A UNIFIED DEFINITION OF ELLIPTIC CURVES AND DRINFELD MODULES*

by

Quentin Gazda & Damien Junger

Contents

1. Introduction

1.1. Motivations. — It is often stated that the Carlitz module is to the ring of univariate polynomials over a finite field what the multiplicative group is to the ring of integers. This analogy extends to the case of “rank 2", where Drinfeld modules play a role similar to that of elliptic curves. This work was born with the aim of finding a common definition for these objects, dependent only on the coefficient ring, and thus, elevating this analogy to a common theory.

Let A be a Dedekind ring [1] finitely generated over $\mathbb{Z}$. Let $\mathbf{G}$ be a scheme of A-modules over a field L; by a *scheme of A-modules*, we mean a functor

$$\mathbf{G} : \mathbf{Alg}_L \longrightarrow \mathbf{Mod}_A$$

from the category of L-algebras to the category of A-modules represented by the points of an L-scheme. We will impose $\mathbf{G}$ to be *algebraic* [2], *connected*, and *smooth*, which means imposing the eponymous conditions on the underlying scheme. We can consider the ℓ-adic Tate modules of $\mathbf{G}$ defined as follows: for ℓ a maximal ideal of A, $\mathrm{T}_\ell\,\mathbf{G}$ is the inverse limit of the ℓ^n-torsion points of $\mathbf{G}$ over a separable closure L^s of L:

$$\mathrm{T}_\ell\,\mathbf{G} := \varprojlim \mathbf{G}[\ell^n](L^s) = \varprojlim \left(\mathbf{G}[\ell](L^s) \longleftarrow \mathbf{G}[\ell^2](L^s) \longleftarrow \cdots\right).$$

It is naturally a module over the ring A_ℓ, obtained by completing A along ℓ. The ℓ-adic Tate module does not depend on the choice of L^s, up to isomorphisms of A_ℓ-modules.

*English translation of the article Pour une définition commune des courbes elliptiques et modules de Drinfeld. For personal use only. For comments on the translation, please e-mail sjoerd.devries@math.su.se.

[1] ↑ By convention, a *Dedekind ring* is a ring of Krull dimension 1 (i.e., we exclude the case of fields).

[2] ↑ This means that the associated scheme morphism $X \to \operatorname{Spec} L$ is of finite type.

Let r be a positive non-zero integer. We will say that $\mathbf{G}$ is *of rank* r if, for every maximal ideal $\ell \subset A$, the module $\mathrm{T}_\ell\,\mathbf{G}$ is free of rank r over A_ℓ (cf. definition 2.2).

By means of introduction, and for stating the results, we assign a name to such objects:

Definition 1.1. — A connected, smooth algebraic scheme of A-modules over L of dimension 1 and rank r is called an *elementary pre-A-module over L*. We will refer to A as the *(ring of) coefficients.*

Example 1.2. — Here, we provide some examples of elementary pre-modules that motivate our definition. We refer to Section 2 for further details.

- The multiplicative group $\mathbb{G}_m$ over $\mathbb{Q}$ is the simplest example with $A = \mathbb{Z}$ and rank 1. We will show that, in fact, the forms of $\mathbb{G}_m$ are the only elementary pre-modules for these parameters (see Theorem 1.7 below).
- Elliptic curves are also examples of elementary pre-modules with coefficients $\mathbb{Z}$, this time with rank 2. Elliptic curves with complex multiplication by $\mathcal{O}_K$, where K is an imaginary quadratic field, viewed as elementary pre-modules with coefficients $\mathcal{O}_K$, have rank 1.
- Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements. The *Drinfeld modules of rank* r are also examples of elementary pre-modules of rank r, with coefficients in A, the ring of regular functions on a smooth projective $\mathbb{F}$-curve with one closed point removed. Recall that for L a finite extension of $\mathbb{F}(C)$, a *Drinfeld module of rank* r *over* L is a functor

  $$E : \mathbf{Alg}_L \longrightarrow \mathbf{Mod}_A$$

  which associates to an L-algebra R the A-module $E(R)$ constructed as follows: as a vector space over $\mathbb{F}$, $E(R)$ is simply R itself, and the action of $a \in A$ is determined by the existence of coefficients $(a)_i \in L$ such that:

  $$\text{For all } x \in R: \quad a \cdot x := (a)_0 x + (a)_1 x^q + (a)_2 x^{q^2} + \cdots + (a)_{rd} x^{q^{rd}}$$

  where $d = \deg(a)$ and $(a)_{rd} \neq 0$. The map $a \mapsto (a)_0$ defines a ring homomorphism $\delta_E : A \to L$ called the *characteristic morphism of* E. We say that E is *generic* if δ_E coincides with the inclusion $A \subset L$ (see subsection 2.4).
- The *Carlitz module* $\mathbf{C}$ is the simplest example of a generic Drinfeld module for $A = \mathbb{F}[t]$, where t acts by $t \cdot x := tx + x^q$.

Although they may appear distinct, the two functors $\mathbf{G}_m$ and $\mathbf{C}$ play analogous roles in arithmetic when following the analogy $(\mathbb{Z}, \mathbb{Q}) \sim (\mathbb{F}[t], \mathbb{F}(t))$. For example, finite abelian extensions of $\mathbb{Q}$ are obtained by adjoining the torsion elements of $\mathbf{G}_m(\bar{\mathbb{Q}})$ (Kronecker-Weber theorem); the same holds for finite abelian extensions of $\mathbb{F}(t)$ by adjoining the torsion of the Carlitz module[(3)] (see [**Ca35, Ca38**]). In rank 2, it is also customary to compare elliptic curves and Drinfeld modules of rank 2.

We are thus seeking a common definition for $\mathbf{G}_m$ and $\mathbf{C}$, and more generally for elliptic curves and Drinfeld modules, that depends only on the global field. Unlike the case of the coefficient ring $\mathbb{Z}$, there exists a plethora of elementary pre-modules of rank 1 with coefficient ring $\mathbb{F}[t]$ that are not forms of $\mathbf{C}$. The notion of elementary pre-modules is therefore insufficient to achieve the desired classification in characteristic $p > 0$, and an additional hypothesis satisfied simultaneously by the listed objects is welcome. In this text, we will study the following two conditions independently.

[3] ↑ By adjoining the torsion of $\mathbf{C}(\mathbb{F}(\theta)^s)$, we would obtain only the maximal abelian extension that is totally ramified at the point ∞ of $\mathbf{P}^1_{\mathbb{F}}$. To obtain the maximal abelian extension, one would also need to add the torsion of the Carlitz module associated with the coefficients $\mathbb{F}[1/t]$, for example.

Elementary module of type (1). — Let K be the field of fractions of A, and let L be a finite extension of K. Let $\mathbf{G}$ be an elementary pre-A-module over L. Its tangent space $\mathrm{Lie}_{\mathbf{G}}(L)$ is an L-vector space of dimension 1 equipped, by functoriality, with the structure of an A-module that commutes with the L-vector space structure. This is called the *tangential action of* A. Since $\mathrm{End}_L(\mathrm{Lie}_{\mathbf{G}}(L))$ canonically identifies with L as a ring, we obtain a ring homomorphism $\delta_{\mathbf{G}} : A \to L$ which is called the *characteristic morphism of* $\boldsymbol{G}$. We propose the following definition:

***Definition 1.3* (cf. definition 2.5).** — We say that $\mathbf{G}$ is an *elementary module of type* (1) if $\delta_{\mathbf{G}}$ coincides with the inclusion $A \subset L$.

Remark 1.4. — It is worth noting that the introduced condition is trivially satisfied when $A = \mathbb{Z}$ because $\mathbb{Z}$ is an initial object. Furthermore, it is satisfied by any generic Drinfeld module, where the tangential action of $a \in A$ is given by

$$\partial(x \mapsto a \cdot x) := \partial_x(ax + (a)_1 x^q + \cdots) = a.$$

Elementary module of type (2). — Let $\mathcal{O}_L$ be the integral closure of A in L. Let $\mathbf{G}$ be an elementary A-module over L. We will say that $\mathbf{G}$ is an elementary module of type (2) if the Galois representation $\mathrm{T}_\ell\,\mathbf{G}$ is *independent of* ℓ in the following sense:

***Definition 1.5* (cf. definition 2.9).** — We will say that $\mathbf{G}$ is an *elementary module of type* (2) if there exists a finite set S of maximal ideals of $\mathcal{O}_L$ such that for every maximal ideal $\mathfrak{P}$ of $\mathcal{O}_L$ outside of S, and for every maximal ideal ℓ of A different from $\mathfrak{p} := \mathfrak{P} \cap A$, the following conditions hold:

(a) The representation $\mathrm{T}_\ell\,\mathbf{G}$ is unramified at $\mathfrak{P}$, i.e., the inertia group $I_{\mathfrak{P}} \subset G_L$ at $\mathfrak{P}$ acts trivially on $\mathrm{T}_\ell\,\mathbf{G}$, and

(b) The determinant $s(\mathfrak{P}) \in A_\ell$ of the action of $\mathrm{Frob}_{\mathfrak{P}} \in G_L/I_{\mathfrak{P}}$ on $\mathrm{T}_\ell\,\mathbf{G}$ belongs to A and is independent of ℓ.

1.2. Presentation of the results.

— The existence of elementary modules is highly restrictive in the ring A. This is what we will show through the following result:

Theorem 1.6. — *Suppose that there exists an elementary module with coefficient ring A. Then,*

(I) *If A has characteristic* 0, *then either $A = \mathbb{Z}$ or $A = \mathcal{O}_K$ where K is an imaginary quadratic field.*

(II) *If A has characteristic $p > 0$, there exists a smooth projective curve $(C, \mathcal{O}_C)$ over $\mathbb{F}_p$ and a closed point ∞ on C such that $A = \mathcal{O}_C(C \setminus \{\infty\})$.*

In particular, the existence of an elementary module forces K to be a global field with at most one infinite place (which is only restrictive for number fields).

We then focus on the classification of elementary modules of type (1) and (2). Our main result states that the mentioned elementary modules are essentially the only ones:

Theorem 1.7. — *Let $\boldsymbol{G}$ be an elementary module of type* (1) *or* (2), *with coefficient ring A and rank r. Then:*

(I) *If the characteristic of A is zero,*
- *If $r = 1$ and $A = \mathbb{Z}$, then $\boldsymbol{G}$ is a form of $\boldsymbol{G}_m$.*
- *If $r = 1$ and $\mathbb{Z} \subsetneq A$, then $A = \mathcal{O}_K$ where K is an imaginary quadratic field, and $\boldsymbol{G}$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$.*
- *If $r = 2$, then $A = \mathbb{Z}$ and $\boldsymbol{G}$ is an elliptic curve.*

(II) *If the characteristic of A is $p > 0$, then A is as in Theorem 1.7(II), and*
- *If $\boldsymbol{G}$ is of type* (1), *then $\boldsymbol{G}$ is a generic Drinfeld module with coefficient ring A and rank r.*

- *If* $\mathbf{G}$ *is of type* (2)*, then* $\mathbf{G}$ *is a Drinfeld module of characteristic* δ*, where* $\delta : A \to L$ *is a raising-to-a-p-th power map.*

Remark 1.8. — The converse of the above theorem is *almost true*, with the exception that an elliptic curve with complex multiplication by $\mathcal{O}_K$ is an elementary module of type (1) only if its only *CM-type* in the sense of Shimura [**Sh98**] (or *characteristic morphism* in our terminology) is the inclusion $\mathcal{O}_K \subset L$ (c.f. proposition 2.8).

Remark 1.9. — If $\mathbf{G}$ is an elementary module over a field L of characteristic $p > 0$, and $\mathrm{Frob}_p : L \to L$ denotes the pth power Frobenius map, then $\mathbf{G}' := \mathrm{Frob}_p^* \mathbf{G}$ is still an elementary module. This is because the Galois group does not see the pth roots, so we have $\mathrm{T}_\ell\, \mathbf{G} \cong \mathrm{T}_\ell\, \mathbf{G}'$ as representations of G_L. This explains why, in (II), we can have non-generic Drinfeld modules (i.e., those whose characteristic morphism differs from the inclusion).

1.2.0.1. *Future work:* — Throughout this text, we have assumed $\mathbf{G}$ to be of dimension 1. It would be highly desirable to remove this assumption and include in this study the case of Anderson modules on one hand and semi-abelian varieties on the other. However, in higher dimensions, one encounters A-module schemes whose Tate modules are trivial (e.g., unipotent groups when $K = \mathbb{Q}$), and the project becomes significantly more complicated.

1.3. Article Outline. — We establish the definitions of elementary modules and present the main examples in Section 2. In Section 3, we recall key results on algebraic groups that are necessary for our study. The proofs of Theorems 1.6 and 1.7 differ significantly depending on the characteristic of A (zero or positive). Therefore, in Section 4, we have decided to treat them in two separate subsections.

1.4. Acknowledgements. — The two authors would like to express their heartfelt gratitude to the Mathematisches Forschungsinstitut Oberwolfach, where the ideas presented in this paper were conceived.

2. Elementary Modules

In this section, we define elementary modules of type (1) and (2) and present the examples of these objects.

2.1. Terminology. — Let A be a Dedekind ring and let L be a field that is an A-algebra. Let L^s be a separable closure of L with absolute Galois group denoted by G_L. Let $\mathbf{G}$ be a scheme of A-modules over L.

Recall that $\mathrm{Lie}_{\mathbf{G}}$ is the functor from the category of L-algebras to the category of A-modules, which assigns to an L-algebra R:

$$\mathrm{Lie}_{\mathbf{G}}(R) := \ker \mathbf{G}\left(R[\varepsilon]/\varepsilon^2 \xrightarrow{\varepsilon \mapsto 0} R\right).$$

The module $\mathrm{Lie}_{\mathbf{G}}(R)$ is also an L-vector space, where scalar multiplication by $l \in L$ is derived from the endomorphism $a + \varepsilon b \mapsto a + \varepsilon l b$ of the ring $R[\varepsilon]/\varepsilon^2$. In particular, $\mathrm{Lie}_{\mathbf{G}}(R)$ is naturally an $A \otimes_{\mathbb{Z}} L$-module. If $\mathbf{G}$ is smooth of dimension d, then $\mathrm{Lie}_{\mathbf{G}}(L)$ is of dimension d over L [**Mi17**, cor. 1.23].

Suppose $\mathbf{G}$ is smooth of dimension $d = 1$.

Definition 2.1. — The unique ring homomorphism $\delta_{\mathbf{G}} : A \to L$ for which the action of $a \in A$ on $\mathrm{Lie}_{\mathbf{G}}(L)$ coincides with scalar multiplication by $\delta_{\mathbf{G}}(a) \in L$, is called the *characteristic morphism of* $\mathbf{G}$. The *characteristic ideal*, denoted by $\mathfrak{c}_{\mathbf{G}}$, is defined as the kernel of $\delta_{\mathbf{G}}$.

For $\ell \subset A$ an ideal, the *Tate module at* ℓ, denoted by $\mathrm{T}_\ell\,\mathbf{G}$, is defined as the inverse limit of the ℓ-torsion elements:

$$\mathrm{T}_\ell\,\mathbf{G} := \varprojlim_n \mathbf{G}[\ell^n](L^s).$$

By denoting A_ℓ as the ℓ-adic completion of A, $\mathrm{T}_\ell\,\mathbf{G}$ is an A_ℓ-module equipped with a compatible action of the group G_L.

Definition 2.2. — For an integer $r \geq 1$, we say that $\mathbf{G}$ *is of rank* r if, for every maximal ideal $\ell \subset A$ distinct from the characteristic ideal $\mathfrak{c}$, the module $\mathrm{T}_\ell\,\mathbf{G}$ is free of rank r over A_ℓ.

Example 2.3. — For $A = \mathbb{Z}$, the multiplicative group $\mathbf{G}_m$ over L has the characteristic morphism given by the map $\mathbb{Z} \to L$. The characteristic ideal of $\mathbf{G}_m$ corresponds to the characteristic of L, which motivates the terminology. For ℓ a prime distinct from the characteristic, the polynomials $X^{\ell^k} - 1$, $k > 0$, are separable, and therefore

$$\mathrm{T}_\ell\,\mathbf{G}_m \cong \varprojlim_{x \mapsto x^\ell} (L^s)^\times$$

is free of rank 1 over $\mathbb{Z}_\ell$. This shows that $\mathbf{G}_m$ is of rank 1. More generally, every elliptic curve over L is of rank 2; we refer the reader to [**Si09**, III.7.1] for this well-known result. From the same reference, we deduce that for $A = \mathcal{O}_K$ where K is an imaginary quadratic extension of $\mathbb{Q}$ and $\mathcal{O}_K$ is its ring of integers, every elliptic curve over L with complex multiplication by A is of rank 1 as a scheme of A-modules over L.

By the A-module structure on $\mathbf{G}$, there is a canonical morphism

$$\varphi : A \longrightarrow \mathrm{End}_{\mathrm{grp}\,/L}(\mathbf{G})$$

from the ring A to the ring of endomorphisms of $\mathbf{G}$ viewed as a group scheme over L. Here is a simple but useful lemma that appears at various places in the classification.

Lemma 2.4. — *Suppose* $\mathbf{G}$ *has rank* $r \geq 1$. *Then the kernel of* φ *is contained in* $\mathfrak{c}$.

Proof. — Let $a \in A \setminus \mathfrak{c}$. Since A is Dedekind, the ideal (a) of A decomposes into a product of prime ideals $\ell_1^{c_1} \cdots \ell_t^{c_t}$, where the ℓ_i are pairwise prime and not contained in $\mathfrak{c}$. We have $\mathbf{G}[a](L^s) \cong \mathbf{G}[\ell_1^{c_1}](L^s) \times \cdots \times \mathbf{G}[\ell_t^{c_t}](L^s)$ by the Chinese Remainder Theorem. By definition, the module $\mathbf{G}[a](L^s)$ is isomorphic to $(A/a)^r$. Thus, since $(a) \neq (a^2)$, the inclusion $\mathbf{G}[a](L^s) \subset \mathbf{G}[a^2](L^s)$ is strict. Therefore, the same holds for the inclusion $\mathbf{G}[a](L^s) \subsetneq \mathbf{G}(L^s)$, and hence $\varphi(a)$ is nonzero. □

2.2. Elementary modules of type (1).

— Suppose now that L is a finite extension of K, the field of fractions of A. Let $\mathbf{G}$ be a smooth connected scheme of A-modules of dimension 1 and rank r over L.

Definition 2.5. — We say that $\mathbf{G}$ is an *elementary* A*-module over* L *of type* (1) if the characteristic morphism of $\mathbf{G}$ coincides with the inclusion $A \subset L$. In particular, the characteristic ideal of $\mathbf{G}$ is zero.

Remark 2.6. — If $A = \mathbb{Z}$, then, since $\mathbb{Z}$ is initial, every A-module scheme over L of rank $r \geq 1$ is an elementary module of type (1).

In view of this remark and the examples 2.3, we obtain:

Proposition 2.7. — *Forms of the multiplicative group and elliptic curves over* L *are elementary* $\mathbb{Z}$*-modules of type* (1).

To an abelian variety A of dimension d defined over a number field k and with complex multiplication by a field K, Shimura associates its *CM-type*, which is a set of d embeddings $K \to k^{\mathrm{alg}}$. If K is an imaginary quadratic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$, and E is an elliptic curve with complex multiplication by K, it follows from the definitions that the type of E is the singleton consisting of the characteristic morphism of E. In particular:

Proposition 2.8. — *The elliptic curve* E *is an elementary* $\mathcal{O}_K$*-module of type* (1) *if its only CM-type according to Shimura coincides with the inclusion* $\mathcal{O}_K \subset L$.

2.3. Elementary modules of type (2). — Let $\mathbf{G}$ be a smooth connected algebraic scheme of A-modules over L of dimension 1 and rank $r \geq 1$. To define elementary modules of type (2), we use the following independence property in ℓ:

Definition 2.9. — We say that $\mathbf{G}$ is an *elementary A-module of type* (2) *over L* if there exists a finite set S of maximal ideals of $\mathcal{O}_L$ such that for every $\mathfrak{P}$ a maximal ideal of $\mathcal{O}_L$ outside S and ℓ a maximal ideal of A different from $\mathfrak{p} := \mathfrak{P} \cap A$,

(*a*) The representation $\mathrm{T}_\ell \mathbf{G}$ is unramified at $\mathfrak{P}$, i.e., the inertia group $I_\mathfrak{P} \subset G_L$ at $\mathfrak{P}$ acts trivially, and

(*b*) The determinant $s(\mathfrak{P}) \in A_\ell$ of the action of $\mathrm{Frob}_\mathfrak{P} \in G_L/I_\mathfrak{P}$ on $\mathrm{T}_\ell \mathbf{G}$ belongs to A and is independent of ℓ.

Example 2.10. — It is well known that, for $A = \mathbb{Z}$, the multiplicative group and elliptic curves satisfy these conditions. When $A = \mathcal{O}_K$ where K is an imaginary quadratic extension of $\mathbb{Q}$, the same is true for elliptic curves with complex multiplication by $\mathcal{O}_K$. We refer the reader to [**Si09**, Prop. V.2.3].

2.4. Drinfeld modules. — Let us conclude this section with a reminder of the theory of Drinfeld modules and show that they are elementary modules of type (1) and (2).

Let p be a prime number, and $\mathbb{F}_p$ the finite field with p elements. Let $(C, \mathcal{O}_C)$ be a smooth projective curve over $\mathbb{F}_p$, and ∞ a closed point of C. Let A be the ring of regular functions on C except at $\{\infty\}$, i.e., $A = \mathcal{O}_C(C \setminus \{\infty\})$. It is a Dedekind ring. For a nonzero element $a \in A$, we denote by $\deg(a)$ the *degree of* a, i.e., the (finite) dimension of $A/(a)$ over $\mathbb{F}_p$.

Let L be a field of characteristic p. We denote by $L\{\tau\}$ the non-commutative ring of finite sums $p(\tau) = \sum_i c_i \tau^i$, $c_i \in L$ for $i \geq 0$, where the multiplication is given by $\tau c = c^q \tau$. We denote by $\deg_\tau p(\tau)$ the integer given by the maximum of $i \geq 0$ such that $c_i \neq 0$. If $\mathbf{G}_a$ denotes the additive group over L, we have a ring morphism $L\{\tau\} \to \mathrm{End}_{\mathrm{grp}/L}(\mathbf{G}_a)$, where $c \in L$ acts by homothety $x \mapsto cx$ on $\mathbf{G}_a$, and τ acts by raising to the p-th power, $x \mapsto x^p$. It can be verified that this is an isomorphism of rings (see, for example, [**DG70**, II.§3, 4.4]).

Given an A-module scheme G over L, the group $M(G) := \mathrm{Hom}_{\mathrm{grp}/L}(G, \mathbf{G}_a)$ is equipped with a left $L\{\tau\}$-module structure by precomposition. $M(G)$ also has an A-module structure, with A acting on G, which commutes with the action of $L\{\tau\}$. These actions coincide over $\mathbb{F}_p$, and thus $M(G)$ is canonically a left $A \otimes_{\mathbb{F}_p} L\{\tau\}$-module. Let us recall the definition of a Drinfeld module :

Definition 2.11 **(Drinfeld A-module).** — An A-module scheme E over L is called a *Drinfeld A-module over L of rank r* if it is isomorphic to $\mathbf{G}_a$ as a group scheme over L, and the $A \otimes_{\mathbb{F}_p} L$-module $M(E)$ is locally free of rank r.

Since every Drinfeld module over L is a 1-dimensional scheme of A-modules, we can associate to it a characteristic morphism δ_E (definition 2.1). One could demonstrate that there is no conflict with our definition of rank (definition 2.2) by using [**Dr74**, prop. 2.2]. However, we will show it using the A-motive associated with a Drinfeld module.

Associated A-motive. — Let σ be the endomorphism of A-algebras that acts as raising to the power p on L. Let $\delta : A \to L$ be a ring homomorphism. The following definition is due to Anderson [**An86**] :

Definition 2.12. — An *(effective, abelian) A-motive of rank r and characteristic δ* is the data of a locally free module M of rank r over $A \otimes_{\mathbb{F}_p} L$ and a σ-linear morphism $\tau_M : M \to M$ whose cokernel is annihilated by a power of the ideal

$$\mathfrak{j}_\delta := \ker(A \otimes_{\mathbb{F}_p} L \to L,\ a \otimes b \mapsto \delta(a)b) \subset A \otimes_{\mathbb{F}_p} L.$$

Given a Drinfeld module E, we obtain an A-motive with the same characteristic morphism and rank. The underlying module is $M(E)$ and the morphism τ_M is obtained by post-composition with $\tau \in \mathrm{End}_{\mathrm{grp}/L}(\mathbf{G}_a)$ on $M(E)$ (we refer to [**Ha19**, Thm. 3.5] for the details of this construction).

Definition 2.13. — The data $\underline{M}(E)$ of $(M(E), \tau_M)$ is called *the associated A-motive of E.*

According to the theorem 3.6 below, the A-motif $\underline{M}(E)$ determines the Drinfeld module E (although not all A-motives are necessarily of the form $\underline{M}(E)$). We recover E using the formula:

$$E : \mathbf{Alg}_L \longrightarrow \mathbf{Mod}_A, \quad R \longmapsto \mathrm{Hom}_{L\{\tau\}}(M(E), R). \tag{1}$$

Let L^s be a separable closure of L with absolute Galois group G_L. Let $\mathrm{T}_\ell\, E$ be the ℓ-adic Tate module of E relative to L^s and the maximal ideal $\ell \subset A$. As a consequence of this description, we have an isomorphism of A_ℓ-linear representations of G_L:

$$\mathrm{T}_\ell\, E \cong \mathrm{Hom}_{L\{\tau\}}\left(M(E)^{\wedge}_{\ell_L}, L^s\right), \tag{2}$$

where $M(E)^{\wedge}_{\ell_L}$ denotes the ℓ_L-adic completion of $M(E)$, and ℓ_L is the ideal $\ell \otimes_{\mathbb{F}_p} L \subset A \otimes_{\mathbb{F}_p} L$. In particular, we deduce from this isomorphism that:

Proposition 2.14. — *If ℓ is different from $\mathfrak{c} = \ker \delta_E$, then $\mathrm{T}_\ell\, E$ is a free A_ℓ-module of rank r.*

Proof. — This is a well-known result for which we provide a sketch of the proof. Let $n \geq 1$. If $\ell \neq \mathfrak{c}$, then the p-linear map on finite-dimensional L-vector spaces $M(E)/\ell_L^n \to M(E)/\ell_L^n$ induced by τ is semisimple (cf. [**Kat73**]). In particular, by the Lang Isogeny Theorem (cf. prop. 1.1 in *loc. cit.*), we deduce that the multiplication map

$$(M(E)/\ell_L^n \otimes_L L^s)^\tau \otimes_{\mathbb{F}_p} L^s \longrightarrow M(E)/\ell_L^n \otimes_L L^s$$

is an isomorphism. Consequently, $(M(E)/\ell_L^n \otimes_L L^s)^\tau$ is a free A/ℓ^n-module of rank r. Moreover, using (1), we obtain isomorphisms of A/ℓ^n-modules:

$$\begin{aligned} E[\ell^n](L^s) &\cong \mathrm{Hom}_{L\{\tau\}}(M(E)/\ell_L^n, L^s) \cong \mathrm{Hom}_{L^s\{\tau\}}(M(E)/\ell_L^n \otimes_L L^s, L^s) \\ &\cong \mathrm{Hom}_{\mathbb{F}_p}((M(E)/\ell_L^n \otimes_L L^s)^\tau, \mathbb{F}_p). \end{aligned}$$

Thus, $E[\ell^n](L^s)$ is a free A/ℓ^n-module of rank r. Since we can choose compatible bases at each step, we conclude that $\mathrm{T}_\ell\, E$ is a free A_ℓ-module of rank r by passing to the limit. □

Drinfeld modules and elementary modules. — Assume that L is a finite extension of K, the fraction field of A. Let E be an A-module of Drinfeld over L of rank r, and let $\delta = \delta_E : A \to L$ be its characteristic morphism.

Definition 2.15. — A Drinfeld A-module E over L is called *generic* (or *of generic characteristic*) if δ_E coincides with the inclusion $A \subset L$.

Then we have:

Proposition 2.16. — *Let E be a generic Drinfeld A-module over L. As an A-module scheme, E is an elementary module of rank r of type* (1) *and* (2).

Proof. — The fact that E is connected and smooth follows from its isomorphism with $\mathbf{G}_a$, and the fact that it has rank r according to Definition 2.2 follows from Proposition 2.14. Since it is generic, it is elementary of type (1). That it is of type (2) follows from [**Go91**, cor. 3.2.4]. □

Let G be an A-module scheme over L. Let $\mathrm{Frob}_p : L \to L$, $x \mapsto x^p$ be the p-Frobenius and let $\mathrm{Frob}_p^* G$ be the A-module scheme over L given by $R \mapsto G(R^{(1)})$, where $R^{(1)}$ is the L-algebra equal to R as rings and where the multiplication by L is through Frob_p. If G is algebraic (resp. connected or smooth), then so is $\mathrm{Frob}_p^* G$. We deduce:

Corollary 2.17. — *Let E be a Drinfeld A-module over L whose characteristic morphism coincides with a raising-to-a-p-th power map. Then E is an elementary module of type* (2).

Proof. — Let $k \geq 0$ such that $\delta = \mathrm{Frob}_p^k$. We have $E \times_L L^{1/p^k} \cong (\mathrm{Frob}_p^k)^* E_0$, where L^{1/p^k} is the field obtained by adjoining the p^k-th roots of elements of L and where E_0 is a Drinfeld module over L^{1/p^k} with characteristic morphism given by the inclusion $A \to L^{1/p^k}$. As an A-module scheme, E_0 is an elementary module of type (2) according to Proposition 2.16, and therefore $E \times_L L^{1/p^k}$ is also elementary of type (2). Since Frob_p commutes with the Galois action, it follows that E is elementary of type (2). □

We conclude this section with further generalities on the determinant of a Drinfeld module, which will be useful in Section 4 for reduction to the case of rank 1.

Determinant of a Drinfeld module. — Let E be a Drinfeld module of rank r with characteristic δ_E. Let $\underline{M}(E) = (M(E), \tau_M)$ be its A-motive. Denote by D the maximal exterior power $\bigwedge^{\max} M(E) = \bigwedge^r M(E)$ taken as an $A \otimes_{\mathbb{F}_p} L$-module. Then D is locally free of rank 1. The action of τ_M, acting diagonally on D, induces a σ-linear map

$$\tau_D : D \longrightarrow D, \quad m_1 \wedge \cdots \wedge m_r \mapsto \tau(m_1) \wedge \cdots \wedge \tau(m_r).$$

It is easy to verify that the data $\underline{D} = (D, \tau_D)$ is also an A-motive with characteristic δ_E, this time of rank 1. The following result is due to Drinfeld (see [**An86**, §0]):

Theorem 2.18. — *The A-motive $\underline{D}$ arises from a Drinfeld module of rank 1 with characteristic δ_E. This Drinfeld module is unique up to isomorphism, and we denote it by* $\det E$.

According to (2), we have an isomorphism of A_ℓ-linear representations of G_L:

$$\mathrm{T}_\ell(\det E) \cong \bigwedge_{A_\ell}^{r} \mathrm{T}_\ell\, E. \tag{3}$$

The above identity will allow us to restrict our proof to the case of rank 1.

3. Generalities on algebraic groups and schemes of modules

In this section, we recall some classical results from the theory of algebraic groups that will be used in our study. We will make use of two powerful theorems: the Barsotti-Chevalley theorem (Theorem 3.1) and the classification of algebraic groups annihilated by Verschiebung in nonzero characteristic (Theorem 3.6).

3.1. Barsotti-Chevalley theorem and a consequence.

— The following theorem plays a major role in our classification (see [**Mi17**, thm. 10.5] for a proof):

Theorem 3.1 **(Barsotti-Chevalley).** — *Every connected algebraic group G over a perfect field fits into an exact sequence of algebraic groups:*

$$1 \longrightarrow H \longrightarrow G \longrightarrow E \longrightarrow 1, \tag{4}$$

where E is an abelian variety and $H \subset G$ is a connected affine normal subgroup.

Let A be a commutative ring with unity. When G is equipped with an A-module scheme structure, one can say more:

Proposition 3.2. — *Let G be a connected scheme of A-modules over a perfect field. Then each term (H or E) of the sequence (4) can be canonically equipped with the structure of scheme of A-modules.*

Proof. — Given $a \in A$, the structure of G as a scheme of A-modules yields an endomorphism $\varphi(a)$ of the algebraic group G. The composition

$$H \longrightarrow G \xrightarrow{\varphi(a)} G \longrightarrow E$$

is a morphism of algebraic groups between a linear group and an abelian variety, and is therefore zero according to [**Co04**, lem. 2.3]. The exactness of (4) means that $\varphi(a)$ factors through $H \to G$ as a unique morphism $\varphi_H(a) : H \to H$. Since the category of commutative algebraic groups is abelian, there exists a unique morphism $\varphi_E(a) : E \to E$ such that (4) completes into a commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r] \arrow[d, "\varphi_H(a)"] & G \arrow[r] \arrow[d, "\varphi(a)"] & E \arrow[r] \arrow[d, "\varphi_E(a)"] & 1 \\
1 \arrow[r] & H \arrow[r] & G \arrow[r] & E \arrow[r] & 1.
\end{tikzcd}$$

By uniqueness, it is easy to see that the assignment of $(\varphi_H(a))_{a\in A}$ and $(\varphi_E(a))_{a\in A}$ endows H and E respectively with structures of schemes of A-modules. □

3.2. Unipotent groups in nonzero characteristic. — Recall that an algebraic group is called *unipotent* if and only if it admits a normal central series whose successive quotients are closed subgroups of $\mathbf{G}_a$.

Remark 3.3. — This definition is equivalent to the existence of invariant vectors in faithful representations, as usually given in the literature (cf. [**Mi17**, prop. 15.23]).

Let k be a field of characteristic $p > 0$ and let k^{perf} be its perfection. Let G be an affine commutative algebraic group over k with Verschiebung V_G.

In the class of unipotent algebraic groups, we distinguish the closed subgroups of $\mathbf{G}_a^d$, which are classified by the following result (cf. [**DG70**, Thm. 6.6]).

Theorem 3.4. — *G is isomorphic to a closed subgroup of $\mathbf{G}_a^d$ for some integer $d > 0$ if and only if its Verschiebung V_G is zero.*

Definition 3.5. — Let G be an algebraic group over k. We denote by

$$M(G) := \mathrm{Hom}_{\mathrm{grp}/k}(G, \mathbf{G}_a)$$

the left $k\{\tau\}$-module obtained by pre-composing with elements of $\mathrm{End}_{\mathrm{grp}/k}(\mathbf{G}_a)$.

Recall that $\mathrm{End}_{\mathrm{grp}/k}(\mathbf{G}_a)$ is isomorphic to the non-commutative ring $k\{\tau\}$, giving $M(G)$ a structure of a left $k\{\tau\}$-module. The construction $G \mapsto M(G)$ is promoted to an equivalence of categories (e.g. cor. 6.7 *loc. cit.*):

Theorem 3.6. — *The assignment $G \mapsto M(G)$ defines an equivalence between the category of commutative affine algebraic groups over k annihilated by Verschiebung and the category of finite-type left $k\{\tau\}$-modules. A pseudo-inverse is given by*

$$M \mapsto U(M) : \big(R \mapsto \mathrm{Hom}_{k\{\tau\}}(M, R)\big)$$

where the homomorphisms are taken in the category of left $k\{\tau\}$-modules, and the k-algebra R is viewed as a left $k\{\tau\}$-module via $\tau \cdot r = r^p$.

Remark 3.7. — Note that under this equivalence, the free left modules over $k\{\tau\}$ correspond to the powers of $\mathbf{G}_a$. For simplicity, we will refer to these groups as *free unipotents.*

A first consequence of this classification is the following result:

Corollary 3.8. — *If G is a smooth connected algebraic group of exponent p, then it is isomorphic to a form of $\mathbf{G}_a^d$ for some $d > 0$, which splits over k^{perf}.*

Proof. — By the Barsotti-Chevalley theorem, we know that $G_{k^{\mathrm{perf}}}$ is a commutative affine algebraic group: indeed, in the exact sequence (4) associated with $G_{k^{\mathrm{perf}}}$, the abelian variety E has exponent p and is therefore trivial. Thus, $G_{k^{\mathrm{perf}}} = H$ is commutative affine.

Since G has exponent p, the same is true for H, and we have the equality $F_H V_H = p = 0$. Since H is smooth, F_H is bijective, which implies $V_H = 0$. Therefore, H is annihilated by Verschiebung, and by Theorem 3.4, we conclude that H is a closed subgroup of $\mathbf{G}_{a,k^{\mathrm{perf}}}^d$. Hence, G is unipotent [**Mi17**, Cor. 15.9].

The left $k^{\mathrm{perf}}\{\tau\}$-module $\mathrm{Hom}_{\mathrm{grp}/k^{\mathrm{perf}}}(G_{k^{\mathrm{perf}}}, \mathbf{G}_{a,k^{\mathrm{perf}}})$ is of finite type and can be decomposed into the direct sum of a free module and a torsion module (by the structure theorem for $k^{\mathrm{perf}}\{\tau\}$-modules, e.g., [**An86**, Prop. 1.4.4]). Since G is connected, the same is true for $G_{k^{\mathrm{perf}}}$, which implies the vanishing of the torsion part. By Theorem 3.6, we conclude that $G_{k^{\mathrm{perf}}}$ is a free unipotent group. □

A second consequence is the following result initially proved by Russell (we refer to [**Ru70**, thm. 2.1 & 3.1] for the proof of the proposition below, which is a consequence of Theorem 3.6).

Proposition 3.9. — *If G is a form of $\boldsymbol{G}_a$, then there exist two integers n and m and elements a_0, ..., a_m in k, with $a_m \neq 0$, such that G is isomorphic to the subgroup of $\boldsymbol{G}_a^2 = \operatorname{Spec} k[x,y]$ given by the equation $y^{p^n} = a_0x + a_1x^p + ... + a_m x^{p^m}$. If $G \ncong \boldsymbol{G}_a$, then $\operatorname{End}_{grp/k}(G)$ is a finite field.*

3.3. Affine algebraic groups.

— We consider two classes of affine algebraic groups: those of *multiplicative type* and those that are *unipotent*. On a perfect field, these two classes are sufficient to describe all affine algebraic groups (see Theorem 3.12).

Recall that an algebraic group M over L is of *multiplicative type* if and only if, for a separable closure L^s of L, there exists a finite abelian group Γ such that M_{L^s} represents the functor $R \mapsto \operatorname{Hom}_{\mathbb{Z}}(\Gamma, R^\times)$. Algebraic groups of multiplicative type over L are uniquely determined by their character group (e.g., [**Mi17**, §14.f]):

Theorem 3.10. — *The functor*

$$M \mapsto \Gamma := \operatorname{Hom}_{\mathrm{grp}\,/L^s}(M_{L^s}, \boldsymbol{G}_{m,L^s})$$

defines an equivalence of categories between the category of algebraic groups of multiplicative type over L and the $\mathbb{Z}$-modules of finite type equipped with a continuous action of the profinite group $G_L = \operatorname{Gal}(L^s|L)$. A pseudo-inverse is given by

$$\Gamma \mapsto M(\Gamma) := \operatorname{Spec}(L^s[\Gamma]^{G_L})$$

where G_L acts diagonally on the group algebra $L^s[\Gamma]$.

We draw inspiration from this equivalence to describe the Tate module of a group M of multiplicative type:

Proposition 3.11. — *Let p be a prime number, M an algebraic group over L of multiplicative type, and Γ its character group. As representations of G_L,*

$$\mathrm{T}_p\, M \cong \operatorname{Hom}_{\mathbb{Z}}\left(\varinjlim \Gamma/p^n\Gamma, (L^s)^\times\right)$$

where $\sigma \in G_L$ acts on the right as $f \mapsto \sigma \circ f \circ \sigma^{-1}$. In particular,

(a) If Γ has p-torsion, then so does $\mathrm{T}_p\, M$.

(b) The rank of $\mathrm{T}_p\, M$ over $\mathbb{Z}_p$ is the same as the rank of Γ over $\mathbb{Z}$.

Proof. — According to Theorem 3.10, we have an isomorphism of groups

$$\theta : \operatorname{Hom}_L(L^s[\Gamma]^{G_L}, L^s) = M(L^s) \cong M_{L^s}(L^s) \cong \operatorname{Hom}_{\mathbb{Z}}(\Gamma, (L^s)^\times) \tag{5}$$

given by $\varphi \mapsto (\varphi \otimes \mathrm{id}_{L^s[\Gamma]})|_\Gamma$, where Γ is seen as a subgroup of $(L^s[\Gamma], \times)$. Denoting by $M[p^n](L^s)$ the p^n-torsion of $M(L^s)$ for a positive integer n, we have

$$\begin{aligned} M[p^n](L^s) &\cong \{f \in \operatorname{Hom}_{\mathbb{Z}}(\Gamma, (L^s)^\times) \mid \forall \gamma \in \Gamma : f(\gamma)^{p^n} = 0\} \\ &\cong \operatorname{Hom}_{\mathbb{Z}}(\Gamma/p^n\Gamma, (L^s)^\times) \end{aligned}$$

and the expression for $\mathrm{T}_p\, M$ follows by taking the limit as n tends to infinity.
It remains to determine the action of G_L on $\mathrm{T}_p\, M$. We seek the unique action of G_L on $\operatorname{Hom}_{\mathbb{Z}}(\Gamma, (L^s)^\times)$ that makes θ equivariant for the action of G_L (the action on $M[p^n](L^s)$ and $\mathrm{T}_p\, M$ will be obtained by restriction and passing to the limit). By definition, an automorphism $\sigma \in G_L$ acts on $(\varphi : L^s[\Gamma]^{G_L} \to L^s) \in M(L^s)$ as $\sigma \circ \varphi$. On the other hand, the map

$$\sigma \circ (\varphi \otimes \mathrm{id}_{L^s[\Gamma]}) \circ \sigma^{-1},$$

where G_L acts diagonally on $L^s[\Gamma]$, is an L^s-linear function that coincides with $\sigma \circ \varphi$ on $(L^s[\Gamma])^{G_L}$. Such a function is unique, so we have

$$(\sigma \circ \varphi) \otimes \mathrm{id}_{L^s[\Gamma]} = \sigma \circ (\varphi \otimes \mathrm{id}_{L^s[\Gamma]}) \circ \sigma^{-1},$$

and then

$$\theta(\sigma \circ \varphi) = \sigma \circ \theta(\varphi) \circ \sigma^{-1}$$

by restriction to Γ. □

Using [**Mi17**, Thm. 17.17 + Cor. 15.17-18], we obtain the announced theorem:

Theorem 3.12. — *Every affine algebraic group H over a perfect field decomposes as $H \cong U \times M$, where U is unipotent and M is of multiplicative type. If H is moreover a scheme over A-modules, then the same holds canonically for U and M.*

4. Proofs

In this section, we prove the theorems stated in the introduction. The proofs are highly sensitive to the characteristic of A, so we will begin with the case of characteristic zero in subsection 4.1, followed by the more sophisticated case of nonzero characteristic in subsection 4.2.

4.1. The case of characteristic zero. — Let A be a finitely generated Dedekind ring of characteristic zero. Let K be its field of fractions, which is a number field with ring of integers A. Let L be a perfect field. Here, we prove Theorems 1.6.(I) and 1.7.(I). Specifically:

Theorem 4.1. — *Let $\mathbf{G}$ be a scheme of A-modules over L that is smooth, connected, of dimension 1, and of rank $r \geq 1$. Then,*

1. *either $A = \mathbb{Z}$, in which case either $r = 1$ and $\mathbf{G}$ is a form of $\mathbf{G}_m$, or $r = 2$ and $\mathbf{G}$ is an elliptic curve;*
2. *or $A = \mathcal{O}_K$, where K is an imaginary quadratic extension of $\mathbb{Q}$, in which case $r = 1$ and $\mathbf{G}$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$.*

Proof. — By applying Proposition 3.2, we obtain an exact sequence of schemes of A-modules over L:

$$1 \longrightarrow H \longrightarrow \mathbf{G} \xrightarrow{f} E \longrightarrow 1.$$

The fibers of f are the classes of H in $\mathbf{G}$, which all have the same dimension. Therefore,

$$\dim H = \dim f^{-1}(\{1_E\}) = \dim \mathbf{G} - \dim E \tag{6}$$

(see, for example, [**GW10**, cor. 14.119]). Since $\dim \mathbf{G} = 1$, we have $\dim H \leq 1$. To determine H, we start by noticing that:

Proposition 4.2. — *H is either trivial or a form of $\mathbf{G}_m$.*

The above proposition follows from the following lemma:

Lemma 4.3. — *Let p be a prime number. Then $\mathrm{T}_p\, \mathbf{G}$ is torsion-free.*

Proof. — If $\mathrm{T}_p\, \mathbf{G}$ has torsion, then $\mathbf{G}(L^s)$ has p-torsion. Therefore, there exists an ideal ℓ of A lying above pA such that $\mathbf{G}(L^s)$ has ℓ-torsion. However, this is impossible because $\mathrm{T}_\ell\, \mathbf{G}$ is free of rank $r \geq 1$ over A_ℓ. □

Proof of proposition 4.2. — Without loss of generality, we assume that H is nontrivial. Since H is an affine algebraic group over a perfect field, it decomposes as $U \times M$, where U is unipotent and M is of multiplicative type (Theorem 3.12).

We claim that U is trivial. Indeed, if $\dim U = 1$, then $\dim H = 1$, and hence $\dim M = \dim E = 0$ (by (6)), which implies that $\mathbf{G} = H$. For a prime number p, we have $\mathrm{T}_p\, \mathbf{G} = \mathrm{T}_p\, U \oplus \mathrm{T}_p\, M = \mathrm{T}_p\, M$. However, since $\dim M = 0$, $\mathrm{T}_p\, \mathbf{G}$ would be a torsion $\mathbb{Z}_p$-module, which is absurd by Lemma 4.3. Thus, $\dim U = 0$, and being unipotent over a field of characteristic 0, U is trivial.

Therefore, we know that H is of multiplicative type, and we denote Γ_H as its character group. Moreover, we have an inclusion $\mathrm{T}_p H \hookrightarrow \mathrm{T}_p \mathbf{G}$, and since $\mathrm{T}_p \mathbf{G}$ is torsion-free, so is $\mathrm{T}_p H$. Since $\operatorname{rank}_{\mathbb{Z}} \Gamma_H = \dim H = 1$, Proposition 3.11 implies that $\Gamma_H \cong \mathbb{Z}$. Thus, H is a form of $\mathbf{G}_m$. □

There are two remaining cases to consider: since $\dim \mathbf{G} = 1$, we have $\dim E \leq 1$. Thus, either E is trivial or E is an elliptic curve.

If E is trivial: then $\mathbf{G} = H$. By Proposition 4.2, $\mathbf{G}$ is a form of $\mathbf{G}_m$. In particular, $\operatorname{End}_L(\mathbf{G}) \cong \mathbb{Z}$, and since $A \hookrightarrow \operatorname{End}_L(\mathbf{G})$ by Lemma 2.4, this implies $A = \mathbb{Z}$.

If E is an elliptic curve: then $\dim H = 0$, and thus H is trivial by Proposition 4.2. Hence, $\mathbf{G}$ is an elliptic curve. Since L has characteristic zero, $\operatorname{End}_L(E)$ is isomorphic either to $\mathbb{Z}$ or to an order in an imaginary quadratic field F. By Lemma 2.4, we have $A \hookrightarrow \operatorname{End}_L(E)$, and since A is Dedekind, this implies $A = \mathbb{Z}$ or $A = \operatorname{End}_L(E) \cong \mathcal{O}_F$, in which case $K \cong F$.

□

Remark 4.4. — As mentioned in Remark 1.8, the converse of Theorem 4.1 is *almost true*, except that an elliptic curve with complex multiplication is an elementary module of type (1) if and only if its characteristic morphism coincides with the inclusion. This *almost converse* follows from Propositions 2.7 and 2.8.

4.2. The case of nonzero characteristic.

— Now, and until the end of this article, we assume that A is a finitely generated Dedekind ring of characteristic $p > 0$. Let K denote its field of fractions. Let L be a field that is also an A-algebra via a morphism $\delta : A \to L$. Let $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ in A. By assumption, $\mathbb{F}_q$ is a finite extension of $\mathbb{F}_p$, and we denote by q its number of elements.

Completion of the proof of Theorem 1.6. — We now complete the proof of Theorem 1.6, which states:

Theorem 4.5. — *Let $\mathbf{G}$ be a smooth connected scheme of A-modules over L of rank $r \geq 1$ and dimension 1. Then there exists a smooth projective curve $(C, \mathcal{O}_C)$ over $\mathbb{F}_p$ and a closed point ∞ of C such that A is isomorphic to $\mathcal{O}_C(C \setminus \{\infty\})$.*

First, we state an equivalent characterization of being the ring of regular functions on a smooth projective curve minus a point. We say that an element $a \in A$ is *constant* if it is algebraic over $\mathbb{F}_p$. We consider the following property:

(P_A) *For every non-constant $a \in A$, A is a finitely generated $\mathbb{F}_p[a]$-module.*

Then we have:

Lemma 4.6. — *The ring A satisfies (P_A) if and only if there exists a smooth projective curve $(C, \mathcal{O}_C)$ over $\mathbb{F}_p$ and a closed point ∞ of C such that*

$$A = \mathrm{H}^0(C \setminus \{\infty\}, \mathcal{O}_C).$$

Proof. — One direction is well-known: Let $(C, \mathcal{O}_C)$ be a smooth projective curve over $\mathbb{F}_p$ and ∞ be a closed point of C. Let $B = \mathrm{H}^0(C \setminus \{\infty\}, \mathcal{O}_C)$. Then property ($P_B$) is satisfied. Indeed, let $b \in B$ be a non-constant element, i.e., the map $\mathbb{F}_p[t] \to B$ sending $t \mapsto b$ is injective. We have an inclusion of fields $\mathbb{F}_p(t) \subset K = \operatorname{Frac}(B)$ which, by the equivalence of categories between function fields over $\mathbb{F}_p$ and smooth projective curves over $\mathbb{F}_p$ [0BY1], gives rise to a morphism $C \to \mathbf{P}^1$ of schemes over $\mathbb{F}_p$. Since $\mathbf{P}^1$ is separated, this morphism is automatically proper [01W6], and note that the unique point of C that is not mapped to $\operatorname{Spec} \mathbb{F}_p[t]$ is the point ∞. Since the property of being *proper* is stable under base change [01W4], the morphism

$$\operatorname{Spec} B = C \times_{\mathbf{P}^1} \operatorname{Spec} \mathbb{F}_p[t] \longrightarrow \mathbf{P}^1 \times_{\mathbf{P}^1} \operatorname{Spec} \mathbb{F}_p[t] = \operatorname{Spec} \mathbb{F}_p[t]$$

is itself proper. Being affine as well [01SH], it is finite [01WN].

Now let's prove the converse. Since A is not a field, there exists a non-constant element $a \in A$. The ring $A \otimes_{\mathbb{F}_p[a]} \mathbb{F}_p(a)$ is a domain (by flatness) and, by (P_A), finite over the field $\mathbb{F}_p(a)$. Hence, $A \otimes_{\mathbb{F}_p[a]} \mathbb{F}_p(a) = K$, where K is the field of fractions of A. Thus, K is a finite extension of $\mathbb{F}_p(a) = \mathbb{F}_p(\mathbf{P}^1)$, which implies the existence of a smooth projective curve $(C, \mathcal{O}_C)$ over $\mathbb{F}_p$ such that $\mathrm{Frac}(A) = \mathbb{F}_p(C)$. Let s be a closed point of C in the complement of $S = \mathrm{Spec}(A)$ (the complement is non-empty since otherwise A would be the field of constants). The ring $B = \mathrm{H}^0(C \setminus \{s\}, \mathcal{O}_C)$ is a subring of A that is Dedekind, and for $b \in B$ non-constant, the inclusion $\mathbb{F}_p[b] \subset A$ is finite by (P_A). Thus, $B \subset A$ is finite, and since B is integrally closed in K, we have $A = B$. □

To prove Theorem 4.5, it suffices to establish property (P_A). Let $\mathbf{G}$ be as in Theorem 4.5.

Proposition 4.7. — *As algebraic groups over L, $\mathbf{G}$ is isomorphic to $\mathbf{G}_a$.*

Proof. — By Corollary 3.8, $\mathbf{G}$ is a form of $\mathbf{G}_a$. By Lemma 2.4, we have that $\mathrm{End}_L(\mathbf{G})$ is infinite. In particular, $\mathbf{G} \cong \mathbf{G}_a$ by Proposition 3.9. □

Let $\square : \mathbf{G} \xrightarrow{\sim} \mathbf{G}_a$ be an isomorphism of algebraic groups over L. The composition

$$\mathrm{End}_{\mathrm{grp}/L}(\mathbf{G}) \xrightarrow{f \mapsto \square f \square^{-1}} \mathrm{End}_{\mathrm{grp}/L}(\mathbf{G}_a) \xrightarrow{\sim} L\{\tau\}$$

induces a (non-canonical) morphism $A \to L\{\tau\}$. We denote

$$\Phi_a(\tau) = \Phi_a^{\square}(\tau) \in L\{\tau\} \tag{7}$$

the polynomial in τ associated to $a \in A$ in this way.

Lemma 4.8. — *The invertible elements of A are the non-zero constant elements.*

Proof. — Since A is an integral domain, every non-zero constant element is invertible. Suppose there exists an invertible element $a \in A$ that is not constant. We claim that there exists a non-constant polynomial $P(x) \in \mathbb{F}_p[x]$ such that $P(a) \notin A^\times$. Indeed, if this were not the case, then $\mathbb{F}_p(a)$ would be a subfield of A. However, since A is of finite type over $\mathbb{F}_p$, we would have $\mathbb{F}_p \subset \mathbb{F}_p(a) \subset A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset A$, where $A/\mathfrak{m}$ is a finite extension of $\mathbb{F}_p$. This is a contradiction, since $\mathbb{F}_p(a)$ is not finite over $\mathbb{F}_p$.

For such a polynomial $P(x)$, the group

$$\mathbf{G}[P(a)](L^s) \cong \left\{ x \in L^s \mid \Phi_{P(a)}(\tau)(x) = 0 \right\} \tag{8}$$

is finite and non-trivial (we used the isomorphism in Proposition 4.7). However, since $\Phi_a \in (L\{\tau\})^\times = L^\times$, we have $\Phi_{P(a)} = P(\Phi_a) \in L^\times$, which contradicts the finiteness (or non-triviality) of the group (8). □

Proof of theorem 4.5. — Let $a \in A$ be a non-constant element. We want to show that $\mathbb{F}_p[a] \to A$ is finite. By Lemma 4.8, a is not invertible, and therefore $\mathbf{G}[a](L^s)$ is finite and non-trivial. Thus, $\deg_\tau \Phi_a > 0$.

We equip $L\{\tau\}$ with a structure of $L \otimes_{\mathbb{F}_p} A$-module, where L acts on the left and $b \in A$ acts on the right by multiplication with $\Phi_b(\tau)$. For a certain $\rho \in \mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)$, this module structure factors through the $L \otimes_{\rho, \mathbb{F}_q} A$-module structure. Since $\deg_\tau \Phi_a > 0$, we can perform left Euclidean division in $L\{\tau\}$ and conclude that it is a finitely generated $L[a] = L \otimes_{\rho,\mathbb{F}_q} \mathbb{F}_q[a]$-module. In particular, we have L-algebra morphisms:

$$L[a] \longrightarrow L \otimes_{\rho, \mathbb{F}_q} A \xrightarrow{h} L\{\tau\}$$

where the composition is of finite type. To show that the first morphism is of finite type, it suffices, by noetherianness, to show that the second one is injective. This is clear because if $\ker h \neq (0)$, then $L \otimes_{\rho, \mathbb{F}_q} A/(\ker h)$ would be of finite dimension over L, which contradicts the fact that the image of h has infinite dimension over L (since it contains $\Phi_a(\tau)$ and its powers).

We have shown that $L[a] \to L \otimes_{\rho, \mathbb{F}_q} A$, and hence $L[a] \to L \otimes_{\mathbb{F}_p} A$, are finite morphisms. The finiteness of A over $\mathbb{F}_p[a]$ follows from faithful flatness. □

Proof of theorem 1.7 for elementary modules of type (1). — We now conclude the proof of Theorem 1.7.(II). Let $\mathbf{G}$ be as in Theorem 4.5. We fix a smooth projective curve $(C, \mathcal{O}_C)$ over $\mathbb{F}_p$ and a closed point ∞ of C such that

$$A = \mathcal{O}_C(C \setminus \{\infty\}).$$

Let $\mathbb{F}_q \subset A$ be the field of constant elements, and let q be its number of elements. Let $e = \log_p q$.

In the proposition below, we list some properties of the polynomials $\Phi_a(\tau) := \Phi_a^{\square}(\tau)$ defined in (7). Let $\delta_{\mathbf{G}}$ be the characteristic morphism of $\mathbf{G}$ (Definition 2.1).

Proposition 4.9. — *(i) For any $a \in A$, $\Phi_a(\tau) \in L\{\tau^e\}$.*

(ii) The constant term of $\Phi_a(\tau)$ is $\delta_{\mathbf{G}}(a)$.

(iii) There exists $t \in \{0, ..., e-1\}$ such that for any $c \in \mathbb{F}_q$, $\Phi_c(\tau) = c^{p^t}$.

(iv) For any nonzero $a \in A$, $\deg_\tau \Phi_a(\tau) = re\deg(a)$.

Proof. — If we restrict the action of A to $\mathbb{F}_q$, it induces a structure of smooth connected $\mathbb{F}_q$-vector space scheme on $\mathbf{G}$, where the endomorphisms of $\varphi(A)$ are $\mathbb{F}_q$-linear. Assertion *(i)* is then a direct consequence of the relation $\Phi_a(\tau)\Phi_c(\tau) = \Phi_c(\tau)\Phi_a(\tau)$ for all $a \in A$ and $c \in \mathbb{F}_q$.

Point *(ii)* follows from the commutativity of the following diagram of rings:

$$\begin{tikzcd}
\Phi^{\square} : A \arrow[r, hook] \arrow[rd, "\delta_{\mathbf{G}}"'] & \mathrm{End}_{\mathrm{grp}\,/L}(\mathbf{G}) \arrow[r, "\square"] \arrow[d, "\mathrm{Lie}"] & \mathrm{End}_{\mathrm{grp}\,/L}(\mathbf{G}_a) \arrow[r, "\sim"] \arrow[d, "\mathrm{Lie}"] & L\{\tau\} \arrow[d, "\partial"] \\
 & \mathrm{End}_{L\text{-vs}\,/L}(\mathrm{Lie}_{\mathbf{G}}) \arrow[r, "\mathrm{Lie}_{\square}"] & \mathrm{End}_{L\text{-vs}\,/L}(\mathbf{G}_a) \arrow[r, "\sim"] & L
\end{tikzcd} \tag{9}$$

which is obtained by functoriality of $\mathbf{G} \mapsto \mathrm{Lie}_{\mathbf{G}}$, and where the vertical arrow $\partial : L\{\tau\} \to L$ sends a polynomial $P(\tau) = a + b\tau + ...$ to its constant term a.

For *(iii)*, it suffices to note that $\delta_{\mathbf{G}}(\mathbb{F}_q^\times) \subset (L\{\tau\})^\times = L^\times$. Thus, by *(ii)*, $\Phi_a(\tau) = \delta_{\mathbf{G}}(a)$ for all $a \in \mathbb{F}_q$. Moreover, $\delta_{\mathbf{G}}$ induced by restriction a field homomorphism $\mathbb{F}_q \to \mathbb{F}_q \subset L$ and coincides with a power t of the p-Frobenius by the Galois Theory of finite fields.

Let us prove *(iv)*. Let $a \in A$ be a nonzero element of degree $d > 0$. By *(iii)*, we know that for any $c \in \mathbb{F}_q$, we have $\deg_\tau \Phi_a(\tau) = \deg_\tau \Phi_{a+c}(\tau)$ and $\deg(a+c) = \deg(a)$ (since $[K : \mathbb{F}_q(a)] = [K : \mathbb{F}_q(a+c)]$). By replacing a with $a+c$, we can assume that the constant coefficient of $\Phi_a(\tau)$ is nonzero. The solutions in the field L^s of

$$\Phi_a(x) = a_0 x + a_1 x^q + ... + a_s x^{q^s} = 0 \quad (x \in L^s) \tag{10}$$

coincide with the elements of $\mathbf{G}[a](L^s)$. On the one hand, the assumption $a_0 \neq 0$ shows that the equation (10) has q^s solutions. On the other hand, the set $\mathbf{G}[a](L^s)$ has q^{rd} elements, and therefore $s = rd$. Indeed, $\mathbf{G}[a](L^s)$ is isomorphic to $\mathbf{G}[\ell_1^{c_1}](L^s) \times \cdots \times \mathbf{G}[\ell_s^{c_s}](L^s)$, and by the definition of elementary modules, it has $q^{rc_1 \deg \ell_1} \cdots q^{rc_s \deg \ell_s}$ elements. This follows from the additivity of degrees. □

The following proposition corresponds to the statement of Theorem 1.7, part (II) for elementary modules of type (1).

Proposition 4.10. — *$\mathbf{G}$ is a Drinfeld module over L with coefficient ring A, of rank r, and with characteristic $\delta_{\mathbf{G}}$.*

Proof. — Let us show that the module $M(\mathbf{G}) = \mathrm{Hom}_{\mathrm{grp}\,/L}(\mathbf{G}, \mathbf{G}_a)$, equipped with its canonical structure as an $A \otimes_{\mathbb{F}_p} L$-module, is locally free of rank r. After choosing coordinates □, $M(\mathbf{G})$ becomes isomorphic to $L\{\tau\}$ where $l \in L$ acts on $p(\tau) \in L\{\tau\}$ by $l \cdot p(\tau)$ and $a \in A$ acts by $p(\tau) \cdot \Phi_a(\tau)$.

Following the decomposition of $A \otimes_{\mathbb{F}_p} L$ by idempotents,

$$A \otimes_{\mathbb{F}_p} L \cong \bigoplus_{s \in \mathbb{Z}/e\mathbb{Z}} A \otimes_{\mathbb{F}_q, c \mapsto c^{p^s}} L, \tag{11}$$

the module $M(\mathbf{G}) \cong_{\square} L\{\tau\}$ decomposes uniquely as a direct sum of submodules $M(\mathbf{G})_s$, $s \in \mathbb{Z}/e\mathbb{Z}$, where $M(\mathbf{G})_s$ is the submodule of elements $m \in M(\mathbf{G})$ on which $c \in \mathbb{F}_q \subset A$ acts as $c^{p^s} \in \mathbb{F}_q \subset L$. As $c \in \mathbb{F}_q \subset A$ acts by $p(\tau) \mapsto p(\tau)c^{p^t}$ (Proposition 4.9.*(iii)*), we find

$$\text{For } s \in \{t, ..., t+e-1\}, \quad M(\mathbf{G})_{\bar{s}} \cong_{\square} L\{\tau^e\}\tau^{s-t}.$$

Let $a \in A$ be a non-constant element. By Euclidean division by $\Phi_a(\tau)$ in $L\{\tau^e\}\tau^{s-t}$, we deduce that $M(\mathbf{G})_{\bar{s}}$ is a free $\mathbb{F}_q[a] \otimes_{\mathbb{F}_q, x \mapsto x^{p^s}} L$-module of rank $r \deg(a)$, with basis $(\tau^{s-t}, \tau^{e+s-t}, ..., \tau^{(r\deg(a)-1)e+s-t})$ (proposition 4.9.*(iv)*). Thus, $M(\mathbf{G})_{\bar{s}}$ is a finitely generated torsion-free module over the Dedekind ring $A \otimes_{\mathbb{F}_q, c \mapsto c^{p^s}} L$; in particular, it is locally free of constant rank. Since $A \otimes_{\mathbb{F}_q, c \mapsto c^{p^s}} L$ is a free $\mathbb{F}_q[a] \otimes_{\mathbb{F}_q, c \mapsto c^{p^s}} L$-module of rank $\deg(a)$, we conclude that $M(\mathbf{G})_{\bar{s}}$ has rank r over $A \otimes_{\mathbb{F}_q, c \mapsto c^{p^s}} L$.

Therefore, the module $M(\mathbf{G})$ is locally free of rank r over $A \otimes_{\mathbb{F}_p} L$. Consequently, $\mathbf{G}$ is a Drinfeld module. Its characteristic being $\delta_{\mathbf{G}}$ follows from the definition. □

4.2.1. *Proof of theorem 1.7 for elementary modules of type* (2). — We conclude here the proof of Theorem 1.7 for elementary modules of type (2). We assume that L is a finite extension of K. Let $\mathcal{O}_L$ be the integral closure of A in L. For $\mathfrak{P}$ a maximal ideal of $\mathcal{O}_L$, we denote by $\mathcal{O}_{(\mathfrak{P})} \subset L$ the subring of L consisting of the $\mathfrak{P}$-integral elements:

$$\mathcal{O}_{(\mathfrak{P})} := \{x \in L \mid v_{\mathfrak{P}}(x) \geq 0\},$$

where $v_{\mathfrak{P}}$ denotes a valuation on L associated with $\mathfrak{P}$. The notation $\mathcal{O}_{\mathfrak{P}}$ is reserved for the completion of $\mathcal{O}_L$ (resp. $\mathcal{O}_{(\mathfrak{P})}$) at the ideal $\mathfrak{P}$, with residue field $\mathbb{F}_{\mathfrak{P}}$. We also denote by $L_{\mathfrak{P}}$ the fraction field of $\mathcal{O}_{\mathfrak{P}}$. Finally, let L^s and $L^s_{\mathfrak{P}}$ be separable closures of L and $L_{\mathfrak{P}}$ respectively, and let $\bar{\mathcal{O}}_{\mathfrak{P}}$ be the integral closure of $\mathcal{O}_{\mathfrak{P}}$ in $L^s_{\mathfrak{P}}$.

Now let us assume that $\mathbf{G}$ is an elementary module of type (2) of dimension 1, with coefficient ring A, base field L, and rank r. Recall that this imposes the following properties: there exists a finite set S of maximal ideals of $\mathcal{O}_L$ such that for any maximal ideal $\mathfrak{P}$ of $\mathcal{O}_L$ outside S, and for any maximal ideal ℓ of A different from $\mathfrak{p} := \mathfrak{P} \cap A$,

(a) The representation $\mathrm{T}_\ell\,\mathbf{G}$ is unramified at $\mathfrak{P}$, i.e., the inertia group $I_{\mathfrak{P}} \subset G_L$ at $\mathfrak{P}$ acts trivially, and

(b) The determinant $s(\mathfrak{P}) \in A_\ell$ of the action of $\mathrm{Frob}_{\mathfrak{P}} \in G_L/I_{\mathfrak{P}}$ on $\mathrm{T}_\ell\,\mathbf{G}$ belongs to A and is independent of ℓ.

Let $\delta = \delta_{\mathbf{G}} : A \to L$ be the characteristic morphism of $\mathbf{G}$ (Definition 2.1). To complete the proof of Theorem 1.7, we need to show that δ coincides with a power of the Frobenius map. For the remainder of the proof, we can assume without loss of generality that $r = 1$. Indeed, by Proposition 4.10, we know that $\mathbf{G}$ is a Drinfeld module. If necessary, we can replace $\mathbf{G}$ with its determinant module $\det \mathbf{G}$, which, by Theorem 2.18, is a Drinfeld module of rank 1 with the same characteristic.

4.2.2. *The heart of the argument.* — The proof proceeds in two steps: first, we show (Proposition 4.11) that $\delta : A \to L$ is $\mathfrak{P}$-integral for almost all finite places $\mathfrak{P}$ of L, and then for any $a \in A$ and all such $\mathfrak{P}$, there exists a positive integer $k = k_{a,\mathfrak{P}}$ such that

$$\delta(a) \equiv a^{p^k} \pmod{\mathfrak{P}}.$$

In the second step, we establish a general result which shows that this condition on δ is sufficient to conclude that it is a power of the Frobenius map (Theorem 4.13).

Proposition 4.11. — *For almost all prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ and every element $a \in A$, there exists a positive integer k (depending on $\mathfrak{P}$ and a) such that $\delta(a) \equiv a^{p^k}$ modulo $\mathfrak{P}$.*

The proof of this proposition will rely on the following lemma 4.12.

Let S_T, "T" standing for *total*, be the set of maximal ideals $\mathfrak{P}$ of $\mathcal{O}_L$ for which there exists $a \in A$ such that one of the coefficients of $\Phi_a(\tau)$ is not $\mathfrak{P}$-integral. Since A is finitely generated as a ring, S_T is finite. In particular, for $\mathfrak{P}$ outside of S_T, the image of δ is contained in $\mathcal{O}_{(\mathfrak{P})}$.

For a non-zero element $a \in A$, let $\varepsilon(a) \in L^\times$ denote the leading coefficient of $\Phi_a(\tau)$. We use the convention that $\varepsilon(0) = 0$. The commutation relations of $\Phi_a(\tau)$ and Proposition 4.10 *(iv)* imply that:

$$\forall a, b \in A, \quad \varepsilon(a)\varepsilon(b)^{q^{r \deg a}} = \varepsilon(b)\varepsilon(a)^{q^{r \deg b}}.$$

In particular, the prime support of $\varepsilon(a)$ (i.e., the set of maximal ideals $\mathfrak{P}$ of $\mathcal{O}_L$ such that $v_{\mathfrak{P}}(\varepsilon(a)) \neq 0$) is independent of $a \neq 0$. Let's denote it by S_D, "D" for *dominant*.

Given a maximal ideal $\mathfrak{P}$ of $\mathcal{O}_L$ outside of S_T, and an ideal $\mathfrak{a}$ of A, we introduce the functor:

$$\mathbf{Z}_{\mathfrak{P}}[\mathfrak{a}] : \mathbf{Alg}_{\mathcal{O}_{(\mathfrak{P})}} \longrightarrow \mathbf{Sets}$$

which assigns to a $\mathcal{O}_{(\mathfrak{P})}$-algebra R the finite subset of R:

$$\mathbf{Z}_{\mathfrak{P}}[\mathfrak{a}](R) := \{x \in R \mid \forall a \in \mathfrak{a} : \ \Phi_a(\tau)(x) = \delta(a)x + \ldots + \varepsilon(a)x^{q^{\deg a}} = 0\}.$$

When restricted to the category of L-algebras, $\mathbf{Z}_{\mathfrak{P}}[\mathfrak{a}](R)$ is equivalent to the functor $R \mapsto \mathbf{G}[\mathfrak{a}](R)$.

Lemma 4.12. — *Let $\mathfrak{P}$ be a maximal ideal of $\mathcal{O}_L$ outside the finite set $S \cup S_T \cup S_D$, and let ℓ be a maximal ideal of A such that $\deg \ell > \deg \mathfrak{P}$. Then,*

1. *If $\lambda \in A$ and $n \geq 1$ are such that $\ell^n = (\lambda)$, then $v_{\mathfrak{P}}(\delta(\lambda)) = 0$.*
2. *For infinitely many integers $n \geq 1$, the arrows obtained by naturality:*
$$\mathbf{Z}_{\mathfrak{P}}[\ell^n](L^s) \longrightarrow \mathbf{Z}_{\mathfrak{P}}[\ell^n](L^s_{\mathfrak{P}}) \longleftarrow \mathbf{Z}_{\mathfrak{P}}[\ell^n](\bar{\mathcal{O}}_{\mathfrak{P}}) \longrightarrow \mathbf{Z}_{\mathfrak{P}}[\ell^n](\bar{\mathbb{F}}_{\mathfrak{P}})$$
are bijections.
3. *We have $\deg s(\mathfrak{P}) = \deg \mathfrak{P}$ and $v_{\mathfrak{P}}(\delta(s(\mathfrak{P}))) > 0$.*

Proof. — For point 1, the kernel of the composition $\delta_{\mathfrak{P}} : A \xrightarrow{\delta} \mathcal{O}_{\mathfrak{P}} \to \mathbb{F}_{\mathfrak{P}}$ defines a maximal ideal of A of degree $\leq \deg \mathfrak{P}$. If $v_{\mathfrak{P}}(\delta(\lambda)) > 0$, then $\lambda \in \ker \delta_{\mathfrak{P}}$, which means $(\ker \delta_{\mathfrak{P}}) | \ell^c$ for some $c > 0$, and hence $\ell = \ker \delta_{\mathfrak{P}}$ by primality. This contradicts our assumption on the degree of ℓ.

Let's prove point 2 when n is a multiple of h, the cardinality of $\mathrm{Cl}(A)$. Let $\lambda \in A$ be a generator of the principal ideal ℓ^h. According to point 1, the polynomial $\Phi_\lambda(\tau)$ can be written as

$$\Phi_\lambda(\tau) = \delta(\lambda) + (\lambda)_1\tau^e + \ldots + \varepsilon(\lambda)\tau^{re \deg \lambda} \in \mathcal{O}_{(\mathfrak{P})}\{\tau\},$$

where $\delta(\lambda)$ and $\varepsilon(\lambda)$ are invertible in $\mathcal{O}_{(\mathfrak{P})}$. In particular, the polynomial

$$\Phi_\lambda(\tau)(x) = \delta(\lambda)x + (\lambda)_1 x^q + \ldots + \varepsilon(\lambda)x^{q^{\deg \lambda}}$$

is separable, which implies that $\mathbf{Z}_{\mathfrak{P}}[\ell^n](L^s) = \mathbf{Z}_{\mathfrak{P}}[\ell^n](L^s_{\mathfrak{P}})$, and its roots are $\mathfrak{P}$-integral in any separably closed extension of L. Hence, we deduce that $\mathbf{Z}_{\mathfrak{P}}[\ell^n](L^s_{\mathfrak{P}}) = \mathbf{Z}_{\mathfrak{P}}[\ell^n](\bar{\mathcal{O}}_{\mathfrak{P}})$. For the last equality, it suffices to observe that $\Phi_\lambda(\tau)(x)$ has simple roots both in $\bar{\mathcal{O}}_{\mathfrak{P}}$ and $\bar{\mathbb{F}}_{\mathfrak{P}}$, and the irreducible factors of $\Phi_\lambda(\tau)(x)$ over $\bar{\mathbb{F}}_{\mathfrak{P}}$ come from those over $\bar{\mathcal{O}}_{\mathfrak{P}}$.

Finally, let's prove point 3. Let $\ell \subset A$ be a maximal ideal of degree greater than $\deg \mathfrak{P}$. Since $\mathbf{G}$ is of rank 1 and $\mathfrak{P}$ is outside S, the automorphism $\mathrm{Frob}_{\mathfrak{P}}$ acts on $\mathrm{T}_\ell \, \mathbf{G}$ by multiplication by $s(\mathfrak{P})$. According to point 2, this means that $\Phi_{s(\mathfrak{P})}(\tau)$ acts on $\mathbf{Z}_{\mathfrak{P}}[\ell^n](\bar{\mathbb{F}}_{\mathfrak{P}})$ by $x \mapsto x^{q^{\deg \mathfrak{P}}}$. Consequently, for any $\gamma \in \mathbf{Z}_{\mathfrak{P}}[\ell^n](\bar{\mathbb{F}}_{\mathfrak{P}}) \subset \bar{\mathbb{F}}_{\mathfrak{P}}$, we have the congruence:

$$\Phi_{s(\mathfrak{P})}(\tau)(\gamma) \equiv \gamma^{q^{\deg \mathfrak{P}}}$$

in $\bar{\mathbb{F}}_{\mathfrak{P}}$. By choosing ℓ with sufficiently large degree, we observe that this identity holds for enough $\gamma \in \bar{\mathbb{F}}_{\mathfrak{P}}$ to be lifted to a polynomial identity:

$$\Phi_{s(\mathfrak{P})}(\tau)(X) \equiv X^{q^{\deg \mathfrak{P}}}.$$

Since $\mathfrak{P}$ is chosen outside S_D, $\varepsilon(s(\mathfrak{P}))$ is a unit of $\mathcal{O}_{\mathfrak{P}}$, and we find $\deg(s(\mathfrak{P})) = \deg \mathfrak{P}$. It also follows that $v_{\mathfrak{P}}(\delta(s(\mathfrak{P}))) > 0$. □

Proof of proposition 4.11. — Let $\mathfrak{P}$ be outside $S \cup S_D \cup S_T$ (finite), and let $\mathfrak{p} := \mathfrak{P} \cap A$. We claim that $\delta(\mathfrak{p}) \subset \mathfrak{P}$. First, let's observe that there exists $l > 0$ such that $(s(\mathfrak{P})) = \mathfrak{p}^l$ as ideals of A: by definition, $s(\mathfrak{P})$ is invertible in A_ℓ for every ℓ different from $\mathfrak{p}$. In particular, the ideal $(s(\mathfrak{P}))$ is a power of $\mathfrak{p}$. If this power were zero, then $s(\mathfrak{P})$ would be a unit in A, which is absurd according to point 3. Thus, we have $\delta(s(\mathfrak{P})) = \delta(\mathfrak{p})^l \subset \mathfrak{P}$, and by maximality of $\mathfrak{P}$, we conclude that $\delta(\mathfrak{p}) \subset \mathfrak{P}$.

Let $a \in A$ be fixed, and let $\bar{a}$ be its image in $\mathbb{F}_\mathfrak{p} \subset \mathbb{F}_\mathfrak{P}$. Let $\pi(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of $\bar{a}$ over $\mathbb{F}_q$. Since $\pi(a) \in \mathfrak{p}$, we have $\delta(\pi(a)) = \pi^{p^t}(\delta(a)) \in \mathfrak{P}$ (cf. Proposition 4.9). But since $\bar{a}^{p^t}$ is also a root of π^{p^t} modulo $\mathfrak{P}$, there exists $c = c_{\mathfrak{P},a} \in \{0, ..., \deg \pi\}$ such that

$$\delta(a) \equiv a^{p^t q^c} \pmod{\mathfrak{P}},$$

which concludes the proof. □

We still need to prove that the map δ is a power of Frobenius. For this, let's work in a more general setting and study triplets (B, C, f) that satisfy the following properties (P_i):

(P_1) *$B \subset C$ are two finite-dimensional integral domains over $\mathbb{F}_p$ of dimension 1,*

(P_2) *$f : B \to C$ is a ring homomorphism such that for all but finitely many prime ideals $\mathfrak{p}$ of C and all $b \in B$, there exists $k \in \mathbb{N}$ (which may depend on $\mathfrak{p}$ and b) such that*

$$f(b) \equiv b^{p^k} \pmod{\mathfrak{p}}.$$

According to Proposition 4.11, the triplet $(A, \mathcal{O}_L[S^{-1}], \delta)$ satisfies properties (P_1) and (P_2), so we reduce the proof to:

Theorem 4.13. — *Let (B, C, f) satisfy (P_1) and (P_2). Then f is the k-th power of the Frobenius, where k is an integer that may be negative*[4].

Remark 4.14. — — The finiteness assumption on $\mathbb{F}_p$ for B and C is necessary to ensure that we have enough prime ideals in C. For example, if C is a local ring of dimension 1, condition (P_2) is vacuous, and f can be any morphism.

— In the particular case of interest to us, namely the triplet $(A, \mathcal{O}_L[S^{-1}], \delta)$, if there exists an element in A that does not have p-th roots in L, this forces the integer k in the previous statement to be positive. Since δ coincides with raising to the power p^t over the field $\mathbb{F}_q$, we also have $k \equiv t \pmod{e}$.

The proof, which will unfold in the final pages of this text, essentially amounts to proving the following two intermediate results:

Lemma 4.15. — *Let (B, C, f) satisfy (P_1) and (P_2), where B is a polynomial algebra $\mathbb{F}_p[X]$ and $C = B[f(X)]$. Then $f(X) = X^{p^k}$ for some integer k, which may be negative.*

Lemma 4.16. — *Let $B \subset C$ be two integral domains over $\mathbb{F}_p$, and let $f : B \to C$ be a ring homomorphism such that for every $b \in B$, there exists $k_b \in \mathbb{Z}$ satisfying $f(b) = b^{p^{k_b}}$. Then f is of the form Frob^k for some integer k, which may be negative.*

Remark 4.17. — Note that in the statement of Lemma 4.16, we did not assume that the triplet (B, C, f) satisfies property (P_1): there is no need to assume that B or C is of finite type over $\mathbb{F}_p$ or of dimension 1.

Let us finish the proof of Theorem 4.13 assuming the two lemmas.

Proof of Theorem 4.13. — According to Lemma 4.16, it suffices to show that $f(b)$ is of the form $b^{p^{k_b}}$ for every element $b \in B$, where $k_b \in \mathbb{Z}$. The arrow f preserves constants (i.e., algebraic elements over $\mathbb{F}_p$) and therefore restricts to an endomorphism of $\mathbb{F}_q$, which is a power of the Frobenius by the Galois theory of finite fields. When b is not a constant, it suffices to

[4] ↑ Note that in the case where k is negative, the statement implies the existence, for any $b \in B$, of a p^{-k}-th root in C (necessarily unique since C is an integral domain) which is the image of b under the map f.

show that the triple $(\mathbb{F}_p[b], \mathbb{F}_p[b, f(b)], f|_{\mathbb{F}_p[b]})$ still satisfies properties (P$_1$) and (P$_2$) by virtue of Lemma 4.15.

The algebras $\mathbb{F}_p[b]$ and $\mathbb{F}_p[b, f(b)]$ are of finite type over $\mathbb{F}$ by construction, and are integral subdomains of C. $\mathbb{F}_p[b]$ has dimension 1, and the same is true for $\mathbb{F}_p[b, f(b)]$: indeed, we have the chain of inclusions $\mathbb{F}_p(b) \subset \mathbb{F}_p(b, f(b)) \subset \operatorname{Frac} C$, showing that $\mathbb{F}_p(b, f(b))$ is a finite extension of $\mathbb{F}_p(b)$.

It remains to show that property (P$_2$) is satisfied. According to Lemma 4.19 (stated below), all but finitely many prime ideals $\mathfrak{p}$ of $\mathbb{F}_p[b, f(b)]$ are of the form $\mathfrak{P} \cap \mathbb{F}_p[b, f(b)]$ with a prime ideal $\mathfrak{P}$ of C and satisfy (P$_2$) for (B, C, f). Thus, $f(b) \equiv b^{p^k} \pmod{\mathfrak{P}}$, hence $f(b) - b^{p^k} \in \mathfrak{P} \cap \mathbb{F}_p[b, f(b)] = \mathfrak{p}$. We deduce (P$_2$) for $(\mathbb{F}_p[b], \mathbb{F}_p[b, f(b)], f|_{\mathbb{F}_p[b]})$, which completes the proof. □

It remains to show Lemmas 4.15, 4.16, as well as Lemma 4.19 stated below.

Proof of Lemma 4.15. — Let (B, C, f) be as stated in the lemma. Let $P(X, Y) \in \mathbb{F}_p[X, Y]$ be a two-variable polynomial that annihilates $f(X)$ over $\mathbb{F}_p(X)$ and whose content [5] (regarded as a polynomial in Y) is assumed to be 1. The kernel of the map

$$\mathbb{F}_p[X, Y] \longrightarrow \mathbb{F}_p[X, f(X)], \quad Y \mapsto f(X),$$

is $P(X, Y)\mathbb{F}_p(X) \cap \mathbb{F}_p[X, Y]$, which is equal to $P(X, Y)\mathbb{F}_p[X, Y]$ by the assumption on the content. Thus,

$$C \cong \mathbb{F}_p[X, Y]/(P). \tag{12}$$

The identity (12) and property (P$_2$) imply the following assertion:

(A) For all but finitely many $x \in \bar{\mathbb{F}}_p$, the roots of $P(x, Y) \in \bar{\mathbb{F}}_p[Y]$ are all of the form x^{p^k} for some integer $k \in \mathbb{Z}$.

We now show that (A) implies:

(B) There exists an integer k such that either $P(X, Y) = X^{p^k} - Y$ or $P(X, Y) = Y^{p^k} - X$.

The following result is a crucial step in the proof:

Lemma 4.18. — *Let $R(X) \in \mathbb{F}_p(X)$ be such that, for almost every $x \in \bar{\mathbb{F}}_p$, there exists an integer n_x such that $R(x) = x^{n_x}$. Then there exists $n \in \mathbb{Z}$ such that $R(X) = X^n$.*

Proof. — Let's write $R(X) = R_1(X)/R_2(X)$ for two polynomials $R_1(X)$ and $R_2(X) \neq 0$. Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$ such that $|\mathbb{F}| - 1$ has two distinct prime odd divisors $\ell_1, \ell_2 > 2\max(\deg R_1, \deg R_2)$. For $\ell \in \{\ell_1, \ell_2\}$, let's choose $\zeta_\ell \in \mathbb{F} \setminus (\mathbb{F})^\ell$ such that $\zeta_\ell^{\ell^m} = 1$ for some m. Let x be an ℓ-th root of ζ_ℓ in $\bar{\mathbb{F}}$. By enlarging $\mathbb{F}$ if necessary, we can assume that $R(x) = x^{n_x}$ for some non-negative integer $n_x \geq 0$. Since $X^\ell - 1$ splits into distinct linear factors in $\mathbb{F}$ by assumption, $X^\ell - \zeta_\ell$ is the minimal polynomial of x over $\mathbb{F}$, and the field $\mathbb{F}(x)$ has degree ℓ over $\mathbb{F}$ by Kummer theory. Writing $n_x = s_x + r_x\ell$ with $-\ell/2 < s_x < \ell/2$, we have $R(x) = \zeta_\ell^{r_x} x^{s_x}$. By swapping R_1 and R_2 if necessary, we can assume that $0 \leq s_x < \ell/2$. Now, the representation $\zeta_\ell^r x^s \in \mathbb{F}(x)$ with $0 \leq r < \operatorname{ord} \zeta_\ell$ and $0 \leq s < \ell/2$ is unique for the pair (r, s), hence we obtain the polynomial congruence $R_1(X) \equiv \zeta_\ell^{r_x} X^{s_x} R_2(X) \pmod{X^\ell - \zeta_\ell}$. This implies $R_1(X) = \zeta_\ell^{r_x} X^{s_x} R_2(X)$ and $R(X) = \zeta_\ell^{r_x} X^{s_x}$ by comparing degrees. In particular, we have $s_x = \deg R$ and $\zeta_\ell^{r_x}$ is independent of $\ell \in \{\ell_1, \ell_2\}$. Since $\zeta_\ell^{r_x}$ is both an ℓ_1^m-th and an ℓ_2^m-th root for sufficiently large m, we have $\zeta_\ell^{r_x} = 1$, which concludes the proof. □

Let us write the polynomial P in the form $P(X, Y) = Q(X, Y^{p^N})$ with N maximal for this property. We observe that property (A) for P implies property (A) for Q. We will determine Q in order to recover P afterwards.

By choice of N, we have $\partial_Y Q \neq 0$. Moreover, Q is irreducible in $\mathbb{F}_p(X)[Y]$ because P is, and by Bézout's theorem we can find $S_1(X, Y), S_2(X, Y) \in \mathbb{F}_p(X)[Y]$ such that:

$$S_1(X, Y)Q(X, Y) + S_2(X, Y)(\partial_Y Q)(X, Y) = 1.$$

[5] ↑ Recall that the content (regarded as a polynomial in Y) of $P(X, Y) = \sum_i P_i(X)Y^i$ is the greatest common divisor of the P_i.

We deduce that, for almost every $x \in \bar{\mathbb{F}}_p$ (more precisely, when x is not a pole of any term of $S_1(X,Y), S_2(X,Y)$), $Q(x,Y)$ and $(\partial_Y Q)(x,Y)$ are coprime, and the polynomial $Q(x,Y)$ seen in $\bar{\mathbb{F}}_p[Y]$ has distinct roots. For such x, we have:

$$Q(x,Y) = c(x)\prod_{i=1}^{d}(Y - x^{p^{n_{i,x}}})$$

in $\bar{\mathbb{F}}_p[Y]$, where d is the degree of Q in Y, and $c(X) \in \mathbb{F}_p[X]$ is the leading coefficient of $Q(X,Y)$ (resp. $P(X,Y)$) viewed as a polynomial in Y. The constant term of $(-1)^{\deg_Y Q}Q(x,Y)/c(x)$ is x^n, where $n \in \mathbb{Z}$ is independent of x according to Lemma 4.18.

Let $m > d + |n|$ be an integer. By choosing m sufficiently large, we can assume that the cyclic group $\mathbb{F}_{p^m}^{\times}$ has a generator x for which $Q(x,Y) \in \bar{\mathbb{F}}_p[Y]$ has distinct roots $x^{p^{k_1}}, \dots, x^{p^{k_d}}$ with $0 \leq k_1 < k_2 < \cdots < k_d < m$. We obtain the congruence:

$$n \equiv \sum_{i=1}^{d} p^{k_i} \pmod{p^m - 1}.$$

Furthermore,

$$\left| n - \sum_{i=1}^{d} p^{k_i} \right| \leq |n| + \sum_{i=1}^{d} p^{k_i} < \sum_{k=0}^{m} p^k \leq p^m - 1,$$

because $d + |n| < m$. Therefore, $n = \sum_i p^{k_i}$.

By the uniqueness of the base-p representation, we see that the values of $(k_i)_i$ do not depend on the choice [6] of the element x satisfying the previous constraints. In particular, since the polynomials $Q(X,Y)$ and $c(X)\prod_i (Y - X^{p^{k_i}})$ in X over $\mathbb{F}_p[Y]$ coincide for infinitely many values of X in $\bar{\mathbb{F}}_p$, these polynomials are equal. Due to the irreducibility of Q and the fact that $\partial_Y Q \neq 0$, we obtain $c(X) = 1$ and $d = 1$. Thus, $Q(X,Y) = Y - X^{p^{k_1}}$, and consequently, $P(X,Y) = Y^{p^N} - X^{p^{k_1}}$. Finally, the irreducibility of P implies $N = 1$ or $k_1 = 1$, which is equivalent to

$$P(X,Y) = X^{p^k} - Y \text{ or } P(X,Y) = Y^{p^k} - X.$$

This completes the proof! □

Proof of 4.16. — For $x, y \in B$, we want to show that [7] $k_x = k_y$. We reason on the sub-$\mathbb{F}_p$-algebra $\mathbb{F}_p[x,y]$ of B generated by x and y, where the restriction of f still satisfies the property stated in the theorem. Similarly, it suffices to prove the result when replacing f by $f \circ \mathrm{Frob}^m$ with sufficiently large m. Thus, we can assume that $k_x, k_y \geq 0$, and f becomes an endomorphism of $\mathbb{F}_p[x,y]$. We distinguish the following three cases, which are exhaustive by the integrality of $\mathbb{F}_p[x,y]$:

1. Both x and y are algebraic over $\mathbb{F}_p$. In this case $\mathbb{F}_p[x,y]$ is a finite field, and f is a power of the Frobenius by Galois theory over $\mathbb{F}_p$.
2. If y is transcendental over $\mathbb{F}_p(x)$, we write

   $$x^{p^{k_{xy}}} y^{p^{k_{xy}}} = f(xy) = f(x)f(y) = x^{p^{k_x}} y^{p^{k_y}},$$

   which implies $k_y = k_{xy}$ and $x^{p^{k_x}} = x^{p^{k_{xy}}} = x^{p^{k_y}}$.
3. If x and y are transcendental over $\mathbb{F}_p$, but y is algebraic over $\mathbb{F}_p(x)$.

   For any ideal $\mathfrak{b}$ of B, we have $f(\mathfrak{b}) \subset \mathfrak{b}$ by assumption. Thus, for any maximal ideal $\mathfrak{m} \subset B$ with residue field $\kappa_{\mathfrak{m}}$, f induces an endomorphism $\bar{f}$ of $\kappa_{\mathfrak{m}}$. Let $d_{\mathfrak{m}}$ be the degree of $\mathfrak{m}$, i.e., the dimension of $\kappa_{\mathfrak{m}}$ over $\mathbb{F}_p$, and let $n_{\bar{x}}$ and $n_{\bar{y}}$ be the dimensions over $\mathbb{F}_p$

[6] ↑ Here, we crucially use the fact that the k_i are distinct. For example, the equality $p^2 = p + \cdots + p$ provides a counterexample when some exponents are repeated.

[7] ↑ Here, we made a slight abuse as the integers are not necessarily unique. We rather mean to have the equalities $f(x) = x^{p^{k_x}} = x^{p^{k_y}}$ (the same applies to $f(y)$).

of the subfields of $\kappa_{\mathfrak{m}}$ generated by $\bar{x}$ and $\bar{y}$, respectively. Since $\kappa_{\mathfrak{m}} = \mathbb{F}_p[\bar{x}, \bar{y}]$, we have $d_{\mathfrak{m}} = [n_{\bar{x}}, n_{\bar{y}}]$.

Since $\kappa_{\mathfrak{m}}$ is a finite field and $\bar{f}$ is an endomorphism of $\kappa_{\mathfrak{m}}$, there exists an integer $0 \leq k_{\mathfrak{m}} < d_{\mathfrak{m}}$ such that $\bar{f}(\bar{b}) = \bar{b}^{k_{\mathfrak{m}}}$ for all $b \in B$. In particular, $k_x \equiv k_{\mathfrak{m}} \pmod{n_{\bar{x}}}$ and $k_y \equiv k_{\mathfrak{m}} \pmod{n_{\bar{y}}}$. We obtain $k_x \equiv k_y \pmod{(n_{\bar{x}}, n_{\bar{y}})}$. To conclude, it suffices to show that the gcd $(n_{\bar{x}}, n_{\bar{y}})$ can be arbitrarily large (by varying $\mathfrak{m}$).

Let $P_x(Y) \in \mathbb{F}_p[x][Y]$ be the minimal polynomial of y over $\mathbb{F}_p(x)$ (normalized). Choosing a pair $(\bar{x}, \bar{y}) \in \bar{\mathbb{F}}_p^2$ such that $P_{\bar{x}}(\bar{y}) = 0$ yields a maximal ideal

$$\mathfrak{m}_{(\bar{x},\bar{y})} = \ker(\mathbb{F}_p[x, y] \to \bar{\mathbb{F}}_p : (x, y) \mapsto (\bar{x}, \bar{y})),$$

and all maximal ideals of $\mathbb{F}_p[x, y]$ are of this form.

Let d be the degree of $P_x(Y)$ in Y. Let $\mathfrak{m}$ be a maximal ideal of B arising from a geometric point $(\bar{x}, \bar{y})$. Since $\bar{y}$ is a root of $P_{\bar{x}}(Y)$, we have $d_{\mathfrak{m}} \leq d \cdot n_{\bar{x}}$. Then we have the inequality

$$(n_{\bar{x}}, n_{\bar{y}}) = \frac{n_{\bar{x}} n_{\bar{y}}}{d_{\mathfrak{m}}} \geq \frac{n_{\bar{y}}}{d}.$$

According to Lemma 4.19, the complement of the image of the map $\operatorname{Spm} \mathbb{F}_p[x, y] \to \operatorname{Spm} \mathbb{F}[y]$ is a finite set, and we can choose $(\bar{x}, \bar{y})$ such that $n_{\bar{y}}$ can be arbitrarily large.

This completes the proof. □

The proofs of the theorem and lemma used the following classical statement:

Lemma 4.19. — *Let $B \subset C$ be two finite-type integral domains over a field k of dimension 1. Then all but finitely many prime ideals of B are of the form $\mathfrak{P} \cap B$, where $\mathfrak{P}$ is a prime ideal of C.*

Proof. — Since the closed sets $V(\lambda)$ are the finite sets in $|\operatorname{Spec} B|$ for any non-invertible element λ in B by dimension reasons, it suffices to find an element λ for which the natural map $|\operatorname{Spec} C[1/\lambda]| \to |\operatorname{Spec} B[1/\lambda]|$ is surjective. To find such an element, we observe that C is of finite type over B and choose a finite family $(x_i)_i$ of generators. Since all algebras are of dimension 1, we can find a polynomial that annihilates each generator in B, and we denote by λ_i the leading coefficient of each polynomial. By construction, the inclusion $B[1/\prod_i \lambda_i] \to C[1/\prod_i \lambda_i]$ is finite and induces a surjective map on the level of spectra. Therefore, the element $\lambda = \prod_i \lambda_i$ satisfies the desired property. □

References

[An86] G. W. Anderson, *t-motives*, Duke Math. J. 53, no. 2, 457–502 (1986).

[Ca35] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. 1, 137–168 (1935).

[Ca38] L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc. 43, 167–182 (1938).

[Co04] B. Conrad, *A Modern Proof of Chevalley's Theorem on Algebraic Groups*, pdf, (2004).

[DG70] M. Demazure, P. Gabriel: *Groupes Algébriques, Tome I*, Masson et Cie, (1970).

[Dr74] V. G. Drinfeld, *Elliptic modules*, Mathematics of the USSR-Sbornik, Vol. 23 (4), 561–592, version anglaise (1974).

[GW10] U. Görtz, T. Wedhorn, *Algebraic Geometry Part I: Schemes. With Examples and Exercises*, Advanced Lectures in Mathematics (2010).

[Go91] D. Goss, *L-series of t-motives and Drinfeld Modules*, The Arithmetic of Function Fields: Proceedings of the Workshop at the Ohio State University (1991).

[Ha19] U. Hartl, *Isogenies of abelian Anderson A-modules and A-motives*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) Vol. XIX, 1429–1470 (2019).

[Kat73] N. Katz, *Une formule de congruence pour la fonction ζ*, Éxposé XXII SGA7 t. II, Lecture Notes in Mathematics (340) (1973).

[Mi17] Milne, J. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*, (Cambridge Studies in Advanced Mathematics). Cambridge: Cambridge University Press, (2017).

[Ru70] P. Russell, *Forms of the affine line and its additive group*, Pacific J. Math. 32, 527–539 (1970).

[Sh98] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton: Princeton University Press (1998).

[Si09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106. Springer-Verlag, New York (2009).

June 2023

Translated by *Sjoerd de Vries*

Quentin Gazda, Centre de Mathématiques Laurent Schwartz (CMLS), École Polytechnique, Cour Vaneau F-91120 Palaiseau • *E-mail :* quentin@gazda.fr • *Url :* https://quentin.gazda.fr

Damien Junger, Mathematisches Institut, Universität Münster, Fachbereich Mathematik und Informatik der Universität Münster, Orléans-Ring 10, D-48149 Münster. • *E-mail :* djunger@uni-muenster.de