The arithmetic of Drinfeld modules

by

Dragos Florin Ghioca

M.S. (University of Pittsburgh) 2000

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA at BERKELEY

Committee in charge:

Professor Bjorn Poonen, Chair
Professor Thomas Scanlon
Professor David A. Forsyth

Spring 2005

The dissertation of Dragos Florin Ghioca is approved:

Chair   Date

Date

Date

University of California at Berkeley

Spring 2005

The arithmetic of Drinfeld modules

Abstract

The arithmetic of Drinfeld modules

by

Dragos Florin Ghioca

Doctor of Philosophy in Mathematics

University of California at Berkeley

Professor Bjorn Poonen, Chair

Over the past century, the following three important questions for an abelian variety A defined over a global field K were intensively studied: finding a (good) lower bound for the canonical height of a non-torsion point, proving a structure theorem for the group of rational points and describing the intersection of a generic subvariety of A with a finitely generated subgroup of A. The first problem is known in literature as the Lehmer inequality for the abelian variety A and is still open for the general case of abelian varieties. The second problem is known as the Mordell-Weil theorem for abelian varieties. Different versions of this theorem were proved by Mordell, Weil, Taniyama, Lang and Néron. In connection with this theorem there is also the interesting question of finding an upper bound for the number of

torsion points of $A(K)$. The third problem is known as the Mordell-Lang theorem for abelian varieties and it was the subject of seminal papers by Faltings and Hrushovski.

All three questions mentioned above can be asked when A is a power of the additive group scheme, only that the answers are either trivial or not of the same type as the ones for a general abelian variety. But if we allow the action of a Drinfeld module on the additive group scheme, all three problems become extremely interesting and they constitute the subject of the present thesis.

Professor Bjorn Poonen
Dissertation Committee Chair

În toţi anii de când lucrez matematică singura constantă din viaţa mea a fost şi este dragostea mamei mele. Niciunul dintre premiile pe care le-am caştigat, niciuna dintre teoremele pe care le-am demonstrat nu s-ar fi realizat fără suportul moral al mamei mele. Astfel, îi mulţumesc mamei pentru tot ce a făcut pentru mine şi îi dedic această teză.

Contents

1 Introduction 1

1.1 Generalities . . . 1
1.2 The Lehmer Conjecture . . . 3
1.3 The Mordell-Weil Theorem . . . 9
1.4 The Mordell-Lang Conjecture . . . 11
1.5 Elliptic curves over the perfect closure of a function field . . . 15

2 Tame modules 16

3 Elliptic curves over the perfect closure of a function field 21

4 Valuations and Heights 27

4.1 Heights associated to Drinfeld modules with respect to good sets of valuations . . . 27
4.2 Examples of good sets of valuations . . . 34

5 A local analysis of heights on Drinfeld modules 38

5.1 A local formulation of the Lehmer inequality for Drinfeld modules . 38
5.2 General valuation theory on Drinfeld modules . . . 41

6 The global Lehmer Inequality for Drinfeld modules 78

7 The Mordell-Weil theorem for Drinfeld modules 90

8 Minimal groups in the theory of separably closed fields associated to Drinfeld modules 100

8.1 General properties of minimal groups in the theory of separably closed fields . . . 100

8.2 The ring of quasi-endomorphisms for minimal groups associated to Drinfeld modules of finite characteristic 111

9 The Mordell-Lang Theorem for Drinfeld modules 130

Bibliography 153

Acknowledgements

First and foremost I would like to thank Thomas Scanlon for being such a wonderful adviser for me over the past two and a half years. I want to thank him for giving me the opportunity to work with him in the beautiful subject of Drinfeld modules. All the results of my thesis are motivated by conjectures he made. Meeting Dr. Scanlon was the single most important moment of my graduate years.

I would also like to thank Thomas Brown for being an excellent Graduate Student Affairs Officer. He helped me in numerous occasions with different administrative problems I had during my graduate years.

Finally, I want to apologize to Bjorn Poonen for wasting his time especially in my first two years as a PhD student and also in the last few months of my PhD program, while he was reading my thesis. Asking him clumsily formulated mathematical questions led only to confusion for both of us.

Chapter 1

Introduction

1.1 Generalities

One of our interests in number theory is concerned with the theory of heights, which provides a framework for discussing the complexity of a number. For example, let x be a rational number. We write x as a fraction $\frac{p}{q}$ of two relatively prime integers with $q \neq 0$. Then the exponential height of x is defined as $\max(|p|, |q|)$. We can define heights for all elements x in finite extensions of $\mathbb{Q}$ and also, we can define heights for rational functions. We may also define canonical heights on abelian varieties and Drinfeld modules. These height functions satisfy the triangle inequality among other properties and they are instrumental in understanding arithmetic properties of abelian varieties and Drinfeld modules.

A natural question is the following. Let K be a finitely generated field of characteristic $p > 0$. Let $P \in K[x]$ be an additive polynomial, i.e. a polynomial such that $P(x+y) = P(x) + P(y)$, for every x and y in K^{alg}. Then $P(x)$ is a sum of monomials of the form $a_n x^{p^n}$, for $n \geq 0$. Let $z \in K^{\mathrm{alg}}$. We consider the sequence

$$z, P(z), P(P(z)), P(P(P(z))) \ldots . \tag{1.1}$$

There are two possibilities:

Case 1. The sequence is eventually periodic.

In this case, we can characterize the elements z for which this happens. For each finite extension L of K, there are finitely many elements $z \in L$, such that the sequence (1.1) is eventually periodic. An interesting question is to give for each integer $d > 0$, an upper bound only in terms of the degree of P, for the number of elements z such that $[K(z) : K] \leq d$ and the corresponding sequence (1.1) is eventually periodic.

Case 2. All the elements of the sequence are distinct.

In this case, the interesting question is to give a notion of how fast does the complexity (i.e. height) of $P(P(\ldots P(z))\ldots)$ grow.

To study the questions raised above we need to work in the context of Drinfeld modules and the heights associated to Drinfeld modules. My thesis addresses, among other problems, also the two questions presented above.

1.2 The Lehmer Conjecture

The classical Lehmer conjecture (see [17], page 476) asserts that there is an absolute constant $C > 0$ so that any algebraic number α that is not a root of unity satisfies the following inequality for its logarithmic height

$$h(\alpha) \geq \frac{C}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

A partial result towards this conjecture is obtained in [9]. The analog of Lehmer conjecture for elliptic curves and abelian varieties has also been much studied (see [5], [15], [20], [29], [1]). The paper [8] formulated a conjecture whose general form is Conjecture 1.2.2, which we refer to as the Lehmer inequality for Drinfeld modules.

Our notation for Drinfeld modules follows the one from [13]: p is a prime number and q is a power of p. We denote by $\mathbb{F}_q$ the finite field with q elements. We let C be a nonsingular projective curve defined over $\mathbb{F}_q$ and we fix a closed point ∞ on C. Then we define A as the ring of functions on C that are regular everywhere except possibly at ∞.

We let K be a field extension of $\mathbb{F}_q$. We fix a morphism $i : A \to K$. We define the operator τ as the power of the usual Frobenius with the property that for every $x \in K^{\text{alg}}$, $\tau(x) = x^q$. Then we let $K\{\tau\}$ be the ring of polynomials in τ with coefficients from K (the addition is the usual one, while the multiplication is the composition of functions).

We fix an algebraic closure of K, denoted K^{alg}. We denote by K^{sep} and K^{per} the separable and perfect closure, respectively, of K in K^{alg}. We denote by $\mathbb{F}_p^{\text{alg}}$ the algebraic closure of $\mathbb{F}_p$ inside K^{alg}.

A Drinfeld module over K is a ring morphism $\phi : A \to K\{\tau\}$ for which the coefficient of τ^0 in ϕ_a is $i(a)$ for every $a \in A$, and there exists $a \in A$ such that $\phi_a \neq i(a)\tau^0$. Following the definition from [13] we call ϕ a Drinfeld module of generic characteristic if $\ker(i) = \{0\}$ and we call ϕ a Drinfeld module of finite characteristic if $\ker(i) \neq \{0\}$. In the latter case, we say that the characteristic of ϕ is $\ker(i)$ (which is a prime ideal of A). In the generic characteristic case we assume i extends to an embedding of $\text{Frac}(A)$ into K.

If $\gamma \in K^{\text{alg}} \setminus \{0\}$, we denote by $\phi^{(\gamma)}$ the Drinfeld module over K^{alg} mapping $a \in A$ to $\gamma^{-1}\phi_a\gamma$. The Drinfeld module $\phi^{(\gamma)}$ is isomorphic to ϕ over $K(\gamma)$ (see [13]).

For each field L containing K, $\phi(L)$ denotes the A-module L with the A-action given by ϕ.

We will need later the following definition.

Definition 1.2.1. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. Let L be a field extension of K and let v be a discrete valuation on L. We say that ϕ has *good* reduction at v if for all $a \in A \setminus \{0\}$, the coefficients of ϕ_a are integral at v and the leading coefficient of ϕ_a is a unit.

If v is not a place of good reduction, then v is a place of *bad* reduction.

Let $\widehat{\mathrm{h}}$ be the global height associated to the Drinfeld module ϕ as in [32] (see also Chapter 4).

Conjecture 1.2.2. Let K be a finitely generated field. For any Drinfeld module $\phi : A \to K\{\tau\}$ there exists a constant $C > 0$ such that any non-torsion point $x \in K^{\mathrm{alg}}$ satisfies $\widehat{\mathrm{h}}(x) \geq \frac{C}{[K(x):K]}$.

Before our work, the only known partial result towards Conjecture 1.2.2 was obtained in [7], which proved the conjecture restricted to the case in which ϕ is the Carlitz module and x is a non-torsion point in K^{sep}.

In this thesis we develop a theory of local heights $\widehat{\mathrm{h}}_v$ for Drinfeld modules over arbitrary fields of characteristic p (see Chapter 4). In all of the theorems that are stated in Chapter 1, for a valuation v, the positive real number $d(v)$ represents the degree of the valuation v (as defined in Chapter 4).

Let M_K be the set of all discrete valuations on the field K. In Chapter 5 we prove the following result (see also Chapter 4 for the definition of *coherent valuations*)..

Theorem 1.2.3. *Let K be a field of characteristic p and let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic. Let $v_0 \in M_K$ be a coherent valuation (on K^{alg}) and $d(v_0)$ be be the degree of v_0. There exists $C > 0$ and $k \geq 1$, both depending only on ϕ, such that if $x \in K^{\mathrm{alg}}$ and $v \in M_{K(x)}$, $v|v_0$ and $\widehat{\mathrm{h}}_v(x) > 0$,* *then*

$$\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{k-1}}$$

where $d(v) = \frac{d(v_0)f(v|v_0)}{[K(x):K]}$ *where* $e(v|v_0)$ *is the ramification index and* $f(v|v_0)$ *is the relative degree between the residue field of* v *and the residue field of* v_0*.*

The proof gives explicit values of C and k (from Theorem 1.2.3) in terms of ϕ. Also, in the case that the place v from Theorem 1.2.3 is not wildly ramified above K, we prove a finer result and we show that this result is the best possible.

We prove in Chapter 5 a similar result as in Theorem 1.2.3 for Drinfeld modules of generic characteristic.

Theorem 1.2.4. *Let* K *be a field of characteristic* p*. Let* $v_0 \in M_K$ *be a coherent valuation (as defined in Chapter* 4*) and let* $d(v_0)$ *be the degree of* v_0*.*

Let ϕ *be a Drinfeld module of generic characteristic. There exist two positive constants* C *and* k *depending only on* ϕ *such that for every* $x \in K^{\mathrm{alg}}$ *and every place* v *of* $K(x)$*, if* $\widehat{\mathrm{h}}_v(x) > 0$ *and* v *does not lie over the place* ∞ *from* $\mathrm{Frac}(A)$*, then*

$$\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{k-1}},$$

where $v_0 \in M_K$ *lies below* v*.*

We show that the hypothesis from Theorem 1.2.4 that v does not lie over the place ∞ of $\mathrm{Frac}(A)$ canot be removed. If v lies over ∞, then $\widehat{\mathrm{h}}_v(x)$ can be positive but arbitrarily small. Also, in case v satisfies the additional hypothesis that is not wildly ramified above K, we prove a finer inequality and show that it is best possible.

In Chapter 6 we prove the first global result towards Conjecture 1.2.2. Before stating our result we need to define a special set of valuations on finitely generated fields.

Let K be a finitely generated field of positive transcendence degree. Let F be the algebraic closure of $\mathbb{F}_p$ in K. Fix a transcendence basis $\{x_1, \ldots, x_n\}$ for K/F.

We first define the set $M_{F(x_1,\ldots,x_n)/F}$ of valuations on $F(x_1, \ldots, x_n)$. Let $\mathbb{P}^n_F$ be the n-dimensional projective space, whose function field is $F(x_1, \ldots, x_n)$. For each irreducible divisor of $\mathbb{P}^n_F$ we construct the corresponding discrete valuation on the function field of $\mathbb{P}^n_F$. The degree of such a valuation is the projective degree of the corresponding subvariety of codimension 1 of $\mathbb{P}^n_F$. The set of all these valuations is $M_{F(x_1,\ldots,x_n)/F}$. Then for every nonzero $x \in F(x_1, \ldots, x_n)$,

$$\sum_{v \in M_{F(x_1,\ldots,x_n)/F}} d(v) \cdot v(x) = 0.$$

We let $M_{K/F}$ be the set of all discrete valuations v on K (normalized so that the range of v is $\mathbb{Z}$) with the property that v lies over a valuation $v_0 \in M_{F(x_1,\ldots,x_n)/F}$.

In general, for every finite extension L of K, if E is the algebraic closure of F in L, we let $M_{L/E}$ be the set of all discrete valuations of L that lie over valuations from $M_{K/F}$. For $w \in M_{L/E}$, if $v \in M_{K/F}$ lies below w, then we define the degree

$d(w)$ of w as $\frac{d(v)f(w|v)}{[L:K]}$.

For each Drinfeld module $\phi : A \to K\{\tau\}$ and for every finite extension L of K as above, we construct the local and global heights associated to ϕ with respect to $M_{L/E}$ (see Chapter 4).

If K is a finite extension of $\mathbb{F}_p$ (i.e. $n = 0$ with the above notation), there are no nontrivial valuations defined on K. Then, the above set of valuations $M_{K/F}$ is the empty set.

Theorem 1.2.5. *Let K be a finitely generated field of characteristic p. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module and assume that there exists a non-constant $t \in A$ such that ϕ_t is monic. Let F be the algebraic closure of $\mathbb{F}_p$ in K. We let $M_{K/F}$ be the coherent good set of valuations on K, constructed as in Chapter 4. Let $\widehat{\mathrm{h}}$ and $\widehat{\mathrm{h}}_v$ be the global and local heights associated to ϕ, constructed with respect to the coherent good set of valuations $M_{K/F}$. Let $x \in K^{\mathrm{alg}}$ and let F_x be the algebraic closure of $\mathbb{F}_p$ in $K(x)$. We construct the good set of valuations $M_{K(x)/F_x}$ which lie above the valuations from $M_{K/F}$. Let S_x be the set of places $v \in M_{K(x)/F_x}$ such that ϕ has bad reduction at v.*

If x is not a torsion point for ϕ, then there exists $v \in M_{K(x)/F_x}$ such that

$$\widehat{\mathrm{h}}_v(x) > q^{-r\left(2+(r^2+r)|S_x|\right)} d(v)$$

where $d(v)$ is as always the degree of the valuation v.

Because every Drinfeld module is isomorphic over K^{alg} to a Drinfeld module that satisfies the hypothesis of Theorem 1.2.5, we are able to derive an uniform bound for the torsion submodule of a Drinfeld module ϕ, depending only on A and on the rank of ϕ.

Theorem 1.2.6. *Let K be a finitely generated field and let $\phi : A \to K\{\tau\}$ be a Drinfeld module. Let t be a non-constant element of A and assume ϕ_t is monic. Let L be a finite extension of K and let E be the algebraic closure of $\mathbb{F}_p$ in L.*

a) If $\phi_t \in E\{\tau\}$, then $\phi_{\text{tor}}(L) = E$.

b) If $\phi_t \notin E\{\tau\}$, let S be the nonempty set of places of bad reduction for ϕ from $M_{L/E}$. Let $b(t) \in \mathbb{F}_q[t]$ be the least common multiple of all the polynomials of degree at most $(r^2 + r)|S|$. Then for all $x \in \phi_{\text{tor}}(L)$, $\phi_{b(t)}(x) = 0$.

The bound on the torsion submodule given in Theorem 1.2.6, b) is sharp in the case of the Carlitz module, as will be shown after the proof of Theorem 1.2.6.

1.3 The Mordell-Weil Theorem

We use Theorems 1.2.5 and 1.2.6 in Chapter 7 to prove certain Mordell-Weil structure theorems for Drinfeld modules over infinitely generated fields.

Definition 1.3.1. The field of definition of a Drinfeld module $\phi : A \to K\{\tau\}$ is defined to be the smallest subfield of K containing all the coefficients of ϕ_a, for every $a \in A$.

Definition 1.3.2. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. The modular transcendence degree of ϕ is the minimum transcendence degree over $\mathbb{F}_p$ of the field of definition for $\phi^{(\gamma)}$, where the minimum is taken over all $\gamma \in K^{\mathrm{alg}} \setminus \{0\}$.

If there exists a non-constant $t \in A$ such that $\phi_t = \sum_{i=0}^{r} a_i \tau^i$ is monic, then the modular transcendence of ϕ equals $\mathrm{trdeg}_{\mathbb{F}_p} \mathbb{F}_p(a_0, \ldots, a_{r-1})$. This result is proved in Chapter 4, where we also introduce the following definition.

Definition 1.3.3. Let K_0 be any subfield of K. Then the relative modular transcendence degree of ϕ over K_0 is the minimum transcendence degree over K_0 of the compositum field of K_0 and the field of definition of $\phi^{(\gamma)}$, the minimum being taken over all $\gamma \in K^{\mathrm{alg}} \setminus \{0\}$.

Also, if $\phi_t = \sum_{i=0}^{r} a_i \tau^i$ is monic, for some non-constant $t \in A$, the concept of relative modular transcendence degree can be defined as

$$\mathrm{trdeg}_{K_0} K_0(a_{r_0}, \ldots, a_{r-1})$$

(see Lemma 7.0.43).

With the above definition, in Chapter 7 we prove the following two theorems.

Theorem 1.3.4. *Let F be a countable field of characteristic p and let K be a finitely generated field over F. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of positive* *relative modular transcendence degree over F. Then $\phi(K)$ is a direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$.*

Theorem 1.3.5. *Let F be a countable, algebraically closed field of characteristic p and let K be a finitely generated field of positive transcendence degree over F. If $\phi : A \to F\{\tau\}$ is a Drinfeld module, then $\phi(K)$ is a direct sum of $\phi(F)$ and a free submodule of rank $\aleph_0$.*

1.4 The Mordell-Lang Conjecture

Faltings proved the Mordell-Lang Conjecture in the following form (see [11]).

Theorem 1.4.1 (Faltings). *Let G be a abelian variety defined over the field of complex numbers $\mathbb{C}$. Let $X \subset G$ be a closed subvariety and $\Gamma \subset G(\mathbb{C})$ a finitely generated subgroup of the group of $\mathbb{C}$-points on G. Then $X(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ.*

If we try to formulate the Mordell-Lang Conjecture in the context of algebraic subvarieties contained in a power of the additive group scheme $\mathbb{G}_a$, the conclusion is either false (in the characteristic 0 case, as shown by the curve $y = x^2$ which has an infinite intersection with the finitely generated subgroup $\mathbb{Z} \times \mathbb{Z}$, without being itself an additive algebraic group) or trivially true (in the characteristic $p > 0$ case, because every finitely generated subgroup of a power of $\mathbb{G}_a$ is finite). The paper

[6] formulated a version of the Mordell-Lang Conjecture in the context of Drinfeld modules. Even though the formulation from [6] is for Drinfeld modules of generic characteristic, we can extend the question to Drinfeld modules of finite characteristic. Thus, our Statement 1.4.3 will cover both cases. Before stating (1.4.3) we need a definition.

Definition 1.4.2. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. For $g \geq 0$ we consider ϕ acting diagonally on $\mathbb{G}_a^g$. An algebraic ϕ-submodule of $\mathbb{G}_a^g$ is a connected algebraic subgroup of $\mathbb{G}_a^g$ which is stable under the action of ϕ.

Let K be a finitely generated field of characteristic p. For the next statement fix a Drinfeld module $\phi : A \to K\{\tau\}$.

Statement 1.4.3 (Mordell-Lang statement for ϕ). Let $g \geq 0$. Let Γ be a finitely generated ϕ-submodule of $\mathbb{G}_a^g(K^{\text{alg}})$. If X is an algebraic subvariety of $\mathbb{G}_a^g$, then there are finitely many algebraic ϕ-submodules $B_1, \ldots, B_s$ and there are finitely many elements $\gamma_1, \ldots, \gamma_s$ of $\mathbb{G}_a^g(K^{\text{alg}})$ such that $X(K^{\text{alg}}) \cap \Gamma = \bigcup_{1 \leq i \leq s}(\gamma_i + B_i(K^{\text{alg}}) \cap \Gamma)$.

Before our work, the only result towards Statement 1.4.3 was the following (see [23]).

Theorem 1.4.4 (Scanlon). *Let K be a finitely generated field of characteristic p. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic and modular tran-*

scendence degree at least 1*. Let* Γ *be a finitely generated* ϕ*-submodule of* $\mathbb{G}_a^g(K^{\mathrm{alg}})$ *and* X *be an algebraic* K^{alg}*-subvariety of* $\mathbb{G}_a^g$*. Then* $X(K^{\mathrm{alg}}) \cap \Gamma$ *is a finite union of translates of subgroups of* Γ*.*

Definition 1.4.5. Let K be a field of characteristic p. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic. We define $\phi^\sharp(K^{\mathrm{sep}}) = \bigcap_{a \in A\setminus\{0\}} \phi_a(K^{\mathrm{sep}})$.

For more details about the concepts used in this section, we refer the reader to Chapter 8. From now on in this section, K is a finitely generated field.

We fix an $\aleph_1$-saturated elementary extension L of K^{sep} in the theory of separably closed fields of finite Ersov invariant. We define

$$\phi^\sharp = \phi^\sharp(L) = \bigcap_{a \in A\setminus\{0\}} \phi_a(L).$$

The group $\phi^\sharp$ was studied by logicians in the context of the model theory of separably closed fields (see [23]). In Chapter 8 we prove the following result about the ring of quasi-endomorphisms of $\phi^\sharp$, denoted $\mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$.

Theorem 1.4.6. *Let* ϕ *be a Drinfeld module of finite characteristic. Assume there exists an inseparable polynomial* $f \in \mathrm{Aut}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$*, i.e.* $f \in \mathrm{Aut}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp) \cap K^{\mathrm{sep}}\{\tau\}\tau$*. Then* $\phi^\sharp \subset \phi_{\mathrm{tor}}$ *and for all* $\psi \in \mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$*, there exists* $n \geq 1$ *such that* $\psi f^n = f^n \psi$ *(the identity being seen in* $\mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$*).*

Using Theorem 1.4.6 we are able to extend the result of Theorem 1.4.4 towards a proof of Statement 1.4.3 for an infinite class of Drinfeld modules of finite characteristic.

Theorem 1.4.7. *If X is an algebraic K^{alg}-subvariety of $\mathbb{G}_a^g$ and $\phi : A \to K\{\tau\}$ is a Drinfeld module of positive modular transcendence degree for which there exists a non-constant $t \in A$ such that $\phi[t^\infty](K^{\text{sep}})$ is finite, then there exists $n \geq 1$ such that for every finitely generated ϕ-submodule Γ of $\mathbb{G}_a^g(K^{\text{alg}})$, $X(K^{\text{alg}}) \cap \Gamma$ is a finite union of translates of $\mathbb{F}_q[t^n]$-submodules of Γ.*

For each $n \geq 2$ let $\phi_n : \mathbb{F}_q[t] \to \mathbb{F}_q(t)\{\tau\}$ be the Drinfeld module given by $(\phi_n)_t = t\tau + \tau^n$. Clearly, $\phi_n[t^\infty](\mathbb{F}_q(t)^{\text{sep}}) = \{0\}$. So, for each $n \geq 2$, ϕ_n satisfies the conditions of Theorem 1.4.7. There are many similar infinite families of Drinfeld modules which satisfy the condition of Theorem 1.4.7. An interesting question that we hope to answer in a future paper is to give a characterisation in terms of only the coefficients of ϕ_t for all the Drinfeld modules ϕ that satisfy the hypothesis of Theorem 1.4.7.

We will also construct a family of Drinfeld modules $\phi : \mathbb{F}_q[t] \to K\{\tau\}$ of finite characteristic (t) (i.e. ϕ_t is inseparable) such that for each ϕ in this family, $\phi[t^\infty](K^{\text{sep}})$ is infinite and for each such ϕ we have an example of a variety X and a ϕ-submodule Γ such that for any $n \geq 1$, $X(K^{\text{alg}}) \cap \Gamma$ is not a finite union of translates of $\mathbb{F}_q[t^n]$-submodules of Γ.

Using specialization arguments we are able to prove in Chapter 9 the following theorem, which can be considered as the generic case of the Mordell-Lang

Conjecture for Drinfeld modules.

Theorem 1.4.8. *Let $\phi : A \to K\{\tau\}$ be a generic characteristic Drinfeld module of relative modular transcendence degree at least* 1 *over* Frac(A)*. Let $g \geq 0$ and X be an algebraic subvariety of $\mathbb{G}_a^g$. Assume that X does not contain a translate of a nontrivial connected algebraic subgroup of $\mathbb{G}_a^g$. Then for every finitely generated ϕ-submodule Γ of $\mathbb{G}_a^g(K^{\mathrm{alg}})$, $X(K^{\mathrm{alg}}) \cap \Gamma$ is finite.*

1.5 Elliptic curves over the perfect closure of a function field

Before studying the Lehmer inequality for Drinfeld modules, we study the Lehmer inequality for elliptic curves. As a consequence of our work, we obtain in Chapter 3 the following result.

Theorem 1.5.1. *Let K be a function field of transcendence degree* 1 *over $\mathbb{F}_p$. Let E be a non-isotrivial elliptic curve defined over K. Then $E(K^{\mathrm{per}})$ is finitely generated.*

Using the result of Theorem 1.5.1, Thomas Scanlon proved the full positive characteristic Mordell-Lang Conjecture for abelian varieties that are isogenous to a product of elliptic curves (see [24]).

Chapter 2

Tame modules

Definition 2.0.2. Let R be an integral domain and let K be its field of fractions. If M is an R-module, then by the *rank* of M, denoted $\mathrm{rk}(M)$, we mean the dimension of the K-vector space $M \otimes_R K$. We call M a *tame* module if every finite rank submodule of M is finitely generated.

Lemma 2.0.3. *Let R be a Dedekind domain and let M be an R-module. Assume there exists a function $h : M \to \mathbb{R}_{\geq 0}$ satisfying the following properties*

(i) (triangle inequality) $h(x \pm y) \leq h(x) + h(y)$, for every $x, y \in M$.

(ii) if $x \in M_{\mathrm{tor}}$, then $h(x) = 0$.

(iii) there exists $c > 0$ such that for each $x \notin M_{\mathrm{tor}}$, $h(x) > c$.

(iv) there exists $a \in R \setminus \{0\}$ such that R/aR is finite and for all $x \in M$, $h(ax) \geq 4h(x)$.

If M_{tor} is finite, then M is a tame R-module.

Proof. By the definition of a tame module, it suffices to assume that M is a finite rank R-module and conclude that it is finitely generated.

Let $a \in R$ as in (iv) of Lemma 2.0.3. By Lemma 3 of [22], M/aM is finite (here we use the assumption that M_{tor} is finite). The following result is the key to the proof of Lemma 2.0.3.

Sublemma 2.0.4. For every $D > 0$, there exists finitely many $x \in M$ such that $h(x) \leq D$.

Proof of Sublemma 2.0.4. If we suppose SubLemma 2.0.4 is not true, then we can define

$$C = \inf\{D \mid \text{ there exists infinitely many } x \in M \text{ such that } h(x) \leq D\}.$$

Properties (ii) and (iii) and the finiteness of M_{tor} yield $C \geq c > 0$. By the definition of C, it must be that there exists an infinite sequence of elements z_n of M such that for every n,

$$h(z_n) < \frac{3C}{2}.$$

Because M/aM is finite, there exists a coset of aM in M containing infinitely many z_n from the above sequence.

But if $k_1 \neq k_2$ and z_{k_1} and z_{k_2} are in the same coset of aM in M, then let

$y \in M$ be such that $ay = z_{k_1} - z_{k_2}$. Using properties (iv) and (i), we get

$$h(y) \leq \frac{h(z_{k_1} - z_{k_2})}{4} \leq \frac{h(z_{k_1}) + h(z_{k_2})}{4} < \frac{3C}{4}.$$

We can do this for any two elements of the sequence that lie in the same coset of aM in M. Because there are infinitely many of them lying in the same coset, we can construct infinitely many elements $z \in M$ such that $h(z) < \frac{3C}{4}$, contradicting the minimality of C. □

From this point on, our proof of Lemma 2.0.3 follows the classical descent argument in the Mordell-Weil theorem (see [25]).

Take coset representatives $y_1, \ldots, y_k$ for aM in M. Define then

$$B = \max_{i \in \{1,\ldots,k\}} h(y_i).$$

Consider the set $Z = \{x \in M \mid h(x) \leq B\}$, which is finite according to Sub-Lemma 2.0.4. Let N be the finitely generated R-submodule of M which is spanned by Z.

We claim that $M = N$. If we suppose this is not the case, then by Sub-Lemma 2.0.4 we can pick $y \in M - N$ which minimizes $h(y)$. Because N contains all the coset representatives of aM in M, we can find $i \in \{1, \ldots, k\}$ such that $y - y_i \in aM$. Let $x \in M$ be such that $y - y_i = ax$. Then $x \notin N$ because otherwise it would follow that $y \in N$ (we already know $y_i \in N$). By our choice of y and by properties (iv) and (i), we have

$$h(y) \leq h(x) \leq \frac{h(y - y_i)}{4} \leq \frac{h(y) + h(y_i)}{4} \leq \frac{h(y) + B}{4}.$$

This means that $h(y) \leq \frac{B}{3} < B$. This contradicts the fact that $y \notin N$ because N contains all the elements $z \in M$ such that $h(z) \leq B$. This contradiction shows that indeed $M = N$ and so, M is finitely generated. □

Corollary 2.0.5. *Let R be a Dedekind domain and let M be a tame R-module.*

(a) If $\mathrm{rk}(M) = \aleph_0$*, then M is a direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$.*

(b) If $\mathrm{rk}(M)$ *is finite and R is a principal ideal domain, then M is a direct sum of a finite torsion submodule and a free submodule of finite rank.*

Proof. Part (a) of Corollary 2.0.5 is proved in Proposition 10 of [22].

If $\mathrm{rk}(M)$ is finite and because M is tame, we conclude that M is finitely generated. Because R is a principal ideal domain we get the result of part (b) of Corollary 2.0.5. □

The following lemma will be used in the proof of Theorem 7.0.44.

Lemma 2.0.6. *Let R be a Dedekind domain. Let $M_1 \subset M_2 \subset M_3$ be R-modules. If M_1 and M_3 have rank $\aleph_0$ and M_3 is tame then M_2 is the direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$.*

Proof of Lemma 2.0.6. The rank of M_2 is at least the rank of M_1 and at most the rank of M_3. Thus, M_2 has rank $\aleph_0$.

Let N be a finite rank submodule of M_2. Then N is also a finite rank submodule of M_3. Because M_3 is tame, N is finitely generated. Thus, because N was an arbitrarily finite rank submodule of M_2, we conclude that M_2 is tame. Corollary 2.0.5 finishes the proof. $\square$

Chapter 3

Elliptic curves over the perfect closure of a function field

The setting for this Chapter is the following: K is a finitely generated field of transcendence degree 1 over $\mathbb{F}_p$ where p is a prime as always. We fix an algebraic closure K^{alg} of K. We denote by $\mathbb{F}_p^{\text{alg}}$ the algebraic closure of $\mathbb{F}_p$ inside K^{alg}.

Let E be a non-isotrivial elliptic curve (i.e. $j(E) \notin \mathbb{F}_p^{\text{alg}}$) defined over K. Let K^{per} be the perfect closure of K inside K^{alg}. We will prove in Theorem 3.0.8 that $E(K^{\text{per}})$ is finitely generated.

For every finite extension L of K we denote by M_L the set of discrete valuations v on L, normalized so that the value group of v is $\mathbb{Z}$. For each $v \in M_L$ we denote by f_v the degree of the residue field of v over $\mathbb{F}_p$. If $P \in E(L)$ and $m \in \mathbb{Z}$, mP

represents the point on the elliptic curve obtained using the group law on E. We define a notion of height for the point $P \in E(L)$ with respect to the field K (see Chapter $VIII$ of [27] and Chapter III of [28])

$$h_K(P) = \frac{-1}{[L:K]} \sum_{v \in M_L} f_v \min\{0, v(x(P))\}. \tag{3.1}$$

Then we define the canonical height of P with respect to K as

$$\widehat{\mathrm{h}}_{E/K}(P) = \frac{1}{2} \lim_{n \to \infty} \frac{h_K(2^n P)}{4^n}. \tag{3.2}$$

We also denote by $\Delta_{E/K}$ the divisor which is the minimal discriminant of E with respect to the field K (see Chapter $VIII$ of [27]). By $\deg(\Delta_{E/K})$ we denote the degree of the divisor $\Delta_{E/K}$ (computed with respect to $\mathbb{F}_p$). We denote by g_K the genus of the function field K.

Theorem 3.0.7 (Goldfeld-Szpiro). *Let E be an elliptic curve over a function field K of one variable over a field in any characteristic. Let $\widehat{\mathrm{h}}_{E/K}$ denote the canonical height on E and let $\Delta_{E/K}$ be the minimal discriminant of E, both computed with respect to K. Then for every point $P \in E(K)$ which is not a torsion point:*

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13} \deg(\Delta_{E/K}) \text{ if } \deg(\Delta_{E/K}) \geq 24(g_K - 1)\ ,$$

and

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13-23g} \deg(\Delta_{E/K}) \text{ if } \deg(\Delta_{E/K}) < 24(g_K - 1).$$

Theorem 3.0.8. *If E is a non-isotrivial elliptic curve defined over the function field K ($\mathrm{trdeg}_{\mathbb{F}_p} K = 1$), then $E(K^{\mathrm{per}})$ is finitely generated.*

Proof. We first observe that replacing K by a finite extension does not affect the conclusion of the theorem. Thus, at the expense of replacing K by a finite extension, we may assume E is semi-stable over K (the existence of such a finite extension is guaranteed by Proposition 5.4 (a) of [27]).

As before, we let $\widehat{\mathrm{h}}_{E/K}$ and $\Delta_{E/K}$ be the canonical height on E and the minimal discriminant of E, respectively, computed with respect to K.

For every $n \geq 1$, we denote by $E^{(p^n)}$ the elliptic curve $F^n(E)$, where F is the usual Frobenius (seen as morphism of varieties). Thus

$$F^n : E(K^{1/p^n}) \to E^{(p^n)}(K) \tag{3.3}$$

is a bijection. Moreover, for every $P \in E\left(K^{1/p}\right)$,

$$pP = (VF)(P) \in V\left(E^{(p)}(K)\right) \subset E(K) \tag{3.4}$$

where V is the Verschiebung. Similarly, we get that

$$p^n E\left(K^{1/p^n}\right) \subset E(K) \text{ for every } n \geq 1. \tag{3.5}$$

Thus $E(K^{\mathrm{per}})$ lies in the p-division hull of the $\mathbb{Z}$-module $E(K)$. Because $E(K)$ is finitely generated (by the Mordell-Weil theorem), we conclude that $E(K^{\mathrm{per}})$, as a $\mathbb{Z}$-module, has finite rank.

We will show next that the height function $\widehat{\mathrm{h}}_{E/K}$ and $p \in \mathbb{Z}$ satisfy the properties (*i*)-(*iv*) of Lemma 2.0.3. Properties (*i*) and (*ii*) are well-known for $\widehat{\mathrm{h}}_{E/K}$ and we also have the formula (see Chapter $VIII$ of [27])

$$\widehat{\mathrm{h}}_{E/K}(pP) = p^2\, \widehat{\mathrm{h}}_{E/K}(P) \geq 4\, \widehat{\mathrm{h}}(P) \text{ for every } P \in E(K^{\mathrm{alg}}),$$

which proves that property (*iv*) of Lemma 2.0.3 holds.

Let P be a non-torsion point of $E(K^{\mathrm{per}})$. Then $P \in E(K^{1/p^n})$ for some $n \geq 0$. Because K^{1/p^n} is isomorphic to K, they have the same genus, which we call it g. We denote by $\widehat{\mathrm{h}}_{E/K^{1/p^n}}$ and $\Delta_{E/K^{1/p^n}}$ the canonical height on E and the minimal discriminant of E, respectively, computed with respect to K^{1/p^n}. Using Theorem 3.0.7, we conclude

$$\widehat{\mathrm{h}}_{E/K^{1/p^n}}(P) \geq 10^{-13-23g} \deg(\Delta_{E/K^{1/p^n}}). \tag{3.6}$$

We have $\widehat{\mathrm{h}}_{E/K^{1/p^n}}(P) = [K^{1/p^n} : K]\, \widehat{\mathrm{h}}_{E/K}(P) = p^n\, \widehat{\mathrm{h}}_{E/K}(P)$. Similarly, using the proof of Proposition 5.4 (*b*) of [27],

$$\deg(\Delta_{E/K^{1/p^n}}) = p^n \deg(\Delta_{E/K}).$$

We conclude that for every $P \in E(K^{\mathrm{per}})$,

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13-23g} \deg(\Delta_{E/K}). \tag{3.7}$$

Because E is non-isotrivial, $\Delta_{E/K} \neq 0$ and so, $\deg(\Delta_{E/K}) \geq 1$. We conclude

$$\widehat{\mathrm{h}}_{E/K}(P) \geq 10^{-13-23g}. \tag{3.8}$$

Inequality (3.8) shows that property (iii) of Lemma 2.0.3 holds for $\widehat{\mathrm{h}}_{E/K}$. Thus properties (i)-(iv) of Lemma 2.0.3 hold for $\widehat{\mathrm{h}}_{E/K}$ and $p \in \mathbb{Z}$.

We show that $E_{\mathrm{tor}}(K^{\mathrm{per}})$ is finite. Equation (3.5) shows that the prime-to-p-torsion of $E(K^{\mathrm{per}})$ equals the prime-to-p-torsion of $E(K)$; thus the prime-to-p-torsion of $E(K^{\mathrm{per}})$ is finite. If there exists infinite p-power torsion in $E\left(K^{\mathrm{per}}\right)$, equation (3.3) yields that we have arbitrarily large p-power torsion in the family of elliptic curves $E^{(p^n)}$ over K. But this contradicts standard results on uniform boundedness for the torsion of elliptic curves over function fields, as established in [18] (actually, [18] proves a uniform boundedness of the entire torsion of elliptic curves over a fixed function field; thus including the prime-to-p-torsion). Hence $E_{\mathrm{tor}}(K^{\mathrm{per}})$ is finite.

Because all the hypothesis of Lemma 2.0.3 hold, we conclude that $E(K^{\mathrm{per}})$ is tame. Because $\mathrm{rk}\left(E(K^{\mathrm{per}})\right)$ is finite we conclude by Corollary 2.0.5 (b) that $E(K^{\mathrm{per}})$ is a direct sum of a finite torsion submodule and a free submodule of finite rank. □

Remark 3.0.9. It is absolutely crucial in Theorem 3.0.8 that E is non-isotrivial. Theorem 3.0.8 fails in the isotrivial case, i.e. there exists no $n \geq 0$ such that $E(K^{\mathrm{per}}) = E(K^{1/p^n})$. Indeed, if E is defined by $y^2 = x^3 + x$ $(p > 2)$, $K = \mathbb{F}_p\left(t, (t^3+t)^{\frac{1}{2}}\right)$ and $P = \left(t, (t^3+t)^{\frac{1}{2}}\right)$, then $F^{-n}P \in E(K^{1/p^n}) \setminus E(K^{1/p^{n-1}})$, for every $n \geq 1$. So, $E(K^{\mathrm{per}})$ is not finitely generated in this case (and we can get a similar example also for the case $p = 2$).

Chapter 4

Valuations and Heights

4.1 Heights associated to Drinfeld modules with respect to good sets of valuations

We continue with the notation from Chapter 1. So, K is a field extension of $\mathbb{F}_q$ and $\phi : A \to K\{\tau\}$ is a Drinfeld module. We define M_K as the set of all discrete valuations of K. We normalize all the discrete valuations $v \in M_K$ so that the range of v is $\mathbb{Z}$. In general, every discrete valuation we work with will have range $\mathbb{Z}$.

Definition 4.1.1. We call a subset $U \subset M_K$ equipped with a function $d : U \to \mathbb{R}_{>0}$ a *good set of valuations* if the following properties are satisfied

(i) for every nonzero $x \in K$, there are finitely many $v \in U$ such that $v(x) \neq 0$.

(ii) for every nonzero $x \in K$,

$$\sum_{v \in U} d(v) \cdot v(x) = 0.$$

The positive real number $d(v)$ will be called the *degree* of the valuation v. When we say that the positive real number $d(v)$ is associated to the valuation v, we understand that the degree of v is $d(v)$.

When U is a good set of valuations, we will refer to property (ii) as the sum formula for U.

Definition 4.1.2. Let U be a good set of valuations on K. The set $\{0\} \cup \{x \in K \mid v(x) = 0 \text{ for all } v \in U\}$ is the set of *constants* for U. We denote this set by $C(U)$.

Lemma 4.1.3. *Let U be a good set of valuations on K. If $x \in K$ is integral at all places $v \in U$, then $x \in C(U)$.*

Proof. Let $x \in K \setminus \{0\}$. By the sum formula for U, if $v(x) \geq 0$ for all $v \in U$, then actually $v(x) = 0$ for all $v \in U$ (a sum of non-negative numbers is 0 if and only if all the numbers are 0). □

Lemma 4.1.4. *Let U be a good set of valuations on a field K. The set $C(U)$ is a subfield of K.*

Proof. By its definition, $C(U)$ is closed under multiplication and division. Because of Lemma 4.1.3, $C(U)$ is closed also under addition. □

Definition 4.1.5. Let $v \in M_K$ of degree $d(v)$. We say that the valuation v is coherent (on K^{alg}) if for every finite extension L of K,

$$\sum_{\substack{w \in M_L \\ w|v}} e(w|v) f(w|v) = [L : K], \tag{4.1}$$

where $e(w|v)$ is the ramification index and $f(w|v)$ is the relative degree between the residue field of w and the residue field of v.

Condition (4.1) says that v is *defectless* in L. In this case, we also let the degree of any $w \in M_L$, $w|v$ be

$$d(w) = \frac{f(w|v)d(v)}{[L : K]}. \tag{4.2}$$

It is immediate to see that condition (4.2) of Definition 4.1.5 is equivalent to the stronger condition that for every two finite extensions of K, $L_1 \subset L_2$ and for every $v_2 \in M_{L_2}$ that lies over $v_1 \in M_{L_1}$, which in turn lies over v,

$$d(v_2) = \frac{f(v_2|v_1)d(v_1)}{[L_2 : L_1]}. \tag{4.3}$$

We will use several times the following result from [10] (see (18.1), page 136).

Lemma 4.1.6. *Let $L_1 \subset L_2 \subset L_3$ be a tower of finite extensions. Let $v \in M_{L_1}$ and denote by $w_1, \ldots, w_s$ all the places of L_2 that lie over v. Then the following two statements are equivalent:*

1) v is defectless in L_3.

2) v is defectless in L_2 and $w_1, \ldots, w_s$ are defectless in L_3.

Lemma 4.1.6 shows that condition (4.1) of Definition 4.1.5 is equivalent to the following statement: for every two finite extensions of K, $L_1 \subset L_2$ and for every $v_1 \in M_{L_1}$, $v_1|v$

$$\sum_{\substack{w \in M_{L_2} \\ w|v_1}} e(w|v_1) f(w|v_1) = [L_2 : L_1]. \tag{4.4}$$

We say that condition (4.1) of Definition 4.1.5 holds relative to the valuation v for the extension L_2/L_1, if we prove (4.4) for all $v_1 \in M_{L_1}$, $v_1|v$. The following result is an immediate consequence of Definition 4.1.5 and Lemma 4.1.6.

Lemma 4.1.7. *If $v \in M_K$ is a coherent valuation (on K^{alg}), then for every finite extension L of K and for every $w \in M_L$ and $w|v$, w is a coherent valuation (on $K^{\text{alg}} = L^{\text{alg}}$).*

Definition 4.1.8. We let U_K be a good set of valuations on K. We call U_K a *coherent* good set of valuations (on K^{alg}) if the following two conditions are satisfied

(i) for every finite extension L of K, if $U_L \in M_L$ is the set of all valuations lying over valuations from U_K, then U_L is a good set of valuations.

(ii) for every $v \in U_K$, the valuation v is coherent (on K^{alg}).

Remark 4.1.9. Using the argument from page 9 of [25], we conclude that condition (i) from Definition 4.1.8 is automatially satisfied if U_K is a good set of valuations and if condition (ii) of Definition 4.1.8 is satisfied.

An immediate corollary to Lemma 4.1.7 is the following result.

Corollary 4.1.10. *If $U_K \subset M_K$ is a good set of valuations that is coherent (on K^{alg}), then for every finite extension L of K, if U_L is the set of all valuations on L which lie over valuations from U_K, then U_L is a coherent good set of valuations.*

Fix now a field K of characteristic p and let $\phi : A \to K\{\tau\}$ be a Drinfeld module. Let $v \in M_K$ be a coherent valuation (on K^{alg}). Let $d(v)$ be the degree of v as in Definition 4.1.5. For such v, we construct the local height $\widehat{\mathrm{h}}_v$ with respect to the Drinfeld module ϕ. Our construction follows [22]. For $x \in K$ and $v \in U$, we set $\tilde{v}(x) = \min\{0, v(x)\}$. For a non-constant element $a \in A$, we define

$$V_v(x) = \lim_{n\to\infty} \frac{\tilde{v}(\phi_{a^n}(x))}{\deg(\phi_{a^n})}. \tag{4.5}$$

This function is well-defined and satisfies the same properties as in Propositions 1-3 from [22]. Mainly, we will use the following facts:

1) if x and all the coefficients of ϕ_a are integral at v, then $V_v(x) = 0$.

2) for all $b \in A \setminus \{0\}$, $V_v(\phi_b(x)) = \deg(\phi_b) \cdot V_v(x)$. Moreover, we can use any non-constant $a \in A$ for the definition of $V_v(x)$ and we will always get the same function V_v.

3) $V_v(x \pm y) \geq \min\{V_v(x), V_v(y)\}$.

4) if $x \in \phi_{\mathrm{tor}}$, then $V_v(x) = 0$.

We define then

$$\widehat{\mathrm{h}}_v(x) = -d(v)V_v(x). \tag{4.6}$$

If L is a finite extension of K and $w \in M_L$ lies over v then we define similarly the function V_w on L and just as above, we let $\widehat{\mathrm{h}}_w(x) = -d(w)V_w(x)$ for every $x \in L$.

If $U = U_K \subset M_K$ is a coherent good set of valuations, then for each $v \in U$, we denote by $\widehat{\mathrm{h}}_{U,v}$ the local height associated to ϕ with respect to v (the construction of $\widehat{\mathrm{h}}_{U,v}$ is identical with the one from above). Then we define the global height associated to ϕ as

$$\widehat{\mathrm{h}}_U(x) = \sum_{v\in U} \widehat{\mathrm{h}}_{U,v}(x). \tag{4.7}$$

For each x, the above sum is finite due to fact 1) stated above (see also Proposition 6 of [22]).

For each finite extension L of K, we let U_L be the set of all valuations of L that lie over places from U_K. As stated in Corollary 4.1.10, U_L is also a coherent good set of valuations and so, we can define the local heights with respect to $w \in U_L$, associated to ϕ for all elements $x \in L$. Then we define the global height of x as

$$\widehat{\mathrm{h}}_{U_L}(x) = \sum_{w\in U_L} \widehat{\mathrm{h}}_w(x).$$

Claim 4.1.11. Let $L_1 \subset L_2$ be finite extensions of K. Let $v \in U_{L_1}$ and $x \in L_1$.

Then

$$\sum_{\substack{w \in U_{L_2} \\ w|v}} \widehat{\mathrm{h}}_{U_{L_2},w}(x) = \widehat{\mathrm{h}}_{U_{L_1},v}(x).$$

Proof. We have

$$\sum_{\substack{w \in U_{L_2} \\ w|v}} \widehat{\mathrm{h}}_{U_{L_2},w}(x) = -\sum_{\substack{w \in U_{L_2} \\ w|v}} d(w) V_w(x).$$

Because $d(w) = \frac{d(v)f(w|v)}{[L_2:L_1]}$ (see (4.3)) and $V_w(x) = e(w|v)V_v(x)$ we get

$$\sum_{\substack{w \in U_{L_2} \\ w|v}} \widehat{\mathrm{h}}_{U_{L_2},w}(x) = \frac{-d(v)V_v(x)}{[L_2 : L_1]} \sum_{\substack{w \in U_{L_2} \\ w|v}} e(w|v)f(w|v).$$

Because v is defectless and $\widehat{\mathrm{h}}_{U_{L_1},v}(x) = -d(v)V_v(x)$, we are done. □

Claim 4.1.11 shows that our definition of the global height is independent of the field L containing x and so, we can drop the index referring to the field L containing x when we work with the global height associated to a coherent good set of valuations.

The above construction for local and global heights depends on the selected good set of valuations U_K on K. We will always specify first which is the good set of valuations that we consider when we will work with heights associated to a Drinfeld module.

4.2 Examples of good sets of valuations

Let F be a field of characteristic p and let $K = F(x_1, \ldots, x_n)$ be the rational function field of transcendence degree $n \geq 1$ over F. We let F^{alg} be the algebraic closure of F inside K^{alg}. We will construct a coherent good set of valuations on K^{alg}.

First we construct a good set of valuations on K and then we will show that this set is also coherent. According to Remark 4.1.9, we only need to show that each of the valuations on K we construct is coherent.

Let $R = F[x_1, \ldots, x_n]$. For each irreducible polynomial $P \in R$ we let v_P be the valuation on K given by

$$v_P(\frac{Q_1}{Q_2}) = \mathrm{ord}_P(Q_1) - \mathrm{ord}_P(Q_2) \text{ for every nonzero } Q_1, Q_2 \in R,$$

where by $\mathrm{ord}_P(Q)$ we denote the order of the polynomial $Q \in R$ at P.

Also, we construct the valuation v_∞ on K given by

$$v_\infty(\frac{Q_1}{Q_2}) = \deg(Q_2) - \deg(Q_1) \text{ for every nonzero } Q_1, Q_2 \in R,$$

where by $\deg(Q)$ we denote the total degree of the polynomial $Q \in R$.

We let $M_{K/F}$ be the set of all valuations v_P for irreducible polynomials $P \in R$ plus the valuation v_∞. We let the degree of v_P be $d(v_P) = \deg(P)$ for every irreducible polynomial $P \in R$ and we also let $d(v_\infty) = 1$. Then, for every nonzero

$x \in K$, we have the sum formula

$$\sum_{v \in M_{K/F}} d(v) \cdot v(x) = 0.$$

So, $M_{K/F}$ is a good set of valuations on K according to Definition 4.1.1. The field F is the field of constants with respect to $M_{K/F}$.

Remark 4.2.1. As mentioned in the *Introduction*, the valuations constructed above are exactly the valuations associated with the irreducible divisors of the projective space $\mathbb{P}^n_F$. The degrees of the valuations are the projective degrees of the corresponding irreducible divisors.

Let K' be a finite extension of K and let F' be the algebraic closure of F in K'. We let $M_{K'/F'}$ be the set of all valuations on K' that extend the valuations from $M_{K/F}$. We normalize each valuation w from $M_{K'/F'}$ so that the range of w is $\mathbb{Z}$. Also, we define

$$d(w) = \frac{f(w|v)d(v)}{[K' : K]} \tag{4.8}$$

for every $w \in M_{K'/F'}$ and $v \in M_{K/F}$ such that $w|v$. Note that strictly speaking, w is an extension of v as a place and *not* as a valuation function. However, we still call w an extension of v.

Remark 4.2.2. Continuing the observations made in Remark 4.2.1, the valuations defined on K' are the ones associated with irreducible divisors of the normalization of $\mathbb{P}^n_F$ in K'. In general, the discrete valuations associated with the irreducible divisors of a variety which is regular in codimension 1 form a coherent good set of valuations.

In order to show that $M_{K/F}$ is a coherent good set of valuations (on K^{alg}), we need to check that condition (4.1) of Definition 4.1.5 is satisfied. This is proved in Chapter 1, Section 4 of [26] (Hypothesis (F) holds for algebras of finite type over fields and so, it holds for localizations of such algebras). For each $v \in M_{K/F}$ we apply Propositions 10 and 11 of [26] to the local ring of v to show v is coherent.

Now, in general, let F be a field of characteristic p and let K be any finitely generated extension over F, of positive transcendence degree over F. If F is algebraically closed in K, we construct a coherent good set of valuations $M_{K/F} \subset M_K$, as follows. We pick a transcendence basis $\{x_1, \ldots, x_n\}$ for K/F and first construct as before the set of valuations on $F(x_1, \ldots, x_n)$:

$$\{v_\infty\} \cup \{v_P \mid P \text{ irreducible polynomial in } F[x_1, \ldots, x_n]\}.$$

Then, by Corollary 4.1.10, we have a unique way of extending coherently this set of valuations to a good set of valuations on K. The set $M_{K/F}$ depends on our initial choice of the transcendence basis for K/F. Thus, in our notation $M_{K/F}$, we suppose that K/F comes equipped with a choice of a transcendence basis for K/F.

We also note that for every $v \in M_{K/F}$, if $v_0 \in M_{F(x_1,\dots,x_n)/F}$ lies below v, then

$$d(v) = \frac{f(v|v_0)d(v_0)}{[K : F(x_1,\dots,x_n)]} \geq \frac{1}{[K : F(x_1,\dots,x_n)]}. \tag{4.9}$$

In general, if K' is a finite extension of K and $v' \in M_{K'}$ lies above $v \in M_K$, then

$$d(v') = \frac{f(v'|v)d(v)}{[K' : K]} \geq \frac{d(v)}{[K' : K]}. \tag{4.10}$$

For each such good set of valuations $M_{K/F}$ and for any Drinfeld module $\phi : A \to K\{\tau\}$, we construct as before the set of local heights and the global height associated to ϕ. We denote the local heights by $\widehat{\mathrm{h}}_{M_{K/F},v}$ and the global height by $\widehat{\mathrm{h}}_{M_{K/F}}$. If F is a finite field, our construction coincides with the one from [32]. Thus, if F is a finite field, we will drop the subscript $M_{K/F}$ from the notation of the local heights and of the global height. Also, when F is a finite field and $\operatorname{trdeg}_F K = 1$, our construction also coincides with the one from [22].

Chapter 5

A local analysis of heights on Drinfeld modules

The setting for this Chapter is the following: K is a field of characteristic p, $v_0 \in M_K$ is a coherent valuation (on K^{alg}), $d(v_0) > 0$ is the degree of v_0 and $\phi : A \to K\{\tau\}$ is a Drinfeld module.

5.1 A local formulation of the Lehmer inequality for Drinfeld modules

The following statement would imply (1.2.2) and we refer to it as the local case of the Lehmer inequality for Drinfeld modules.

Statement 5.1.1. Let $v_0 \in M_K$ be a coherent valuation (on K^{alg}) and $d(v_0)$ be the degree of v_0. For the Drinfeld module $\phi : A \to K\{\tau\}$ there exists a constant $C > 0$, depending only on ϕ, such that for any $x \in K^{\text{alg}}$ and any place $v|v_0$ of $K(x)$, if $\widehat{\mathrm{h}}_v(x) > 0$, then $\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v_0)}{[K(x):K]}$.

In this Chapter we will prove that (5.1.1) is false but in the case of Drinfeld modules of finite characteristic there is the following result.

Theorem 5.1.2. *Let K be a field of characteristic p and let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic. Let $v_0 \in M_K$ be a coherent valuation (on K^{alg}) and $d(v_0)$ be the degree of v_0. There exist two positive constants C and k depending only on ϕ such that if $x \in K^{\text{alg}}$ and $v|v_0$ is a place of $K(x)$ for which $\widehat{\mathrm{h}}_v(x) > 0$, then $\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v_0)}{d^k}$ (where $d = [K(x) : K]$).*

Before going further on, we want to point out that the field K is part of the data associated to the Drinfeld module ϕ and so, any constant C as in Theorem 5.1.2 might also depend on the field K. Also, at the beginning of the proof of Theorem 5.1.2 we will (possibly) replace K by a finite extension and we will explain how the constant C will be affected by this change. Finally, just to make things clearer, we will point out during key steps while proving Theorem 5.1.2 what is the dependence of C in terms of ϕ.

Theorem 5.1.2 will follow from Theorem 1.2.3, which we restate here.

Theorem 5.1.3. *Let K be a field of characteristic p and let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic. Let $v_0 \in M_K$ be a coherent valuation (on K^{alg}) and $d(v_0)$ be the degree of v_0. There exist $C > 0$ and $k \geq 1$, both depending only on ϕ, such that if $x \in K^{\mathrm{alg}}$ and $v \in M_{K(x)}$, $v|v_0$ and $\widehat{\mathrm{h}}_v(x) > 0$, then $\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{k-1}}$.*

An immediate corollary to Theorem 5.1.3 is the following.

Corollary 5.1.4. *With the notation from Theorem 5.1.3, if L is a finite extension of $K(x)$ and $w \in M_L$ lies above v, then $\widehat{\mathrm{h}}_w(x) \geq \frac{Cd(w)}{e(w|v_0)^{k-1}}$.*

Proof. The proof is immediate once we note that $\widehat{\mathrm{h}}_w(x) = \frac{d(w)e(w|v)}{d(v)}\widehat{\mathrm{h}}_v(x)$ and $e(w|v_0) = e(w|v)e(v|v_0)$ and $e(w|v) \geq 1$. □

Moreover if p does not divide $e(v|v_0)$, then we can give a very easy expression for the exponent k in (5.1.3). If p does not divide $e(v|v_0)$, our value for k is optimal, as shown by Example 5.2.22 (see Theorem 5.2.24).

Proof of Theorem 5.1.2. By Theorem 5.1.3, there exists a constant $C > 0$ depending only on ϕ such that

$$\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{k-1}}.$$

Because $d(v) = \frac{d(v_0)f(v|v_0)}{[K(x):K]}$ and $f(v|v_0) \geq 1$ and $e(v|v_0) \leq [K(x) : K]$, we obtain the result of Theorem 5.1.2. □

As Example 5.2.25 will show, there are infinitely many Drinfeld modules $\phi : A \to K\{\tau\}$ of generic characteristic and there exists $v_0 \in M_K$ such that for every $C > 0$ and every k, there exists $x \in K^{\rm alg}$ and there exists $v|v_0$, $v \in M_{K(x)}$ such that $0 < \widehat{\rm h}_v(x) < \frac{C}{[K(x):K]^k}$. In Theorem 5.2.26 (Chapter 5), we will give the best result towards Statement 5.1.1 for Drinfeld modules of generic characteristic.

5.2 General valuation theory on Drinfeld modules

We fix a coherent valuation $v_0 \in M_K$ of degree $d(v_0)$. As before, for each finite extension L of K and for each $v \in M_L$ such that $v|v_0$, we let $d(v) = \frac{f(v|v_0)d(v_0)}{[L:K]}$. Also, let $\phi : A \to K\{\tau\}$. Most of our results are true for both finite characteristic and generic characteristic Drinfeld modules. We will specify when we restrict ourselves to the case of Drinfeld modules of finite characteristic.

In proving (5.1.3), replacing K by a finite extension K' may induce only a constant factor $[K' : K]$ in the denominator of the lower bound for the local height (see Corollary 5.1.4 and inequality (4.10)).

Fix a nonconstant $t \in A$ and let $\phi_t = \sum_{i=r_0}^{r} a_i\tau^i$, where both a_{r_0} and a_r are nonzero and $0 \leq r_0 \leq r$, while $r \geq 1$. Theorem 5.1.3 is not affected if we replace ϕ by a Drinfeld module that is isomorphic to ϕ. Thus we can conjugate

ϕ by an element $\gamma \in K^{\text{alg}} \setminus \{0\}$ such that $\phi^{(\gamma)}$, the conjugated Drinfeld module, has the property that $\phi_t^{(\gamma)}$ is monic as a polynomial in τ. Then ϕ and $\phi^{(\gamma)}$ are isomorphic over $K(\gamma)$, which is a finite extension of K (because γ satisfies the equation $\gamma^{q^r-1}a_r = 1$).

So, we will prove Theorem 5.1.3 for $\phi^{(\gamma)}$ and because $\widehat{\mathrm{h}}_{\phi,v}(x) = \widehat{\mathrm{h}}_{\phi^{(\gamma)},v}(\gamma^{-1}x)$ for every place $v|v_0$ of $K(\gamma, x)$ (as proved in [22], Proposition 2) the result will follow for ϕ.

From now on, in this chapter, ϕ_t is monic as a polynomial in τ.

Let L be a finite extension of K and let $v \in M_L$ be a place lying over v_0. Denote by $S = S_L$ the subset of M_L where the coefficients a_i, for $i \in \{r_0, \ldots, r-1\}$, have poles. Also, denote by $S_0 = S_K$ the set of places from M_K where the coefficients a_i have poles. Thus, $v \in S$ if and only if $v_0 \in S_0$. We recall here the definition of places of good reduction.

Definition 5.2.1. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. Let L be a finite extension of K. We call $v \in M_L$ a place of *good* reduction for ϕ if for all $a \in A \setminus \{0\}$, the coefficients of ϕ_a are integral at v and the leading coefficient of ϕ_a is a unit in the valuation ring at v. If $v \in M_L$ is not a place of good reduction, we call it a place of *bad* reduction.

Lemma 5.2.2. *The set S_L is the set of all places from M_L at which ϕ has bad reduction.*

Proof. By the construction of the set S_L, the places from S_L are of bad reduction for ϕ. We will prove that these are all the bad places for ϕ.

Let $a \in A$. The equation $\phi_a \phi_t = \phi_t \phi_a$ will show that all the places where not all of the coefficients of ϕ_a are integral, are from S_L. Suppose this is not the case and take a place $v \notin S_L$ at which some coefficient of ϕ_a is not integral. Let $\phi_a = \sum_{i=0}^{r'} a'_i \tau^i$ and assume that i is the largest index for a coefficient a'_i that is not integral at v.

We equate the coefficient of τ^{i+r} in $\phi_a \phi_t$ and $\phi_t \phi_a$, respectively. The former is

$$a'_i + \sum_{j>i} a'_j a_{r+i-j}^{q^j} \tag{5.1}$$

while the latter is

$$a_i'^{q^r} + \sum_{j>i} a_{r+i-j} a_j'^{q^{r+i-j}}. \tag{5.2}$$

Thus the valuation at v of (5.1) is $v(a'_i)$, because all the a'_j (for $j > i$) and a_{r+i-j} are integral at v, while $v(a'_i) < 0$. Similarly, the valuation of (5.2) is $v(a_i'^{q^r}) = q^r v(a'_i) < v(a'_i)$ ($r \geq 1$ because t is non-constant). This fact gives a contradiction to $\phi_a \phi_t = \phi_t \phi_a$. So, the coefficients of ϕ_a for all $a \in A$, are integral at all places of $M_L \setminus S_L$.

Now, using the same equation $\phi_a \phi_t = \phi_t \phi_a$ and equating the leading coefficients in both polynomials we obtain

$$a'_{r'} = a_{r'}'^{q^r}.$$

So, $a'_{r'} \in \mathbb{F}_p^{\mathrm{alg}}$. Thus, all the leading coefficients for polynomials ϕ_a are constants. So, if $v \in M_L \setminus S_L$, then all the coefficients of ϕ_a are integral at v and the leading coefficient of ϕ_a is a unit in the valuation ring at v for every $a \in A \setminus \{0\}$. Thus, $v \notin S_L$ is a place of good reduction for ϕ. □

For each $v \in M_L$ denote by

$$M_v = \min_{i \in \{r_0, \ldots, r-1\}} \frac{v(a_i)}{q^r - q^i} \tag{5.3}$$

where by convention: $v(0) = +\infty$. If $r_0 = r$, definition (5.3) is void and in that case we define $M_v = +\infty$.

Note that $M_v < 0$ if and only if $v \in S$.

For each $v \in S$ we fix a uniformizer $\pi_v \in L$ of the place v. We define next the concept of angular component for every $y \in L \setminus \{0\}$.

Definition 5.2.3. Assume $v \in S$. For every nonzero $y \in L$ we define the angular component of y at v, denoted by $\mathrm{ac}_{\pi_v}(y)$, to be the residue at v of $y\pi_v^{-v(y)}$. (Note that the angular component is never 0.)

We can define in a similar manner as above the notion of angular component at each $v \in M_L$ but we will work with angular components at the places from S only.

The main property of the angular component is that for every $y, z \in L \setminus \{0\}$, $v(y - z) > v(y) = v(z)$ if and only if $(v(y), \mathrm{ac}_{\pi_v}(y)) = (v(z), \mathrm{ac}_{\pi_v}(z))$.

Our strategy for proving (5.1.3) will be to prove that if $\widehat{\mathrm{h}}_v(x) > 0$ then *either*

$$\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}$$

where $C > 0$ is a constant depending only on ϕ, *or*

$v \in S$ and $(v(x), \mathrm{ac}_{\pi_v}(x))$ belongs to a set of cardinality we can control.

If $v \in S$ we define P_v as the set containing $\{0\}$ and all the negatives of the non-negative slopes of the Newton polygon of ϕ_t, i.e. numbers of the form

$$\alpha = -\frac{v(a_i) - v(a_j)}{q^i - q^j} = \frac{v(a_i) - v(a_j)}{q^j - q^i} \leq 0, \tag{5.4}$$

for some $i \neq j$ in $\{r_0, \ldots, r\}$ such that

$$v(a_i) + q^i\alpha = v(a_j) + q^j\alpha = \min_{r_0 \leq l \leq r} \left(v(a_l) + q^l\alpha \right).$$

Clearly, $|P_v| \leq r - r_0 + 1$, because there are at most $(r - r_0)$ sides of the Newton polygon of ϕ_t.

For each $\alpha \in P_v$ we let $l \geq 1$ and let $i_0 < i_1 < \cdots < i_l$ be all the indices i for which $a_i \neq 0$ and

$$v(a_i) + q^i\alpha = \min_{r_0 \leq j \leq r} \left(v(a_j) + q^j\alpha \right).$$

Moreover, if $l \geq 1$ then for $j, k \in \{0, \ldots, l\}$ with $j \neq k$, we have

$$\frac{v(a_{i_j}) - v(a_{i_k})}{q^{i_k} - q^{i_j}} = \alpha. \tag{5.5}$$

We define $R_v(\alpha)$ as the set containing $\{1\}$ and all the nonzero solutions of the equation

$$\sum_{j=0}^{l} \mathrm{ac}_{\pi_v}(a_{i_j}) X^{q^{i_j}} = 0, \tag{5.6}$$

where the indices i_j are the ones associated to α as in (5.5). Clearly, for every $\alpha \in P_v$, $|R_v(\alpha)| \leq q^r$, because there are at most $(q^r - 1)$ nonzero solutions to (5.6).

Note that if $\alpha = 0$, there might be no indices i_j and i_k as in (5.5). In that case, the construction of $R_v(0)$ from (5.6) is void and so, $R_v(0) = \{1\}$. The motivation for the special case $0 \in P_v$ and $1 \in R_v(0)$ is explained in the proof of Lemma 5.2.9.

We remind the reader that our setting for this Chapter will always be that $v_0 \in M_K$ is a coherent valuation and for a finite extension L of K, the place $v \in M_L$ lies over v_0.

Lemma 5.2.4. *Assume $v \in S$ and let $x \in L$. If $v(\phi_t(x)) > \min_{i \in \{r_0, \ldots, r\}} v(a_i x^{q^i})$ then $(v(x), \mathrm{ac}_{\pi_v}(x)) \in P_v \times R_v(v(x))$.*

Proof. If $v(\phi_t(x)) > \min_{i \in \{r_0, \ldots, r\}} v(a_i x^{q^i})$ it means that there exists $l \geq 1$ and

$$i_0 < \cdots < i_l$$

such that

$$v(a_{i_0} x^{q^{i_0}}) = \cdots = v(a_{i_l} x^{q^{i_l}}) = \min_{i \in \{r_0, \ldots, r\}} v(a_i x^{q^i}) \tag{5.7}$$

and also

$$\sum_{j=0}^{l} \mathrm{ac}_{\pi_v}(a_{i_j}) \, \mathrm{ac}_{\pi_v}(x)^{q^{i_j}} = 0. \tag{5.8}$$

Equations (5.7) and (5.8) yield $v(x) \in P_v$ and $\mathrm{ac}_{\pi_v}(x) \in R_v(v(x))$ respectively, according to (5.4) and (5.6). □

Lemma 5.2.5. *Let $v \in M_L$ and let $x \in L$. If $v(x) < \min\{0, M_v\}$, then $\widehat{\mathrm{h}}_v(x) = -d(v) \cdot v(x)$.*

Proof. For every $i \in \{r_0, \ldots, r-1\}$, $v(a_i x^{q^i}) = v(a_i) + q^i v(x) > q^r v(x)$ because $v(x) < M_v = \min_{i \in \{r_0, \ldots, r-1\}} \frac{v(a_i)}{q^r - q^i}$. This shows that $v(\phi_t(x)) = q^r v(x) < v(x) < \min\{0, M_v\}$. By induction, $v(\phi_{t^n}(x)) = q^{rn} v(x)$ for all $n \geq 1$. So, $V_v(x) = v(x)$ and

$$\widehat{\mathrm{h}}_v(x) = -d(v) \cdot v(x).$$

□

An immediate corollary to (5.2.5) is the following result.

Lemma 5.2.6. *Assume $v \notin S$ and let $x \in L$. If $v(x) < 0$ then $\widehat{\mathrm{h}}_v(x) = -d(v) \cdot v(x)$, while if $v(x) \geq 0$ then $\widehat{\mathrm{h}}_v(x) = 0$.*

Proof. First, it is clear that if $v(x) \geq 0$ then for all $n \geq 1$, $v(\phi_{t^n}(x)) \geq 0$ because all the coefficients of ϕ_t and thus of ϕ_{t^n} have non-negative valuation at v. Thus $V_v(x) = 0$ and so,

$$\widehat{\mathrm{h}}_v(x) = 0.$$

Now, if $v(x) < 0$, then $v(x) < M_v$ because $M_v \geq 0$ ($v \notin S$). So, applying the result of (5.2.5) we conclude the proof of this lemma. □

We will get a better insight into the local heights behaviour with the following lemma.

Lemma 5.2.7. *Let $x \in L$. Assume $v \in S$ and $v(x) \leq 0$. If $(v(x), \mathrm{ac}_{\pi_v}(x)) \notin P_v \times R_v(v(x))$ then $v(\phi_t(x)) < M_v$, unless $q = 2$, $r = 1$ and $v(x) = 0$.*

Proof. Lemma 5.2.4 implies that there exists $i_0 \in \{r_0, \ldots, r\}$ such that for all $i \in \{r_0, \ldots, r\}$ we have $v(a_i x^{q^i}) \geq v(a_{i_0} x^{q^{i_0}}) = v(\phi_t(x))$.

Suppose (5.2.7) is not true and so, there exists $j_0 < r$ such that

$$\frac{v(a_{j_0})}{q^r - q^{j_0}} \leq v(\phi_t(x)) = v(a_{i_0}) + q^{i_0} v(x).$$

This means that

$$v(a_{j_0}) \leq (q^r - q^{j_0}) v(a_{i_0}) + (q^{r+i_0} - q^{i_0+j_0}) v(x). \tag{5.9}$$

On the other hand, by our assumption about i_0, we know that $v(a_{j_0} x^{q^{j_0}}) \geq v(a_{i_0} x^{q^{i_0}})$ which means that

$$v(a_{j_0}) \geq v(a_{i_0}) + (q^{i_0} - q^{j_0}) v(x). \tag{5.10}$$

Putting together inequalities (5.9) and (5.10), we get

$$v(a_{i_0}) + (q^{i_0} - q^{j_0}) v(x) \leq (q^r - q^{j_0}) v(a_{i_0}) + (q^{r+i_0} - q^{i_0+j_0}) v(x).$$

Thus

$$v(x)(q^{r+i_0} - q^{i_0+j_0} - q^{i_0} + q^{j_0}) \geq -v(a_{i_0})(q^r - q^{j_0} - 1). \tag{5.11}$$

But $q^{r+i_0} - q^{i_0+j_0} - q^{i_0} + q^{j_0} = q^{r+i_0}(1 - q^{j_0-r} - q^{-r} + q^{j_0-r-i_0})$ and because $j_0 < r$ and $q^{j_0-r-i_0} > 0$, we obtain

$$1 - q^{j_0-r} - q^{-r} + q^{j_0-r-i_0} > 1 - q^{-1} - q^{-r} \geq 1 - 2q^{-1} \geq 0. \qquad (5.12)$$

Also, $q^r - q^{j_0} - 1 \geq q^r - q^{r-1} - 1 = q^{r-1}(q-1) - 1 \geq 0$ with equality if and only if $q = 2$, $r = 1$ and $j_0 = 0$. We will analyze this case separately. So, as long as we are not in this special case, we do have

$$q^r - q^{j_0} - 1 > 0. \qquad (5.13)$$

Now we have two possibilities (remember that $v(x) \leq 0$):

(i) $v(x) < 0$

In this case, (5.11), (5.12) and (5.13) tell us that $-v(a_{i_0}) < 0$. Thus, $v(a_{i_0}) > 0$. But we know from our hypothesis on i_0 that $v(a_{i_0}x^{q^{i_0}}) \leq v(x^{q^r})$ which is in contradiction with the combination of the following facts: $v(x) < 0$, $i_0 \leq r$ and $v(a_{i_0}) > 0$.

(ii) $v(x) = 0$

Then another use of (5.11), (5.12) and (5.13) gives us $-v(a_{i_0}) \leq 0$; thus $v(a_{i_0}) \geq 0$. This would mean that $v(a_{i_0}x^{q^{i_0}}) \geq 0$ and this contradicts our choice for i_0 because we know from the fact that $v \in S$, that there exists $i \in \{r_0, \ldots, r\}$ such that $v(a_i) < 0$. So, then we would have

$$v(a_i x^{q^i}) = v(a_i) < 0 \leq v(a_{i_0}x^{q^{i_0}}).$$

Thus, in either case (i) or (ii) we get a contradiction that proves the lemma except in the special case that we excluded above: $q = 2$, $r = 1$ and $j_0 = 0$. If we have $q = 2$ and $r = 1$ then

$$\phi_t(x) = a_0 x + x^2.$$

By the definition of S and because $v \in S$, $v(a_0) < 0$. Also, $M_v = v(a_0)$.

If $v(x) < 0$, then either $v(x) < M_v = v(a_0)$, in which case again $v(\phi_t(x)) < M_v$ (as shown in the proof of lemma (5.2.5)), or $v(x) \geq M_v$. In the latter case,

$$v(\phi_t(x)) = v(a_0 x) = v(a_0) + v(x) < v(a_0) = M_v.$$

So, we see that indeed, only $v(x) = 0$, $q = 2$ and $r = 1$ can make $v(\phi_t(x)) \geq M_v$ in the hypothesis of (5.2.7). $\square$

Lemma 5.2.8. *Assume $v \in S$ and let $x \in L$. Excluding the case $q = 2$, $r = 1$ and $v(x) = 0$, we have that if $v(x) \leq 0$ then either $\widehat{\mathrm{h}}_v(x) > \frac{-d(v)M_v}{q^r}$ or $(v(x), ac_{\pi_v}(x)) \in P_v \times R_v(v(x))$.*

Proof. If $v(x) \leq 0$ then

either: (i) $v(\phi_t(x)) < M_v$,

in which case by (5.2.5) we have that $\widehat{\mathrm{h}}_v(\phi_t(x)) = -d(v) \cdot v(\phi_t(x))$. So, case (i) yields

$$\widehat{\mathrm{h}}_v(x) = -d(v) \cdot \frac{v(\phi_t(x))}{\deg \phi_t} > -d(v) \cdot \frac{M_v}{q^r} \tag{5.14}$$

$$or\text{: (ii) } v(\phi_t(x)) \geq M_v \ ,$$

in which case, lemma (5.2.7) yields

$$v(\phi_t(x)) > v(a_{i_0}x^{q^{i_0}}) = \min_{i\in\{r_0\dots,r\}} v(a_i x^{q^i}). \tag{5.15}$$

Using (5.15) and lemma (5.2.4) we conclude that case (ii) yields $(v(x), \mathrm{ac}_{\pi_v}(x)) \in P_v \times R_v(v(x))$. □

Now we analyze the excluded case from lemma (5.2.8).

Lemma 5.2.9. *Assume $v \in S$ and let $x \in L$. If $v(x) \leq 0$, then either*

$$(v(x), ac_{\pi_v}(x)) \in P_v \times R_v(v(x))$$

or $\widehat{\mathrm{h}}_v(x) \geq \frac{-d(v)M_v}{q^r}$.

Proof. Using the result of (5.2.8) we have left to analyze the case: $q = 2$, $r = 1$ and $v(x) = 0$.

As shown in the proof of (5.2.7), in this case $\phi_t(x) = a_0x + x^2$ and

$$v(\phi_t(x)) = v(a_0) = M_v < 0.$$

Then, either $v(\phi_{t^2}(x)) = v(\phi_t(x)^2) = 2M_v < M_v$ or $v(\phi_{t^2}(x)) > v(a_0\phi_t(x)) = v(\phi_t(x)^2)$. If the former case holds, then by (5.2.5),

$$\widehat{\mathrm{h}}_v(\phi_{t^2}(x)) = -d(v) \cdot 2M_v$$

and so,

$$\widehat{\mathrm{h}}_v(x) = \frac{-d(v) \cdot 2M_v}{4}.$$

If the latter case holds, i.e. $v(\phi_t(\phi_t(x))) > v(a_0\phi_t(x)) = v(\phi_t(x)^2)$, then $\mathrm{ac}_{\pi_v}(\phi_t(x))$ satisfies the equation

$$\mathrm{ac}_{\pi_v}(a_0)X + X^2 = 0.$$

Because the angular component is never 0, it must be that $\mathrm{ac}_{\pi_v}(\phi_t(x)) = \mathrm{ac}_{\pi_v}(a_0)$ (remember that we are working now in characteristic 2). But, because $v(a_0x) < v(x^2)$ we can relate the angular component of x and the angular component of $\phi_t(x)$ and so,

$$\mathrm{ac}_{\pi_v}(a_0) = \mathrm{ac}_{\pi_v}(\phi_t(x)) = \mathrm{ac}_{\pi_v}(a_0x) = \mathrm{ac}_{\pi_v}(a_0)\,\mathrm{ac}_{\pi_v}(x).$$

This means $\mathrm{ac}_{\pi_v}(x) = 1$ and so, the excluded case amounts to a dichotomy similar to the one from (5.2.8): either $(v(x), \mathrm{ac}_{\pi_v}(x)) = (0, 1)$ or $\widehat{\mathrm{h}}_v(x) = \frac{-d(v)M_v}{2}$. The definitions of P_v and $R_v(\alpha)$ from (5.4) and (5.6) respectively, yield that $(0, 1) \in P_v \times R_v(0)$. □

Finally, we note that in (5.2.9) we have

$$-\frac{d(v)M_v}{q^r} = -\frac{d(v)e(v|v_0)M_{v_0}}{q^r}.$$

We have obtained the following dichotomy.

Lemma 5.2.10. *Assume $v \in S$ and let $x \in L$. If $v(x) \leq 0$ then either*

$$\widehat{\mathrm{h}}_v(x) \geq \frac{-d(v)e(v|v_0)M_{v_0}}{q^r}$$

or

$$(v(x), \mathrm{ac}_{\pi_v}(x)) \in P_v \times R_v(v(x))$$

with $|P_v| \leq r - r_0 + 1$ and for each $\alpha \in P_v$, $|R_v(\alpha)| \leq q^r$.

The following lemma shows that if $(v(x), \mathrm{ac}_{\pi_v}(x)) \notin P_v \times R_v(v(x))$, then $v(\phi_t(x))$ is determined completely only in terms of $v(x)$.

Lemma 5.2.11. *There are no x and x' in L verifying the following properties*

(a) $v(x) \neq v(x')$;

(b) $(v(x), \mathrm{ac}_{\pi_v}(x)) \notin P_v \times R_v(v(x))$ and $(v(x'), \mathrm{ac}_{\pi_v}(x')) \notin P_v \times R_v(v(x'))$;

(c) $v(\phi_t(x)) = v(\phi_t(x'))$.

Proof. Condition (b) yields

$$v(\phi_t(x)) = \min_{r_0 \leq i \leq r} v(a_i x^{q^i})$$

and

$$v(\phi_t(x')) = \min r_0 \leq i \leq r v(a_i x'^{q^i}).$$

Then the conclusion of our lemma is immediate because the function

$$F(y) = \min_{r_0 \leq i \leq r} v(a_i y^{q^i})$$

is a strictly increasing piecewise linear function. □

Lemma 5.2.12. *Assume $v \in S$. Given (α_1, γ_1), there are at most q^r possible values of $\mathrm{ac}_{\pi_v}(x)$ when x ranges over nonzero elements of L such that $(v(x), \mathrm{ac}_{\pi_v}(x)) \notin P_v \times R_v(v(x))$ and $(\alpha_1, \gamma_1) = (v(\phi_t(x)), \mathrm{ac}_{\pi_v}(\phi_t(x)))$.*

Proof. Indeed, we saw in lemma (5.2.11) that $v(x)$ is uniquely determined given $\alpha_1 = v(\phi_t(x))$ under the hypothesis of (5.2.12). We also have

$$\mathrm{ac}_{\pi_v}(\phi_t(x)) = \sum_j \mathrm{ac}_{\pi_v}(a_{i_j})\, \mathrm{ac}_{\pi_v}(x)^{q^{i_j}} \tag{5.16}$$

where i_j runs through a prescribed subset of $\{r_0, \dots, r\}$ corresponding to those i such that $v(a_i) + q^i v(x) = v(\phi_t(x)) = \min_{i \in \{r_0, \dots, r\}} v(a_i x^{q^i})$. This subset of indices i_j, depends only on $\alpha_1 = v(x)$. So, there are at most q^r possible values for $\mathrm{ac}_{\pi_v}(x)$ to solve (5.16) given $\gamma_1 = \mathrm{ac}_{\pi_v}(\phi_t(x))$. □

From now on in this Chapter, unless otherwise stated, we will suppose that

$$\boxed{r_0 \geq 1, \text{ i.e. } \phi \text{ has finite characteristic and } \phi_t \text{ is inseparable.}}$$

Because for every Drinfeld module of finite characteristic we can find a non-constant $t \in A$ such that ϕ_t is inseparable, the above boxed condition will always be achieved for some $t \in A$, in the case of Drinfeld modules of finite characteristic.

Lemma 5.2.13. *If $v \in S$ define $N_v = \max\left\{\frac{-v(a_i)}{q^i - 1} \mid r_0 \leq i \leq r\right\}$ (remember our convention $v(0) = +\infty$). If $v(x) \geq N_v$, then $\widehat{\mathrm{h}}_v(x) = 0$.*

Proof. Indeed, if $v(x) \geq N_v$ then $v(\phi_t(x)) \geq \min_{1 \leq i \leq r}\{q^i v(x) + v(a_i)\} \geq v(x) \geq N_v$. By induction, we get that $v(\phi_{t^n}(x)) \geq N_v$ for all $n \geq 1$, which yields that

$V_v(x) = 0$ and so,

$$\widehat{h}_v(x) = 0.$$

□

Thus, if $v \in S$ and $\widehat{\mathrm{h}}_v(x) > 0$ it must be that $v(x) < N_v$.

Lemma 5.2.14. *Assume $v \in S$ and let $x \in L$. If $v(x) < N_v$ and if $(v(x), \mathrm{ac}_{\pi_v}(x)) \notin P_v \times R_v(v(x))$ then $v(\phi_t(x)) < v(x)$.*

Proof. Indeed, by the hypothesis and by Lemma 5.2.4, there exists $i_0 \in \{r_0, \ldots, r\}$ such that for all $i \in \{r_0, \ldots, r\}$,

$$v(a_{i_0}) + q^{i_0} v(x) = v(\phi_t(x)) \leq v(a_i) + q^i v(x). \tag{5.17}$$

If $v(\phi_t(x)) \geq v(x)$ then, using (5.17), we get that

$$v(x) \leq v(a_i) + q^i v(x)$$

which implies that $v(x) \geq -\frac{v(a_i)}{q^i - 1}$ for every i. Thus

$$v(x) \geq N_v,$$

contradicting the hypothesis of our lemma. So, we must have $v(\phi_t(x)) < v(x)$. In particular, we also get that $v(a_{i_0}) + q^{i_0} v(x) < v(x)$, i.e.

$$v(x) < \frac{-v(a_{i_0})}{q^{i_0} - 1}. \tag{5.18}$$

□

Our goal is to establish a dichotomy similar to the one from Lemma 5.2.10 under the following hypothesis:

$\boxed{v \in S,\ x \in L,\ \widehat{\mathrm{h}}_v(x) > 0 \text{ and } 0 < v(x) < N_v.}$

In Lemma 5.2.14 we saw that if $v(x) < N_v$ then either $(v(x), \mathrm{ac}_{\pi_v}(x)) \in P_v \times R_v(v(x))$ or $v(\phi_t(x)) < v(x)$. In the latter case, if $v(\phi_t(x)) > 0$ we apply then the same reasoning to $\phi_t(x)$ and derive that either $(v(\phi_t(x)), \mathrm{ac}_{\pi_v}(\phi_t(x))) \in P_v \times R_v(v(\phi_t(x)))$ or $v(\phi_{t^2}) < v(\phi_t(x))$. We repeat this analysis and after a finite number of steps, say n, we must have that either

$$v(\phi_{t^n}(x)) \leq 0$$

or

$$(v(\phi_{t^n}(x)), \mathrm{ac}_{\pi_v}(\phi_{t^n}(x))) \in P_v \times R_v(v(\phi_{t^n}(x))).$$

But we analyzed in (5.2.10) what happens to the cases in which, for an element y of positive local height at v, $v(y) \leq 0$. We obtained that either

$$\widehat{h}_v(y) \geq \frac{-d(v) M_{v_0} e(v|v_0)}{q^r} \tag{5.19}$$

or

$$(v(y), \mathrm{ac}_{\pi_v}(y)) \in P_v \times R_v(v(y)) \tag{5.20}$$

and $|P_v| \leq r - r_0 + 1 \leq r$ because $r_0 \geq 1$.

We will use repeatedly equations (5.19) and (5.20) for $y = \phi_{t^n}(x)$. So, if (5.19) holds for $y = \phi_{t^n}(x)$ then

$$\widehat{h}_v(x) \geq \frac{-d(v)M_{v_0}e(v|v_0)}{q^{rn}q^r}. \tag{5.21}$$

We will see next what happens if (5.20) holds. We can go back through the steps that we made in order to get to (5.20) and see that actually $v(x)$ and $\mathrm{ac}_{\pi_v}(x)$ belong to prescribed sets of cardinality independent of n.

Lemma 5.2.15. *Assume $v \in S$ and suppose that $v(x) < N_v$. If*

$$(v(\phi_{t^k}(x)), \mathrm{ac}_{\pi_v}(\phi_{t^k}(x))) \notin P_v \times R_v(v(\phi_{t^k}(x)))$$

for $0 \leq k \leq n-1$, then for each value

$$(\alpha_n, \gamma_n) = (v(\phi_{t^n}(x)), \mathrm{ac}_{\pi_v}(\phi_{t^n}(x))),$$

the valuation of x is uniquely determined and $\mathrm{ac}_{\pi_v}(x)$ belongs to a set of cardinality at most q^{r^2-r}.

Proof. The fact that $v(x)$ is uniquely determined follows after n successive applications of Lemma 5.2.11 to $\phi_{t^{n-1}}(x), \ldots, \phi_t(x), x$.

Because $(v(\phi_{t^k}(x)), \mathrm{ac}_{\pi_v}(\phi_{t^k}(x))) \notin P_v \times R_v(v(\phi_{t^k}(x)))$ for $k < n$, then we are solving an equation of the form

$$\sum_j \mathrm{ac}_{\pi_v}(a_{i_j})\, \mathrm{ac}_{\pi_v}(\phi_{t^k}(x))^{q^{i_j}} = \mathrm{ac}_{\pi_v}(\phi_{t^{k+1}}(x)) \tag{5.22}$$

in order to express $\mathrm{ac}_{\pi_v}(\phi_{t^k}(x))$ in terms of $\mathrm{ac}_{\pi_v}(\phi_{t^{k+1}}(x))$ for each $k < n$. The equations (5.22) are uniquely determined by the sets of indices $i_j \in \{r_0, \dots, r\}$ which in turn are uniquely determined by $v(\phi_{t^k}(x))$, i.e. for each k and each corresponding index i_j

$$v(a_{i_j}\phi_{t^k}(x)^{q^{i_j}}) = \min_{i\in\{r_0,\dots,r\}} v(a_i\phi_{t^k}(x)^{q^i}). \tag{5.23}$$

Using the result of (5.2.14) and the hypothesis of our lemma, we see that

$$v(x) > v(\phi_t(x)) > v(\phi_{t^2}(x)) > \cdots > v(\phi_{t^n}(x)) \tag{5.24}$$

and so the equations from (5.22) appear in a prescribed order. Now, in most of the cases, these equations will consist of only one term on their left-hand side; i.e. they will look like

$$\mathrm{ac}_{\pi_v}(a_{i_0})\,\mathrm{ac}_{\pi_v}(\phi_{t^k}(x))^{q^{i_0}} = \mathrm{ac}_{\pi_v}(\phi_{t^{k+1}}(x)). \tag{5.25}$$

Equation (5.25) has a unique solution. The other equations of type (5.22) but not of type (5.25) are associated to some of the values of $v(\phi_{t^k}(x)) \in P_v$. Indeed, according to the definition of P_v from (5.4), only for those values (of the slopes of the Newton polygon of ϕ_t) we can have for $i \neq i'$

$$v(a_i) + q^i v(x) = v(a_{i'}) + q^{i'} v(x) \tag{5.26}$$

and so, both indices i and i' can appear in (5.22).

Thus the number of equations of type (5.22) but not of type (5.25) is at most $r-1$, because there are at most $r - r_0$ different segments (with different slopes) in the Newton polygon of ϕ_t (and also, remember that we are working under the assumption that ϕ_t is inseparable, i.e. $r_0 \geq 1$). Moreover these equations will appear in a prescribed order, each not more than once, because of (5.24). These observations determine the construction of the finite set that will contain all the possible values for $\mathrm{ac}_{\pi_v}(x)$, given $\gamma_n = \mathrm{ac}_{\pi_v}(\phi_{t^n}(x)))$. An equation of type (5.22) can have at most q^r solutions; thus $\mathrm{ac}_{\pi_v}(x)$ lives in a set of cardinality at most q^{r^2-r}. □

Because of the result of (5.2.15), we know that we can construct in an unique way $v(x)$ given $v(\phi_{t^n}(x))$ and the fact that for every $j < n$, $\phi_{t^j}(x)$ does not satisfy (5.20). So, for each n there are at most $|P_v|$ values for $v(x)$ such that

$$(v(\phi_{t^n}(x)), \mathrm{ac}_{\pi_v}(\phi_{t^n}(x))) \in P_v \times R_v(v(\phi_{t^n}(x))) \tag{5.27}$$

and (5.27) does not hold for $n' < n$. We denote by $P_v(n)$ this set of values for $v(x)$. Clearly $P_v(0) = P_v$.

Lemma 5.2.15 yields that for each fixed $(\alpha_n, \gamma_n) \in P_v \times R_v(\alpha_n)$, there are at most q^{r^2-r} possible values for $\mathrm{ac}_{\pi_v}(x)$ such that

$$(v(\phi_{t^n}(x)), \mathrm{ac}_{\pi_v}(\phi_{t^n}(x))) = (\alpha_n, \gamma_n)$$

and $\phi_{t^j}(x)$ does not satisfy (5.20) for $j < n$. For $\alpha = v(x) \in P_v(n)$ we define by $R_v(\alpha)$ the set of all possible values for $\mathrm{ac}_{\pi_v}(x)$ such that (5.27) holds. Let

$v(\phi_{t^n}(x)) = \alpha_n \in P_v$ and using the definition of $R_v(\alpha_n)$ for $\alpha_n \in P_v$ from (5.6), we get

$$|R_v((v(\phi_{t^n}(x)))| \leq q^r. \tag{5.28}$$

Inequality (5.28) and the result of Lemma 5.2.15 gives the estimate:

$$|R_v(\alpha)| \leq |R_v(v(\phi_{t^n}(x)))| \cdot q^{r^2-r} \leq q^r \cdot q^{r^2-r} = q^{r^2} \tag{5.29}$$

for every $\alpha \in P_v(n)$ and for every $n \geq 0$.

Now, we estimate the magnitude of n, i.e. the number of steps that we need to make starting with $0 < v(x) < N_v$ such that in the end $\phi_{t^n}(x)$ satisfies either (5.19) or (5.20).

Lemma 5.2.16. *Assume $v \in S$ and $\widehat{\mathrm{h}}_v(x) > 0$. Then there exists a set P of cardinality bounded in terms of r and $e(v|v_0)$ such that either $(v(x), \mathrm{ac}_{\pi_v}(x)) \in P \times R_v(v(x))$ or $\widehat{\mathrm{h}}_v(x) > \frac{c_1 d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}$ with $c_1 > 0$ depending only on ϕ.*

Proof. If (5.20) does not hold for x then we know that there exists $i_0 \geq r_0$ such that $v(\phi_t(x)) = q^{i_0}v(x) + v(a_{i_0})$.

Now, if $\phi_t(x)$ also does not satisfy (5.20) then for some i_1

$$v(\phi_{t^2}(x)) = q^{i_1}v(x) + v(a_{i_1}) \leq q^i v(\phi_t(x)) + v(a_i)$$

for all $i \in \{r_0, \ldots, r\}$. So, in particular

$$v(\phi_{t^2}(x)) \leq q^{i_0}v(\phi_t(x)) + v(a_{i_0}) \tag{5.30}$$

and in general

$$v(\phi_{t^{k+1}}(x)) \leq q^{i_0} v(\phi_{t^k}(x)) + v(a_{i_0}) \tag{5.31}$$

if $(v(\phi_{t^k}(x)), \mathrm{ac}_{\pi_v}(\phi_{t^k}(x))) \notin P_v \times R_v(v(\phi_{t^k}(x)))$. Let us define the sequence $(y_j)_{j\geq 0}$ by

$$y_0 = v(x) \text{ and for all } j \geq 1\text{: } y_j = q^{i_0} y_{j-1} + v(a_{i_0}).$$

If $\phi_{t^i}(x)$ does not satisfy (5.20) for $i \in \{0, \ldots, n-1\}$ then by (5.31),

$$y_n \geq v(\phi_{t^n}(x)). \tag{5.32}$$

The sequence $(y_j)_{j\geq 0}$ can be easily computed and we see that

$$y_j = q^{i_0 j} \left(v(x) + \frac{v(a_{i_0})}{q^{i_0} - 1} \right) - \frac{v(a_{i_0})}{q^{i_0} - 1}. \tag{5.33}$$

But $v(x) < -\frac{v(a_{i_0})}{q^{i_0}-1}$, as a consequence of $v(x) < N_v$ and the proof of Lemma 5.2.14 (see equation (5.18)). Thus,

$$v(x) + \frac{v(a_{i_0})}{q^{i_0} - 1} \leq -\frac{1}{q^{i_0} - 1} \tag{5.34}$$

because $v(x), v(a_{i_0}) \in \mathbb{Z}$. Using inequality (5.34) in the formula (5.33) we get

$$y_j \leq \frac{1}{q^{i_0} - 1}(-q^{i_0 j} - v(a_{i_0})). \tag{5.35}$$

We define

$$c_{v_0} = \max \left\{ -v_0(a_i) | r_0 \leq i \leq r \right\}. \tag{5.36}$$

So, $c_{v_0} \geq 1$ because we know that at least one of the a_i has a pole at v, thus at v_0 (we are working under the assumption that $v \in S$). Clearly, c_{v_0} depends only on ϕ (the dependence on K is part of the Drinfeld module data for ϕ). For simplicity, we denote c_{v_0} by c. Because of the definition of c, we have

$$-v(a_{i_0}) \leq e(v|v_0)c \tag{5.37}$$

where $e(v|v_0)$ is as always the ramification index of v over v_0. Now, if we pick m minimal such that

$$q^{r_0 m} \geq ce(v|v_0) \tag{5.38}$$

then we see that m depends only on ϕ and $e(v|v_0)$. Using that $i_0 \geq r_0$ we get that

$$q^{i_0 m} \geq ce(v|v_0). \tag{5.39}$$

So, using inequalities (5.35), (5.37) and (5.39) we obtain $y_m \leq 0$. Because of (5.32) we derive that

$$v(\phi_{t^m}(x)) \leq 0$$

which according to the dichotomy from Lemma 5.2.10 yields that $\phi_{t^m}(x)$ satisfies either (5.19) or (5.20). Thus, we need at most m steps to get from x to some $\phi_{t^n}(x)$ for which one of the two equations (5.19) or (5.20) is valid. This means that either

$$\widehat{h}_v(x) \geq \frac{-d(v)M_{v_0}e(v|v_0)}{q^{rm}q^r} \text{ (which holds if (5.19) is valid after } n \leq m \text{ steps),} \tag{5.40}$$

or

$$\phi_{t^n}(x)\,\text{satisfies (5.20) for}\,n \le m. \tag{5.41}$$

This last equation implies that $(v(x), \mathrm{ac}_{\pi_v}(x)) \in P_v(n) \times R_v(v(x))$ for some $n \le m$.

We analyze now the inequality from equation (5.40). By the minimality of m satisfying (5.38), we have

$$q^{rm} = (q^{r_0(m-1)})^{\frac{r}{r_0}} q^r < (ce(v|v_0))^{\frac{r}{r_0}} q^r. \tag{5.42}$$

So, if (5.40) holds, we have the following inequality

$$\widehat{h}_v(x) > \frac{-d(v)M_{v_0}e(v|v_0)}{c^{\frac{r}{r_0}} q^{2r} e(v|v_0)^{\frac{r}{r_0}}}. \tag{5.43}$$

We denote by $P = \bigcup_{i=0}^{m} P_v(i)$. We proved that for $i \ge 1$, $|P_v(i)| \le |P_v(0)|$ (and $P_v = P_v(0)$ has cardinality depending only on r; this was mainly the content of (5.2.15)). To simplify the notation in the future we introduce new constants c_i, that will always depend only on ϕ. For example, M_{v_0} is a negative number which is at most $-\frac{1}{q^r-1}$ and so, (5.43) says that

$$\widehat{h}_v(x) > \frac{c_1 d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}} \text{ or } (v(x), \mathrm{ac}_{\pi_v}(x)) \in P \times R_v(v(x)) \tag{5.44}$$

and $|R_v(v(x))| \le q^{r^2}$, while $|P| \le r(m+1)$ with m satisfying (5.42). □

For the convenience of the reader we restate the exact findings of Lemma 5.2.16 in a separate corollary.

Corollary 5.2.17. *Assume $v \in S$ and $\widehat{\mathrm{h}}_v(x) > 0$. Let $c = \max_i -v_0(a_i)$. Let m be the first integer such that $q^{r_0 m} \geq ce(v|v_0)$. There exists a positive constant c_1 depending only on ϕ and there exists a set P of cardinality bounded above by $r(m+1)$ such that either*

$$(v(x, \mathrm{ac}_{\pi_v}(x)) \in P \times R_v(v(x))$$

or $\widehat{\mathrm{h}}_v(x) > \frac{c_1 d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}$. Moreover, if the former case holds, then $|R_v(v(x))| \leq q^{r^2}$.

Lemma 5.2.18. *Let L be a field extension of $\mathbb{F}_q$ and let v be a discrete valuation on L. Let I be a finite set of integers. Let N be an integer greater or equal than all the elements of I. For each $\alpha \in I$, let $R(\alpha)$ be a nonempty finite set of nonzero elements of the residue field at v. Let W be an $\mathbb{F}_q$-vector subspace of L with the property that for all $w \in W$, $(v(w), \mathrm{ac}_{\pi_v}(w)) \in I \times R(v(w))$ whenever $v(w) \leq N$.*

Let f be the smallest positive integer greater or equal than $\max_{\alpha \in I} \log_q |R(\alpha)|$. Then the $\mathbb{F}_q$-codimension of $\{w \in W \mid v(w) > N\}$ is bounded by $|I|f$.

Proof. Let $i = |I|$. Let $\alpha_0 < \cdots < \alpha_{i-1}$ be the elements of I, and let $\alpha_i = N+1$. For $0 \leq j \leq i$, define $W_j = \{w \in W | v(w) \geq \alpha_j\}$. For $0 \leq j < i$, the hypothesis gives an injection

$$W_j/W_{j+1} \to R(\alpha_j) \cup \{0\}$$

taking w to the residue of $w/\pi_v^{\alpha_j}$. Thus

$$q^{\dim_{\mathbb{F}_q} W_j/W_{j+1}} \leq q^f + 1 < q^{f+1},$$

so $\dim_{\mathbb{F}_q} W_j/W_{j+1} \leq f$ (note that we used the fact that $f > 0$ in order to have the inequality $q^f + 1 < q^{f+1}$). Summing over j gives $\dim_{\mathbb{F}_q} W_0/W_i \leq if$, as desired. □

We are ready to prove Theorem 5.1.3.

Proof of Theorem 5.1.3. We know that $\widehat{\mathrm{h}}_v(x) > 0$. Because ϕ is a Drinfeld module of finite characteristic, there exists a non-constant $t \in A$ such that ϕ_t is inseparable.

First we observe that if $v \notin S$ then by Lemma 5.2.6 we automatically get the lower bound $\widehat{\mathrm{h}}_v(x) \geq d(v)$, because it must be that $v(x) < 0$, otherwise we would have $\widehat{\mathrm{h}}_v(x) = 0$. So, from now on we suppose that the valuation v is from S.

Let $z = |P|$. Let f be the smallest positive integer such that

$$f \geq \max_{\alpha \in P} \log_q |R_v(\alpha)|.$$

So $f \leq r^2$, as shown by the proof of Lemma 5.2.16 (see Corollary 5.2.17). We also have the following inequality (see Corollary 5.2.17)

$$z \cdot f \leq r(m+1) \cdot r^2 = r^3(m+1). \tag{5.45}$$

Let $W = \mathrm{Span}(\{x, \phi_t(x), \ldots, \phi_{t^{zf}}(x)\})$. Because $\widehat{\mathrm{h}}_v(x) > 0$ we know that $x \notin \phi_{\mathrm{tor}}$ and so, $\dim_{\mathbb{F}_q} W = 1 + zf$. We also get from $\widehat{\mathrm{h}}_v(x) > 0$ that for all $0 \neq w \in W$, $\widehat{\mathrm{h}}_v(w) > 0$. Then by Lemma 5.2.13, we get that for all $0 \neq w \in W$, $v(w) \leq N_v - 1$.

We apply Lemma 5.2.18 to W with $I = P$, $R = R_v$, $N = N_v - 1$ and conclude that there exists $0 \neq b \in \mathbb{F}_q[t]$, of degree at most zf in t such that

$$(v(\phi_b(x)), \mathrm{ac}_{\pi_v}(\phi_b(x))) \notin P \times R_v(v(\phi_b(x))). \tag{5.46}$$

We know that $\widehat{h}_v(x) > 0$ and so $\widehat{h}_v(\phi_b(x)) > 0$. Equations (5.46) and (5.44) yield

$$\widehat{h}_v(\phi_b(x)) > \frac{c_1 d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}.$$

Thus

$$\widehat{h}_v(x) > \frac{c_1 d(v)}{q^{r\deg(b)} e(v|v_0)^{\frac{r}{r_0}-1}}.$$

But, using inequality (5.45), we obtain

$$q^{r\deg(b)} \leq q^{rzf} \leq q^{r^4(m+1)} = q^{r^4}(q^{rm})^{r^3}.$$

We use (5.42) and we get

$$q^{r\deg(b)} < q^{r^4}(ce(v|v_0))^{\frac{r}{r_0}\cdot r^3} q^{r^4}.$$

Thus there exists a constant $C > 0$ depending only on c_1, c, q and r such that

$$\widehat{h}_v(x) > \frac{Cd(v)}{e(v|v_0)^{\frac{r^4+r}{r_0}-1}}. \tag{5.47}$$

Because c_1 and c depend only on ϕ we get the conclusion of (5.1.3). □

Remark 5.2.19. From the above proof we see that the constant C depends only on q, r and the numbers $v_0(a_i)$ for $r_0 \leq i \leq r-1$, under the hypothesis that ϕ_t is monic as a polynomial in τ. As we said before, for the general case, when ϕ_t is not neccessarily monic, the constant C from (5.1.3) will be multiplied by the inverse of the degree of the extension of K that we have to allow in order to construct a conjugated Drinfeld module $\phi^{(\gamma)}$ for which $\phi_t^{(\gamma)}$ is monic. The degree of this extension is at most $(q^r - 1)$ because $\gamma^{q^r-1} a_r = 1$.

Remark 5.2.20. It is interesting to note that (5.47) shows that the original statement of (5.1.1) holds, i.e. $k = 1$, in the case that $e(v|v_0) = 1$, which is the case when x belongs to an unramified extension above v_0. Also, as observed in the beginning of the proof of (5.1.3), if v and so, equivalently v_0 is not a pole for any of the a_i then we automatically get exponent $k = 1$ in Theorem 5.1.3, as proved in Lemma 5.2.6.

So, we see that in the course of proving (5.1.3) we got an even stronger result that allows us to conclude that Conjecture 5.1.1 and so, implicitly Conjecture 1.2.2 hold in the maximal extension unramified above the finitely many places in S_0.

Remark 5.2.21. Also, it is interesting to note that the above proof shows that for every place v associated to L (as in Chapter 2), there exists a number n depending only on r and $e(v|v_0)$ so that there exists $b \in \mathbb{F}_q[t]$ of degree at most n in t for which either $v(\phi_b(x)) < M_v$ (in which case $\widehat{\mathrm{h}}_v(x) > 0$), or $v(\phi_b(x)) \geq N_v$ (in which case $\widehat{\mathrm{h}}_v(x) = 0$).

Example 5.2.22. The result of Theorem 5.1.3 is optimal in the sense that we cannot hope to get the conjectured Lehmer inequality for the local height, i.e. $\frac{C}{d}$. We can only get, in the general case for the local height, an inequality with some exponent $k > 1$, i.e. $\frac{C}{d^k}$.

For example, take $A = \mathbb{F}_q[t]$, $K = \mathbb{F}_q(t)$ and define for some $r \geq 2$,

$$\phi_t = \tau^r - t^{1-q}\tau.$$

Let $d = q^m - 1$, for some $m \geq r$. Then let $x = t\alpha$ where α is a root of

$$\alpha^d - \alpha - \frac{1}{t} = 0.$$

Then $L = K(x)$ is totally ramified above t of degree d. Let v be the unique valuation of L for which $v(t) = d$. We compute

$$P_v = \left\{ \frac{-d(q-1)}{q^r - q} \right\}$$

$$M_v = -\frac{d(q-1)}{q^r - q}$$

$$N_v = d$$

$$v(x) = d - 1 = q^m - 2.$$

We compute easily $v(\phi_{t^i}(x)) = d - q^i$ for every $i \in \{0, \ldots, m\}$. Furthermore, $v(\phi_{t^m}(x)) = d - q^m = -1 \neq \frac{-d(q-1)}{q^r-q}$, because $\frac{-d(q-1)}{q^r-q} \notin \mathbb{Z}$ (since q does not divide $d(q-1)$). Thus $v(\phi_{t^m}(x))$ is negative and not in P_v and so, (5.2.7) yields

$$v(\phi_{t^{m+1}}(x)) < M_v.$$

Actually, because $m \geq r$, an easy computation shows that

$$v(\frac{\phi_{t^m}(x)^q}{t^{q-1}}) = -q - d(q-1) = -q^{m+1} + q^m - 1 < -q^r = v((\phi_{t^m}(x))^{q^r}).$$

This shows that $v(\phi_{t^{m+1}}(x)) = -q^{m+1} + q^m - 1 < M_v < 0$ and so, by (5.2.5)

$$\widehat{\mathrm{h}}_v(x) = \frac{\widehat{\mathrm{h}}_v(\phi_{t^{m+1}}(x))}{q^{r(m+1)}} = \frac{q^{m+1} - q^m + 1}{q^{r(m+1)}d} < \frac{q^{m+1}}{q^{m+r}q^{(r-1)m}d} < \frac{q^{1-r}}{d^r},$$

because $d = q^m - 1 < q^m$.

This computation shows that for Drinfeld modules of type

$$\phi_t = \tau^r - t^{1-q}\tau$$

the exponent k from (5.1.3) should be at least r. The exact same computation will give us that in the case of a Drinfeld module of the form

$$\phi_t = \tau^r - t^{1-q^{r_0}}\tau^{r_0}$$

for some $1 \leq r_0 < r$ and x of valuation $(q^{r_0 m} - 2)$ at a place v that is totally ramified above the place of t with ramification index $q^{r_0 m} - 1$, the exponent k in Theorem 5.1.3 should be at least $\frac{r}{r_0}$. In Theorem 5.2.24 we will prove that for non-wildly ramified extensions above places from S_0, we get exponent $k = \frac{r}{r_0}$. But before doing this, we observe that the present example is just a counter-example to Statement 5.1.1, not to Conjecture 1.2.2. In other words, the global Lehmer inequality holds for our example even if the local one fails.

Indeed, because x was chosen to have positive valuation at the only place from S, then there exists another place, call it v' which is not in S, for which $v'(x) < 0$. But then by lemma (5.2.6), we get that $\widehat{\mathrm{h}}_{v'}(x) \geq \frac{1}{d}$, which means that also $\widehat{\mathrm{h}}(x) \geq \frac{1}{d}$. Thus we obtain a lower bound for the global height as conjectured in (1.2.2).

Now, in order to get to the result of (5.2.24) we prove a lemma.

Lemma 5.2.23. *With the notation from the proof of Theorem 5.1.3, let*

$$L = \mathrm{lcm}_{i \in \{1,\dots,r-r_0\}}\{q^i - 1\}.$$

If v is not wildly ramified above v_0 (i.e., p does not divide $e(v|v_0)$), then $e(v|v_0)$ divides $L\alpha$ for every $\alpha \in P$.

Proof. Indeed, from its definition (5.4), P_v contains $\{0\}$ and numbers of the form

$$\frac{v(a_i) - v(a_j)}{q^j - q^i} = \frac{v(a_i) - v(a_j)}{q^i(q^{j-i} - 1)},$$

for $j > i$. Clearly, every number of this form, times L is divisible by $e(v|v_0)$, because we supposed that $p \nmid e(v|v_0)$. The set $P_v(1)$ contains numbers of the form

$$\frac{\alpha - v(a_i)}{q^i} \tag{5.48}$$

where $\alpha \in P_v = P_v(0)$ and $a_i \neq 0$. Using again that p does not divide $e(v|v_0)$ we get that $e(v|v_0) \mid L\alpha_1$ for all $\alpha_1 \in P_v(1)$. Repeating the process from (5.48) we obtain all the elements of $P_v(n)$ for every $n \geq 1$ and by induction on n, we conclude that $e(v|v_0) \mid L\alpha_n$ for all $\alpha_n \in P_v(n)$. Because $P = \bigcup_{n=0}^{m} P_v(n)$ we get the result of this lemma. □

Theorem 5.2.24. *Let K be a field of characteristic p. Let $v_0 \in M_K$ be a coherent valuation and let $d(v_0)$ be the degree of v_0.*

Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic. Let $t \in A$ such that $\phi_t = \sum_{i=r_0}^{r} a_i\tau^i$ is inseparable and assume $a_{r_0} \neq 0$. Let $x \in K^{\text{alg}}$ and let $v \in M_{K(x)}$ be a place lying over v_0. Assume that $\widehat{\text{h}}_v(x) > 0$.

There exists a constant $C > 0$ depending only on ϕ such that if v is not wildly ramified above v_0, then $\widehat{h}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}$.

Proof. Just as we observed in Remark 5.2.19, it suffices to prove (5.2.24) under the hypothesis that ϕ_t is monic in τ.

Let now $d = [K(x) : K]$. We observe again that from (5.2.6) it follows that if $v \notin S$ then $\widehat{\text{h}}_v(x) \geq d(v) \geq \frac{d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}$.

So, from now on we consider the case $v \in S$.

Then, using the result of (5.2.23) in (5.18) we see that

$$v(x) + \frac{v(a_{i_0})}{q^{i_0} - 1} \leq -\frac{\frac{e(v|v_0)}{L}}{q^{i_0} - 1}, \tag{5.49}$$

if $v(x) \in P$. Then also (5.35) changes into

$$y_m \leq \frac{1}{q^{i_0} - 1}(-q^{i_0 m}\frac{e(v|w)}{L} - v(a_{i_0})). \tag{5.50}$$

So, then we choose m' minimal such that

$$q^{r_0 m'} \geq cL \tag{5.51}$$

where $c = c_{v_0}$ is the same as in (5.36). Thus m' depends only on ϕ and K, but the dependence on K can be considered as part of the dependence on ϕ. We redo the computations from (5.40) to (5.44), this time with m' in place of m and because of (5.50) and (5.51), we get that

$$\widehat{h}_v(x) > \frac{c_1 d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}} \text{ or } (v(x), \mathrm{ac}_{\pi_v}(x)) \in P' \times R_v(v(x)) \tag{5.52}$$

where $P' = \bigcup_{i=0}^{m'} P_v(i)$. At this moment we can redo the argument from the proof of (5.1.3) using P' instead of P, only that now $z' = |P'|$ is independent of x or d. We conclude once again that there exists b, a polynomial in t of degree at most $z'f$ such that

$$\widehat{h}_v(\phi_b(x)) > \frac{c_1 d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}.$$

But because both f and z' depend only on ϕ, we conclude that indeed,

$$\widehat{h}(x) \geq \frac{C d(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}$$

with $C > 0$ depending only on ϕ. $\square$

Example 5.2.25. We discuss now Statement 5.1.1 for Drinfeld modules of generic characteristic. Consider the Carlitz module defined on $\mathbb{F}_p[t]$ by $\phi_t = t\tau^0 + \tau$, where $\tau(x) = x^p$ for all x. Take $K = \mathbb{F}_p(t)$. Let L be a finite extension of K which is totally ramified above ∞ and let the ramification index equal $d = [L : K]$. Also, let v be the unique valuation of L sitting above ∞.

Let $x \in L$ be of valuation nd at v for some $n \geq 1$. An easy computation shows that for all $m \in \{1, \ldots, n\}$, $v(\phi_{t^m}(x)) = dn - dm$. So, in particular $v(\phi_{t^n}(x)) = 0$

and so,

$$v(\phi_{t^{n+1}}(x)) = -d < M_v = \frac{-d}{p-1} \ .$$

This shows, after using Lemma 5.2.5, that $\widehat{\mathrm{h}}_v(\phi_{t^{n+1}}(x)) = \frac{d}{d} = 1$. This in turn implies that

$$\widehat{\mathrm{h}}_v(x) = \frac{1}{p^{n+1}}.$$

But we can take n arbitrarily large, which shows that there is no way to obtain a result similar to Theorem 5.1.3 for generic characteristic Drinfeld modules.

The reader might recognize in this example the analytic uniformization at the place ∞ for ϕ, present in Tamagawa's proof for the rigidity of Drinfeld modules of generic characteristic (see the proof of Theorem 4.13.9 from [13]). The idea is that over any function field, there are points arbitrary close to 0 in the ∞-adic topology, which have arbitrary small positive local height at ∞.

The next theorem shows that Example 5.2.25 is in some sense the only way Theorem 5.1.3 fails for Drinfeld modules of generic characteristic.

Theorem 5.2.26. *Let K be a field of characteristic p. Let $v_0 \in M_K$ be a coherent valuation and let $d(v_0)$ be the degree of v_0.*

Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic. Let $x \in K^{\mathrm{alg}}$ and let v be a place of $K(x)$ that lies over v_0. Assume $\widehat{\mathrm{h}}_v(x) > 0$.

If v_0 does not lie over the place ∞ from $\mathrm{Frac}(A)$, then there exist two positive *constants* C *and* k *depending only on* ϕ *such that* $\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{k-1}}$.

Proof. Let $t \in A$ be a non-constant element and $\phi_t = t\tau^0 + \sum_{i=r_0}^{r} a_i\tau^i$, where a_{r_0} and a_r are nonzero (and $1 \leq r_0 \leq r$).

Again, as we mentioned before, it suffices to prove this theorem under the hypothesis that ϕ_t is monic in τ. Also, if $v \notin S$ Theorem 5.2.26 holds as shown by Lemma 5.2.6.

The analysis of local heights from the present Chapter applies to both finite and generic characteristic until Lemma 5.2.13. So, we still get the conclusion of Lemma 5.2.10. Thus, if $v(x) \leq 0$ then either $\widehat{\mathrm{h}}_v(x) \geq \frac{-d(v)M_{v_0}e(v|v_0)}{q^r}$ or $(v(x), \mathrm{ac}_{\pi_v}(x)) \in P_v \times R_v(v(x))$, with $|P_v|$ and $|R_v(v(x))|$ depending only on q and r (the upper bounds for their cardinalities are slightly larger than in the case of a Drinfeld module of finite characteristic, because the maximal number of segments in the Newton polygon for ϕ_t is r and not $r-1$).

We know from our hypothesis (v does not lie over ∞) that $v(t) \geq 0$ and so,

$$v(tx) \geq v(x). \tag{5.53}$$

Now, if $v(x) \geq N_v$ (with N_v defined as in Lemma 5.2.13), then $v(a_i x^{q^i}) \geq v(x)$, for all $i \geq r_0$ (by the definition of N_v) and using also equation (5.53), we get

$$v(\phi_t(x)) \geq v(x) \geq N_v.$$

Iterating this computation we get that $v(\phi_{t^n}(x)) \geq N_v$, for all $n \geq 1$ and so,

$\widehat{\mathrm{h}}_v(x) = 0$, contradicting the hypothesis of our theorem. This argument is the equivalent of Lemma 5.2.13 for Drinfeld modules of generic characteristic under the hypothesis $v(t) \geq 0$.

Thus it must be that $v(x) < N_v$. Then, Lemma 5.2.14 holds identically. This yields that either $(v(x), \mathrm{ac}_{\pi_v}(x)) \in P_v \times R_v(v(x))$ or $v(\phi_t(x)) < v(x)$.

From this point on, the proof continues just as for Theorem 5.1.3. We form just as before the sets $P_v(n)$ and their union will be again denoted by P. We conclude once again as in (5.43) that *either*

$$\widehat{\mathrm{h}}_v(x) \geq \frac{-M_{v_0} d(v)}{q^{2r} c^{\frac{r}{r_0}} e(v|v_0)^{\frac{r}{r_0}-1}}$$

with the same $c > 0$ depending only on q, r and ϕ as in the proof of (5.1.3), *or*

$$(v(x), \mathrm{ac}_{\pi_v}(x)) \in P \times R_v(v(x))$$

where $|P|$ is of the order of $\log e(v|v_0)$. We observe that when we use equations (5.31), (5.33), (5.34), (5.35) the index i_0 is still at least $r_0 \geq 1$. This is the case because if $v(x) < N_v$ and $(v(x), \mathrm{ac}_{\pi_v}(x)) \notin P_v \times R_v(v(x))$ then there exists $i_0 \geq 0$ such that

$$v(\phi_t(x)) = v(a_{i_0}) + q^{i_0} v(x) = \min_{i \in \{0\} \cup \{r_0, \ldots, r\}} v(a_i x^{q^i}).$$

But $v(x) < N_v$ means that there exists at least one index $i \in \{r_0, \ldots, r\}$ such that $v(tx) \geq v(x) > v(a_i x^{q^i})$.

Finally, Lemma 5.2.18 finishes the proof of Theorem 5.2.26. $\square$

So, we get the conclusion for Theorem 5.2.26 in the same way as in the proof of (5.1.3). The difference made by v not lying above ∞ is that for $v(x) \geq 0$, $v(\phi_t(x))$ can decrease only if $v(x) < N_v$, i.e. only if there exists $i \geq 1$ such that $v(a_i x^{q^i}) < v(x)$. If v lies over ∞, then $v(tx) < v(x)$ and so, $v(\phi_t(x))$ might decrease just because of the $t\tau^0$ term from ϕ_t. Thus, in that case, as Example 5.2.25 showed, we can start with x having arbitrarily large valuation and we are able to decrease it by applying ϕ_t to it repeatedly, making the valuation of $\phi_{t^n}(x)$ be less than M_v, which would mean that $\widehat{\mathrm{h}}_v(x) > 0$. But in doing this we will need a number n of steps (of applying ϕ_t) that we will not be able to control; so $\widehat{\mathrm{h}}_v(x)$ will be arbitrarily small.

It is easy to see that Remarks 5.2.20 and 5.2.21 are valid also for Theorem 5.2.26 in the hypothesis that v does not sit over the place ∞ of $\mathrm{Frac}(A)$. Also, just as we were able to derive Theorem 5.2.24 from the proof of (5.1.3), we can do the same thing in Theorem 5.2.26 and find a specific value of the constant k that will work in the case that v is not wildly ramified above $v_0 \in M_K$. The result is the following theorem whose proof goes along the same lines as the proof of (5.2.24).

Theorem 5.2.27. *Let K be a field of characteristic p. Let $v_0 \in M_K$ be a coherent valuation and let $d(v_0)$ be the degree of v_0. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic and let $\phi_t = t\tau^0 + \sum_{i=r_0}^{r} a_i\tau^i$, with $a_{r_0} \neq 0$ (of course, $r_0 \geq 1$). Assume v_0 does not lie over the place ∞ of* Frac(A)*. There exists a* *constant* $C > 0$*, depending only on* ϕ *such that for every* $x \in K^{\mathrm{alg}}$ *and every place* $v \in M_{K(x)}$ *such that* $v|v_0$ *and* v *is not wildly ramified above* v_0*, if* $\widehat{\mathrm{h}}_v(x) > 0$ *then* $\widehat{\mathrm{h}}_v(x) \geq \frac{Cd(v)}{e(v|v_0)^{\frac{r}{r_0}-1}}$.

We can also construct an example similar to (5.2.22) which shows that constant $k = \frac{r}{r_0}$ in the above theorem is optimal. Indeed, if we take a Drinfeld module ϕ defined on $\mathbb{F}_q[t]$ by

$$\phi_t = t\tau^0 + t^{1-q^{r_0}}\tau^{r_0} + \tau^r$$

and x as in example (5.2.22) then a similar computation will show that we cannot hope for an exponent k smaller than $\frac{r}{r_0}$.

The constants C in Theorems 5.2.24, 5.2.26 and 5.2.27 and the constant k in (5.2.26) have the same dependency on q, r and ϕ as explained in the proof of Theorem 5.1.3.

Chapter 6

The global Lehmer Inequality for Drinfeld modules

In this Chapter we will prove Theorem 6.0.29, which is a special case of the Lehmer inequality for Drinfeld modules. We will actually prove a more general result (Theorem 6.0.32) from which we will be able to infer Theorems 6.0.28 and 6.0.29.

Let K be a field of characteristic p and let $\phi : A \to K\{\tau\}$ be a Drinfeld module. We fix a non-constant element $t \in A$ and we let

$$\phi_t = \sum_{i=0}^{r} a_i \tau^i.$$

As explained in Chapter 5, the statement of Conjecture 1.2.2 is not affected if we replace K by a finite extension K' since if we find a constant C' that works for K' in Conjecture 1.2.2, then $C = \frac{C'}{[K':K]}$ will work for K. Also, as explained in Chapter 5, if we conjugate ϕ by $\gamma \in K^{\text{alg}} \setminus \{0\}$, we obtain a new Drinfeld module, which we denote by $\phi^{(\gamma)}$ and these two Drinfeld modules are isomorphic over $K(\gamma)$. As a particular case of Proposition 2 of [22] we get that $\widehat{\mathrm{h}}_{\phi}(x) = \widehat{\mathrm{h}}_{\phi^{(\gamma)}}(\gamma^{-1}x)$.

Then, if Conjecture 1.2.2 is proved for $\phi^{(\gamma)}$, it will also hold for ϕ. So, having these in mind, we replace ϕ by one of its conjugates that has the property that $\phi_t^{(\gamma)}$ is monic, i.e. with the above notations, γ satisfies the equation $\gamma^{q^r-1}a_r = 1$. Because $[K(\gamma) : K] \leq q^r - 1$, working over $K(\gamma)$ instead of K, we may introduce a factor of $\frac{1}{q^r-1}$ at the worst in the constant C in Conjecture 1.2.2, as explained in the previous paragraph. Also, the module structure theorems that we will be proving in the next Chapter will not be affected by replacing ϕ with an isomorphic Drinfeld module or by replacing K with a finite extension. We will use throughout this Chapter the above convention about ϕ_t being monic.

For each finite extension L of K, we let as before S_L be the set of places $v \in M_L$ for which there exists a coefficient a_i of ϕ_t such that $v(a_i) < 0$, i.e. S_L is the set of places of bad reduction for ϕ (see Lemma 5.2.2).

Theorem 6.0.28. *Let K be a finitely generated field of characteristic p. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module and assume that there exists a non-constant $t \in A$ such that ϕ_t is monic. Let F be the algebraic closure of $\mathbb{F}_p$ in K. We let $M_{K/F}$ be the coherent good set of valuations on K, constructed as in Chapter 4. Let $\widehat{\mathrm{h}}$ and*

$\widehat{\mathrm{h}}_v$ *be the global and local heights associated to* ϕ*, constructed with respect to the coherent good set of valuations* $M_{K/F}$*. Let* $x \in K^{\mathrm{alg}}$ *and let* F_x *be the algebraic closure of* $\mathbb{F}_p$ *in* $K(x)$*. We construct the good set of valuations* $M_{K(x)/F_x}$ *which lie above the valuations from* $M_{K/F}$*. Let* S_x *be the set of places* $v \in M_{K(x)/F_x}$ *such that* ϕ *has bad reduction at* v*.*

If x *is not a torsion point for* ϕ*, then there exists* $v \in M_{K(x)/F_x}$ *such that*

$$\widehat{\mathrm{h}}_v(x) > q^{-r\left(2+(r^2+r)|S_x|\right)} d(v)$$

where $d(v)$ *is as always the degree of the valuation* v*.*

Let $\{x_1, \ldots, x_n\}$ be the transcendence basis for K/F associated to the construction of $M_{K/F}$. Let $v_0 \in M_{K/F}$ be the place lying below the place v from the conclusion of Theorem 6.0.28. Then $d(v) = \frac{d(v_0) f(v|v_0)}{[K(x):K]}$. Because $f(v|v_0) \geq 1$, $d(v_0) \geq \frac{1}{[K:F(x_1,\ldots,x_n)]}$ (see (4.9)) and $\widehat{\mathrm{h}}(x) \geq \widehat{\mathrm{h}}_v(x)$, Theorem 6.0.28 has the following corollary.

Theorem 6.0.29. *With the notation from Theorem 6.0.28, if* $x \notin \phi_{\mathrm{tor}}$*, then*

$$\widehat{\mathrm{h}}(x) > \frac{q^{-r\left(2+(r^2+r)|S_x|\right)}}{[K(x) : F(x_1, \ldots, x_n)]}.$$

Remark 6.0.30. Theorem 6.0.29 is a weaker form of Conjecture 1.2.2 because our constant C for which $\widehat{\mathrm{h}}(x) \geq \frac{C}{[K(x):K]}$ for $x \notin \phi_{\mathrm{tor}}$, is not completely independent of $K(x)$. For us,

$$C = \frac{q^{-r\left(2+(r^2+r)|S_x|\right)}}{[K : F(x_1, \ldots, x_n)]}$$

and S_x depends on $K(x)$.

Fix now a finite extension L of K and let U be a good set of valuations on L. Let $S = S_L \cap U$.

For each $v \in U$ we recall the definition (5.3)

$$M_v = \min_{i \in \{0,\ldots,r-1\}} \frac{v(a_i)}{q^r - q^i} \tag{6.1}$$

where by convention: $v(0) = +\infty$. We observe again that $M_v < 0$ if and only if $v \in S$.

Let $v \in S$. We recall the definition (5.4) of P_v as the subset of the negatives of the slopes of the Newton polygon associated to ϕ_t, consisting of those α for which there exist $i \neq j$ in $\{r_0, \ldots, r\}$ such that

$$\alpha = \frac{v(a_i) - v(a_j)}{q^j - q^i} \leq 0, \tag{6.2}$$

and $v(a_i)+q^i\alpha = v(a_j)+q^j\alpha = \min_{r_0 \leq l \leq r} \left(v(a_l) + q^l\alpha\right)$. If ϕ is the Carlitz module in characteristic 2, i.e. $\phi = \psi_2$, where $\psi_2 : \mathbb{F}_2[t] \to K\{\tau\}$ is defined by $\psi_2(x) = tx + x^2$ for every x, then we want the set P_v to contain $\{0\}$, even if 0 is not in the set from (6.2) (see Lemma 5.2.9).

Let

$$N_\phi = \begin{cases} 1 + r = 2, \text{ if } \phi = \psi_2 \\ r, \text{ otherwise.} \end{cases}$$

Clearly, for every ϕ and $v \in S$, $|P_v| \leq N_\phi$. We recall the definition (5.5): for each $\alpha \in P_v$ we let $l \geq 1$ and let $i_0 < i_1 < \cdots < i_l$ be all the indices i for which $a_i \neq 0$, and for $j, k \in \{0, \ldots, l\}$ with $j \neq k$, we have

$$\frac{v(a_{i_j}) - v(a_{i_k})}{q^{i_k} - q^{i_j}} = \alpha. \tag{6.3}$$

We recall the definition of $R_v(\alpha)$ as the set containing all the nonzero solutions of the equation

$$\sum_{j=0}^{l} \mathrm{ac}_{\pi_v}(a_{i_j}) X^{q^{i_j}} = 0, \tag{6.4}$$

where the indices i_j are the ones associated to α as in (6.3). For $\alpha = 0$, we want the set $R_v(\alpha)$ to contain also $\{1\}$ in addition to the numbers from (6.4). If $\alpha = 0$ there might be no indices i_j and i_k satisfying (6.3). In that case, $R_v(0) = \{1\}$. Clearly, for every $\alpha \in P_v$, $|R_v(\alpha)| \leq q^r$. Then Lemma 5.2.9 reads

Lemma 6.0.31. *Assume $v \in S$. If $v(x) \leq 0$ then either $(v(x), ac_{\pi_v}(x)) \in P_v \times R_v(v(x))$ or $\widehat{\mathrm{h}}_{U,v}(x) \geq \frac{-M_v d(v)}{q^r}$. Moreover, by its definition $M_v < -\frac{1}{q^r}$ and so, if the above latter case holds for x, then $\widehat{\mathrm{h}}_{U,v}(x) > \frac{d(v)}{q^{2r}}$.*

We will deduce Theorem 6.0.28 from the following more general result.

Theorem 6.0.32. *Let K be a field extension of $\mathbb{F}_q$ and let $\phi : A \to K\{\tau\}$ be a Drinfeld module. Let L be a finite field extension of K. Let t be a non-constant element of A and assume that $\phi_t = \sum_{i=0}^{r} a_i \tau^i$ is monic. Let U be a good set of* *valuations on L and let $C(U)$ be, as always, the field of constants with respect to U. Let S be the finite set of valuations $v \in U$ such that ϕ has bad reduction at v. Let $x \in L$.*

a) If S is empty, then either $x \in C(U)$ or there exists $v \in U$ such that $\widehat{\mathrm{h}}_{U,v}(x) \geq d(v)$.

b) If S is not empty, then either $x \in \phi_{\mathrm{tor}}$, or there exists $v \in U$ such that $\widehat{\mathrm{h}}_{U,v}(x) > q^{-2r-r^2 N_\phi |S|} d(v) \geq q^{-r\left(2+(r^2+r)|S|\right)} d(v)$. Moreover, if S is not empty and $x \in \phi_{\mathrm{tor}}$, then there exists a polynomial $b(t) \in \mathbb{F}_q[t]$ of degree at most $rN_\phi |S|$ such that $\phi_{b(t)}(x) = 0$.

Proof. a) Assume S is empty.

Then either $v(x) \geq 0$ for all $v \in U$ or there exists $v \in U$ such that $v(x) < 0$. If the latter statement is true, then Lemma 5.2.14 shows that for the valuation $v \in U$ for which $v(x) < 0$, we have

$$\widehat{\mathrm{h}}_{U,v} \geq d(v),$$

because $v \notin S$ (S is empty).

Now, if the former statement is true, i.e. x is integral at all places from U, then by Lemma 4.1.3, $x \in C(U)$.

b) Assume S is not empty.

Let $v \in S$. We apply Lemma 5.2.18 with $N = 0$, $I = P_v$ and $R(\alpha) = R_v(\alpha)$ for every $\alpha \in P_v$. Because $|P_v| \leq N_\phi$ and

$|R_v(\alpha)| \le q^r$ for every $\alpha \in P_v$, we obtain the following result.

Fact 6.0.33. *Let $v \in S$. Let W be an $\mathbb{F}_q$-subspace of L with the property that for all $w \in W$, $(v(w), \mathrm{ac}_{\pi_v}(w)) \in P_v \times R_v(v(w))$ whenever $v(w) \le 0$.*

Then the $\mathbb{F}_q$-codimension of $\{w \in W \mid v(w) > 0\}$ in W is bounded above by rN_ϕ.

We apply Fact 6.0.33 for each $v \in S$ and we deduce the following two results.

Fact 6.0.34. *Let W be an $\mathbb{F}_q$-subspace of L such that $(v(w), \mathrm{ac}_{\pi_v}(w)) \in P_v \times R_v(v(x))$ whenever $v \in S$, $w \in W$ and $v(w) \le 0$. Then the $\mathbb{F}_q$-codimension of*

$$\{w \in W \mid v(w) > 0 \text{ for all } v \in S\}$$

in W is bounded by $rN_\phi|S|$.

Fact 6.0.35. *Let notation be as in Corollary 6.0.34. If moreover, $\dim_{\mathbb{F}_q} W > rN_\phi|S|$, then there exists a nonzero $w \in W$ such that $v(w) > 0$ for all $v \in S$.*

Using the above facts we prove the following claim which is the key for obtaining the result of Theorem 6.0.32.

Claim 6.0.36. Assume $|S| \ge 1$. If W is an $\mathbb{F}_q$-subspace of L and $\dim_{\mathbb{F}_q} W > rN_\phi|S|$, then there exists $w \in W$ and there exists $v \in U$ such that $\widehat{\mathrm{h}}_{U,v}(w) > \frac{d(v)}{q^{2r}}$.

Proof of Claim 6.0.36. If there exists $v \in U \setminus S$ and $w \in W$ such that $v(w) < 0$, then by Lemma 5.2.14,

$$\widehat{\mathrm{h}}_v(w) \geq d(v) > \frac{d(v)}{q^{2r}}.$$

Thus, suppose from now on in the proof of this lemma, that for every $v \in U \setminus S$ and every $w \in W$, $v(w) \geq 0$.

Because $\dim_{\mathbb{F}_q} W > rN_\phi|S|$, Fact 6.0.35 guarantees the existence of a nonzero $w \in W$ for which *either* $v(w) > 0$ for all $v \in S$, *or* there exists $v \in S$ such that

$$v(w) \leq 0 \text{ but } (v(w), \mathrm{ac}_{\pi_v}(w)) \notin P_v \times R_v(v(w)). \tag{6.5}$$

The former case is impossible because we already supposed that $v(w) \geq 0$ for all $v \in U \setminus S$. Because $|S| \geq 1$ there is no nonzero w that has non-negative valuation at all the places from U and positive valuation at at least one place from U. Its existence would contradict the sum formula for the valuations from U.

Thus, the latter case holds, i.e. there exists $v \in S$ satisfying (6.5). But then, Lemma 6.0.31 gives $\widehat{\mathrm{h}}_{U,v}(w) > \frac{d(v)}{q^{2r}}$. ☐

Using Claim 6.0.36 we can finish the proof of part *b*) of Theorem 6.0.32.

Consider $W = \mathrm{Span}_{\mathbb{F}_q}\left(\left\{x, \phi_t(x), \ldots, \phi_{t^{rN_\phi|S|}}(x)\right\}\right)$. If there exists no polynomial $b(t)$ as in the statement of part *b*) of Theorem 6.0.32, then $\dim_{\mathbb{F}_q} W = 1 + rN_\phi|S|$. Applying Claim 6.0.36 to W, we find some $w \in W$ and some $v \in U$ such that

$$\widehat{\mathrm{h}}_{U,v}(w) > \frac{d(v)}{q^{2r}}. \tag{6.6}$$

By the construction of W, then there exists a nonzero polynomial $d(t) \in \mathbb{F}_q[t]$ of degree at most $rN_\phi|S|$ such that

$$w = \phi_{d(t)}(x). \tag{6.7}$$

Using equation (6.6) and (6.7), we obtain

$$\widehat{\mathrm{h}}_{U,v}(x) = \frac{\widehat{\mathrm{h}}_{U,v}(w)}{\deg(\phi_{d(t)})} > \frac{\frac{d(v)}{q^{2r}}}{q^{r \cdot rN_\phi|S|}}\ ,$$

as desired. □

Proof of Theorem 6.0.28. There are two cases.

Case 1. The set S_x is empty.

By Lemma 4.1.3, all the coefficients a_i of ϕ_t are from F_x. Let $\mathbb{F}_{q^l}$ be a finite field containing all these coefficients.

Assume $x \in \mathbb{F}_p^{\text{alg}}$. Let $\mathbb{F}_{q^{ll'}} = \mathbb{F}_{q^l}(x)$. Then for every $n \geq 1$, $\phi_{t^n}(x) \in \mathbb{F}_{q^{ll'}}$. Because $\mathbb{F}_{q^{ll'}}$ is finite, there exist distinct positive integers n and n' such that $\phi_{t^n}(x) = \phi_{t^{n'}}(x)$. Thus $\phi_{t^{n'}-t^n}(x) = 0$; i.e. $x \in \phi_{\text{tor}}$, which is a contradiction with our hypothesis that x is not a torsion point.

Thus, in *Case 1*, $x \notin \mathbb{F}_p^{\text{alg}}$. So, x is not a constant with respect to the valuations from $M_{K(x)/F_x}$. Then, by Theorem 6.0.32 a), there exists $v \in M_{K(x)/F_x}$ such that

$$\widehat{\mathrm{h}}_v(x) \geq d(v) > q^{-2r}d(v).$$

Case 2. The set S_x is not empty.

Because $x \notin \phi_{\mathrm{tor}}$, Theorem 6.0.32 shows that there exists $v \in M_{K(x)/F_x}$ such that

$$\widehat{\mathrm{h}}_v(x) > q^{-2r-r^2 N_\phi |S_x|} d(v) \geq q^{-r\left(2+(r^2+r)|S_x|\right)} d(v).$$

□

Remark 6.0.37. Assume that we have a Drinfeld module $\phi : A \to K\{\tau\}$ and a non-constant element $t \in A$ for which ϕ_t is monic. Suppose we are in *Case 1* of the proof of Theorem 6.0.28. Then that proof shows that for every non-torsion $x \in K^{\mathrm{alg}}$, there exists $v \in M_{K(x)/F_x}$ such that $\widehat{\mathrm{h}}_v(x) \geq \frac{d(v_0)}{[K(x):K]}$, where v_0 is the place of $M_{K/F}$ that sits below v. Because of inequality (4.9), $d(v_0) \geq \frac{1}{[K:F(x_1,\ldots,x_n)]}$, where $\{x_1, \ldots, x_n\}$ is the transcendence basis for K/F with respect to which we constructed the good set of valuations $M_{K/F}$. Thus Conjecture 1.2.2 holds in this case, i.e. when all the coefficients a_i are from $\mathbb{F}_p^{\mathrm{alg}}$, with $C = \frac{1}{[K:F(x_1,\ldots,x_n)]}$.

With the help of Theorem 6.0.28 we can get a characterization of the torsion submodule of a Drinfeld module. Let K be a finitely generated field and let $\phi : A \to K\{\tau\}$ be a Drinfeld module. If none of the non-constant $a \in A$ has the property that ϕ_a is monic, then just pick some non-constant $t \in A$ and conjugate ϕ by $\gamma \in K^{\mathrm{alg}} \setminus \{0\}$ such that $\phi_t^{(\gamma)}$ is monic. Then ϕ and $\phi^{(\gamma)}$ are isomorphic over $K(\gamma)$, which is a finite extension of K of degree at most $\deg(\phi_t) - 1$. So, describing $\phi_{\mathrm{tor}}(K(\gamma))$ is equivalent with describing $\phi_{\mathrm{tor}}^{(\gamma)}(K(\gamma))$. The following result does exactly this. Its proof is immediate after the proof of Theorem 6.0.32.

Corollary 6.0.38. *Let K be a finitely generated field and let $\phi : A \to K\{\tau\}$ be a Drinfeld module. Let t be a non-constant element of A. Let $\phi_t = \sum_{i=0}^{r} a_i\tau^i$ and assume that $a_r = 1$. Let L be a finite extension of K and let E be the algebraic closure of $\mathbb{F}_p$ in L.*

a) If $a_0, \ldots, a_{r-1} \in E$, then $\phi_{\text{tor}}(L) = E$.

b) If not all of the coefficients $a_0, \ldots, a_{r-1}$ are in E, let $S = S_L \cap M_{L/E}$. Let $b(t) \in \mathbb{F}_q[t]$ be the least common multiple of all the polynomials of degree at most $rN_\phi|S|$. Then for all $x \in \phi_{\text{tor}}(L)$, $\phi_{b(t)}(x) = 0$.

Remark 6.0.39. We can bound the size of the torsion of a Drinfeld module ϕ over a fixed field K by specializing ϕ at a place of good reduction. This is the classical method used to bound torsion for abelian varieties. The bound that we would obtain by using this more classical method will be much larger than the one from Corollary 6.0.38 if K contains a large finite field. However, because our bound is obtained through completely different methods, one can use both methods and then choose the better bound provided by either one.

The bound from Corollary 6.0.38 *b*) for the torsion subgroup of $\phi(L)$ is sharp when ϕ is the Carlitz module, as shown by the following example.

Example 6.0.40. For each prime number p let $v_\infty : \mathbb{F}_p(t)^* \to \mathbb{Z}$ be the valuation such that $v(b) = -\deg(b)$ for each $b \in \mathbb{F}_p[t] \setminus \{0\}$. It is the same notation that we used in Chapter 2. Also, for each prime number p, let ψ_p be the Carlitz module in characteristic p, i.e. $\psi_p : \mathbb{F}_p[t] \longrightarrow \mathbb{F}_p(t)\{\tau\}$, given by $(\psi_p)_t = t\tau^0 + \tau$.

If $p = 2$, we let $L = \mathbb{F}_2(t)$. Then with the notation from Corollary 6.0.38, $S = \{v_\infty\}$. Also, $r = 1$, $N_{\psi_2} = 2$ and so, $rN_{\psi_2}|S| = 2$. It is immediate to see that $\psi_2[t] \subset L$ and also $\psi_2[1+t] \subset L$. Thus we need a polynomial $b(t)$ of degree 2, i.e. $b(t) = t^2 + t$, to kill the torsion of $\psi_2(L)$.

If $p > 2$, we let $L = \mathbb{F}_2\left((-t)^{\frac{1}{p-1}}\right)$. Then $\psi_p[t] \subset L$. With the notation from Corollary 6.0.38, $r = 1$ and $N_{\psi_p} = 1$. Also, $S = \{w_\infty\}$, where w_∞ is the unique place of L sitting above v_∞. So, again we see that we need a polynomial $b(t)$ of degree $rN_{\psi_p}|S| = 1$ to kill the torsion of $\psi_p(L)$.

Chapter 7

The Mordell-Weil theorem for Drinfeld modules

In this Chapter we will be using Definitions 1.3.1, 1.3.2 and 1.3.3.

Lemma 7.0.41. *The field of definition of a Drinfeld module is finitely generated.*

Proof. Let $\phi : A \to K\{\tau\}$. Let $t_1, \ldots, t_s$ be generators of A as an $\mathbb{F}_p$-algebra. Let K_0 be the field extension of $\mathbb{F}_q$ generated by all the coefficients of $\phi_{t_1}, \ldots, \phi_{t_s}$. Then K_0 is finitely generated and by construction, K_0 is the field of definition for ϕ. $\square$

Lemma 7.0.42. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module and let E be its field of definition. Let $t \in A$ be a non-constant element and let $\phi_t = \sum_{i=0}^{r} a_i\tau^i$. Let $E_0 = \mathbb{F}_p(a_0, \ldots, a_r)$ and let E_0^{alg} be the algebraic closure of E_0 inside K^{alg}. Then $E_0 \subset E \subset E_0^{\text{alg}}$.*

Proof. Let ψ be the restriction of ϕ to $\mathbb{F}_p[t]$. Clearly, ψ is defined over E_0. For every $a \in A$, ϕ_a is an endomorphism of ψ. Thus for every $a \in A$, by Proposition 4.7.4 of [13], the coefficients of ϕ_a are algebraic over E_0. $\square$

Lemma 7.0.43. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. Assume that there exists a non-constant element $t \in A$ for which ϕ_t is monic. Let E be the field of definition for ϕ. Then the modular transcendence degree of ϕ is* $\operatorname{trdeg}_{\mathbb{F}_p} E$.

Proof. By the definition of modular transcendence degree of ϕ, we have to show that for every $\gamma \in K^{\mathrm{alg}} \setminus \{0\}$, if $E^{(\gamma)}$ is the field of definition for $\phi^{(\gamma)}$, then

$$\operatorname{trdeg}_{\mathbb{F}_p} E^{(\gamma)} \geq \operatorname{trdeg}_{\mathbb{F}_p} E. \tag{7.1}$$

Let $\gamma \in K^{\mathrm{alg}} \setminus \{0\}$. If $\phi_t = \sum_{i=0}^{r} a_i \tau^i$, then $\phi_t^{(\gamma)} = \sum_{i=0}^{r} a_i \gamma^{q^i-1} \tau^i$.

By Lemma 7.0.42, $\operatorname{trdeg}_{\mathbb{F}_p} E = \operatorname{trdeg}_{\mathbb{F}_p} \mathbb{F}_p(a_0, \ldots, a_{r-1})$ and

$$\operatorname{trdeg}_{\mathbb{F}_p} E^{(\gamma)} = \operatorname{trdeg}_{\mathbb{F}_p} \mathbb{F}_p\left(a_0, a_1\gamma^{q-1}, \ldots, a_{r-1}\gamma^{q^{r-1}-1}, \gamma^{q^r-1}\right).$$

So, in order to prove inequality (7.1), it suffices to show that

$$\operatorname{trdeg}_{\mathbb{F}_p} \mathbb{F}_p\left(a_0, a_1\gamma^{q-1}, \ldots, a_{r-1}\gamma^{q^{r-1}-1}, \gamma^{q^r-1}\right) \geq \operatorname{trdeg}_{\mathbb{F}_p} \mathbb{F}_p(a_0, \ldots, a_{r-1}). \tag{7.2}$$

But,

$$\operatorname{trdeg}_{\mathbb{F}_p} \mathbb{F}_p\left(a_0, \ldots, a_{r-1}\gamma^{q^{r-1}-1}, \gamma^{q^r-1}\right) = \operatorname{trdeg}_{\mathbb{F}_p} \mathbb{F}_p\left(a_0, \ldots, a_{r-1}\gamma^{q^{r-1}-1}, \gamma\right). \tag{7.3}$$

On the other hand,

$$\mathbb{F}_p(a_0, \ldots, a_{r-1}) \subset \mathbb{F}_p\left(a_0, a_1\gamma^{q-1}, \ldots, a_{r-1}\gamma^{q^{r-1}-1}, \gamma\right). \tag{7.4}$$

Equations (7.3) and (7.4) yield (7.2). □

Theorem 7.0.44. *Let F be a countable field of characteristic p and let K be a finitely generated field over F. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of positive relative modular transcendence degree over F. Then $\phi(K)$ is a direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$.*

Proof. We first recall the definition of a *tame* module. The module M is tame if every finite rank submodule of M is finitely generated. According to Proposition 10 from [22], in order to prove Theorem 7.0.44, it suffices to show that $\phi(K)$ is a tame module of rank $\aleph_0$.

We first prove the following lemma which will allow us to make certain reductions during the proof of Theorem 7.0.44.

Lemma 7.0.45. *Let K' be a field extension of K. Assume that $\phi(K')$ is a direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$. Then also $\phi(K)$ is a direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$.*

Proof of Lemma 7.0.45. Let K_0 be the field of definition for ϕ. By Lemma 7.0.41, K_0 is finitely generated. Because ϕ has positive modular transcendence degree,

$\operatorname{trdeg}_{\mathbb{F}_p} K_0 \geq 1$. Thus, as proved in [32], $\phi(K_0)$ is a tame module of rank $\aleph_0$. Then we can apply Lemma 2.0.6 to

$$\phi(K_0) \subset \phi(K) \subset \phi(K')$$

and conclude that also $\phi(K)$ is tame of rank $\aleph_0$. □

Let t be a non-constant element of A. Let $\phi_t = \sum_{i=0}^{r} a_i \tau^i$.

Let $\gamma \in K^{\text{alg}}$ satisfy $\gamma^{q^r-1} a_r = 1$. Assume that $\phi^{(\gamma)}(L(\gamma))$ is a direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$. Because $\phi^{(\gamma)}$ is isomorphic to ϕ over $K(\gamma)$, it follows that also $\phi(K(\gamma))$ is a direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$. Using Lemma 7.0.45 for $K' = K(\gamma)$, we obtain that $\phi(K)$ is a direct sum of a finite torsion submodule and a free module of rank $\aleph_0$. Thus, it suffices to prove Theorem 7.0.44 under the hypothesis that ϕ_t is monic.

Also, we may assume that F is algebraically closed in K. If not, replace F by its algebraic closure in K; the field K is not changed by this.

Choose a transcendence basis $\{x_1, \ldots, x_n\}$ of K/F and construct the good set of valuations $M_{K/F}$ as in Chapter 3. Let S_0 be the set of places in $M_{K/F}$ where ϕ has bad reduction. Because we supposed that ϕ_t is monic, Lemma 5.2.2 yields that S_0 is the set of places from $M_{K/F}$ where not all of the coefficients $a_0, \ldots, a_{r-1}$ are integral.

Lemma 7.0.46. *The set S_0 is not empty.*

Proof of Lemma 7.0.46. If S_0 is empty, then by Lemma 4.1.3, $a_i \in F$ for all i. Then by Lemma 7.0.42, we derive that ϕ is defined over $F^{\text{alg}} \cap K = F$, which is a contradiction with our assumption that ϕ has positive relative modular transcendence degree over F. □

Because S_0 is not empty, we use Theorem 6.0.32 b) and conclude that for every non-torsion $x \in K$, there exists $v \in M_{K/F}$ such that

$$\widehat{\mathrm{h}}_{M_{K/F},v}(x) > q^{-r\left(2+(r^2+r)|S_0|\right)} d(v). \tag{7.5}$$

Using inequality (4.9), we conclude that

$$\widehat{\mathrm{h}}_{M_{K/F},v}(x) > \frac{q^{-r\left(2+(r^2+r)|S_0|\right)}}{[L : F(x_1, \ldots, x_n)]} =: c > 0. \tag{7.6}$$

Because $\widehat{\mathrm{h}}_{M_{K/F}}(x) \geq \widehat{\mathrm{h}}_{M_{K/F},v}(x)$ we conclude that for every non-torsion $x \in K$,

$$\widehat{\mathrm{h}}_{M_{K/F}}(x) > c. \tag{7.7}$$

On the other hand, Theorem 6.0.32 b) shows that $\phi_{\text{tor}}(K)$ is bounded. Moreover, if $b(t) \in \mathbb{F}_q[t]$ is the least common multiple of all polynomials in t of degree at most $(r^2 + r)|S_0|$, then for every $x \in \phi_{\text{tor}}(K)$, $\phi_{b(t)}(x) = 0$.

Let $a \in A$ be an element such that $\deg(\phi_a) \geq 4$ (we will need this assumption because we will apply next Lemma 2.0.3). Because of the finiteness of $\phi_{\text{tor}}(K)$ and because of the equation (7.7), the Dedekind domain A, $a \in A$, $\phi(K)$ and $\widehat{\mathrm{h}}_{M_{K/F}}$ satisfy the hypothesis of Lemma 2.0.3 (note that A/aA is finite as shown in [22]). We conclude that $\phi(K)$ is a tame module. Because F is countable and K is finitely generated over F, $\phi(K)$ is countable and so, it has at most countable rank. On the other hand, as shown in the proof of Lemma 7.0.45, $\phi(K)$ has at least countable rank because ϕ has positive modular transcendence degree. Thus $\phi(K)$ has rank $\aleph_0$. An application of part (a) of Corollary 2.0.5 finishes the proof of Theorem 7.0.44. ☐

Theorem 7.0.47. *Let F be a countable, algebraically closed field of characteristic p and let K be a finitely generated extension of F of positive transcendence degree over F. We fix an algebraic closure K^{alg} of K. If $\phi : A \to F\{\tau\}$ is a Drinfeld module, then $\phi(K)$ is the direct sum of $\phi(F)$ and a free submodule of rank $\aleph_0$.*

Proof. Let t be a non-constant element of A. Because ϕ is defined over F and F is algebraically closed, we can find $\gamma \in F$ such that $\phi_t^{(\gamma)}$ is monic. Because ϕ and $\phi^{(\gamma)}$ are isomorphic over F, it suffices to prove Theorem 7.0.47 for $\phi^{(\gamma)}$. Thus we assume from now on that ϕ_t is monic.

We will show next that the module $\phi(K)/\phi(F)$ is tame.

Let $\{x_1, \ldots, x_n\}$ be a transcendence basis for K/F. We construct the good set of valuations $M_{K/F}$ with respect to $\{x_1, \ldots, x_n\}$, as described in Chapter 4. Then we construct the local and global heights associated to ϕ.

Lemma 7.0.48. *For every $x \in F$, $\widehat{\mathrm{h}}_{K/F}(x) = 0$.*

Proof of Lemma 7.0.48. For every $x \in F$ and for every $a \in A$, because ϕ is defined over F, $\phi_a(x) \in F$. Thus for every $v \in M_{K/F}$, $\widehat{\mathrm{h}}_{K/F,v}(x) = 0$. □

We define the following function $\widehat{\mathrm{H}} : \phi(K)/\phi(F) \to \mathbb{R}_{\geq 0}$ by

$$\widehat{\mathrm{H}}\left(x + \phi(F)\right) = \widehat{\mathrm{h}}_{K/F}(x)$$

for every $x \in K$. We will prove in the next lemma that this newly defined function is indeed well-defined.

Lemma 7.0.49. *The function $\widehat{\mathrm{H}}$ is well-defined.*

Proof of Lemma 7.0.49. To show that $\widehat{\mathrm{H}}$ is well-defined, it suffices to show that for every $x, y \in K$, if $x - y = z \in F$, then $\widehat{\mathrm{h}}_{K/F}(x) = \widehat{\mathrm{h}}_{K/F}(y)$.

Using the triangle inequality and using $\widehat{\mathrm{h}}_{K/F}(z) = 0$ (see Lemma 7.0.48), we get

$$\widehat{\mathrm{h}}_{K/F}(x) \leq \widehat{\mathrm{h}}_{K/F}(y) + \widehat{\mathrm{h}}_{K/F}(z) = \widehat{\mathrm{h}}_{K/F}(y). \tag{7.8}$$

Similarly, using this time $\widehat{\mathrm{h}}_{K/F}(-z) = 0$ (also $-z \in F$), we get

$$\widehat{\mathrm{h}}_{K/F}(y) \leq \widehat{\mathrm{h}}_{K/F}(x) + \widehat{\mathrm{h}}_{K/F}(-z) = \widehat{\mathrm{h}}_{K/F}(x). \tag{7.9}$$

Inequalities (7.8) and (7.9) show that $\widehat{\mathrm{h}}_{K/F}(x) = \widehat{\mathrm{h}}_{K/F}(y)$, as desired. □

For each $x \in K$, we denote by $\overline{\mathrm{x}}$ its image in $\phi(K)/\phi(F)$.

Lemma 7.0.50. *The function* $\widehat{\mathrm{H}}$ *satisfies the properties:*

(i) $\widehat{\mathrm{H}}\left(\overline{x+y}\right) \leq \widehat{\mathrm{H}}\left(\overline{\mathrm{x}}\right) + \widehat{\mathrm{H}}\left(\overline{\mathrm{y}}\right)$*, for all* $x, y \in K$*.*

(ii) $\widehat{\mathrm{H}}\left(\phi_a(\overline{\mathrm{x}})\right) = \deg(\phi_a) \cdot \widehat{\mathrm{H}}\left(\overline{\mathrm{x}}\right)$*, for all* $x \in K$ *and all* $a \in A \setminus \{0\}$*.*

(iii) $\widehat{\mathrm{H}}\left(\overline{\mathrm{x}}\right) \geq \frac{1}{[K:F(x_1,\ldots,x_n)]}$*, for all* $x \notin F$*.*

Proof of Lemma 7.0.50. Properties (i) and (ii) follow immediately from the definition of $\widehat{\mathrm{H}}$ and the fact that ϕ is defined over F and $\widehat{\mathrm{h}}_{K/F}$ satisfies the triangle inequality and $\widehat{\mathrm{h}}_{K/F}(\phi_a(x)) = \deg(\phi_a) \cdot \widehat{\mathrm{h}}_{K/F}(x)$, for all $x \in K$ and all $a \in A \setminus \{0\}$.

Using the result of Theorem 6.0.32 part a), we conclude that if $x \notin F$, there exists $v \in M_{K/F}$ such that

$$\widehat{\mathrm{h}}_{K/F,v}(x) \geq d(v). \tag{7.10}$$

Using inequality (4.9) in (7.10), we get $\widehat{\mathrm{h}}_{K/F,v}(x) \geq \frac{1}{[K:F(x_1,\ldots,x_n)]}$.

Because $\widehat{\mathrm{h}}_{K/F}(x) \geq \widehat{\mathrm{h}}_{K/F,v}(x)$, we conclude that

$$\widehat{\mathrm{h}}_{K/F}(x) \geq \frac{1}{[K : F(x_1, \ldots, x_n)]}.$$

□

Now we can finish the proof of Theorem 7.0.47. The rank of $\phi(K)/\phi(F)$ is at most $\aleph_0$ because K is countable (F is countable and K is a finitely generated extension of F). Because $\widehat{\mathrm{H}}$ satisfies the properties (i)-(iii) from Lemma 7.0.50, Lemma 2.0.3 yields that $\phi(K)/\phi(F)$ is tame.

Lemma 7.0.51. *The rank of* $\phi(K)/\phi(F)$ *is* $\aleph_0$*.*

Proof of Lemma 7.0.51. We need to show only that the rank of the above module is at least $\aleph_0$. Assume the rank is finite and we will derive a contradiction.

Let $y_1, \ldots, y_g \in K$ be the generators of $(\phi(K)/\phi(F)) \otimes_A \mathrm{Frac}(A)$ as a $\mathrm{Frac}(A)$-vector space. Let $v \in M_{K/F}$ be a place different from the finitely many places from $M_{K/F}$ where $y_1, \ldots, y_g$ have poles. Let $x \in K$ be an element which has a pole at v. Then for every $a \in A \setminus \{0\}$, $\phi_a(x)$ has a pole at v. On the other hand, for every $a \in A$ and every $i \in \{1, \ldots, g\}$, $\phi_a(y_i)$ is integral at v. Thus the equation

$$\phi_a(x) = z + \sum_{i=1}^{g} \phi_{a_i}(y_i)$$

has no solutions $a, a_1, \ldots, a_g \in A$ and $z \in F$ with $a \neq 0$. This provides a contradiction to our assumption that $y_1, \ldots, y_g$ are generators for $(\phi(K)/\phi(F)) \otimes_A \mathrm{Frac}(A)$ as a $\mathrm{Frac}(A)$-vector space. □

Hence the rank of $\phi(K)/\phi(F)$ is $\aleph_0$. Because $\phi(K)/\phi(F)$ is tame, Corollary 2.0.5 yields that $\phi(K)/\phi(F)$ is a direct sum of its torsion submodule and a free submodule of rank $\aleph_0$. We know that $\phi(K)/\phi(F)$ is torsion-free (if $\phi_a(x) \in F$ for some $a \in A \setminus \{0\}$, then $x \in F$, because $\phi_a \in F\{\tau\}$). Hence $\phi(K)/\phi(F)$ is free of rank $\aleph_0$. We have the exact sequence:

$$0 \to \phi(F) \to \phi(K) \to \phi(K)/\phi(F) \to 0.$$

Because $\phi(K)/\phi(F)$ is free, the above exact sequence splits. Thus, $\phi(K)$ is a direct sum of $\phi(F)$ and a free submodule of rank $\aleph_0$. □

The following result is an immediate corollary of Theorem 7.0.47.

Theorem 7.0.52. *Let K be a finitely generated field of positive transcendence degree over $\mathbb{F}_p$. If $\phi : A \to K\{\tau\}$ is a Drinfeld module defined over a finite subfield of K, then $\phi(\mathbb{F}_p^{\mathrm{alg}}K)$ is a direct sum of an infinite torsion submodule (which is $\mathbb{F}_p^{\mathrm{alg}}$, the entire torsion submodule of ϕ) and a free submodule of rank $\aleph_0$.*

Chapter 8

Minimal groups in the theory of separably closed fields associated to Drinfeld modules

8.1 General properties of minimal groups in the theory of separably closed fields

Everywhere in the remaining sections of this thesis, for two sets A and B, the notation $A \subset B$ means that A is a subset, not necessarily proper, of B.

Let K be a finitely generated field of characteristic $p > 0$. Let τ_0 be the usual Frobenius, i.e. $\tau_0(x) = x^p$, for every x. We let $K\{\tau_0\}$ be the non-commutative ring of all polynomials in τ_0 with coefficients from K, where the addition is the usual one while the multiplication is the composition of functions. If $f, g \in K\{\tau_0\}$, fg will represent the composition of f and g.

Fix an algebraic closure K^{alg} of K. Let K^{sep} be the separable closure of K inside K^{alg}. Let $\mathbb{F}_p^{\text{alg}}$ be the algebraic closure of $\mathbb{F}_p$ inside K^{sep}.

There exists a non-negative integer ν such that $[K : K^p] = [K^{\text{sep}} : K^{\text{sep}^p}] = p^\nu > 1$. The number ν is called the Ersov invariant of K. When K is a finitely generated field, $\nu = \text{trdeg}_{\mathbb{F}_p} K$.

Notation 8.1.1. Let k be a positive integer. We denote by $p^{(k)}$ the set of functions

$$f : \{1, \ldots, k\} \to \{0, \ldots, p-1\}.$$

Definition 8.1.2. A subset $B = \{b_1, \ldots, b_\nu\} \subset K$ is called a p-basis of K, or equivalently, of K^{sep}, if the following set of monomials,

$$\left\{ m_i = \prod_{j=1}^{\nu} b_j^{i(j)} \mid i \in p^{(\nu)} \right\}$$

forms a basis for K/K^p, or equivalently for $K^{\text{sep}}/K^{\text{sep}^p}$.

For the rest of this paper we fix a p-basis B for K. There exists a unique collection of functions $\lambda_i : K^{\text{sep}} \to K^{\text{sep}}$ for $i \in p^{(\nu)}$, such that for every $x \in K^{\text{sep}}$,

$$x = \sum_{i \in p^{(\nu)}} \lambda_i(x)^p m_i.$$

We call these functions λ_i the λ-functions of level 1. For every $k \geq 2$ and for every choice of $i_1, \ldots, i_k \in p^{(\nu)}$,

$$\lambda_{i_1, i_2, \ldots, i_k} = \lambda_{i_1} \circ \lambda_{i_2} \circ \cdots \circ \lambda_{i_k}$$

is called a λ-function of level k.

Definition 8.1.3. We let $\mathrm{SCF}_{\mathrm{p},\nu}$ be the theory of separably closed fields of characteristic p and Ersov invariant ν in the language

$$\mathfrak{L}_{p,\nu} = \{0, 1, +, -, \cdot\} \cup \{b_1, \ldots, b_\nu\} \cup \{\lambda_i \mid i \in p^{(\nu)}\}.$$

From now on we consider a finitely generated field K of Ersov invariant ν and so, K^{sep} is a model of $\mathrm{SCF}_{\mathrm{p},\nu}$. We let L be an $\aleph_1$-saturated elementary extension of K^{sep}. Because L is an elementary extension of K^{sep}, $L \cap K^{\mathrm{alg}} = K^{\mathrm{sep}}$. We are interested in studying infinitely definable subgroups G of $(L, +)$, i.e. G is possibly an infinite intersection of definable subgroups of $(L, +)$. If $k \geq 1$ and G is an infinitely definable subgroup of $(L, +)$, then the *relatively* definable subsets of G^k (the cartesian product of G with itself k times) are the intersections of G^k with definable subsets of $(L, +)^k$. If there is no risk of ambiguity, we will say a definable subset of G^k, instead of relatively definable subset of G^k. The structure *induced* by L on G over a set S of parameters, is the set G together with all the relatively S-definable subsets of the cartesian powers of G. We will consider only the case when the set S of parameters equals K^{sep}. Thus, when we say a definable subset, we will mean a K^{sep}-definable subset. Also, we call the subgroups of $(L, +)$ *additive*. Finally, we observe that because the theory of separably closed fields is a stable theory (see Messmer's article from [19]), a definable subgroup of an infinitely definable group $G \subset L$ is the intersection of G with a definable subgroup of L.

Remark 8.1.4. In all of our arguments we will work with infinitely definable subgroups G of $(L, +)$. To interpret such a group G from a purely model theoretic point of view, we could do the following. We associate to G the (partial) type P with the property that the realizations of P in the model L of separably closed fields is G, i.e. $G = P(L)$. Thus in our results we will loosely interchange the notion of G as a subgroup of $(L, +)$ and G as the set of realizations of a (partial) type in the language of separably closed fields.

Definition 8.1.5. For every infinitely definable subgroup G, the connected component of G, denoted G^0, is the intersection of all definable subgroups of finite index in G.

Definition 8.1.6. The group G is connected if $G = G^0$.

The following result will be used in the proof of Theorem 9.0.19.

Lemma 8.1.7. *The cartesian product of a finite number of connected groups is connected.*

Proof. Using induction, it is enough to prove the product of two connected groups is connected. Therefore, we assume G_1 and G_2 are connected and $H \subset G_1 \times G_2$ is a definable subgroup of finite index. Let π_1 be the projection of $G_1 \times G_2$ on the first component. Because $[G_1 \times G_2 : H]$ is finite, $[G_1 : \pi_1(H)]$ is also finite. Because G_1 is connected and $\pi_1(H)$ is definable, we conclude $\pi_1(H) = G_1$. Let π_2 be the second projection of $G_1 \times G_2$. Then $H_2 := \pi_2(\mathrm{Ker}(\pi_1|_H))$ is a definable subgroup of G_2. Because $[G_1 \times G_2 : H]$ is finite, $[G_2 : H_2]$ is also finite. Because G_2 is connected, we conclude $H_2 = G_2$. Hence $H = G_1 \times G_2$, which concludes the proof of Lemma 8.1.7. □

Definition 8.1.8. Let G be an infinitely definable additive subgroup of L. We denote by $\mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(G)$ the set of K^{sep}-definable endomorphisms f of G.

The endomorphisms $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(G)$ that are both injective and surjective, form the group of K^{sep}-automorphisms of G, denoted $\mathrm{Aut}_{\mathrm{K}^{\mathrm{sep}}}(G)$.

Remark 8.1.9. If G is a connected group, then the graph of f is a connected subgroup of $G \times G$.

From now on, "endomorphism of G" means "element of $\mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(G)$" and "automorphism of G" means "element of $\mathrm{Aut}_{\mathrm{K}^{\mathrm{sep}}}(G)$".

Definition 8.1.10. Let G and H be infinitely definable connected groups. We call the subgroup $\psi \subset G \times H$ a K^{sep}-quasi-morphism from G to H if the following three properties are satisfied

1) ψ is a connected, K^{sep}-definable subgroup of $G \times H$.

2) the first projection $\pi_1(\psi)$ equals G.

3) the set $\{x \in H \mid (0, x) \in \psi\}$ is finite.

The set of all K^{sep}-quasi-morphisms from G to H is denoted by $\mathrm{QsM}_{\mathrm{K^{sep}}}(G, H)$.

When $G = H$, we call ψ a K^{sep}-quasi-endomorphism of G. The set of all K^{sep}-quasi-endomorphisms of G is denoted by $\mathrm{QsE}_{\mathrm{K^{sep}}}(G)$.

For every infinitely definable connected subgroup G, a "quasi-endomorphism of G" will be an element of $\mathrm{QsE}_{\mathrm{K^{sep}}}(G)$.

Let f be an endomorphism of the connected group G. We interpret f as a quasi-endomorphism of G by

$$f = \{(x, f(x)) \mid x \in G\} \in \mathrm{QsE}_{\mathrm{K^{sep}}}(G).$$

Definition 8.1.11. Let G be an infinitely definable connected group. We define the following two operations that will induce a ring structure on $\mathrm{QsE}_{\mathrm{K^{sep}}}(G)$.

1) *Addition.* For every $\psi_1, \psi_2 \in \mathrm{QsE}_{\mathrm{K^{sep}}}(G)$, we let $\psi_1 + \psi_2$ be the connected component of the group

$$\{(x, y) \in G \times G \mid \exists y_1, y_2 \in G \text{ such that } (x, y_1) \in \psi_1 \text{ , } (x, y_2) \in \psi_2 \text{ and } y_1 + y_2 = y\}.$$

2) *Composition.* For every $\psi_1, \psi_2 \in \mathrm{QsE}_{\mathrm{K^{sep}}}(G)$, we let $\psi_1\psi_2$ be the connected component of the group

$$\{(x, y) \in G \times G \mid \text{ there exists } z \in G \text{ such that } (x, z) \in \psi_2 \text{ and } (z, y) \in \psi_1\}.$$

See [2] for the proof that the above defined operations endow $\mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(G)$ with a ring structure.

Definition 8.1.12. Let G be an infinitely definable additive subgroup. Then G is c-minimal if it is infinite and every definable subgroup of G is either finite or has finite index.

Lemma 8.1.13. *If G is a c-minimal connected group, then for all $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(G) \setminus \{0\}$, $f(G) = G$.*

Proof. Because $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(G)$ and G is connected, $f(G)$ is a definable, connected subgroup of G. Thus, since $f \neq 0$, $f(G)$ cannot be finite. Then, because G is c-minimal, $f(G)$ has finite index in G. Because G is connected, we conclude that f is surjective. $\square$

The next result is proved in a larger generality in Chapter 4.4 of [31]. Because for the case we are interested in we can give a simpler proof, we present our argument below.

Proposition 8.1.14. *If G is a c-minimal, connected group, then $\mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(G)$ is a division ring.*

Proof. Let $\psi \in \mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(G) \setminus \{0\}$. Let $\pi_2(\psi)$ be the projection of $\psi \subset G \times G$ on the second component. Then $\pi_2(\psi)$ is a definable subgroup of G. Because ψ

is connected and $\psi \neq 0$, $\pi_2(\psi)$ is not finite. Then, because G is a c-minimal, connected group, $\pi_2(\psi) = G$.

Because $\pi_2(\psi) = G$ and G is c-minimal and $\psi \neq G \times G$, the set

$$\{x \in G \mid (x, 0) \in \psi\} \tag{8.1}$$

is finite. We define $\phi = \{(y, x) \in G \times G \mid (x, y) \in \psi\}$. Because ψ is a connected, K^{sep}-definable subgroup of $G \times G$, then also ϕ is a connected, K^{sep}-definable subgroup of $G \times G$. By construction, $\pi_1(\phi) = \pi_2(\psi) = G$. By construction of ϕ,

$$\{x \in G \mid (0, x) \in \phi\} = \{x \in G \mid (x, 0) \in \psi\}.$$

Using (8.1), we conclude that $\{x \in G \mid (0, x) \in \phi\}$ is finite. Thus condition 3) of Definition 8.1.10 holds and so, $\phi \in \mathrm{QsE}_{\mathrm{K^{sep}}}(G)$. By definition of ϕ, $\psi\phi$ (as defined in Definition 8.1.11) is the identity function on G. Thus $\mathrm{QsE}_{\mathrm{K^{sep}}}(G)$ is a division ring ($1 \neq 0$ because G is infinite). □

Definition 8.1.15. Let $f \in K\{\tau_0\}\tau_0 \setminus \{0\}$. We define $f^\sharp = f^\sharp(L) = \bigcap_{n \geq 1} f^n(L)$.

In [2] (Lemma 4.23) and [23] the following result is proved.

Theorem 8.1.16. *If $f \in K\{\tau_0\}\tau_0 \setminus \{0\}$, then $f^\sharp$ is c-minimal. In particular, $f^\sharp$ is infinite.*

The theory of separably closed fields is stable, as shown in [19]. Because [21] proves that every stable field is connected as an additive group, the following result holds.

Theorem 8.1.17. *The groups* $(K^{\text{sep}}, +)$ *and* $(L, +)$ *are connected.*

Because the image of a connected group through a definable map is also connected, we get the following result.

Corollary 8.1.18. *For every* $f \in K\{\tau_0\}$, $f(K^{\text{sep}})$ *is connected.*

Lemma 8.1.19. *Let* $(H_n)_{n\geq 1}$ *be a countable collection of descending connected definable subgroups of* $(L, +)$*. Then the infinitely definable subgroup* $H = \bigcap_{n\geq 1} H_n$ *is connected.*

Proof. It suffices to show that for every definable additive subgroup G of L, if G intersects H in a subgroup of finite index, then G contains H. So, let G be a definable additive subgroup of L such that $[H : G \cap H]$ is finite.

Assume that there exists $n \geq 1$ such that $[H_n : G \cap H_n]$ is finite. For such n, because H_n is connected (see Corollary 8.1.18), we conclude that $H_n = G \cap H_n$. So, $H_n \subset G$. Then, by the definition of H, we get that $H \subset G$.

Suppose that for all $n \geq 1$, $[H_n : G \cap H_n]$ is infinite. By compactness and the fact that the groups H_n form a descending sequence and the fact that L is $\aleph_1$-saturated, we conclude that also $[H : G \cap H]$ is infinite, which contradicts our assumption. For reader's convenience, we provide the compactness argument.

Let the descending sequence of groups H_i be represented by formulas ϕ_i. Also, let the group G be represented by the formula ψ.

For each positive integer m and for each finite subset of indices $n_1 < \cdots < n_k$ let $F_{m,n_1,\ldots,n_k}(x_1,\ldots,x_m)$ be the formula which says:

$\phi_{n_i}(x_j)$ for every $1 \leq i \leq k$ and for every $1 \leq j \leq m$ (i.e. each x_j realizes each formula ϕ_{n_i}) and for different j and j' between 1 and m, $\neg\psi(x_j - x_{j'})$ (i.e. for different j and j', $x_j - x_{j'} \notin G$). So, the x_j are in all the groups H_{n_i} but they live in different cosets modulo G.

We know that each individual formula $F_{m,n_1,\ldots,n_k}(x_1,\ldots,x_m)$ has a realization in the model L (to see this, we recall the ϕ_{n_i} are descending and so, $F_{m,n_1,\ldots,n_k}$ says that $[H_{n_k} : H_{n_k} \cap G]$ is at least m, because n_k is the largest index among $n_1,\ldots,n_k$).

Then for every finite subset of formulas $F_{m,n_1,\ldots,n_k}$, let M be the largest among the numbers m appearing as an index for the formulas F. We prove there exist $x_1,\ldots,x_M$ realizing simultaneously all of the formulas $F_{m,n_1,\ldots,n_k}$. Indeed, just replace all of the formulas $F_{m,n_1,\ldots,n_k}$ with just one formula $F_{M,l_1,\ldots,l_s}$ where the indices $l_1,\ldots,l_s$ form a set containing all the indices $n_1,\ldots,n_k$ from all the formulas F of the chosen finite subset of formulas. We know that $F_{M,l_1,\ldots,l_s}$ is realizable and so, all of the finitely many formulas F from above are also realizable. Then we can use compactness and $\aleph_1$-saturation to conclude $G \cap \bigcap_{n\geq 1} H_n$ has infinite index in $\bigcap_{n\geq 1} H_n$. $\square$

The following result is an immediate corollary to Lemma 8.1.19.

Lemma 8.1.20. *If $f \in K\{\tau_0\}\tau_0 \setminus \{0\}$, then $f^\sharp$ is connected.*

Proof. Because of Corollary 8.1.18 we can apply Lemma 8.1.19 to the collection of connected groups $f^n(L)$. ☐

Corollary 8.1.21. *Let $f, g \in K\{\tau_0\}\tau_0 \setminus \{0\}$. If $g^\sharp \subset f^\sharp$, then $f^\sharp = g^\sharp$.*

Proof. By Theorem 8.1.16 and our hypothesis, $g^\sharp$ is an infinite subgroup of $f^\sharp$. Thus for every $n \geq 1$, $g^n(L) \cap f^\sharp$ is a definable infinite subgroup of $f^\sharp$. By Theorem 8.1.16 and Lemma 8.1.20, $f^\sharp \subset g^n(L)$. Because this last inclusion holds for all $n \geq 1$, we conclude that $f^\sharp \subset g^\sharp$. Thus $f^\sharp = g^\sharp$. ☐

In [2] (see Proposition 3.1 and the *Remark* after the proof of Lemma 3.8) the following result is proved.

Proposition 8.1.22. *The following statements hold:*

(i) The Frobenius τ_0, the λ-functions of level 1 and the elements of K^{sep} seen as scalar multiplication functions generate $\text{End}_{K^{\text{sep}}}(L, +)$ as a ring (i.e., with respect to the addition and the composition of functions). Each such element of $\text{End}_{K^{\text{sep}}}(L, +)$ will be called an (additive) λ-polynomial. (Because we will only deal with additive λ-polynomials, we will call them simply λ-polynomials.)

(ii) For every $\psi \in \text{End}_{K^{\text{sep}}}(L, +)$, there exists $n \geq 1$ such that for all $g \in K^{\text{sep}}\{\tau_0\}\tau_0^n$, $\psi g \in K^{\text{sep}}\{\tau_0\}$.

(iii) Let G be an infinitely definable subgroup of $(L,+)$. Then each endomorphism $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(G)$ extends to an element of $\mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(L,+)$.

8.2 The ring of quasi-endomorphisms for minimal groups associated to Drinfeld modules of finite characteristic

Let q be a power of p and let τ be the power of the Frobenius for which $\tau(x) = x^q$, for every x. Let K be a finitely generated field extension of $\mathbb{F}_q$ of positive transcendence degree. We let as before $K\{\tau\}$ be the ring of all polynomials in τ with coefficients from K. Let

$$f = \sum_{i=0}^{r} a_i \tau^i \in K\{\tau\},$$

with $a_r \neq 0$. The *order* $\mathrm{ord}_\tau f$ of f is defined as the smallest i such that $a_i \neq 0$. Thus, f is inseparable if and only if $\mathrm{ord}_\tau f > 0$.

As in the previous subsection, let L be an $\aleph_1$-saturated elementary extension of K^{sep}. We recall Definition 1.4.5.

Definition 8.2.1 (Definition 1.4.5). Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic. We define

$$\phi^\sharp = \phi^\sharp(L) = \bigcap_{a \in A \setminus \{0\}} \phi_a(L).$$

Lemma 8.2.2. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic $\mathfrak{p}$. Let $t \in \mathfrak{p} \setminus \{0\}$. Then*

$$\phi^\sharp = \bigcap_{n \geq 1} \phi_{t^n}(L) = (\phi_t)^\sharp.$$

Proof. If $a \notin \mathfrak{p}$, then ϕ_a is a separable polynomial and $\phi_a(L) = L$. Thus

$$\phi^\sharp = \bigcap_{a \in \mathfrak{p} \setminus \{0\}} \phi_a(L). \tag{8.2}$$

Let $a \in \mathfrak{p} \setminus \{0\}$. Because $t \in \mathfrak{p} \setminus \{0\}$, there exist $n, m \geq 1$ and there exist $u, v \in A \setminus \mathfrak{p}$ such that $t^n v = a^m u$. Then ϕ_u and ϕ_v are separable and so,

$$\phi_{a^m}(L) = \phi_{a^m}(\phi_u(L)) = \phi_{a^m u}(L) = \phi_{t^n v}(L) = \phi_{t^n}(\phi_v(L)) = \phi_{t^n}(L). \tag{8.3}$$

So, $\phi_{t^n}(L) \subset \phi_a(L)$. Thus, using (8.2), we conclude that the result of Lemma 8.2.2 holds. □

The following result is an immediate consequence of Lemmas 8.2.2 and 8.1.20 and Theorem 8.1.16.

Corollary 8.2.3. *The group $\phi^\sharp$ is a c-minimal, connected additive group.*

Lemma 8.2.4. *Let ϕ be a Drinfeld module of finite characteristic. Let* $\mathrm{End}_{\mathrm{K^{sep}}}(\phi)$ *be the ring of endomorphisms of ϕ (defined as in [13]). Then each endomorphism* *of ϕ induces an endomorphism of $\phi^\sharp$, and this association defines an injective ring homomorphism, i.e.* $\mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi) \subset \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp) \subset \mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$.

Proof. Let t be a uniformizer of the prime ideal of A which is the characteristic of ϕ. The inclusion $\mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp) \subset \mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$ is clear. Let now $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi)$ and $x \in \phi^\sharp$. We need to show that $f(x) \in \phi^\sharp$. Because $x \in \phi^\sharp$, for all $n \geq 1$, there exists $x_n \in L$ such that $x = \phi_{t^n}(x_n)$. Because $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi)$, $f(x) = f(\phi_{t^n}(x_n)) = \phi_{t^n}(f(x_n)) \in \phi_{t^n}(L)$, for all $n \geq 1$. Thus indeed, $f(x) \in \phi^\sharp$ (see Lemma 8.2.2). Finally, the above defined association is injective because $\phi^\sharp$ is an infinite set and so, there is no nonzero endomorphism of ϕ which restricted to $\phi^\sharp$ is identically equal to 0. ∎

Corollary 8.2.5. *If ϕ is a finite characteristic Drinfeld module, then*

$$\phi^\sharp = \bigcap_{f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)\setminus\{0\}} f(L).$$

Proof. For every nonzero $a \in A$, $\phi_a \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi) \subset \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$. Thus

$$\bigcap_{f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)} f(L) \subset \bigcap_{a \in A\setminus\{0\}} \phi_a(L) = \phi^\sharp.$$

But by Lemma 8.1.13 and Corollary 8.2.3, all the endomorphisms of $\phi^\sharp$ are surjective on $\phi^\sharp$. So, then indeed

$$\phi^\sharp = \bigcap_{f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)} f(L).$$

∎

Using Corollary 8.2.3 and Proposition 8.1.22, we get the following result.

Corollary 8.2.6. *Let $f \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp)$. Then f is a λ-polynomial. In particular, there exists $m \geq 1$ such that for all $h \in K^{\mathrm{sep}}\{\tau\}\tau^m$, $fh \in K^{\mathrm{sep}}\{\tau\}$.*

As before, for every $a \in A \setminus \{0\}$, we let $\phi[a] = \{x \in K^{\mathrm{alg}} \mid \phi_a(x) = 0\}$. Then for $a \in A \setminus \{0\}$, we let $\phi[a^\infty] = \cup_{n \geq 1}\phi[a^n]$. If $\mathfrak{p}$ is any nontrivial prime ideal in A, then we define

$$\phi[\mathfrak{p}'] = \{x \in K^{\mathrm{alg}} \mid \text{ there exists } a \notin \mathfrak{p} \text{ such that } \phi_a(x) = 0\}.$$

We define $\phi^\sharp(K^{\mathrm{sep}}) = \phi^\sharp(L) \cap K^{\mathrm{sep}}$. We claim that this definition for $\phi^\sharp(K^{\mathrm{sep}})$ is equivalent with $\phi^\sharp(K^{\mathrm{sep}}) = \bigcap_{a \in A\setminus\{0\}} \phi_a(K^{\mathrm{sep}})$. Indeed, if $x \in \phi^\sharp(L) \cap K^{\mathrm{sep}}$, then for every $a \in A \setminus \{0\}$, there exists $x_a \in L$ such that $x = \phi_a(x_a)$. Because $\phi_a \in K^{\mathrm{sep}}\{\tau\}$ and $x \in K^{\mathrm{sep}}$, $x_a \in K^{\mathrm{alg}}$. Because $L \cap K^{\mathrm{alg}} = K^{\mathrm{sep}}$, $x_a \in K^{\mathrm{sep}}$. Moreover, a similar proof as in Lemma 8.2.2, shows that $\phi^\sharp(K^{\mathrm{sep}}) = \bigcap_{n \geq 1} \phi_{t^n}(K^{\mathrm{sep}})$, if ϕ_t is inseparable.

We will continue to denote by $\phi^\sharp$ the group $\phi^\sharp(L)$ and by $\phi^\sharp(K^{\mathrm{sep}})$, its subgroup contained in K^{sep}.

Lemma 8.2.7. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic $\mathfrak{p}$. Then $\phi[\mathfrak{p}'] \subset \phi^\sharp(K^{\mathrm{sep}})$.*

Proof. Let $x \in \phi[\mathfrak{p}']$ and let $a \notin \mathfrak{p}$ such that $\phi_a(x) = 0$. Because ϕ_a is separable,

$x \in K^{\text{sep}}$. Let t be an element of $\mathfrak{p}$, coprime with a, i.e. t and a generate the unit ideal in A.

Let $n \geq 1$. Because t and a are coprime, so are t^n and a. Thus there exist $r, s \in A$ such that $t^n r + as = 1$. Applying this last equality to x gives $\phi_{t^n}(\phi_r(x)) = x$, which shows that $x \in \phi_{t^n}(K^{\text{sep}})$. Because n was arbitrary, we conclude $x \in \phi^\sharp(K^{\text{sep}})$. ☐

Theorem 8.2.8. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic $\mathfrak{p}$. Assume there exists a non-constant $t \in A$ such that $\phi[t^\infty] \cap K^{\text{sep}}$ is finite. Then $\phi^\sharp(K^{\text{sep}}) = \phi[\mathfrak{p}']$. Moreover, with the above hypothesis on ϕ_t, we have that for every $\psi \in \mathrm{QsE}_{\mathrm{K}^{\text{sep}}}(\phi^\sharp)$, there exists $n \geq 1$ such that $\psi\phi_{t^n} = \phi_{t^n}\psi$ in $\mathrm{QsE}_{\mathrm{K}^{\text{sep}}}(\phi^\sharp)$.*

Proof. Clearly, $t \in \mathfrak{p} \setminus \{0\}$, because for all $a \in A \setminus \mathfrak{p}$, ϕ_a is separable and so, $\phi[a^\infty] \subset K^{\text{sep}}$. By Lemma 8.2.2, we know that

$$\phi^\sharp = \bigcap_{n \geq 1} \phi_{t^n}(L) \tag{8.4}$$

and $\phi^\sharp(K^{\text{sep}}) = \bigcap_{n\geq 1} \phi_{t^n}(K^{\text{sep}})$.

Because $\phi[t^\infty] \cap K^{\text{sep}}$ is finite, let $N_0 \geq 1$ satisfy

$$\phi[t^\infty] \cap K^{\text{sep}} \subset \phi[t^{N_0}]. \tag{8.5}$$

Thus

$$\phi[t^\infty] \cap \phi^\sharp = \{0\}. \tag{8.6}$$

We will prove Theorem 8.2.8 through a series of lemmas.

Lemma 8.2.9. *Under the hypothesis of Theorem 8.2.8,* $\phi_t \in \mathrm{Aut}_{\mathrm{K^{sep}}}(\phi^\sharp)$*.*

Proof of Lemma 8.2.9. By Lemma 8.2.4, we know that $\phi_t \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp)$. By the definition of $\phi^\sharp$, we know that ϕ_t is a surjective endomorphism of $\phi^\sharp$. By (8.6), we know that ϕ_t is an injective endomorphism of $\phi^\sharp$. $\square$

Lemma 8.2.10. *Assume* $x \in \phi^\sharp(K^{\mathrm{sep}})$*. We can find a sequence* $(x_n)_{n\geq 0} \subset \phi^\sharp(K^{\mathrm{sep}})$ *such that* $x_0 = x$ *and for all* $n \geq 0$*,* $\phi_t(x_{n+1}) = x_n$*.*

Proof of Lemma 8.2.10. Let $x \in \phi^\sharp(K^{\mathrm{sep}})$. Let N be a positive integer. Because $x \in \phi^\sharp(K^{\mathrm{sep}})$, there exists $x_N \in K^{\mathrm{sep}}$ such that $x = \phi_{t^N}(x_N)$. For each $1 \leq n \leq N$ we let $x_{N-n} = \phi_{t^n}(x_N)$. Thus we constructed the sequence $(x_n)_{0\leq n\leq N} \subset K^{\mathrm{sep}}$ such that $x = x_0$ and for every $0 \leq n \leq N-1$, $x_n = \phi_t(x_{n+1})$. We can do repeat this construction for each positive integer N. By compactness, because L is $\aleph_1$-saturated, there exists an infinite coherent sequence $(x_n)_{n\geq 0} \subset L$ such that $x = x_0$ and for every $n \geq 0$, $x_n = \phi_t(x_{n+1})$. Because $x \in K^{\mathrm{sep}}$ and $\phi_t \in K\{\tau\}$, $(x_n)_{n\geq 0} \subset K^{\mathrm{alg}} \cap L = K^{\mathrm{sep}}$ (the intersection of the two fields being taken inside a fixed algebraic closure of L which contains K^{alg}). $\square$

An immediate corollary of the above proof is the following result.

Corollary 8.2.11. *For an arbitrary Drinfeld module* $\psi : A \to K\{\tau\}$ *of positive characteristic and for* $t \in A$ *such that* ψ_t *is inseparable, the set* $\psi[t^\infty](K^{\mathrm{sep}})$ *is finite if and only if* $\psi_t \in \mathrm{Aut}_{\mathrm{K^{sep}}}(\psi^\sharp)$*.*

Proof of Corollary 8.2.11. If $\psi[t^\infty](K^{\text{sep}})$ is finite, then clearly there is no t-power-torsion of ψ in $\psi^\sharp$ and so, ψ_t is injective on $\psi^\sharp$. Because all the endomorphisms of $\psi^\sharp$ are surjective ($\psi^\sharp$ is a c-minimal, connected group), then indeed, $\psi_t \in \text{Aut}_{\text{K}^{\text{sep}}}(\psi^\sharp)$.

If $\psi_t \in \text{Aut}_{\text{K}^{\text{sep}}}(\psi^\sharp)$, we claim there is finite t-power-torsion of ψ in K^{sep}. Assume this is not the case. Then there are arbitrarily long sequences $(x_n)_{0\leq n\leq m} \in \psi[t^\infty](K^{\text{sep}})$ such that

$$x_n = \psi_t(x_{n+1}) \text{ , for all } n \in \{0, \dots, m-1\} \text{ and } x_0 \neq 0.$$

Arguing as in the proof of Lemma 8.2.10, we conclude there exists an infinite coherent sequence $(x_n)_{n\geq 0} \in \psi[t^\infty](K^{\text{sep}})$ such that

$$x_n = \psi_t(x_{n+1}) \text{ , for all } n \geq 0 \text{ and } x_0 \neq 0.$$

Hence $x_0 \in \psi^\sharp \cap \psi[t^\infty]$, which provides a contradiction with our assumption. This concludes the proof of Corollary 8.2.11. □

The result of Lemma 8.2.10 is instrumental in proving that $\phi^\sharp(K^{\text{sep}}) \subset \phi_{\text{tor}}$. Indeed, take $x \in \phi^\sharp(K^{\text{sep}})$ and construct the associated sequence $(x_n)_{n\geq 0}$ as in (8.2.10).

Let $K' = K(x)$. We claim that $x_n \in K'$, for all $n \geq 1$.

Fix $n \geq 1$ and pick any $\sigma \in \text{Gal}(K^{\text{sep}}/K')$. Because $\phi_t \in K\{\tau\} \subset K'\{\tau\}$, for every $m \geq 1$, $\sigma(x_m) = \sigma(\phi_t(x_{m+1})) = \phi_t(\sigma(x_{m+1}))$. So, for every $m \geq 1$,

$x_n - \sigma(x_n) = \phi_{t^m}(x_{n+m} - \sigma(x_{n+m}))$. Thus,

$$x_n - \sigma(x_n) \in \phi^\sharp. \tag{8.7}$$

But $\phi_{t^n}(x_n - \sigma(x_n)) = \phi_{t^n}(x_n) - \phi_{t^n}(\sigma(x_n)) = \phi_{t^n}(x_n) - \sigma(\phi_{t^n}(x_n)) = x - \sigma(x) = 0$, because $x \in K'$. Thus

$$x_n - \sigma(x_n) \in \phi[t^n]. \tag{8.8}$$

As shown by (8.6), there is no t-power torsion of ϕ in $\phi^\sharp$. Equations (8.8) and (8.7) yield

$$x_n - \sigma(x_n) = 0. \tag{8.9}$$

So, $x_n = \sigma(x_n)$, for all $n \geq 1$ and for all $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K')$. Thus, $x_n \in K'$, for all $n \geq 1$ as it was claimed. If $x \notin \phi_{\mathrm{tor}}$, then $x_n \notin \phi_{\mathrm{tor}}$ for all $n \geq 1$. This will give a contradiction to the structure theorem for $\phi(K')$.

In [22] (for fields of transcendence degree 1 over $\mathbb{F}_p$) and in [32] (for fields of arbitrary positive transcendence degree) it is established that a finitely generated field (as K' in our setting) has the following ϕ-module structure: a direct sum of a finite torsion submodule and a free module of rank $\aleph_0$. In particular this means that there cannot be an infinitely t-divisible non-torsion element $x \in L$. So, $x \in \phi_{\mathrm{tor}}$ and we conclude that $\phi^\sharp(K^{\mathrm{sep}}) \subset \phi_{\mathrm{tor}}$.

By Lemma 8.2.7, we know that $\phi[\mathfrak{p}'] \subset \phi^\sharp$. We will prove next that under the hypothesis from Theorem 8.2.8 (see (8.5)), $\phi^\sharp(K^{\mathrm{sep}}) = \phi[\mathfrak{p}']$.

Suppose that there exists $x \in \phi^\sharp(K^{\text{sep}}) \setminus \phi[\mathfrak{p}']$. Because we already proved that $\phi^\sharp(K^{\text{sep}}) \subset \phi_{\text{tor}}$, $x \in \phi_{\text{tor}}$. Then there exists $a \in \mathfrak{p} \setminus \{0\}$ such that $\phi_a(x) = 0$. Because $t \in \mathfrak{p} \setminus \{0\}$, there exist $n, m \geq 1$ and $u, v \in A \setminus \mathfrak{p}$ such that $t^n v = a^m u$. Then

$$\phi_{t^n v}(x) = \phi_{a^m u}(x) = \phi_{a^{m-1}u}(\phi_a(x)) = 0.$$

So, $x \in \phi[t^n v]$. By our assumption, $x \notin \phi[\mathfrak{p}']$ and so, $y := \phi_v(x) \neq 0$. Thus

$$y \in \phi[t^n] \setminus \{0\}. \tag{8.10}$$

By Lemma 8.2.4, because $x \in \phi^\sharp(K^{\text{sep}})$ and $\phi_v \in \text{End}_{\text{K}^{\text{sep}}}(\phi)$,

$$y = \phi_v(x) \in \phi^\sharp(K^{\text{sep}}). \tag{8.11}$$

Equations (8.10) and (8.11) provide a contradiction to (8.6). So, indeed $\phi^\sharp(K^{\text{sep}}) = \phi[\mathfrak{p}']$.

In order to prove the second part of our Theorem 8.2.8 regarding the quasi-endomorphisms of $\phi^\sharp$, we split the proof in two cases.

Case 1. The polynomial ϕ_t is purely inseparable.

Then $\phi_t = \alpha\tau^r$ for some $\alpha \in K$ and some $r \geq 1$. Let $\gamma \in K^{\text{sep}}$ such that $\gamma^{q^r-1}\alpha = 1$.

Let $\phi^{(\gamma)}$ be the Drinfeld module defined by $\phi^{(\gamma)} = \gamma^{-1}\phi\gamma$. We call $\phi^{(\gamma)}$ the conjugate of ϕ by γ. Then $\phi_t^{(\gamma)} = \tau^r$. Moreover, because for all $a \in A$, $\phi^{(\gamma)} = \gamma^{-1}\phi_a\gamma$

and $\gamma \in K^{\text{sep}}$, we conclude that

$$\phi^{(\gamma)^\sharp} = \gamma^{-1}\phi^\sharp \tag{8.12}$$

and

$$\text{QsE}_{\text{K}^{\text{sep}}}(\phi^\sharp) = \gamma\, \text{QsE}_{\text{K}^{\text{sep}}}\left(\phi^{(\gamma)^\sharp}\right)\gamma^{-1}. \tag{8.13}$$

Because $\phi_t^{(\gamma)} = \tau^r$, $\phi^{(\gamma)^\sharp} = \bigcap_{n\geq 1} L^{p^n} := L^{p^\infty}$. By [2] (Proposition 4.10), the ring $\text{QsE}_{\text{K}^{\text{sep}}}\left(L^{p^\infty}\right)$ is the division ring of fractions of the Ore ring $\mathbb{F}_p^{\text{alg}}\{\tau_0, \tau_0^{-1}\}$, where τ_0 is the usual Frobenius (see [13] for constructing the division ring of fractions for an Ore ring). Then clearly, for all $\psi \in \text{QsE}_{\text{K}^{\text{sep}}}\left(\phi^{(\gamma)^\sharp}\right)$, there exists $n \geq 1$ such that

$$\phi_{t^n}^{(\gamma)} = \tau^{rn}$$

commutes with ψ in $\text{QsE}_{\text{K}^{\text{sep}}}(\phi^{(\gamma)^\sharp})$. By (8.13), we conclude that also for every $\psi \in \text{QsE}_{\text{K}^{\text{sep}}}(\phi^\sharp)$, there exists $n \geq 1$ such that $\psi\phi_{t^n} = \phi_{t^n}\psi$.

Case 2. The polynomial ϕ_t is not purely inseparable, i.e. $\phi[t] \neq \{0\}$.

Lemma 8.2.12. *For every $\psi \in \text{QsE}_{\text{K}^{\text{sep}}}(\phi^\sharp)$ there exists $a \in A\backslash\{0\}$ and $n \geq 1$ such that $\phi_a\psi\phi_{t^n} \in \text{End}_{\text{K}^{\text{sep}}}(\phi^\sharp) \cap K^{\text{sep}}\{\tau\}$ (the intersection is taken inside $\text{QsE}_{\text{K}^{\text{sep}}}(L)$).*

Proof. Let $\psi \in \text{QsE}_{\text{K}^{\text{sep}}}(\phi^\sharp)$ and let $S = \{x \in \phi^\sharp | (0, x) \in \psi\}$. Thus, S is a finite, K^{sep}-definable subgroup of $\phi^\sharp$. Because L is an elementary extension of K^{sep}, $S \subset K^{\text{sep}}$. Thus $S \subset \phi^\sharp(K^{\text{sep}}) \subset \phi_{\text{tor}}$. Hence there exists $a \in A \setminus \{0\}$ such that $S \subset \phi[a]$. By Lemma 8.2.4, $\phi_a\psi \in \text{QsE}_{\text{K}^{\text{sep}}}(\phi^\sharp)$ and its cokernel is trivial by our choice for

a. Thus, $\phi_a\psi$ is actually an endomorphism of $\phi^\sharp$. Also, according to Proposition 8.1.22, the endomorphisms of $\phi^\sharp$ are λ-polynomials. Thus, by Corollary 8.2.6, because ϕ_t is inseparable, there exists $n \geq 1$ such that $\phi_a\psi\phi_{t^n} \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp) \cap K^{\mathrm{sep}}\{\tau\}$. □

Proposition 8.2.13. *Let R be a domain, i.e. a unital (not necessarily commutative) ring with no nontrivial zero-divisors.*

a) Let $y \in R$ be nonzero and suppose that $g \in R$ commutes with y and xy for some $x \in R$. Then g also commutes with x.

b) Let $y \in R$ be nonzero and suppose that $g \in R$ commutes with y and yx for some $x \in R$. Then g also commutes with x.

Proof of Proposition 8.2.13. It suffices to prove a), because the proof of b) follows from a) applied to R^{op}.

Thus, for the proof of a), we know that

$$(gx)y = g(xy) = (xy)g = x(yg) = x(gy) = (xg)y. \tag{8.14}$$

Because $y \in R \setminus \{0\}$ and R is a domain, equation (8.14) concludes the proof of Proposition 8.2.13 a). □

We use Proposition 8.2.13 with $R = \mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$ because from Proposition 8.1.14, we know that $\mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$ is a division ring. Then by Lemma 8.2.12 and Proposition 8.2.13, it suffices to prove Theorem 8.2.8 for $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp) \cap K^{\mathrm{sep}}\{\tau\}$.

Let $f \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp) \cap K^{\mathrm{sep}}\{\tau\}$. By Lemma 8.2.9, $\phi_t^{-1} \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp)$ and so, $\phi_t^{-1} f \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp)$. Hence, $\phi_t^{-1} f$ is a λ-polynomial. By Proposition 8.2.6, there exists $m \geq 1$ such that for every polynomial $h \in K\{\tau\}\tau^m$,

$$\phi_t^{-1} h \in K^{\mathrm{sep}}\{\tau\}. \tag{8.15}$$

Because ϕ_t has inseparable degree at least 1 and $f \in K^{\mathrm{sep}}\{\tau\}$, equation (8.15) yields that $g_1 := \phi_t^{-1} f \phi_{t^m} \in K^{\mathrm{sep}}\{\tau\}$. Moreover, by Lemma 8.2.9, $g_1 \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp)$. This means that the equation

$$f\phi_{t^m} = \phi_t g_1, \tag{8.16}$$

which initially was true only on $\phi^\sharp$ is an identity in $K^{\mathrm{sep}}\{\tau\}$. Indeed, $\phi^\sharp$ is infinite (see Lemma 8.2.7) and so, (8.16) holds for infinitely many points of L. Thus, because $f\phi_{t^m}$ and $\phi_t g_1$ are polynomials, (8.16) holds identically in L.

Because in equation (8.16) all the functions are polynomials in τ, we can equate the order of τ in g_1. We obtain

$$\mathrm{ord}_\tau\, g_1 = \mathrm{ord}_\tau\, f + (m-1)\,\mathrm{ord}_\tau\, \phi_t \geq (m-1)\,\mathrm{ord}_\tau\, \phi_t \geq m-1. \tag{8.17}$$

Thus $\mathrm{ord}_\tau(g_1\phi_t) \geq m$ and using (8.15), we get that $\phi_t^{-1} g_1 \phi_t \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp) \cap K^{\mathrm{sep}}\{\tau\}$. So, denote by $g_2 = \phi_t^{-1} g_1 \phi_t$. This means that the identity

$$\phi_t g_2 = g_1 \phi_t, \tag{8.18}$$

which initially was true only on $\phi^\sharp$ is actually true everywhere. It is the same argument as above when we explained that equation (8.16) is an identity of polynomials from $K^{\mathrm{sep}}\{\tau\}$.

We equate the order of τ of the polynomials from (8.18) and conclude that

$$\operatorname{ord}_\tau g_2 = \operatorname{ord}_\tau g_1 \geq m - 1. \tag{8.19}$$

So, then again $\operatorname{ord}_\tau(g_2\phi_t) \geq m$ and we can apply (8.15) and find a polynomial

$$g_3 \in K^{\mathrm{sep}}\{\tau\} \cap \operatorname{End}_{\mathrm{K^{sep}}}(\phi^\sharp) \text{ such that } \phi_t g_3 = g_2\phi_t.$$

Once again $\operatorname{ord}_\tau g_3 = \operatorname{ord}_\tau g_2$ and so the above process can continue and we construct an infinite sequence $(g_n)_{n\geq 1} \in K^{\mathrm{sep}}\{\tau\} \cap \operatorname{End}_{\mathrm{K^{sep}}}(\phi^\sharp)$ such that for every $n \geq 1$,

$$\phi_t g_{n+1} = g_n\phi_t. \tag{8.20}$$

Let $g_0 = f\phi_{t^{m-1}}$. Then, using (8.16), we conclude that equation (8.20) holds also for $n = 0$.

An easy induction will show that for every $k \geq 1$ and for all $n \geq 0$,

$$\phi_{t^k} g_{n+k} = g_n\phi_{t^k}. \tag{8.21}$$

Indeed, case $k = 1$ is equation (8.20). So, we suppose that (8.21) holds for some $k \geq 1$ and for all $n \geq 0$ and we will prove it holds for $k+1$ and all $n \geq 0$. By equations (8.20) and (8.21) we have that

$$\phi_{t^{k+1}} g_{n+k+1} = \phi_t(\phi_{t^k} g_{n+1+k}) = \phi_t g_{n+1}\phi_{t^k} = g_n\phi_t\phi_{t^k} = g_n\phi_{t^{k+1}},$$

which proves the inductive step of our assertion.

Equation (8.21) shows that for every $k \geq 1$, g_{n+k} maps $\phi[t^k]$ into itself, for every $n \geq 0$. Equation (8.20) shows that all the polynomials g_n have the same degree, call it d. Because ϕ_t is not purely inseparable, we may choose $k_0 \geq 1$ such that

$$|\phi[t^{k_0}]| > d. \tag{8.22}$$

Because $\phi[t^{k_0}]$ is a finite set and our sequence of polynomials $(g_n)_{n\geq 0}$ is infinite, it means that there exist $n_2 > n_1 \geq 0$ such that

$$g_{n_1+k_0}|_{\phi[t^{k_0}]} = g_{n_2+k_0}|_{\phi[t^{k_0}]}. \tag{8.23}$$

By another application of the fact that all g_n are polynomials, equations (8.22) and (8.23) yield that

$$g_{n_1+k_0} = g_{n_2+k_0}. \tag{8.24}$$

But then, using (8.21) (with $k = n_2 - n_1$ and $n = n_1 + k_0$) we conclude that

$$\phi_{t^{n_2-n_1}} g_{n_2+k_0} = g_{n_1+k_0} \phi_{t^{n_2-n_1}}. \tag{8.25}$$

If we denote by g the polynomial represented by both $g_{n_2+k_0}$ and $g_{n_1+k_0}$ (according to (8.24)), equation (8.25) shows that g commutes with $\phi_{t^{n_2-n_1}}$. We let $n_0 = n_2 - n_1 \geq 1$ and so,

$$g\phi_{t^{n_0}} = \phi_{t^{n_0}} g. \tag{8.26}$$

The definition of $g = g_{n_1+k_0}$ and equation (8.21) (with $k = n_1 + k_0$ and $n = 0$) give

$$\phi_{t^{n_1+k_0}} g = g_0 \phi_{t^{n_1+k_0}}. \tag{8.27}$$

Equation (8.26) shows that $\phi_{t^{n_0}}$ commutes with $\phi_{t^{n_1+k_0}} g$. Thus, by equation (8.27), $\phi_{t^{n_0}}$ commutes also with $g_0\phi_{t^{n_1+k_0}}$. We apply now Proposition 8.2.13 *a*) to conclude that $\phi_{t^{n_0}}$ commutes with g_0. Because $g_0 = f\phi_{t^{m-1}}$, another application of the above mentioned proposition gives us

$$\phi_{t^{n_0}} f = f \phi_{t^{n_0}}$$

and ends the proof of Theorem 8.2.8. □

Theorem 8.2.14. *Let ϕ be a Drinfeld module of finite characteristic $\mathfrak{p}$. Assume that there exists $f \in \mathrm{Aut}_{\mathrm{K^{sep}}}(\phi^\sharp) \cap K^{\mathrm{sep}}\{\tau\}\tau$. Then $\phi^\sharp(K^{\mathrm{sep}}) \subset \phi_{\mathrm{tor}}$ and for all $\psi \in \mathrm{QsE}_{\mathrm{K^{sep}}}(\phi^\sharp)$, there exists $n \geq 1$ such that $\psi f^n = f^n \psi$ (the identity being seen in $\mathrm{QsE}_{\mathrm{K^{sep}}}(\phi^\sharp)$).*

Proof. Construct another Drinfeld module $\Phi : \mathbb{F}_q[t] \to K^{\mathrm{sep}}\{\tau\}$ by $\Phi_t = f$. By Lemma 8.2.2, $\Phi^\sharp = f^\sharp$. Using Corollary 8.2.5 and $f \in \mathrm{End}_{\mathrm{K^{sep}}}(\phi^\sharp)$, we get that

$$\phi^\sharp \subset \Phi^\sharp. \tag{8.28}$$

Because both $\phi^\sharp$ and $\Phi^\sharp$ are connected, c-minimal groups (see Corollary 8.2.3), applying Corollary 8.1.21, we conclude that they are equal.

Because $\Phi_t \in \mathrm{Aut}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp) = \mathrm{Aut}_{\mathrm{K}^{\mathrm{sep}}}(\Phi^\sharp)$, $\Phi[t^\infty] \cap K^{\mathrm{sep}}$ is finite (or otherwise we would have t-power-torsion of Φ in $\Phi^\sharp$, as shown by Corollary 8.2.11). Hence, we are in the hypothesis of Theorem 8.2.8 with Φ and t. Thus, we conclude that

$$\Phi^\sharp(K^{\mathrm{sep}}) = \Phi[(t)'], \tag{8.29}$$

where by $\Phi[(t)']$ we denoted the prime-to-t-torsion of Φ.

Because for all $a \in A$, $\phi_a \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi) \subset \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp) = \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\Phi^\sharp)$, there exists $n_a \geq 1$ such that $\phi_a f^{n_a} = f^{n_a}\phi_a$, by Theorem 8.2.8. Because A is finitely generated as an $\mathbb{F}_p$-algebra, we can find $n_0 \geq 1$ such that for all $a \in A$, $\phi_a f^{n_0} = f^{n_0}\phi_a$, i.e. $f^{n_0} \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi)$.

Claim Let $c(t) \in \mathbb{F}_q[t] \setminus \{0\}$ and let $m \geq 1$. Then there exists $d(t) \in \mathbb{F}_q[t^m] \setminus \{0\}$ such that $c(t)$ divides $d(t)$.

Proof of Claim. Because $\mathbb{F}_q[t]/(c(t))$ is finite and because $\mathbb{F}_q[t^m]$ is infinite, there exist $d_1(t) \neq d_2(t)$, both polynomials in $\mathbb{F}_q[t^m]$, such that $c(t)$ divides $d(t) = d_1(t) - d_2(t)$. □

Let $x \in \Phi_{\mathrm{tor}}$ and let $c(t) \in \mathbb{F}_q[t] \setminus \{0\}$ such that $\Phi_{c(t)}(x) = 0$. By the above **Claim**, we may assume that $c(t) \in \mathbb{F}_q[t^{n_0}]$. Because $\Phi_{t^{n_0}} = f^{n_0} \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi)$, $\Phi_{c(t)} \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi)$.

Let a be a non-constant element of A. Then for all $y \in \Phi[c(t)]$,

$$\Phi_{c(t)}(\phi_a(y)) = \phi_a(\Phi_{c(t)}(y)) = 0.$$

Thus $\phi_a(y) \in \Phi[c(t)]$ for all $y \in \Phi[c(t)]$. Similarly, ϕ_{a^m} maps $\Phi[c(t)]$ into itself for every $m \geq 1$. Because $\Phi[c(t)]$ is a finite set and $x \in \Phi[c(t)]$, there exist $m_2 > m_1 \geq 1$ such that $\phi_{a^{m_2}}(x) = \phi_{a^{m_1}}(x)$. Thus $x \in \phi[a^{m_2} - a^{m_1}]$ and $a^{m_2} - a^{m_1} \neq 0$ (a is not constant). This shows that $x \in \phi_{\text{tor}}$ and because x was an arbitrary torsion point of Φ, then $\Phi_{\text{tor}} \subset \phi_{\text{tor}}$. Actually, because the above argument can be used reversely by starting with an arbitrary torsion point x of ϕ and concluding that $x \in \Phi_{\text{tor}}$, we have $\phi_{\text{tor}} = \Phi_{\text{tor}}$. In any case, the inclusion $\Phi_{\text{tor}} \subset \phi_{\text{tor}}$ is sufficient to conclude that

$$\phi^{\sharp}(K^{\text{sep}}) = \Phi^{\sharp}(K^{\text{sep}}) \subset \Phi_{\text{tor}} \subset \phi_{\text{tor}}.$$

Also, Theorem 8.2.8 applied to Φ and $f = \Phi_t$ shows that for all

$$\psi \in \mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\Phi^{\sharp}) = \mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^{\sharp}),$$

there exists $n \geq 1$ such that $\psi f^n = f^n \psi$ (in $\mathrm{QsE}_{\mathrm{K}^{\mathrm{sep}}}(\phi^{\sharp})$). □

The following example shows that one possible way of strengthening Theorem 8.2.8 does not hold and also shows how Theorem 8.2.14 applies when we do not have the hypothesis of (8.2.8).

Example 8.2.15. Assume $p > 2$. Let t be an indeterminate and $K = \mathbb{F}_q(t)$. Let $f = t\tau + \tau^3$. Then, for all $\lambda \in \mathbb{F}_{q^2}$,

$$f\lambda = \lambda^q f \tag{8.30}$$

where λ is seen as the operator $\lambda\tau^0$.

Define $\phi : \mathbb{F}_q[t] \to \mathbb{F}_q(t)\{\tau\}$ by $\phi_t = f(\tau^0 + f)$. We claim that

$$\phi[t^\infty] \cap K^{\text{sep}} \text{ is infinite.} \tag{8.31}$$

Because for all $n \geq 1$, $\phi_{t^n} = f^n(\tau^0 + f)^n$, $\operatorname{Ker}((\tau^0 + f)^n) \subset \operatorname{Ker}\phi_{t^n}$. Because $\tau^0 + f$ is a separable polynomial, all the roots of $(\tau^0 + f)^n$ are distinct and separable over K. So, indeed, (8.31) holds.

statement (8.31) shows that the hypothesis of Theorem 8.2.8 fails for ϕ and t. We will prove the conclusion of Theorem 8.2.8 regarding the quasi-endomorphisms of $\phi^\sharp$ fails, i.e. there exists a quasi-endomorphism of $\phi^\sharp$ that does not commute with any power of ϕ_t.

Let $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Applying Lemma 8.2.2, we get that $\phi^\sharp = (\phi_t)^\sharp$. Applying Corollary 8.1.21 to ϕ_t and f^2 we conclude that $\phi^\sharp = (f^2)^\sharp$ (because f^2 is an endomorphism of ϕ and so, by Corollary 8.2.5, $(\phi_t)^\sharp = \phi^\sharp \subset (f^2)^\sharp$). But

$$f^2\lambda = \lambda f^2 \text{ (apply equation (8.30) twice).} \tag{8.32}$$

Thus, with the help of Lemma 8.2.4 applied to the Drinfeld module $\psi : \mathbb{F}_q[t] \to K\{\tau\}$ given by $\psi_t = f^2$, we get that

$$\lambda \in \operatorname{End}_{K^{\text{sep}}}(\psi^\sharp) = \operatorname{End}_{K^{\text{sep}}}\left((f^2)^\sharp\right) = \operatorname{End}_{K^{\text{sep}}}(\phi^\sharp).$$

Suppose that there exists $n \geq 1$ such that $\phi_{t^n}\lambda = \lambda\phi_{t^n}$ on $\phi^\sharp$. Because $\phi^\sharp$ is infinite, $\phi_{t^n}\lambda = \lambda\phi_{t^n}$, as polynomials. Then also $\phi_{t^{2n}}\lambda = \lambda\phi_{t^{2n}}$. But $\phi_{t^{2n}} =$

$f^{2n}(\tau^0 + f)^{2n}$ and using (8.32) and Proposition 8.2.13 applied to the domain $K\{\tau\}$, we get

$$(\tau^0 + f)^{2n}\lambda = \lambda(\tau^0 + f)^{2n}. \tag{8.33}$$

We will prove that (8.33) is impossible. Because of the skew commutation of f and λ as shown in equation (8.30), the only way for equation (8.33) to hold is if in the expansion of $(\tau^0 + f)^{2n}$, all the nonzero terms are even powers of f. Let p^l be the largest power of p that is less or equal to $2n$. Then $\binom{2n}{p^l} \neq 0$ (in $\mathbb{F}_p$) and its corresponding power of f is odd. This shows that indeed, (8.33) cannot hold when $p > 2$.

On the other hand, $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi)$ and the hypothesis of Theorem 8.2.14 is verified for ϕ and f. Indeed, $f \in \mathrm{End}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$ and $\mathrm{Ker}(f) \cap K^{\mathrm{sep}} = \{0\}$; thus $f \in \mathrm{Aut}_{\mathrm{K}^{\mathrm{sep}}}(\phi^\sharp)$. As we can see from equation (8.32), also the conclusion of (8.2.14) regarding the commutation of the quasi-endomorphism λ of ϕ (i.e. the scalar multiplication function associated to λ) with a power of f holds with the power being f^2.

For the case $p = 2$ we can construct a similar example by taking $f = t\tau + \tau^4$ and defining the Drinfeld module $\phi : \mathbb{F}_q[t] \to \mathbb{F}_q(t)\{\tau\}$ by $\phi_t = f(\tau^0 + f)$. In this case, $\lambda \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ will play the role of the endomorphism of $\phi^\sharp$ that commutes with a power of an endomorphism of ϕ, i.e. it commutes with f^3, but it does not commute with any power of ϕ_t.

Chapter 9

The Mordell-Lang Theorem for Drinfeld modules

In this Chapter, by “subvariety” we understand “closed subvariety”.

Let K be a finitely generated field of characteristic p. As in the previous chapter, we let L be an $\aleph_1$-saturated elementary extension of K^{sep} in the theory of separably closed fields.

Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. In Chapter 7 we proved that if there exists a non-constant $t \in A$ such that $\phi_t = \sum_{i=0}^{r} a_i\tau^i$ is monic, then the modular transcendence degree of ϕ is $\operatorname{trdeg}_{\mathbb{F}_p} \mathbb{F}_p(a_0, \dots, a_{r-1})$.

We restate Theorem 1.4.4 here.

Theorem 9.0.16 (Theorem 1.4.4). *Let K be a finitely generated field of char-*

acteristic p. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of finite characteristic and modular transcendence degree at least 1*. Let* Γ *be a finitely generated* ϕ*-submodule of* $\mathbb{G}_a^g(K^{\text{alg}})$ *and* X *be an algebraic subvariety of* $\mathbb{G}_a^g$*. Then* $X(K^{\text{alg}}) \cap \Gamma$ *is a finite union of translates of subgroups of* Γ*.*

Using Theorem 8.2.8, we are able to strengthen the conclusion of (1.4.4) by showing that one could replace *subgroups* by ϕ*-submodules.* Before stating and proving our result, we need to prove a technical lemma regarding groups of U-rank 1. For a definition and basic properties of the U-rank (also called, the Lascar rank) we refer the reader to Delon's article in [4]. We also mention that Lemma 9.0.18 is true in a larger generality; for example it is true if the U-rank is replaced by the Morley rank (for the definition of the Morley rank, see Ziegler's article in [4]) and so, it holds in the context of classical algebraic geometry. We denote by rk the U-rank. For reader's convenience we recall here the properties of the U-rank that we will use in Lemma 9.0.18.

Proposition 9.0.17. *Let* G *be an infinitely definable group for which the* U*-rank is defined.*

1) *The* U*-rank of* G *is* 0 *if and only if* G *is finite.*

2) *If* H *is a definable subgroup of* G*, then* H *has* U*-rank. Moreover,* $\text{rk}(H) \leq \text{rk}(G)$*, with equality if and only if* $[G : H]$ *is finite.*

3) *If* H *is another group for which the* U*-rank is defined and* $f : G \to H$ *is a*

definable map, then both $\mathrm{Im}(f)$ *and* $\mathrm{Ker}(f)$ *have* U*-rank and* $\mathrm{rk}(G) = \mathrm{rk}(\mathrm{Im}(f)) + \mathrm{rk}(\mathrm{Ker}(f))$.

4) *For each* $n \geq 0$*, the cartesian product* G^n *is a group for which the* U*-rank is defined. (By convention, the zeroth cartesian power of* G *is the trivial group.)*

Lemma 9.0.18. *Let* G *be a connected, infinitely definable subgroup of* L *of* U*-rank* 1 *over* K^{sep}*. Let* n *be a non-negative integer and let* H *be a definable subgroup of* G^n *of* U*-rank* d*. There exists a projection* π *of* G^n *to some* d *coordinates of* G^n *such that* $\pi(H) = \pi(G^n) = G^d$ *and the fibers of* $\pi|_H$ *are finite.*

Proof. Our proof is by induction on n. If $n = 0$, then the conclusion of our lemma holds trivially (the projection being the zero map).

Assume Lemma 9.0.18 holds for $n-1$, for some $n \geq 1$ and we prove it holds also for n. Let π_1 be the projection of G^n on the first $(n-1)$ coordinates. By property 3) of Proposition 9.0.17, $\mathrm{Ker}(\pi_1|_H)$ is a subgroup of G of U-rank equal either 0 or 1.

If the former case holds, i.e. $\mathrm{rk}(\mathrm{Ker}(\pi_1|_H)) = 0$, then $\mathrm{Ker}(\pi_1|H)$ is finite, by property 1) of Proposition 9.0.17. Also, $\mathrm{rk}(\pi_1(H)) = d$, by property 3) of Proposition 9.0.17. We can apply the induction hypothesis to $\pi_1(H) \subset G^{n-1}$ and conclude there exists a suitable projection map π_2 such that $\pi_2(\pi_1(H)) = G^d$ and $\mathrm{Ker}(\pi_2|_{\pi_1(H)})$ is finite. Hence the projection map $\pi_2 \circ \pi_1$ satisfies the conclusion of Lemma 9.0.18 with respect to $H \subset G^n$.

If the latter case holds, i.e. $\mathrm{rk}(\mathrm{Ker}(\pi_1|_H)) = 1$, then $\mathrm{Ker}(\pi_1|_H) = G$, because of property 2) of Proposition 9.0.17 and the fact that G is connected. Thus $H = \pi_1(H) \times G$. We apply the induction hypothesis to $\pi_1(H) \subset G^{n-1}$ and conclude there exists a suitable projection map $\pi_2 : G^{n-1} \to G^{d-1}$ such that $\pi_2|_{\pi_1(H)}$ is surjective and $\mathrm{Ker}(\pi_2|_{\pi_1(H)})$ is finite. Considering the projection map $\pi_3 : G^n \to G^{d-1} \times G$ defined as $(\pi_2 \circ \pi_1, \pi_n)$ (where π_n is the projection of G^n on the last coordinate) and using the fact that $H = \pi_1(H) \times G$, we obtain the conclusion of Lemma 9.0.18. □

Theorem 9.0.19. *Let K be a finitely generated field of characteristic p. If X is a K^{alg}-subvariety of $\mathbb{G}_a^g$ and $\phi : A \to K\{\tau\}$ is a Drinfeld module of positive modular transcendence degree for which there exists a non-constant $t \in A$ such that $\phi[t^\infty](K^{\mathrm{sep}})$ is finite, then there exists $n \geq 1$ such that for every finitely generated ϕ-submodule Γ of $\mathbb{G}_a^g(K^{\mathrm{alg}})$, $X(K^{\mathrm{alg}}) \cap \Gamma$ is a finite union of translates of $\mathbb{F}_q[t^n]$-submodules of Γ.*

Proof. First we prove the following

Claim 9.0.20. Let K_1 be a finite extension of K. Then $\phi[t^\infty](K_1^{\mathrm{sep}})$ is finite.

Proof of Claim 9.0.20. Let p^k be the inseparable degree of the finite extension K_1/K. Then $K_1^{\mathrm{sep}} \subset K^{\mathrm{sep}^{1/p^k}}$.

If we assume the set $\phi[t^\infty](K_1^{\mathrm{sep}})$ is infinite then, as shown in the proof of Corollary 8.2.11, there exists an infinite coherent sequence $(x_n)_{n\geq 0} \in \phi[t^\infty](K_1^{\mathrm{sep}})$

such that

$$x_n = \phi_t(x_{n+1}) \text{ , for all } n \geq 0 \text{ and } x_0 \neq 0.$$

Thus we know that for every $n \geq 0$, $x_n = \phi_{t^k}(x_{n+k})$. Because $\phi_{t^k} \in K\{\tau\}\tau^k$ and $x_{n+k} \in K_1^{\text{sep}} \subset K^{\text{sep}^{1/p^k}}$, we conclude that $x_n \in K^{\text{sep}}$, for every $n \geq 0$. This contradicts our hypothesis that $\phi[t^\infty](K^{\text{sep}})$ is finite and concludes the proof of Claim 9.0.20. ☐

Using Claim 9.0.20, it suffices to prove Theorem 9.0.19 under the hypothesis that both X is defined over K and $\Gamma \subset \mathbb{G}_a^g(K)$. Then $X(K^{\text{alg}}) \cap \Gamma = X(K) \cap \Gamma$.

As in Theorem 1.4.4, let H be an irreducible algebraic subgroup of $\mathbb{G}_a^g$ such that for some $\gamma \in \mathbb{G}_a^g(K^{\text{alg}})$,

$$\gamma + \big(H(K^{\text{alg}}) \cap \Gamma\big) \subset X(K^{\text{alg}}) \cap \Gamma.$$

At the expense of replacing K by a finite extension, we may assume H is defined over K (note that replacing K by a finite extension does not change $X(K^{\text{alg}}) \cap \Gamma$ because $\Gamma \subset \mathbb{G}_a^g(K)$).

We may assume that $H(K) \cap \Gamma$ is dense in H (otherwise we replace H by an irreducible component of the Zariski closure of $H(K) \cap \Gamma$ and again replace K by a finite extension so that H is defined over K). From this point on in this proof, the setting is that H is an irreducible algebraic subgroup of $\mathbb{G}_a^g$ defined over K, which appears in the conclusion of Theorem 1.4.4. Also, X is defined over K and

$\Gamma \subset \mathbb{G}_a^g(K)$. In order to prove Theorem 9.0.19, we will prove H is invariant under a power of ϕ_t.

Let L be an $\aleph_1$-saturated elementary extension of K^{sep}. We apply Lemma 9.0.18 to the definable subgroup $H(L) \cap \phi^\sharp(L)^g$ of the infinitely definable group $\phi^\sharp(L)^g$ ($\phi^\sharp(L)$ is connected by Corollary 8.2.3 and $\phi^\sharp(L)$ has U-rank 1 as proved in [23]). We conclude there exists a projection map π satisfying the conclusions of the above mentioned lemma. We identify $\pi(\phi^\sharp(L^g))$ with $\phi^\sharp(L)^d$, where d is the U-rank of $H(L) \cap \phi^\sharp(L)^g$. Thus for every point

$$(x_1, \ldots, x_d) \in \phi^\sharp(L)^d$$

there is one and at most finitely many points

$$(x_{d+1}, \ldots, x_g) \in \phi^\sharp(L)^{g-d}$$

such that

$$(x_1, \ldots, x_g) \in H(L) \cap \phi^\sharp(L)^g.$$

Hence, we may identify π with the corresponding quasi-morphism between $\phi^\sharp(L)^d$ and $\phi^\sharp(L)^{g-d}$ (the above defined correspondence is additive because H is a group and $\phi^\sharp(L)^d$ and $\phi^\sharp(L)^{g-d}$ are connected, according to Lemma 8.1.7). More exactly, the connected component of $H(L) \cap \phi^\sharp(L)^g$ is the graph of this quasi-morphism between $\phi^\sharp(L)^d$ and $\phi^\sharp(L)^{g-d}$. By *Lemme* 3.5.3 of [3],

$$\mathrm{QsM}_{\mathrm{K^{sep}}}\left(\phi^\sharp(L)^d, \phi^\sharp(L)^{g-d}\right) \xrightarrow{\sim} M_{g-d,d}\left(\mathrm{QsE}_{\mathrm{K^{sep}}}(\phi^\sharp(L))\right),$$

where by $M_{g-d,d}\left(\mathrm{QsE}_{\mathrm{K^{sep}}}(\phi^\sharp(L))\right)$ we denote the ring of $(g-d)\times d$ matrices over the ring $\mathrm{QsE}_{\mathrm{K^{sep}}}(\phi^\sharp(L))$. The image of π in $\mathrm{QsM}_{\mathrm{K^{sep}}}\left(\phi^\sharp(L)^d, \phi^\sharp(L)^{g-d}\right)$ commutes with a power of ϕ_t (by Theorem 8.2.8). Let $\phi_{t^{n_0}}$ be this power for some $n_0 \geq 1$.

For each $\overline{\mathrm{x}} = (x_1, \dots, x_d) \in \phi^\sharp(L)^d$, let

$$H_{\overline{\mathrm{x}}} = \{(y_1, \dots, y_{g-d}) \in \phi^\sharp(L)^{g-d} \mid (x_1, \dots, x_d, y_1, \dots, y_{g-d}) \in \left(H(L) \cap \phi^\sharp(L)^g\right)^0\}.$$

Because π commutes with $\phi_{t^{n_0}}$, for each $\overline{\mathrm{x}} \in \phi^\sharp(L)^d$, $\phi_{t^{n_0}} H_{\overline{\mathrm{x}}} \subset H_{\phi_{t^{n_0}}(\overline{\mathrm{x}})}$. Thus

$$\phi_{t^{n_0}}\left(H(L) \cap \phi^\sharp(L)^g\right)^0 \subset \left(H(L) \cap \phi^\sharp(L)^g\right)^0.$$

Because the connected component of $H(L) \cap \phi^\sharp(L)^g$ is invariant under $\phi_{t^{n_0}}$, the entire group $H(L) \cap \phi^\sharp(L)^g$ is invariant under some power $\phi_{t^{n_1}}$ of $\phi_{t^{n_0}}$. Because L is $\aleph_1$-saturated, by compactness we conclude there exists $m \geq 1$ such that

$$\phi_{t^{n_1}}\left(H(L) \cap \phi_{t^m}(L)^g\right) \subset H(L). \tag{9.1}$$

We know that $H(L) \cap \Gamma$ is Zariski dense in H. Thus, because $\Gamma/\phi_{t^m}(\Gamma)$ is finite, there exists $\alpha \in \Gamma$ such that $H(L) \cap (\alpha + \phi_{t^m}(L)^g)$ is Zariski dense in H. But

$$H(L) \cap (\alpha + \phi_{t^m}(L)^g) = \beta + (H(L) \cap \phi_{t^m}(L)^g)$$

for any $\beta \in (\alpha + \phi_{t^m}(L)^g) \cap H(L)$. Because $H(L) \cap (\alpha + \phi_{t^m}(L)^g)$ is Zariski dense in H, we conclude that $H(L) \cap \phi_{t^m}(L)^g$ is Zariski dense in H. Thus the set $H(L) \cap \phi_{t^m}(L)^g$ is Zariski dense in H and it is mapped by $\phi_{t^{n_1}}$ inside $H(L)$. Hence H is invariant under $\phi_{t^{n_1}}$, as desired. $\square$

Remark 9.0.21. The result of Theorem 9.0.19 is sharp in the sense that its conclusion can fail for $n = 1$. For example, let the Drinfeld module $\phi : \mathbb{F}_q[t] \to \mathbb{F}_q(t)\{\tau\}$ be defined by $\phi_t = \tau + t\tau^3$ and $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Let $X \subset \mathbb{G}_a^2$ be the curve $y = \lambda x$ and let Γ be the cyclic ϕ-submodule of $\mathbb{G}_a^2(\mathbb{F}_{q^2}(t))$ generated by $(1, \lambda)$. As shown in Example 8.2.15, $\phi_{t^2}\lambda = \lambda\phi_{t^2}$. Thus for every $n \geq 1$, $(\phi_{t^{2n}}(1), \phi_{t^{2n}}(\lambda)) \in X(\mathbb{F}_{q^2}(t))$. So, $X(\mathbb{F}_q(t)^{\mathrm{alg}}) \cap \Gamma$ is Zariski dense in X. But X is not invariant under ϕ_t; X is invariant under ϕ_{t^2}. Hence in this example (i.e. for this particular X and ϕ), Theorem 9.0.19 holds with $n = 2$.

Remark 9.0.22. If we drop the hypothesis on ϕ_t from Theorem 9.0.19 (i.e. allow $\phi[t^\infty](K^{\mathrm{sep}})$ be infinite) we may lose the conclusion, as it is shown by the following example.

Let $p > 2$ and let ϕ, λ, X and Γ be as in Remark 9.0.21. Let $u = t + t^2$. As shown in Example 8.2.15, $\phi[u^\infty] \cap \mathbb{F}_p(t)^{\mathrm{sep}}$ is infinite and X is not invariant under any power of ϕ_u. But, as shown in Remark 9.0.21, $X(\mathbb{F}_p(t)^{\mathrm{alg}}) \cap \Gamma$ is infinite.

The above two remarks 9.0.21 and 9.0.22 show that the result of Theorem 9.0.19 is the most we can hope towards Statement 1.4.3 for Drinfeld modules of finite characteristic.

Theorem 9.0.23. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic and of relative modular transcendence degree at least* 1 *over* $\mathrm{Frac}(A)$. *Let $g \geq 0$ and X be a K^{alg}-subvariety of $\mathbb{G}_a^g$. Assume that X does not contain a translate of* *a nontrivial connected algebraic subgroup of* $\mathbb{G}_a^g$*. Then for every finitely generated* ϕ*-submodule* Γ *of* $\mathbb{G}_a^g(K^{\text{alg}})$*, we have that* $X(K^{\text{alg}}) \cap \Gamma$ *is finite.*

Proof. First we replace K by a finitely generated field L, which satisfies the following conditions:

1) ϕ is defined over L;

2) $\Gamma \subset \mathbb{G}_a^g(L)$;

3) X is defined over L.

If we prove Theorem 9.0.23 for L, then the result follows automatically for K. Hence, from now on, we assume that K has the properties $1) - 3)$.

Let $F = \text{Frac}(A)$ and we let F^{alg} be the algebraic closure of F inside K^{alg}. For any two subextensions of K^{alg}, their compositum is taken inside K^{alg}. We may replace K by any finite extension and prove the result for the larger field and then the result will also hold for K. Also, during this proof we will replace F by a finite extension contained in K.

In the beginning we will prove several reduction steps.

Step 1. It suffices to prove Theorem 9.0.23 for Γ of the form Γ_0^g where Γ_0 is a finitely generated ϕ-submodule of $\mathbb{G}_a(K)$. Indeed, if we let Γ_0 be the finitely generated ϕ-submodule of K generated by all the g coordinate projections of Γ then $\Gamma \subset \Gamma_0^g$. So, we suppose that Γ has the form Γ_0^g. To simplify the notation we work with a finitely generated ϕ-submodule Γ of $\mathbb{G}_a(K)$ and prove that $X(K) \cap \Gamma^g$

is finite.

Step 2. Let t be a non-constant element of A. Let $\gamma \in K^{\mathrm{alg}}$ such that for the Drinfeld module $\phi^{(\gamma)} = \gamma^{-1}\phi\gamma$, $\phi^{(\gamma)}_t$ is monic. We let $\gamma^{-1}X$ be the variety whose vanishing ideal is composed of functions of the form $f \circ \gamma$, where f is in the vanishing ideal of X and γ is interpreted as the multiplication-by-γ-map on each component of $\mathbb{G}_a^g$. The conclusion of Theorem 9.0.23 is equivalent with showing that

$$(\gamma^{-1}X)(K^{\mathrm{alg}}) \cap (\gamma^{-1}\Gamma)^g \text{ is finite.}$$

The variety $\gamma^{-1}X$ has the same property as X: it does not contain a translate of a non-trivial connected algebraic subgroup of $\mathbb{G}_a^g$. The group $\gamma^{-1}\Gamma$ is a finitely generated $\phi^{(\gamma)}$-submodule. So, it suffices to prove Theorem 9.0.23 under the extra hypothesis that ϕ_t is monic. From now on, let

$$\phi_t = \tau^r + a_{r-1}\tau^{r-1} + \cdots + a_0\tau^0.$$

Step 3. Let W be a variety defined over F whose function field is K. At the expense of replacing K by a finite extension and replacing F by a finite extension contained in K, we may assume that W is a projective, smooth, geometrically irreducible F-variety (see Remark 4.2 in [14]). We let C be a smooth projective curve defined over a finite field, whose function field is F. We spread out W over an open, dense subset $C_0 \subset C$ and obtain a projective, smooth C_0-variety $V_0 \subset \mathbb{P}^n_{C_0}$ (for some n) (we can always do this because there are finitely many polynomials defining the variety W and so, there are finitely many places of C that lie below poles of the coefficients of these polynomials). We let V be the projective closure of V_0 in $\mathbb{P}^n_C$. We let $\pi : V \to C$ be the natural morphism. The generic fiber of π is smooth and geometrically irreducible, because this is how we chose W. Finally, we replace V by its normalization. By doing this last step, the generic fiber of π remains smooth and geometrically irreducible because V_0 is isomorphic to its preimage in the normalization.

The irreducible divisors $\mathfrak{P}$ of V are of two types:

(i) *vertical*, which means that $\pi(\mathfrak{P}) = \mathfrak{p}$ is a closed point of C.

(ii) *horizontal*, which means that $\pi|_{\mathfrak{P}} : \mathfrak{P} \to C$ is surjective.

We call a divisor of V *horizontal* if it has at least one irreducible component that is horizontal.

Let S be the set of horizontal divisors of V that are irreducible components of the poles of the coefficients a_i of ϕ_t. According to Lemma 5.2.2, the set S is the set of horizontal irreducible divisors of V that are places of bad reduction for ϕ.

At the expense of replacing F by a finite extension F' and replacing K by $F'K$ and replacing V and W by their respective normalizations in $F'K$, we may assume that for each $\gamma \in S$, the generic fiber of $\gamma \to C$ is geometrically irreducible (we can do this because for each $\gamma \in S$, there exists a finite extension of F such that after the base extension, γ splits into finitely many divisors whose generic fibers are geometrically irreducible). Also, the properties of being smooth and geometrically irreducible (for the generic fiber of π) are unaffected by a base extension. So, from now on we work under the following assumptions for the projective, normal varieties V and C:

$$\text{The generic fiber of the morphism } \pi : V \to C \tag{9.2}$$

$$\text{is smooth and geometrically irreducible.} \tag{9.3}$$

$$\text{For each } \gamma \in S\text{, the generic fiber of } \gamma \text{ is geometrically irreducible.} \tag{9.4}$$

Step 4. We define the *division hull* of Γ, by

$$\overline{\Gamma} = \{\gamma \in K^{\mathrm{alg}} \mid \text{there exists } a \in A \setminus \{0\} \text{ such that } \phi_a(\gamma) \in \Gamma\}.$$

Using the result of Theorem 7.0.44 for F^{alg}, which is countable, and for $F^{\mathrm{alg}}K$, which is finitely generated over F^{alg}, and for ϕ, which has positive relative modular transcendence degree over F^{alg}, we conclude that $\phi(F^{\mathrm{alg}}K)$ is the direct sum of a finite torsion submodule and a free submodule of rank $\aleph_0$. Thus, because $\overline{\Gamma}$ has finite rank, $\overline{\Gamma} \cap F^{\mathrm{alg}}K$ is finitely generated. At the expense of replacing F by a finite extension F' and K by $F'K$ and V and W by their respective normalizations in $F'K$, we may assume that $\overline{\Gamma} \cap F^{\mathrm{alg}}K \subset K$.

Step 5. We may replace Γ by $\overline{\Gamma} \cap K$, which is also a finitely generated ϕ-submodule that contains Γ. Thus we may assume that $\Gamma = \overline{\Gamma} \cap F^{\mathrm{alg}}K$.

From now on, we assume all of the above reductions made.

For each irreducible divisor $\mathfrak{P}$ of V, we let $K_{\mathfrak{P}}$ be the residue field of K at $\mathfrak{P}$. For any element x in the valuation ring $R_{\mathfrak{P}}$ of $\mathfrak{P}$, we let $x_{\mathfrak{P}}$ be the reduction of x at $\mathfrak{P}$. Also, we denote by $r_{\mathfrak{P}}$ the reduction map at $\mathfrak{P}$. If all the elements of Γ are integral at $\mathfrak{P}$, we let

$$\Gamma_{\mathfrak{P}} = \{x_{\mathfrak{P}} \mid x \in \Gamma\}.$$

If ϕ has good reduction at $\mathfrak{P}$, then we denote by $\phi^{\mathfrak{P}}$ the corresponding reduction.

The following two results are standard (see Theorem 2.10 (i) of [30], which proves that for an algebraic variety the property of being geometrically irreducible is a first order definable property).

Lemma 9.0.24. *Because the generic fiber of $\pi : V \to C$ is geometrically irreducible, for all but finitely many closed points $\mathfrak{p} \in C$, $\pi^{-1}(\mathfrak{p})$ is geometrically irreducible.*

Lemma 9.0.25. *Let $\gamma \in S$. Because the generic fiber of $\gamma \to C$ is geometrically irreducible, for all but finitely many closed points $\mathfrak{p} \in C$, $\gamma \cap \pi^{-1}(\mathfrak{p})$ is geometrically irreducible.*

Lemma 9.0.26. *Let T be the set of vertical irreducible divisors $\mathfrak{P}$ of V which satisfy the following properties:*

a) ϕ has good reduction at $\mathfrak{P}$.

b) $\phi^{\mathfrak{P}}$ is a finite characteristic Drinfeld module of positive modular transcen-

dence degree.

c) the projective variety $\mathfrak{P}$ *is smooth and* $\pi^{-1}(\pi(\mathfrak{P}))$ *is geometrically irreducible.*

d) for each $\gamma \in S$, $\gamma_{\mathfrak{P}} := \gamma \cap \beta$ *is geometrically irreducible.*

e) for all $x \in \Gamma$, x *is integral at* $\mathfrak{P}$.

Then the set T *is cofinite in the set of all vertical irreducible divisors of* V.

Proof of Lemma 9.0.26. We will show that each of the conditions $a)$-$e)$ is verified by all but finitely many vertical irreducible divisors of V.

$a)$ There are finitely many irreducible divisors of V that are places of bad reduction for ϕ. So, in particular, there are finitely many irreducible vertical divisors of V that do not satisfy $a)$.

$b)$ By the definition of reduction at $\mathfrak{P}$ (which is a place sitting above a prime divisor of A), $\phi^{\mathfrak{P}}$ is a finite characteristic Drinfeld module.

Because ϕ has positive relative modular transcendence degree over F, there exists $a \in A$ and a coefficient c of ϕ_a such that $c \notin F^{\text{alg}}$. We view c as a dominant rational map from the generic fiber W of V to $\mathbb{P}^1_F$. We spread out c to a rational map $\tilde{c} : V \to \mathbb{P}^1_C$, whose generic fiber is c. Because c is dominant, $\tilde{c}$ is dominant. For all but finitely many closed points $\mathfrak{p} \in C$, the fiber $\tilde{c_{\mathfrak{p}}}$ is not constant. According to the result of Lemma 9.0.24, for all but finitely many $\mathfrak{p}$, $\pi^{-1}(\mathfrak{p}) = \mathfrak{P}$ is geometrically irreducible. For such $\mathfrak{P}$, we identify $\tilde{c_{\mathfrak{p}}}$ with the reduction of c at the place $\mathfrak{P}$, denoted $c_{\mathfrak{P}}$. Thus for all but finitely many irreducible vertical divisors $\mathfrak{P}$, $c_{\mathfrak{P}} \notin \mathbb{F}_p^{\text{alg}}$.

So, for these divisors $\mathfrak{P}$, $\phi^{\mathfrak{P}}$ has positive modular transcendence degree (remember that $\phi_t^{\mathfrak{P}}$ is still monic because ϕ_t is monic).

c) Since V is projective, all the irreducible divisors of V are projective varieties.

Because the generic fiber of π is smooth and geometrically irreducible, for all but finitely many $\mathfrak{p} \in C$, $\pi^{-1}(\mathfrak{p})$ is also smooth and geometrically irreducible.

d) This is proved by Lemma 9.0.25.

e) Because Γ is finitely generated as a ϕ-module and ϕ has good reduction at all but finitely many irreducible divisors, the elements of Γ are integral at all but finitely many irreducible divisors of V. □

Lemma 9.0.27. *The set S is nonempty.*

Proof of Lemma 9.0.27. Assume all poles of all coefficients of ϕ_t are vertical. Because there are infinitely many $\mathfrak{P} \in T$, we can find $\mathfrak{P} \in T$ such that $\mathfrak{P}$ is disjoint from all the poles of the coefficients of ϕ_t (we can achieve this because they are finitely many and they are all vertical). Then the reduction of ϕ at $\mathfrak{P}$ is a Drinfeld module of modular transcendence degree at least 1 (by condition *b*) of Lemma 9.0.26. But on the other hand, because all the poles of the coefficients of ϕ_t are vertical and disjoint from $\mathfrak{P}$, the coefficients of $\phi_t^{\mathfrak{P}}$ are integral on $\mathfrak{P}$. Because $\mathfrak{P}$ is a projective variety, then the coefficients of $\phi_t^{\mathfrak{P}}$ are constant. This is a contradiction with the modular transcendence degree of $\phi^{\mathfrak{P}}$. □

For each $\mathfrak{P} \in T$, we let $S_{\mathfrak{P}}$ be the set of all the irreducible divisors of $\mathfrak{P}$ which are poles of the coefficients of $\phi_t^{\mathfrak{P}}$. As explained in Lemma 5.2.2, the places from $S_{\mathfrak{P}}$ are all the places of bad reduction for $\phi^{\mathfrak{P}}$.

Lemma 9.0.28. *For each $\mathfrak{P} \in T$, $1 \leq |S_{\mathfrak{P}}| \leq |S|$.*

Proof of Lemma 9.0.28. Fix $\mathfrak{P} \in T$. Let c be a coefficient of ϕ_t. We view c as a rational map from V to $\mathbb{P}^1_F$. The divisor of the pole of c is the pullback of $\infty \in \mathbb{P}^1_F$. Thus the poles of $c_{\mathfrak{P}}$ are the intersections of this divisor of poles with the vertical divisor $\mathfrak{P}$ (also remember that $\mathfrak{P}$ is a place of good reduction for ϕ and so, $\mathfrak{P}$ is not part of the pole of c). Using Lemma 9.0.26 d), the divisors of $\mathfrak{P}$ which are irreducible components of the divisor of poles of $c_{\mathfrak{P}}$ are of the form $\gamma_{\mathfrak{P}}$ for $\gamma \in S$. Thus, because S is nonempty (see Lemma 9.0.27), $1 \leq |S_{\mathfrak{P}}| \leq |S|$ (the second inequality might be strict because it is possible for two horizontal divisors from S have the same intersection with the vertical divisor $\mathfrak{P}$). □

Lemma 9.0.29. *For all but finitely many $\mathfrak{P} \in T$, the reduction map $r_{\mathfrak{P}}$ is injective on Γ_{tor}.*

Proof of Lemma 9.0.29. Because Γ_{tor} is finite (Γ is finitely generated), only finitely many $\mathfrak{P}$ from T appear as irreducible components of the divisor of zeros for some torsion element of Γ. □

Lemma 9.0.30. *There exists a non-constant $a \in A$ such that for all $\mathfrak{P} \in T$, $\Gamma_{\mathfrak{P}} \cap \phi^{\mathfrak{P}}[a] = \{0\}$.*

Proof of Lemma 9.0.30. Let $\mathfrak{P} \in T$. We note that $\mathfrak{P}$ is regular in codimension 1 (according to condition c) of Lemma 9.0.26) and so, the valuations associated to its irreducible divisors form a good set of valuations on the finitely generated field $K_{\mathfrak{P}}$ (see Remark 4.2.2). Hence, using Lemma 9.0.28 and using Corollary 6.0.38 we conclude that for all $x \in \phi^{\mathfrak{P}}_{\mathrm{tor}}(K_{\mathfrak{P}})$, there exists a polynomial $b(t) \in \mathbb{F}_q[t]$ of degree at most $(r^2 + r)|S|$ such that $\phi^{\mathfrak{P}}_{b(t)}(x) = 0$. Because $\Gamma_{\mathfrak{P}} \subset K_{\mathfrak{P}}$, Lemma 9.0.30 holds with $a \in \mathbb{F}_q[t]$ being any irreducible polynomial of degree greater than $(r^2 + r)|S|$. □

Lemma 9.0.31. *Let a be a non-constant element of A. For almost all $\mathfrak{P} \in T$, $r_{\mathfrak{P}} : \Gamma/\phi_a(\Gamma) \to \Gamma_{\mathfrak{P}}/\phi^{\mathfrak{P}}_a(\Gamma_{\mathfrak{P}})$ is injective.*

Proof of Lemma 9.0.31. We know that all the divisors $\mathfrak{P} \in T$ have the property that if $\mathfrak{p} = \pi(\mathfrak{P})$, then $\pi^{-1}(\mathfrak{p})$ is geometrically irreducible (this was part of condition c) from Lemma 9.0.26). Thus, specifying $\mathfrak{p}$ determines uniquely $\mathfrak{P}$ and so, just to simplify the notation in this lemma, we will use the convention that if $\mathfrak{P}$ is the only irreducible divisor lying above a closed point $\mathfrak{p} \in C$, then $K_{\mathfrak{p}}$ is the residue field of K at $\mathfrak{P}$ and "reducing $x \in K$ at $\mathfrak{p}$" is "reducing $x \in K$ at $\mathfrak{P}$". Also, we will identify T with the set of closed points $\mathfrak{p} \in C$ lying below the vertical divisors

$\mathfrak{P} \in T$.

Suppose there are infinitely many irreducible divisors $\mathfrak{P}$ for which the map in (9.0.31) is not injective. Because $\Gamma/\phi_a(\Gamma)$ is finite, there exists $x \in \Gamma \setminus \phi_a(\Gamma)$ and there exists an infinite subset U of $T \subset C$ such that for every $\mathfrak{p}$ in this infinite subset, $x_{\mathfrak{p}} \in \phi_a^{\mathfrak{p}}(\Gamma_{\mathfrak{p}})$. For each such $\mathfrak{p}$, let $z(\mathfrak{p}) \in \Gamma_{\mathfrak{p}} \subset K_{\mathfrak{p}}$ be such that

$$x_{\mathfrak{p}} = \phi_a^{\mathfrak{p}}(z(\mathfrak{p})). \tag{9.5}$$

Let L be the finite extension of K generated by all the roots $z_1, \ldots, z_s \in K^{\mathrm{alg}}$ of the equation (in z) $\phi_a(z) = x$. For each $\mathfrak{p} \in U$ choose a place $\mathfrak{p}_1$ of L lying above $\mathfrak{p}$.

Fix now $\mathfrak{p} \in U$. Because $\mathfrak{p} \in T$ (and so, $\mathfrak{p}_1$) is a place of good reduction for ϕ, $z_1, \ldots, z_s$ are integral at $\mathfrak{p}_1$ and their reductions at $\mathfrak{p}_1$, called $z_{1,\mathfrak{p}_1}, \ldots, z_{s,\mathfrak{p}_1}$ are all the roots of the equation (in z) $\phi_a^{\mathfrak{p}}(z) = x_{\mathfrak{p}}$. Using (9.5), we conclude there exists $i \in \{1, \ldots, s\}$ such that

$$z_{i,\mathfrak{p}_1} = z(\mathfrak{p}). \tag{9.6}$$

We apply the above argument for each $\mathfrak{p} \in U$ (and for the corresponding $\mathfrak{p}_1$) and so, conclude that for each $\mathfrak{p} \in U$, there exists some $i \in \{1, \ldots, s\}$ such that (9.6) holds. Because U is infinite, there exists an infinite subset $U_1 \subset U$ and there exists $z \in \{z_1, \ldots, z_s\}$ such that for each $\mathfrak{p} \in U_1$,

$$z_{\mathfrak{p}_1} = z(\mathfrak{p}) \in K_{\mathfrak{p}}, \tag{9.7}$$

because $z(\mathfrak{p}) \in K_{\mathfrak{p}}$. Let $K' = K(z)$. Because $z \in \overline{\Gamma}$ and $\overline{\Gamma} \cap F^{\mathrm{alg}}K = \Gamma$, K' is not contained in $F^{\mathrm{alg}}K$. So, if we let F' be the algebraic closure of F in K', then

$$l := [K' : F'K] > 1. \tag{9.8}$$

Let C' be the normalization of C in F'. Let V' be the normalization of V in $F'K$ and let V_1' be the normalization of V in K'. Let $\pi' : V' \to C'$ and $\pi_1' : V_1' \to C'$ be the induced morphisms. Thus the generic fibers W' and W_1' of π' and π_1', respectively, are geometrically irreducible. Let $f : V_1' \to V'$ be the induced finite morphism.

Because ϕ is a generic characteristic Drinfeld module, ϕ_a is a separable polynomial and so, K'/K is a separable extension. Thus f is ramified for finitely many irreducible divisors of V'. Also, let P be the minimal polynomial for z over $F'K$.

Let U_1' be the set of closed points of C' satisfying the following properties:

1) each $\mathfrak{p}' \in U_1'$ lies above some $\mathfrak{p} \in U_1$,

2) for each $\mathfrak{p}' \in U_1'$, the vertical divisor $\mathfrak{P}_1' := \pi_1'^{-1}(\mathfrak{p}')$ of V_1' is geometrically irreducible,

3) for each $\mathfrak{p}' \in U_1'$, f is not ramified at the divisor $\mathfrak{P}' := \pi'^{-1}(\mathfrak{p}')$ of V' (note that $\mathfrak{P}'$ is geometrically irreducible, once 2) holds),

4) for each $\mathfrak{p}' \in C'$, all the coefficients of P are integral at the corresponding $\mathfrak{P}'$ (and implicitly, at $\mathfrak{P}_1'$). Moreover, $\mathfrak{p}'$ is not an irreducible component of the divisor of zeros of $P'(z)$.

In all that will follow next in our argument, "condition i)" for $i \in \{1, \ldots, 4\}$ is one of the above 4 conditions.

Because U_1 is infinite, condition 1) is satisfied by infinitely many $\mathfrak{p}' \in C'$. Condition 2) is satisfied by all but finitely many $\mathfrak{p}' \in C'$ because the generic fiber of π_1' is geometrically irreducible. Condition 3) is satisfied because f ramifies at finitely many irreducible divisors of V'. The first part of condition 4) is satisfied because there are finitely many divisors of V' (or V_1') which are irreducible components for the divisors of poles of the coefficients of P. The second part of condition 4) is satisfied because $P'(z) \neq 0$ (P is a separable polynomial because it divides ϕ_a, which is a separable polynomial). So, we conclude U_1' is infinite.

Let $\mathfrak{p}' \in U_1'$ and let $\mathfrak{P}'$ and $\mathfrak{P}_1'$ be the corresponding vertical divisors of V' and V_1', respectively. Because $\mathfrak{P}_1'$ is the only place of K' lying above the place $\mathfrak{p}'$ of C' (see condition 2)), (9.7) yields $z_{\mathfrak{P}_1'} \in (F'K)_{\mathfrak{P}'}$. Also by condition 2), $\mathfrak{P}_1'$ is the only place of K' lying above the place $\mathfrak{P}'$ of $F'K$.

Let R be the valuation ring of $F'K$ at $\mathfrak{P}'$ and let R' be the integral closure of R in K'. Because K' is not ramified above $\mathfrak{P}'$, the different of R'/R is the unit ideal in R' (see Theorem 1, page 53, [26]). By condition 4), $P'(z)$ is also a unit in R'. By Corollary 2 (page 56) of [26], $R' = R[z]$. Because P is defined over R (see condition 4)), Lemma 4 (page 18) of [26] yields the relative residue degree $f(\mathfrak{P}_1'|\mathfrak{P}')$ between the place $\mathfrak{P}_1'$ of K' and the place $\mathfrak{P}'$ of $F'K$ is 1. Using condition 3), we conclude that also the ramification index $e(\mathfrak{P}_1'|\mathfrak{P}')$ of $\mathfrak{P}_1'$ over

$\mathfrak{P}'$ is 1. As explained in Remark 4.2.2, the valuations associated to irreducible divisors of a projective variety defined over a field, are defectless and so, because $e(\mathfrak{P}'_1|\mathfrak{P}') = f(\mathfrak{P}'_1|\mathfrak{P}') = 1$ and $\mathfrak{P}'_1$ is the only place of K' lying above the place $\mathfrak{P}'$ of $F'K$, we conclude $[K' : F'K] = 1$. This contradicts (9.8). This contradiction comes from our assumption that there are infinitely many primes $\mathfrak{P}$ for which Lemma 9.0.31 is false. So, for all but finitely many $\mathfrak{P} \in T$, the conclusion of Lemma 9.0.31 holds, as desired. □

Using Lemmas 9.0.29, 9.0.30 and 9.0.31 we prove the following key result.

Lemma 9.0.32. *For all but finitely many $\mathfrak{P} \in T$, the reduction $\Gamma \to \Gamma_{\mathfrak{P}}$ is injective.*

Proof of Lemma 9.0.32. Shrink T so that all of the three lemmas 9.0.29, 9.0.30 and 9.0.31 hold for $\mathfrak{P} \in T$. Also, let a be as in Lemma 9.0.30.

If $x \in \Gamma \cap \mathrm{Ker}(r_{\mathfrak{P}})$, then by Lemma 9.0.31, $x \in \phi_a(\Gamma)$. This means that there exists $x_1 \in \Gamma$ such that $\phi_a(x_1) = x$. Reducing at $\mathfrak{P}$, we get $\phi_a^{\mathfrak{P}}(x_{1_{\mathfrak{P}}}) = 0$ which by Lemma 9.0.30 implies that $x_{1_{\mathfrak{P}}} = 0$. But then applying again 9.0.31, this time to x_1, we conclude $x_1 \in \phi_a(\Gamma)$; i.e. there exists $x_2 \in \Gamma$ such that $x_1 = \phi_a(x_2)$.

So, repeating the above process, an easy induction shows that

$$x \in \bigcap_{n \geq 1} \phi_{a^n}(\Gamma) = \Gamma_{\mathrm{tor}},$$

because Γ is finitely generated. But, by Lemma 9.0.29, Γ_{tor} injects through the reduction at $\mathfrak{P}$. Thus $x = 0$ and so the proof of Lemma 9.0.32 ends. $\square$

Now, the property $\mathcal{P}$: *"X does not contain any translate of a nontrivial connected algebraic subgroup of* $\mathbb{G}_a^g$*"* is a definable property as shown in Lemma 11 (page 203) of [4] (there it is proved that the set of connected algebraic subgroups of an algebraic group G that are maximal under the property that one of their translates lies inside a given algebraic variety $X \subset G$ is definable). This means that property $\mathcal{P}$ is inherited by all but finitely many of the reductions of X. Coupling this result with Lemma 9.0.32, we see that for all but finitely many irreducible vertical divisors $\mathfrak{P}$ of V, the reduction of X, called $X_{\mathfrak{P}}$, is also a variety that satisfies the same hypothesis as X and moreover, Γ injects through such reduction. This means that

$$|X(K) \cap \Gamma^g| \leq |X_{\mathfrak{P}}(K_{\mathfrak{P}}) \cap \Gamma_{\mathfrak{P}}^g|. \tag{9.9}$$

According to condition $b)$ of Lemma 9.0.26, for all $\mathfrak{P} \in T$, $\phi^{\mathfrak{P}}$ satisfies the hypothesis of Theorem 1.4.4. Thus, applying Theorem 1.4.4, $X_{\mathfrak{P}} \cap \Gamma_{\mathfrak{P}}$ is a finite union of translates of cosets of subgroups of $\Gamma_{\mathfrak{P}}$. Suppose that one of these subgroups of $\Gamma_{\mathfrak{P}}$ is infinite. Then $X_{\mathfrak{P}}$ contains the Zariski closure of the corresponding coset, which is a translate of a positive dimension algebraic subgroup of $\mathbb{G}_a^g$. This would contradict the property inherited by $X_{\mathfrak{P}}$ from X. Thus $X_{\mathfrak{P}}(K_{\mathfrak{P}}) \cap \Gamma_{\mathfrak{P}}^g$ is finite. Using (9.9), we conclude that $X(K) \cap \Gamma^g$ is finite. $\square$

Remark 9.0.33. Theorem 9.0.23 is a special case of Statement 1.4.3 because if we assume (1.4.3) and we work with the hypothesis on X from Theorem 9.0.23, then, with the notation from (1.4.3), the intersection of X with any translate of B_i is finite. Otherwise, the Zariski closure of $X \cap (\gamma_i + B_i)$ would be a translate of a positive dimension algebraic subgroup of $\mathbb{G}_a^g$, and it would be contained in X.

Bibliography

[1] M. Baker, J. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions.* Math. Res. Lett. 11 (2004), no. 2-3, 377-396.

[2] T. Blossier, *Subgroups of the additive group of a separably closed field.* submitted for publication, 2004.

[3] T. Blossier, *Ensembles minimaux localement modulaires.* Thèse de doctorat, 2001.

[4] E. Bouscaren (editor) , *Model theory and algebraic geometry.* An introduction to E.Hrushovski's proof of the geometric Mordell-Lang conjecture, Lecture Notes in Mathematics, 1696. Springer-Verlag, 1998.

[5] S. David, J. Silverman, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M.* (French) [Lower bound for the Néron-Tate height on abelian varieties of CM type] J. Reine Angew. Math. 529 (2000), 1-74.

[6] L. Denis, *Géométrie diophantienne sur les modules de Drinfeld.* (French) [Diophantine geometry on Drinfeld modules] The arithmetic of function fields (Columbus, OH, 1991), 285-302, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.

[7] L. Denis, *Hauteurs canoniques et modules de Drinfeld.* (French) [Canonical heights and Drinfeld modules] Math. Ann. 294 (1992), no. 2, 213-223.

[8] L. Denis, *Problème de Lehmer en caractéristique finie.* (French) [The Lehmer problem in finite characteristic] Compositio Math. 98 (1995), no. 2, 167-175.

[9] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta Arith. 34, no. 4, 391-401, (1979).

[10] O. Endler, *Valuation theory.* To the memory of Wolfgang Krull (26 August 1899–12 April 1971). Universitext. Springer-Verlag, New York-Heidelberg, 1972. xii+243 pp.

[11] G. Faltings, *The general case of S. Lang's conjecture.* Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), 175-182, Perspect. Math., 15, Academic Press, San Diego, CA, 1994.

[12] D. Goldfeld, L. Szpiro, *Bounds for the order of the Tate-Shafarevich group.*

Special issue in honour of Frans Oort. Compositio Math. 97 (1995), no. 1-2, 71-87.

[13] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 35. Springer-Verlag, Berlin, 1996.

[14] A. J. de Jong, *Smoothness, semi-stability and alterations.* Inst. Hautes Études Sci. Publ. Math. No. 83 (1996), 51-93.

[15] M. Hindry, J. Silverman, *On Lehmer's conjecture for elliptic curves.* Séminaire de Théorie des Nombres, Paris 1988-1989, 103-116, Progr. Math., No. 91, Birkhäuser Boston, Boston, MA, 1990.

[16] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, Journal of Amer.Math.Soc **9** (1996), no.3, 667-690.

[17] D. H. Lehmer, *Factorization of certain cyclotomic polynomials*, Ann. of Math. (2) 34 (1933), no. 3, 461-479.

[18] M. Levin, *On the group of rational points on elliptic curves over function fields*, Amer.J.Math 90, 1968 ,456-462.

[19] D. Marker, M. Messmer, A. Pillay, *Model theory of fields*, Lecture Notes in Logic, 5. Springer-Verlag, Berlin, 1996, x+ 154 pp.

[20] D.W. Masser, *Counting points of small height on elliptic curves*. Bull. Soc. Math. France 117 (1989), no. 2, 247-265.

[21] B. Poizat, *Stable groups*. Translated from the 1987 French original by Moses Gabriel Klein. Mathematical Surveys and Monographs, 87. American Mathematical Society, Providence, RI, 2001. xiv+129 pp.

[22] B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfeld modules*, Compositio Mathematica **97** (1995), 349-368.

[23] T. Scanlon, *A Drinfeld module version of the Mordell-Lang conjecture*. available online at `http://Math.Berkeley.EDU/~scanlon/papers/papers.html`.

[24] T. Scanlon, *Positive characteristic Manin-Mumford theorem*. preprint, 2003, available online at `http://Math.Berkeley.EDU/~scanlon/papers/papers.html`.

[25] J.-P. Serre, *Lectures on the Mordell-Weil theorem*. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. x+218 pp.

[26] J.-P. Serre. *Local fields*. Translated from the French by Matin Jay Greenberg. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1979. viii+241 pp.

[27] J. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986. xii+400 pp.

[28] J. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. xiv+525 pp.

[29] J. Silverman, *A lower bound for the canonical height on elliptic curves over abelian extensions.* J. Number Theory 104 (2004), no. 2, 353-372.

[30] L. van den Dries, K. Schmidt, *Bounds in the theory of polynomial rings over fields. A nonstandard approach.* Invent. Math. 76 (1984), no. 1, 77-91.

[31] F. O. Wagner, *Stable groups.* London Mathematical Society Lecture Note Series, 240. Cambridge University Press, Cambridge, 1997. x+309 pp.

[32] J. T.-Y. Wang, *The Mordell-Weil theorems for Drinfeld modules over finitely generated function fields*, Manuscripta math. **106**, 305-314 (2001)