Diss. ETH No. 15138

Galois Representations Associated to Drinfeld Modules in Special Characteristic and the Isogeny Conjecture for t-Motives

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZÜRICH

for the degree of
Doctor of Mathematics

presented by
MATTHIAS TRAULSEN
Dipl.-Math. Universität Gesamthochschule Essen
born February 3rd, 1971
citizen of the Federal Republic of Germany

accepted on the recommendation of
Prof. Dr. Richard Pink, examiner
Prof. Dr. Ernst-Ulrich Gekeler, co-examiner

2003

εἰς τὴν ἀνάμνησιν
τοῦ ἐμοῦ πάππου

ADOLF PALM

For a long time I lie staring into what seems pitch blackness, though I know the roof of the tent is only an arm's length away. No thought that I think, no articulation, however antonymic, of the origin of my desire seems to upset me. 'I must be tired,' I think. 'Or perhaps whatever can be articulated is falsely put.' My lips move, silently composing and recomposing the words. 'Or perhaps it is the case that only that which has not been articulated has to be lived through.'

J. M. Coetzee, *Waiting for the Barbarians*

Acknowledgments

I have benefited a lot from Richard Pink's advisorship and guidance. He suggested the topic of this project, was highly committed to ensuring its success and contributed many an idea. Numerous questions found an answer in his unfailing store of knowledge and techniques.

I am much indebted to Gebhard Böckle who supported me greatly in both personal and mathematical matters. His encouragement and advice vitally helped to keep my work going.

Moreover, I want to express my gratitude to all those who gave me support in some way and especially to those who shared these last years with me. What I owe to them reaches far beyond the scope of science.

In particular, thanks go to: Oliver Baues, Eva Bayer-Fluckiger, Patrick Bonvin, Thomas Borek, Ralph Chill, Jean-François and Christelle Couchot, Antje and Günter Dieckmann, Gerhard Frey, Urs Hartl, Katrin and Bodo Köhl, Silke Lekaus, Renate Leukert, Frithjof Lutscher, Michael Müller, Hassan Oukhaba, Liselotte Palm, Hans-Georg Rück, Heinz Schöch, Eva and Hans Scholz, Christian and Susanne Traulsen, Monika and Hans-Dietrich Traulsen, Iris Traulsen, Evelina Viada-Aehle and Robert Aehle, Lesley Wessels.

Contents

English Abstract

Let F and K be two fields of transcendence degree 1 over the finite field $\mathbb{F}_q$, and let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group of K. Fix a place ∞ of F and let A be the ring of all elements in F which are integral outside ∞.

In this thesis we study Galois representations associated to Drinfeld A-modules over K in special characteristic, in particular residual representations on the $\mathfrak{p}$-adic Tate modules modulo $\mathfrak{p}$. We determine the A-algebra generated by the image of Galois under these representations and its commutant. From this we derive the finiteness of the isogeny class of certain A-motives. In detail, we present the following results:

Let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module over K which has special characteristic. For every prime ideal $\mathfrak{p}$ in A different from the characteristic of ϕ, we get a Galois representation

$$\rho_{\mathfrak{p}} : G_K \longrightarrow \mathrm{Aut}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(\phi)\big)$$

on the $\mathfrak{p}$-adic Tate module of ϕ. By

$$\overline{\rho_{\mathfrak{p}}} : G_K \longrightarrow \mathrm{Aut}_{k_{\mathfrak{p}}}\big(\phi[\mathfrak{p}]\big)$$

we denote the induced residual Galois representation modulo $\mathfrak{p}$. Under the condition that all K-endomorphisms of ϕ are scalar, we prove that the latter representation has the following property:

(**A**) Assume that $\mathrm{End}_K(\phi) = A$. Then for almost all primes $\mathfrak{p}$ in A, the residual representation $\overline{\rho_{\mathfrak{p}}}$ is absolutely irreducible.

Then we generalize this result to the residual representations associated to Drinfeld A-modules with arbitrary endomorphism ring. The generalization comprises two parts: one on the A-algebra generated by the image of Galois, and one on its commutant.

(**B**) For almost all primes $\mathfrak{p}$ in A and all $n > 0$, the natural map

$$\mathrm{End}_K(\phi) \longrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}^n]\big)$$

is surjective, and the $A/\mathfrak{p}^n$-algebra which is generated by the image of Galois in $\mathrm{End}_A(\phi[\mathfrak{p}^n])$ is a direct sum of matrix algebras.

Further, let M be an A-motive which is the direct sum of A-submotives associated to Drinfeld A-modules over K in special characteristic. Based on the preceding results we prove the isogeny conjecture for such an A-motive:

(**C**) Up to K-isomorphism, there are only finitely many A-motives M' over K such that there exists a separable K-isogeny $M' \to M$ of degree prime to the characteristic.

Assuming that (A) holds for representations associated to Drinfeld modules in generic characteristic, our results (B) and (C) generalize to generic characteristic.

Deutsche Zusammenfassung

Seien F und K zwei Körper vom Transzendenzgrad 1 über dem endlichen Körper $\mathbb{F}_q$, und sei $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ die absolute Galoisgruppe von K. Wir wählen eine feste Stelle ∞ von F und bezeichnen mit A den Ring aller Elemente in F, die ausserhalb von ∞ ganz sind.

In der vorliegenden Arbeit untersuchen wir Galoisdarstellungen, die Drinfeld-A-Moduln über K in spezieller Charakteristik assoziiert sind, insbesondere Restklassendarstellungen auf den $\mathfrak{p}$-adischen Tate-Moduln modulo $\mathfrak{p}$. Wir bestimmen die A-Algebra, die vom Bild einer Restklassendarstellung erzeugt wird, und ihre Kommutante. Hieraus leiten wir die Endlichkeit der Isogenieklasse gewisser A-Motive ab. Im einzelnen zeigen wir:

Sei $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ ein Drinfeld-A-Modul über K mit spezieller Charakteristik. Für jedes Primideal $\mathfrak{p}$ in A, das von der Charakteristik von ϕ verschieden ist, gibt es eine Galoisdarstellung

$$\rho_{\mathfrak{p}} : G_K \longrightarrow \mathrm{Aut}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(\phi)\big)$$

auf dem $\mathfrak{p}$-adischen Tate-Modul von ϕ. Modulo $\mathfrak{p}$ induziert $\rho_{\mathfrak{p}}$ die Restklassendarstellung

$$\overline{\rho_{\mathfrak{p}}} : G_K \longrightarrow \mathrm{Aut}_{k_{\mathfrak{p}}}\big(\phi[\mathfrak{p}]\big).$$

Unter der Voraussetzung, dass alle K-Endomorphismen von ϕ skalar sind, beweisen wir die folgende Eigenschaft der Restklassendarstellung:

(**A**) Wir nehmen an, dass $\mathrm{End}_K(\phi) = A$ ist. Dann ist die Restklassendarstellung $\overline{\rho_{\mathfrak{p}}}$ für fast alle Primideale $\mathfrak{p}$ in A absolut irreduzibel.

Danach beweisen wir eine Verallgemeinerung für Restklassendarstellungen, die von Drinfeld-A-Moduln mit beliebigem Endomorphismenring herkommen. Sie besteht aus zwei Teilen: einem für die A-Algebra, die vom Bild der Darstellung erzeugt wird, und einem für deren Kommutante.

(**B**) Für fast alle Primideale $\mathfrak{p}$ in A und alle $n > 0$ ist die natürliche Abbildung

$$\mathrm{End}_K(\phi) \longrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}^n]\big)$$

surjektiv und die $A/\mathfrak{p}^n$-Algebra, die vom Bild der absoluten Galoisgruppe in $\mathrm{End}_A(\phi[\mathfrak{p}^n])$ erzeugt wird, eine direkte Summe von Matrixalgebren.

Weiter sei M ein A-Motiv, das eine direkte Summe von A-Motiven ist, die von Drinfeld-Moduln über K in spezieller Charakteristik induziert sind. Auf den vorangehenden Ergebnissen aufbauend beweisen wir die Isogenie-Vermutung für solche A-Motive:

(**C**) Bis auf K-Isomorphie gibt es nur endlich viele A-Motive M' über K, für die eine separable K-Isogenie $M' \to M$ existiert, deren Grad prim zur Charakteristik ist.

Unter der Annahme, dass (A) auch für Darstellungen gilt, die von Drinfeld-Moduln in generischer Charakteristik herkommen, erhalten wir ausserdem die Ergebnisse (B) und (C) in beliebiger Charakteristik.

Introduction

The Historical Context

Back in 1963/64, John Tate stated a conjecture on abelian varieties which has attained great importance in arithmetic algebraic geometry: Let k be a field which is finitely generated over its prime field, and let G_k be its absolute Galois group. Tate conjectured that, given two abelian varieties A and B over k with ℓ-adic Tate modules $T_\ell(A)$ and $T_\ell(B)$, the natural map

$$\mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell[G_k]}\big(T_\ell(A), T_\ell(B)\big)$$

is an isomorphism.[1] At that time, due to results of David Mumford and Jean-Pierre Serre, this had been known for elliptic curves over finite fields and over number fields with at least one real prime.

This conjecture is commonly referred to as the *Tate conjecture*. In order to bring its twofold significance to a point, assume that $A = B$. Then the Tate conjecture claims firstly that the endomorphisms of an abelian variety are distinguished by their action on the Tate module. This is the easy part. Secondly, the conjecture describes the commutant of the $\mathbb{Z}_\ell$-algebra generated by the image of Galois in the endomorphism ring of the Tate module: It consists of the endomorphisms which are induced by endomorphisms of the abelian variety. The proof of this second part is far from being obvious.

Actually, Tate did not state this as a conjecture in its own right. It originally appeared as a special case of a more general conjecture[2] on algebraic cycles, the primary interest being in the étale cohomology of abelian varieties and the corresponding Galois representations.

A few years later, in 1966, Tate published a proof of his conjecture in the case of abelian varieties over finite fields.[3] A key element is the following property: We say that an abelian variety A over a (not necessarily finite) field k satisfies hypothesis (F) for a prime ℓ different from the characteristic of k, if there are, up to isomorphism, only finitely many abelian varieties B over k with a polarization of fixed degree and an isogeny $B \to A$ of ℓ-power degree. Tate proved that (F) is satisfied by abelian varieties

[1] Tate [**44**] (8).

[2] *loc. cit.* Conjecture 1.

[3] Tate [**45**].

over finite fields, and that the Tate conjecture holds for abelian varieties satisfying (F) at least in certain cases which include the finite field setting.

The next major step in the quest for a general proof of the Tate conjecture was Yuri Zarhin's work in 1974. He gave a proof of the finiteness property (F) and the Tate conjecture over fields of transcendence degree 1 over a finite field in odd characteristic. He further showed that (F) follows from a conjecture on the resolution of singularities of algebraic varieties.[4] Together with earlier results on the resolution of singularities of algebraic surfaces due to Shreeram S. Abhyankar, this yielded a proof of (F) over fields of transcendence degree at most 3 over a finite field in odd characteristic.

In 1976 Zarhin achieved a proof of the Tate conjecture over fields of arbitrary finite transcendence degree over a finite field of odd characteristic. Simultaneously, he proved the finiteness property (F) and the *semisimplicity conjecture* for abelian varieties over the same type of fields.[5]

The semisimplicity conjecture is the assertion that, after tensoring with $\mathbb{Q}_\ell$, the ℓ-adic Tate module of an abelian variety is a semisimple Galois module. Sometimes in the literature it is subsumed under the name of *Tate conjecture*; sometimes it seems to be referred to as a special case of the *Grothendieck-Serre conjecture*.

Independently and with a different method, in 1977 Shigefumi Mori gave a proof of the results of Zarhin's 1976 paper.[6] He was able to reduce the problem to the case of transcendence degree 1, solved by Zarhin in 1974.

Then, in 1983, a milestone in arithmetic algebraic geometry was reached. In his famous article *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*[7], Gerd Faltings was able to confirm Tate's conjecture for abelian varieties over algebraic number fields. He proved the Tate conjecture together with two more fundamental conjectures for abelian varieties over number fields: the semisimplicity conjecture and the *Šafarevič conjecture*, which in turn implies the *Mordell conjecture*.

By Mordell's conjecture a nonsingular projective algebraic curve of genus at least two over a number field has at most finitely many rational points.

The Šafarevič conjecture states that, given a finite set of places S and a positive integer g, there are only finitely many isomorphism classes of abelian varieties of dimension g having good reduction outside S. At the International Congress of Mathematicians in Stockholm in 1962, Igor R. Šafarevič had raised this as a question and given a proof for the case of elliptic curves over number fields.[8] (In fact, his question and proof were put more generally for algebraic varieties and algebraic curves over number fields, with some constraint on curves of genus 1 not affecting elliptic curves.)

---

[4] Zarhin [**46**] Theorem 1, [**47**] Corollary 1.4 and [**48**]

[5] Zarhin [**49**] Theorem and Corollaries 1, 2.

[6] Mori [**21**] Corollary 1.3 and Corollary 5.3.

[7] Faltings [**11**], English translation in Cornell-Silverman [**5**].

[8] Šafarevič [**30**] §3.

The connection between the Mordell conjecture and the Šafarevič conjecture has been established by Aleksey N. Paršin in the late 1960s.[9]

A somewhat stronger version of the finiteness property (F) is the *isogeny conjecture*. It claims that the isogeny class of an abelian variety contains only finitely many isomorphism classes. Here again, the terminology is not uniform; in the literature the name isogeny conjecture can refer to different conjectures. The isogeny conjecture is a corollary to the Šafarevič conjecture, thus to Šafarevič's theorem in the case of elliptic curves over number fields, and to Faltings' theorems in the case of abelian varieties over number fields. Conversely, the isogeny conjecture can be used to prove each one of the Tate, Šafarevič and semisimplicity conjectures for abelian varieties.

During the years between the announcement of Tate's conjecture and Faltings' proof of the number field case, the arithmetic of function fields with finite field of constants had seen major advancements in totally new branches. In 1974, Vladimir G. Drinfeld had introduced the notion of *elliptic module*[10], nowadays called *Drinfeld module*, which turned out to be extremely fruitful. In the arithmetic of function fields, Drinfeld modules take on very much the role that elliptic curves play in the arithmetic of number fields and even go beyond that. After almost thirty years of research and the publication of numerous articles, the theory of Drinfeld modules seems far from being exhausted.

Later, in 1986, Greg W. Anderson initiated the theory of *t-motives*[11], which generalize Drinfeld modules and provide for an analog of abelian varieties. Many questions familiar from the theory of abelian varieties were to be met again in the new setting. It thus stood to reason to study analogs, in particular of Faltings' results, in the case of Drinfeld modules and t-motives.

Important contributions to the function field setting have come from Japanese mathematicians. The isogeny conjecture and the semisimplicity conjecture for Drinfeld modules have been proved by Yuichiro Taguchi in the 1990s.[12] He largely used Faltings' ideas, constructing minimal models for Drinfeld modules and introducing an appropriate height function. Furthermore, the Tate conjecture for t-motives, containing the Tate conjecture for Drinfeld modules as a special case, has been proved independently by Akio Tamagawa in 1994 and by Yuichiro Taguchi in 1995.[13]

So far, the isogeny conjecture for t-motives has remained unproved. The methods used by Taguchi in the case of Drinfeld modules do not generalize in an obvious way. Yet, with a different approach, the isogeny conjecture for t-motives will partly be settled in the thesis at hand. Again, the Tate conjecture comes into the picture as an important tool.

---

[9] Paršin [**23**] Chapter 3 §2 Remark 2 and [**24**] Théorème 1.

[10] Drinfeld [**9**].

[11] Anderson [**1**].

[12] Taguchi [**35**], [**36**] and [**39**].

[13] Tamagawa [**41**], [**42**], [**43**] and Taguchi [**37**], [**38**].

Notation

Throughout this thesis, we use the following notation:

For any field L we denote by $\overline{L}$ a fixed algebraic closure of L and by L^{sep} the separable closure of L in $\overline{L}$. Let $G_L = \mathrm{Gal}(L^{\mathrm{sep}}/L)$ be the absolute Galois group of L.

Let p be a prime number and q be a power of p. Let $\mathcal{C}$ and $\mathcal{X}$ be two smooth, projective, connected curves over the finite field $\mathbb{F}_q$ with q elements. By F and K we denote the respective function fields. Let ∞ be a fixed closed point on $\mathcal{C}$ of degree d_∞ over $\mathbb{F}_q$ and let A be the ring of functions in F which are regular outside ∞.

By v_∞ we denote the valuation on F associated to the prime ∞, and by $|\cdot|_\infty$ the corresponding normalized absolute value. Then we have

$$|\alpha|_\infty = q^{-d_\infty v_\infty(\alpha)}$$

for all $\alpha \in F$.

We assume that K is an A-field, i. e. we fix and name a ring homomorphism

$$\iota : A \to K.$$

We call the ideal $\ker \iota \subset A$ the *characteristic* of K and say that K has *generic characteristic* if ι is injective and that K has *special characteristic* $\mathfrak{p}_0$ if $\mathfrak{p}_0 = \ker \iota$ is nonzero.

Let $x \in \mathcal{X}$ be a closed point. We fix the following notation:

$K^{\mathrm{ab}} \subset \overline{K}$	the maximal abelian extension of K,
$K^{\mathrm{nr}} \subset \overline{K}$	the maximal unramified extension of K,
$K^{\mathrm{ab,nr}} \subset \overline{K}$	the maximal unramified abelian extension of K,
K_x	the completion of K at x,
$\mathcal{O}_x \subset K_x$	the valuation ring in K_x.

Let k_0 be the field of constants of K. By $k_{0,d}$ we denote the field extension of k_0 of degree d. The absolute Galois group G_{k_0} of k_0 is isomorphic to the Prüfer group $\widehat{\mathbb{Z}}$ and is topologically generated by the arithmetic Frobenius Frob_{k_0}.

By ϕ we denote a Drinfeld A-module of rank r over K which has special characteristic (see below Chapter I Section 1). By M we denote an A-motive over K which is a direct sum of A-motives associated to Drinfeld A-modules over K (see below Chapter II Section 1).

References. In this text, bibliographic references include the name of the author followed by a number in squared brackets that refers to the bibliography at the end of this volume.

Cross references within the same chapter are given in arabic numbers (e. g. Section 1, Proposition 4.3). References from one chapter to another are preceded by the corresponding roman numeral (e. g. Section II.2, Lemma I.3.3).

Outline of the Thesis

The main goals of this treatise are the study of certain Galois representations associated to Drinfeld modules and, as already mentioned at the end of the historical overview, a proof of the isogeny conjecture for a special class of A-motives. The A-motives considered are, loosely speaking, direct sums of Drinfeld modules.

According to these goals, the material is organized in two main parts: in a chapter on Drinfeld modules and Galois representations (Chapter I) and a chapter on A-motives and the isogeny conjecture (Chapter II). Except for the introductory sections, we assume all Drinfeld modules and A-motives to have special characteristic.

Chapter I. The first chapter deals with Galois representations associated to Drinfeld modules in special characteristic. To be precise, we study the representations of the absolute Galois group G_K of the function field K on the $\mathfrak{p}$-adic Tate module of a Drinfeld module, and the induced residual representations modulo $\mathfrak{p}$.

In Section 1 we give a concise overview over the theory of Drinfeld modules, to the extent that is relevant in our context. In Section 2 we compile selected results on Galois representations on Tate modules of Drinfeld modules. These will be needed later on for the proofs of our results. The contents of the first two sections can be found in the literature; we therefore mostly omit the proofs.

In the remaining sections of Chapter I, the main focus will be on the study of the residual representations in special characteristic. Two main results will be proved. First, we consider Drinfeld modules which only have scalar endomorphisms.

Theorem A. *Assume that* $\mathrm{End}_K(\phi) = A$. *Then for almost all primes* $\mathfrak{p}$ *of* A *the residual representation*

$$\overline{\rho_{\mathfrak{p}}} : G_K \longrightarrow \mathrm{Aut}_{k_{\mathfrak{p}}}\big(\phi[\mathfrak{p}]\big)$$

is absolutely irreducible.

Then we extend Theorem A to Drinfeld modules with arbitrary endomorphism ring. Of course, we can no longer expect that the residual representation is irreducible, let alone absolutely irreducible. However, the theorem generalizes if we translate absolute irreducibility into a consequence for the commutant of the image of Galois. This is the topic of

Theorem B. *For almost all primes* $\mathfrak{p}$ *in* A *and all* $n > 0$,

(1) *the natural map*

$$\mathrm{End}_K(\phi) \longrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}^n]\big)$$

is surjective,

(2) *the image of the group algebra* $A[G_K]$ *in* $\mathrm{End}_A(\phi[\mathfrak{p}^n])$ *is a direct sum of full matrix algebras.*

The proofs of these two theorems are given in Sections 3 and 4.

In Section 3 we develop a proof of Theorem A under the additional hypothesis that the endomorphism ring of the Drinfeld module ϕ does not become larger under extensions of the base field K.

The three most important ingredients in Section 3 are the isogeny conjecture for Drinfeld modules, due to Taguchi, Deligne's theorem on the equidistribution of Frobenius elements in the absolute Galois group, and a result on the density of the image of Galois in GL_r, contributed by Pink.

On the basis of this special case of Theorem A we shall establish Theorem B in Section 4. Here, the key element in the proof will be, besides the weak version of Theorem A, the isogeny conjecture for Drinfeld modules.

Once Theorem B is proven, the general version of Theorem A follows as a direct consequence.

In Section 5 we include an unpublished result by Richard Pink comparing the residual representations associated to non-isogenous Drinfeld modules. It states that only for finitely many primes these representations can have a nontrivial common subquotient. Pink's proof uses Theorem B.

Chapter II. In the second part we discuss A-motives and their isogenies. Here we develop our third main result, the proof of the isogeny conjecture for a certain class of A-motives.

In Section 1 we give the definition and the most important properties of A-motives. As in the introduction to Drinfeld modules, only references to the proofs are given.

From then on, we assume that the A-motives considered be direct sums of A-motives associated to Drinfeld A-modules in special characteristic. In Section 2 we show that, given a finite separable extension K'/K of the base field, in the K-isogeny class of such an A-motive M there are only finitely many K-isomorphism classes of A-motives which become isomorphic to M over K'.

Originally, this had been intended to provide for a reduction step in the proof of the isogeny conjecture for A-motives, and became needless when we realized an enhancement of Theorems A and B. Now, the outcome of this relic is a tedious proof of a trivial consequence of the isogeny conjecture. Yet we left this section in its place.

The core of Chapter II is in Section 3. It presents a proof of the isogeny conjecture for A-motives of the form described above:

Theorem C. *Let M be an A-motive which is the direct sum of A-motives associated to Drinfeld A-modules defined over K.*

Then, up to K-isomorphism, there are only finitely many A-motives M' over K for which there exists a separable K-isogeny $M \to M'$ of degree not divisible by the characteristic of M.

The idea on which we build has already been applied successfully in the context of abelian varieties. It translates isogenies to M into adelic lattices in the rational Tate module of M.

As central components of the proof we have the Tate conjecture for A-motives, due to Taguchi and Tamagawa, the semisimplicity conjecture for Drinfeld modules, proven by Taguchi, the theorem of Jordan-Zassenhaus on lattices over orders in semisimple algebras, Pink's comparison of the residual representations associated to non-isogenous Drinfeld modules, and Theorem B.

Restrictions and open ends. We conclude the introduction with some remarks on questions which remain open at the end of this thesis and at which the work done could find a continuation.

First, we have restricted ourselves to Drinfeld modules and A-motives in special characteristic. This naturally calls for an extension to generic characteristic, which should well be possible. In fact, as the reader will find, only Section I.3 really necessitates the assumption of special characteristic. The reason why we have to argue differently in generic characteristic lies in Proposition I.2.8, which in turn is essential for Lemma I.3.3.

Proposition I.2.8 makes use of the criterion of Néron-Ogg-Šafarevič, which does not rule out the possibility that the Tate module of a Drinfeld module with good reduction is ramified at some special place of K. Only in special characteristic we can exclude the bothersome place in a useful way. In generic characteristic there will remain a place of K at which the character $\overline{\chi_{\mathfrak{p}}}$ is ramified, and our argument fails.

However, all proofs from Section I.4 on carry over to generic characteristic without modification; often they even simplify because the endomorphism rings of Drinfeld modules in generic characteristic are commutative.

Therefore, in order to accomplish a proof of the isogeny conjecture for A-motives in generic characteristic one would need nothing more (or less, depending on the point of view) than a proof of Theorem A, the absolute irreducibility of the residual representation, in generic characteristic.

The second restriction we had to make is the assumption that the A-motives considered be direct sums of A-motives associated to Drinfeld modules. This restriction is of much more structural nature; it is due to the approach to the isogeny conjecture we have chosen. Properties of Galois representations associated to Drinfeld modules—such are at the heart of our proof—can only be applied if the A-motives decompose in a suitable way.

Nonetheless, it should be expected that the isogeny conjecture holds for a more general class of A-motives. For the general statement, we call an A-motive *semisimple up to isogeny* if it is isogenous to a direct sum of simple A-motives.

Conjecture. *Let M be an A-motive over K that is semisimple up to K-isogeny. Then, up to K-isomorphism, there are only finitely many A-motives M' over K for which there exists a K-isogeny $M \to M'$ of degree not divisible by the characteristic of M.*

The proximate idea would be to follow Faltings and Taguchi in their proofs of the isogeny conjecture for abelian varieties and Drinfeld modules. This would require the construction of minimal models of A-motives and the definition of a height function which is invariant under isogenies. The appropriate objects for such an enterprise might be τ-sheaves associated to A-motives rather than A-motives themselves.

Another question arises in the context of Chapter I. We give a description of the A-algebra generated by the image of Galois in $\mathrm{End}_{k_\mathfrak{p}}(\phi[\mathfrak{p}])$ for almost all $\mathfrak{p}$. Although this is sufficient for our purposes, it is only part of the story. One should also ask for the image of Galois itself. It could be hoped that for almost all primes $\mathfrak{p}$ the image of $\overline{\rho_\mathfrak{p}}$ equals $\mathrm{Aut}_{E^*}(\phi[\mathfrak{p}])$, where E^* is the subgroup of automorphisms of $\phi[\mathfrak{p}]$ induced by K-endomorphisms of ϕ.

CHAPTER I

Drinfeld Modules

In the arithmetic of function fields with finite field of constants, Drinfeld modules play an essential role. They have been introduced by Vladimir G. Drinfeld in 1974, who then called them *elliptic modules*. Drinfeld constructed their moduli spaces, developed a uniformization theory and used them to prove the local Langlands conjecture for GL_2 over a function field (see Drinfeld [**9**] and [**10**]).

This groundbreaking result was only the starting point for a broad variety of applications. The areas to which the theory of Drinfeld modules has contributed (or has even been fundamental) include, among others, explicit class field theory, the theories of automorphic forms, modular forms and L-series, transcendence theory and Galois representations.

A great strength of the concept of Drinfeld modules is the large number of striking analogies with elliptic curves. Some of them will appear in Sections 1 and 2. In our context, the most important analogy concerns Galois representations on Tate modules of Drinfeld modules. The present chapter will deal with these representations.

The first two sections give an overview over well-known material. After a brief general introduction to Drinfeld modules, we give an account of several important results on Galois representations associated to Drinfeld modules. Then, Sections 3 and 4 contain our contributions to residual representations in special characteristic. In Section 5 we include a result comparing residual representations, contributed by Richard Pink.

Whenever we point out an analogy between Drinfeld modules and elliptic curves, the results on elliptic curves are mentioned without reference. For the interested reader, the necessary arithmetic theory of elliptic curves is covered in Joseph H. Silverman's textbook [**33**].

1. A Brief Introduction to Drinfeld Modules

The following paragraphs contain an exposition of the basic theory of Drinfeld modules. We assume that the reader is familiar with algebraic number theory and the main ideas of algebraic geometry, profitably with the theory of elliptic curves as well.

The presentation is neither comprehensive nor completely self-contained. It is an overview tailored for our needs, and for most of the proofs we refer to the literature. We omit some algebraic results which only hold for Drinfeld modules in generic characteristic, and we skip the whole analytic theory. Readers familiar with the theory will notice many more omissions.

The first reference which should be consulted as a complement to this introduction is Drinfeld's original paper [**9**]. Another two useful and more detailed accounts are given in the survey article [**8**] by Pierre Deligne and Dale Husemöller and in the textbook [**13**] by David Goss. Supplementary information can be gained from the various articles cited below.

Additive Polynomials. Although the theory of Drinfeld modules can be developed in great abstraction, it often comes in handy to have a concrete description for constructive proofs and computations. The abstract language is, of course, algebraic geometry. The instrument on the concrete side are additive polynomials.

As it will be fundamental for the following discussion, we recall the well-known fact that we have

$$(x+y)^p = x^p + y^p$$

for x, y in any field of characteristic p. Let L denote a field containing the finite field $\mathbb{F}_q$, and let $P \in L[T]$ be a polynomial with coefficients in L.

Definition 1.1. We say that P is *additive* if

$$P(x+y) = P(x) + P(y)$$

for all $x, y \in L$. We say that P is $\mathbb{F}_q$*-linear* if P is additive and

$$P(\alpha x) = \alpha P(x)$$

for all $\alpha \in \mathbb{F}_q$ and all $x \in L$.

It is immediate that we obtain rings if we endow the sets of additive and $\mathbb{F}_q$-linear polynomials over L with addition and composition; in general these rings are noncommutative.

At this point, we give a caveat: A polynomial which is additive over L does not need to be additive over extension fields of L. Indeed, the polynomial

$$T + (T^3 - T)^2 = T^6 + T^4 + T^2 + T \in \mathbb{F}_3[T]$$

is additive over $\mathbb{F}_3$, but it is not additive over any nontrivial extension of $\mathbb{F}_3$. However, if L is an infinite field, all additive polynomials over L are additive over $\overline{L}$.

Clearly every polynomial over a field L of characteristic p that consists of monomials of p-power degree only, is additive over $\overline{L}$. We shall see in a moment that over infinite fields all additive polynomials have this form. We set

$$\tau_p(T) = T^p \in L[T]$$

and by $L\{\tau_p\}$ we denote the subring of the ring of all additive polynomials over L (with the ring structure defined by addition and composition) which is generated by τ_p. Note that in $L\{\tau_p\}$ we have the commutation rule

$$\tau_p x = x^p \tau_p \tag{1}$$

for all $x \in L$.

The following proposition uncovers the structure of the additive polynomials over an infinite field.

Proposition 1.2. *Assume that L is infinite and let $P \in L[T]$ be a polynomial with coefficients in L. Then P is additive if and only if $P \in L\{\tau_p\}$.*

Proof. Goss [**13**] Proposition 1.1.5. □

Now assume that $q = p^m$. We let $\tau = \tau_p^m$ be the polynomial which induces the q-th power mapping on L and let $L\{\tau\}$ be the subring of $L\{\tau_p\}$ generated by τ. If L is infinite, one easily sees that $L\{\tau\}$ is the $\mathbb{F}_q$-algebra of $\mathbb{F}_q$-linear polynomials over L.

Let $P \in L\{\tau\}$ be a nonzero $\mathbb{F}_q$-linear polynomial over L. Then, as we just have stated, P has the form

$$P(T) = \sum_{i=0}^{n} c_i T^{q^i}$$

with all coefficients $c_i \in L$ and the leading coefficient $c_n \neq 0$. Its degree necessarily is a power of q. Because P only contains monomials of q-power degree, we can view P as a polynomial in τ, that is

$$P(\tau) = \sum_{i=0}^{n} c_i \tau^i.$$

The notation $P(\tau)$ always refers to this representation. The product (defined as the composition) of two $\mathbb{F}_q$-linear polynomials P, Q then is denoted by $P(\tau)Q(\tau)$; it may be computed as an ordinary product of polynomials in τ if taking into account the commutation rule (1). We call $L\{\tau\}$ the *twisted polynomial ring* over L.

The polynomial $P(\tau)$ is called *monic* if $P(T)$ is monic, i. e. if $c_n = 1$. The degree of P as a polynomial in τ is defined to be n, therefore

$$\deg P(\tau) = q^{\deg P(T)}.$$

In our context, zeros of $\mathbb{F}_q$-linear polynomials play an important role. It can easily be seen that for any $\mathbb{F}_q$-linear polynomial $P \in L\{\tau\}$, the set of zeros of P in $\overline{L}$ is an $\mathbb{F}_q$-vector space. Conversely, we have

Proposition 1.3. *Let $P \in L[T]$ be a separable polynomial over L. Then P is $\mathbb{F}_q$-linear if and only if the set of zeros of P in $\overline{L}$ is an $\mathbb{F}_q$-vector space.*

Proof. Goss [**13**] Corollary 1.2.2. □

Another point of importance for our discussion concerns divisibility in the multiplicative structure (by composition) of $L\{\tau\}$.

Let again $P, Q \in L\{\tau\}$ be $\mathbb{F}_q$-linear polynomials over L. We say that $P(\tau)$ is *right divisible* by $Q(\tau)$ in $L\{\tau\}$ if there exists an $\mathbb{F}_q$-linear polynomial $Q_0 \in L\{\tau\}$ such that

$$P(\tau) = Q_0(\tau)Q(\tau).$$

In the following sense, right division in $L\{\tau\}$ behaves like division in an ordinary polynomial (or Euclidean) ring:

Proposition 1.4. *Let $P, Q \in L\{\tau\}$ be two $\mathbb{F}_q$-linear polynomials, $Q \neq 0$. Then there exist $\mathbb{F}_q$-linear polynomials $Q_0, R \in L\{\tau\}$ with* $\deg R(\tau) < \deg Q(\tau)$ *such that*

$$P(\tau) = Q_0(\tau)Q(\tau) + R(\tau).$$

Proof. This is the well-known Euclidean algorithm. □

The existence of the right division algorithm has the following easy but important consequence:

Corollary 1.5. *Every left ideal of $L\{\tau\}$ is principal.*

Proof. Clear. □

Finally, we establish a link to algebraic geometry and, in doing so, prepare the grounds for the application of additive polynomials to the theory of Drinfeld modules. Let $\mathbb{G}_{a,L}$ be the additive group scheme over L. Then we have

Proposition 1.6.

$$\mathrm{End}_L(\mathbb{G}_{a,L}) = L\{\tau_p\}.$$

Proof. Deligne-Husemöller [**8**] Proposition 1.2. □

The Category of Drinfeld Modules. We come to the definition of Drinfeld modules, the most fundamental notion in this thesis.

Let $q = p^m$ and let again L be an A-field containing the finite field $\mathbb{F}_q$. We thus have a ring homomorphism $\iota_L : A \to L$, whose kernel is called the *characteristic* of L. As in the previous paragraph, $\tau_p(T) = T^p \in L[T]$ denotes the polynomial which induces the p-th power mapping on L, and $\tau = \tau_p^m$. We introduce (*ad hoc*) two more homomorphisms

$$\varepsilon : L \longrightarrow L\{\tau_p\} : c \mapsto c\tau_p^0$$

and

$$D : L\{\tau_p\} \longrightarrow L : \sum_{i=0}^{n} c_i \tau_p^i \mapsto c_0.$$

These homomorphisms are used to formalize the following idea: A Drinfeld module over L should be a ring homomorphism from A into the twisted polynomial ring over L, such that the image of a non-constant $a \in A$ is non-constant and its constant term is $\iota_L(a)$. The intention behind this construction is to get a “non-constant” A-module structure on L which reflects the structure of L as an A-field, whence the name Drinfeld A-module.

Definition 1.7 (Drinfeld modules)**.**

(1) Let $\phi : A \to \mathrm{End}_L(\mathbb{G}_{a,L})$ be a ring homomorphism. Then ϕ is called a *Drinfeld A-module* over L if
  (a) $\iota_L = D \circ \phi$ and
  (b) $\phi \neq \varepsilon \circ \iota_L$.
  For every $a \in A$, the image of a under ϕ is denoted by ϕ_a.

(2) A *morphism* $P : \phi \to \phi'$ of Drinfeld A-modules over L is an additive polynomial $P \in L\{\tau_p\}$ such that for all $a \in A$

$$P(\tau_p)\phi_a(\tau_p) = \phi'_a(\tau_p)P(\tau_p).$$

A nonzero morphism of Drinfeld A-modules is called an *isogeny*, a morphism which has a two-sided inverse is called an *isomorphism*.

The characteristic $\ker \iota_L$ of L is also referred to as the characteristic of the Drinfeld A-module ϕ.

Sometimes in the literature, definitions require that the image of a Drinfeld module consists of $\mathbb{F}_q$-linear polynomials. However, this property follows from our definition, as we explain in

Remark 1.8 (Linearity of the polynomials)**.** By our definition, a Drinfeld A-module over L is a ring homomorphism

$$\phi : A \longrightarrow L\{\tau_p\}.$$

However, we know more: We have assumed that L contains $\mathbb{F}_q$. Thus the image of ϕ contains $\mathbb{F}_q\tau_p^0$. Because the image of ϕ is commutative and in view of the commutation rule in $L\{\tau_p\}$, we see that the image of ϕ must be contained in $L\{\tau\}$. Therefore a Drinfeld A-module over L actually is a ring homomorphism

$$\phi : A \longrightarrow L\{\tau\}.$$

Similarly, we see that morphisms of Drinfeld A-modules over L must be $\mathbb{F}_q$-linear polynomials, so we have

$$\mathrm{Hom}_L(\phi, \phi') \subset L\{\tau\}.$$

Before we go on, we want to have a quick look at the notion of isogeny of Drinfeld modules and link it to the corresponding notions for elliptic curves and abelian varieties.

Remark 1.9 (On isogenies)**.** A Drinfeld A-module over L induces a structure of A-module on the additive group scheme $\mathbb{G}_{a,L}$. An isogeny $P : \phi \to \phi'$ of Drinfeld A-modules over L induces an A-linear morphism from $\mathbb{G}_{a,L}$ endowed with the A-module structure via ϕ to $\mathbb{G}_{a,L}$ endowed with the A-module structure via ϕ'. The homomorphism on the points of $\mathbb{G}_{a,L}$ is given by evaluation of the polynomial P. Over an algebraically closed field it is surjective and has finite kernel; therefore the notion of isogeny agrees with the one known from elliptic curves and abelian varieties.

Having discussed at length the definition of Drinfeld modules and their morphisms, we give the first—basic but important—properties.

Proposition 1.10. *Let $\phi : A \to \mathrm{End}_L(\mathbb{G}_{a,L})$ be a Drinfeld A-module. Then*

(1) *the ring homomorphism ϕ is injective,*

(2) *there exists an integer* $r > 0$ *such that*

$$\deg \phi_a(T) = q^{\deg \phi_a(\tau)} = |a|_\infty^r$$

for all nonzero $a \in A$.

Proof. Drinfeld [**9**] Proposition 2.1 and Corollary to Proposition 2.2. $\square$

Definition 1.11. The integer r in Proposition 1.10 (2) is called the *rank* of the Drinfeld module ϕ.

Remark 1.12. Comparing degrees, we see that an isogeny $\phi \to \phi'$ can only exist if ϕ and ϕ' have the same rank.

Torsion and Galois representations. We now specialize to Drinfeld A-modules over the function field K. We do not use Drinfeld modules over other fields except in a few places where K will be replaced by its algebraic or separable closure, and in connection with reduction theory below.

Let us have a brief excursion to elliptic curves. On an elliptic curve E over an algebraically closed field, multiplication with an integer n is an isogeny $E \to E$. Its kernel $E[n]$ is a finite Galois invariant $\mathbb{Z}$-module, called the *n-torsion module* of E. As a $\mathbb{Z}$-module, $E[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

For a rational prime ℓ and $m > 0$, the modules $E[\ell^m]$ form a projective system under multiplication with ℓ. The projective limit $T_\ell(E)$ is a $\mathbb{Z}_\ell$-module carrying a continuous Galois action; it is called the *ℓ-adic Tate module* of E. The associated ℓ-adic representations are an important class of Galois representations.

Now we are going to carry out the very same constructions for Drinfeld modules. The role of the ring of rational integers $\mathbb{Z}$ is being taken over by the Dedekind ring A.

Let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module of rank r and let $\mathfrak{a} \subset A$ be a nonzero ideal. As A is a Dedekind domain, the ideal $\mathfrak{a}$ is generated by at most two elements $a_1, a_2 \in A$. We have seen that the left ideal in $K\{\tau\}$ generated by ϕ_{a_1} and ϕ_{a_2} is principal; let $\phi_{\mathfrak{a}}$ be its monic generator. If $\mathfrak{a} = (a)$ is a principal ideal, then clearly $\phi_{\mathfrak{a}} = c\phi_a$ for some $c \in K^*$.

Definition 1.13. The module of $\mathfrak{a}$-torsion of ϕ is defined to be the finite subgroup scheme

$$\phi[\mathfrak{a}] = \ker \phi_{\mathfrak{a}} \subset \mathbb{G}_{a,K}.$$

We should notice that $\phi[\mathfrak{a}]$ is stable under the action of A via ϕ. Further, the $\overline{K}$-valued points of $\phi[\mathfrak{a}]$ are the zeros of the polynomial $\phi_{\mathfrak{a}}$ in $\overline{K}$. As $\phi_{\mathfrak{a}}$ is $\mathbb{F}_q$-linear, it follows that $\phi[\mathfrak{a}](\overline{K})$ is an $\mathbb{F}_q$-vector space and an A-module.

Proposition 1.14. *Let* $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ *be a Drinfeld A-module of rank* r *and* $\mathfrak{a} \subset A$ *an ideal which is not divisible by the characteristic of* ϕ. *Then*

(1) $\phi[\mathfrak{a}](\overline{K})$ *is a free* $A/\mathfrak{a}$*-module of rank* r,

(2) $\phi[\mathfrak{a}](\overline{K}) \subset K^{\mathrm{sep}}$,

(3) $\phi[\mathfrak{a}](\overline{K})$ *is invariant under* G_K.

Proof. (1) Deligne-Husemöller [**8**] Theorem 3.3. (2) If $\mathfrak{a}$ is not divisible by the characteristic, then the constant term of $\phi_\mathfrak{a}$ is nonzero. As $\phi_\mathfrak{a}$ is $\mathbb{F}_q$-linear, this means that $\phi_\mathfrak{a}$ is a separable polynomial. (3) Clear. □

Notation 1.15.

(1) If the characteristic of ϕ does not divide the ideal $\mathfrak{a}$, then by abuse of notation we write $\phi[\mathfrak{a}]$ for the $\overline{K}$-valued points of this group scheme as well.
(2) Let $a \in A$. Then we set $\phi[a] = \phi[(a)]$.

Now we gather all $\mathfrak{p}$-power torsion of ϕ in one object, the $\mathfrak{p}$-adic Tate module. It will be used as representation space for our $\mathfrak{p}$-adic Galois representations.

Definition 1.16. For every prime ideal $\mathfrak{p}$ in A we define the $\mathfrak{p}$-adic Tate module of ϕ to be

$$T_\mathfrak{p}(\phi) = \mathrm{Hom}_A\big(F_\mathfrak{p}/A_\mathfrak{p}, \phi[\mathfrak{p}^\infty]\big)$$

where $\phi[\mathfrak{p}^\infty] = \bigcup_{i=1}^{\infty} \phi[\mathfrak{p}^i]$ is the A-module consisting of all $\mathfrak{p}$-power torsion of ϕ. We set

$$V_\mathfrak{p}(\phi) = T_\mathfrak{p}(\phi) \otimes_{A_\mathfrak{p}} F_\mathfrak{p}$$

and call this the *rational* Tate module.

We know that the class number of A is finite, so $\mathfrak{p}^m$ is a principal ideal for some $m > 0$. Let a be a generator of $\mathfrak{p}^m$. Then we have

$$T_\mathfrak{p}(\phi) \cong \varprojlim_i \phi[a^i]$$

revealing once more a tight analogy with the elliptic curve setting.

Proposition 1.17. *Let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module of rank r and let $\mathfrak{p}$ be a prime ideal in A different from the characteristic of K. Then*

(1) *$T_\mathfrak{p}(\phi)$ is a free $A_\mathfrak{p}$-module of rank r,*
(2) *the absolute Galois group G_K acts continuously on $T_\mathfrak{p}(\phi)$.*

Proof. This follows from Proposition 1.14. □

Associated to the Galois action on $T_\mathfrak{p}(\phi)$, we get a Galois representation

$$\rho_\mathfrak{p} : G_K \longrightarrow \mathrm{Aut}_{A_\mathfrak{p}}\big(T_\mathfrak{p}(\phi)\big) \cong \mathrm{GL}_r(A_\mathfrak{p})$$

on the $\mathfrak{p}$-adic Tate module. Modulo $\mathfrak{p}$, it induces the residual representation

$$\overline{\rho_\mathfrak{p}} : G_K \longrightarrow \mathrm{Aut}_{k_\mathfrak{p}}\big(\phi[\mathfrak{p}]\big) \cong \mathrm{GL}_r(k_\mathfrak{p})$$

where $k_\mathfrak{p}$ is the residue field of A at $\mathfrak{p}$. The first representation is relatively well known (cf. Section 2); the latter is the main object of study in this chapter.

Now let $P : \phi \to \phi'$ be a morphism of Drinfeld A-modules. Then P induces a G_K-equivariant homomorphism $\phi[\mathfrak{a}] \to \phi'[\mathfrak{a}]$ for every ideal $\mathfrak{a}$ in A, and a G_K-equivariant homomorphism $\phi[\mathfrak{p}^\infty] \to \phi'[\mathfrak{p}^\infty]$ for every prime ideal $\mathfrak{p}$. We therefore have a natural group homomorphism

$$\mathrm{Hom}_K(\phi, \phi') \longrightarrow \mathrm{Hom}_{A_\mathfrak{p}[G_K]}\big(T_\mathfrak{p}(\phi), T_\mathfrak{p}(\phi')\big)$$

for every prime $\mathfrak{p}$ in A. We shall see below (Remark 1.22) that this is in fact a homomorphism of A-modules. The image of a morphism P under this map is denoted by $T_{\mathfrak{p}}P$. We have already encountered such a homomorphism in connection with the Tate conjecture for abelian varieties, and we shall state a Tate conjecture for Drinfeld modules in Section 2. We shall come across this map on several occasions.

Morphisms of Drinfeld Modules. Next we need to collect some important properties of morphisms and isogenies of Drinfeld modules. We start with two definitions.

Definition 1.18.

(1) Let $P : \phi \to \phi'$ be an isogeny of Drinfeld A-modules and assume that ϕ, ϕ' and P are defined over K. Then we call P *separable* if it has the form $P(\tau) = \sum_{i=0}^{n} c_i \tau^i$ with $c_0 \neq 0$.

(2) Let $P : \phi \to \phi'$ be a separable isogeny of Drinfeld A-modules. Then $\ker P$ is a finite A-module, hence of the form $\bigoplus_{i=1}^{t} A/\mathfrak{a}_i$ for suitable $t > 0$ and ideals $\mathfrak{a}_i \subset A$. The *degree* of P is defined to be the ideal $\deg P = \prod_{i=1}^{t} \mathfrak{a}_i \subset A$.

Recall that for an elliptic curve we have the concept of dual isogenies, i. e. for an isogeny of elliptic curves there exists an isogeny in the reverse direction such that their composition is multiplication by an integer. We recover a weak analog of this concept for Drinfeld modules.

Proposition 1.19. *Let $P : \phi \to \phi'$ be a separable isogeny of Drinfeld A-modules, and let $a \in A$ be a nonzero element which annihilates $(\ker P)(\overline{K})$. Then there exists an isogeny $\widehat{P} : \phi' \to \phi$ such that*

$$\widehat{P} \circ P = \phi_a \quad \textit{and} \quad \big(\ker \widehat{P}\big)(\overline{K}) = P\big(\phi[a](\overline{K})\big),$$
$$P \circ \widehat{P} = \phi'_a \quad \textit{and} \quad \big(\ker P\big)(\overline{K}) = \widehat{P}\big(\phi'[a](\overline{K})\big).$$

Proof. The construction of P with the first two properties is explained in Deligne-Husemöller [**8**] 4.1. Then note that

$$P \circ \widehat{P} \circ P = P \circ \phi_a = \phi'_a \circ P.$$

Canceling P on the right yields the third property. The equation for $\ker P$ follows by symmetry. □

Remark 1.20. Let $P : \phi \to \phi'$ be an isogeny of Drinfeld A-modules.

(1) Clearly $(\ker P)(\overline{K})$ is a finite A-module. Hence there always exists some $a \in A$ which annihilates the kernel of P.

(2) If P is a separable isogeny, then $\widehat{P}$ can be chosen to be separable as well.

The field of definition of a morphism of Drinfeld A-modules over K cannot become arbitrarily large. In fact, every morphism is defined over a finite separable algebraic extension of K:

Proposition 1.21. *Let ϕ, ϕ' be two Drinfeld A-modules over K and let L be an arbitrary extension field of K^{sep}. Then the inclusion*

$$\mathrm{Hom}_{K^{\mathrm{sep}}}(\phi, \phi') \hookrightarrow \mathrm{Hom}_L(\phi, \phi')$$

is an equality.

Proof. Goss [**13**] Proposition 4.7.4 and Remark 4.7.5. □

We have given some properties of individual morphisms of Drinfeld modules. Now we come to the structure of the endomorphism ring.

Remark 1.22. Let ϕ and ϕ' be Drinfeld A-modules over K. Then we have a canonical inclusion

$$A \hookrightarrow \mathrm{End}_K(\phi),$$

and $\mathrm{Hom}_K(\phi, \phi')$ carries a natural structure of A-module.

Indeed, since $\phi(A) \subset K\{\tau\}$ is commutative, for every $a \in A$ the polynomial ϕ_a is an endomorphism of ϕ. Furthermore, A acts on $\mathrm{Hom}_K(\phi, \phi')$ via $(a, P) \mapsto P \circ \phi_a$ for $a \in A$ and $P \in \mathrm{Hom}_K(\phi, \phi')$. It is immediate that the action of A via ϕ', defined as $(a, P) \mapsto \phi'_a \circ P$, yields the same A-module structure.

Proposition 1.23. *Let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module of rank r. Then*

(1) $\mathrm{End}_K(\phi)$ *is a projective A-module of rank not exceeding r^2,*
(2) $\mathrm{End}_K(\phi) \otimes_A F$ *is a finite dimensional division algebra over F.*

Proof. (1) Drinfeld [**9**] Proposition 2.4. (2) This follows from Proposition 1.19: For every endomorphism α of ϕ there exists a dual endomorphism $\widehat{\alpha}$ such that $\widehat{\alpha}\alpha = \phi_a$ for some $a \in A$. Hence, when tensored with F, every nonzero endomorphism becomes invertible. □

We end this paragraph on morphisms with a deep result which is due to Yuichiro Taguchi. It is the isogeny conjecture for Drinfeld modules. Taguchi's proof uses methods similar to the ones invented by Gerd Faltings for the proof of the Šafarevič conjecture for abelian varieties.

In Taguchi's papers, the proof of the isogeny conjecture is the main part of a proof of the semisimplicity conjecture for Drinfeld modules (see below).

Theorem 1.24 (Isogeny conjecture for Drinfeld modules)**.** *Up to K-isomorphism, there are only finitely many Drinfeld A-modules ϕ' for which there exists a separable K-isogeny $\phi \to \phi'$ of degree not divisible by the characteristic of ϕ.*

Proof. Taguchi [**35**] Theorem 0.2 in special characteristic, Taguchi [**39**] in generic characteristic. □

Remark 1.25. In generic characteristic every isogeny of Drinfeld A-modules is separable. Therefore in this case Theorem 1.24 can be stated in the familiar form that the number of isomorphism classes in an isogeny class of Drinfeld A-modules is finite.

Reduction Theory. Given an elliptic curve over a local field and a Weierstrass equation with coefficients in the valuation ring, one can reduce the equation modulo the maximal ideal. The reduced equation may or may not define a nonsingular elliptic curve over the residue field. We refer to these cases as good and bad reduction, respectively.

In our context, reduction theory is important with respect to the criterion of Néron-Ogg-Šafarevič. It states that an elliptic curve has good reduction if and only if the Galois action on the Tate module is unramified. Again, we recover the very same situation for Drinfeld modules.

Let x be a closed point of $\mathcal{X}$. Then x gives rise to a valuation v_x on K. Let $\mathcal{O}_x \subset K$ be the valuation ring of v_x and $\mathfrak{m}_x$ its maximal ideal. By $k_x = \mathcal{O}_x/\mathfrak{m}_x$ we denote its residue field and by $R_x : \mathcal{O}_x \to k_x$ the reduction map. We assume that $\iota(A) \subset \mathcal{O}_x$, then k_x is an A-field via $R_x \circ \iota$.

The twisted polynomial ring $\mathcal{O}_x\{\tau\}$ over the valuation ring $\mathcal{O}_x$ is defined in the obvious way. To a ring homomorphism

$$\psi : A \longrightarrow \mathcal{O}_x\{\tau\}$$

we associate its reduction modulo $\mathfrak{m}_x$, which is the ring homomorphism

$$\psi^x : A \longrightarrow k_x\{\tau\}$$

defined as follows: For $a \in A$ and ψ_a written as $\psi_a(\tau) = \sum_{i=0}^n c_i \tau^i$, we set

$$\psi_a^x(\tau) = \sum_{i=0}^n R_x(c_i)\tau^i.$$

Definition 1.26. Let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module of rank r and let x be a closed point of $\mathcal{X}$. We say that

(1) ϕ has *stable reduction* at x if there exists a Drinfeld A-module ϕ' isomorphic to ϕ such that $\phi'(A) \subset \mathcal{O}_x\{\tau\}$ and such that the reduction of ϕ' modulo $\mathfrak{m}_x$ is a Drinfeld A-module over k_x,

(2) ϕ has *good reduction* at x if ϕ has stable reduction at x and the reduction of ϕ' modulo $\mathfrak{m}_x$ has rank r.

As the next proposition explicates, every Drinfeld module over K is close to falling in one of these two categories.

Proposition 1.27. *Every Drinfeld A-module ϕ over K has potentially stable reduction at x, i. e. there exists a finite field extension K'/K such that ϕ as a Drinfeld A-module over K' has stable reduction at x.*

Proof. Drinfeld [**9**] Proposition 7.1. □

We are now going to formulate the criterion of Néron-Ogg-Šafarevič for Drinfeld modules. Let $\mathfrak{p}$ be a prime ideal in A, and let x be a closed point of $\mathcal{X}$. We say that the G_K-module $T_{\mathfrak{p}}(\phi)$ is *unramified* at x if the inertia subgroup of G_K at x acts trivially on $T_{\mathfrak{p}}(\phi)$.

Theorem 1.28 (Criterion of Néron-Ogg-Šafarevič)**.** *Let x be a closed point of $\mathcal{X}$ and let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module.*

Then ϕ has good reduction at x if and only if the G_K-module $T_\mathfrak{p}(\phi)$ is unramified at x for any prime $\mathfrak{p}$ in A different from the characteristic of k_x.

Proof. Takahashi [**40**] Theorem 1. □

2. Galois Representations on the Tate Module

In this section, we give more details on Galois representations on the Tate module of a Drinfeld module. Essentially, it contains a compilation of well-known results from the literature. Much of the material should be familiar from the theory of elliptic curves. Among others, it covers analogs of famous results due to Jean-Pierre Serre (cf. [**31**]) and Gerd Faltings (cf. [**11**]). The theorems presented here will prove eminent importance for the sequel.

In the following, let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module defined over K.

Let us begin with the semisimplicity conjecture. Proved for abelian varieties over number fields by Gerd Faltings, its version for Drinfeld modules is due to Yuichiro Taguchi.

Theorem 2.1. *Let $\mathfrak{p}$ be a prime of A, different from the characteristic of ϕ. Then the $F_\mathfrak{p}[G_K]$-module $V_\mathfrak{p}(\phi)$ is semisimple.*

Proof. Taguchi [**35**] Theorem 0.1 in special characteristic, Taguchi [**36**] Theorem 0.1 in generic characteristic. □

We also have a version of the Tate conjecture for Drinfeld modules. Proofs of it have been given independently by Akio Tamagawa and Yuichiro Taguchi. Both of them work in a much more general setting, namely with A-premotives (Tamagawa) and ϕ-modules (Taguchi). These include the case of A-motives needed in Chapter II. For the time being, we only state a "small" version of the result for Drinfeld modules.

Theorem 2.2 (Tate conjecture for Drinfeld modules)**.** *Let ϕ_1 and ϕ_2 be two Drinfeld A-modules over K. Then for all primes $\mathfrak{p}$ of A, different from the characteristic of K, the natural map*

$$\mathrm{Hom}_K(\phi_1, \phi_2) \otimes_A A_\mathfrak{p} \longrightarrow \mathrm{Hom}_{A_\mathfrak{p}[G_K]}\big(T_\mathfrak{p}(\phi_1), T_\mathfrak{p}(\phi_2)\big)$$

is an isomorphism.

Proof. Taguchi [**38**] (0.1) or Tamagawa [**41**]. A sketch of Tamagawa's proof is also given in Tamagawa [**42**] §3 and [**43**] §3. □

From these two theorems, we can deduce another important result on the structure of the Tate module. Although it will not be used in this work, it is included because it parallels Theorem 3.1 below.

Theorem 2.3. *Assume that* $\mathrm{End}_K(\phi) = A$. *Then the representation*

$$\rho_{\mathfrak{p}} : G_K \longrightarrow \mathrm{Aut}_{A_{\mathfrak{p}}}\big(V_{\mathfrak{p}}(\phi)\big)$$

is absolutely irreducible for all primes $\mathfrak{p}$ *of* A *different from the characteristic of* ϕ.

Proof. Combine Theorem 2.1 and Theorem 2.2. □

We are also interested in the size of the image of Galois under the representation on the Tate module. Jean-Pierre Serre showed that for an elliptic curve without complex multiplication, the image of Galois under the associated representation is open in $\mathrm{Aut}(T_\ell)$.

The analogous problem for Drinfeld modules has been studied by Richard Pink. He proved that openness of the image of Galois holds for Drinfeld modules without non-scalar endomorphisms in generic characteristic. For Drinfeld modules in special characteristic, the result necessarily is weaker:

Theorem 2.4. *Assume that* $\mathrm{End}_{\overline{K}}(\phi) = A$. *Then the image of* $\rho_{\mathfrak{p}}$ *is Zariski dense in* $\mathrm{GL}_{r,F_{\mathfrak{p}}}$ *for all primes* $\mathfrak{p}$ *of* A *different from the characteristic of* ϕ.

Proof. Pink [**25**] Theorem 0.1 in generic characteristic, Pink [**26**] in special characteristic. □

Studying Galois representations, one sooner or later will encounter Frobenius elements, which play a very important role. By Čebotarev's theorem they are known to form a dense subset of G_K. Here we give information on their characteristic polynomials on the Tate module.

Proposition 2.5. *Let* $\mathfrak{p}$ *be a prime of* A *different from the characteristic of* ϕ. *Then for every closed point* $x \in \mathcal{X}$ *in which* ϕ *has good reduction, the characteristic polynomial of* $\rho_{\mathfrak{p}}(\mathrm{Frob}_x)$ *has coefficients in* A *and is independent of* $\mathfrak{p}$.

Proof. Cf. Goss [**13**] 4.12.12 (2). □

Next, we can give a characterization of the Galois invariant submodules of the $\mathfrak{p}$-power torsion of a Drinfeld module.

Recall that every endomorphism of ϕ naturally induces a G_K-equivariant endomorphism of the torsion modules $\phi[\mathfrak{p}^n]$.

Proposition 2.6. *For almost all primes* $\mathfrak{p}$ *of* A *and all* $n > 0$, *every* G_K*-invariant* $A/\mathfrak{p}^n$*-submodule of* $\phi[\mathfrak{p}^n]$ *has the form* $\alpha(\phi[\mathfrak{p}^n])$ *for some* $\alpha \in \mathrm{End}_K(\phi)$.

Proof. Let $\mathfrak{p}_0$ be the characteristic of ϕ. By the isogeny conjecture for Drinfeld modules (Theorem 1.24), there are only finitely many isomorphism classes of Drinfeld A-modules over K admitting a separable isogeny to ϕ of degree not divisible by $\mathfrak{p}_0$. We choose a set of representatives ϕ^i for $1 \leq i \leq t$ of these isomorphism classes, together with separable isogenies

$$\varepsilon_i : \phi^i \longrightarrow \phi$$

of degree not divisible by $\mathfrak{p}_0$. Let S be the finite set of all primes of A that divide the degree of one of these isogenies.

Assume that we are given a prime $\mathfrak{p}$ of A outside $S \cup \{\mathfrak{p}_0\}$ and a positive integer n, and let

$$H_\mathfrak{p} \subset \phi[\mathfrak{p}^n]$$

be a G_K-invariant $A/\mathfrak{p}^n$-submodule. Then there exists a Drinfeld A-module $\phi^\mathfrak{p}$ over K and a separable K-isogeny

$$\eta_\mathfrak{p} : \phi \longrightarrow \phi^\mathfrak{p}$$

with kernel $H_\mathfrak{p}$ (cf. Deligne-Husemöller [**8**] 4.1). Clearly the degree of $\eta_\mathfrak{p}$ is not divisible by $\mathfrak{p}_0$. Further, there is an isomorphism

$$\lambda : \phi^\mathfrak{p} \xrightarrow{\sim} \phi^i$$

for some i, and by assumption $\mathfrak{p}$ does not divide the degree of ε_i. The composite morphism

$$\alpha = \varepsilon_i \circ \lambda \circ \eta_\mathfrak{p}$$

is an endomorphism of ϕ. Now pick a nonzero $a \in A$ that annihilates $\phi[\mathfrak{p}^n]$ and the kernel of α. By Proposition 1.19 there exists an endomorphism $\widehat{\alpha}$ of ϕ such that

$$\alpha \circ \widehat{\alpha} = \phi_a \quad \text{and} \quad \big(\ker \alpha\big)(\overline{K}) = \widehat{\alpha}\big(\phi[a](\overline{K})\big).$$

Therefore, restricting the endomorphism of $\phi[a]$ induced by $\widehat{\alpha}$ to $\phi[\mathfrak{p}^n]$, we see that its image in $\phi[\mathfrak{p}^n]$ is the kernel of α on $\phi[\mathfrak{p}^n]$ and hence equals $H_\mathfrak{p}$. $\square$

By Serre's results, the p-torsion of an elliptic curve without complex multiplication is known to be an irreducible Galois module for almost all primes $p \in \mathbb{Z}$. The corresponding assertion for Drinfeld modules is one of the useful consequences of the preceding proposition.

Corollary 2.7. *Assume that* $\mathrm{End}_K(\phi) = A$. *Then the representation* $\overline{\rho_\mathfrak{p}}$ *is irreducible for almost all primes* $\mathfrak{p}$ *of* A.

Proof. Proposition 2.6 tells us that for almost all $\mathfrak{p}$ every G_K-invariant submodule of $\phi[\mathfrak{p}]$ is the image of a polynomial map ϕ_a for some $a \in A$. Since $\mathfrak{p}$ is a prime ideal, we either have $\mathfrak{p}|a$, then $\phi[a] \supset \phi[\mathfrak{p}]$ and ϕ_a vanishes on $\phi[\mathfrak{p}]$. Or $\phi[a]$ and $\phi[\mathfrak{p}]$ have zero intersection and ϕ_a is an automorphism of $\phi[\mathfrak{p}]$. Hence the only G_K-invariant submodules of $\phi[\mathfrak{p}]$ are the trivial ones. $\square$

Finally, to complete this survey, we have a glance at the action of inertia on the Tate module of a Drinfeld module in special characteristic:

Proposition 2.8. *Assume that* ϕ *has special characteristic* $\mathfrak{p}_0$. *After replacing* K *by a suitable finite extension, for all primes* $\mathfrak{p}$ *of* A *different from* $\mathfrak{p}_0$ *and for all closed points* $x \in \mathcal{X}$, *the restriction of* $\rho_\mathfrak{p}$ *to the inertia group at* x *is unipotent.*

Proof. First we note the following: The fact that ϕ has special characteristic $\mathfrak{p}_0$ implies that for all closed points x in $\mathcal{X}$ the residue field k_x, as an A-field, has special characteristic $\mathfrak{p}_0$ as well.

Let $\mathfrak{p}$ be a prime of A different from $\mathfrak{p}_0$. Then the criterion of Néron-Ogg-Šafarevič (Theorem 1.28) yields that if ϕ has good reduction at a place $x \in \mathcal{X}$, then the inertia group at x operates trivially on $T_\mathfrak{p}(\phi)$. So we choose $x \in \mathcal{X}$ at which ϕ has bad reduction.

We consider the Tate uniformisation (ψ, Γ) of ϕ, where ψ is a Drinfeld module of rank $r' < r$ over K_x which has potentially good reduction, and Γ is an A-lattice in K_x^{sep} via ψ of rank $r - r'$ with G_{K_x}-action (cf. Drinfeld [**9**] §7).

Replacing K by a finite extension, we can achieve that ψ has good reduction at x. Then the inertia group at x acts trivially on $T_\mathfrak{p}(\psi)$.

Because Γ is discrete and finitely generated, all its generators are contained in a finite extension of K_x. Replacing K_x by this extension, we make sure that G_{K_x} operates trivially on Γ.

Now let us put together these pieces. For all $n > 0$, we have the short exact sequence

$$0 \to \psi[\mathfrak{p}^n] \to \phi[\mathfrak{p}^n] \to \Gamma/\mathfrak{p}^n\Gamma \to 0.$$

Since the inertia group at x operates trivially on the first term and on the third term, the operation on the second term is unipotent.

Finally, there is only a finite number of points on $\mathcal{X}$ where ϕ has bad reduction, so there exists a finite extension of K for which all K_x are large enough and over which the restriction of $\rho_\mathfrak{p}$ to the inertia group at x becomes unipotent for all closed points $x \in \mathcal{X}$. □

3. Absolute Irreducibility of the Residual Representation

So far we have given some fundamentals on Drinfeld modules and a review of properties of the Galois representations on Tate modules of Drinfeld modules. Having completed these preparations, we get to the main parts of this thesis. At its core we encounter residual representations on the $\mathfrak{p}$-adic Tate module of a Drinfeld module modulo $\mathfrak{p}$, which will be the subject for the remainder of Chapter I. Therefor, we shall only consider the case of special characteristic. First, we investigate residual representations associated to a Drinfeld module without non-scalar endomorphisms.

From now on and for the rest of this treatise, we assume that K is a global A-field of special characteristic $\mathfrak{p}_0$ and we let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module over K. By r we denote its rank. In the present section, ϕ is required to satisfy the condition $\mathrm{End}_{\overline{K}}(\phi) = A$. Our aim is to prove the following theorem:

Theorem 3.1. *For almost all primes $\mathfrak{p}$ of A the representation*

$$\overline{\rho_\mathfrak{p}} : G_K \longrightarrow \mathrm{Aut}_{k_\mathfrak{p}}\big(\phi[\mathfrak{p}]\big)$$

is absolutely irreducible.

It is sufficient to prove Theorem 3.1 for the restriction of $\overline{\rho_{\mathfrak{p}}}$ to an open subgroup of G_K, so we can replace K by a finite field extension. We do replace K by the finite extension, given by Proposition 2.8, over which for all $\mathfrak{p} \neq \mathfrak{p}_0$ and all closed points x on $\mathcal{X}$, the restriction of $\rho_{\mathfrak{p}}$ to the inertia group at x is unipotent.

In Corollary 2.7 we have seen that for almost all primes $\mathfrak{p}$ of A the residual representation $\overline{\rho_{\mathfrak{p}}}$ is irreducible. By Schur's lemma, for these primes the ring $\mathrm{End}_{k_{\mathfrak{p}}}(\overline{\rho_{\mathfrak{p}}})$ is a finite dimensional division algebra over the residue field $k_{\mathfrak{p}}$. Since $k_{\mathfrak{p}}$ is finite, every finite dimensional division algebra over $k_{\mathfrak{p}}$ is a commutative field. The degree of this extension field, denoted by $s_{\mathfrak{p}}$, must divide r. We denote the extension field by $k_{\mathfrak{p},s_{\mathfrak{p}}}$.

For $s|r$ let S_s be the set of all primes $\mathfrak{p}$ for which $\overline{\rho_{\mathfrak{p}}}$ is irreducible and $s_{\mathfrak{p}} = s$. In order to develop an indirect proof of Theorem 3.1, we make the following

Assumption 3.2. There exists $s > 1$ such that S_s is infinite.

This is equivalent to the assumption that $\overline{\rho_{\mathfrak{p}}}$ is irreducible but not absolutely irreducible for an infinite number of primes $\mathfrak{p}$. We fix such s and put $t = \frac{r}{s}$.

For $\mathfrak{p} \in S_s$ we may consider $\overline{\rho_{\mathfrak{p}}}$ as a map $G_K \to \mathrm{GL}_t(k_{\mathfrak{p},s})$. We write $\det_s$ for the determinant map

$$\det{}_s : \mathrm{GL}_t\big(k_{\mathfrak{p},s}\big) \longrightarrow k_{\mathfrak{p},s}^*$$

and $\overline{\chi_{\mathfrak{p}}}$ for the character which arises from the composition

$$\overline{\chi_{\mathfrak{p}}} = \det{}_s \circ \overline{\rho_{\mathfrak{p}}} : G_K \longrightarrow k_{\mathfrak{p},s}^*.$$

In a first lemma, we extend K such that whenever $\overline{\rho_{\mathfrak{p}}}$ is not absolutely irreducible, the induced character $\overline{\chi_{\mathfrak{p}}}$ comes from a character of the absolute Galois group of the constant field k_0.

Lemma 3.3. *There is a finite field extension K'/K such that for every prime $\mathfrak{p} \in S_s$ the representation $\overline{\chi_{\mathfrak{p}}}|_{G_{K'}}$ factors through a map $\overline{\overline{\chi_{\mathfrak{p}}}} : G_{k_0} \to k_{\mathfrak{p},s}^*$.*

Proof. By Proposition 2.8, for all closed points $x \in \mathcal{X}$ the inertia subgroup of G_K at x has trivial image in $k_{\mathfrak{p},s}^*$, so $\overline{\chi_{\mathfrak{p}}}$ is unramified everywhere. This means that $\overline{\chi_{\mathfrak{p}}}$ factors through $\mathrm{Gal}(K^{\mathrm{nr}}/K)$. Moreover, it obviously factors through the maximal abelian quotient $\mathrm{Gal}(K^{\mathrm{ab,nr}}/K)$.

Let $\mathbb{A}_K$ be the ring of adèles of K. For any group G, we denote its profinite completion by $\widehat{G}$. By class field theory the Galois group of the maximal abelian extension and of the maximal unramified abelian extension of K are known:

$$\mathrm{Gal}\big(K^{\mathrm{ab}}/K\big) \cong \big(\mathbb{A}_K^*/K^*\big)^{\widehat{}},$$
$$\mathrm{Gal}\big(K^{\mathrm{ab,nr}}/K\big) \cong \Big(\mathbb{A}_K^*/K^* \prod_{x\in\mathcal{X}} \mathcal{O}_x^*\Big)^{\widehat{}}.$$

We want to determine the intermediate field $K \subset K\overline{k_0} \subset K^{\mathrm{ab,nr}}$. In order to describe the Galois groups of these field extensions, we define a homomorphism $\mathbb{A}_K^* \to \mathbb{Z}$ by

$$(c_x)_{x\in\mathcal{X}} \longmapsto \frac{\log \|(c_x)_{x\in\mathcal{X}}\|}{\log |k_0|} = \sum_{x\in\mathcal{X}} \mathrm{ord}_x(c_x) \cdot [k_x : k_0]$$

and let $\mathbb{A}_K^1$ be the subgroup of the idèle group $\mathbb{A}_K^*$ which is defined by the short exact sequence

$$1 \to \mathbb{A}_K^1 \to \mathbb{A}_K^* \to \mathbb{Z} \to 0$$

with the homomorphism $\mathbb{A}_K^* \to \mathbb{Z}$ defined above. As an immediate consequence of the product formula for the valuations of K we have the inclusion

$$K^* \prod_{x \in \mathcal{X}} \mathcal{O}_x^* \subset \mathbb{A}_K^1.$$

Standard results on the idèle class group yield that $\mathbb{A}_K^1/K^*$ is a compact group, hence the quotient

$$\mathbb{A}_K^1 \Big/ K^* \prod_{x \in \mathcal{X}} \mathcal{O}_x^*$$

is finite. Now in the short exact sequence for $\mathbb{A}_K^1$ and $\mathbb{A}_K^*$ we can divide out the subgroup $K^* \prod_{x \in X} \mathcal{O}_x^*$ and take the profinite completion. The sequence then transforms into a short exact sequence

$$1 \to \mathbb{A}_K^1 \Big/ K^* \prod_{x \in \mathcal{X}} \mathcal{O}_x^* \to \Big(\mathbb{A}_K^* \Big/ K^* \prod_{x \in \mathcal{X}} \mathcal{O}_x^*\Big)^{\widehat{}} \to \widehat{\mathbb{Z}} \to 0.$$

The middle term is isomorphic to the Galois group of $K^{\mathrm{ab,nr}}/K$, and $\widehat{\mathbb{Z}}$ is isomorphic to the Galois group of $K\overline{k_0}/K$. The first term is a finite group and must be isomorphic to the Galois group of $K^{\mathrm{ab,nr}}/K\overline{k_0}$. Therefore we can choose a finite extension field K' of K in $K^{\mathrm{ab,nr}}$ such that

$$K'\overline{k_0} = K^{\mathrm{ab,nr}} \quad \text{and} \quad K' \cap K\overline{k_0} = K.$$

Then we have

$$\mathrm{Gal}\big(K^{\mathrm{ab,nr}}/K'\big) = \mathrm{Gal}\big(K'\overline{k_0}/K'\big) \cong G_{k_0},$$

and it follows that the restriction of the character $\overline{\chi_{\mathfrak{p}}}$ to $G_{K'}$ factors through G_{k_0}:

$$\begin{tikzcd}
G_K \arrow[rr, "\overline{\chi_{\mathfrak{p}}}"] \arrow[dr] & & k_{\mathfrak{p},s}^* \\
\cup & \mathrm{Gal}\big(K^{\mathrm{ab,nr}}/K\big) \arrow[ur] & \\
G_{K'} \arrow[dr] & \cup & \\
& \mathrm{Gal}\big(K^{\mathrm{ab,nr}}/K'\big) \arrow[uuur] &
\end{tikzcd}$$

This proves the claim. $\square$

We replace K by the extension field K' constructed in Lemma 3.3. Since we may apply Corollary 2.7 (irreducibility of $\overline{\rho_{\mathfrak{p}}}$ at almost all $\mathfrak{p}$) over K', by this replacement the representation $\overline{\rho_{\mathfrak{p}}}$ has become reducible for at most finitely many primes $\mathfrak{p} \in S_s$. We remove these primes from S_s.

For the sake of clearness we pause for a moment and try to keep track of our definitions. In the following commutative diagram with exact rows we sum up the various mappings:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}\big(K^{\mathrm{sep}}/K\overline{k_0}\big) \arrow[r] \arrow[d] & G_K \arrow[r] \arrow[d, "\overline{\rho_{\mathfrak{p}}}"'] \arrow[dr, "\overline{\chi_{\mathfrak{p}}}"] & G_{k_0} \arrow[r] \arrow[d, "\overline{\overline{\chi_{\mathfrak{p}}}}"] & 1 \\
1 \arrow[r] & \mathrm{SL}_t\big(k_{\mathfrak{p},s}\big) \arrow[r] \arrow[d, hook] & \mathrm{GL}_t\big(k_{\mathfrak{p},s}\big) \arrow[r, "\det_s"'] \arrow[d, hook] & k_{\mathfrak{p},s}^* \arrow[r] \arrow[d, "\mathrm{Norm}"] & 1 \\
1 \arrow[r] & \mathrm{SL}_r\big(k_{\mathfrak{p}}\big) \arrow[r] & \mathrm{GL}_r\big(k_{\mathfrak{p}}\big) \arrow[r, "\det"] & k_{\mathfrak{p}}^* \arrow[r] & 1
\end{tikzcd}$$

Remember that this diagram exists for every prime $\mathfrak{p}$ in S_s. The fact that the upper right square is commutative, together with Assumption 3.2, turns out to have consequences for the the zeros of the characteristic polynomials of Frobenius elements in G_K.

As a tool for the study of several zeros of a polynomial at a time, we introduce a polynomial P_m that we associate to polynomials with coefficients in A and its residue fields. It also will help comparing zeros of several polynomials.

Definition 3.4. Let R be an integral domain and f a monic polynomial of degree ℓ with coefficients in R. By $\alpha_1, \ldots, \alpha_\ell$ we denote the zeros of f in an algebraic closure of the quotient field of R. Let T be an indeterminate. For $1 \leq m \leq \ell$ we define

$$P_m(f, T) = \prod_I \Big(T - \prod_{i \in I} \alpha_i \Big)$$

where the first product ranges over all subsets $I \subset \{1, \ldots, \ell\}$ of cardinality m.

Since $P_m(f, T)$ is symmetric as a function in the zeros of f, it can be written as a polynomial over $\mathbb{Z}[T]$ in elementary symmetric functions on these zeros. Hence $P_m(f, T)$ is a polynomial in the coefficients of f. Obviously, for α in the algebraic closure of $\mathrm{Quot}(R)$, we have $P_m(f, \alpha) = 0$ if and only if f has m zeros with product α.

In the following, let $\mathcal{X}^{\mathrm{good}}$ be the open subscheme of $\mathcal{X}$ over which ϕ has good reduction. For every closed point $x \in \mathcal{X}^{\mathrm{good}}$, let us denote the characteristic polynomial of $\rho_{\mathfrak{p}}(\mathrm{Frob}_x)$ by f_x. It has coefficients in A and is independent of $\mathfrak{p}$ (Proposition 2.5).

In the next lemma, we use Assumption 3.2 that S_s is infinite. It shows that t-fold products of eigenvalues of Frobenius elements are related one with another.

Lemma 3.5. *For all $d > 0$ and all $x, x' \in \mathcal{X}^{\mathrm{good}}(k_{0,d})$ the resultant of the polynomials $P_t(f_x, T)$ and $P_t(f_{x'}, T)$ vanishes.*

Proof. Let $\mathfrak{p} \in S_s$. By Lemma 3.3, we know that

$$\overline{\chi_{\mathfrak{p}}}\big(\mathrm{Frob}_x\big) = \overline{\overline{\chi_{\mathfrak{p}}}}\big(\mathrm{Frob}_{k_0}^d\big) = \overline{\chi_{\mathfrak{p}}}\big(\mathrm{Frob}_{x'}\big).$$

So the determinants of $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_x)$ and $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_{x'})$ over $k^*_{\mathfrak{p},s}$ are equal. Thus, if we consider $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_x)$ and $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_{x'})$ as elements of $\mathrm{GL}_t(k_{\mathfrak{p},s})$, their characteristic polynomials g_x and $g_{x'}$ have the same constant term. This means that the product of the t zeros of g_x equals the product of the t zeros of $g_{x'}$.

Now the polynomials f_x and $f_{x'}$ are congruent modulo $\mathfrak{p}$ to the characteristic polynomials of $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_x)$ and $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_{x'})$ as elements of $\mathrm{GL}_r(k_{\mathfrak{p}})$, respectively. So g_x and $g_{x'}$ divide f_x and $f_{x'}$ modulo $\mathfrak{p}$, respectively, as polynomials over $\overline{k_{\mathfrak{p}}}$. Therefore $P_t(f_x, T)$ and $P_t(f_{x'}, T)$ must have a common zero modulo $\mathfrak{p}$. Hence their resultant vanishes modulo the infinitely many $\mathfrak{p}$ in S_s. This proves the assertion. □

Now fix some prime $\mathfrak{p}$ in S_s. For $n > 0$ we denote the images of the Galois groups G_K and $\mathrm{Gal}(K^{\mathrm{sep}}/K\overline{k_0})$ under the representation $\rho_{\mathfrak{p}}$ modulo $\mathfrak{p}^n$ by $\Gamma_{\mathfrak{p},n}$ and $\Gamma'_{\mathfrak{p},n}$, respectively. We set $\Gamma''_{\mathfrak{p},n} = \Gamma_{\mathfrak{p},n}/\Gamma'_{\mathfrak{p},n}$. We have the following diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}\big(K^{\mathrm{sep}}/K\overline{k_0}\big) & \longrightarrow & G_K & \longrightarrow & G_{k_0} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \Gamma'_{\mathfrak{p},n} & \longrightarrow & \Gamma_{\mathfrak{p},n} & \longrightarrow & \Gamma''_{\mathfrak{p},n} & \longrightarrow & 1 \\
 & & \cap & & \cap & & & & \\
 & & \mathrm{SL}_r\big(A/\mathfrak{p}^n\big) & & \mathrm{GL}_r\big(A/\mathfrak{p}^n\big) & & & &
\end{array}$$

We define the groups

$$\Gamma_{\mathfrak{p}} \subset \mathrm{GL}_r(A_{\mathfrak{p}}) \quad \text{and} \quad \Gamma'_{\mathfrak{p}} \subset \mathrm{SL}_r(A_{\mathfrak{p}})$$

to be the respective limits of $\Gamma_{\mathfrak{p},n}$ and $\Gamma'_{\mathfrak{p},n}$ for $n \to \infty$.

In the next lemma we bring a second aspect into the picture. In Lemma 3.7 below, it will meet the line of reasoning which has been developed up to Lemma 3.5. This new aspect concerns density of the Frobenius elements.

For our purpose, Čebotarev's theorem is somewhat too weak, because we have to take into account the degree of the Frobenius elements. What we need in fact is yielded by a theorem on the equidistribution of Frobenius elements due to Pierre Deligne.

From Čebotarev's theorem it follows that the Frobenius elements in G_K cover all of $\Gamma'_{\mathfrak{p},n}$. Beyond that we show that Frobenius elements of bounded degree do so. This result is independent of Assumption 3.2.

Lemma 3.6. *For all $n > 0$, there is some $d > 0$ such that every element of $\Gamma'_{\mathfrak{p},n}$ has an inverse image in G_K of the form Frob_x for $x \in \mathcal{X}^{\mathrm{good}}(k_{0,d})$.*

Proof. The essential tool in this proof is Pierre Deligne's equidistribution theorem (see Appendix A.1).

The group $\Gamma''_{\mathfrak{p},n}$ is cyclic; let e be its order. We define K_e to be the composite field $Kk_{0,e}$. Then the image of G_{K_e} under the representation $\rho_{\mathfrak{p}}$ modulo $\mathfrak{p}^n$ is $\Gamma'_{\mathfrak{p},n}$. By $\mathcal{X}^{\mathrm{good}}_e$ we denote the curve $\mathcal{X}^{\mathrm{good}} \times_{k_0} k_{0,e}$.

Let $\overline{x}$ be a fixed geometric point of $\mathcal{X}_e^{\text{good}}$, let $\pi_1(\mathcal{X}_e^{\text{good}}, \overline{x})$ be the arithmetic fundamental group of $\mathcal{X}_e^{\text{good}}$ and

$$\pi_1^{\text{geom}}\big(\mathcal{X}_e^{\text{good}}, \overline{x}\big) = \pi_1\big(\mathcal{X}_e^{\text{good}} \times_{k_{0,e}} \overline{k_{0,e}}, \overline{x}\big)$$

its geometric fundamental group. For every $x \in \mathcal{X}^{\text{good}}$ and all $\mathfrak{p}$ different from the characteristic of ϕ the criterion of Néron-Ogg-Šafarevič (Theorem 1.28) assures that the representations $\rho_{\mathfrak{p}}$ are unramified at x. It follows that $\rho_{\mathfrak{p}}$ factors through $\pi_1(\mathcal{X}_e^{\text{good}}, \overline{x})$. Thus we have the following commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}\big(K^{\text{sep}}/K\overline{k_0}\big) \arrow[r] & G_K \arrow[r] & G_{k_0} \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{Gal}\big(K_e^{\text{sep}}/K_e\overline{k_{0,e}}\big) \arrow[r] \arrow[u, equal] \arrow[d] & G_{K_e} \arrow[r] \arrow[u, phantom, "\cup"] \arrow[d] & G_{k_{0,e}} \arrow[r] \arrow[u, phantom, "\cup"] \arrow[d, equal] & 1 \\
1 \arrow[r] & \pi_1^{\text{geom}}\big(\mathcal{X}_e^{\text{good}}, \overline{x}\big) \arrow[r] \arrow[d] & \pi_1\big(\mathcal{X}_e^{\text{good}}, \overline{x}\big) \arrow[r] \arrow[d] & G_{k_{0,e}} \arrow[r] & 1 \\
& \Gamma'_{\mathfrak{p},n} \arrow[r, equal] & \Gamma'_{\mathfrak{p},n} & &
\end{tikzcd}$$

By $(\Gamma'_{\mathfrak{p},n})^\natural$ we denote the set of conjugacy classes of $\Gamma'_{\mathfrak{p},n}$. On $(\Gamma'_{\mathfrak{p},n})^\natural$ we define a measure μ by

$$\mu(\gamma^\natural) = \frac{|\gamma^\natural|}{|\Gamma'_{\mathfrak{p},n}|}$$

for all conjugacy classes $\gamma^\natural$ in $(\Gamma'_{\mathfrak{p},n})^\natural$. For all $i > 0$ let

$$I_i = \big\{x \in \mathcal{X}_e^{\text{good}}\big(\overline{k_{0,e}}\big) \;\big|\; \deg x = i\big\}.$$

Then we have a sequence of measures ν_i on $(\Gamma'_{\mathfrak{p},n})^\natural$, given by

$$\nu_i = \frac{1}{|I_i|} \sum_{x \in I_i} \delta_{\mathrm{Frob}_x}$$

where δ_{Frob_x} denotes the Dirac measure on $(\Gamma'_{\mathfrak{p},n})^\natural$ supported in the image of Frob_x.

For the application of the equidistribution theorem in Katz' version (Appendix A, Theorem 1.1), we need to pay attention to one more condition: the measures in the theorem only take the semisimple part of the δ_{Frob_x} into account. But $\Gamma'_{\mathfrak{p},n}$ is finite, so we may embed it into $\mathrm{GL}_{m,\overline{\mathbb{Q}}_\ell}$ for some m and some $\ell \neq p$, and elements of finite order in $\mathrm{GL}_{m,\overline{\mathbb{Q}}_\ell}$ are semisimple.

Now the equidistribution theorem asserts that the measures ν_i tend weak-$*$ to μ. Hence for any $\mathbb{C}$-valued function f on $(\Gamma'_{\mathfrak{p},n})^\natural$ we have

$$\int_{(\Gamma'_{\mathfrak{p},n})^\natural} f\,d\mu = \lim_{i\to\infty} \int_{(\Gamma'_{\mathfrak{p},n})^\natural} f\,d\nu_i.$$

Since $(\Gamma'_{\mathfrak{p},n})^\natural$ is finite, there must be some d such that the support of $\sum_{x\in I_d} \delta_{\mathrm{Frob}_x}$ is all of $(\Gamma'_{\mathfrak{p},n})^\natural$. This means that in each conjugacy class of $\Gamma'_{\mathfrak{p},n}$ there is an element which has an inverse image Frob_x with $x \in \mathcal{X}^{\mathrm{good}}(k_{0,d})$. Conjugates of Frobenius elements in $\pi_1(\mathcal{X}_e^{\mathrm{good}}, \overline{x})$ are again Frobenius elements, thus every element of each conjugacy class has such an inverse image. $\square$

Putting together the pieces collected so far, we now can prove, still under Assumption 3.2, that the elements of $\Gamma'_{\mathfrak{p}}$ satisfy an algebraic relation. It then remains to see that this is a nontrivial relation which conflicts with the density of the image of Galois in $\mathrm{GL}_{r,F_{\mathfrak{p}}}$.

Lemma 3.7. *Let $\gamma \in \Gamma'_{\mathfrak{p}}$ and let f_γ be its characteristic polynomial. Then $P_t(f_\gamma, 1)$ vanishes.*

Proof. Let $n > 0$ and choose $d > 0$ as in Lemma 3.6. Then we can find x and x' in $\mathcal{X}^{\mathrm{good}}(k_{0,d})$ such that Frob_x maps to $\gamma \bmod \mathfrak{p}^n$ and $\mathrm{Frob}_{x'}$ to 1 in $\Gamma'_{\mathfrak{p},n}$. We get

$$f_x \equiv f_\gamma \pmod{\mathfrak{p}^n} \quad \text{and} \quad f_{x'} \equiv (T-1)^r \pmod{\mathfrak{p}^n}.$$

Thus

$$P_t(f_x, T) \equiv P_t(f_\gamma, T) \pmod{\mathfrak{p}^n}$$

and

$$P_t(f_{x'}, T) \equiv P_t\big((T-1)^r, T\big) = (T-1)^{\binom{r}{t}} \pmod{\mathfrak{p}^n}$$

By Lemma 3.5 the resultant of

$$P_t(f_x, T) \quad \text{and} \quad P_t(f_{x'}, T)$$

vanishes, hence the resultant of

$$P_t(f_\gamma, T) \quad \text{and} \quad (T-1)^{\binom{r}{t}}$$

is congruent 0 modulo $\mathfrak{p}^n$. Letting $n \to \infty$, it is clear that it must vanish. But this implies that $P_t(f_\gamma, 1) = 0$. $\square$

Before we can conclude the proof of Theorem 3.1, we still need to point out that the commutator morphism on the general linear group is a dominant map to the special linear group.

Proposition 3.8. *The commutator morphism*

$$\begin{array}{rcl} [\,\cdot\,,\,\cdot\,] : \mathrm{GL}_r \times \mathrm{GL}_r & \longrightarrow & \mathrm{SL}_r \\ (x, y) & \longmapsto & [x, y] = yxy^{-1}x^{-1} \end{array}$$

is dominant.

Proof. It is known that the morphism $y \mapsto yxy^{-1}x^{-1}$ for fixed x has differential $1 - \operatorname{Ad} x$. In turn, $x \mapsto \operatorname{Ad} x(Y) - Y$ has differential $-\operatorname{ad} Y$, where $\operatorname{ad} Y(Z)$ is the Lie bracket on $\mathfrak{gl}_r$. (Both results e. g. in Borel [**3**] I 3.16.)

Rather elementary computation shows that the Lie bracket is a surjective morphism $\mathfrak{gl}_r \oplus \mathfrak{gl}_r \to \mathfrak{sl}_r$. But the surjectivity of this differential implies that $[\,\cdot\,,\,\cdot\,]$ is dominant (Springer [**34**] Theorem 4.3.6). □

Proof of Theorem 3.1. By $\mathbb{A}^r_{F_\mathfrak{p}}$ we denote affine r-space over $F_\mathfrak{p}$. Let

$$\psi : \mathrm{GL}_{r,F_\mathfrak{p}} \to \mathbb{A}^r_{F_\mathfrak{p}}$$

be the morphism which maps an element of $\mathrm{GL}_{r,F_\mathfrak{p}}$ to the r-tuple of coefficients of its characteristic polynomial (forgetting the leading one). The image of $\mathrm{SL}_{r,F_\mathfrak{p}}$ under ψ consists precisely of the monic polynomials of degree r with coefficients in $F_\mathfrak{p}$ and constant term $(-1)^r$. It is closed in $\mathbb{A}^r_{F_\mathfrak{p}}$.

For the proof we proceed in three steps:

(1) $\Gamma'_\mathfrak{p}$ *is Zariski dense in* $\mathrm{SL}_{r,F_\mathfrak{p}}$.
Indeed, all commutators of G_K are contained in $\mathrm{Gal}(K^{\mathrm{sep}}/K\overline{k_0})$, so the image of $\Gamma_\mathfrak{p} \times \Gamma_\mathfrak{p}$ under the commutator morphism

$$[\,\cdot\,,\,\cdot\,] : \mathrm{GL}_{r,F_\mathfrak{p}} \times \mathrm{GL}_{r,F_\mathfrak{p}} \to \mathrm{SL}_{r,F_\mathfrak{p}}$$

is contained in $\Gamma'_\mathfrak{p}$. Further $\Gamma_\mathfrak{p}$ is Zariski dense in $\mathrm{GL}_{r,F_\mathfrak{p}}$ by Theorem 2.4. We get

$$\big[\mathrm{GL}_{r,F_\mathfrak{p}}, \mathrm{GL}_{r,F_\mathfrak{p}}\big] = \big[\,\overline{\Gamma_\mathfrak{p}}, \overline{\Gamma_\mathfrak{p}}\,\big] \subset \overline{\big[\Gamma_\mathfrak{p}, \Gamma_\mathfrak{p}\big]} \subset \overline{\Gamma'_\mathfrak{p}}.$$

Proposition 3.8 tells us that $[\,\cdot\,,\,\cdot\,]$ is dominant. Hence

$$\mathrm{SL}_{r,F_\mathfrak{p}} = \overline{\big[\mathrm{GL}_{r,F_\mathfrak{p}}, \mathrm{GL}_{r,F_\mathfrak{p}}\big]} \subset \overline{\Gamma'_\mathfrak{p}} \subset \mathrm{SL}_{r,F_\mathfrak{p}}.$$

(2) $\psi(\Gamma'_\mathfrak{p})$ *is Zariski dense in* $\psi(\mathrm{SL}_{r,F_\mathfrak{p}})$.
This follows from (1):

$$\psi\big(\mathrm{SL}_{r,F_\mathfrak{p}}\big) = \psi\Big(\overline{\Gamma'_\mathfrak{p}}\Big) \subset \overline{\psi(\Gamma'_\mathfrak{p})} \subset \psi\big(\mathrm{SL}_{r,F_\mathfrak{p}}\big).$$

(3) $\psi(\Gamma'_\mathfrak{p})$ *is not Zariski dense in* $\psi(\mathrm{SL}_{r,F_\mathfrak{p}})$.
Indeed, $\psi(\mathrm{SL}_{r,F_\mathfrak{p}})$ clearly is the closed subset of $\psi(\mathrm{GL}_{r,F_\mathfrak{p}})$ which is defined by $P_r(\,\cdot\,,1)$. The polynomial $P_r(\,\cdot\,,1)$ is irreducible and, because there exists f in $\psi(\mathrm{GL}_{r,F_\mathfrak{p}})$ such that $P_r(f,1) = 0$ but $P_t(f,1) \neq 0$, we know that $P_r(\,\cdot\,,1)$ does not divide $P_t(\,\cdot\,,1)$. Hence $P_t(\,\cdot\,,1)$ defines a closed proper subset of $\psi(\mathrm{SL}_{r,F_\mathfrak{p}})$. By Lemma 3.7 this subset contains $\psi(\Gamma'_\mathfrak{p})$.

In view of the contradiction between (2) and (3), Assumption 3.2 turns out to be false, and the theorem is proven. □

4. Endomorphisms of the Residual Representation

So far we have studied the Galois action on the torsion points of a Drinfeld module without non-scalar endomorphisms. Now we want to have a look at Drinfeld modules with more endomorphisms.

Let $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ be a Drinfeld A-module defined over K in special characteristic $\mathfrak{p}_0$. All endomorphisms in $\mathrm{End}_{\overline{K}}(\phi)$ are defined over a finite separable extension K' of K. We may assume that K'/K is a Galois extension. We fix such K' and set

$$E' = \mathrm{End}_{K'}(\phi) = \mathrm{End}_{\overline{K}}(\phi).$$

As E' is a subring of $K^{\mathrm{sep}}\{\tau\}$, the absolute Galois group G_K acts on E'. By construction, the G_K-invariants in E' are precisely the elements of $\mathrm{End}_K(\phi)$.

We set $E = \mathrm{End}_K(\phi)$. For any nonzero ideal $\mathfrak{a} \subset A$ we have natural homomorphisms

$$\sigma : E \longrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{a}]\big) \quad \text{and} \quad \sigma' : E' \longrightarrow \mathrm{End}_{A[G_{K'}]}\big(\phi[\mathfrak{a}]\big).$$

In the present section our attention will be concentrated on these maps. The first part of the description is given by

Proposition 4.1. *For every ideal $\mathfrak{a} \subset A$, prime to the characteristic of ϕ, the homomorphism σ factors through $E/\mathfrak{a}E$ and the induced map*

$$E/\mathfrak{a}E \longrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{a}]\big)$$

is injective.

Proof. Every element of $\mathfrak{a}E$ vanishes on $\phi[\mathfrak{a}]$ because $\mathfrak{a} \subset A$ is central in E and ϕ_a is zero on $\phi[\mathfrak{a}]$ for $a \in \mathfrak{a}$. Thus σ factors through $E/\mathfrak{a}E$.

Conversely, let α be in the kernel of σ. Recall that the image of ϕ in $\mathrm{End}_K(\mathbb{G}_{a,K})$ is contained in the twisted polynomial ring $K\{\tau\}$.

If $\mathfrak{a}$ is a principal ideal, let $a \in \mathfrak{a}$ be a generator. Then ϕ_a generates the left ideal $K\{\tau\} \cdot \{\phi_b \mid b \in \mathfrak{a}\}$ of all polynomials vanishing on $\phi[\mathfrak{a}]$. Because the polynomial α vanishes on $\phi[\mathfrak{a}]$ and because we have a right division algorithm in $K\{\tau\}$, we see that $\alpha = P_0\phi_a$ for some P_0 in $K\{\tau\}$. Both α and ϕ_a are endomorphisms, so P_0 must be an endomorphism of ϕ as well. Hence $\alpha \in \mathfrak{a}E$.

If $\mathfrak{a}$ is not principal, let $a \in \mathfrak{a} \setminus \mathfrak{p}_0$. By the principal ideal case and with the well-known vertical isomorphisms we have the commutative diagram

$$\begin{tikzcd}
E/aE \arrow[r, hook] \arrow[dd, "\wr"] & \mathrm{End}_A\big(\phi[a]\big) \arrow[d, "\wr"] \\
& \mathrm{Mat}_{r\times r}\big(A/(a)\big) \arrow[d, "\wr"] \\
\big(A/(a)\big)^s \arrow[r, hook] & \big(A/(a)\big)^{r^2}
\end{tikzcd}$$

where s is the rank of E over A. Since $(A/(a))^s$ and $(A/(a))^{r^2}$ are free modules, the first is a direct summand of the second. Hence, dividing out $\mathfrak{a}$, the map remains injective. □

Before we complement Proposition 4.1 by this section's main result, as a preparation we note

Remark 4.2. Let Z be the center of $\mathrm{End}_K(\phi)$ and let m be the inseparable degree of Z over A. In a separable extension almost all prime ideals are unramified. Therefore almost all primes $\mathfrak{p}$ in A decompose as $\mathfrak{p} = \prod_{i=1}^{s} \mathfrak{P}_i^m$ with $s > 0$ and pairwise distinct prime ideals $\mathfrak{P}_i$ in Z.

This fact (and notation) will be used permanently. Now we complete the description of the homomorphism σ and, at the same time, determine the A-algebra generated by the image of Galois under the residual representation:

Theorem 4.3 (= Theorem B)**.** *For almost all primes $\mathfrak{p}$ of A and all $n > 0$,*

(1) *the natural map*

$$\mathrm{End}_K(\phi) \longrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}^n]\big)$$

is surjective,

(2) *the image of $A[G_K]$ in $\mathrm{End}_A(\phi[\mathfrak{p}^n])$ is isomorphic to*

$$\bigoplus_{i=1}^{s} \mathrm{Mat}_{e\times e}\big(Z/\mathfrak{P}_i^{mn}\big)$$

with suitable $e > 0$.

Remark 4.4. If d^2 denotes the rank of $\mathrm{End}_K(\phi)$ over Z and r' the rank of the extension of ϕ to a Drinfeld Z-module (see Remark 4.6 below), then the integer e in Theorem 4.3 (2) is $e = \frac{r'}{d}$.

As an immediate consequence of Theorem 4.3, we see that Theorem 3.1 in fact holds in greater generality than proven in Section 3: We can drop the assumption that $\mathrm{End}_K(\phi) = \mathrm{End}_{\overline{K}}(\phi)$.

Corollary 4.5 (= Theorem A)**.** *Assume that $\mathrm{End}_K(\phi) = A$. Then for almost all primes $\mathfrak{p}$ of A the residual representation*

$$\overline{\rho_{\mathfrak{p}}} : G_K \longrightarrow \mathrm{Aut}_{k_{\mathfrak{p}}}\big(\phi[\mathfrak{p}]\big)$$

is absolutely irreducible.

The remainder of the section deals with the proof of the preceding theorem and proposition. Before we tackle this task, we should point out the following

Remark 4.6 (Extension of Drinfeld modules)**.** Let A' be a commutative subring of $\mathrm{End}_K(\phi)$ containing A. It is obvious that the Drinfeld module $\phi : A \to \mathrm{End}_K(\mathbb{G}_{a,K})$ extends to a ring homomorphism $\phi' : A' \to \mathrm{End}_K(\mathbb{G}_{a,K})$. This homomorphism has all properties of a Drinfeld A'-module, except for the fact that A' might be a non-maximal order in its quotient field.

Two approaches to deal with this deficiency can be gained from Hayes [**16**]. In that paper a theory of Drinfeld modules for non-maximal orders is developed, and we could make use of this more general notion of Drinfeld module. However, we choose to follow the second approach which requires less technical effort: By Proposition 3.2 in [**16**] there exists a Drinfeld A-module ψ, isogenous to ϕ, such that the normalization $\tilde{A}'$ of A' is contained in $\mathrm{End}_K(\psi)$.

In the following, when needed, we replace ϕ by such a Drinfeld A-module that extends to a proper Drinfeld $\tilde{A}'$-module. We may do this thanks to

Lemma 4.7. *If Theorem 4.3 holds for one Drinfeld module ϕ, it holds for every Drinfeld module in the isogeny class of ϕ.*

Proof. By hypothesis, for almost all primes $\mathfrak{p}$ in A and all $n > 0$ the monomorphism

$$\mathrm{End}_K(\phi)/\mathfrak{p}^n\,\mathrm{End}_K(\phi) \hookrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}^n]\big)$$

is an isomorphism. Let $\psi \to \phi$ be an isogeny. For all primes $\mathfrak{p}$ it induces a G_K-equivariant homomorphism $\psi[\mathfrak{p}^n] \to \phi[\mathfrak{p}^n]$ which is an isomorphism unless $\mathfrak{p}$ is in the support of the kernel of the isogeny. This isomorphism, in turn, induces an isomorphism

$$\lambda : \mathrm{End}_{A[G_K]}\big(\psi[\mathfrak{p}^n]\big) \xrightarrow{\sim} \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}^n]\big).$$

Hence for almost all $\mathfrak{p}$ and all n we get a commutative diagram

$$\begin{tikzcd}
\mathrm{End}_K(\psi)/\mathfrak{p}^n\,\mathrm{End}_K(\psi) \arrow[r, hook, "\sigma_2"] \arrow[d, "\sigma_1^{-1}\circ\lambda\circ\sigma_2"'] & \mathrm{End}_{A[G_K]}\big(\psi[\mathfrak{p}^n]\big) \arrow[d, "\lambda", "\wr"'] \\
\mathrm{End}_K(\phi)/\mathfrak{p}^n\,\mathrm{End}_K(\phi) \arrow[r, "\sim", "\sigma_1"'] & \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}^n]\big).
\end{tikzcd}$$

As A-modules, $\mathrm{End}_K(\psi)$ and $\mathrm{End}_K(\phi)$ are projective of the same finite rank; therefore for almost all $\mathfrak{p}$ and all n, their quotients

$$\mathrm{End}_K(\psi)/\mathfrak{p}^n\,\mathrm{End}_K(\psi) \quad \text{and} \quad \mathrm{End}_K(\phi)/\mathfrak{p}^n\,\mathrm{End}_K(\phi)$$

are free $A/\mathfrak{p}^n$-modules of the same rank. Then, as a monomorphism of $A/\mathfrak{p}^n$-algebras of the same rank, $\sigma_1^{-1} \circ \lambda \circ \sigma_2$ is an isomorphism. In this case σ_2 is surjective.

Further, for all primes $\mathfrak{p}$ at which the isomorphism λ defined above exists, it yields a commutative diagram

$$\begin{tikzcd}
& A[G_K] \arrow[dl] \arrow[dr] & \\
\mathrm{End}_A\big(\psi[\mathfrak{p}^n]\big) \arrow[rr, "\sim", "\lambda"'] & & \mathrm{End}_A\big(\phi[\mathfrak{p}^n]\big)
\end{tikzcd}$$

which proves the second part. $\square$

Now we can take the first steps towards Theorem 4.3. Before we prove the theorem in full generality, we treat the special case where $n = 1$ and the center of E is separable over A. Moreover, on several occasions, we have to work over the extension field K' of K. We start with the following observation on separable, maximal commutative subalgebras of E':

Lemma 4.8. *Let A' be a maximal commutative A-subalgebra of E' which is separable over A. Then for almost all primes $\mathfrak{p}$ of A, the image of A' under σ' is its own centralizer in* $\mathrm{End}_{k_{\mathfrak{p}}[G_{K'}]}(\phi[\mathfrak{p}])$.

Proof. We extend ϕ to a Drinfeld A'-module ϕ'. Since A' is maximal commutative, $\mathrm{End}_{\overline{K}}(\phi') = A'$. By Theorem 3.1 we know that for almost all primes $\mathfrak{P}$ in A' the representation (over $A'/\mathfrak{P}$) of $G_{K'}$ on $\phi'[\mathfrak{P}]$ is absolutely irreducible. Thus for those $\mathfrak{P}$ we have

$$\mathrm{End}_{A'[G_{K'}]}\big(\phi'[\mathfrak{P}]\big) = A'/\mathfrak{P}.$$

Now $\phi[\mathfrak{p}] = \phi'[\mathfrak{p}A']$ and $\mathfrak{p}A' = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$. Since A' is separable over A, for almost all $\mathfrak{p}$ and all $\mathfrak{P}|\mathfrak{p}$ we have $e(\mathfrak{P}/\mathfrak{p}) = 1$. Hence for those $\mathfrak{p}$ we get the decompositions

$$A'/\mathfrak{p}A' = \bigoplus_{\mathfrak{P}|\mathfrak{p}} A'/\mathfrak{P}$$

and

$$\phi[\mathfrak{p}] = \bigoplus_{\mathfrak{P}|\mathfrak{p}} \phi'[\mathfrak{P}].$$

Putting these results together, we see that for almost all primes $\mathfrak{p}$ in A the endomorphism ring $\mathrm{End}_{A'[G_{K'}]}(\phi[\mathfrak{p}])$ is isomorphic to $A'/\mathfrak{p}A'$, in other words A' maps surjectively onto $\mathrm{End}_{A'[G_{K'}]}(\phi[\mathfrak{p}])$. But the latter is precisely the centralizer of $\sigma'(A')$ in $\mathrm{End}_{A[G_{K'}]}(\phi[\mathfrak{p}])$. □

Let us continue the treatment of our special case. We are seeking to determine the image of σ, which is isomorphic to the endomorphism ring of ϕ modulo the ideal generated by $\mathfrak{p}$. So we clarify the structure of the former by analyzing the latter.

Lemma 4.9. *Assume that the center of* $\mathrm{End}_K(\phi)$ *is separable over A. Then for almost all primes $\mathfrak{p}$ of A, the $k_{\mathfrak{p}}$-algebra $E/\mathfrak{p}E$ is semisimple.*

Proof. By Proposition 1.23 we know that $\mathrm{End}_K(\phi) \otimes_A F$ is a simple F-algebra. Further, since the center $Z(E)$ of E is separable over A, the algebra $Z(E) \otimes_A F$ is separable over F. Now Reiner [**29**] Theorem 9.19 states that the reduced trace on $E \otimes_A F$ gives rise to a nondegenerate associative bilinear form κ on $(E \otimes_A F) \times (E \otimes_A F)$. Accordingly κ is nondegenerate on $E \times E$.

We know that a bilinear form is nondegenerate if and only if its matrix is nonsingular. In this case the determinant of the matrix of κ vanishes modulo at most finitely many primes of A. Thus for all but finitely many primes $\mathfrak{p}$ the induced bilinear form $\kappa_{\mathfrak{p}}$ on $E/\mathfrak{p}E \times E/\mathfrak{p}E$ is nondegenerate.

For every such $\mathfrak{p}$, we can deduce that the $k_\mathfrak{p}$-algebra $E/\mathfrak{p}E$ is semisimple. Indeed, otherwise the radical R of $E/\mathfrak{p}E$ is a nilpotent ideal, i. e. $R^\ell = (0)$ for some $\ell > 1$, but $R^{\ell-1} \neq (0)$. Thus we have

$$\kappa_\mathfrak{p}\big(R, R^{\ell-1}\big) = \kappa_\mathfrak{p}\big(E/\mathfrak{p}E, R^\ell\big) = 0,$$

hence $R^{\ell-1}$ is contained in its own orthogonal complement. But $\kappa_\mathfrak{p}$ was supposed to be nondegenerate. □

On the other hand, we want to gain insight into the structure of $\phi[\mathfrak{p}]$ and its endomorphism ring, which contains the image of σ.

For this purpose, we introduce the following notation: Let $\mathfrak{p}$ be a prime of A for which $E/\mathfrak{p}E$ is semisimple. Let

$$E/\mathfrak{p}E = \bigoplus_{i=1}^{t} \overline{E_i}$$

be the decomposition into simple factors. Wedderburn's theorem tells us that each $\overline{E_i}$ is of the form $\mathrm{Mat}_{d\times d}(k_{\mathfrak{p},i})$, where $k_{\mathfrak{p},i}$ is the center of $\overline{E_i}$, and d^2 is the rank of E over its center. We know that each $k_{\mathfrak{p},i}$ is a finite field extension of $k_\mathfrak{p}$. For every i let

$$\overline{V_i} = k_{\mathfrak{p},i}^{\oplus d}$$

be the evident irreducible representation of $\overline{E_i}$ and set

$$\overline{W_i} = \mathrm{Hom}_{E/\mathfrak{p}E}\big(\overline{V_i}, \phi[\mathfrak{p}]\big).$$

We let G_K act trivially on $\overline{V_i}$ and $E/\mathfrak{p}E$ act trivially on $\overline{W_i}$.

Lemma 4.10. *For every prime $\mathfrak{p}$ of A at which $E/\mathfrak{p}E$ is semisimple, we have a G_K-equivariant decomposition*

$$\phi[\mathfrak{p}] = \bigoplus_{i=1}^{t} \overline{V_i} \otimes_{k_{\mathfrak{p},i}} \overline{W_i}.$$

Proof. As $E/\mathfrak{p}E$ is semisimple, the $E/\mathfrak{p}E$-module $\phi[\mathfrak{p}]$ is completely reducible. So the natural homomorphism

$$\bigoplus_{i=1}^{t} \overline{V_i} \otimes_{k_{\mathfrak{p},i}} \overline{W_i} \to \phi[\mathfrak{p}]$$

is an isomorphism.

Furthermore, letting G_K act trivially on $\overline{V_i}$, we obtain a natural G_K-action on $\overline{W_i}$. With $E/\mathfrak{p}E$ acting trivially on $\overline{W_i}$, the above isomorphism becomes $(E/\mathfrak{p}E)[G_K]$-equivariant. □

With this information, we can prove Theorem 4.3 (1) in a first special case.

Proposition 4.11. *Assume that the center of E' is separable over A. Then for almost all primes $\mathfrak{p}$ of A, the map*

$$E'/\mathfrak{p}E' \longrightarrow \mathrm{End}_{A[G_{K'}]}\big(\phi[\mathfrak{p}]\big)$$

is bijective.

Proof. Clearly we may apply the preceding lemmata with K' in the place of K. Let $\mathfrak{p}$ be a prime of A at which $E'/\mathfrak{p}E'$ is semisimple, and write $E'/\mathfrak{p}E' = \bigoplus_{i=1}^{t} \overline{E_i'}$. We denote the center of $\overline{E_i'}$ by $k'_{\mathfrak{p},i}$ and as in Lemma 4.10 we have a $G_{K'}$-equivariant decomposition

$$\phi[\mathfrak{p}] = \bigoplus_{i=1}^{t} \overline{V_i'} \otimes_{k'_{\mathfrak{p},i}} \overline{W_i'}.$$

Now by Proposition 2.6 and Lemma 4.10 any $G_{K'}$-invariant $k_{\mathfrak{p}}$-subspace of $\phi[\mathfrak{p}]$ must have the form

$$\bigoplus_{i=1}^{t} \overline{U_i'} \otimes_{k'_{\mathfrak{p},i}} \overline{W_i'}$$

with $k'_{\mathfrak{p},i}$-subspaces $\overline{U_i'} \subset \overline{V_i'}$, and conversely every $k_{\mathfrak{p}}$-subspace of this form is $G_{K'}$-invariant. For every $0 \neq \overline{v_i} \in \overline{V_i'}$ the image of the embedding

$$\overline{W_i'} \hookrightarrow \phi[\mathfrak{p}] : \overline{w} \mapsto \overline{v_i} \otimes \overline{w}$$

is a $G_{K'}$-invariant $k_{\mathfrak{p}}$-subspace of $\phi[\mathfrak{p}]$. Again by Proposition 2.6 we see that $\overline{W_i'}$ must be $k_{\mathfrak{p}}[G_{K'}]$-irreducible. Thus Schur's Lemma and Wedderburn's Theorem force

$$\ell'_{\mathfrak{p},i} = \mathrm{End}_{k_{\mathfrak{p}}[G_{K'}]}\big(\overline{W_i'}\big)$$

to be a finite field extension of $k'_{\mathfrak{p},i}$.

Further the $\overline{W_i'}$ are pairwise non-equivalent, because the graph of a non-zero homomorphism between two of them would give rise to a $G_{K'}$-invariant subspace of $\phi[\mathfrak{p}]$ which is not of the given form. So we see that

$$\begin{aligned}
\mathrm{End}_{k_{\mathfrak{p}}[G_{K'}]}\big(\phi[\mathfrak{p}]\big) &= \bigoplus_{i=1}^{t} \mathrm{End}_{k_{\mathfrak{p}}[G_{K'}]}\big(\overline{V_i'} \otimes_{k'_{\mathfrak{p},i}} \overline{W_i'}\big) \\
&= \bigoplus_{i=1}^{t} \mathrm{End}_{k_{\mathfrak{p}}}\big(\overline{V_i'}\big) \otimes_{k'_{\mathfrak{p},i}} \mathrm{End}_{k_{\mathfrak{p}}[G_{K'}]}\big(\overline{W_i'}\big) \qquad (2) \\
&= \bigoplus_{i=1}^{t} \overline{E_i'} \otimes_{k'_{\mathfrak{p},i}} \ell'_{\mathfrak{p},i}.
\end{aligned}$$

Since $\mathrm{End}_{K'}(\phi) \otimes_A F$ is a simple F-algebra (Proposition 1.23), it follows from Bourbaki [**4**] §10, no 4, Proposition 4, that E' contains a maximal commutative $k_{\mathfrak{p}}$-subalgebra A' which is separable over the center of E'. Because of the separability assumption on the center and because separability is transitive, A' is separable over A. The image of A' in $\mathrm{End}_{k_{\mathfrak{p}}[G_{K'}]}(\phi[\mathfrak{p}])$ is centralized by every element $\overline{e_i} \otimes x_i$ with $\overline{e_i}$ in the center of $\overline{E_i'}$ and x_i in $\ell'_{\mathfrak{p},i}$. So Lemma 4.8 implies that $\ell'_{\mathfrak{p},i} = k'_{\mathfrak{p},i}$ for all i. The claim follows. □

In the next step, we want to redescend from K' to K. We prepare this step with two lemmata. First we give a condition under which taking invariants under a group action on a module commutes with taking quotients of the module. The second lemma tells us that no inseparability can occur in the extension E'/E.

Lemma 4.12. *Let M be an A-module of finite type and let G be a finite subgroup of* $\mathrm{Aut}_A(M)$. *Then for almost all primes $\mathfrak{p}$ in A we have an isomorphism*

$$M^G/\mathfrak{p}M^G \xrightarrow{\sim} (M/\mathfrak{p}M)^G.$$

Proof. We define a map

$$\begin{aligned} \varepsilon : M &\longrightarrow \bigoplus_{g\in G} M \\ m &\longmapsto \big((g-1)m\big)_{g\in G} \end{aligned}$$

whose kernel clearly is M^G. Then we have two obvious short exact sequences

$$0 \to \ker\varepsilon \to M \to \mathrm{im}\,\varepsilon \to 0$$

and

$$0 \to \mathrm{im}\,\varepsilon \to \bigoplus_{g\in G} M \to \mathrm{coker}\,\varepsilon \to 0.$$

The image and the cokernel of ε are A-modules of finite type. Therefore they are locally free at almost all primes $\mathfrak{p}$. For those $\mathfrak{p}$ the modules $\mathrm{Tor}_1^A(\mathrm{im}\,\varepsilon, A/\mathfrak{p})$ and $\mathrm{Tor}_1^A(\mathrm{coker}\,\varepsilon, A/\mathfrak{p})$ vanish. It follows that the horizontal and the vertical sequence in the following diagram are exact:

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
0 \arrow[r] & \ker(\varepsilon)/\mathfrak{p}\ker(\varepsilon) \arrow[r] & M/\mathfrak{p}M \arrow[r] \arrow[dr, "\overline{\varepsilon}"'] & \mathrm{im}(\varepsilon)/\mathfrak{p}\,\mathrm{im}(\varepsilon) \arrow[r] \arrow[d] & 0 \\
 & & & \bigoplus_{g\in G} M/\mathfrak{p}M &
\end{tikzcd}$$

Here $\overline{\varepsilon}$ is the map $\overline{m} \mapsto \big((g-1)\overline{m}\big)_{g\in G}$. We see that

$$\ker(\varepsilon)/\mathfrak{p}\ker(\varepsilon) = \ker\overline{\varepsilon}$$

and the lemma is proven. □

Lemma 4.13. *The center of E' is separable over the center of E.*

Proof. Let Z be the center of E and Z' be the center of E'. Let F_1 and F_1' be the respective quotient fields of Z and Z'. Clearly Z' is invariant under the action of G_K on E', and the action on Z' extends to F_1'. We therefore have a group homomorphism

$$G_K \longrightarrow \mathrm{Aut}_{F_1}(F_1'),$$

and F_1' is a Galois extension over the subfield of F_1' fixed by the image of G_K. The G_K-invariants of F_1' are contained in F_1, so F_1' is separable over F_1. □

Now we can bring down Proposition 4.11 to the base field K, and thus get one step closer to Theorem 4.3.

Proposition 4.14. *Assume that the center of E is separable over A. Then for almost all primes $\mathfrak{p}$ in A, the map*

$$E/\mathfrak{p}E \longrightarrow \mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}]\big)$$

is bijective.

Proof. Because the center of E is separable over A and by Lemma 4.13, the center of E' is separable over A. Thus for almost all $\mathfrak{p}$, Propositions 4.1 and 4.11 yield an isomorphism

$$E'/\mathfrak{p}E' \xrightarrow{\sim} \mathrm{End}_{A[G_{K'}]}\big(\phi[\mathfrak{p}]\big).$$

On both sides we have a G_K-action. Clearly the G_K-invariants on the right hand side are precisely $\mathrm{End}_{A[G_K]}(\phi[\mathfrak{p}])$. Thus we need to know that for all but finitely many of these $\mathfrak{p}$ we have

$$(E')^{G_K}/(\mathfrak{p}E')^{G_K} = (E'/\mathfrak{p}E')^{G_K}.$$

This is the assertion of Lemma 4.12. □

From the preceding considerations we should retain the following fact which will be important for the proof of Theorem 5.1 below:

Remark 4.15. We recall that if the center of E is separable over A, for almost all $\mathfrak{p}$ we have decompositions

$$E/\mathfrak{p}E = \bigoplus_{i=1}^{t} \overline{E_i}$$

and

$$\phi[\mathfrak{p}] = \bigoplus_{i=1}^{t} \overline{V_i} \otimes_{k_{\mathfrak{p},i}} \overline{W_i}$$

and we note that as in Equation (2) in the proof of Proposition 4.11 we have

$$\mathrm{End}_{k_{\mathfrak{p}}[G_K]}\big(\phi[\mathfrak{p}]\big) = \bigoplus_{i=1}^{t} \overline{E_i} \otimes_{k_{\mathfrak{p},i}} \ell_{\mathfrak{p},i}$$

for suitable field extensions $\ell_{\mathfrak{p},i}/k_{\mathfrak{p},i}$. Then by Proposition 4.14 it follows immediately that $\ell_{\mathfrak{p},i} = k_{\mathfrak{p},i}$ and that the $\overline{W_i}$ are absolutely irreducible $k_{\mathfrak{p}}[G_K]$-modules.

Now we have to solve the general case. The possible occurance of inseparability and the need of higher powers of the prime ideal necessitate the use of arguments which are technically more involved. Although this is partly tedious and uninspiring, it has the benefit that we gain a concrete description of the A-algebra generated by the image of Galois.

Recall that Z denotes the center of E and m the inseparable degree of Z over A. We have seen that almost all prime ideals $\mathfrak{p}$ in A decompose as a product $\mathfrak{p} = \prod_{i=1}^{s} \mathfrak{P}_i^m$ with pairwise distinct primes $\mathfrak{P}_i$ in Z. Further, the rank of E over Z is d^2. We extend ϕ to a Drinfeld Z-module ϕ' whose rank we denote by r'. We have $d|r'$ and set $e = \frac{r'}{d}$.

Lemma 4.16. *For almost all primes $\mathfrak{p} \subset A$ that decompose as $\mathfrak{p} = \prod_{i=1}^{s} \mathfrak{P}_i^m$ in Z, the following assertions hold:*

$$E/\mathfrak{p}E = \bigoplus_{i=1}^{s} E/\mathfrak{P}_i^m E, \tag{1}$$

$$\mathrm{End}_{A[G_K]}\big(\phi[\mathfrak{p}]\big) = \bigoplus_{i=1}^{s} \mathrm{End}_{Z[G_K]}\big(\phi'[\mathfrak{P}_i^m]\big). \tag{2}$$

Proof. (1) is immediate. For (2) we observe that $\phi[\mathfrak{p}] = \bigoplus_{i=1}^{s} \phi'[\mathfrak{P}_i^m]$ and that the $Z[G_K]$-modules $\phi'[\mathfrak{P}_i^m]$ pairwise have no common subfactors. Hence the ring of G_K-equivariant endomorphisms decomposes as a direct sum as above. □

A part of the technical difficulties is resolved by the following lemma. It is purely algebraic and totally independent of the other results.

Lemma 4.17. *Let k be any field and let $\ell, n > 0$. We set $R = k[T]/(T^{\ell})$ and $S = \mathrm{Mat}_{n\times n}(R)$. Let $M = R^n$ be the module with the natural S-action and pick a subring $S_1 \subset S$ containing the identity. Assume that*

(1) *every S_1-submodule of M is an S-submodule of the form $T^j M$,*
(2) *$S_1 + TS = S$.*

Then $S_1 = S$.

We isolate the following statement from the demonstration of the lemma and prove it separately:

Lemma 4.18. *We adopt notation and hypotheses of Lemma 4.17. Additionally, let $s \geq 0$ and let $N \subset M^s$ be an S_1-submodule such that there exists an S_1-epimorphism $N \twoheadrightarrow (M/TM)^t$ for some $t \geq 0$. Then $t \leq s$.*

Proof. This is easily proven by induction on s. If $s = 0$ then there is nothing to prove. If $s = 1$ then N is an S_1-submodule of M, hence of the form $T^j M$. We have $T^j M \twoheadrightarrow (M/TM)^t$ with kernel either $T^j M$ or $T^{j+1}M$. This means either

$$(M/TM)^t \cong T^j M/T^{j+1}M \cong M/TM$$

or

$$(M/TM)^t = 0.$$

Therefore $t \leq 1$.

Let $s > 1$ and assume that the claim holds for $s-1$. Let an S_1-submodule $N \subset M^s$ and an S_1-epimorphism $N \twoheadrightarrow (M/TM)^t$ for some t be given. We put

$$N' = N \cap \big(M^{s-1} \oplus \{0\}\big).$$

Since M/TM is a simple S_1-module, the image of N' is isomorphic to $(M/TM)^{t'}$ with $t' \leq t$. The hypothesis shows that $t' \leq s-1$. On the other hand, N/N' is an S_1-submodule of M and maps surjectively onto $(M/TM)^{t-t'}$. In this case we have seen that $t - t' \leq 1$. The claim follows. □

Proof of Lemma 4.17. Now we can carry out the proof by induction on ℓ. If $\ell = 1$, then we have merely restated assumption (2).

Let $\ell > 1$ and assume that the lemma holds for $\ell - 1$, that is, we have the equality $S_1 + T^{\ell-1}S = S$. We observe that $S \cong M^n$ as S-modules. For $1 \leq i \leq n$ we define $S_{1,i}$ to be the intersection of S_1 and $\{0\}^{i-1} \oplus M \oplus \{0\}^{n-i}$. If one of the $S_{1,i}$ were zero, then we would find S_1 to be an S_1-submodule of M^{n-1} with quotient

$$S_1/(S_1 \cap TS) \cong (S_1 + TS)/TS = S/TS \cong (M/TM)^n$$

which is impossible by Lemma 4.18. Furthermore, every $S_{1,i}$ is an S_1-submodule of M, hence it is of the form $S_{1,i} \cong T^{\ell_i}M$ with $\ell_i < \ell$. We see that S_1 contains the S-modules $\bigoplus_{i=1}^n T^{\ell_i}M \supset T^{\ell-1}S$. Therefore

$$S = S_1 + T^{\ell-1}S = S_1$$

which completes the proof. □

Let us come back to arithmetic. We are now ready to give a proof of the two parts of Theorem 4.3. Not surprisingly, the surjectivity of σ and the structure of the A-algebra generated by the image of Galois are entwined. Summarily, the common argument for both problems has the following structure:

We compare the algebra generated by the image of Galois with the commutant of the endomorphism ring of ϕ modulo $\mathfrak{p}^n$. The latter is known to have the structure of matrix algebra that we want to have for the former. The special case of the theorem that already has been proven allows to reduce the problem to Lemma 4.17, which yields equality. Now surjectivity of σ follows comparing the commutants on both sides.

Proof of Theorem 4.3. In view of the decomposition that is given by Lemma 4.16, we may replace A by the maximal subring of Z which is separable over A. So we reduce to the case that Z is purely inseparable over A. For Theorem 4.3 (1), it then remains to show that

$$E/\mathfrak{P}^n E \cong \mathrm{End}_{Z[G_K]}\big(\phi'[\mathfrak{P}^n]\big)$$

for almost all primes $\mathfrak{P} \subset Z$ and all $n = mn'$ with $n' > 0$.

Recall that $Z/\mathfrak{P}^n \cong k_{\mathfrak{P}}[T]/(T^n)$, that $\phi'[\mathfrak{P}^n]$ is a free $k_{\mathfrak{P}}[T]/(T^n)$-module of rank $r' = de$ and that $E/\mathfrak{P}^n E$ is isomorphic to $\mathrm{Mat}_{d\times d}\big(k_{\mathfrak{P}}[T]/(T^n)\big)$.

Let C be the commutant of $E/\mathfrak{P}^n E$ in $\mathrm{End}_Z(\phi'[\mathfrak{P}^n])$ and $C_G \subset C$ the image of $A[G_K]$ in $\mathrm{End}_Z(\phi'[\mathfrak{P}^n])$. Clearly

$$C \cong \mathrm{Mat}_{e\times e}\big(k_{\mathfrak{P}}[T]/(T^n)\big).$$

For Theorem 4.3 (2), we now have to show that $C = C_G$, and this equality also implies (1).

Naturally C acts on the module $N = \big(k_{\mathfrak{P}}[T]/(T^n)\big)^{\oplus e}$. We claim that all C_G-submodules of N have the form $T^j N$ for $j \geq 0$. This can be seen as follows: We can view N as a submodule of $\phi'[\mathfrak{P}^n]$ and, choosing a suitable basis, we may assume that

$$N \oplus \{0\}^{d-1} \subset \phi'[\mathfrak{P}^n].$$

Let N_1 be a C_G-submodule of N, then $N_1 \oplus \{0\}^{d-1}$ is a C_G-submodule of $\phi'[\mathfrak{P}^n]$. By Proposition 2.6 we have

$$N_1 \oplus \{0\}^{d-1} = \alpha\phi'[\mathfrak{P}^n]$$

for some $\alpha \in \mathrm{Mat}_{d\times d}\big(k_{\mathfrak{P}}[T]/(T^n)\big)$. We see that all rows of α but the first must be zero. Let $a_1, \dots, a_d$ be the entries of the first row of α. Then

$$N_1 = \sum_{i=1}^{d} a_i N = (a_1, \dots, a_d)N = (T^j)N$$

for some $j \geq 0$, because $(a_1, \dots, a_d)$ is an ideal in $k_{\mathfrak{P}}[T]/(T^n)$. This proves the claim.

By Proposition 4.14 (the special case of the theorem already known), for almost all $\mathfrak{P}$ we have

$$E/\mathfrak{P}E \cong \mathrm{End}_{k_{\mathfrak{P}}[G_K]}\big(\phi'[\mathfrak{P}]\big).$$

This means that modulo T the commutant of C_G is $E/\mathfrak{P}^n E$. By Lemma 4.10 the $k_{\mathfrak{P}}[G_K]$-module $\phi'[\mathfrak{P}]$ is semisimple for almost all $\mathfrak{P}$, thus C_G is its own bicommutant modulo T (cf. Lang [**20**] XVII Theorem 3.2). Therefore modulo T the commutant of $E/\mathfrak{P}^n E$ is C_G, whence $C_G + TC = C$.

Then Lemma 4.17, applied to $k = k_{\mathfrak{P}}$, $M = N$, $S = C$ and $S_1 = C_G$, shows that C_G equals the commutant of $E/\mathfrak{P}^n E$. Hence $\mathrm{End}_{Z[G_K]}(\phi'[\mathfrak{P}^n])$ equals the bicommutant of $E/\mathfrak{P}^n E$, which is $E/\mathfrak{P}^n E$ itself. $\square$

5. Representations Associated to Non-Isogenous Drinfeld Modules

Let ϕ_1 and ϕ_2 be two Drinfeld A-modules over K with special characteristic $\mathfrak{p}_0$. In the following the associated residual representations are compared in the case that ϕ_1 and ϕ_2 are non-isogenous.

The proof of the following unpublished result has been communicated to the author by Richard Pink ([**27**]). It is reproduced with his kind permission.

Theorem 5.1. *Let ϕ_1 and ϕ_2 be non-isogenous Drinfeld A-modules over K. Then the set of primes $\mathfrak{p}$ of A for which the $k_\mathfrak{p}[G_K]$-modules $\phi_1[\mathfrak{p}]$ and $\phi_2[\mathfrak{p}]$ have a nontrivial common subfactor is finite.*

Proof. (0) Let us first sketch the argument in the case $E_1 = E_2 = A$. Then $\phi_1[\mathfrak{p}]$ and $\phi_2[\mathfrak{p}]$ are irreducible $k_\mathfrak{p}[G_K]$-modules for almost all $\mathfrak{p}$, so it suffices to prove that they are inequivalent for almost all $\mathfrak{p}$.

If that is not the case, the characteristic polynomials on ϕ_1 and ϕ_2 of all Frobenius elements are congruent modulo infinitely many $\mathfrak{p}$; hence they are equal. Now we apply this knowledge to $V_\mathfrak{p}(\phi_1)$ and $V_\mathfrak{p}(\phi_2)$ for any fixed $\mathfrak{p}$. By density of the Frobenius elements, we deduce that these two irreducible $F_\mathfrak{p}[G_K]$-modules have the same character and are therefore isomorphic. Then, by the Tate conjecture, the Drinfeld modules are isogenous.

(1) Set $E_i = \mathrm{End}_K(\phi_i)$, let A_i be its center, and denote the corresponding Drinfeld A_i-module by ϕ'_i. (For the following one should really pass to the normalization of A_i. But as this affects only finitely many primes of A, I allow myself to neglect this point for the moment.) Then for every prime $\mathfrak{p}$ of A we have

$$T_\mathfrak{p}(\phi_i) = \bigoplus_{\mathfrak{p}_i|\mathfrak{p}} T_{\mathfrak{p}_i}(\phi'_i).$$

The structure of $\phi_i[\mathfrak{p}]$ depends on the ramification and the degree of inseparability of A_i over A. But in any case $\phi_i[\mathfrak{p}]$ is a successive extension of copies of the different $\phi'_i[\mathfrak{p}_i]$ for primes $\mathfrak{p}_i$ of A_i over $\mathfrak{p}$.

(2) Write $d_i^2 = \mathrm{rk}_{A_i} E_i$. Then whenever $\mathfrak{p}_i$ is unramified in E_i, and in particular for all but finitely many $\mathfrak{p}_i$, the module $\phi'_i[\mathfrak{p}_i]$ is a direct sum of d_i copies of some $k_{\mathfrak{p}_i}[G_K]$-module $\overline{W}_{\mathfrak{p}_i}$. From Proposition 2.6 it follows (as in the proof of Proposition 4.11) that this is a simple $k_\mathfrak{p}[G_K]$-module, and by Remark 4.15 we know that it is absolutely irreducible over $k_{\mathfrak{p}_i}$. Similarly, the Tate module $T_{\mathfrak{p}_i}(\phi'_i)$ is a direct sum of d_i copies of some $A_{i,\mathfrak{p}_i}[G_K]$-module that I call $T_{\mathfrak{p}_i}\overline{W}_i$. By the Tate conjecture the associated rational Tate module $T_{\mathfrak{p}_i}\overline{W}_i \otimes_{A_{i,\mathfrak{p}_i}} F_{i,\mathfrak{p}_i}$ is an absolutely irreducible representation of G_K over $F_{i,\mathfrak{p}_i}$.

(3) Steps (1) and (2) show that $\phi_1[\mathfrak{p}]$ and $\phi_2[\mathfrak{p}]$ have a non-trivial common subfactor if and only if there exist $\mathfrak{p}_1|\mathfrak{p}$ and $\mathfrak{p}_2|\mathfrak{p}$ so that $\overline{W}_{\mathfrak{p}_1} \cong \overline{W}_{\mathfrak{p}_2}$ as $k_\mathfrak{p}[G_K]$-modules. We assume that this happens for $\mathfrak{p}$ in an infinite set of primes P, and must show that then ϕ_1 and ϕ_2 are isogenous.

(4) Let $A_c = A_1 \otimes_A A_2$. This is a commutative A-algebra which is torsion free and of finite type as A-module; but it is not necessarily an integral domain. The idea in what follows is to extend scalars from each A_i to the common overring A_c and to apply the argument (0) there. We can view this as working with the A_c-modules $\widehat{\phi_i} = \phi'_i \otimes_{A_i} A_c$ in the sense of Anderson, but it is more efficient to proceed ad hoc. Thus for any prime

$\mathfrak{p}_c$ of A_c over a prime $\mathfrak{p}_i$ of A_i we simply set

$$\widehat{W}_{i,\mathfrak{p}_c} = \overline{W}_{\mathfrak{p}_i} \otimes_{k_{\mathfrak{p}_i}} k_{\mathfrak{p}_c}$$

as a $k_{\mathfrak{p}_c}[G_K]$-module.

(5) The absolute irreducibility (2) implies that for $\mathfrak{p} \in P$ there exists an isomorphism $\alpha : k_{\mathfrak{p}_1} \xrightarrow{\sim} k_{\mathfrak{p}_2}$ such that $\overline{W}_{\mathfrak{p}_1} \cong \overline{W}_{\mathfrak{p}_2}$ as $k_{\mathfrak{p}_1}[G_K]$-modules. The choice of α corresponds to the choice of a prime $\mathfrak{p}_c$ of A_c above $\mathfrak{p}_1$ and $\mathfrak{p}_2$, such that $\widehat{W}_{1,\mathfrak{p}_c} \cong \widehat{W}_{2,\mathfrak{p}_c}$ as $k_{\mathfrak{p}_c}[G_K]$-modules. Thus for all $\mathfrak{p}_c$ in some infinite set P_c of primes of A_c we have $\widehat{W}_{1,\mathfrak{p}_c} \cong \widehat{W}_{2,\mathfrak{p}_c}$ as $k_{\mathfrak{p}_c}[G_K]$-modules.

(6) The scheme Spec A_c is of finite type over $\mathbb{F}_p$ and of dimension 1. Thus the Zariski closure of any infinite subset contains the generic point of an irreducible component of dimension 1. Let $\mathfrak{q}$ be such a generic point in the Zariski closure of P_c. After shrinking P_c we may assume without loss of generality that all points $\mathfrak{p}_c \in P_c$ lie in the irreducible component corresponding to $\mathfrak{q}$, that is, satisfy $\mathfrak{q} \subset \mathfrak{p}_c$. Then we have a natural injective map $A_c/\mathfrak{q} \hookrightarrow \prod_{\mathfrak{p}_c \in P_c} k_{\mathfrak{p}_c}$.

(7) Now for any good place x of K let $\mathrm{Frob}_x \in G_K$ denote an associated Frobenius element, i. e. one that acts as Frobenius on any extension that is unramified in x. Its characteristic polynomial $f_{\overline{W}_i,x}(T)$ on $T_{\mathfrak{p}_i}\overline{W}_i$ over $A_{i,\mathfrak{p}_i}$ lies in $A_i[T]$ and is independent of $\mathfrak{p}_i$. We will look at its image in $A_c[T]$, noting first that its image in $k_{\mathfrak{p}_c}[T]$ is the characteristic polynomial of Frob_x on $\widehat{W}_{i,\mathfrak{p}_c}$ over $k_{\mathfrak{p}_c}$.

(8) By (5) for $\mathfrak{p}_c \in P_c$ this characteristic polynomial is independent of i. Thus $f_{\overline{W}_1,x}(T)$ and $f_{\overline{W}_2,x}(T) \in A_c[T]$ are congruent modulo $\mathfrak{p}_c$. Using (6) this implies that they are actually congruent modulo $\mathfrak{q}$. This means that their images in $(A_c/\mathfrak{q})[T]$ coincide.

(9) Now fix any suitable $\mathfrak{p}$. Fix any prime $\mathfrak{p}_c$ of A_c above $\mathfrak{p}$ which contains $\mathfrak{q}$. Let $\mathfrak{p}_i$ be the prime of A_i under $\mathfrak{p}_c$. By definition the characteristic polynomial of Frob_x on $T_{\mathfrak{p}_i}\overline{W}_i$ over $A_{i,\mathfrak{p}_i}$ is $f_{\overline{W}_i,x}(T)$. Let $F_{\ldots}$ abbreviate $\mathrm{Quot}(A_{\ldots})$. Then the characteristic polynomial of Frob_x on

$$T_{\mathfrak{p}_i}\overline{W}_i \otimes_{A_{i,\mathfrak{p}_i}} F_{c,\mathfrak{p}_c}$$

over $F_{c,\mathfrak{p}_c}$ is the image of $f_{\overline{W}_i,x}(T)$ in $(A_c/\mathfrak{q})[T]$. So by (8) it is independent of i.

(10) Since the Frob_x form a dense subset of G_K, the equality of characteristic polynomials follows for all $\sigma \in G_K$. Since the representations are also absolutely irreducible, we deduce that they are isomorphic.

(11) Now $T_{\mathfrak{p}_i}\overline{W}_i$ is a direct summand of $T_{\mathfrak{p}}(\phi_i)$ as an $A_{\mathfrak{p}}[G_K]$-module. Thus the projection map $T_{\mathfrak{p}}(\phi_i) \twoheadrightarrow T_{\mathfrak{p}_i}\overline{W}_i$ induces an $A_{i,\mathfrak{p}_i}[G_K]$-linear surjection

$$T_{\mathfrak{p}}(\phi_i) \otimes_{A_{\mathfrak{p}}} A_{i,\mathfrak{p}_i} \twoheadrightarrow T_{\mathfrak{p}_i}\overline{W}_i$$

and hence an $A_{c,\mathfrak{p}_c}[G_K]$-linear surjection

$$T_{\mathfrak{p}}(\phi_i) \otimes_{A_{\mathfrak{p}}} F_{c,\mathfrak{p}_c} \twoheadrightarrow T_{\mathfrak{p}_i}\overline{W}_i \otimes_{A_{i,\mathfrak{p}_i}} F_{c,\mathfrak{p}_c}.$$

The same argument applied to the $A_{\mathfrak{p}}$-dual, respectively $A_{i,\mathfrak{p}_i}$-dual module yields, after dualizing again with respect to $F_{c,\mathfrak{p}_c}$, an $A_{c,\mathfrak{p}_c}[G_K]$-linear injection

$$T_{\mathfrak{p}_i}\overline{W}_i \otimes_{A_{i,\mathfrak{p}_i}} F_{c,\mathfrak{p}_c} \hookrightarrow T_{\mathfrak{p}}(\phi_i) \otimes_{A_{\mathfrak{p}}} F_{c,\mathfrak{p}_c}.$$

(The dualizing argument was necessitated by the possibility that A_i might be inseparable over A.) Altogether we find a non-zero $A_{c,\mathfrak{p}_c}[G_K]$-linear homomorphism

$$T_{\mathfrak{p}}(\phi_1) \otimes_{A_{\mathfrak{p}}} F_{c,\mathfrak{p}_c} \longrightarrow T_{\mathfrak{p}}(\phi_2) \otimes_{A_{\mathfrak{p}}} F_{c,\mathfrak{p}_c}.$$

(12) The isomorphism

$$\begin{aligned}\operatorname{Hom}_{F_{c,\mathfrak{p}_c}[G_K]}\big(T_{\mathfrak{p}}(\phi_1) \otimes_{A_{\mathfrak{p}}} F_{c,\mathfrak{p}_c}, T_{\mathfrak{p}}(\phi_2) \otimes_{A_{\mathfrak{p}}} F_{c,\mathfrak{p}_c}\big)&\\ \cong \operatorname{Hom}_{A_{\mathfrak{p}}[G_K]}\big(T_{\mathfrak{p}}(\phi_1), T_{\mathfrak{p}}(\phi_2)\big) \otimes_{A_{\mathfrak{p}}} F_{c,\mathfrak{p}_c}&\end{aligned}$$

now shows that $\operatorname{Hom}_{A_{\mathfrak{p}}[G_K]}\big(T_{\mathfrak{p}}(\phi_1), T_{\mathfrak{p}}(\phi_2)\big) \neq 0.$ By the Tate conjecture this implies that ϕ_1 and ϕ_2 are isogenous, as desired. □

CHAPTER II

A-Motives

In the research on Drinfeld modules, several attempts have been made to generalize these objects. One of these generalizations, A-motives, will be presented and studied in this chapter; two others, preceding and motivating the invention of A-motives, are going to be mentioned.

One of these is due to Vladimir G. Drinfeld, suggesting a translation of Drinfeld modules into the language of locally free sheaves on algebraic curves. The objects arising are known as *F-sheaves* or *shtukas*.

In another line of generalization, the strong analogies between Drinfeld modules and elliptic curves downright called for something like a "Drinfeld abelian variety", a higher dimensional generalization of Drinfeld modules. In this context, *Hilbert-Blumenthal-Drinfeld modules* appeared.

A very powerful and influential generalization in this latter direction has been given by Greg W. Anderson in 1986 in his paper [**1**]. A twofold motivation was at its bottom: On the one hand, Anderson studied a question concerning the determinant of shtukas raised by Drinfeld, and on the other hand, he tried to solve a problem on Hilbert-Blumenthal-Drinfeld modules that had been put forth by Benedict H. Gross.

Anderson's simultaneous solution to these two problems introduced a pair of new notions, *t-modules* and *t-motives*. In his paper, he gives their definition and a couple of fundamental algebraic properties, and afterwards turns towards uniformization theory. Since then, algebraic and analytic aspects have been studied by various authors.

Now what is a t-motive? We let Greg Anderson give a first answer to this question, citing the introduction of his paper on t-motives:

> An abelian t-module is at once a higher-dimensional generalization of an elliptic A-module with $A = \mathbb{F}_p[t]$ and an analog of an abelian variety; a t-motive is a kind of module over a noncommutative ring, the two notions being linked by a contravariant functor under which the category of the former is anti-equivalent to the category of the latter.[1]

We may add that an abelian t-module is an algebraic group isomorphic to the direct sum of finitely many copies of the additive group variety, endowed with an endomorphism t satisfying a certain condition. In the case of a Drinfeld $\mathbb{F}_p[t]$-module ϕ, this endomorphism is given by $\phi_t \in \mathrm{End}(\mathbb{G}_a)$.

---

[1] Anderson [**1**] p. 460.

However, in this chapter we only adopt the point of view of t-motives, although the more natural generalization of a Drinfeld module is the t-module. As pointed out in the quotation above, this mainly is a choice of language; we lose nothing but a somewhat broader view. In exchange, we shall use an extended notion of t-motive which allows general A in the place of $\mathbb{F}_p[t]$.

As in the previous chapter, our study is algebraic in nature and motivated by questions borrowed from arithmetic geometry over number fields. This chapter presents an approach to the isogeny conjecture for t-motives and, more generally, for A-motives. This approach cannnot give an anwer to the whole question. It accomplishes a proof for A-motives arising as direct sums of Drinfeld modules in special characteristic. This is explained in detail in Section 3.

Beforehand, Section 1 explains the definition and some properties of A-motives, and in Section 2 we study how the number of isomorphism classes in an isogeny class of A-motives changes under extensions of the base field.

1. A-Motives: An Overview

As for Drinfeld modules in Chapter I, we start with a brief introdution to the notions and the basic algebraic theory. Again, for the proofs we refer to the literature.

We retain the notation used since the introduction. In particular, we consider the function field K as an A-field via the ring homomorphism $\iota : A \to K$. The characteristic of K is the ideal $\mathfrak{p}_0 = \ker \iota$. In this introductory section, the characteristic may be generic or special, later on it will be required to be special. Recall that by $K\{\tau\}$ we denote the twisted polynomial ring over K. In this section $\mathfrak{p}$ denotes a prime ideal and $\mathfrak{a}$ an arbitrary ideal in A.

Let us start right away with the fundamental definition. Originally, as introduced by Greg Anderson in [**1**], t-motives were defined as modules over the ring

$$K[t, \tau] = K\{\tau\} \otimes_{\mathbb{F}_q} \mathbb{F}_q[t].$$

In our terminology, this means that they were only defined in the case $A = \mathbb{F}_q[t]$. We want to generalize Anderson's t-motives to arbitrary A. This is accomplished in

Definition 1.1 (A-motives)**.** Let I be the ideal of $K \otimes_{\mathbb{F}_q} A$ which is generated by all elements of the form $\iota(a) \otimes 1 - 1 \otimes a$ with $a \in A$. An *A-motive* M is a left module over $K\{\tau\} \otimes_{\mathbb{F}_q} A$ such that

(1) M is finitely generated and projective over $K \otimes_{\mathbb{F}_q} A$,
(2) M is finitely generated over $K\{\tau\}$,
(3) the support of $M/\tau M$ as a $K \otimes_{\mathbb{F}_q} A$-module is contained in the set of primes of $K \otimes_{\mathbb{F}_q} A$ dividing I.

A *morphism* of A-motives is defined to be a homomorphism of the underlying modules over $K\{\tau\} \otimes_{\mathbb{F}_q} A$. An *isomorphism* is a morphism which has a two-sided inverse.

The characteristic $\mathfrak{p}_0$ of the A-field K is also referred to as the characteristic of the A-motive M.

Although we have extended Anderson's notion of t-motive, his paper [**1**] remains the basic and comprehensive reference for this section. The proofs of all relevant results on t-motives carry directly over to A-motives. We abstain from executing this straightforward task.

In a first step and with the intention to animate the somewhat inapproachable definition, we want to reveal the connection between Drinfeld A-modules and A-motives.

Remark 1.2. The category of Drinfeld A-modules is anti-equivalent to a full subcategory of the category of A-motives.

The anti-equivalence is established by the functor $\phi \mapsto M_\phi$ which associates an A-motive M_ϕ to every Drinfeld A-module ϕ by setting $M_\phi = K\{\tau\}$ and letting A act on M_ϕ by $am = m\phi_a$. The functor $\phi \mapsto M_\phi$ is contravariant and fully faithful (cf. Anderson [**1**] Theorem 1). Its image consists of all A-motives which are free of rank 1 over $K\{\tau\}$.

In contrast to the category of Drinfeld A-modules, in the category of A-motives direct sums exist. This is obvious from the definition. In a certain subcategory of A-motives, the subcategory of so-called *pure* A-motives, we also have existence of tensor products. This subcategory includes Drinfeld A-modules, so in the category of A-motives we can form direct sums and tensor products of Drinfeld A-modules. However, tensor products will not be needed in this chapter.

Let M be an A-motive over K. In the following, we shall repeatedly view τ as a Frobenius-linear endomorphism of M, which will then be considered as a module over $K \otimes_{\mathbb{F}_q} A$. This means that τ is viewed as a homomorphism of modules over $K \otimes_{\mathbb{F}_q} A$

$$\tau : \sigma^* M \longrightarrow M$$

where σ is the Frobenius endomorphism on K. The existence of such a Frobenius-linear endomorphism has important consequences. We are going to explain two of these:

Lemma 1.3. *Let V be a finite dimensional K-vector space and let ω be a Frobenius-linear automorphism of V. Then the K^{sep}-vector space $V \otimes_K K^{\mathrm{sep}}$ has an ω-invariant basis, which is also a basis of the $\mathbb{F}_q$-vector space of ω-invariants $(V \otimes_K K^{\mathrm{sep}})^\omega$.*

Proof. Let n be the dimension of V and let σ be the Frobenius endomorphism of K. We can view ω as an isomorphism of K-vector spaces

$$\omega : \sigma^* V \xrightarrow{\sim} V.$$

We choose a K-basis of V and write $\omega = B\sigma$ for some $B \in \mathrm{GL}_n(K)$. Serge Lang's theorem for algebraic groups over finite fields (Lang [**19**] Corollary to Theorem 1) states that the map

$$\begin{aligned} \mathrm{GL}_n(\overline{K}) &\longrightarrow \mathrm{GL}_n(\overline{K}) \\ g &\longmapsto g^{-1}\sigma(g) \end{aligned}$$

is surjective, and the corresponding morphism of algebraic groups is étale. Therefore there exists a matrix $C \in \mathrm{GL}_n(K^{\mathrm{sep}})$ such that $B = C^{-1}\sigma(C)$. Then

$$\omega = B\sigma = C^{-1}\sigma(C)\sigma = C^{-1}\sigma C$$

or equivalently

$$\sigma = C\omega C^{-1}.$$

The columns of C^{-1} are an ω-invariant K^{sep}-basis of $V \otimes_K K^{\mathrm{sep}}$ and an $\mathbb{F}_q$-basis of $(V \otimes_K K^{\mathrm{sep}})^{\omega}$. □

Corollary 1.4. *Let N be a $K \otimes_{\mathbb{F}_q} A$-module which has finite dimension as K-vector space, and assume that N has a Frobenius-linear automorphism. Then there exists a nonzero element of A that annihilates N.*

Proof. Let ω be a Frobenius-linear automorphism of the $K \otimes_{\mathbb{F}_q} A$-module N. By Lemma 1.3 the ω-invariants $(N \otimes_K K^{\mathrm{sep}})^{\omega}$ form a finite A-module, therefore there exists a nonzero a in A that annihilates $(N \otimes_K K^{\mathrm{sep}})^{\omega}$.

Again by Lemma 1.3, we know that $(N \otimes_K K^{\mathrm{sep}})^{\omega}$ generates $N \otimes_K K^{\mathrm{sep}}$ over K^{sep}. It follows that a annihilates $N \otimes_K K^{\mathrm{sep}}$ and in particular N. □

We return to the specific situation of A-motives. As for Drinfeld modules and abelian varieties, we have isogenies as a special class of morphisms. The A-motives being "higher-dimensional" objects, not every nonzero morphism will be an isogeny. Further, we have already seen that the transition from Drinfeld A-modules to A-motives is contravariant, so isogenies of A-motives will not be surjective, but injective mappings.

Definition 1.5 (Isogenies and their degree)**.** An *isogeny* of A-motives is an injective morphism of A-motives with cokernel of finite length. We say that an isogeny η is *separable* if the Frobenius-linear morphism induced by τ on the $K \otimes_{\mathbb{F}_q} A$-module $\operatorname{coker}\eta$ is an automorphism.

Let η be a separable isogeny of A-motives. By Lemma 1.3, the τ-invariants in $(\operatorname{coker}\eta) \otimes_K K^{\mathrm{sep}}$ form a finite A-module and are hence of the form $\bigoplus_{i=1}^{t} A/\mathfrak{a}_i$ for suitable $t > 0$ and ideals $\mathfrak{a}_i \subset A$. The *degree* of η is defined to be the ideal

$$\deg\eta = \prod_{i=1}^{t} \mathfrak{a}_i \subset A.$$

One would expect now that isogenies of A-motives, like isogenies of Drinfeld modules or abelian varieties, admit a *dual isogeny*. Indeed, we have

Proposition 1.6. *Let $\eta : M \to M'$ be a separable isogeny of A-motives. Then there exists a separable isogeny $\widehat{\eta} : M' \to M$ such that the endomorphism $\widehat{\eta} \circ \eta$ of M is multiplication by an element of A.*

Moreover, we can choose $\widehat{\eta}$ such that $\deg\widehat{\eta}$ *is divisible only by primes dividing* $\deg\eta$.

Proof. The cokernel of η is a finite dimensional K-vector space, and as η is separable, τ induces a Frobenius-linear automorphism on $\operatorname{coker}\eta$. Hence by Corollary 1.4 the cokernel of η is annihilated by a nonzero element $a \in A$, and aM' is contained in the image of η. This already guarantees the existence of a dual isogeny

$$\widehat{\eta} : M' \longrightarrow M$$

which makes the diagram

$$\begin{tikzcd} M \arrow[rr, "\eta"] & & M' \\ & M' \arrow[ul, dashed, "\widehat{\eta}"] \arrow[ur, "a"'] & \end{tikzcd}$$

commutative. By construction, the composite morphism $\eta \circ \widehat{\eta}$ is multiplication by a on M'. Since η is a homomorphism of A-modules, we have

$$\eta \circ \widehat{\eta} \circ \eta = a \circ \eta = \eta \circ a.$$

Canceling η on the left (possible because η is injective) yields that the composite $\widehat{\eta} \circ \eta$ is multiplication by a on M.

Because some power of $\deg \eta$ is a principal ideal, we can choose a such that it is only divisible by primes dividing $\deg \eta$. The only primes dividing $\deg \widehat{\eta}$ are the ones dividing a. □

Unwinding the canonical program, we come to torsion modules of A-motives, the associated Tate modules and Galois representations.

As A-motives generalize Drinfeld A-modules, their torsion modules generalize the torsion modules of Drinfeld modules. However, in a sense that will be made precise below, the definition of torsion modules for A-motives is dual to the one for Drinfeld modules.

For the upcoming definition and for the rest of the chapter, we introduce the following notation: For an A-motive M over K, we set

$$\overline{M} = M \otimes_K \overline{K}.$$

We give $\overline{M}$ the structure of a left module over $\overline{K}\{\tau\} \otimes_{\mathbb{F}_q} A$ by defining

$$\tau(m \otimes x) = \tau m \otimes x^q, \quad a(m \otimes x) = am \otimes x \quad \text{and} \quad y(m \otimes x) = m \otimes yx$$

for $x, y \in \overline{K}$, for $a \in A$ and $m \in M$.

Definition 1.7 (Torsion and Tate modules)**.** Let M be an A-motive over K. Then

(1) for any ideal $\mathfrak{a} \subset A$, the *module of* $\mathfrak{a}$*-torsion* of M is defined to be

$$M[\mathfrak{a}] = \left(\overline{M}/\mathfrak{a}\overline{M}\right)^{\tau} = \left\{\overline{m} \in \overline{M}/\mathfrak{a}\overline{M} \;\middle|\; \tau\overline{m} = \overline{m}\right\},$$

(2) for every prime $\mathfrak{p} \subset A$, the $\mathfrak{p}$*-adic Tate module* of M is defined to be

$$T_{\mathfrak{p}}(M) = \varprojlim_i M[\mathfrak{p}^i]$$

where the maps in the inverse system are the quotient maps. We set

$$V_{\mathfrak{p}}(M) = T_{\mathfrak{p}}(M) \otimes_{A_{\mathfrak{p}}} F_{\mathfrak{p}}$$

and call this the *rational* Tate module.

The absolute Galois group G_K acts on $M[\mathfrak{a}]$, on $T_{\mathfrak{p}}(M)$ and on $V_{\mathfrak{p}}(M)$.

We briefly analyze the structure of the torsion modules and Tate modules of A-motives. For any A-motive M over K, set $M^{\text{sep}} = M \otimes_K K^{\text{sep}}$. In the same way as for $\overline{M}$ above, on M^{sep} we define a structure of left module over $K^{\text{sep}}\{\tau\} \otimes_{\mathbb{F}_q} A$.

Proposition 1.8. *Let M be an A-motive over K. Then*

(1) *for all ideals $\mathfrak{a}$ in A not divisible by $\mathfrak{p}_0$, we have*

$$M[\mathfrak{a}] = \left(\overline{M}/\mathfrak{a}\overline{M}\right)^{\tau} = \left(M^{\text{sep}}/\mathfrak{a}M^{\text{sep}}\right)^{\tau},$$

(2) *for all ideals $\mathfrak{a}$ in A not divisible by $\mathfrak{p}_0$, the torsion module $M[\mathfrak{a}]$ is a free module of rank r over $A/\mathfrak{a}$,*

(3) *for all primes $\mathfrak{p} \neq \mathfrak{p}_0$, the Tate module $T_{\mathfrak{p}}(M)$ is a free module of rank r over $A_{\mathfrak{p}}$.*

Proof. For this discussion, confer also Anderson [**1**] Lemma 1.8.2. Let $\mathfrak{a}$ be a nonzero ideal in A not divisible by the characteristic $\mathfrak{p}_0$. First we note that $M/\mathfrak{a}M$ is a K-vector space of finite dimension, say, n. As $\mathfrak{a}$ is not divisible by $\mathfrak{p}_0$, the action of τ on $M/\mathfrak{a}M$ gives a Frobenius-linear automorphism of $M/\mathfrak{a}M$.

By Lemma 1.3, we can choose an $\mathbb{F}_q$-basis of $\left(M^{\text{sep}}/\mathfrak{a}M^{\text{sep}}\right)^{\tau}$ which generates $M^{\text{sep}}/\mathfrak{a}M^{\text{sep}}$. Let r be the rank of M as a projective module over $K \otimes_{\mathbb{F}_q} A$. Then $M/\mathfrak{a}M$ is a free module of rank r over $(K \otimes_{\mathbb{F}_q} A)/(K \otimes_{\mathbb{F}_q} \mathfrak{a})$. It follows that both $\left(\overline{M}/\mathfrak{a}\overline{M}\right)^{\tau}$ and $\left(M^{\text{sep}}/\mathfrak{a}M^{\text{sep}}\right)^{\tau}$ are free of rank r over $A/\mathfrak{a}$. This proves (1) and (2), and (3) is a direct consequence of (2). □

Now that we have seen definitions and structure of A-motives, we want to give the above mentioned duality of the torsion of a Drinfeld A-module and the torsion of the associated A-motive. It reflects the contravariancy of this association:

Proposition 1.9. *Let ϕ be a Drinfeld A-module over K and suppose that the ideals $\mathfrak{p}$ and $\mathfrak{a}$ are not divisible by $\mathfrak{p}_0$. By Ω_A we denote the module of Kähler differentials of A. Then we have canonical G_K-equivariant isomorphisms*

$$\phi[\mathfrak{a}] \cong \operatorname{Hom}_A\left(M_\phi[\mathfrak{a}], \mathfrak{a}^{-1}\Omega_A/\Omega_A\right)$$

and

$$T_{\mathfrak{p}}(\phi) \cong \operatorname{Hom}_{A_{\mathfrak{p}}}\left(T_{\mathfrak{p}}(M_\phi), \Omega_A \otimes_A A_{\mathfrak{p}}\right).$$

Proof. This is explicated in Anderson [**1**] Proposition 1.8.3. □

As for Drinfeld modules, every morphism

$$\eta : M' \longrightarrow M$$

of A-motives induces a G_K-equivariant homomorphism

$$M'[\mathfrak{a}] \longrightarrow M[\mathfrak{a}]$$

on the $\mathfrak{a}$-torsion modules for every ideal $\mathfrak{a}$ in A, as well as a G_K-equivariant homomorphism

$$T_{\mathfrak{p}}(M') \longrightarrow T_{\mathfrak{p}}(M)$$

on the $\mathfrak{p}$-adic Tate modules for every prime $\mathfrak{p}$ in A. We denote the latter homomorphism by $T_{\mathfrak{p}}\eta$.

Now we roughly know torsion and Tate modules of A-motives. This allows us to open up the indispensable resource in this section, the Tate conjecture for A-motives. Its proof is independently due to Yuichiro Taguchi and Akio Tamagawa. We have already cited the result and their proofs in the special case of a Drinfeld module in Theorem I.2.2.

Theorem 1.10 (Tate conjecture for A-motives)**.** *Let M be an A-motive. For all primes $\mathfrak{p}$ of A, different from the characteristic of K, the natural map*

$$\mathrm{End}_K(M) \otimes_A F_{\mathfrak{p}} \longrightarrow \mathrm{End}_{F_{\mathfrak{p}}[G_K]}\big(V_{\mathfrak{p}}(M)\big)$$

is an isomorphism.

Proof. Taguchi [**37**] and [**38**] or Tamagawa [**41**]. □

Finally, we give a description of isogenies of A-motives in terms of Galois invariant lattices in the rational Tate module. By definition, the cokernel of an isogeny has finite length; this means it is nontrivial at only finitely many primes. We are going to see that all information on the cokernel of an isogeny is encoded in the difference of the Tate modules at these primes.

Conversely, such data defines an isogeny. This means, given Galois submodules of full rank in the Tate modules of an A-motive at finitely many primes, there is an isogenous A-motive with the prescribed Tate modules.

Proposition 1.11. *Let M be an A-motive. There exists a bijective correspondence*

$$\big\{[M',\eta] \bigm| \eta : M' \xrightarrow{\text{isog}} M\big\} \longleftrightarrow \big\{(\Lambda_{\mathfrak{p}})_{\mathfrak{p}\neq\mathfrak{p}_0} \bigm| \Lambda_{\mathfrak{p}} \subset V_{\mathfrak{p}}(M)\big\} \big/ F^*$$

where $[M',\eta]$ is an isomorphism class of pairs of A-motives M' together with a separable isogeny $\eta : M' \to M$ of degree not divisible by $\mathfrak{p}_0$, and where $(\Lambda_{\mathfrak{p}})_{\mathfrak{p}\neq\mathfrak{p}_0}$ is a family of G_K-invariant $A_{\mathfrak{p}}$-lattices $\Lambda_{\mathfrak{p}} \subset V_{\mathfrak{p}}(M)$ such that $\Lambda_{\mathfrak{p}} = T_{\mathfrak{p}}(M)$ for almost all $\mathfrak{p}$.

Proof. Let $\eta : M' \to M$ be a separable isogeny of degree not divisible by $\mathfrak{p}_0$. Then $T_{\mathfrak{p}}\eta\big(T_{\mathfrak{p}}(M')\big)$ is a G_K-invariant $A_{\mathfrak{p}}$-lattice in $V_{\mathfrak{p}}(M)$ for all $\mathfrak{p} \neq \mathfrak{p}_0$, and

$$T_{\mathfrak{p}}\eta\big(T_{\mathfrak{p}}(M')\big) = T_{\mathfrak{p}}(M)$$

for almost all $\mathfrak{p}$. Clearly we get the same family of lattices if we change (M', η) by an isomorphism.

Conversely, let a family $(\Lambda_\mathfrak{p})_{\mathfrak{p}\neq\mathfrak{p}_0}$ as in the proposition be given. We consider families of lattices up to multiplication with F^*, thus we may assume that $\Lambda_\mathfrak{p}$ is a submodule of $T_\mathfrak{p}(M)$ for all $\mathfrak{p}$.

Let $\mathfrak{p}_1$ be a prime different from $\mathfrak{p}_0$ at which $\Lambda_{\mathfrak{p}_1} \neq T_{\mathfrak{p}_1}(M)$. The quotient $T_{\mathfrak{p}_1}(M)/\Lambda_{\mathfrak{p}_1}$ is contained in $M[\mathfrak{p}_1^m]$ for some $m > 0$. Let

$$N = \Lambda_{\mathfrak{p}_1} \Big/ \big(\Lambda_{\mathfrak{p}_1} \cap \mathfrak{p}_1^m T_{\mathfrak{p}_1}(M)\big) \subset M[\mathfrak{p}_1^m].$$

By $\pi : \overline{M} \to \overline{M}/\mathfrak{p}_1^m\overline{M}$ we denote the quotient map. We set

$$\overline{M_1} = \pi^{-1}\big(N \otimes_{\mathbb{F}_q} \overline{K}\big) \quad \text{and} \quad M_1 = \big(\overline{M_1}\big)^{G_K}.$$

Then M_1 is an A-motive over K and the inclusion map $M_1 \hookrightarrow M$ is an isogeny of $\mathfrak{p}_1$-power degree. We apply this construction recursively for every prime at which $\Lambda_\mathfrak{p} \neq T_\mathfrak{p}(M)$ and obtain an A-motive M' such that $T_\mathfrak{p}(M') = \Lambda_\mathfrak{p}$ for all $\mathfrak{p} \neq \mathfrak{p}_0$. $\square$

2. Extending the Base Field

This section is obsolete. It has been written at a time when only weaker versions of Theorem I.4.3 and Corollary I.4.5 were available. Proposition 2.1 was intended for allowing an extension of the base field in the proof of Theorem 3.1. It follows trivially from Theorem 3.1 which can now be proved by means of the above mentioned results without base field extension. Therefore the present section can be skipped without loss of information.

In this and the next section, assume that the A-field K has special characteristic $\mathfrak{p}_0$, and let M be a finite direct sum of A-motives associated to Drinfeld A-modules defined over K. It is silently understood that all morphisms are defined over K unless explicitely mentioned.

Preparing a reduction step in the proof of our main theorem, we investigate how extensions of the base field affect the isomorphism classes in the isogeny class of M. We want to prove that a finite base field extension causes only a finite number of isomorphism classes to “collapse”.

If K'/K is a field extension, we set $M' = M \otimes_K K'$ and write $E' = \mathrm{End}_{K'}(M')$ and $E'_F = E' \otimes_A F$.

Proposition 2.1. *Let K' be a finite separable field extension of K. Then there are only finitely many K-isomorphism classes of A-motives K-isogenous to M that become isomorphic to M' over K'.*

The proof of this proposition, split into three arguments, will occupy the rest of the present section.

Because every finite separable extension is contained in a finite Galois extension, it suffices to carry out the case that K'/K is a Galois extension. We set $G = \mathrm{Gal}(K'/K)$.

The following argument will use nonabelian Galois cohomology. For this end, we need to introduce the appropriate Galois actions. Let $E'_F[G]$ be the "crossed" group ring which is defined by the multiplication rule

$$a_1[\sigma_1] \cdot a_2[\sigma_2] = a_1\sigma_1(a_2)[\sigma_1\sigma_2]$$

for $a_1, a_2 \in E'_F$ and $\sigma_1, \sigma_2 \in G$. Then E'_F is a left $E'_F[G]$-module via

$$\Bigl(\sum_{\sigma\in G} a_\sigma[\sigma]\Bigr) \cdot b = \sum_{\sigma\in G}\Bigl(a_\sigma\sigma(b)\Bigr)$$

for $a_\sigma, b \in E'_F$.

The commutant of E'_F as $E'_F[G]$-module consists of the G-invariants $(E'_F)^G$ operating on E'_F by right multiplication. Therefore E'_F can be considered as a module over $E'_F[G] \otimes_F (E'^G_F)^{\mathrm{opp}}$.

The first step in the proof is an observation on the structure of E'_F as a module over $E'_F[G]$. It creates the basis for a forthcoming application of the Jordan-Zassenhaus theorem.

Lemma 2.2. *The $E'_F[G]$-module E'_F is semisimple.*

Proof. By assumption, M is a direct sum of A-motives associated to Drinfeld A-modules defined over K, say $M = \bigoplus_i M_{\phi_i}$. Therefore, as an F-module,

$$E'_F = \mathrm{End}_{K'}(M') \otimes_A F = \bigoplus_i \bigoplus_j \mathrm{Hom}_{K'}\bigl(M'_{\phi_i}, M'_{\phi_j}\bigr) \otimes_A F.$$

For every i and j set

$$H_{i,j} = \mathrm{Hom}_{K'}\bigl(M'_{\phi_i}, M'_{\phi_j}\bigr) \otimes_A F \subset E'_F.$$

Because all M_{ϕ_i} are associated to Drinfeld modules defined over K, every $H_{i,j}$ is invariant under the action of G. Moreover, for all i the F-module $\bigoplus_j H_{i,j}$ is invariant under the action of E'_F. Thus $\bigoplus_j H_{i,j}$ is a module over $E'_F[G]$ for all i.

Now for given i, j, either the two Drinfeld modules ϕ_i and ϕ_j are non-isogenous over K', then $H_{i,j}$ is zero, or they are isogenous over K', in which case $H_{i,j}$ must be simple as a module over $H_{j,j}$. Further, for all ℓ every nonzero element of $H_{j,\ell}$ induces a homomorphism

$$H_{i,j} \to H_{i,\ell},$$

and if both sides are nontrivial, such a map must be an E'_F-isomorphism. Hence for every i the action of E'_F on $\bigoplus_j H_{i,j}$ permutes the nontrivial $H_{i,j}$ transitively.

We see that each $\bigoplus_j H_{i,j}$ is a simple module over E'_F, in particular it is simple over $E'_F[G_K]$. This yields the claim. $\square$

With the following algebraic result we complete the preparation for the proof of Proposition 2.1. It gives reformulation of the Jordan-Zassenhaus theorem which fits better into the context at the end of this section.

Lemma 2.3. *Let B be an A-order in a semisimple F-algebra B_F and let N_F be a finitely generated B_F-module. We write $C_F = \mathrm{End}_{B_F}(N_F)$.*

Then up to elements of C_F^*, there is only a finite number of finitely generated B-submodules $N \subset N_F$ such that $N \otimes_A F = N_F$.

Proof. The Jordan-Zassenhaus theorem (see Appendix A.2) states that there exist only finitely many isomorphism classes of B-invariant A-lattices of given rank. Every isomorphism of two B-invariant A-lattices in N_F extends to an element of C_F^*, whence the assertion. □

The standard approach for dealing with the problem of Proposition 2.1 are K'/K-forms, principal homogeneous spaces and nonabelian Galois cohomology, as explained in detail in Serre [**32**]. In our case, the cohomology set in question is not obviously finite. Therefore we transform the problem, given in terms of Galois cohomology, into the setting of lattices in a module over a semisimple algebra, in which the Jordan-Zassenhaus theorem is at our disposal.

Proof of Proposition 2.1. We define $\mathcal{F}(K'/K, M)$ to be the set of K-isomorphism classes of K'/K-forms of M, i. e. of A-motives over K that become isomorphic to M' over K'.

If N is a K'/K-form of M, then the set of K'-isomorphisms from N' to M' is a principal homogeneous space over the G-group E'^*. By Serre [**32**] I.5.2 it defines an element of the cohomology set $H^1(G, E'^*)$.

This induces a well-defined injection of the K-isomorphism classes of K'/K-forms of M into $H^1(G, E'^*)$. Further, via Galois descent, we can reverse this construction. Therefore we get a canonical bijection

$$\mathcal{F}(K'/K, M) \xrightarrow{\sim} H^1(G, E'^*).$$

The K'/K-forms of M relevant to our problem are the ones that are K-isogenous to M. In order to determine these, consider an element of $H^1(G, E_F'^*)$: it is the class of a principal homogeneous space

$$\big(\mathrm{Hom}_{K'}(N', M') \otimes_A F\big)^*$$

for some K'/K-form N of M. We claim that two such principal homogeneous spaces

$$\big(\mathrm{Hom}_{K'}(N_1', M') \otimes_A F\big)^* \quad \text{and} \quad \big(\mathrm{Hom}_{K'}(N_2', M') \otimes_A F\big)^*$$

belong to the same class if and only if N_1 and N_2 are K-isogenous. In order to see this, we first note that a morphism of A-motives is an isogeny if and only if it becomes invertible in the ring of morphisms tensored with F. Then the "only if" part is obvious. In the opposite direction, the isomorphism of principal homogeneous spaces and the G-action yield a K'-isogeny $N_1' \to N_2'$ together with a Galois descent datum. This defines a K-isogeny $N_1 \to N_2$. (For the theory of descent in general cf. SGA 1 §1 (Grothendieck [**14**]), and for Galois descent in particular Knus-Ojanguren [**18**] §5.)

So we have seen that the K'/K-forms of M we need to consider are the ones in the kernel of the morphism of pointed sets

$$\varepsilon : H^1(G, E'^*) \longrightarrow H^1(G, E'^*_F).$$

We are going to prove that the kernel of ε is finite. By definition

$$\ker \varepsilon = \left\{ (\gamma_\sigma) \in Z^1(G, E'^*) \,\middle|\, \exists g \in E'^*_F : \forall \sigma \in G : \sigma(g)g^{-1} = \gamma_\sigma \right\} \Big/ \!\sim$$

where $(\gamma_\sigma) \sim (\gamma'_\sigma) \iff \exists \gamma \in E'^* : (\gamma'_\sigma) = (\sigma(\gamma)\gamma_\sigma\gamma^{-1})$. Differently put, this is the set of equivalence classes

$$\left\{ g \in E'^*_F \,\middle|\, \forall \sigma : \sigma(g)g^{-1} \in E'^* \right\} \Big/ \!\sim$$

where $g \sim g' \iff \exists \gamma \in E'^* : \forall \sigma \in G : \sigma(\gamma)\sigma(g)g^{-1}\gamma^{-1} = \sigma(g')g'^{-1}$. Having a look at the condition for equivalence of two such elements, we see that

$$\begin{aligned} g \sim g' &\iff \exists \gamma \in E'^* : \forall \sigma \in G : \sigma(g'^{-1}\gamma g) = g'^{-1}\gamma g \\ &\iff \exists \gamma \in E'^* : g'^{-1}\gamma g \in (E'^*_F)^G \\ &\iff \exists \gamma \in E'^* : \exists h \in (E'^*_F)^G : g' = \gamma g h. \end{aligned}$$

It follows that the above equivalence classes correspond bijectively to the elements of

$$\left\{ [g] \in E'^* \backslash E'^*_F / (E'^*_F)^G \,\middle|\, \forall \sigma \in G : \sigma(g)g^{-1} \in E'^* \right\}.$$

We rewrite the condition on the double cosets $[g]$ in this set as follows:

$$\begin{aligned} & \forall \sigma \in G : \sigma(g)g^{-1} \in E'^* \\ \iff & \forall \sigma \in G : E'^*\sigma(g) = E'^* g \\ \iff & \forall \sigma \in G : \sigma(E'g) = E'\sigma(g) = E'g \\ \iff & E'g \text{ is } G\text{-invariant.} \end{aligned}$$

So we get a bijective correspondence of these double cosets with the elements of

$$\left\{ \text{left } E'[G]\text{-submodules of } E'_F, \text{ free of rank 1 as } E'\text{-modules} \right\} \Big/ \, (E'^*_F)^G$$

which form a subset of

$$\left\{ E'[G]\text{-submodules } N \subset E'_F, \text{ finitely generated, s.t. } N \otimes_A F = E'_F \right\} \Big/ \, (E'^*_F)^G.$$

Now we note that Lemma 2.2 is equivalent to the image of $E'_F[G]$ in $\mathrm{End}_F(E'_F)$ being a semisimple F-algebra. Together with Lemma 2.3 this implies that the last set is finite. □

3. The Isogeny Conjecture for A-Motives

In the final part we present the main result of Chapter II, the isogeny conjecture for a certain class of A-motives. As in the preceding section, we assume that K has special characteristic, we let M be an A-motive over K and require M to be the direct sum of A-motives associated to Drinfeld A-modules over K. Under this condition, we can prove

Theorem 3.1 (= Theorem C: Isogeny conjecture for A-motives)**.** *Let M be an A-motive which is the direct sum of A-motives associated to Drinfeld A-modules defined over K.*

Then, up to K-isomorphism, there are only finitely many A-motives M' for which there exists a separable K-isogeny $M' \to M$ of degree not divisible by the characteristic of K.

One should expect this assertion to hold for any A-motive that is semisimple up to isogeny and in generic characteristic, as well. The assumption of special characteristic is imposed by Section I.3. Assuming a version of the absolute irreducibity theorem I.3.1 for generic characteristic, our proof yields Theorem 3.1 without restriction on the characteristic.

The restriction on the structure of M, however, is more fundamental. As the argument rests on the results of Chapter I, the techniques we use do not reach far enough to give a proof for more general A-motives. Here a different approach seems to be inevitable.

After these remarks on the scope of our result, we start into the proof of Theorem 3.1 with some notation. We want to group direct summands of M which are isogenous. So we write

$$M = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{k_i} M_{\phi^{i,j}}$$

with Drinfeld A-modules $\phi^{i,j}$ such that for each i all $\phi^{i,j}$ belong to the same isogeny class and for $i_1 \neq i_2$ and all j the Drinfeld modules $\phi^{i_1,j}$ and $\phi^{i_2,j}$ are non-isomorphic.

Now for such an A-motive M Proposition 1.9 yields that for every nonzero ideal $\mathfrak{a}$ in A the torsion module

$$M[\mathfrak{a}] = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{k_i} M_{\phi^{i,j}}[\mathfrak{a}]$$

is dual to

$$\bigoplus_{i=1}^{n} \bigoplus_{j=1}^{k_i} \phi^{i,j}[\mathfrak{a}],$$

and for each $M_{\phi^{i,j}}[\mathfrak{a}]$ the results of Sections I.4 and I.5 apply.

The first ingredient in the proof of Theorem 3.1 is an analog of Proposition I.2.6 for A-motives. It characterizes the G_K-invariant submodules of the Tate module as the images of G_K-equivariant endomorphisms. The proposition is preceded by an algebraic auxiliary, and by a lemma which allows a decomposition of Galois invariant submodules of the Tate module.

Lemma 3.2. *Let R be a principal ideal domain and $s, t > 0$. We set $N = (R^s)^t$ and let $B = \mathrm{Mat}_{s\times s}(R)$ act on N in the obvious way. Set further $C = \mathrm{End}_B(N)$. Then every B-submodule of N is the image of an element of C.*

Proof. Let $V = R^t$ be the evident representation of $C \cong \mathrm{Mat}_{t\times t}(R)$, and set $W = \mathrm{Hom}_C(V, N)$. Then $W \cong R^s$ is a free R-module; we choose a basis $\{e_j\}$. If we let B act trivially on V and C act trivially on W, then we get a natural isomorphism of $C \otimes_R B$-modules

$$V \otimes_R W \xrightarrow{\sim} N.$$

Now let H be a nontrivial B-submodule of N. Note that the projection pr_j on the j-th component of W is an element of B. Hence H contains $\mathrm{pr}_j(H)$. For $\sum_i v_i \otimes w_i \in H$ we have

$$\mathrm{pr}_j\Big(\sum_i v_i \otimes w_i\Big) = \sum_i \big(v_i \otimes \mathrm{pr}_j(w_i)\big) = \sum_i \big(v_i \otimes \alpha_{i,j} e_j\big) = \Big(\sum_i \alpha_{i,j} v_i\Big) \otimes e_j$$

with suitable $\alpha_{i,j} \in R$. Thus $\mathrm{pr}_j(H) = H_j \otimes e_j$ for an R-submodule H_j of V. The B-submodule of N generated by $H_j \otimes e_j$ is $H_j \otimes_R W$, it is a submodule of H. Then we get

$$H = \bigoplus_j \mathrm{pr}_j(H) = \bigoplus_j H_j \otimes e_j \subset \sum_j \big(H_j \otimes_R W\big) \subset H.$$

Therefore

$$H = \sum_j \big(H_j \otimes_R W\big) = \Big(\sum_j H_j\Big) \otimes_R W.$$

But $\sum_j H_j$, as a submodule of the free module V over the principal ideal domain R, is the image of an element of $\mathrm{End}_R(V) = C$. □

Lemma 3.3. *For almost all primes $\mathfrak{p}$ of A, every $A_\mathfrak{p}[G_K]$-submodule H of $T_\mathfrak{p}(M)$ has a decomposition $H = \bigoplus_{i=1}^n H_i$ into inequivalent $A_\mathfrak{p}[G_K]$-submodules H_i of $T_\mathfrak{p}\big(\bigoplus_{j=1}^{k_i} M_{\phi^{i,j}}\big)$.*

Proof. By Theorem I.5.1 we know that for almost all $\mathfrak{p}$ and all j_1, j_2 the $k_\mathfrak{p}[G_K]$-modules $M_{\phi^{i_1,j_1}}[\mathfrak{p}]$ and $M_{\phi^{i_2,j_2}}[\mathfrak{p}]$ have no nontrivial common subquotient if $i_1 \neq i_2$.

As for every $\ell > 0$ the modules $M_{\phi^{i_1,j}}[\mathfrak{p}^\ell]$ and $M_{\phi^{i_2,j}}[\mathfrak{p}^\ell]$ are successive extensions of copies of $M_{\phi^{i_1,j}}[\mathfrak{p}]$ and $M_{\phi^{i_2,j}}[\mathfrak{p}]$, respectively, they have no nontrivial common subquotient, either. The same property holds for the projective limits and the lemma follows. □

Proposition 3.4. *There exists a finite set S_0 of primes of A such that for all $\mathfrak{p}$ outside S_0, every $A_\mathfrak{p}[G_K]$-submodule of $T_\mathfrak{p}(M)$ is the image of an endomorphism in* $\mathrm{End}_{A_\mathfrak{p}[G_K]}\big(T_\mathfrak{p}(M)\big)$.

Proof. Let S_0 be the finite set of primes for which Lemma 3.3 fails, plus the characteristic $\mathfrak{p}_0$. We choose a prime $\mathfrak{p}$ outside S_0 and let H be an $A_\mathfrak{p}[G_K]$-submodule of $T_\mathfrak{p}(M)$. By Lemma 3.3, the module H has a decomposition $H = \bigoplus_{i=1}^n H_i$ into inequivalent $A_\mathfrak{p}[G_K]$-submodules

$$H_i \subset T_\mathfrak{p}\Big(\bigoplus_{j=1}^{k_i} M_{\phi^{i,j}}\Big).$$

So we may reduce to the case that $n = 1$, which means that $M = \bigoplus_{j=1}^{k} M_{\phi^j}$ for Drinfeld A-modules ϕ^j all belonging to the same isogeny class.

For almost all primes $\mathfrak{p}$ in A and all j_1, j_2 we have $T_{\mathfrak{p}}(M_{\phi^{j_1}}) \cong T_{\mathfrak{p}}(M_{\phi^{j_2}})$. We extend S_0 by the finitely many primes of A for which this does not hold. Then for all $\mathfrak{p}$ outside S_0 we get $T_{\mathfrak{p}}(M) \cong T_{\mathfrak{p}}\big((M_{\phi^1})^{\oplus k}\big)$. We write $\phi = \phi^1$.

Let Z be the center of $\mathrm{End}_K(\phi)$. By m we denote the inseparable degree of Z over A. We extend S_0 by the finitely many primes $\mathfrak{p}$ of A which do not decompose as $\mathfrak{p} = \prod_{i=1}^{s} \mathfrak{P}_i^m$ into prime ideals $\mathfrak{P}_i \subset Z$. Let M' be the Z-motive $(M_{\phi'})^{\oplus k}$ where ϕ' is the Drinfeld Z-module extending ϕ according to Remark I.4.6. Then for all $\mathfrak{p}$ outside S_0 we have

$$T_{\mathfrak{p}}(M) = \bigoplus_{i=1}^{s} T_{\mathfrak{P}_i}(M')$$

as $A_{\mathfrak{p}}[G_K]$-modules and as $Z[G_K]$-modules. From Lemma I.4.16 it follows that for every choice of i, j with $i \neq j$ the $Z[G_K]$-modules $T_{\mathfrak{P}_i}(M')$ and $T_{\mathfrak{P}_j}(M')$ have no equivalent subquotients. Therefore every $A_{\mathfrak{p}}[G_K]$-submodule of $T_{\mathfrak{p}}(M)$ is a direct sum of inequivalent $Z_{\mathfrak{P}_i}[G_K]$-submodules of $T_{\mathfrak{P}_i}(M')$.

Now add to S_0 the finitely many primes in A at which Theorem I.4.3 does not hold for ϕ, and let $\mathfrak{p}$ be a prime outside S_0. The image of $A_{\mathfrak{p}}[G_K]$ in $\mathrm{End}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(M)\big)$ is isomorphic to the image of $A_{\mathfrak{p}}[G_K]$ in $\mathrm{End}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(\phi)\big)$. The latter is the projective limit of the images of $A[G_K]$ in $\mathrm{End}_A\big(\phi[\mathfrak{p}^j]\big)$, which by Theorem I.4.3 (2) are

$$\bigoplus_{i=1}^{s} \mathrm{Mat}_{e\times e}\big(Z/\mathfrak{P}_i^{mj}\big)$$

for suitable $e \mid \mathrm{rk}\,\phi'$. Thus the image of $A_{\mathfrak{p}}[G_K]$ in $\mathrm{End}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(M)\big)$ is isomorphic to

$$\bigoplus_{i=1}^{s} \mathrm{Mat}_{e\times e}\big(Z_{\mathfrak{P}_i}\big).$$

Applying Lemma 3.2 for each summand completes the proof. □

From now on we write $E = \mathrm{End}_K(M)$ and $E_{\mathfrak{p}} = E \otimes_A A_{\mathfrak{p}}$. By $\Gamma_{\mathfrak{p}}$ we denote the image of G_K in $\mathrm{Aut}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(M)\big)$. Then $\Gamma_{\mathfrak{p}}$ is contained in $\mathrm{Aut}_{E_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(M)\big)$.

In the following lemma we investigate the group ring generated by the image of Galois in the endomorphism ring of $V_{\mathfrak{p}}(M)$ and see that it is as large as we can hope for.

Lemma 3.5. *For all primes $\mathfrak{p}$ of A, different from $\mathfrak{p}_0$, the group ring $A_{\mathfrak{p}}[\Gamma_{\mathfrak{p}}]$ is an $A_{\mathfrak{p}}$-order in* $\mathrm{End}_{E_{\mathfrak{p}}}\big(V_{\mathfrak{p}}(M)\big)$.

Proof. As a consequence of Theorem I.2.1, the $F_{\mathfrak{p}}[G_K]$-module

$$V_{\mathfrak{p}}(M) = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{k_i} V_{\mathfrak{p}}\big(M_{\phi^{i,j}}\big)$$

is semisimple. Therefore Jacobson's density theorem (Lang [**20**] XVII Theorem 3.2) yields that $F_\mathfrak{p}[\Gamma_\mathfrak{p}]$ is its own bicommutant in $\mathrm{End}_{F_\mathfrak{p}}\big(V_\mathfrak{p}(M)\big)$. By the Tate conjecture, we know that $E \otimes_A F_\mathfrak{p}$ is the commutant of $F_\mathfrak{p}[\Gamma_\mathfrak{p}]$, thus $F_\mathfrak{p}[\Gamma_\mathfrak{p}]$ is the commutant of $E \otimes_A F_\mathfrak{p}$. This yields the claim. □

The next two results deal with the action of $(E \otimes_A F_\mathfrak{p})^*$ on the G_K-invariant lattices in $V_\mathfrak{p}(M)$. We show that the action is almost always transitive and always "almost transitive".

Lemma 3.6. *For all primes $\mathfrak{p}$ of A, different from $\mathfrak{p}_0$, the number of orbits of the action of $(E \otimes_A F_\mathfrak{p})^*$ on the set of G_K-invariant $A_\mathfrak{p}$-lattices in $V_\mathfrak{p}(M)$ is finite.*

Proof. From the proof of Lemma 3.5 we retain that $V_\mathfrak{p}(M)$ is semisimple as a module over $F_\mathfrak{p}[G_K]$, and that $\mathrm{End}_{E_\mathfrak{p}}\big(V_\mathfrak{p}(M)\big)$ is the commutant of $\mathrm{End}_{F_\mathfrak{p}[G_K]}\big(V_\mathfrak{p}(M)\big)$ in $\mathrm{End}_{F_\mathfrak{p}}\big(V_\mathfrak{p}(M)\big)$. These two facts show that $\mathrm{End}_{E_\mathfrak{p}}\big(V_\mathfrak{p}(M)\big)$ is a semisimple $F_\mathfrak{p}$-algebra.

By Lemma 3.5 we know that $A_\mathfrak{p}[\Gamma_\mathfrak{p}]$ is an order in $\mathrm{End}_{E_\mathfrak{p}}(V_\mathfrak{p}(M))$. Hence we may apply the Jordan-Zassenhaus theorem (see Appendix A.2) which tells us that there are only finitely many isomorphism classes of $A_\mathfrak{p}[\Gamma_\mathfrak{p}]$-invariant $A_\mathfrak{p}$-lattices in $V_\mathfrak{p}(M)$.

Every isomorphism of G_K-invariant $A_\mathfrak{p}$-lattices in $V_\mathfrak{p}(M)$ extends to a G_K-equivariant automorphism of $V_\mathfrak{p}(M)$. By the Tate conjecture, these are precisely the elements of $(E \otimes_A F_\mathfrak{p})^*$. □

Lemma 3.7. *For all primes $\mathfrak{p}$ outside $S_0 \cup \{\mathfrak{p}_0\}$, the action of $(E \otimes_A F_\mathfrak{p})^*$ on the set of G_K-invariant $A_\mathfrak{p}$-lattices in $V_\mathfrak{p}(M)$ is transitive.*

Proof. Let $\mathfrak{p}$ be a prime outside $S_0 \cup \{\mathfrak{p}_0\}$ and let $\Lambda_\mathfrak{p}$ be a G_K-invariant $A_\mathfrak{p}$-lattice in $V_\mathfrak{p}(M)$. There exists an element $\alpha \in A_\mathfrak{p}$ such that $\alpha\Lambda_\mathfrak{p} \subset T_\mathfrak{p}(M)$. By Proposition 3.4 we know that $\alpha\Lambda_\mathfrak{p}$ is the image of a G_K-equivariant endomorphism ε of $T_\mathfrak{p}(M)$.

Then there is a G_K-equivariant homomorphism $\eta : \Lambda_\mathfrak{p} \to T_\mathfrak{p}(M)$ which makes the diagram

$$\begin{tikzcd} \Lambda_\mathfrak{p} \arrow[rr, "\alpha"] \arrow[dr, dashed, "\eta"'] & & T_\mathfrak{p}(M) \\ & T_\mathfrak{p}(M) \arrow[ur, "\varepsilon"'] & \end{tikzcd}$$

commutative. By construction η is an isomorphism. It extends to a G_K-equivariant automorphism of $V_\mathfrak{p}(M)$, thus to an element of $(E \otimes_A F_\mathfrak{p})^*$. □

At the end, we adopt an adelic view on these lattices and establish the link with isogenies of A-motives.

Let $S = \{\infty, \mathfrak{p}_0\}$ be the set containing the place at infinity and the characteristic of K. Let

$$\mathbb{A}_F^S = \prod_{\mathfrak{p} \notin S} F_\mathfrak{p} \quad \text{and} \quad \widehat{A}^S = \prod_{\mathfrak{p} \notin S} A_\mathfrak{p}$$

be the ring of partial adèles of F away from S and the subring of S-integral adèles, respectively.

Lemma 3.8. *The number of double cosets*

$$\big(E \otimes_A F\big)^* \setminus \big(E \otimes_A \mathbb{A}_F^S\big)^* \,/\, \big(E \otimes_A \widehat{A}^S\big)^*$$

is finite.

Proof. For every $\underline{e} \in \big(E \otimes_A \mathbb{A}_F^S\big)^*$, we define

$$\Lambda_{\underline{e}} = \big(E \otimes_A \widehat{A}^S\big) \cdot \underline{e}^{-1} \cap E \otimes_A F.$$

Then $\Lambda_{\underline{e}}$ is a left E-module and discrete as an A-module in $E \otimes_A F$. As $\underline{e}^{-1}$ has only finitely many poles, we have $\Lambda_{\overline{e}} \otimes_A F = E \otimes_A F$. Hence it is an E-invariant A-lattice in $E \otimes_A F$. For all $\varepsilon \in (E \otimes_A F)^*$ and $\underline{k} \in \big(E \otimes_A \widehat{A}^S\big)^*$, we have the transformation rule

$$\Lambda_{\varepsilon \underline{e} \underline{k}} = \Lambda_{\underline{e}} \varepsilon^{-1}.$$

Now assume we are given two E-invariant A-lattices of the form $\Lambda_{\underline{e}}$ and $\Lambda_{\underline{e}'}$ in $E \otimes_A F$. They are isomorphic if and only if there exists an $\varepsilon \in (E \otimes_A F)^*$ such that

$$\Lambda_{\varepsilon \underline{e}} = \Lambda_{\underline{e}} \varepsilon^{-1} = \Lambda_{\underline{e}'}.$$

Tensoring a lattice $\Lambda_{\underline{e}}$ with $\widehat{A}^S$, we recover the coset of $E \otimes_A \widehat{A}^S$ in $E \otimes_A \mathbb{A}_F^S$ defined by $\underline{e}$. Therefore the above equality is equivalent to

$$\big(E \otimes_A \widehat{A}^S\big)(\varepsilon \underline{e})^{-1} = \Lambda_{\varepsilon \underline{e}} \otimes_A \widehat{A}^S = \Lambda_{\underline{e}'} \otimes_A \widehat{A}^S = \big(E \otimes_A \widehat{A}^S\big)(\underline{e}')^{-1}.$$

These equalities hold if and only if

$$\underline{e}' \in \varepsilon \underline{e} \big(E \otimes_A \widehat{A}^S\big)^*.$$

This means that $\underline{e}$ and $\underline{e}'$ belong to the same double coset.

Consequently the double cosets can be identified with isomorphism classes of E-invariant A-lattices in $E \otimes_A F$ of rank at most $\mathrm{rk}_A E$.

We recall that E is an order in the semisimple A-algebra $E \otimes_A F$. Therefore by the Jordan-Zassenhaus theorem there are only finitely many isomorphism classes of E-invariant A-lattices in $E \otimes_A F$ of bounded rank. $\square$

We are now ready to conclude and give the proof of Theorem 3.1. The argument follows Deligne [**7**] Corollaire 2.8, where the case of abelian varieties over number fields is treated.

Proof of Theorem 3.1. We have seen in Proposition 1.11 that the isomorphism classes of isogenies $M' \to M$ correspond bijectively to families $(\Lambda_\mathfrak{p})_{\mathfrak{p} \notin S}$ of G_K-invariant $A_\mathfrak{p}$-lattices $\Lambda_\mathfrak{p}$ in $V_\mathfrak{p}(M)$ such that $\Lambda_\mathfrak{p} = T_\mathfrak{p}(M)$ for all but finitely many $\mathfrak{p}$. The A-motive M' is isomorphic to M if and only if there exists $\eta \in (E \otimes_A F)^*$ with $\eta \Lambda_\mathfrak{p} = T_\mathfrak{p}(M)$ for all $\mathfrak{p}$.

The group $\big(E \otimes \mathbb{A}_F^S\big)^*$ acts on the set of families $(\Lambda_\mathfrak{p})_{\mathfrak{p} \notin S}$ of G_K-invariant $A_\mathfrak{p}$-lattices in $V_\mathfrak{p}(M)$ such that $\Lambda_\mathfrak{p} = T_\mathfrak{p}(M)$ for almost all $\mathfrak{p}$. By Lemmata 3.6 and 3.7 the number of orbits under this action is finite.

Fix one of these orbits and let $\mathcal{K}$ be the stabilizer of a family of lattices in this orbit. Then $\mathcal{K}$ is an open compact subgroup of $\big(E \otimes \mathbb{A}_F^S\big)^*$. It is conjugate to the stabilizer of any family of lattices in the orbit. Thus the isomorphism classes of A-motives corresponding to this orbit can be identified with the double cosets in

$$\left(E \otimes_A F\right)^* \setminus \left(E \otimes_A \mathbb{A}_F^S\right)^* / \mathcal{K}.$$

We have to show that the number of these double cosets is finite.

Note that if the number of these double cosets is finite, then the number of double cosets is finite for any open compact subgroup of $\left(E \otimes_A \mathbb{A}_F^S\right)^*$ in the place of $\mathcal{K}$. Hence we may replace $\mathcal{K}$ by $\left(E \otimes_A \widehat{A}^S\right)^*$. Thus the problem is reduced to the finiteness of the class number.

Then the proof is either completed by another application of the Jordan-Zassenhaus theorem, as carried out in Lemma 3.8, or using general theory: By Behr [**2**] Satz 7 the class number of a reductive algebraic group over a global field is finite, and we know that $(E \otimes_A F)^*$ is reductive over its center. Thanks to the reduction theory developed in Harder [**15**], the extra conditions (V) in Behr's paper are obsolete. $\square$

APPENDIX A

Background from Other Areas

1. Deligne's Equidistribution Theorem

In the study of representations of the absolute Galois group, important information is given by Frobenius elements. The classical result in this context is Čebotarev's density theorem. It yields that Frobenius elements form a dense subset of the absolute Galois group.

A much stronger result on Frobenius elements has been obtained by Deligne in the article [**6**] *La conjecture de Weil II*. He could show that they are not only dense but equidistributed. In this section we want to state Deligne's theorem and roughly explain the meaning of "equidistributed".

The following paragraphs are an extract of Katz [**17**] Chapter 3. More details and background are given in Katz' text. The original source for Theorem 1.1 is Deligne [**6**] (3.5), in particular Théorème 3.5.3.

Fix an embedding $\overline{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$. We let $\mathcal{U}$ be a smooth, geometrically connected curve over $\mathbb{F}_q$, which is the complement of a finite set of closed points on a proper smooth geometrically connected curve over $\mathbb{F}_q$. By $\overline{x}$ we denote a geometric point of $\mathcal{U}$ and we set

$$\pi_1^{\mathrm{arith}} = \pi_1\big(\mathcal{U}, \overline{x}\big) \quad \text{and} \quad \pi_1^{\mathrm{geom}} = \pi_1\big(\mathcal{U} \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{x}\big).$$

Suppose given a lisse $\overline{\mathbb{Q}_\ell}$-sheaf $\mathcal{F}$ on $\mathcal{U}$ of rank $n \geq 1$ which is pointwise pure of weight 0 with respect to the complex embedding of $\overline{\mathbb{Q}_\ell}$ and let

$$\rho : \pi_1^{\mathrm{arith}} \longrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}_\ell}}\big(\mathcal{F}_{\overline{x}}\big) \cong \mathrm{GL}_n\big(\overline{\mathbb{Q}_\ell}\big)$$

be the monodromy representation of $\mathcal{F}$.

By G we denote the Zariski closure of $\rho\big(\pi_1^{\mathrm{geom}}\big)$ in $\mathrm{GL}_{n,\overline{\mathbb{Q}_\ell}}$. We let $\mathcal{K}$ be a maximal compact subgroup of the complex Lie group $G(\mathbb{C})$ and write $\mathcal{K}^\natural$ for the set of conjugacy classes in $\mathcal{K}$.

Assume that $\rho\big(\pi_1^{\mathrm{arith}}\big) \subset G(\overline{\mathbb{Q}_\ell})$ inside $\mathrm{GL}_n(\overline{\mathbb{Q}_\ell})$. Since $\mathcal{F}$ is pure of weight 0, for every closed point $u \in \mathcal{U}$ the eigenvalues of $\rho(\mathrm{Frob}_u)$ have absolute value 1. Therefore the semisimple part (in the sense of the Jordan decomposition) of $\rho(\mathrm{Frob}_u)$ defines an element of $\mathcal{K}^\natural$; we denote this element by $\theta(u)$.

Viewing $\mathcal{K}^\natural$ as a quotient space of $\mathcal{K}$, it acquires a quotient topology for which it is compact, and for which the continuous functions on $\mathcal{K}^\natural$ are precisely the continuous central functions on $\mathcal{K}$. We denote by $\mu^\natural$ the direct image on $\mathcal{K}^\natural$ of the normalized Haar measure on $\mathcal{K}$.

We define three sequences of positive measures of mass 1 on $\mathcal{K}^\natural$. The indices n are supposed to be large enough that $\mathcal{U}$ has a closed point of degree n. We set

$$X_n = \left(\frac{1}{\#\mathcal{U}(\mathbb{F}_{q^n})}\right) \sum_{\deg(u)|n} \deg(u)\delta\big(\theta(u)^{n/\deg(u)}\big),$$

$$Y_n = \left(\frac{1}{\#\{u \text{ of } \deg = n\}}\right) \sum_{\deg(u)=n} \delta\big(\theta(u)\big),$$

$$Z_n = \left(\frac{1}{\#\{u \text{ of } \deg \leq n\}}\right) \sum_{\deg(u)\leq n} \delta\big(\theta(u)\big).$$

where $\delta(x)$ denotes the Dirac delta measure supported at x.

Theorem 1.1 (Deligne). *The sequences of measures $\{X_n\}$, $\{Y_n\}$ and $\{Z_n\}$ on $\mathcal{K}^\natural$ all tend weak-$*$ to $\mu^\natural$; for any continuous $\mathbb{C}$-valued function f on $\mathcal{K}^\natural$, we have*

$$\int_{\mathcal{K}^\natural} f\,d\mu^\natural = \lim_{n\to\infty} \int_{\mathcal{K}^\natural} f\,dX_n = \lim_{n\to\infty} \int_{\mathcal{K}^\natural} f\,dY_n = \lim_{n\to\infty} \int_{\mathcal{K}^\natural} f\,dZ_n.$$

Proof. Katz [**17**] Theorem 3.6. □

2. The Jordan-Zassenhaus Theorem

This second part of the appendix recalls a theorem which is completely independent of arithmetic questions and methods. However, it contributes decisively to our work. It is a finiteness result from the theory of semisimple algebras, known as the *Jordan-Zassenhaus theorem*. First we state the version of the Jordan-Zassenhaus theorem for global fields in which it usually appears in the literature.

Theorem 2.1 (Jordan-Zassenhaus). *Let R be any Dedekind domain whose quotient field L is a global field. Then for each R-order Λ in a semisimple L-algebra B, and for each positive integer t, there are only finitely many isomorphism classes of left Λ-lattices of R-rank at most t.*

Proof. Zassenhaus [**50**] Satz 5 for algebraic number fields, Reiner [**29**] Theorem 26.4 for the general case. □

Additionally, we need a "local" version of the Jordan-Zassenhaus theorem. It arises as a direct consequence of the theorem for global fields.

Corollary 2.2. *We keep the assumptions of Theorem 2.1. Let $\mathfrak{p}$ be a prime ideal in R. Then for each $R_\mathfrak{p}$-order $\Lambda_\mathfrak{p}$ in a semisimple $L_\mathfrak{p}$-algebra $B_\mathfrak{p}$, and for each positive integer t, there are only finitely many isomorphism classes of left $\Lambda_\mathfrak{p}$-lattices of $R_\mathfrak{p}$-rank at most t.*

Bibliography

[1] G. W. Anderson, t-Motives, *Duke Math. J.* **53** (1986), 457–502.

[2] H. Behr, Endliche Erzeugbarkeit arithmetischer Gruppen über Funktionenkörpern, *Invent. Math.* **7** (1969), 1–32.

[3] A. Borel, *Linear algebraic groups*, 2nd enlarged edition, Graduate Texts in Math. **126**, Springer-Verlag, 1991.

[4] N. Bourbaki, Algèbre, Chapitre 8: Modules et anneaux semi-simples, *Éléments de mathématique XXIII*, Hermann, 1958.

[5] G. Cornell and J. H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, 1986.

[6] P. Deligne, La conjecture de Weil II, *Publ. Math. IHES* **52** (1980), 138–252.

[7] P. Deligne, Preuve des conjectures de Tate et de Shafarevitch [d'après G. Faltings], Séminaire Bourbaki, 36e année, 1983/84, no. 616, *Astérisque* **121–122** (1985), 25–41.

[8] P. Deligne and D. Husemöller, Survey of Drinfeld modules, *Contemp. Math.* **67** (1987), 25–91.

[9] V. G. Drinfeld, Elliptic modules (Russian), *Mat. Sbornik* **94** (1974), 594–627, transl. *Math. USSR Sbornik* **23** (1974), 561–592.

[10] V. G. Drinfeld, Elliptic modules II (Russian), *Mat. Sbornik* **102** (1977), 182–194, transl. *Math. USSR Sbornik* **31** (1977), 159–170.

[11] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. math.* **73** (1983), 349–366.

[12] G. Faltings, G. Wüstholz et. al., *Rational points*, 3rd enlarged ed., Vieweg, 1992.

[13] D. Goss, *Basic structures of function field arithmetic*, Springer-Verlag, 1996.

[14] A. Grothendieck, *Revêtements étales et groupe fondamental* (SGA 1), Lecture Notes in Math. **224**, Springer-Verlag, 1971.

[15] G. Harder, Minkowskische Reduktionstheorie über Funktionenkörpern, *Invent. Math.* **7** (1969), 33–54.

[16] D. R. Hayes, Explicit class field theory in global function fields, in: *Studies in Algebra and Number Theory*, Adv. Math. Suppl. Stud. **6** (1979), 173–217.

[17] N. M. Katz, *Gauss sums, Kloosterman sums and monodromy groups*, Princeton University Press, 1988.

[18] M. A. Knus and M. Ojanguren, *Théorie de la descente et algèbres d'Azumaya*, Lecture Notes in Math. **389**, Springer-Verlag, 1974.

[19] S. Lang, Algebraic groups over finite fields, *Amer. J. Math* **78** (1956), 555–563.

[20] S. Lang, *Algebra*, 3rd edition, Addison-Wesley, 1993.

[21] S. Mori, On Tate conjecture concerning endomorphisms of abelian varieties, *Intl. Symp. on Algebraic Geometry Kyoto 1977*, Kinokuniya Book Store, 1978, 219–230.

[22] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, 1992.

[23] A. N. Paršin, Algebraic curves over function fields I (Russian), *Izv. Akad. Nauk. SSSR Ser. Mat.* **32** (1968), 1191–1219, transl. *Math. USSR Izvestija* **2** (1968), 1145–1170.

[24] A. N. Paršin, Quelques conjectures de finitude en géométrie diophantienne, *Actes Congrès intern. math.*, 1970, Tome I, 167–471.

[25] R. Pink, The Mumford-Tate conjecture for Drinfeld modules, *Publ. RIMS Kyoto University* **33** No. 3 (1997), 393–425.

[26] R. Pink, *Private communication*, July 2001.

[27] R. Pink, *Letter to the author*, February 17, 2003.

[28] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Academic Press, 1994.

[29] I. Reiner, *Maximal orders*, Academic Press, 1975.

[30] I. R. Šafarevič, Algebraic number fields (Russian), *Proc. Internat. Congr. Math. (Stockholm 1962)*, Inst. Mittag-Leffler, 1963, 163–176, transl. *Amer. Math. Soc. Transl.* (2) **31** (1963), 25–39.

[31] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Benjamin, 1968.

[32] J.-P. Serre, *Galois cohomology*, Springer-Verlag, 1997.

[33] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer-Verlag, 1986.

[34] T. A. Springer, *Linear algebraic groups*, 2nd edition, Birkhäuser, 1998.

[35] Y. Taguchi, Semisimplicity of the Galois representations attached to Drinfeld modules over fields of "finite characteristics", *Duke Math. J.* **62** (1991), 593–599.

[36] Y. Taguchi, Semisimplicity of the Galois representations attached to Drinfeld modules over fields of "infinite characteristics", *J. Number Theory* **44** (1993), 292–314.

[37] Y. Taguchi, The Tate conjecture for t-motives, *Proc. Amer. Math. Soc.* **123** No. 11 (1995), 3285–3287.

[38] Y. Taguchi, On φ-modules, *J. Number Theory* **60** (1996), 124–141.

[39] Y. Taguchi, Finiteness of an isogeny class of Drinfeld modules, *J. Number Theory* **74** (1999), 337–348.

[40] T. Takahashi, Good reduction of elliptic modules, *J. Math. Soc. Japan* **34** (1982), 475–487.

[41] A. Tamagawa, The Tate conjecture for A-premotives, *Preprint*, 1994.

[42] A. Tamagawa, Generalization of Anderson's t-motives and Tate conjecture, *RIMS Kōkyūroku* **884** (1994), 154–159.

[43] A. Tamagawa, The Tate conjecture and the semisimplicity conjecture for t-modules, *RIMS Kōkyūroku* **925** (1995), 89–94.

[44] J. T. Tate, Algebraic cycles and poles of zeta functions, in: *Arithmetical algebraic geometry* (Proc. Conf. Purdue Univ. 1963), Harper & Row, 1965, 93–110.

[45] J. T. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.

[46] Y. G. Zarhin, A finiteness theorem for isogenies of abelian varieties over function fields of finite characteristic (Russian), *Funkcional. Anal. i Priložen* **8** (1974), 31–34, transl. *Functional Anal. Appl.* **8** (1974), 301–303.

[47] Y. G. Zarhin, A remark on endomorphisms of abelian varieties over function fields of finite characteristic (Russian), *Izv. Akad. Nauk. SSSR Ser. Mat.* **38** (1974), 471–474, transl. *Math. USSR Izvestija* **8** (1974), 477–480.

[48] Y. G. Zarhin, Isogenies of abelian varieties over fields of finite characteristic (Russian), *Mat. Sbornik* **95** (1974), 461–470, 472, transl. *Math. USSR Sbornik* **24** (1974), 451–461.

[49] Y. G. Zarhin, Abelian varieties in characteristic p (Russian), *Mat. Zametki* **19** (1976), 393–400, transl. *Math. Notes* **19** (1976), 240–244.

[50] H. Zassenhaus, Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen, *Abh. Math. Semin. Hansische Univ.* **12** (1938), 276–288.

Curriculum Vitae

On February 3rd, 1971, I was born in Stuttgart (Germany). There I attended primary and secondary school (*Gymnasium*) and passed the school leaving examination attaining the *allgemeine Hochschulreife* in May 1990. The following twelve months I served in the German army.

In fall 1991, I took up my studies in mathematics and computer science at the Eberhard-Karls-Universität Tübingen (Germany). In September 1993, I passed the intermediate examinations (*Diplom-Vorprüfung*) in mathematics as major and computer science as minor subject.

I spent the academic year 1994/95 at the Université de Franche-Comté in Besançon (France) and attained the *Diplôme de Maîtrise de Mathématiques (Mention Mathématiques Pures)* in July 1995.

Thereafter I continued my studies at the Universität Gesamthochschule Essen (Germany). In July 1997, after the final examinations in mathematics as major and computer science as minor subject, I was awarded the title of *Diplom-Mathematiker*.

From July 1997 to September 1999 I held a grant in the graduate school *Theoretische und experimentelle Methoden der reinen Mathematik* (Theoretical and experimental methods of pure mathematics) at the Universität Gesamthochschule Essen. From March to July 1999 I stayed at the Université de Franche-Comté in Besançon. Since October 1999 I have been assistant in the Department of Mathematics of the Swiss Federal Institute of Technology Zürich.