslash\Omega$ as its only irreducible component. This curve has genus 0, and is identified with C by means of a j-invariant

$$j : \Gamma\backslash\Omega \xrightarrow{\cong} C .$$

One can calculate the genus of the higher modular curves by the Hurwitz formula. Some other properties of higher modular curves in this special case may be found in [20,21].
Let now again A be arbitrary. One reason for the interest in the curves M_Γ, concerns diophantine geometry (by a theorem of Grothendieck and Deligne, the analogue of Taniyama-Weil's conjecture on the parametrization

of elliptic curves is true in this context); another one comes from the relations with the cohomology of Γ' and with vector bundles over the nonsingular model of K [61]. In view of the work of Ribet, Wiles, Kubert-Lang, and Mazur-Wiles, one should also study the groups of divisor classes of degree zero supported by the cusps of such curves. These groups are finite by (VI 5.12).

Of course, the main tools in the investigation of these curves are modular forms, i.e. C-valued functions on Ω with the usual transformation behavior and certain holomorphy conditions. The basic examples of modular forms are the Eisenstein series introduced by D.Goss [27], and certain coefficient functions constructed from 2-D-modules varying with z in Ω (see V.3).
(Note: "Modular forms" are certain C-valued functions, whereas the term "automorphic form" means some characteristic-0-valued mapping, i.e. both have an a priori completely different meaning.)

In this context, we have different "analytic" theories:

a) the theory of the complex zeta function and L-series of K. This is well known and presents no analytic difficulties, these functions being rational in $S = q^{-s}$. Nevertheless, the special values of partial zeta functions at the negative integers $1 - r$ ($r \geq 1$) are of arithmetic interest;

b) the theory of automorphic forms;

c) the C-valued theory of the functions e_Λ, the modular forms, and related functions.

One link between a) and c) is given by Deligne-Tate's theorem on Stark's conjecture in the function field case [66, Ch.V] resp. by (IV 4.10, 4.13) and (VI 3.9, 4.11). It depends on the distribution property of division points of Drinfeld modules.
(After having a Satake type compactification of the higher rank modular schemes at our disposal, we can generalize this relation: In complete analogy with (IV 4.10) and (VI 4.11), the product expansions of modular forms of rank $r \geq 3$ around cuspidal divisors correspond to the values of partial zeta functions at $1 - r$ [73]. It is not clear, where one should look for a corresponding result in the number field case. Is it reasonable to expect analogous properties for Siegel modular forms?)

Further, modular forms may be considered as multi-differentials on modular curves, whereas automorphic forms occur in the l-adic cohomology of such curves, thereby connecting b) and c).

In this work, modular forms of the Drinfeld type are investigated, and consequences for modular curves are derived. Therefore, representation theory plays no role here. Beyond that, I refrained from discussing Drinfeld's Thm.2, though it certainly gave the motivation for introducing the general theory. For better orientation of the reader, I tried, wherever possible, to indicate the analogies with the number field case.

The emphasis is in the analytic theory of modular forms above C :

- description of C-valued points of modular curves;
- behavior of modular forms at cusps: product expansion , properties of the coefficients, zero orders at cusps;
- behavior at elliptic points;
- determination of the C-algebra of modular forms....;
- arithmetic consequences.

The relations with algebraic modular forms in the sense of [27] are carried out only as far as possible without going beyond this framework.

One important prerequisite is Hayes' normalization of Drinfeld modules of rank 1. With its help, we may define the generalized cyclotomic polynomials occuring in the product expansions.
As a result, I am able to compute the genera of the modular curves which were not known before (except in the special case mentioned). In particular, an answer is given to the question for the first Betti number of Γ (or of groups commensurable with Γ) which has been left open in [61].

The state of problem differs from that in the classical case. For the group $SL(2,\mathbb{Z})$, one has the well known fundamental domain which leads to the value 0 for the genus of the modular curve "without level structure", and by means of Hurwitz's formula, it is easy to compute the genera of arbitrary modular curves. For $A = \mathbb{F}_q[T]$, one may follow the same lines, this case being treated in [17]. However, for a general A , the equations defining Drinfeld modules become so complicated that, already in the next simple case (genus of $K = 0$ and $\delta = 2$), it seems hopeless to try to compute the genera in this naive way. Using the Bruhat-

Tits tree, it is possible to construct a fundamental domain for Γ in some very restricted cases [61], but this does not help much. Instead, we use the description of the elliptic points and of the parameters at cusps to get a relation between modular forms for Γ and multi-differentials on $\bar{M}_\Gamma$. This allows the computation of $g(\bar{M}_\Gamma)$, if the divisor of one single modular form is known. Finally, the divisors of certain modular forms are obtained from the above mentioned product expansions.

The organization of the work is as follows:

Since Drinfeld modules do not (as yet) belong to the basic tools of the number theorist, the needed definitions, concepts and properties are collected in Chapter I. It contains no proofs; these may be found in [10,11] and, partially, in [36]. The deepest facts cited are the non-singularity of the modular schemes (1.10), the description (4.1) of M^1 and the compactification of M^2 (4.2).

In Chapter II, one finds properties of lattices often needed throughout the work (§ 1), relations between the coefficients of power series associated with lattices, and the links with lattice sums (§2), as well as additive polynomials related to morphisms of lattices (§ 3). A simple, but very important fact is (2.10): lattices Λ resp. Drinfeld modules are completely determined by the values of finitely many Eisenstein series $E^{(k)}(\Lambda)$.

Still some preparations are done in Chapter III. In the first paragraph, well known facts on the zeta functions of K and A are collected, and partial zeta functions for elements of $\mathrm{Pic}\, A$ are defined and compared with complex valued lattice sums. We obtain a distribution on the set of pairs $(a,\mathfrak{n})$, where a lies in K and $\mathfrak{n}$ is a fractional A-ideal in K. This distribution takes values in the field $\mathbb{C}(S)$ of rational functions $(S = q^{-s})$. Its evaluation at places $s = 1-r$ describes a $\mathbb{C}$-valued distribution which, later on, will turn out to be the distribution constructed from division points of Drinfeld modules of rank r. An explicit presentation of the rational function $Z_{a,\mathfrak{n}}$ by means of generalized Weierstraß gaps is given in § 2. In the third section, certain finite sums occurring later are interpreted as values of $Z_{a,\mathfrak{n}}$ at $S = 1$ resp. q, i.e. as zeta values at $s = 0$ resp. $s = -1$. There is a uniform upper bound for the numbers $Z'_{a,\mathfrak{n}}(1)$ which assures the convergence of our product expansions in VI.

In Chapter IV, we deal with Drinfeld modules of rank 1 over C. This will be necessary for the rank 2 theory, but is also interesting for its

own sake. First, we handle the most simple case $A = \mathbb{F}_q[T]$. Here, all 1-D-modules are isomorphic with the module studied by Carlitz [4,5,6]. Its division points generate the maximal abelian extension of K which is completely split at ∞ . The analogy with the Kronecker-Weber theorem is obvious, so this example will serve as a motivation for what follows. For arbitrary A , the isomorphism classes of 1-D-modules are parametrized by $\operatorname{Pic} A$. For generalizing the above example, we need "canonical" 1-D-modules, i.e. for each isomorphism class a distinguished module. These modules are not given by Drinfeld's theory. If $\delta = 1$, it is easy to see:

> For each element of $\operatorname{Pic} A$, there exists a 1-D-module (uniquely determined up to trivial transformations) with coefficients in the ring of integers of the ring class field H of A and leading coefficients in $\mathbb{F}_q^*$.

Under this assumption, the wanted generalization causes no problems [37]. This is no longer true for $\delta > 1$. In [39], Hayes shows how to proceed in the general case to generate class fields of K by division points of D-modules. First, one has to choose a sign function sgn , i.e. a co-section of the embedding $\mu_w \subset\!\longrightarrow K_\infty^*$, where $w = q^\delta - 1$. Then one considers D-modules ϕ with the following property: The function $A \to C$ which associates to each $a \in A$ the leading coefficient of the additive polynomial ϕ_a agrees up to Galois twist with $\operatorname{sgn}|A$. In each isomorphism class, there exist such ϕ . They are uniquely determined up to twists with w-th roots of unity, and have coefficients in a finite abelian extension $\tilde{H}$ of K which contains H . In § 2, we give, as far as needed, and without proofs, a summary of Hayes' theory of "sgn-normalization".

Now we are able to define the ξ-invariants of rank 1 lattices up to w-th roots of unity. In sections 3 and 4, these invariants are computed. We obtain product formulae (4.10, 4.13) analogous with the classical

$$\pi = 2 \prod_{a \geq 1} (1 - 1/4a^2)^{-1} .$$

Perhaps the most striking consequence is the relation of such formulae with the values of derivatives of partial zeta functions at $s = 0$. Proceeding, one can construct units in abelian extensions of K with absolute values (at the different infinite places) prescribed by Stark's conjectures. This gives in fact a constructive proof of Deligne-Tate's theorem on Stark's conjecture in our situation (see [39]). Another result

is the determination of the Galois twist by which the "leading coefficient function" differs from sgn (4.11). For later computations in the rank 2 case, we have to fix our ξ-invariants. By means of (4.11), we have control on the effect of the choices made, and we are able to describe the isogenies of different D-modules.

In V, we come to the central point. First, Drinfeld's upper half-plane is described in more detail (building mapping, analytic structure). In § 2, we show how the analytic space $\Gamma\backslash\Omega$ is compactified by adjoining a finite number of cusps. In the next section, modular forms are introduced, their behavior at cusps is discussed and some examples are given for the construction of forms by means of 2-D-modules. Elliptic points of the groups GL(Y) are investigated in section 4 (existence, number, structure of stabilizers). This relates modular forms and differentials. The resulting formula (5.5) expresses the genus of a modular curve in terms of the divisor of a modular form. The chapter ends with an appendix not further used in this work. Up to some details, which may be found in [11], a proof of $g(\bar{M}_{\Gamma'}) = b(\Gamma')$ is given. With the results of V and VI, one obtains the first Betti number $b(\Gamma')$ for all arithmetic subgroups $\Gamma' \subset \Gamma$ (not only for those which are p'-torsion free [61]).

Chapter VI is devoted to the computation of expansions of modular forms around cusps. After some preliminaries, in § 3, the expansions of the division functions e_u (some sort of Fricke functions) around the cusp ∞ are determined. A major ingredient is the rank 1 theory developed in IV. The result is (3.9) which presents e_u as an infinite product with positive radius of convergence. The pole order of e_u can be expressed, in view of (III 3.11), by zeta values. The fourth section uses these results for the computation of similar product expansions for the "discriminant functions" $\Delta_{\mathfrak{n}}$ associated with positive divisors $\mathfrak{n}$. For principal divisors $\mathfrak{n} = (f)$, this product takes the particularly simple form (4.12), which is, on the one hand, a translation of

$$\Delta = (2\pi i)^{12} q \prod_{n \geq 1} (1-q^n)^{24} ;$$

on the other hand, it is a two-dimensional analogue of the products for the ξ-invariants in IV. The determination of the root-of-unity factor in (4.12) is somewhat delicate, because some of the preceding calculations yield results only up to $(q-1)$-st roots of unity.

The transfer to other cusps is easy. This is carried out in § 5, where

we also draw some conclusions:

- final determination of the genus for the modular curves associated to maximal arithmetic subgroups;
- existence of a distinguished cusp form of weight $q^{2\delta} - 1$;
- finiteness of the group of cuspidial divisor classes of degree 0.

In VII, the results of VI are transferred to higher modular curves, and rings of modular forms are computed. First, the function field of the modular scheme $M^2(\mathfrak{n})$ is determined, as well as the field of definition of the cusps and of the elliptic points. After the preceding considerations, it suffices to apply some well known arguments (see for example [62]). For being able to compute the dimensions of the spaces of modular forms, it is (up to a small number of exceptions) enough to know the behavior of the Eisenstein series of weight $q-1$ at the elliptic points. In § 3, these series are shown to have simple zeroes at elliptic points. So we are able to give, for the present, dim $M_k(\Gamma)$ for maximal arithmetic groups. Nevertheless, the arithmetic meaning of the modular forms occurring is not at all clear already in the simple examples discussed in § 4. It would be desirable to have a description by generators and relations, where the generating modular forms should have an elementary interpretation by means of Drinfeld modules. In § 5, the genera of modular curves for full congruence subgroups $\Gamma(\mathfrak{n})$ are computed, and a formula is given for the Hecke congruence subgroup $\Gamma_0(\mathfrak{n})$, in the case $\mathfrak{n} = \mathfrak{p}$ is a prime ideal. (If one works patiently enough, it is possible and not too difficult, to write down a generally valid formula. The corresponding Betti number depends only on the decomposition type of the divisor $\mathfrak{n}$ and, of course, the zeta function of K .) Finally, the dimensions of $M_k(\Gamma')$ are given for some congruence subgroups Γ' of $\Gamma = GL(2,A)$. For $k = 1$, we get only a lower bound for the dimension.

The final chapter VIII contains some additional material and remarks on relations with other questions. In § 1, the Hecke operators $T_{\mathfrak{p}}$ are introduced. A priori, $T_{\mathfrak{p}}$ is a correspondence on the set of 2-lattices in C . One obtains

a) a correspondence on the modular scheme $\bar{M}^2(\mathfrak{n})$;

b) an operator on characteristic-zero valued automorphic forms;

c) an operator on modular forms.

The Eisenstein series are easily seen to be eigenvectors for the $T_{\mathfrak{p}}$ ($\mathfrak{p}$ = principal ideal), whilst the effect of Hecke for instance on the discriminant functions Δ_n is totally unknown. In the second section, the connection with the classification of elliptic curves is discussed. Finally, some questions are raised which have or have not a counterpart in the number field case.

For ease of handling, we have included an index and a list of symbols. References inside the text are made in the form

(x.y) number x.y in the present chapter;

(V x.y) number x.y in Chapter V;

[xy] item xy in the Bibliography.

The end of a proof is labelled by □ . The symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the usual number sets.

#(S) is the cardinality of a set S, X - Y the complement of Y in X , $f|Y$ the restriction of the map f to Y .

For a ring R and r in R, R^*, (r), R/r denote the multiplicative group, the principal ideal generated by r , the factor ring respectively. The group G acting on X, $G\backslash X$ resp. G/X is the orbit space, X^G the fixed point set and G_x the stabilizer of $x \in X$. For g,h in G , $h^g = ghg^{-1}$. Further, Gal(L:K) is the Galois group of the field extension L:K, $\bar{K}$ an algebraic closure of K and μ_n the group of n-th roots of unity.

"RS" is the abbreviation for "system of representatives",

"oBdA" means "without loss of generality",

and "N >> 0" says "the number N is sufficiently large".

The present text is a slightly complemented english translation of the authors "Habilitationsschrift" at the Faculty of Sciences, Bonn 1985. He wants to thank the staff of the "Max-Planck-Institut für Mathematik" in Bonn for support. In particular, he is grateful to Miss M.Grau who did an excellent job in preparing the manuscript.

Table of Contents

0. Notations

Throughout the text, q denotes a power of the prime number p, and $\mathbb{F}_q$ is the finite field with q elements. Let further

K be a function field in one variable over the field of constants $\mathbb{F}_q$, of genus g;

∞ a place of K fixed once for all, of degree $\delta \geq 1$;

A the ring of functions f in K with poles at most at ∞;

K_∞ the ∞-adic completion of K, with ring of integers O_∞ and residue field k.

We choose a uniformizing parameter π at ∞, and we determine the degree function deg and the absolute value on K_∞ by

$$\deg \pi = -\delta \ , \quad |x| = q^{\deg x} \ .$$

In particular, $\deg 0 = -\infty$. Divisors on K which are prime to ∞ are written multiplicatively and identified with fractional ideals of A. They are denoted by $\mathfrak{a},\mathfrak{b}...\mathfrak{m},\mathfrak{n}$. Correspondingly, $\mathfrak{p},\mathfrak{q}...$ are places resp. prime ideals of A.

For a divisor $\mathfrak{a}$, let $|\mathfrak{a}| = q^{\deg \mathfrak{a}}$ and $\mathfrak{a}_N = \{a \in \mathfrak{a} \mid \deg a \leq N\}$. We use "$\mathfrak{a} > 1$" or "$\mathfrak{a} \subset A$" to designate positive divisors $\mathfrak{a}$. Further, we need

$\mathbb{A} = \mathbb{A}_f \times K_\infty$ the ring of adeles of K, with finite part $\mathbb{A}_f$; correspondingly, we let

$I = I_f \times K_\infty^*$ the group of ideles of K and

$E = E_f \times E_\infty$ the group of unit ideles.

For $\mathfrak{a} > 1$, let $E(\mathfrak{a}) = E_f(\mathfrak{a}) \times E_\infty = \{\underline{e} \in E \mid \underline{e} \equiv 1 \bmod \mathfrak{a}\}$. Finally,

$\hat{A} = \varprojlim_{\mathfrak{n}>1} A/\mathfrak{n}$ is the ring of integral finite adeles. As occasion demands, we consider K as a subring of A, A_f, or K_∞.

I. Drinfeld Modules

1. Algebraic Theory [10,11,36]

(1.1) Let L be a field of characteristic p and $\mathrm{End}_L(G_a)$ the ring of those endomorphisms of the additive group scheme G_a which are defined over L. Then $\mathrm{End}_L(G_a)$ is a non-commutative polynomial ring over L, generated by the Frobenius endomorphism

$$\tau_p : L \longrightarrow L$$
$$x \longmapsto x^p .$$

We write $\mathrm{End}_L(G_a) = L\{\tau_p\}$, the curly braces indicating the commutation rule $\tau_p x = x^p \tau_p$ for $x \in L$. By $\tau_p \longmapsto X^p$, $\mathrm{End}_L(G_a)$ is isomorphic with the ring of additive polynomials over L, i.e. the ring of polynomials of the form

$$\sum l_i X^{p^i} ,$$

the multiplication being defined by substitution. We do not distinguish between both points of view, and we write "τ_p^i" or "X^{p^i}", depending on the context.

The structure of $\mathrm{End}_L(G_a)$ has first been studied by Ore [53]; for example, $\mathrm{End}_L(G_a)$ is right euclidean, and each left ideal is principal.

(1.2) We now assume that L has a structure $\gamma : A \to L$ as an A-algebra. By definition, the characteristic of L is the prime ideal ∞, if γ is injective, and $\mathrm{Ker}\ \gamma$ otherwise. An injective ring homomorphism

$$\phi : A \longrightarrow \mathrm{End}_L(G_a)$$
$$a \longmapsto \phi_a$$

defines by

$$\|a\| = \text{degree of the additive polynomial corresponding to } \phi_a$$

an absolute value $\| \ \|$ on A, provided there exists an a with $\|a\| > 1$. Under this assumption, the extension of $\| \ \|$ to K is equivalent with $| \ |$. Hence, there exists a real number $r > 0$ such that for all a in K, we have $\|a\| = |a|^r$. In fact, r is even a natural number, and ϕ takes values in $L\{\tau\} \subset \mathrm{End}_L(G_a)$. Here, $\tau = \tau_p^s$ is the element corresponding to X^q, where $q = p^s$. Each element f of $L\{\tau\}$ can be written uniquely in the form $f = \sum l_i \tau^i$ with left coefficients $l_i = l_i(f)$. We put $D(f) = l_o(f)$ = "constant term" of f and $l(f) = l_{\deg f}$ = "leading coefficient" of f, where $\deg f$ is the degree of f in τ.

1.3. Definition. A Drinfeld module over L of rank $r \in \mathbb{N}$ is an injective ring homomorphism

$$\phi : A \longrightarrow \mathrm{End}_L(G_a)$$
$$a \longmapsto \phi_a ,$$

such that for all $a \in A$, we have

(i) $\deg \phi_a = r \cdot \deg a$ ($\deg \phi_a$ = degree of ϕ_a in τ), and

(ii) $D(\phi_a) = \gamma(a)$.

We abbreviate the notation "Drinfeld module" resp. "Drinfeld module of rank r" by "D-module" resp. "r-D-module".

By ϕ, the additive group scheme over L becomes a scheme of A-modules. Let ϕ and Ψ be D-modules over L. A morphism $u : \phi \to \Psi$ is a L-endomorphism u of G_a with the property

$$u \circ \phi_a = \Psi_a \circ u$$

for all a in A. If u is an automorphism of G_a, i.e. a constant different from 0, u is called an isomorphism. Non-trivial morphisms u are already in $L\{\tau\} \subset L\{\tau_p\}$; they may exist only between Drinfeld modules of the same rank and are therefore called isogenies.

1.4. Example. If K is the field $\mathbb{F}_q(T)$ of rational functions and A the ring $\mathbb{F}_q[T]$ of polynomials in an indeterminate T, a r-D-module ϕ is given by

$$\phi_T = \sum_{0 \le i \le r} l_i \tau^i ,$$