University of Amsterdam

MSc Mathematics

Master Thesis

Torsors under finite locally free group schemes in characteristic p

Author:
Olivier de Gaay Fortman

Supervisor:
dr. Christopher Lazda

Examination date:
June 24, 2019

Korteweg-de Vries Institute for Mathematics

Abstract

This thesis stems from an attempt of the author to understand group scheme actions by commutative finite locally free group schemes in characteristic p with zero relative Frobenius, and in particular whether it is possible to describe such actions in terms of morphisms of sheaves of restricted Lie algebras. Such a description can be useful for questions of descent, for which one could want to make a scheme into a torsor. An application is given in this respect, for inseparable field extensions, where classical Galois descent fails. We believe that over a field of characteristic p, any finite inseparable field extension of degree p can be made into a torsor under any finite commutative connected group scheme of order p.

Acknowledgements
I would like to express my sincere appreciation to my thesis supervisor Christopher Lazda, for his encouragement, suggestions and critiques. It has been a pleasure to work under his guidance. I would like to thank Nola for all her understanding and support.

Project details
Title: Torsors under finite locally free group schemes in characteristic p
Author: Olivier de Gaay Fortman, olivierfortman@hotmail.com, 10739521
Supervisor: dr. Christopher Lazda
Examiner: dr. Arno Kret
Second reviewer: prof. dr. Lenny Taelman
Examination date: June 24, 2019
Korteweg-de Vries Institute for Mathematics
University of Amsterdam
Science Park 105-107, 1098 XG Amsterdam
`http://kdvi.uva.nl`

Contents

Introduction **4**

Notations and conventions **6**

1 Finite locally free group schemes **7**

1.1 Group schemes and Hopf algebras 7

1.2 Cartier duality 11

1.3 Finite locally free group schemes in characteristic p 12

2 Frobenius modules **13**

2.1 Finite locally free group schemes and Frobenius modules 13

2.2 Left-invariant derivations 17

2.3 Restricted Lie algebras 19

2.4 Classification of finite connected order p group schemes over a field 22

3 Actions by finite locally free group schemes **26**

3.1 Actions by group schemes 26

3.2 Actions by Frobenius modules 28

3.3 Examples 32

4 Inseparable extensions and finite group schemes with zero Frobenius **33**

4.1 Modular field extensions 33

4.2 Torsors under finite connected group schemes of order p 35

4.3 A number theoretical conjecture 37

Popular summary **43**

References **45**

Introduction

Consider a field k. Suppose one wants to carry out a construction X in the category of schemes over k, say prove that a scheme, morphism, or sheaf on a scheme in that category satisfies a certain property P. Sometimes all one can do is base change the problem over some field extension k', and carry out X in the category of schemes over k' instead, or prove that P holds there. Then one is faced with deciding whether X or P is the base extension of its analogue in the category of schemes over k. This problem is a special case of what is known as *descent.*

Weil ([22]) gave conditions which were necessary and sufficient for descending a quasi-projective k'-variety if the extension k'/k is finite Galois. Grothendieck ([9]) observed that these conditions were analogous to the conditions for reconstructing an object by gluing local data, which led him to generalise Weil's idea to *fpqc descent.* This is a generalisation in the sense that $\operatorname{Spec} k' \to \operatorname{Spec} k$ is replaced by an arbitrary fpqc morphism of schemes $S' \to S$. Let us give some examples:

1. If the extension k'/k is finite Galois, $V \mapsto V \otimes k'$ induces an equivalence between the category of k-vector spaces and the category of k'-vector spaces equipped with a $\operatorname{Gal}(k'/k)$-action over k (see [8, 14.83]).

2. Under the assumption of Example 1, let X' be a quasi-projective k'-scheme. For each $\sigma \in \operatorname{Gal}(k'/k)$, denote by $X_\sigma^{'}$ the pullback of X via the morphism of k-schemes $\operatorname{Spec} k' \to \operatorname{Spec} k'$ that σ induces. Suppose that, for each $\sigma \in \operatorname{Gal}(k'/k)$, we are given k'-isomorphisms $f_\sigma : X_\sigma^{'} \to X'$ that satisfy the cocycle condition $f_{\sigma\tau} = f_\sigma \cdot (f_\tau)^\sigma$ for all $\sigma, \tau \in G$. Then $X' = X_{k'}$ for some k-scheme X ([15, 4.4.6]).

3. More generally than Example 1: let $f : S' \to S$ be a morphism of schemes, suppose G is a group scheme over S which is faithfully flat quasi-compact over S, and let $G \times_S S' \to S'$ be a group scheme action of G on S' over S that makes S' into a G-torsor over S (see Definition 3.3 in Section 3). Then $\mathscr{F} \mapsto f^*\mathscr{F}$ induces an equivalence between the category of quasi-coherent $\mathcal{O}_S$-modules, and the category of G-equivariant quasi-coherent $\mathcal{O}_{S'}$-modules (see [8, 14.85]).

4. Under the assumptions of Example 3, the assignment $X \mapsto X \times_S S'$ induces an equivalence between the category of S-schemes X that are affine over S, and the category of G-equivariant S'-schemes X' that are affine over S' (see [8, 14.86]).

Remark that Examples 1 and 2 fail when k'/k is inseparable - say when $k = \mathbb{F}_p(t)$ and $k' = \mathbb{F}_p(t^{1/p})$ for a prime number p - Galois descent is impossible. However, descent along torsors, as in Examples 3 and 4, possibly still works. Descent along torsors thus provides a natural solution to the problem of descent via inseparable field extensions.

So suppose one has been given a finite purely inseparable field extension L/k, where k is a field of characteristic p for a prime number p, and one wants to descend from the category of L-schemes to the category of k-schemes. By the observations above, one option is to start with a k-group scheme G which is quasi-compact (e.g. affine), and acts on $\operatorname{Spec} L$ over k making it into a torsor. But how many such k-group schemes exist, and which of those have desirable properties? Such questions have motivated the writing of this thesis. There is reason to believe the following:

Conjecture 0.1. *Let L/k be an inseparable field extension of degree p. Let G be a commutative k-group scheme. Then $\operatorname{Spec} L$ can be made into a G-torsor over k if and only if G is connected and finite of order p over k.*

To understand such a question, we have tried to apprehend a much more general phenomenon. Namely, the aim of this thesis is to understand actions of commutative finite locally free group schemes over a scheme S of characteristic p, killed by their relative Frobenius, on schemes that are affine over S. To do so, we describe such group schemes in terms of pairs $(\mathscr{M}, \varphi)$, where $\mathscr{M}$ is a finite locally free $\mathcal{O}_S$-module, and φ an $\mathcal{O}_S$-linear map $F_S^*\mathscr{M} \to \mathscr{M}$, with F_S the absolute Frobenius on S. For a finite locally free S-group scheme G, the sheaf of left-invariant derivations is denoted by $\mathscr{L}(G)$.

Theorem 0.2. *The following assignment induces an equivalence of categories:*

$$\big(\text{commutative finite locally free } S\text{-group schemes } G : F_{G/S} = 0\big) \;\to\; \big(\text{pairs } (\mathscr{M}, \varphi) \text{ as above}\big),$$

$$G \qquad \mapsto \qquad (\mathscr{L}(G), F_S^*\mathscr{L}(G) \xrightarrow{D\otimes 1 \mapsto D^p} \mathscr{L}(G)).$$

We then observe that $\mathscr{L}(G)$ is a sheaf of restricted $\mathcal{O}_S$-Lie algebras, and show that its bracket is trivial. This brings us in the position to prove that group scheme actions correspond to morphisms of sheaves of restricted Lie algebras:

Theorem 0.3. *Let G be a commutative finite locally free group scheme over S with $F_{G/S} = 0$. Group scheme actions of G on a scheme X affine over S are in bijection with morphisms of sheaves of restricted $\mathcal{O}_S$-Lie algebras $\mathscr{L}(G) \to \mathscr{D}er_{\mathcal{O}_S}(\mathcal{O}_X, \mathcal{O}_X)$.*

The structure of this thesis is as following. In Section 1, we present some of the basic theory on commutative finite locally free group schemes in characteristic p. In Section 2, we prove Theorem 0.2. A corollary is a classification of commutative finite connected order p group schemes over a field. At the end of Section 2, we show that the restricted enveloping algebra of $\mathscr{L}(G)$ is canonically isomorphic to the dual Hopf algebra $(\mathcal{O}_G)^D$. In Section 3, we prove Theorem 0.3. In Section 4, we consider actions of finite commutative k-group schemes G on finite purely inseparable field extensions L over k. If $[L : k] = p$, there are some obvious conditions to impose on G if $\operatorname{Spec} L$ should be a G-torsor. We apply the results of Sections 1-3 to show how reasonable it is to assume these conditions are sufficient, which is Conjecture 0.1. We end Section 4 by presenting our results in favour of 0.1. In particular, the truth of Conjecture 0.4 would imply the truth of 0.1:

Conjecture 0.4. *For every prime number $p \geqslant 5$, the following is true:*

$$\sum_{\substack{1<n_1<n_2<\ldots<n_r<p-1 \\ n_{m+1}-n_m \geqslant 2}} \frac{1}{n_1 \cdot n_2 \cdots n_r} \equiv 0 \mod p \qquad \text{for } r = 1, \ldots, \frac{p-3}{2}.$$

Notations and conventions

Throughout this thesis, rings are commutative with unit. The prime number p is fixed, as is the field k of characteristic p. We will use the sign $=$ to denote canonical isomorphisms, and $\cong$ if the isomorphism requires a non-canonical choice. R is a ring and S is a scheme. We denote by Sch/S the category of schemes over S, by Set the category of sets, by Grp the category of groups, and by R-Mod the category of R-modules. For any two morphisms in a category $f : A \to B$ and $g : B \to C$ we write $f^*(g) = g_*(f) = g \circ f$. If X and T are schemes over S, we write $X_S(T) = \mathrm{Hom}_{\mathsf{Sch}/S}(T, X)$; if it is clear that we are in the category of schemes over S we shall write $X(T) = X_S(T)$. Note that if $f : X \to Y$ and $g : T' \to T$ are morphisms in Sch/S, one obtains maps $f^* : X(T) \to X(T')$ and $g_* : X(T) \to Y(T)$ in Set. We write $h_X : \mathsf{Sch}/S^{\mathrm{opp}} \to \mathsf{Set}$ for the functor $(h_X(T) = X(T), h_X(f) = f^*)$ and denote by $\mathrm{pr}_1 : X \times_S Y \to X$ and $\mathrm{pr}_2 : X \times_S Y \to Y$ the two projections.

For any morphism $\varphi : X \to Y$ of schemes over S, and any scheme T over S, we write $\varphi_T : X_T \to Y_T$ for the induced morphism of schemes over T. For any sheaf $\mathcal{F}$ on S and any morphism of schemes $f : T \to S$, we will denote by $\mathcal{F}_T$ or $\mathcal{F} \otimes \mathcal{O}_T$ the pullback $f^*\mathcal{F} = f^{-1}\mathcal{F} \otimes_{f^{-1}\mathcal{O}_T} \mathcal{O}_T$ of the sheaf $\mathcal{F}$ to the scheme T, which we will also call the base change of $\mathcal{F}$ by T. For a map $f : Y \to Y$ where Y is any object in a category, we denote by f^n the n-th composite $f \circ ... \circ f$. When $f : X \to S$ is an affine morphism of schemes we will sometimes abuse notation and write $\mathcal{O}_X$ for the sheaf of $\mathcal{O}_S$-algebras $f_* \mathcal{O}_X$. When $\mu : \mathrm{Spec}\,\mathcal{B} \to \mathrm{Spec}\,\mathcal{A}$ is a morphism of schemes that are affine over R (resp. over S) we write $\tilde{\mu} : \mathcal{A} \to \mathcal{B}$ for the corresponding morphism of R-algebras (resp. of sheaves of quasi-coherent $\mathcal{O}_S$-algebras).

1 Finite locally free group schemes

We start by treating the basic theory of finite locally free group schemes in characteristic p. Group schemes occur frequently in algebraic geometry, think of elliptic curves or, more generally, abelian varieties. They are also useful for solving problems of descent - for this we will develop some theory on actions of group schemes on arbitrary schemes - but this will come up in later chapters. Apart from the applications, hopefully in this section it becomes clear that group schemes are interesting enough in their own right.

We will start by giving some basic definitions in Section 1.1, such as those of a group scheme over S and a homomorphism of group schemes over S. In the affine case, the theory of group schemes is the theory of Hopf algebras. When group schemes are finite, flat and locally of finite presentation they have a lot of structure, as we will see in Section 1.2. We are mainly interested in the case where S is a scheme over $\mathbb{F}_p$, a case that we will start to consider in Section 1.3. One of the motivations behind this interest is the following: in characteristic 0 all group schemes are reduced, whereas in characteristic p this is no longer true, and genuinely new phenomena occur. For example, Galois theory fails for inseparable extensions L/k, but this can be fixed to some extent by finding a finite k-group scheme G with zero relative Frobenius that can make L into a G-torsor. But this will come across much later - let us first consider some of the basic theory of finite locally free group schemes in characteristic p.

1.1 Group schemes and Hopf algebras

By the Yoneda Lemma, sending a scheme X over S to the functor h_X defines an embedding of the category of schemes over S into the category of contravariant functors $\mathsf{Sch}/S \to \mathsf{Set}$. A functor $F : \mathsf{Sch}/S^{\mathrm{opp}} \to \mathsf{Set}$ is called *representable* if F is isomorphic to a functor h_X in the image of this embedding. We also say that F is *represented* by the scheme X over S. It follows from Yoneda's lemma that X is unique up to unique isomorphism. We call a functor $F : \mathsf{Sch}/S^{\mathrm{opp}} \to \mathsf{Grp}$ *representable* if its composition with the forgetful functor $\mathsf{Grp} \to \mathsf{Set}$ is representable.

Definitions 1.1. A *group scheme over* S is a pair (G, m) where G is a scheme over S and $m : G \times_S G \to G$ is a morphism of schemes over S such that the composition of $G(T) \times G(T) = (G \times_S G)(T)$ with $m_* : (G \times_S G)(T) \to G(T)$ makes $G(T)$ into a group for every S-scheme T. A group scheme G over S is *commutative* if the group $G(T)$ is commutative for every scheme T over S. If G and H are group schemes over S, a *homomorphism of group schemes over* S is a morphism $\varphi : G \to H$ in the category Sch/S such that, for every S-scheme T, the map $\varphi_* : G(T) \to H(T)$ is a homomorphism of groups. A closed subscheme $H \hookrightarrow G$ of an S-group scheme G is a *subgroup scheme of* G *over* S if $H(T) \subset G(T)$ is a subgroup for each S-scheme T.

Sometimes we will shorten "group scheme over S" to "group scheme", when it is clear what the base scheme is. Likewise we will occasionally use G to denote an S-group scheme (G, m); we then implicitly assume the existence of a fixed group law $m : G \times_S G \to$

G. If we say that G is a group scheme over R we will mean that G is a group scheme over $\operatorname{Spec} R$.

Remark 1.2. Group schemes over S correspond to contravariant functors from Sch/S to Grp which are representable. Indeed, an S-group scheme (G, m) lifts h_G to a group-valued functor, and if on the other hand the composition of a contravariant functor $\mathsf{Sch}/S \to \mathsf{Grp}$ with the forgetful functor $\mathsf{Grp} \to \mathsf{Set}$ is representable by a scheme G over S, then m can be retrieved as the image of the identity $\mathrm{id}_{G\times_S G}$ under the map

$$h_{G\times_S G}(G \times_S G) = h_G(G \times_S G) \times h_G(G \times_S G) \to h_G(G \times_S G).$$

Group schemes have many applications in algebraic geometry, for example, as remarked before, they can be useful in studying questions of descent. Their study is also motivated by the study of abelian varieties, e.g. the kernel of an isogeny of abelian varieties over k is a finite k-group scheme whose Cartier dual is isomorphic to the kernel of the dual isogeny (see Section 1.2 and [17, 2.9.8]). An abelian variety is a group scheme itself, with a lot of additional structure: it is a complete geometrically integral group scheme over a field. We give some more examples.

Examples 1.3.

1. The scheme S is trivially an S-group scheme. In fact, it is the zero object in the category of S-group schemes, where the morphisms are the homomorphisms of S-group schemes.

2. Recall that an elliptic curve over S is a proper smooth morphism of schemes $p : E \to S$ whose fibers are geometrically connected curves of genus 1, together with a section $e : S \to E$. Then an elliptic curve over S is an S-group scheme by [6, II, 2.7] or [14, 2.1.2 (Abel)].

3. For any morphism of schemes $T \to S$, the base change of an S-group scheme G naturally inherits the structure of a T-group scheme: base change the group law m of G to a composition law m_T of G_T and check that this makes G_T into a T-group scheme. In fact, if $\pi : T' \to T$ is a morphism of schemes, this makes the maps

   $$f(T') : G(T') \to G_T(T'), \quad g \mapsto (g, \pi), \quad G_T(T') \to G(T'), \quad \phi \mapsto \mathrm{pr}_1 \circ \phi$$

   homomorphisms of groups, inverse to each other and functorial in T'.

4. One checks that the assignments $\mathcal{O} : T \to \Gamma(T, \mathcal{O}_T)$ and $\mathcal{O}^* : T \to \Gamma(T, \mathcal{O}_T)^*$ define contravariant functors from Sch/S to Grp. Indeed, for any morphism $T' \to T$ of schemes over S the induced map $\Gamma(T, \mathcal{O}_T) \to \Gamma(T', \mathcal{O}'_T)$ preserves addition and multiplication, and clearly $\mathcal{O}$ and $\mathcal{O}^*$ respect composition and identity maps. By 1.2 we obtain group schemes if these functors are representable. But they are:

5. Let x be a variable and let $\mathbb{G}_a = \operatorname{Spec} \mathbb{Z}[x] \times_{\mathbb{Z}} S = \operatorname{Spec} \mathcal{O}_S[x]$. Then $\mathbb{G}_a(T) = \mathcal{O}(T)$, functorially in T. This makes the $\mathbb{G}_a$ into a group scheme over S. Use 1.2 to observe that the group law m is induced by the morphism of $\mathcal{O}_S$-algebras

   $$\mathcal{O}_S[x] \to \mathcal{O}_S[x] \otimes_{\mathcal{O}_S} \mathcal{O}_S[x], \quad x \mapsto x \otimes 1 + 1 \otimes x.$$

6. Similarly, let $\mathbb{G}_m = \operatorname{Spec} \mathcal{O}_S[x, x^{-1}]$. Then $\mathbb{G}_m(T) = \mathcal{O}^*(T)$, functorially in T. Again we use Remark 1.2 to see that the group law m is induced by the morphism of $\mathcal{O}_S$-algebras
$$\mathcal{O}_S[x, x^{-1}] \to \mathcal{O}_S[x, x^{-1}] \otimes_{\mathcal{O}_S} \mathcal{O}_S[x, x^{-1}], \quad x \mapsto x \otimes x.$$

7. Let $\mu_n = \operatorname{Spec} \mathcal{O}_S[x]/(x^n - 1)$ where $n \in \mathbb{Z}_{\geqslant 0}$. Then for any scheme T over S we have $\mu_n(T) = \{\zeta \in \Gamma(T, \mathcal{O}_T)^* : \zeta^n = 1\} \subset \mathbb{G}_m(T)$. The natural map $\mu_n \to \mathbb{G}_m$ is a closed immersion which makes μ_n a subgroup scheme of $\mathbb{G}_m$ over S.

8. If S is a scheme over $\mathbb{F}_p$, the closed subscheme of $\mathbb{G}_a$ defined by $x^p = 0$ is a subgroup scheme of $\mathbb{G}_a$ over S which we denote by α_p.

9. Let Γ be an abstract group. Let $\underline{\Gamma} = \coprod_{g \in \Gamma} S$, the disjoint union of copies of S indexed by the set Γ. Then $\underline{\Gamma}$ is an S-group scheme in the following way: for any S-scheme T the set $\underline{\Gamma}(T)$ is the set of locally constant functions from $|T|$ to Γ, which can be multiplied using the group structure on Γ.

For an S-group scheme G, the inclusion $S(T) \subset G(T)$ and the map $G(T) \to G(T), g \mapsto g^{-1}$ are functorial in T. They induce morphisms e and inv using the Yoneda Lemma, and the latter is a homomorphism of group schemes if and only if G is commutative. The Yoneda Lemma is also the main ingredient in the proof of the following proposition.

Proposition 1.4. *Suppose that G is an S-scheme with structure morphism $\pi : G \to S$, equipped with a morphism of S-schemes $m : G \times_S G \to G$.*

1. *(G, m) is a group scheme over S if and only if there exist maps $e : S \to G$ and $\operatorname{inv} : G \to G$ such each of the following diagrams commutes:*

$$\begin{tikzcd}
G \times G \times G \arrow[r, "\operatorname{id} \times m"'] \arrow[d, "m \times \operatorname{id}"] & G \times G \arrow[d, "m"] \\
G \times_S G \arrow[r, "m"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "="] \arrow[d, "="] \arrow[ddrr, "\operatorname{id}"] & G \times_S S \arrow[r, "\operatorname{id} \times e"'] & G \times_S G \arrow[dd, "m"] \\
S \times_S G \arrow[d, "e \times \operatorname{id}"] & & \\
G \times_S G \arrow[rr, "m"] & & G
\end{tikzcd}$$

$$\begin{tikzcd}
G \times_S G \arrow[r, "\operatorname{inv} \times \operatorname{id}"'] & G \times_S G \arrow[d, "m"] \\
G \arrow[u, "\Delta"] \arrow[r, "e \circ \pi"] & G.
\end{tikzcd}$$

2. *If 1.4.1 holds, then G is a commutative group scheme if and only if the following diagram commutes:*

$$\begin{tikzcd}
G \times_S G \arrow[rr, "(\operatorname{pr}_2, \operatorname{pr}_1)"] \arrow[dr, "m"'] & & G \times_S G \arrow[dl, "m"] . \\
& G &
\end{tikzcd}$$

Proof. See [21, 1.5]. □

Suppose $S = \operatorname{Spec} R$. Let $G = \operatorname{Spec} A$ be an affine R-scheme. By the anti-equivalence of categories of R-algebras and affine R-schemes, to make G into an R-group scheme (respectively, commutative R-group scheme) is to give R-algebra homomorphisms

$$\tilde{m} : A \to A \otimes_R A, \quad \tilde{e} : A \to R, \quad \widetilde{\operatorname{inv}} : A \to A,$$

corresponding to the morphisms m, e and inv discussed in 1.4.1, which make the diagrams commute that are obtained from the diagrams in 1.4.1 (respectively, 1.4.1 and 1.4.2), by reversing the arrows, replacing S by R, G by A, $\times_S$ by $\otimes_R$, and putting $\sim$ on the labels of the arrows. We call $\tilde{m}$ the *comultiplication*, $\tilde{e}$ the *augmentation*, and $\widetilde{\operatorname{inv}}$ the *antipode*. The kernel $I \subset A$ of the augmentation $\tilde{e} : A \to R$ will be called the *augmentation ideal*.

Definition 1.5. A *Hopf algebra over R* is an R-algebra A together with morphisms $\tilde{m}, \tilde{e}$ and $\widetilde{\operatorname{inv}}$ satisfying the above-stated commutative diagrams obtained from the diagrams in Proposition 1.4.1. If $\tilde{m}$ in addition satisfies the commutative diagram obtained from the diagram in Proposition 1.4.2, then $(A, \tilde{m}, \tilde{e}, \widetilde{\operatorname{inv}})$ is called *cocommutative*.

As in the case of group schemes, we will often write A for a Hopf R-algebra $(A, \tilde{m}, \tilde{e}, \widetilde{\operatorname{inv}})$. Sometimes we shorten "Hopf algebra over R" to "Hopf algebra" if there is no risk of confusion. Note that the category of Hopf algebras over R, with the obvious definition of a *morphism of Hopf algebras over R*, is anti-equivalent to the category of affine R-group schemes.

Convention 1.6. In the remaining part of this thesis, each *group scheme over S* will be a commutative group scheme over S, and each *Hopf algebra over R* will be a cocommutative Hopf algebra over R.

Notation 1.7. We let Gr/S be the category of group schemes over S, and R-Hopf the category of Hopf algebras over R.

Because each G in Gr/S is commutative by Convention 1.6, for any $n \in \mathbb{Z}_{\geqslant 0}$ we can functorially define a homomorphism of group schemes $[n] : G \to G$ as multiplication by n. We say G is *killed by n* if $[n] = [0]$ as group scheme endomorphisms on G, which is equivalent to $ng = e_T \in G(T)$ for each $g \in G(T)$ and each S-scheme T, and to the factorisation of $[n]$ through $e : S \to G$. More generally, if $\varphi : G \to H$ is a homorphism of S-group schemes, when we write $\varphi = 0$, or say that G is *killed by* φ, we mean that φ factors through $S \to H$, or equivalently that $\varphi_*(g) = 0$ for each $g \in G(T)$ and each S-scheme T.

Recall that a morphism of schemes $f : X \to S$ is finite locally free if f is affine and $f_* \mathcal{O}_X$ is a finite locally free $\mathcal{O}_S$-module. A morphism of schemes $X \to S$ is then finite locally free if and only if it is finite, flat, and locally of finite presentation; and if S is locally noetherian, $X \to S$ is finite locally free if and only if it is finite and flat (see [19, 28.46.2]). If S is locally noetherian and G a finite flat group scheme over S with structure morphism $\pi : G \to S$, the rank of $\pi_* \mathcal{O}_G$ over $\mathcal{O}_S$ is a locally constant function on S with integer values $\geqslant 0$ which we call the *order of G over S*, denoted by $[G : S]$.

We will often deal with the case $S = \operatorname{Spec} k$, when G being finite locally free over S is equivalent to G being affine and $\Gamma(G, \mathcal{O}_G)$ a finite k-algebra. In this case, the order of G over S is a positive integer.

1.2 Cartier duality

We denote the dual of an R-module M by $M^D = \operatorname{Hom}_{R\text{-}\mathsf{Mod}}(M, R)$.

Remark 1.8. If M and N in R-Mod are locally free of finite rank, the natural homomorphisms $M \mapsto M^{DD}$ and $M^D \otimes_R N^D \to (M \otimes_R N)^D$ are isomorphisms.

For an R-linear map $f : M \to N$, the dual map $f^* : N^D \to M^D$ will be linear over R. Because this makes the assignment $M \mapsto M^{DD}$ natural in M, the assignment $(M \mapsto M^D, f \mapsto f^*)$ defines an anti-equivalence of the category of all such modules with itself.

Now suppose R is noetherian. Let G be a finite flat R-group scheme with structure morphism $\pi : G \to \operatorname{Spec} R$ and diagonal $\Delta : G \to G \times_R G$. From the discussion above we see $G = \operatorname{Spec} A$, for an R-Hopf algebra A which is locally free of finite rank as R-module. By dualising all the maps that define the Hopf algebra structure of A one equips the R-module A^D with maps

$$\tilde{e}^* : R \to A^D, \qquad \tilde{m}^* : A^D \otimes_R A^D \to A^D, \qquad \tilde{\Delta}^* : A^D \to A^D \otimes A^D$$

$$\tilde{\pi}^* : A^D \to R, \qquad \tilde{\operatorname{inv}}^* : A^D \to A^D.$$

These maps satisfy the necessary requirements to make A^D into a Hopf algebra over R with structure map $\tilde{e}^*$, multiplication map $\tilde{m}^*$, comultiplication map $\tilde{\Delta}^*$, augmentation map $\tilde{\pi}^*$ and antipode $\tilde{\operatorname{inv}}^*$. Moreover, the evaluation map $\operatorname{ev} : A \to A^{DD}$ is a homomorphism of Hopf algebras, and an isomorphism by Remark 1.8. Because the assignment $A \mapsto A^D$ is functorial in A, and the isomorphism $A = A^{DD}$ natural in A, it follows that the assignment $G \mapsto G^D = \operatorname{Spec} A^D$ induces an anti-equivalence of the category of finite flat R-group schemes with itself.

This generalises. Let $G \in \operatorname{Ob}(\mathsf{Gr}/S)$ be finite locally free over S with structure morphism $\pi : G \to S$. Write $\mathcal{A} = \pi_* \mathcal{O}_G$ and note that $\mathcal{A}$ is a *sheaf of $\mathcal{O}_S$-Hopf algebras.* Sheafify the above construction to obtain the sheaf of $\mathcal{O}_S$-Hopf algebras $\mathcal{A}^D$, which is again finite locally free over $\mathcal{O}_S$. Again write $\operatorname{ev} : \mathcal{A} \to \mathcal{A}^{DD}$ for the $\mathcal{O}_S$-linear evaluation map, and note that ev is a morphism of $\mathcal{O}_S$-Hopf algebras. On the other hand, for group schemes G and H over S the functor $\mathscr{H}om(G, H) : \mathsf{Sch}/S^{\text{opp}} \to \mathsf{Grp}$ assigns to each S-scheme T the group $\operatorname{Hom}_{\mathsf{Gr}/T}(G_T, H_T)$. For $G \in \operatorname{Ob}(\mathsf{Gr}/S)$ finite locally free, the following theorem shows that $\mathscr{H}om(G, \mathbb{G}_m)$ is representable by G^D.

Theorem 1.9 (Cartier Duality)**.** *The group scheme $G^D = \operatorname{Spec} \mathcal{A}^D$ is finite locally free over S, and the homomorphism of S-group schemes $G^{DD} \to G$ induced by the morphism $\mathrm{ev} : \mathcal{A} \to \mathcal{A}^{DD}$ is an isomorphism. Moreover, $\mathscr{H}om(G, \mathbb{G}_m)$ is isomorphic to h_{G^D}.*

Proof. The first statement we have seen. The second statement is true because ev is an isomorphism locally by Remark 1.8. For the third statement, see [7, 3.22]. □

Remark 1.10. The S-group scheme G^D is called the *Cartier dual* of G. Note that the functor $G \mapsto G^D$ is compatible with base change: if T is an S-scheme and G is a finite locally free S-group scheme then $(G_T)^D = (G^D)_T$. Also remark that the morphism of $\mathcal{O}_S$-Hopf algebras $\mathrm{ev} : \mathcal{A} \to \mathcal{A}^{DD}$ is natural in $\mathcal{A}$. Together with Theorem 1.9 this shows that sending a group scheme to its Cartier dual induces an anti-equivalence of the category of finite locally free group schemes over S with itself.

Examples 1.11. The functorial description of the dual of a finite locally free group scheme makes it easier to calculate:

1. Consider $\underline{\mathbb{Z}/n\mathbb{Z}}$ for some $n \in \mathbb{Z}_{\geqslant 1}$. By evaluating $\mathscr{H}om(\underline{\mathbb{Z}/n\mathbb{Z}}, \mathbb{G}_m)$ on S-schemes T it becomes clear that $\underline{\mathbb{Z}/n\mathbb{Z}^D} = \mu_n$. Therefore $\underline{\mathbb{Z}/n\mathbb{Z}}$ and μ_n are Cartier dual to each other.

2. Assume the scheme S is a scheme over $\mathbb{F}_p$. The S-group scheme α_p is its own Cartier dual via the natural pairing, defined on T-valued points:
$$\alpha_p \times \alpha_p \to \mathbb{G}_m, \quad (x, y) \mapsto \exp(xy) = \sum_{i=0}^{p-1} \frac{(xy)^i}{i!}.$$

1.3 Finite locally free group schemes in characteristic p

In the sequel we want to study phenomena that are specific to schemes of characteristic p. We thus adopt the following convention.

Convention 1.12. In the rest of this thesis, the scheme S is a scheme over $\mathbb{F}_p$.

Let X be a scheme over S. Define a morphism of sheaves of rings $\mathcal{O}_X \to \mathcal{O}_X$ by $x \mapsto x^p$. The induced morphism on stalks is local: we obtain a morphism of schemes $F_X : X \to X$ if we define F_X to be the identity on the topological space of X. We call F_X the *absolute Frobenius of* X. Because F_X is in general not a morphism of S-schemes, we consider the relative situation: define $X^{(p/S)} \to S$ to be the pull-back of $X \to S$ via $F_S : S \to S$. We see that $F_X : X \to X$ defines a morphism of S-schemes $F_{X/S} : X \to X^{(p)}$, called the *relative Frobenius of X over S*. If there is no risk of confusion we write $X^{(p)}$ for $X^{(p/S)}$; note that in general this scheme depends on the base scheme S. If $X = G$ is a group scheme over S, then $G^{(p)}$ naturally obtains the structure of an S-group scheme by Example 1.3.3, and the relative Frobenius $F_{G/S} : G \to G^{(p)}$ is a homomorphism of S-group schemes in this case. If G is finite locally free we use Remark 1.10 to define the homomorphism of S-group schemes $V_{G/S}$ called the *Verschiebung of G over S*:

$$V_{G/S} : G^{(p)} = (G^{DD})^{(p)} = ((G^D)^{(p)})^D \xrightarrow{F^*_{G^D/S}} G^{DD} = G.$$

2 Frobenius modules

The main goal of this section is to show that if we impose one extra condition on an S-group scheme G that is finite locally free, namely $F_{G/S} = 0$, we can describe G in terms of a sheaf of restricted Lie algebras. The purpose of this will become clear in Section 3, namely describing actions on schemes over S in terms of morphisms of restricted $\mathcal{O}_S$-Lie algebras. We define Frobenius modules in Section 2.1. The sheaves $\omega_G^\vee$ and α_G will be our first examples of those. We show that the category of Frobenius modules is equivalent to the category $\mathscr{G}r/S^{F=0}$ of finite locally free group schemes killed by their relative Frobenius. In Section 2.2 we prove that $\omega_G^\vee$ is canonically isomorphic to the sheaf of left-invariant derivations on G over S, which implies yet another description of $\mathscr{G}r/S^{F=0}$. The results thus obtained imply a nice corollary, which we present in Section 2.4: a classification of finite connected order p group schemes over a field. Before doing so, in Section 2.3 we show that the bracket on the sheaf of left-invariant derivations of a finite locally free S-group scheme is trivial. The implication is that Frobenius modules are restricted Lie algebras. A finite locally free S-group scheme G is killed by p if it is killed by $F_{G/S}$ by [7, 5.19] - for a description of general finite locally free group schemes killed by p, in terms of Dieudonné modules over a scheme over $\mathbb{F}_p$, see [5].

2.1 Finite locally free group schemes and Frobenius modules

Notation 2.1. Denote by $\mathscr{G}r/S$ the category of finite locally free group schemes over S, by $\mathscr{G}r/S^{F=0}$ the category of finite locally free group schemes over S with zero relative Frobenius, and by $\mathscr{G}r/S^{V=0}$ the category of finite locally free group schemes over S with zero Verschiebung. We regard these as full subcategories of Gr/S and thus have inclusions $\mathscr{G}r/S^{F=0} \subset \mathscr{G}r/S \subset \mathsf{Gr}/S$ and $\mathscr{G}r/S^{V=0} \subset \mathscr{G}r/S \subset \mathsf{Gr}/S$. If G is any group scheme over S, following Proposition 1.4, we let it have structure morphism $\pi : G \to S$, multiplication $m : G \times G \to G$, unit section $e : S \to G$ and inverse homomorphism $\operatorname{inv} : G \to G$.

Let $G = \operatorname{Spec} \mathcal{A}$ be a group scheme that is affine over S. Note that the assignment $U \mapsto \operatorname{Hom}_{\mathrm{Gr}/U}(G_U, (\mathbb{G}_a)_U)$ defines a sheaf of $\mathcal{O}_S$-modules which we denote by α_G. We also define a sheaf of $\mathcal{O}_S$-modules $\mathscr{P}rim(G)$ that associates to any open $U \subset S$ the $\mathcal{O}_S(U)$-module $\operatorname{Prim}(\mathcal{A}(U))$ consisting of the *primitive elements* of $\mathcal{A}(U)$, i.e. the elements $\alpha \in \mathcal{A}$ that satisfy $\tilde{m}(\alpha) = \alpha \otimes 1 + 1 \otimes \alpha$.

Lemma 2.2. *There is a canonical isomorphism of $\mathcal{O}_S$-modules $\alpha_G = \mathscr{P}rim(G)$.*

Proof. This is $\alpha_G \xrightarrow{f \mapsto \tilde{f}} \mathscr{H}om_{\mathcal{O}_S\text{-}\mathsf{Hopf}}(\mathcal{O}_S[x], \mathcal{A}) \xrightarrow{\tilde{f} \mapsto \tilde{f}(x)} \mathscr{P}rim(G)$. □

Since the structure morphism $\pi : G \to S$ is affine, G is separated over S which makes the unit section $e : S \to G$ a closed immersion by [7, 3.12.i]. Let $\mathcal{I}'$ be the quasi-coherent ideal sheaf that defines $e(S)$ in G, i.e. the kernel of $\mathcal{O}_G \to e_* \mathcal{O}_S$. Define $\mathcal{I} = \pi_* \mathcal{I}'$, which will be the kernel of $\tilde{e} : \mathcal{A} \to \mathcal{O}_S$ by left-exactness of π_*. We call $\mathcal{I}$ the *augmentation ideal sheaf* of G over S. Define a sheaf of $\mathcal{O}_S$-modules $\omega_G = \mathcal{I}/\mathcal{I}^2$.

Lemma 2.3. *There is a canonical isomorphism of $\mathcal{O}_S$-modules $\omega_G = e^*\Omega^1_{G/S}$.*

Proof. See [11, II, 4.11.4.c]. □

Remark that the assignments $\omega : G \mapsto \omega_G$ and $\alpha : G \mapsto \alpha_G$ are functorial in G and thus define functors from the category of group schemes that are affine over S to the category of $\mathcal{O}_S$-modules. In fact, the following is true.

Proposition 2.4.

1. *ω defines a contravariant functor from the category of group schemes over S to the category of quasi-coherent $\mathcal{O}_S$-modules.*

2. *ω commutes with base change: for each scheme T over S one has $(\omega_G)_T = \omega_{G_T}$.*

3. *If G is locally of finite presentation then ω_G is an $\mathcal{O}_S$-module of finite presentation.*

Proof. The statements follow from Lemma 2.3. □

We proceed to show how the functors ω and α can be used to describe finite locally free S-group schemes G with zero Frobenius in terms of certain finite locally free $\mathcal{O}_S$-modules. Such a description will be useful later when we want to find actions of such group schemes on schemes over S. First we prove a duality between α_G and ω_G.

Proposition 2.5. *Let G be a finite locally free group scheme over S. There are canonical isomorphisms of $\mathcal{O}_S$-modules*

$$\omega_G^\vee = \mathscr{P}rim(G^D) = \alpha_{G^D}.$$

Proof. The second isomorphism is Lemma 2.2. To prove the first, write $G = \operatorname{Spec} \mathcal{A}$. Because the augmentation $\tilde{e} : \mathcal{A} \to \mathcal{O}_S$ has a section $\tilde{\pi} : \mathcal{O}_S \to \mathcal{A}$ we have $\mathcal{A} = \mathcal{O}_S \oplus \mathcal{I}$ as $\mathcal{O}_S$-modules. We claim that it suffices to show that the following condition holds:

$$\alpha \in \mathcal{A}^D \text{ is primitive if and only } \alpha(1) = \alpha(\mathcal{I}^2) = 0. \tag{1}$$

Suppose condition (1) holds. Then

$$\mathscr{P}rim(G^D) = \{\alpha \in \mathscr{H}om_{\mathcal{O}_S}(\mathcal{A}, \mathcal{O}_S) : \alpha(1) = \alpha(\mathcal{I}^2) = 0\} \subset \mathcal{A}^D.$$

The decomposition $\mathcal{A} = \mathcal{O}_S \oplus \mathcal{I}$ gives a canonical morphism of $\mathcal{O}_S$-modules

$$\phi : \mathscr{H}om_{\mathcal{O}_S}(\mathcal{I}/\mathcal{I}^2, \mathcal{O}_S) \to \mathscr{P}rim(G^D), \quad \phi(f)(a, b) = f(b \bmod \mathcal{I}^2),$$

which is an isomorphism. Therefore it remains to show that condition (1) holds. By definition, $\alpha \in \mathcal{A}^D$ is primitive if

$$\tilde{\Delta}^*(\alpha) = \alpha \otimes \tilde{e} + \tilde{e} \otimes \alpha. \tag{2}$$

Equation (2) holds if and only for each pair of local sections $x, y \in \mathcal{A}$, one has

$$\alpha(xy) = \alpha(x)\tilde{e}(y) + \tilde{e}(x)\alpha(y). \tag{3}$$

Because $\mathcal{A} = \mathcal{O}_S \oplus \mathcal{I}$, equation (3) holds if and only if $\alpha(1) = \alpha(\mathcal{I}^2) = 0$. □

Corollary 2.6. *The assignment $\alpha : G \mapsto \alpha_G$ defines a contravariant functor from $\mathscr{G}r/S$ to the category of quasi-coherent $\mathcal{O}_S$-modules.*

Proof. This follows from Proposition 2.4 and [19, 17.20.5]. □

Since our aim is to describe finite locally free group schemes G in terms of certain finite locally free $\mathcal{O}_S$-modules via α and ω, in order to make ω_G and α_G finite locally free we need to put extra assumptions on G.

Proposition 2.7. *Let G be a finite locally free group scheme over S.*

1. *If the relative Frobenius of G is zero then ω_G is finite locally free. For such group schemes G, the functors $G \mapsto \omega_G^\vee$ and $G \mapsto \alpha_{G^D}$ commute with base change.*

2. *If the Verschiebung of G is zero then α_G is finite locally free. In this case the functor $G \mapsto \alpha_G$ commutes with base change.*

Proof. 1. If $F_{G/S} = 0$ then ω_G is finite locally free by [11, VII$_A$, 7.4]. By Proposition 2.4 there is a natural isomorphism of $\mathcal{O}_T$-modules $(\omega_G)_T = \omega_{G_T}$. The canonical map $\omega_G^\vee \otimes \mathcal{O}_T \to \mathscr{H}om_{\mathcal{O}_T}(\omega_G \otimes \mathcal{O}_T, \mathcal{O}_T)$ is an isomorphism because ω_G is finite locally free, so $G \mapsto \omega_G^\vee$ commutes with base change. Furthermore, $\omega_G^\vee = \alpha_{G^D}$ by Proposition 2.5, and one checks that this isomorphism is compatible with base change.

2. If $V_{G/S} = 0$ then $F_{G^D/S} = 0$ and so ω_{G^D} is finite locally free by Proposition 2.7.1. This makes $\alpha_G = \omega_{G^D}^\vee$ finite locally free using Proposition 2.5, and this isomorphism is compatible with base change. The functor $G \mapsto \omega_{G^D}^\vee$ from $\mathscr{G}r/S^{V=0}$ to the category of finite locally free $\mathcal{O}_S$-modules is the composition of the Cartier duality functor $\mathscr{G}r/S^{V=0} \to \mathscr{G}r/S^{F=0}$ and the functor from $\mathscr{G}r/S^{F=0}$ to the category of finite locally free $\mathcal{O}_S$-modules, both compatible with base change by 1.10 and 2.7.1. □

As $G \mapsto \omega_G^\vee$ is functorial in G, $\omega^\vee$ gives a covariant functor from $\mathscr{G}r/S^{F=0}$ to the category of finite locally free $\mathcal{O}_S$-modules by Proposition 2.7. For any object G in $\mathscr{G}r/S^{F=0}$, Proposition 2.7 also shows that $F_S^*\omega_G^\vee = \omega_{G^{(p)}}^\vee$. Using Proposition 2.4 the Verschiebung $V_{G/S}$ gives a map $\omega(V_{G/S}) : \omega_G \to \omega_{G^{(p)}}$ which induces a map $\omega_{G^{(p)}}^\vee \to \omega_G^\vee$. The composition gives a morphism of $\mathcal{O}_S$-modules $F_S^*\omega_G^\vee \to \omega_G^\vee$ which we denote by $\varphi(\omega_G^\vee)$. Dually, if G is an object in $\mathscr{G}r/S^{V=0}$, the composite of $F_S^*\alpha_G = \alpha_{G^{(p)}}$ with $\alpha(F_{G/S}) : \alpha_{G^{(p)}} \to \alpha_G$ gives a morphism $\varphi(\alpha_G) : F_S^*\alpha_G \to \alpha_G$ by 2.7 and 2.6.

Remark 2.8. If G is an object in $\mathscr{G}r/S^{F=0}$, the morphism $\varphi(\omega_G^\vee) : F_S^*\omega_G^\vee \to \omega_G^\vee$ corresponds to the morphism $\varphi(\alpha_{G^D}) : F_S^*\alpha_{G^D} \to \alpha_{G^D}$ under the isomorphism $\alpha_{G^D} = \omega_G^\vee$ from Proposition 2.5. Similarly, for G in $\mathscr{G}r/S^{V=0}$, by Proposition 2.5 and Theorem 1.9, there exists an isomorphism $\alpha_G = \omega_{G^D}^\vee$, and the morphism $\varphi(\alpha_G) : F_S^*\alpha_G \to \alpha_G$ corresponds to the morphism $\varphi(\omega_{G^D}^\vee) : F_S^*\omega_{G^D}^\vee \to \omega_{G^D}^\vee$ under this identification.

The $\mathcal{O}_S$-modules $\omega_G^\vee$ and α_G for G in $\mathscr{G}r/S$ with $F_{G/S} = 0$, respectively $V_{G/S} = 0$, are our first examples of Frobenius modules.

Definition 2.9. A *Frobenius $\mathcal{O}_S$-module* is a finite locally free $\mathcal{O}_S$-module $\mathscr{M}$ equipped with an $\mathcal{O}_S$-linear map $\varphi : F_S^*\mathscr{M} \to \mathscr{M}$.

Let $(\mathscr{M}, \varphi)$ and $(\mathscr{N}, \psi)$ be two Frobenius $\mathcal{O}_S$-modules. A *morphism of Frobenius $\mathcal{O}_S$-modules* is a morphism of $\mathcal{O}_S$-modules $\mathscr{M} \to \mathscr{N}$ such that the induced map $F_S^*\mathscr{M} \to F_S^*\mathscr{N}$ gives a commutative diagram

$$\begin{tikzcd}
\mathscr{M} \arrow[r] & \mathscr{N} \\
F_S^*\mathscr{M} \arrow[u, "\varphi"] \arrow[r] & F_S^*\mathscr{N}. \arrow[u, "\psi"']
\end{tikzcd}$$

In this way Frobenius $\mathcal{O}_S$-modules form a category which we denote by M_S.

Remark that the assignments $(\omega^\vee, \varphi(\omega^\vee)) : G \mapsto (\omega_G^\vee, \varphi(\omega_G^\vee))$ and $(\alpha, \varphi(\alpha)) : G \mapsto (\alpha_G, \varphi(\alpha_G))$ are functorial in G, i.e. define functors from $\mathscr{G}r/S^{F=0}$ (resp. $\mathscr{G}r/S^{V=0}$) to M_S. We proceed to show how to go the other way, so that we can prove that $\omega^\vee$ and α are equivalences of categories. Let $(\mathscr{M}, \varphi)$ be a Frobenius $\mathcal{O}_S$-module. There is an injection $F_S^*\mathscr{M} \hookrightarrow \mathrm{Sym}^p(\mathscr{M})$ sending $m \otimes 1$ to m^p. Let $\mathscr{J}$ be the ideal in $\mathrm{Sym}(\mathscr{M})$ generated by elements $x - \varphi(x \otimes 1)$ for local sections $x \in F_S^*\mathscr{M} \subset \mathrm{Sym}^p(\mathscr{M})$. Put $\mathcal{A}(\mathscr{M}, \varphi) = \mathrm{Sym}(\mathscr{M})/\mathscr{J}$ which is a sheaf of quasi-coherent $\mathcal{O}_S$-algebras. $\mathcal{A}(\mathscr{M}, \varphi)$ can be made into a sheaf of $\mathcal{O}_S$-Hopf algebras with comultiplication

$$\mathcal{A}(\mathscr{M}, \varphi) \to \mathcal{A}(\mathscr{M}, \varphi) \otimes \mathcal{A}(\mathscr{M}, \varphi), \quad m \mapsto m \otimes 1 + 1 \otimes m \quad \text{for } m \in \mathscr{M}.$$

In this way we obtain a group scheme $G(\mathscr{M}, \varphi) = \mathrm{Spec}\,\mathcal{A}(\mathscr{M}, \varphi)$ that is affine over S. Observe that the assignment $(\mathscr{M}, \varphi) \mapsto G(\mathscr{M}, \varphi)$ is functorial in $\mathscr{M}$. If $(\mathscr{M}, \varphi)$ is a Frobenius module, the S-group scheme $G(\mathscr{M}, \varphi)^D$ is killed by the relative Frobenius $F_{G(\mathscr{M},\varphi)^D/S}$ by [11, VII$_A$, 7.2], and finite locally free by [11, VII$_A$, 5.5.2]. Therefore, $(\mathscr{M}, \varphi) \mapsto G(\mathscr{M}, \varphi)^D$ gives a covariant functor from M_S to $\mathscr{G}r/S^{F=0}$, and dually, $(\mathscr{M}, \varphi) \mapsto G(\mathscr{M}, \varphi)$ gives a contravariant functor from M_S to $\mathscr{G}r/S^{V=0}$.

Proposition 2.10. *1. The covariant functors*

$$\begin{aligned} \mathscr{G}r/S^{F=0} \quad &\to \quad \mathsf{M}_S, \quad G \mapsto (\omega_G^\vee, F_S^*\omega_G^\vee \xrightarrow{\varphi(\omega_G^\vee)} \omega_G^\vee), \\ \mathsf{M}_S \quad &\to \quad \mathscr{G}r/S^{F=0}, \quad (\mathscr{M}, \varphi) \mapsto G(\mathscr{M}, \varphi)^D \end{aligned}$$

are quasi-inverse to one-another. This makes $\mathscr{G}r/S^{F=0}$ equivalent to M_S.

2. Dually, the contravariant functors

$$\begin{aligned} \mathscr{G}r/S^{V=0} \quad &\to \quad \mathsf{M}_S, \quad G \mapsto (\alpha_G, F_S^*\alpha_G \xrightarrow{\varphi(\alpha_G)} \alpha_G), \\ \mathsf{M}_S \quad &\to \quad \mathscr{G}r/S^{V=0}, \quad (\mathscr{M}, \varphi) \mapsto G(\mathscr{M}, \varphi) \end{aligned}$$

are quasi-inverse to one-another. This makes $\mathscr{G}r/S^{V=0}$ anti-equivalent to M_S.

Proof. This is a direct consequence of the above constructions and [11, VII$_A$, 7.4]. □

2.2 Left-invariant derivations

If G is in $\mathscr{G}r/S^{F=0}$ and if X is a scheme which is affine over S, Theorem 2.10 can help us to find actions of G on X over S. In order to get there we need a more explicit description of the morphism $\varphi(\omega_G^\vee) : F_S^*\omega_G^\vee \to \omega_G^\vee$, which requires an identification of $\omega_G^\vee$ with a sheaf of restricted $\mathcal{O}_S$-Lie algebras. We let $G = \operatorname{Spec}\mathcal{A}$ be an object in $\mathscr{G}r/S^{F=0}$ and consider the sheaf of $\mathcal{O}_S$-modules $\mathscr{D}er_{\mathcal{O}_S}(\mathcal{A},\mathcal{A})$, that assigns to an open $U \subset S$ the $\Gamma(U,\mathcal{O}_S)$-module $\operatorname{Der}_{\mathcal{O}_U}(\mathcal{A}_U,\mathcal{A}_U)$ of $\mathcal{O}_U$-linear derivations $\mathcal{A}_U \to \mathcal{A}_U$.

Definition 2.11. A derivation $D : \mathcal{A}_U \to \mathcal{A}_U$ is *left-invariant* if the following diagram commutes:

$$\begin{tikzcd}
\mathcal{A}_U \arrow[r, "\tilde{m}"] \arrow[d, "D"] & \mathcal{A}_U \otimes \mathcal{A}_U \arrow[d, "\mathrm{id} \otimes D"] \\
\mathcal{A}_U \arrow[r, "\tilde{m}"] & \mathcal{A}_U \otimes \mathcal{A}_U.
\end{tikzcd}$$

Then $\mathscr{D}er_{\mathcal{O}_S}(\mathcal{A},\mathcal{A})$ admits a sub $\mathcal{O}_S$-module that assigns to each open $U \subset S$ the $\Gamma(U,\mathcal{O}_S)$-module $\text{L-Der}_{\mathcal{O}_U}(\mathcal{A}_U,\mathcal{A}_U) \subset \operatorname{Der}_{\mathcal{O}_U}(\mathcal{A}_U,\mathcal{A}_U)$, where $\text{L-Der}_{\mathcal{O}_U}(\mathcal{A}_U,\mathcal{A}_U)$ consists of the left-invariant $\mathcal{O}_U$-derivations $\mathcal{A}_U \to \mathcal{A}_U$. We define $\mathscr{L}(G) \subset \mathscr{D}er_{\mathcal{O}_S}(\mathcal{A},\mathcal{A})$ to be this $\mathcal{O}_S$-module. Remark that for any left-invariant $\mathcal{O}_U$-derivation $D : \mathcal{A}_U \to \mathcal{A}_U$, its p-th composite D^p is again a $\mathcal{O}_U$-derivation because we are in characteristic p, and left-invariant by the commutativity of the outer diagram in the following composite of diagrams:

$$\begin{tikzcd}
\mathcal{A}_U \arrow[r, "D"] \arrow[d, "\tilde{m}"] & \mathcal{A}_U \arrow[r, "D"] \arrow[d, "\tilde{m}"] & \mathcal{A}_U \arrow[r, "D"] \arrow[d, "\tilde{m}"] & \cdots & \cdots \arrow[r, "D"] & \mathcal{A}_U \arrow[d, "\tilde{m}"] \\
\mathcal{A}_U \otimes \mathcal{A}_U \arrow[r, "\mathrm{id} \otimes D"] & \mathcal{A}_U \otimes \mathcal{A}_U \arrow[r, "\mathrm{id} \otimes D"] & \mathcal{A}_U \otimes \mathcal{A}_U \arrow[r, "\mathrm{id} \otimes D"] & \cdots & \cdots \arrow[r, "\mathrm{id} \otimes D"] & \mathcal{A}_U.
\end{tikzcd}$$

Proposition 2.12. *Let G be an object in $\mathscr{G}r/S^{F=0}$. There is a canonical isomorphism*

$$\omega_G^\vee = \mathscr{L}(G).$$

Moreover, the morphism $\varphi(\omega_G^\vee) : F_S^*\omega_G^\vee \to \omega_G^\vee$ from Proposition 2.10 corresponds to the morphism $F_S^*\mathscr{L}(G) \to \mathscr{L}(G), D \otimes 1 \mapsto D^p$ under this identification.

Proof. Because $\omega_G^\vee = \alpha_{G^D}$ by Proposition 2.5, and because the morphism $\varphi(\omega_G^\vee) : F_S^*\omega_G^\vee \to \omega_G^\vee$ corresponds to the morphism $\varphi(\alpha_{G^D}) : F_S^*\alpha_{G^D} \to \alpha_{G^D}$ under this identification by Remark 2.8, it suffices to prove the claim for α_{G^D} and $\varphi(\alpha_{G^D})$.

Consider the space of $\mathcal{O}_S$-derivations $\mathscr{D}er_{\tilde{e},\mathcal{O}_S}(\mathcal{A},\mathcal{O}_S)$ where $\mathcal{A}$ acts on $\mathcal{O}_S$ via $\tilde{e}$. Because $\alpha(xy) = \alpha(x)\tilde{e}(y) + \tilde{e}(x)\alpha(y)$ for all local sections $x, y \in \mathcal{A}^D$ if and only if $\tilde{m}(\alpha) = \alpha \otimes \tilde{e} + \tilde{e} \otimes \alpha$, we see that $\mathscr{D}er_{\tilde{e},\mathcal{O}_S}(\mathcal{A},\mathcal{O}_S) = \mathscr{P}rim(G^D)$. We claim that $\mathscr{L}(G) = \mathscr{D}er_{\tilde{e},\mathcal{O}_S}(\mathcal{A},\mathcal{O}_S)$. To define a natural map $\mathscr{D}er_{\tilde{e},\mathcal{O}_S}(\mathcal{A},\mathcal{O}_S) \to \mathscr{L}(G)$, observe that if $\alpha \in \mathscr{D}er_{\tilde{e},\mathcal{O}_S}(\mathcal{A},\mathcal{O}_S)$, then $(\mathrm{id} \otimes \alpha) \circ \tilde{m}$ is a left-invariant $\mathcal{O}_S$-derivation $\mathcal{A} \to \mathcal{A}$. Write $D_\alpha = (\mathrm{id} \otimes \alpha) \circ \tilde{m}$. Conversely, to define $\mathscr{L}(G) \to \mathscr{D}er_{\tilde{e},\mathcal{O}_S}(\mathcal{A},\mathcal{O}_S)$, observe that if an $\mathscr{O}_S$-linear map $D : \mathcal{A} \to \mathcal{A}$ is a left-invariant derivation, then $\tilde{e} \circ D$ is a derivation $\mathcal{A} \to \mathscr{O}_S$. Both maps are linear in $\mathscr{O}_S$; we shall show they are inverse. Let $D \in \mathscr{L}(G)$. Then

$$D_{\tilde{e}\circ D} = (\mathrm{id} \otimes (\tilde{e} \circ D)) \circ \tilde{m} = (\mathrm{id} \otimes \tilde{e}) \circ (\mathrm{id} \otimes D) \circ \tilde{m} = (\mathrm{id} \otimes \tilde{e}) \circ \tilde{m} \circ D = D.$$

For $\alpha \in \mathscr{D}er_{\tilde{e},\mathscr{O}_S}(\mathcal{A}, \mathscr{O}_S)$, we have

$$\tilde{e} \circ D_\alpha = \tilde{e} \circ (\mathrm{id} \otimes \alpha) \circ \tilde{m} = (\tilde{e} \otimes \alpha) \circ \tilde{m} = \tilde{e} \cdot \alpha = \alpha,$$

which proves $\mathscr{L}(G) = \mathscr{D}er_{\tilde{e},\mathscr{O}_S}(\mathcal{A}, \mathscr{O}_S)$. This gives an isomorphism of $\mathscr{O}_S$-modules

$$\mathscr{P}rim(G^D) \to \mathscr{L}(G), \quad \alpha \mapsto D_\alpha.$$

To prove the second claim, observe that the relative Frobenius $F_{G^D/S} : G^D \to (G^D)^{(p)}$ corresponds to the map of $\mathscr{O}_S$-algebras

$$F_{\mathcal{A}^D/\mathscr{O}_S} = \tilde{F}_{G^D/S} : \mathcal{A}^D \otimes \mathscr{O}_S \to \mathcal{A}^D, \quad F_{\mathcal{A}^D/\mathscr{O}_S}(\alpha \otimes 1) = \alpha^p.$$

This gives a map

$$F_{\mathcal{A}^D/\mathscr{O}_S,*} : \mathscr{H}om_{\mathscr{O}_S\text{-}\mathsf{Hopf}}(\mathscr{O}_S[x], \mathcal{A}^D \otimes \mathscr{O}_S) \to \mathscr{H}om_{\mathscr{O}_S\text{-}\mathsf{Hopf}}(\mathscr{O}_S[x], \mathcal{A}^D).$$

But $\mathscr{H}om_{\mathscr{O}_S\text{-}\mathsf{Hopf}}(\mathscr{O}_S[x], \mathcal{A}^D) = \mathscr{P}rim(G^D)$ and $\mathscr{H}om_{\mathscr{O}_S\text{-}\mathsf{Hopf}}(\mathscr{O}_S[x], \mathcal{A}^D \otimes \mathscr{O}_S) = \mathscr{P}rim(G^D \otimes \mathscr{O}_S) = \mathscr{P}rim(G^D) \otimes \mathscr{O}_S$ by Lemma 2.2 and Proposition 2.7, where the second map is an isomorphism because $F_{G/S} = 0$. Under this identification the map $F_{\mathcal{A}^D/\mathscr{O}_S,*}$ corresponds to

$$\mathscr{P}rim(G^D) \otimes \mathscr{O}_S \to \mathscr{P}rim(G^D), \quad \alpha \otimes 1 \mapsto \alpha^p.$$

As D_α is the locally the composite

$$\mathcal{A} \xrightarrow{\tilde{m}} \mathcal{A} \otimes \mathcal{A} \xrightarrow{\mathrm{id} \otimes \alpha} \mathcal{A} \otimes \mathscr{O}_S = \mathcal{A},$$

its dual morphism D_α^* is locally the composite

$$\mathcal{A}^D \xleftarrow{\text{mult}} \mathcal{A}^D \otimes \mathcal{A}^D \xleftarrow{\beta \otimes \alpha \leftarrow\!\shortmid \beta \otimes 1} \mathcal{A}^D \otimes \mathscr{O}_S = \mathcal{A}^D.$$

But this map is nothing but $\beta \mapsto \beta\alpha$, the multiplication by α. It follows that we have $D^*_{\alpha^p} = (D^*_\alpha)^p$. Take the dual on both sides, and note that $(D^*_\alpha \circ D^*_\alpha \circ ... \circ D^*_\alpha)^* = D^{**}_\alpha \circ D^{**}_\alpha \circ ... \circ D^{**}_\alpha = D^p_\alpha$. This gives the equality $D_{\alpha^p} = D^p_\alpha$, and proves the proposition. □

By Proposition 2.12 we can restate Proposition 2.10.1 to obtain the following theorem.

Theorem 2.13. *The covariant functor*

$$\mathscr{G}r/S^{F=0} \quad \to \quad \mathsf{M}_S, \quad G \mapsto (\mathscr{L}(G), F_S^*\mathscr{L}(G) \xrightarrow{\varphi_G} \mathscr{L}(G)) \quad \text{with} \quad \varphi_G(D \otimes 1) = D^p$$

is an equivalence of categories, with quasi-inverse $(\mathscr{L}, \varphi) \mapsto G(\mathscr{L}, \varphi)^D$. □

Remark 2.14. For each $r \in \mathbb{Z}_{\geqslant 0}$ we denote by $\mathscr{G}r/S_r^{F=0} \subset \mathscr{G}r/S^{F=0}$ the full subcategory of objects in $\mathscr{G}r/S^{F=0}$ which are finite locally free of order p^r, and by $\mathsf{M}_S^r \subset \mathsf{M}_S$ the Frobenius modules which are finite locally free of rank r. Then restricting the equivalence of Theorem 2.13 to $\mathscr{G}r/S_r^{F=0}$ induces an equivalence of categories

$$\mathscr{G}r/S_r^{F=0} \xrightarrow{\sim} \mathsf{M}_S^r.$$

Indeed, given a Frobenius module $(\mathscr{M}, \varphi)$, let $U \subset S$ be open such that $\mathscr{M}|_U$ is free of rank r. The $\mathcal{O}_S|_U$-algebra $\mathrm{Sym}(\mathscr{M}|_U)$ is finitely generated, namely by the r elements x_i that generate $\mathscr{M}|_U$ as an $\mathcal{O}_S|_U$-module. The ideal sheaf $\mathscr{J}|_U$ is generated by the elements $x_i^p - \varphi(x_i \otimes 1)$, and so modding out by $\mathscr{J}|_U$ makes $\mathcal{A}(\mathscr{M}, \varphi)|_U = \mathrm{Sym}(\mathscr{M}|_U)/\mathscr{J}|_U$ free of rank p^r as a sheaf of modules over $\mathcal{O}_S|_U$.

2.3 Restricted Lie algebras

Convention 2.15. We continue to assume S is a scheme over $\mathbb{F}_p$. In the preceeding all our algebras were commutative. In Section 2.3 we relax this condition.

Let G be an object in $\mathscr{G}r/S^{F=0}$. There is another description of Frobenius modules, one that will prove important in later sections, when we want to use Theorem 2.13 to produce actions of G on any scheme X that is affine over S. Recall the definition of a *Lie algebra over a ring* as in [1, 2.1]. Recall further that a *sheaf of $\mathcal{O}_S$-Lie algebras* is a sheaf of $\mathcal{O}_S$-modules $\mathfrak{g}$ such that, for every open $U \subset S$ the $\mathcal{O}_S(U)$-module $\mathfrak{g}(U)$ has the structure of a Lie algebra over the ring $\mathcal{O}_S(U)$, and this structure is natural in U. Finally, recall that, for such a sheaf of Lie algebras $\mathfrak{g}$, for any $x \in \mathfrak{g}$ the map $\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g}$ is the $\mathcal{O}_S$-linear map defined by $\mathrm{ad}_x(y) = [x, y]$.

Definition 2.16. A *sheaf of restricted $\mathcal{O}_S$-Lie algebras* is a sheaf of Lie algebras $\mathfrak{g}$ over $\mathcal{O}_S$ equipped with a map $(\cdot)^{[p]} : \mathfrak{g} \to \mathfrak{g}$, called the *p-operation*, such that, for all $a \in \mathcal{O}_S$ and for all $x, y \in \mathfrak{g}$, we have

- $(ax)^{[p]} = a^p x^{[p]}$
- $\mathrm{ad}_{x^{[p]}} = \mathrm{ad}_x^p$
- $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x, y)/i$, where $s_i(x, y)$ is the coefficient of t^{i-1} in the expression $\mathrm{ad}_{tx+y}^{p-1}(x)$.

Examples 2.17.
1. Let $\mathcal{A}$ be a sheaf of $\mathcal{O}_S$-algebras. Define a bracket and p-operation on $\mathcal{A}$ by $x^{[p]} = x^p$ and $[x, y] = xy - yx$ for all $x, y \in \mathcal{A}$. This makes $\mathcal{A}$ a sheaf of restricted Lie algebras which we denote by $\mathcal{A}'$ (see [12, 1]).

2. Let X be a scheme over S. Write $\mathscr{D}er_{X/S} = \mathscr{D}er_{\mathcal{O}_S}(\mathcal{O}_X, \mathcal{O}_X)$. Define $[-,-]$ on $\mathscr{D}er_{X/S}$ by $[D, D'] = D \circ D' - D' \circ D$ for local sections $D, D' \in \mathscr{D}er_{X/S}$, and a p-operation by $D \mapsto D^p$. Then $\mathscr{D}er_{X/S}$ is a restricted $\mathcal{O}_S$-Lie algebra (see [12, 4]).

3. Consider the description of Frobenius modules in Theorem 2.13. Every Frobenius $\mathcal{O}_S$-module $\mathscr{M}$ is isomorphic to the sheaf of left-invariant derivations $\mathscr{L}(G)$ for a group scheme G in $\mathscr{G}r/S^{F=0}$, so we can define a restricted Lie algebra structure on $\mathscr{M}$ via this isomorphism. We have a Lie-algebra structure on $\mathscr{D}er_{G/S}$ by 2.17.2, and $\mathscr{L}(G) \subset \mathscr{D}er_{G/S}$ is a sub-Lie algebra of $\mathscr{D}er_{G/S}$ by the remark under 2.11, and by the fact that the bracket of two left-invariant derivations is left-invariant.

We proceed to define morphisms of restricted Lie algebras. Naturally they need to respect the algebraic structure of restricted Lie algebras, in order to obtain a category.

Definition 2.18. Let $\mathfrak{g}$ and $\mathfrak{h}$ be restricted Lie algebras. An $\mathcal{O}_S$-linear map $f : \mathfrak{g} \to \mathfrak{h}$ is a *morphism of restricted $\mathcal{O}_S$-Lie algebras* if

- $f([x, y]) = [f(x), f(y)]$ for all $x, y \in \mathfrak{g}$,
- $f(x^{[p]}) = f(x)^{[p]}$ for all $x \in \mathfrak{g}$.

Definition 2.19. Let $\mathfrak{g}$ be a restricted $\mathcal{O}_S$-Lie algebra. The *restricted enveloping algebra* of $\mathfrak{g}$ is a sheaf of $\mathcal{O}_S$-algebras $\mathcal{A}$ together with a map of restricted Lie algebras $h : \mathfrak{g} \to \mathcal{A}'$ satisfying the following universal property: given any $\mathcal{O}_S$-algebra $\mathcal{B}$ and any map of restricted Lie algebras $f : \mathfrak{g} \to \mathcal{B}'$, there exists a unique map of $\mathcal{O}_S$-algebras $g : \mathcal{A} \to \mathcal{B}$ such that $f = g \circ h$.

It is clear that if the restricted enveloping algebra of $\mathfrak{g}$ exists, it is unique up to unique isomorphism. Therefore we denote it by $U(\mathfrak{g})$. To prove existence, let $T(\mathfrak{g})$ be the tensor algebra of $\mathfrak{g}$, considered as a sheaf of $\mathcal{O}_S$-modules. Notice that $\mathfrak{g} \hookrightarrow T(\mathfrak{g})$. Let $I \subset T(\mathfrak{g})$ be the ideal sheaf generated by elements of the form $x \otimes y - y \otimes x - [x, y]$ for $x, y \in \mathfrak{g}$. Let $J \subset T(\mathfrak{g})$ be the ideal sheaf generated by elements of the form $x^{\otimes p} - x^{[p]}$. Set $U(\mathfrak{g}) = T(\mathfrak{g})/(I, J)$. There is an embedding $\mathfrak{g} \hookrightarrow U(\mathfrak{g})$ defined by sending $x \in \mathfrak{g}$ to the element $x + I + J \in U(\mathfrak{g})$. This embedding induces a map of restricted $\mathcal{O}_S$-Lie algebras $h : \mathfrak{g} \hookrightarrow U(\mathfrak{g})'$ because quotienting out by I and J forces the bracket and p-operation in $U(\mathfrak{g})'$ to agree with the bracket and p-operation of $\mathfrak{g}$. Then $U(\mathfrak{g})$ satisfies the universal property of Definition 2.19.

Example 2.20. Consider Example 2.17.3. Let $I \subset T(\mathscr{L}(G))$ be the ideal sheaf generated by elements of the form $y \otimes z - z \otimes y - [y, z]$ for $y, z \in \mathscr{L}(G)$. Let $J \subset T(\mathscr{L}(G))$ be the ideal sheaf generated by elements of the form $x^{\otimes p} - \varphi_G(x \otimes 1)$ for $x \in \mathscr{L}(G)$. Finally, let $K \subset T(\mathscr{L}(G))$ be the ideal sheaf generated by elements of the form $y \otimes z - z \otimes y$ for $y, z \in \mathscr{L}(G)$. Note that the restricted enveloping algebra $U(\mathscr{L}(G))$ of $\mathscr{L}(G)$ is

$$U(\mathscr{L}(G)) = T(\mathscr{L}(G))/(I, J)$$

whereas

$$\mathcal{A}(\mathscr{L}(G), \varphi_G)) = \mathrm{Sym}(\mathscr{L}(G))/J = T(\mathscr{L}(G))/(J, K).$$

The latter is isomorphic to $\mathcal{A}^D$ by Theorem 2.13. Then $\mathcal{A}(\mathscr{L}(G), \varphi_G)) = U(\mathscr{L}(G)) = \mathcal{A}^D$ if and only if the bracket on $\mathscr{L}(G)$ is trivial - but this is true by the following proposition.

Proposition 2.21. *For a group scheme G in $\mathscr{G}r/S^{F=0}$, the bracket on the sheaf of restricted $\mathcal{O}_S$-Lie algebras $\mathscr{L}(G)$ is trivial.*

Proof. This is a consequence of [11, p.89]. We show the construction. For any finite locally free S-group scheme G killed by $F_{G/S}$, the strategy is to show that there is an isomorphism $\omega_G^\vee \to \mathscr{L}(G), x \mapsto d_x$, and that for each $x, y \in \omega_G^\vee$ one has $d_x d_y - d_y d_x = 0$.

Define $\mathcal{O}_I = \mathcal{O}_S[\epsilon]/(\epsilon^2)$, $\mathcal{O}_{I'} = \mathcal{O}_S[\epsilon']/(\epsilon'^2)$, $I = \operatorname{Spec} \mathcal{O}_I$ and $I' = \operatorname{Spec} \mathcal{O}_{I'}$. For any S scheme T we have a morphism $T \to I_T$ of schemes over T, defined by $\mathcal{O}_T[\epsilon]/(\epsilon^2) \to \mathcal{O}_T, \epsilon \mapsto 0$. This gives a homomorphism of groups $G_T(I_T) \to G_T(T)$. Define a functor $\underline{\mathrm{Lie}}(G/S) : \mathsf{Sch}/S^{\mathrm{opp}} \to \mathsf{Grp}$ to be the kernel of this homomorphism. By restricting $\underline{\mathrm{Lie}}(G/S)$ to opens $U \hookrightarrow S$, one retrieves the sheaf $\omega_G^\vee$ (this follows from [11, I, 4.6.5.1]).

Now let $x \in \underline{\mathrm{Lie}}(G/S)(I) \subset \mathrm{Hom}_{\mathsf{Sch}/I}(I \times I', G \times I)$. Then x induces a map

$$x' = (x, \mathrm{pr}_2) : I \times I' \to G \times I \times I'.$$

Similarly $y' \in \underline{\mathrm{Lie}}(G/S)(I') \subset \mathrm{Hom}_{\mathsf{Sch}/I'}(I \times I', G \times I')$ defines a map

$$y = (y', \mathrm{pr}_2) : I \times I' \to G \times I \times I'.$$

Let

$$\lambda_x, \lambda_y : G \times I \times I' \to G \times I \times I'$$

be the right translation maps by x' and y. Then λ_x and λ_y are automorphisms of $G_{I \times I'}$ as a group scheme over $I \times I'$. In particular λ_x and λ_y are automorphisms of $G_{I \times I'}$ as a scheme over S, where λ_x induces the identity on $G_{I'}$, and λ_y induces the identity on G_I. Therefore these maps correspond to $\mathcal{O}_S$-automorphisms u and v of $\mathcal{O}_{G_{I \times I'}} = \mathcal{O}_G[\epsilon, \epsilon']/(\epsilon^2, \epsilon'^2)$, where u is the identity on $\mathcal{O}_{G \times I'} = \mathcal{O}_G[\epsilon']/(\epsilon'^2)$ and v is the identity on $\mathcal{O}_{G \times I} = \mathcal{O}_G[\epsilon]/(\epsilon^2)$. But then u and v must be of the form

$$u = \mathrm{id} + \epsilon \cdot D_1 \qquad \text{and} \qquad v = \mathrm{id} + \epsilon' \cdot D_2$$

for $\mathcal{O}_S$-linear maps $D_1, D_2 : \mathcal{O}_G \to \mathcal{O}_G$. In fact, D_1 and D_2 are $\mathcal{O}_S$-linear derivations, and one can show they are left-invariant. We define $d_x = D_1 \in \Gamma(S, \mathscr{L}(G))$, and $d_y = D_2 \in \Gamma(S, \mathscr{L}(G))$.

Moreover, by [11, 4.7.3] there is an injection $\underline{\mathrm{Lie}}(G/S)(S) \hookrightarrow \underline{\mathrm{Lie}}(G/S)(I)$. By [11, 4.11] this makes the following map an isomorphism of $\Gamma(S, \mathcal{O}_S)$-Lie algebras:

$$\underline{\mathrm{Lie}}(G/S)(S) \to \mathscr{L}(G)(S), \quad x \mapsto d_x.$$

Because $\underline{\mathrm{Lie}}(G/S)(T) = \underline{\mathrm{Lie}}(G_T/T)(T)$ for every S-scheme T, it follows that the functors $\underline{\mathrm{Lie}}(G/S)$ and $T \mapsto \Gamma(T, \mathscr{L}(G)_T)$ are isomorphic. Restricting both functors to opens $U \hookrightarrow S$ we obtain an isomorphism

$$\omega_G^\vee \to \mathscr{L}(G), \quad x \mapsto d_x.$$

Let $D, D' \in \mathscr{L}(G)$. Then $D = d_x$ and $D' = d_y$ for some $x, y \in \omega_G^\vee$. Since G is commutative, we have

$$\lambda_x \lambda_y \lambda_x^{-1} \lambda_y^{-1} = \mathrm{id}\,.$$

It follows that

$$v^{-1} u^{-1} v u = \mathrm{id}\,.$$

But then $d_y d_x - d_x d_y = 0$. □

2.4 Classification of finite connected order p group schemes over a field

We will make explicit use of Theorem 2.13 in Section 3. A more immediate corollary is a classification of the group schemes over k which are connected and finite of order p. To give this result we first need to prove that those are precisely the k-group schemes which are killed by their relative Frobenius and finite of order p.

Convention 2.22. In Sections 2.3 and 2.4, $S = \operatorname{Spec} k$.

Lemma 2.23. *Any finite k-group scheme G with $F_{G/k} = 0$ is connected.*

Proof. There is a direct sum decomposition as k-vector spaces $\mathcal{O}_G(G) = k \oplus I$. Therefore $F_{G/k}$ factors through S if and only if the following diagram commutes:

$$\begin{tikzcd}
(k \oplus I) \otimes_{F_k} k \arrow[r, "(\lambda{,}b)\otimes 1 \mapsto (\lambda^p{,}b^p)"] \arrow[d, "(\lambda{,}b)\otimes 1 \mapsto \lambda^p"] & k \oplus I \\
k \arrow[r, "\mathrm{id}"] & k, \arrow[u, "\lambda \mapsto (\lambda{,}0)"']
\end{tikzcd}$$

which happens if and only if $I^p = (0)$. Let $\mathfrak{p} \subset \mathcal{O}_G(G)$ be a prime ideal. Then $(0) = I^p \subset \mathfrak{p}$, therefore $I \subset \mathfrak{p}$, hence $I = \mathfrak{p}$. □

In case $[G : k] = p$, the converse of Lemma 2.23 is true.

Lemma 2.24. *A finite k-group scheme G of order p is connected if and only if $F_{G/k} = 0$.*

Proof. Let $G^0 \subset G$ be the connected component of the identity $e \in G(k)$. Then G^0 is a subgroup scheme of G over k. The fppf-sheafification of the cokernel $T \mapsto G(T)/G^0(T)$ is representable by a k-scheme G/G^0 ([16, 5.1]). This quotient group scheme $G^{\mathrm{et}} = G/G^0$ is finite étale ([21, 3.7.I]), and $[G : k] = p = [G^0 : k][G^{\mathrm{et}} : k]$ ([21, 3.5]). In other words: $G = G^0$ or $G = G^{\mathrm{et}}$, so G is disconnected if and only if $G = G^{\mathrm{et}}$, if and only if G is étale, if and only if $F_{G/k}$ is invertible, if and only if $F_{G/k} \neq 0$. □

Lemma 2.24 implies that we can classify finite connected order p k-group schemes if and only if we can classify finite order p k-group schemes killed by their relative Frobenius. But the category of the latter is equivalent to M_k^1 by Theorem 2.13 and Remark 2.14, and the equivalence classes of M_k^1 are much easier to understand: this is linear algebra over k.

Lemma 2.25. *The set of isomorphism classes of finite connected order p group schemes over k is in bijection with $k/(k^*)^{p-1}$.*

Proof. By Theorem 2.13, Remark 2.14 and Lemma 2.24, we have to show that the set of isomorphism classes of one-dimensional Frobenius k-vector spaces is in bijection with the set $k/(k^*)^{p-1}$. Let $\gamma \in \mathrm{Ob}(\mathsf{M}_k^1)/\cong$ be an isomorphism class, and let $(M, \varphi) \in \gamma$ be a representative. We claim that choosing a basis $\{x\}$ of M, and sending γ to the unique element $c \in k$ that satisfies $\varphi(x \otimes 1) = cx$, gives a well-defined bijective map

$$f : \mathrm{Ob}(\mathsf{M}_k^1)/\cong \quad \to \quad k/(k^*)^{p-1}.$$

Another basis $\{y\}$ of M gives another element $d \in k$ with $\varphi(y \otimes 1) = dy \in k$, but as $y = \lambda x$ for some $\lambda \in k^*$, we have $d\lambda x = \varphi(y \otimes 1) = \varphi(\lambda x \otimes 1) = \varphi(x \otimes \lambda^p) = \lambda^p cx$, so $d = \lambda^{p-1}c$. Let $(N, \psi) \in \gamma$ be another representative, choose a basis $\{y\}$ for N and let $d \in k$ be the element with $\psi(y \otimes 1) = dy$. If $g : M \to N$ defines the isomorphism, we must have $g(x) = \lambda y$ for some $\lambda \in k^*$. By Definition 2.9, the following diagram commutes:

$$\begin{tikzcd}
M \arrow[r, "g"] & N \\
M \otimes_{F_k} k \arrow[u, "\varphi"] \arrow[r, "g\otimes\mathrm{id}"] & N \otimes_{F_k} k. \arrow[u, "\psi"']
\end{tikzcd}$$

Therefore $\lambda^p dy = \psi(y \otimes \lambda^p) = \psi(g(x) \otimes 1) = g(\varphi(x \otimes 1)) = c\lambda y$, so again: $c = \lambda^{p-1}d$. Surjectivity of f is clear. For injectivity: if (M, φ) and (N, ψ) in $\mathrm{Ob}(\mathsf{M}_k^1)$ give rise to $c, d \in k$ such that $c = \lambda^{p-1}d$ for $\lambda \in k^*$, then $x \mapsto \lambda y$ defines $M \cong N$. □

We have thus been given a somewhat more concrete description of the isomorphism classes of the finite connected order p group schemes over k via Lemma 2.25. We shall finish Section 2.4 by giving an explicit description of an object in each of those classes.

Notation 2.26. For $c \in k$, define two finite k-group schemes H_c and G_c as follows:

$$H_c = \mathrm{Spec}\, k[x]/(x^p - cx) \subset \mathbb{G}_a, \qquad \text{and} \qquad G_c = H_c^D.$$

Proposition 2.27. *Every finite connected k-group scheme of order p is isomorphic to G_c for some $c \in k$.*

Proof. We can identify

$$\mathrm{Spec}\,\mathrm{Sym}(k)/(1^p - c \cdot 1) \cong \mathrm{Spec}\, k[x]/(x^p - cx) = H_c \subset \mathbb{G}_a\,.$$

The proposition follows from 2.13, 2.14, 2.24 and 2.25. □

By Proposition 2.27, starting with *any* finite connected order p group scheme over k, it is possible to obtain an explicit formula for the group law of an object in its isomorphism class. Namely, all that is left to do, is to dualise the object H_c for $c \in k$. Let this thus be our aim. Take any element c in k, and let A_c be the k-algebra $k[y]/(y^p)$ equipped with a comultiplication

$$\tilde{m}_c : A_c \to A_c \otimes_k A_c, \quad \tilde{m}_c(y) = y \otimes 1 + 1 \otimes y + \sum_{i=1}^{p-1} \frac{c}{(p-i)!i!} y^i \otimes y^{p-i}.$$

Define $\tilde{e}_c : A_c \to k$ by $\tilde{e}_c(y) = 0$, and $\widetilde{\mathrm{inv}}_c : A_c \to A_c$ by $\widetilde{\mathrm{inv}}_c(y) = -y$. One checks this makes $(A_c, \tilde{m}_c, \tilde{e}_c, \widetilde{\mathrm{inv}}_c)$ into a Hopf algebra over k.

Proposition 2.28. *We have $G_c \cong \operatorname{Spec} A_c$ as group schemes over k.*

Proof. We dualise the morphisms that define the Hopf algebra structure of $\mathcal{O}_{H_c}(H_c)$ to obtain the Hopf algebra structure of $\mathcal{O}_{G_c}(G_c)$. As a vector space we have

$$\mathcal{O}_{G_c}(G_c) = \mathrm{Hom}_{k\text{-}\mathsf{Mod}}(k[x]/(x^p - cx), k) = \oplus_{i=1}^{p-1} k \cdot \widehat{x^i}.$$

Here $\widehat{x^i}(x^j) = 1$ if $j = i$ and 0 else. Let $\tilde{m}$ be the comultiplication of $\mathcal{O}_{G_c}(G_c)$ and $\tilde{\Delta}$ the multiplication. For $a, b \in \mathcal{O}_{G_c}(G_c)$, we have

$$\tilde{\Delta}(a \otimes b)(x^k) = \sum_{i=0}^{k} \binom{k}{i} a(x^{k-i}) b(x^i).$$

We see that $\tilde{\Delta}(\widehat{x^n} \otimes \widehat{x^m})(x^k) = 0$ if $k \neq n + m$ and $\binom{n+m}{m} \widehat{x^n}(x^n) \widehat{x^m}(x^m) = \binom{n+m}{m}$ else. It follows that

$$\tilde{\Delta}(\widehat{x^n} \otimes \widehat{x^m}) = \binom{n+m}{m} \widehat{x^{n+m}}.$$

Therefore, $\mathcal{O}_{G_c}(G_c)$ is generated by $\hat{x}$. To obtain $\tilde{m}$ it thus suffices to determine its value on $\hat{x}$: we have

$$\tilde{m} : \mathcal{O}_{G_c}(G_c) \to \mathcal{O}_{G_c}(G_c) \otimes_k \mathcal{O}_{G_c}(G_c),$$

$$\tilde{m}(\hat{x}) = \sum_{i=0}^{p-1} \widehat{x^i} \otimes [x^j \mapsto \hat{x}(x^{i+j})] = \hat{x} \otimes \hat{1} + \hat{1} \otimes \hat{x} + c \cdot \sum_{i=1}^{p-1} \widehat{x^i} \otimes \widehat{x^{p-i}}.$$

As the equality $(\hat{x})^n = n!\widehat{x^n}$ holds for all $n \in \mathbb{Z}_{\geqslant 0}$, the map $\widehat{x^i} \mapsto (1/i!)y^i$ for $0 \leqslant i \leqslant p-1$ defines a k-algebra isomorphism $f : \mathcal{O}_{G_c}(G_c) \xrightarrow{\sim} A_c$. It remains to show that f is compatible with comultiplication. Indeed: the image of $\tilde{m}(\hat{x})$ under $f \otimes f$ is equal to

$$(f \otimes f \ \circ \tilde{m})(\hat{x}) = y \otimes 1 + 1 \otimes y + \sum_{i=1}^{p-1} \frac{c}{(p-i)!i!} y^i \otimes y^{p-i} = \tilde{m}_c(y) = \tilde{m}_c(f(\hat{x})).$$

□

Examples 2.29.

1. Let $c = 0$. It is immediate from the descriptions that
$$\operatorname{Spec} A_0 = H_0 = \alpha_p.$$
Proposition 2.28 gives an isomorphism $\alpha_p^D \cong \alpha_p$ - compare this to the one in 1.11.2.

2. Let $c = 1$. We have $H_1 = \underline{\mathbb{Z}/p\mathbb{Z}}$, so $G_1 = \underline{\mathbb{Z}/p\mathbb{Z}}^D = \mu_p$ by Example 1.11.1. One can show that exp defines an isomorphism of k-group schemes between $\operatorname{Spec} A_1$ and $\mu_p = \operatorname{Spec} k[y]/(y^p - 1)$:
$$\exp : k[y]/(y^p - 1) \xrightarrow{\sim} k[y]/(y^p), \qquad \exp(y) = \sum_{i=0}^{p-1} \frac{y^i}{i!}.$$

Remark 2.30. Over a separable closure k^{sep} of k, up to isomorphism the examples in 2.29 are the *only* examples of finite connected order p group schemes over k^{sep}. This is a consequence of Lemma 2.25. The group schemes in $\mathscr{G}r/k_1^{F=0}$ with $V_{G/k} = 0$ are all isomorphic to α_p, as group schemes over k. The group schemes in $\mathscr{G}r/k_1^{F=0}$ with $V_{G/k}$ an isomorphism become isomorphic to $\mu_{p,k^{\mathrm{sep}}}$ after base changing to k^{sep}. We can summarise this by saying that every finite connected order p group scheme over k is either α_p or a *twist* of μ_p.

3 Actions by finite locally free group schemes

In the first two chapters we have given a description of finite locally free group schemes in characteristic p killed by their relative Frobenius, in terms of Frobenius modules and restricted Lie algebras. In Section 3, we give necessary and sufficient conditions for the existence of actions of such group schemes G on any scheme X that is affine over the base S. To do so, we shall need to translate group scheme actions of G on X over S into restricted Lie algebra morphisms of $\mathscr{L}(G)$ into the sheaf of derivations on X over S.

3.1 Actions by group schemes

The notion of an action of a group scheme on a scheme is defined in the obvious way.

Definition 3.1. Let G be an S-group scheme and X an S-scheme. A morphism of S-schemes $\mu : G \times X \to X$ is called an *action of* G *on* X *over* S if for all S-schemes T the map $\mu(T) : G(T) \times X(T) = (G \times X)(T) \xrightarrow{\mu_*} X(T)$ is an action of the group $G(T)$ on the set $X(T)$. We call the pair (X, μ) a *G-scheme*, or a *scheme with G-action μ.*

As usual we will occasionally abbreviate a G-scheme (X, μ) to X, and simply call X a G-scheme or a scheme with G-action.

Remark 3.2. For an S-group scheme G and an S-scheme X, if G and X are affine over S, actions of a G on X over S correspond to $\mathcal{O}_S$-algebra maps $\mathcal{O}_X \to \mathcal{O}_G \otimes \mathcal{O}_X$ that give $\mathcal{O}_X$ the structure of an $\mathcal{O}_G$-comodule. If X is moreover finite over S, with S noetherian, they correspond to homomorphisms of S-group schemes $G \to \underline{\mathrm{Aut}}_{X/S}$: homomorphisms of G into the *automorphism group scheme* of X over S (see [2, 2.4.i] for example).

Definition 3.3. Let $f : X \to S$ be a morphism of schemes and suppose that X is equipped with an action μ of a group scheme G over S. We say that X is a *G-torsor over S* if it satisfies the following conditions:

1. The square

$$\begin{tikzcd} G \times_S X \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\mu"] & X \arrow[d] \\ X \arrow[r] & S \end{tikzcd}$$

   is cartesian.

2. There is an fppf-morphism $S' \to S$ such that $X(S') \neq \varnothing$.

Remarks 3.4. 1. Condition 3.3.1 may be rephrased as follows: for any S-scheme T and any points $x, y \in X(T)$ we have $f(x) = f(y)$ if and only if there exists a unique $g \in G(T)$ such that $y = g \cdot x$. This is the scheme-theoretic version of the notion of principal bundle in topology.

2. The G-schemes over S form a category if we let a morphism between two G-schemes X and Y over S be a morphisms of S-schemes $X \to Y$ such that the following diagram commutes:

$$\begin{tikzcd} G \times_S X \arrow[r, "\mu"] \arrow[d, "\mathrm{id} \times h"'] & X \arrow[d, "h"] \\ G \times_S Y \arrow[r, "\mu"] & Y. \end{tikzcd}$$

   Similar to 3.4.1 this condition is equivalent to the condition that $h(g \cdot x) = g \cdot h(x)$ on T-valued points. The G-torsors over S form then a full subcategory of the category of S-schemes with G-action. It follows from 3.3.1 that every morphism in this category is an isomorphism: the category of G-torsors over S is a groupoid.

3. A G-torsor X is called a *trivial torsor* if it is isomorphic to G acting by multiplication on itself. In this case $X(S) \neq \emptyset$. Conversely, if X is a G-torsor and $X(S) \neq \emptyset$, then the G-action induces a morphism $G \to X$ of G-torsors and thus X is trivial. We can thus read condition 3.3.2 as saying that after an fppf base change every G-torsor X is trivial.

As outlined in Remark 3.4.1, torsors under group schemes are analogs of principle bundles in topology, and in algebraic geometry they are important for questions of descent. Torsors can also be used to find rational points, or give obstructions to local-global principles in this search. We give more examples of where they come up.

Examples 3.5.

1. Let K be a perfect field, and C a geometrically integral smooth projective curve over K of genus 1. The Jacobian $Jac(C)$ over C is an abelian variety of dimension 1, hence an elliptic curve over K, equipped with a natural action on C over K that makes C a $Jac(C)$-torsor. In fact, for every elliptic curve E/K acting on C over K making C into an E-torsor, $E = Jac(C)$. In other words, C is an E-torsor if and only if E is canonically isomorphic to the Jacobian of C (see [18, X, 3.8]).

2. If X is a G-torsor, then any morphism of schemes $T \to S$ makes X_T a G_T-torsor.

3. If S is a variety over $\bar{k}$ and $n \in \mathbb{Z}_{\geqslant 0}$, S-torsors X under the projective linear group $\mathrm{PGL}_n = \mathrm{Aut}(\mathbb{P}^n)$ are in bijection with $\mathbb{P}^n$-bundles (see [10, 7&8]).

4. Let $S = \operatorname{Spec} k$ and let L/k be a finite Galois extension of fields. There is a natural action of $\underline{\mathrm{Gal}(L/k)}$ on $\operatorname{Spec} L$ over k that makes $\operatorname{Spec} L$ into a $\underline{\mathrm{Gal}(L/k)}$-torsor .

5. More generally, let $X \to S$ be an étale Galois covering with Galois group G. Then X is a G-torsor over S: we have $X \times_S X \cong X \bigsqcup \ldots \bigsqcup X = \underline{G} \times_S X$.

6. $\operatorname{Spec} R[x]/(x^p - \lambda)$ is an α_p and μ_p-torsor over R, for $\lambda \in R$ and $\mathrm{char}(R) = p$.

7. In particular, if L/k is any inseparable field extension of degree p, then $\operatorname{Spec} L$ is a torsor under both α_p and μ_p. We will conjecture later in this thesis that this is a special case of a general phenomenon: we expect that any degree p inseparable extension of k is a torsor under any finite connected k-group scheme of order p.

3.2 Actions by Frobenius modules

Let $X = \operatorname{Spec} \mathcal{O}_X$ be a scheme, affine over S, and let G an object in $\mathscr{G}r/S^{F=0}$. The restricted Lie algebra structure on $\mathscr{L}(G)$ from 2.20 gives us a recipe to obtain an action of G on X over S. Recall that $\mathscr{D}er_{X/S}$ is a restricted $\mathcal{O}_S$-Lie algebra by Example 2.17.2.

Definition 3.6. Let $\mathfrak{g}$ be a sheaf of restricted Lie algebras over $\mathcal{O}_S$. An *action of* $\mathfrak{g}$ *on* X *over* S is a morphism of restricted $\mathcal{O}_S$-Lie algebras $\mathfrak{g} \to \mathscr{D}er_{X/S}$.

By Definition 2.18, an action of $\mathscr{L}(G)$ on X over S is thus an $\mathcal{O}_S$-linear map $\mathscr{L}(G) \to \mathscr{D}er_{X/S}, \alpha \mapsto D_\alpha$ compatible with the bracket and p-operation: for any $\alpha, \beta \in \mathscr{L}(G)$ we should have $D_{[\alpha,\beta]} = [D_\alpha, D_\beta]$ and $D_{\alpha^p} = D_\alpha^p$. However, recall that the bracket on $\mathscr{L}(G)$ is trivial by Proposition 2.21, and so the first condition means that $[D_1, D_2] = 0$ for each D_1, D_2 in the image of $\mathscr{L}(G) \to \mathscr{D}er_{X/S}$. If X affine is over S, we claim that actions of $\mathscr{L}(G)$ on X over S correspond to actions of G on X over S.

Theorem 3.7. *Let $G = \operatorname{Spec} \mathcal{A}$ be an object in $\mathscr{G}r/S^{F=0}$, and let $X = \operatorname{Spec} \mathcal{O}_X$ be a scheme that is affine over S. The set of group scheme actions of G on X over S is in bijection with the set of restricted Lie algebra actions of $\mathscr{L}(G)$ on X over S.*

Proof. Denote by $(\mathscr{L}, \varphi) = (\mathscr{L}(G), F_S^*\mathscr{L}(G) \xrightarrow{\varphi_G} \mathscr{L}(G))$ the Frobenius $\mathcal{O}_S$-module that G gives rise to. An action of $\mathscr{L}$ on X over S is an $\mathcal{O}_S$-linear map

$$\mathscr{L} \to \mathscr{D}er_{X/S}, \quad \alpha \mapsto D_\alpha, \tag{4}$$

$$\text{such that} \quad [D_\alpha, D_\beta] = 0 \quad \text{and} \quad D_{\alpha^p} = D_\alpha^p \quad \text{for all} \quad \alpha, \beta \in \mathscr{L}.$$

As $\mathscr{D}er_{X/S} \subset (\mathscr{E}nd_{\mathcal{O}_S}\mathcal{O}_X)'$, this induces a morphism of restricted $\mathcal{O}_S$-Lie algebras

$$\mathscr{L} \to (\mathscr{E}nd_{\mathcal{O}_S}\mathcal{O}_X)'.$$

Then firstly because $\mathscr{L} = \mathscr{P}rim(G^D)$ by the proof of Proposition 2.12, secondly by the universal property of the restricted enveloping algebra as in Definition 2.19, and thirdly because $U(\mathscr{L}) = \mathcal{A}(\mathscr{L}, \varphi) = \mathcal{A}^D$ by 2.20 and 2.21, to give (4) is to give a morphism of $\mathcal{O}_S$-algebras

$$D : \mathcal{A}^D \to \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X) \tag{5}$$

such that the following diagram commutes:

$$\begin{tikzcd}
\mathscr{L} \arrow[d, equal] \arrow[rd] & \\
\mathscr{P}rim(G^D) \arrow[r] \arrow[d, hook] & \mathscr{D}er_{X/S} \arrow[d, hook] \\
\mathcal{A}^D \arrow[r, "D"] & \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X).
\end{tikzcd} \tag{6}$$

To give (5) is to give a map

$$\bar{D} : \mathcal{A}^D \otimes \mathcal{O}_X \to \mathcal{O}_X\,. \tag{7}$$

We have $\mathscr{H}om_{\mathcal{O}_S}(\mathcal{A}^D \otimes \mathcal{O}_X, \mathcal{O}_X) = \mathscr{H}om_{\mathcal{O}_S}(\mathcal{O}_X, \mathscr{H}om_{\mathcal{O}_S}(\mathcal{A}^D, \mathcal{O}_X))$ by the tensor-hom adjunction, and there is a canonical morphism of $\mathcal{O}_S$-modules

$$f : \mathscr{H}om_{\mathcal{O}_S}(\mathcal{A}^D, \mathcal{O}_S) \otimes \mathcal{O}_X \to \mathscr{H}om_{\mathcal{O}_S}(\mathcal{A}^D, \mathcal{O}_X), \quad f(\varphi \otimes x)(\alpha) = x \cdot \varphi(\alpha),$$

which is an isomorphism because $\mathcal{A}^D$ is finite locally free. Because $\mathscr{H}om_{\mathcal{O}_S}(\mathcal{A}^D, \mathcal{O}_S) = \mathcal{A}$ this implies that $\mathscr{H}om_{\mathcal{O}_S}(\mathcal{A}^D \otimes \mathcal{O}_X, \mathcal{O}_X) = \mathscr{H}om_{\mathcal{O}_S}(\mathcal{O}_X, \mathcal{A} \otimes \mathcal{O}_X)$. Therefore, to give (7) is equivalent to giving a morphism of $\mathcal{O}_S$-modules

$$\tilde{\mu} : \mathcal{O}_X \to \mathcal{A} \otimes \mathcal{O}_X \,. \tag{8}$$

We claim that the following are true:

1. The map D in (5) is a morphism of $\mathcal{O}_S$-algebras if and only if the map $\tilde{\mu}$ in (8) gives $\mathcal{O}_X$ the structure of an $\mathcal{A}$-comodule.

2. The map D in (5) makes diagram (6) commute if and only if the map $\tilde{\mu}$ in (8) is a morphism of $\mathcal{O}_S$-algebras.

This claim would finish the proof by Remark 3.2. We start with Claim 1: consider the following diagrams:

$$\begin{tikzcd}
\mathcal{A}^D \otimes \mathcal{O}_X \arrow[d, "\bar{D}"'] & \mathcal{O}_S \otimes \mathcal{O}_X \arrow[l, "\tilde{e}^* \otimes \mathrm{id}"'] \arrow[d, equal] & \mathcal{A}^D \otimes \mathcal{O}_X \arrow[d, "\bar{D}"'] & \mathcal{A}^D \otimes \mathcal{A}^D \otimes \mathcal{O}_X \arrow[l, "\tilde{m}^* \otimes \mathrm{id}"'] \arrow[d, "\mathrm{id} \otimes \bar{D}"] \\
\mathcal{O}_X & \mathcal{O}_X \arrow[l, "\mathrm{id}"'] & \mathcal{O}_X & \mathcal{A}^D \otimes \mathcal{O}_X \,. \arrow[l, "\bar{D}"']
\end{tikzcd} \tag{9}$$

Left diagram (9) commutes if and only if $\bar{D}(\tilde{e} \otimes x) = D(\tilde{e})(x) = x$ for all $x \in \mathcal{O}_X$, which is equivalent to $D(\tilde{e}) = \mathrm{id}$. Right diagram (9) commutes if and only if for all $\alpha, \beta \in \mathcal{A}^D$ and all $x \in \mathcal{O}_X$ one has $\bar{D}(\alpha \otimes \bar{D}(\beta \otimes x)) = \bar{D}(\alpha \otimes D(\beta)(x)) = D(\alpha)(D(\beta)(x)) = D(\alpha\beta)(x)$, which is true if and only if $D(\alpha\beta) = D(\alpha)D(\beta)$ for all $\alpha, \beta \in \mathcal{A}^D$. Therefore, the map D in (5) is a morphism of $\mathcal{O}_S$-algebras if and only if diagrams (9) commute - but this is equivalent to the commutativity of their dual diagrams:

$$\begin{tikzcd}
\mathcal{A} \otimes \mathcal{O}_X \arrow[r, "\tilde{e} \otimes \mathrm{id}"] & \mathcal{O}_S \otimes \mathcal{O}_X & \mathcal{A} \otimes \mathcal{O}_X \arrow[r, "\tilde{m} \otimes \mathrm{id}"] & \mathcal{A} \otimes \mathcal{A} \otimes \mathcal{O}_X \\
\mathcal{O}_X \arrow[u, "\tilde{\mu}"] \arrow[r, "\mathrm{id}"] & \mathcal{O}_X \arrow[u, equal] & \mathcal{O}_X \arrow[u, "\tilde{\mu}"] \arrow[r, "\tilde{\mu}"] & \mathcal{A} \otimes \mathcal{O}_X \,. \arrow[u, "\mathrm{id} \otimes \tilde{\mu}"']
\end{tikzcd} \tag{10}$$

This proves Claim 1.

We can now prove Claim 2 under the assumption that $D(\tilde{e}) = \mathrm{id}$. Define

$$\widehat{D \otimes D} : \mathcal{A}^D \otimes \mathcal{A}^D \to \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X \otimes \mathcal{O}_X), \quad \widehat{D \otimes D}(\alpha \otimes \beta)(x \otimes y) = D(\alpha)(x) \otimes D(\beta)(y).$$

We denote by $\mathrm{mult} = \tilde{\Delta}_X : \mathcal{O}_X \otimes \mathcal{O}_X \to \mathcal{O}_X$ the multiplication morphism, where $\Delta_X : X \to X \times_S X$ is the diagonal of X over S. Observe that each $\alpha \in \mathscr{P}rim(G^D)$ and $x, y \in \mathcal{O}_X$, we have

$$\begin{aligned}(\mathrm{mult} \circ \widehat{D \otimes D} \circ \tilde{\Delta}^*(\alpha))(x \otimes y) &= (\mathrm{mult} \circ (\widehat{D \otimes D}))(\alpha \otimes \tilde{e} + \tilde{e} \otimes \alpha)(x \otimes y) \\ = \mathrm{mult}(D(\alpha)(x) \otimes y) &+ \mathrm{mult}(x \otimes D(\alpha)(y)) = yD(\alpha)(x) + xD(\alpha)(y).\end{aligned}$$

Therefore $D(\alpha)(xy) = yD(\alpha)(x) + xD(\alpha)(y)$ for all $x, y \in \mathcal{O}_X$ if and only if

$$D(\alpha) \circ \mathrm{mult} = \mathrm{mult} \circ \widehat{D \otimes D} \circ \tilde{\Delta}(\alpha) : \mathcal{O}_X \otimes \mathcal{O}_X \to \mathcal{O}_X \,.$$

In other words, the map D in (5) makes diagram (6) commute if and only if diagram (11) commutes:

$$\begin{tikzcd}
\mathcal{A}^D \otimes \mathcal{A}^D \arrow[r, "\widehat{D\otimes D}"] & \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X \otimes \mathcal{O}_X) \arrow[r, "\mathrm{mult}_*"] & \mathscr{H}om_{\mathcal{O}_S}(\mathcal{O}_X \otimes \mathcal{O}_X, \mathcal{O}_X) \\
\mathscr{P}rim(G^D) \arrow[u, "\tilde{\Delta}^*"] \arrow[rr, "D"] & & \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X). \arrow[u, "\mathrm{mult}^*"']
\end{tikzcd} \tag{11}$$

Because $\mathscr{P}rim(G^D)$ generates $\mathcal{A}^D$ as $\mathcal{O}_S$-algebra this is equivalent to the commutativity of diagram (12):

$$\begin{tikzcd}
\mathcal{A}^D \otimes \mathcal{A}^D \arrow[r, "\widehat{D\otimes D}"] & \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X \otimes \mathcal{O}_X) \arrow[r, "\mathrm{mult}_*"] & \mathscr{H}om_{\mathcal{O}_S}(\mathcal{O}_X \otimes \mathcal{O}_X, \mathcal{O}_X) \\
\mathcal{A}^D \arrow[u, "\tilde{\Delta}^*"] \arrow[rr, "D"] & & \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X). \arrow[u, "\mathrm{mult}^*"']
\end{tikzcd} \tag{12}$$

Write $\widetilde{D \otimes D} = \mathrm{mult}_* \circ \widehat{D \otimes D} : \mathcal{A}^D \otimes \mathcal{A}^D \to \mathscr{H}om_{\mathcal{O}_S}(\mathcal{O}_X \otimes \mathcal{O}_X, \mathcal{O}_X)$. Then (12) becomes

$$\begin{tikzcd}
\mathcal{A}^D \otimes \mathcal{A}^D \arrow[r, "\widetilde{D\otimes D}"] & \mathscr{H}om_{\mathcal{O}_S}(\mathcal{O}_X \otimes \mathcal{O}_X, \mathcal{O}_X) \\
\mathcal{A}^D \arrow[u, "\tilde{\Delta}^*"] \arrow[r, "D"] & \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X). \arrow[u, "\mathrm{mult}^*"']
\end{tikzcd}$$

By tensor-hom adjunction we obtain the diagram

$$\begin{tikzcd}
& \mathcal{A}^D \otimes \mathcal{A}^D \otimes \mathcal{O}_X \otimes \mathcal{O}_X \arrow[r] & \mathcal{O}_X \arrow[dd, "\mathrm{id}"] \\
\mathcal{A}^D \otimes \mathcal{O}_X \otimes \mathcal{O}_X \arrow[ur, "\tilde{\Delta}^* \otimes \mathrm{id}"] \arrow[dr, "\mathrm{id} \otimes \mathrm{mult}"'] & & \\
& \mathcal{A}^D \otimes \mathcal{O}_X \arrow[r, "\bar{D}"] & \mathcal{O}_X,
\end{tikzcd}$$

which we rewrite as

$$\begin{tikzcd}
& \mathcal{A}^D \otimes \mathcal{A}^D \otimes \mathcal{O}_X \otimes \mathcal{O}_X \arrow[r, equal] & \mathcal{A}^D \otimes \mathcal{O}_X \otimes \mathcal{A}^D \otimes \mathcal{O}_X \arrow[r, "\bar{D} \otimes \bar{D}"] & \mathcal{O}_X \otimes \mathcal{O}_X \arrow[dd, "\mathrm{mult}"] \\
\mathcal{A}^D \otimes \mathcal{O}_X \otimes \mathcal{O}_X \arrow[ur, "\tilde{\Delta}^* \otimes \mathrm{id}"] \arrow[dr, "\mathrm{id} \otimes \mathrm{mult}"'] & & & \\
& \mathcal{A}^D \otimes \mathcal{O}_X \arrow[rr, "\bar{D}"] & & \mathcal{O}_X \,.
\end{tikzcd}$$

Again, by tensor-hom adjunction, this diagram commutes if and only if (13) does:

$$\begin{tikzcd}
& \mathcal{A} \otimes \mathcal{A} \otimes \mathcal{O}_X \otimes \mathcal{O}_X \arrow[dl, "\tilde{\Delta} \otimes \mathrm{id}"'] \arrow[dd, "\tilde{\Delta} \otimes \mathrm{mult}"] & \mathcal{O}_X \otimes \mathcal{O}_X \arrow[l, "\tilde{\mu} \otimes \tilde{\mu}"'] \arrow[dd, "\mathrm{mult}"] \\
\mathcal{A} \otimes \mathcal{O}_X \otimes \mathcal{O}_X \arrow[dr, "\mathrm{id} \otimes \mathrm{mult}"'] & & \\
& \mathcal{A} \otimes \mathcal{O}_X & \mathcal{O}_X \,. \arrow[l, "\tilde{\mu}"']
\end{tikzcd} \tag{13}$$

Because $\tilde{\Delta} \otimes \mathrm{mult} = \tilde{\Delta} \otimes \tilde{\Delta}_X = \tilde{\Delta}_{G_X}$, where $\Delta_{G_X} : G_X \to G_X \times_S G_X$ is the diagonal of $G \times_S X$ over S, diagram (13) commutes if and only if $\tilde{\mu}$ is a morphism of $\mathcal{O}_S$-algebras. Therefore, D in (5) makes (6) commute if and only if $\tilde{\mu}$ in (8) is a morphism of $\mathcal{O}_S$-algebras. This proves Claim 2, and thereby the theorem. Indeed, reversing the arrows in (8) and (10), replacing $\mathcal{A}$ by G, $\mathcal{O}_X$ by X, $\otimes$ by $\times$ and $\tilde{\mu}$ by μ, shows that to give a morphism of quasi-coherent $\mathcal{O}_S$-algebras (8) with commuting diagrams (10) is equivalent to giving a morphism of schemes over S

$$\mu : G \times X \to X$$

that defines an action of G on X over S. □

Corollary 3.8. *The bijection in Theorem 3.7 is given as follows: suppose $\mathscr{L}(G)$ acts on X over S via a morphism $\phi : \mathscr{L}(G) \to \mathscr{D}er_{X/S}$ that factors through $\mathcal{A}^D$ as follows:*

$$\begin{tikzcd}
\mathscr{L} \arrow[r, "\phi"] \arrow[d, hook] & \mathscr{D}er_{X/S} \arrow[d, hook] \\
\mathcal{A}^D \arrow[r, "D"] & \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{O}_X).
\end{tikzcd}$$

Then $\tilde{\mu} : \mathcal{O}_X \to \mathcal{A} \otimes \mathcal{O}_X$ is the morphism of $\mathcal{O}_S$-algebras defined locally as

$$\tilde{\mu}(s) = \sum_{i=1}^{p^r} e_i \otimes D(\hat{e_i})(s).$$

Here $\{e_i\}_{i=1}^{p^r}$ is a local basis for $\mathcal{A}$ as sheaf of $\mathcal{O}_S$-modules, and $\{\hat{e_i}\}_{i=1}^{p^r}$ the dual basis.

Proof. This is chasing through the bijections in the proof of Theorem 3.7. □

3.3 Examples

1. Consider the case $X = G = \operatorname{Spec}\mathcal{A} \in \operatorname{Ob}(\mathscr{G}r/S^{F=0})$. Under the bijection of Theorem 3.7, the action of $\mathscr{L}(G)$ on G over S, defined by the natural inclusion $\mathscr{L}(G) \hookrightarrow \mathscr{D}er_{G/S}$, corresponds to the natural action of G on G over S given by translation: one can show that both actions correspond to the same morphism $D : \mathcal{A}^D \to \mathscr{E}nd_{\mathcal{O}_S}(\mathcal{A})$.

2. Let $G = \operatorname{Spec}\mathcal{A}$ in $\mathscr{G}r/S_1^{F=0}$ and let X be a scheme, affine over S. Let

$$\phi : \mathscr{L}(G) \to \mathscr{D}er_{X/S}.$$

be an action of $\mathscr{L}(G)$ on X over S. Locally, we can give an explicit description of the comodule morphism $\tilde{\mu} : \mathcal{O}_X \to \mathcal{A} \otimes \mathcal{O}_X$ that corresponds to ϕ.

The sheaf $\mathscr{L}(G)$ is invertible by Remark 2.14. Let $U \subset S$ ben an open subset such that $\mathscr{L}(G)|_U$ is free of rank 1, and choose a basis $\{m\}$ for $\mathscr{L}(G)|_U$ over $\mathcal{O}_U$. As φ_G is defined as follows:

$$\varphi_G : \mathscr{L}(G)_U \otimes \mathcal{O}_U \to \mathscr{L}(G)_U, \quad m \otimes 1 \mapsto m^p,$$

we must have $m^p = cm$ for a section $c \in \mathcal{O}_U$. Under this choice of basis, Theorem 2.13 shows that

$$\mathcal{A}_U^D \cong \mathcal{O}_U[x]/(x^p - cx).$$

Let $\partial \in \mathscr{D}er_{X_U/U}$ be the image of m under ϕ. Proposition 2.28 provides the following isomorphism of $\mathcal{O}_U$-Hopf algebras between $(\mathcal{O}_U[x]/(x^p - cx))^D$ and $\mathcal{O}_U[y]/(y^p)$:

$$(\mathcal{O}_U[x]/(x^p - cx))^D \to \mathcal{O}_U[y]/(y^p), \quad \widehat{x^i} \mapsto \frac{y^i}{i!}.$$

Using Corollary 3.8 we conclude that if we restrict $\tilde{\mu}$ to the open $U \subset S$, it is defined as following:

$$\tilde{\mu} : \mathcal{O}_X\,|_U \to \mathcal{O}_U[y]/(y^p) \otimes \mathcal{O}_X\,|_U, \quad \tilde{\mu}(s) = \sum_{i=0}^{p-1} \frac{y^i}{i!} \otimes \partial^i(s).$$

We will see applications of this fact in the following section.

4 Inseparable extensions and finite group schemes with zero Frobenius

In this section we apply the results from the previous sections by setting $S = \operatorname{Spec} k$ and considering actions of finite k-group schemes G on finite purely inseparable field extensions L over k. If the exponent of L/k is equal to one, then there are two necessary conditions for the existence of an action of G on $\operatorname{Spec} L$ over k making it into a G-torsor: (1) G is killed by its relative Frobenius and (2) the order $[G : k]$ is equal to the degree of the field extension L/k. If both are equal to p, the results of Sections 1-3 can be applied to show how reasonable it is to assume these conditions are sufficient.

In this line of reasoning, we conjecture that for every inseparable field extension L/k of degree p, and every finite connected k-group scheme G of order p, there exists an action of G on $\operatorname{Spec} L$ over k making it into a torsor. Such an extension L/k is modular, which is why we provide some basic results on modular field extensions in Section 4.1. In the purely inseparable case, modular field extensions are tensor products of simple field extensions. In Section 4.2 we present our results in favour of the conjecture above, and we translate it to a number theoretical conjecture in Section 4.3.

4.1 Modular field extensions

The notion of modular for inseparable field extensions is the analogue of the notion of normal for separable field extensions. Modular field extensions thus naturally come up when wants to study the inseparable theory. An extension L/k is modular if L^{p^r} and k are linearly disjoint over $L^{p^r} \cap k$ for all $r > 0$. This definition is due to Sweedler. For example, separable extensions are modular. Sweedler's paper [20] was followed by a number of 'Galois theories' for purely inseparable extensions in which the 'Galois extensions' L/k are modular, such as [3] and [4]. The idea is to replace the Galois group by the truncated automorphism group scheme $G_t(L/k)$ of L over k ([4]). For instance, there is an inverse lattice bijection between the lattice of fields F with $k \subset F \subset L$ and L/F modular, and the lattice of certain truncated k-subgroup schemes $G \subset G_t(L/k)$. See [4] for details. Let us provide some results on modular field extensions in our context.

Recall that a purely inseparable field extension L/k is said to have *finite exponent* if there exists a positive integer n such that $x^{p^n} \in k$ for each $x \in L$, and that in that case, the smallest such n is called the *exponent* of L/k.

Proposition 4.1. *Let L be a purely inseparable field extension of k of finite exponent. The following are equivalent.*

(a) L is isomorphic to the tensor product over k of simple extensions of k.

(b) There are higher derivations of L over k relative to which k is the field of constants (see [20, 1] for a definition).

(c) L^{p^i} and k are linearly disjoint over their intersection for all positive i.

Proof. See [20, 1]. □

Definition 4.2. An arbitrary field extension L/k is called *modular* if it satisfies 4.1(c).

Examples 4.3.

1. Let L be a finite purely inseparable field extension of k of degree p^n and exponent one. Then $L^p = k$, so L^{p^i} and k are linearly disjoint over their intersection for all positive i, and L/k is modular. Indeed, as L has exponent one we have
$$L \cong k(\alpha_1) \otimes_k k(\alpha_2) \otimes \ldots \otimes k(\alpha_n).$$
Here $[k(\alpha_i) : k] = p$ for each i.

2. One may thus be led to believe that every finite purely inseparable field extension is modular, but this is not true. Let $K = k[X^p, Y^p, Z^{p^2}]$ and let $L = K[Z, XZ + Y]$. Then L has exponent 2 over K and Z^p is in the field of constants relative to all higher derivations of L over K by [13, p. 196, Ex. 6 (Weisfeld)]. Therefore L is not modular over K by Proposition 4.1.

Definition 4.4. Given a k-group scheme G and an action $\tilde{\mu} : L \to \mathcal{O}_G(G) \otimes L$ on a field extension L/k, we denote by L^G the intermediate field $k \subset L^G \subset L$ of elements α in L such that $\tilde{\mu}(\alpha) = 1 \otimes \alpha$.

Lemma 4.5. *An action of a finite group scheme G on a finite field extension L/k makes* $\operatorname{Spec} L$ *a G-torsor if and only if $L^G = k$ and $[G : k] = [L : k]$.*

Proof. See [4, 5.1]. □

Every Galois extension L/k is modular, and a torsor under the natural action of the constant group scheme associated to the Galois group $\operatorname{Gal}(L/k)$. In fact, a finite field extenion L/k is normal and separable if and only if it is a torsor under some constant k-group scheme. This fact has the following inseparable analogue.

Proposition 4.6. *The following are equivalent for a finite field extension $k \subsetneq L$.*

1. *L/k is purely inseparable of exponent one.*

2. *$L^G = k$ for some k-group scheme acting G on L/k with $F_{G/k} = 0$.*

3. *L/k is a torsor under α_p^n for some $n \geqslant 1$.*

Proof. This follows from [4, 2.2] and [4, 5.2]. □

Proposition 4.7. *Let G be a finite k-group scheme acting on a finite field extension L/k making* $\operatorname{Spec} L$ *into a G-torsor over k. Then G is killed by its relative Frobenius if and only if L/k is purely inseparable of exponent one.*

Proof. If $F_{G/k} = 0$ then L/k is purely inseparable of exponent one by Lemma 4.5 and Proposition 4.6. Conversely, suppose that L/k is purely inseparable of exponent one, with $[L : k] = p^n$ for some $n \geqslant 1$. Then $[G : k] = p^n$ by Lemma 4.5. Observe that

$$\mathcal{O}_{G_L}(G_L) = \mathcal{O}_G(G) \otimes_k L \cong L \otimes_k L \cong L[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p),$$

where the second isomorphism comes from the action of G on L over k. Denote this composite of maps by $f : \mathcal{O}_{G_L}(G_L) \xrightarrow{\sim} L[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$. Because faithfully flatness is stable under base change, the map $\phi : G_L \to G$ is faithfully flat and in particular surjective. This gives a surjective map

$$\operatorname{Spec} L[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p) \to G.$$

The topological space of G must be a point, and $\mathcal{O}_G(G)$ a local k-algebra, with no other prime ideals then the augmentation ideal $I \subset \mathcal{O}_G(G)$. This makes

$$g = f \circ \tilde{\phi} : \mathcal{O}_G(G) \to L[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$$

a local morphism of local rings. It follows that

$$g(I) \subset (x_1, \dots, x_n) \bmod (x_1^p, \dots, x_n^p),$$

hence $g(I^p) = 0$. But g is injective by flatness of $\mathcal{O}_G(G)$ over k, therefore $I^p = (0)$. □

Proposition 4.7 implies the following. Let G be a finite k-group scheme that acts on a finite purely inseparable field extension L/k of exponent one, such that $\operatorname{Spec} L$ is a G-torsor. Then $[G : k] = [L : k]$ and $F_{G/k} = 0$. We believe that if $[L : k] = [G : k] = p$, the converse statement is true.

Conjecture 4.8. *Let L/k be an inseparable degree p extension and G a k-group scheme.* $\operatorname{Spec} L$ *can be made into a G-torsor over k if and only if G is finite connected of order p.*

4.2 Torsors under finite connected group schemes of order p

Let L/k be an inseparable field extension of degree p. Let $X = \operatorname{Spec} L$ and let G be a k-group scheme. By Proposition 4.7, if one wants to prove Conjecture 4.8, it suffices to assume G is finite, connected, with $[G : k] = p$, and prove the existence of an action of G on X over k that makes X a G-torsor. Section 4.2 is devoted to the translation of that problem to a problem of number theoretic nature.

So assume indeed that $G \in \operatorname{Ob}(\mathcal{G}r/k^{F_1=0})$. For $c \in k$, recall that A_c is the Hopf algebra $k[y]/(y^p)$ with comultiplication

$$\tilde{m}_c : A_c \to A_c \otimes_k A_c, \quad \tilde{m}_c(y) = y \otimes 1 + 1 \otimes y + \sum_{i=1}^{p-1} \frac{c}{(p-i)!i!} y^i \otimes y^{p-i}.$$

Write $L(G) = \mathscr{L}(G)(\operatorname{Spec} k)$, which is a one-dimensional vector space by 2.14. Define $\operatorname{Der}_k(L)$ as

$$\operatorname{Der}_k(L) = \mathscr{D}er_{L/k}(\operatorname{Spec} L) = \{k\text{-derivations } \partial : L \to L\}.$$

Theorem 4.9. *Let G be a finite connected k-group scheme of order p. Let L/k be an inseparable field extension of degree p. Write $X = \operatorname{Spec} L$. Let $\{\alpha\}$ be a basis for the vector space $L(G)$ over k. Then $\alpha^p = c \cdot \alpha$ for some $c \in k$, and the following are true.*

1. *The following function is a bijection.*
$$\{\partial \in \mathrm{Der}_k(L) \text{ satisfying } \partial^p = c \cdot \partial\} \xrightarrow{\mu} \{\text{actions of } \operatorname{Spec} A_c \text{ on } X \text{ over } k\},$$
$$\widetilde{\mu(\partial)} : L \to A_c \otimes_k L, \quad \widetilde{\mu(\partial)}(r) = \sum_{i=0}^{p-1} \frac{y^i}{i!} \otimes \partial^i(r).$$
2. *Under the bijection of 4.9.1, non-zero derivations $\partial \in \mathrm{Der}_k(L)$ satisfying $\partial^p = c \cdot \partial$ correspond to actions of* $\operatorname{Spec} A_c$ *on X over k making X into a* $\operatorname{Spec} A_c$*-torsor.*
3. *For every non-zero $\partial \in \mathrm{Der}_k(L)$ satisfying $\partial^p = c\cdot\partial$, X can be made into a G-torsor.*

Proof. 1. This follows from Theorem 3.7 and Example 3.3.2.

2. Let $\partial \in \mathrm{Der}_k(L)$ such that $\partial^p = c\cdot\partial$. We have $L = k[x]/(x^p - a)$ for some $a \notin k^p$. By 4.9.1 there is an action of $\operatorname{Spec} A_c$ on X over k defined by the k-algebra morphism
$$\tilde{\mu} : L \to A_c \otimes L, \qquad \tilde{\mu}(x) = \sum_{i=0}^{p-1} \frac{y^i}{i!} \otimes \partial^i(x).$$
Write $H = \operatorname{Spec} A_c$. As $[H : k] = p$, Lemma 4.5 implies the following: if $L^H = k$, then X is a H-torsor. Observe that $k \subset L^H \subset L$, where $[L : k] = p$. Therefore $L^H = k$ or $L^H = L$, and so it suffices to show $x \notin L^H$. We have $A_c \otimes L \cong L[y]/(y^p)$, and the elements $1, y, \dots, y^{p-1}$ are a basis for $L[y]/(y^p)$ over L. In particular, they are linearly independent over L. Under this isomorphism, the map $\tilde{\mu}$ becomes
$$\tilde{\mu} : L \to L[y]/(y^p), \quad \tilde{\mu}(x) = x + \partial(x)y + \frac{\partial^2(x)}{2!}y^2 + ... + \frac{\partial^{p-1}(x)}{(p-1)!}y^{p-1}.$$
We have
$$\tilde{\mu}(x) = x \quad \text{ if and only if } \quad \partial(x)y + \frac{\partial^2(x)}{2!}y^2 + ... + \frac{\partial^{p-1}(x)}{(p-1)!}y^{p-1} = 0.$$
But this is false, because the y^i are linearly independent over L, and $\partial \neq 0$ if and only if $\partial(x) \neq 0$. Therefore $x \notin L^H$, which finishes the proof.

3. This is true by 4.9.2: we let G act on X over k via the isomorphism $G \cong \operatorname{Spec} A_c$ of Proposition 2.28.

□

Corollary 4.10. *If for every $a \in k \backslash k^p$ and every $c \in k$ there exists a non-zero k-derivation*
$$\partial : k[x]/(x^p - a) \to k[x]/(x^p - a) \quad \text{with} \quad \partial^p = c\partial,$$
then Conjecture 4.8 holds. □

For example, for $c = 0$ and $\partial = \frac{d}{dx}$ we have $\partial^p = c\partial$, and for $c = 1$ and $\partial = x\frac{d}{dx}$ we have $\partial^p = c\partial$. By Theorem 4.9, Conjecture 4.8 is true for $G = \alpha_p$ and $G = \mu_p$: they can act on $\operatorname{Spec} L$ over k making it into a G-torsor, for any degree p inseparable extension L/k.

4.3 A number theoretical conjecture

In Section 4.2 we have proved Corollary 4.10, which reduces Conjecture 4.8 to the problem of finding a non-zero derivation $\partial : L \to L$ that satisfies $\partial^p = c\partial$, for every degree p inseparable extension L/k, and every c in k. In Section 4.3 we provide a natural candidate ∂ that would satisfy the hypothesis of Corollary 4.10. The problem of proving that ∂ does in fact satisfy $\partial^p = c\partial$ seems to be harder than may appear at first sight.

Conjecture 4.11. *Let $a \in k\backslash k^p$ and $c \in k$. Then $\partial^p = c\partial$ for the k-linear derivation*

$$\partial : k[x]/(x^p - a) \to k[x]/(x^p - a) \quad \text{defined by} \quad \partial = (cx^{p-1} - 1)\frac{d}{dx}.$$

The following is true.

Proposition 4.12. *Conjecture 4.11 implies Conjecture 4.8.* □

Convention 4.13. In the remaining part of Section 4.3, we stick to the following notation: $a \in k\backslash k^p$, $L = k[x]/(x^p - a)$, $c \in k$ and $\partial = (cx^{p-1} - 1)d/dx$ as a derivation on L over k. Denote by D the k-linear derivation on $k[x]$ defined as $D = (cx^{p-1} - 1)d/dx$.

Remark 4.14. Computer calculations show that $\partial^p = c\partial$ for all primes p up to 2000.

We will show that $\partial^p = c\partial$ if and only if $D^p = cD$. For this we need to control the behaviour of D^n for increasing values of n.

Lemma 4.15. *We have $D(x) = (cx^{p-1} - 1)$, and for $n = 2, \ldots, p$, the following is true:*

$$D^n(x) = \sum_{\substack{1 \leqslant i,j \leqslant p \\ i+j=n+1}} \lambda_{i,j} c^i x^{ip-2i-j+2} \quad \in k[x], \tag{14}$$

with $\lambda_{i,j} \in k$ satisfying the recursion relation

$$\lambda_{i,j} = (4 - 2i - j)\lambda_{i-1,j} - (3 - 2i - j)\lambda_{i,j-1}, \quad \lambda_{1,1} = 1. \tag{15}$$

Proof. This follows by induction on n. □

Lemma 4.16. *Conjecture 4.11 is true if and only if $D^p = cD$.*

Proof. Lemma 4.15 implies that

$$D^p(x) = \sum_{i+j=p+1} \lambda_{i,j} c^i x^{ip-2i-j+2} \quad \text{in} \quad k[x]. \tag{16}$$

For $\partial^p(x) \in L$, we obtain

$$\partial^p(x) = \sum_{i+j=p+1} \lambda_{i,j} c^i a^{i-1} x^{p-2i-j+2} \quad \text{in} \quad L. \tag{17}$$

Note that we may assume that $c \neq 0$, because for $c = 0$, we have $D^p = 0$ as well as $\partial^p = 0$. Therefore, assume that $c \neq 0$. The elements $x^{ip-2i-j+2} \in k[x]$ for $1 \leqslant i, j \leqslant p$

such that $i + j = p + 1$, as appearing in sum (16), are linearly independent over k. As $c \neq 0$, this implies that $D^p(x) = cD(x)$ in $k[x]$ if and only if

$$\lambda_{p-j+1,j} = 0 \in k \quad \text{for} \quad j = 1, \dots, p-2, \quad \text{and} \quad \lambda_{2,p-1} = 1, \quad \lambda_{1,p} = -1 \in k. \tag{18}$$

But the elements $x^{p-2i-j+2} \in L$ for $1 \leqslant i, j \leqslant p$ such that $i + j = p + 1$, as appearing in sum (17), are still linearly independent over k, and $a \neq 0$. Hence $\partial^p(x) = c\partial(x)$ in L if and only if condition (18) holds. □

Proposition 4.17. *Conjecture 4.11 is true if and only if* $\lambda_{(p-2k+1)/2,2k} = 0$ *for the values* $k = 1, \dots, (p-3)/2$ *and* $p \geqslant 5$.

Proof. That Conjecture 4.11 is true for $p = 2$ and $p = 3$ is easy to check. We thus assume $p \geqslant 5$. It follows from recursion relation (15) in Lemma 4.15 that $\lambda_{1,p-1} = 1$, $\lambda_{1,p} = 1$, and

$$\lambda_{2,p-1} = (4 - 4 - (p-1))\lambda_{1,p-1} - (3 - 4 - (p-1))\lambda_{2,p-2} = \lambda_{1,p-1} = 1.$$

Therefore Conjecture 4.11 holds if and only if $\lambda_{p-j+1,j} = 0 \in k$ for $j = 3, \dots, p$. By Lemma 4.16, it thus suffices to show that the following conditions are equivalent:

1. $\lambda_{p-j+1,j} = 0$, for $j = 3, \dots, p$,
2. $\lambda_{(p-2k+1)/2,2k} = 0$, for $k = 1, \dots, (p-3)/2$.

Assume that condition 2 holds. We claim by induction on j that the following holds: $\lambda_{i,j} = 0$ for i, j with $j = 1, 2, \dots, p-2$ and $i \geqslant (p - j + 1)/2 + 3/4(1 + (-1)^{j+1})$.

So let $j = 1$. Then $\lambda_{i,1} = 0$ for $i = (p+3)/2$ by (15), using that $4 - 2i - j \equiv 0 \bmod p$ for $j = 1$ and $i = (p+3)/2$. This further implies $\lambda_{i,1} = 0$ for $i \geqslant (p+3)/2$, using (15) again.

Next, let $m \in \mathbb{Z}_{\geqslant 0}$, for some $1 \leqslant m \leqslant (p-3)/2$, and suppose that

$$\lambda_{i,2m-1} = 0, \quad \text{for all} \quad i \geqslant (p - (2m-1) + 4)/2. \tag{19}$$

We have $\lambda_{(p-2m+1)/2,2m} = 0$ by condition 2. Because for $i = (p - 2m + 3)/2$ we have $3 - 2i - 2m \equiv 0 \bmod p$, it follows that $\lambda_{(p-2m+3/2),2m} = 0$ by (15). Then (19) and (15) imply further that $\lambda_{i,2m} = 0$ for all $i \geqslant (p - 2m + 1)/2$.

Finally, let $m \in \mathbb{Z}$ with $1 \leqslant m \leqslant (p-3)/2$, and suppose that

$$\lambda_{i,2m} = 0, \quad \text{for all} \quad i \geqslant (p - 2m + 1)/2. \tag{20}$$

Because $\lambda_{i,2m} = 0$ for $i = (p - 2m + 3)/2$, and because $4 - 2i - (2m + 1) \equiv 0 \bmod p$ for $i = (p - 2m + 3)/2$, equation (15) implies that $\lambda_{(p-2m+3)/2,2m+1} = 0$. Then (20) and (15) imply further that $\lambda_{i,2m+1} = 0$ for all $i \geqslant (p - 2m + 3)/2$.

Conversely, suppose that condition 1 holds. Similarly, using (15), it follows by induction on j that $\lambda_{i,p-j-1} = 0$ for $j = 1, 2, \dots, p-2$ and $i \geqslant (j+2)/2 + 3/4(1 + (-1)^{j+1})$. □

We proceed to give an explicit formula for the $\lambda_{i,j}$ as in (14), for any $n \in \{1, \ldots, p\}$. To simplify notation, for $i, j \in \mathbb{Z}_{\geqslant 1}$, let $I(i,j) \subset \mathbb{Z}^{j-1}$ be the set consisting of all elements $(l_1, \ldots, l_{j-1})$ in $\mathbb{Z}^{j-1}$ that satisfy $1 \leqslant l_1 < l_2 < \ldots < l_{j-1} \leqslant i + j - 2$. Then

$$\lambda_{i,j} = (-1)^{i+1} \sum_{I(i,j)} \quad \prod_{1 \leqslant k \leqslant l_1} (2k-1) \prod_{l_1 < k \leqslant l_2} (2k-2) \cdots \prod_{l_{j-2} < k \leqslant l_{j-1}} (2k-(j-1)) \prod_{l_{j-1} < k \leqslant i+j-2} (2k-j)$$

$$= (-1)^{i+1} \sum_{I(i,j)} \prod_{1 \leqslant k \leqslant l_1} (2k-1) \prod_{2 \leqslant n \leqslant j-1,\, l_{n-1} < k \leqslant l_n} \prod (2k-n) \prod_{l_{j-1} < k \leqslant i+j-2} (2k-j). \qquad (\star)$$

Formula $(\star)$ can be checked by verifying initial condition and recursion relation (15). Let us simplify Formula $(\star)$ for $\lambda_{(p-2k+1)/2,2k}$ with $k \in \{1, \ldots, (p-3)/2\}$, and $p \geqslant 5$. First substitute $r = (p-2k-1)/2$. Then $\lambda_{(p-2k+1)/2,2k} = \lambda_{r+1,p-2r-1}$.

Proposition 4.18. *For $p \geqslant 5$ and $r = 1, \ldots, (p-3)/2$, we have*

$$\lambda_{r+1,p-2r-1} \equiv (-1)^r \sum_{\substack{1 < n_1 < n_2 < \ldots < n_r < p-1 \\ n_{m+1} - n_m \geqslant 2}} \frac{1}{n_1 \cdot n_2 \cdots n_r} \mod p.$$

Proof. For each $i, j \in \mathbb{Z}_{\geqslant 1}$ with $1 \leqslant i, j \leqslant p$, define $\tilde{\lambda}_{i,j} \in \mathbb{Z}$ as

$$\tilde{\lambda}_{i,j} = (-1)^{i+1} \sum_{I(i,j)} \prod_{1 \leqslant k \leqslant l_1} (2k-1) \prod_{2 \leqslant n \leqslant j-1,\, l_{n-1} < k \leqslant l_n} \prod (2k-n) \prod_{l_{j-1} < k \leqslant i+j-2} (2k-j) \quad \in \mathbb{Z}\,.$$

With this notation, we can write

$$\tilde{\lambda}_{r+1,p-2r-1} = \sum_{I(r+1,p-2r-1)} (-1)^r a(l_1, l_2, \ldots, l_{p-2r-2}), \qquad (21)$$

with

$$a(l_1, \ldots, l_{p-2r-2}) = \prod_{1 \leqslant k \leqslant l_1} (2k-1) \prod_{2 \leqslant n \leqslant p-2r-2,\, 1 \leqslant k \leqslant l_n,} \prod (2k-n) \prod_{l_{p-2r-2} < k \leqslant p-r-2} (2k-(p-2r-1)).$$

Each such $a(l_1, l_2, \ldots, l_{p-2r-2})$ can be written uniquely in the form $a(l_1, l_2, \ldots, l_{p-2r-2}) = (p-2)!/(n_1 \cdot n_2 \cdots n_r)$ for some $n_1, \ldots, n_r \in \mathbb{Z}_{\geqslant 0}$ such that $1 < n_1 < \ldots < n_r < p-1$, with $n_{m+1} - n_m \geqslant 2$ for each $m \in \{1, \ldots, r-1\}$. Conversely, let $n_1, \ldots, n_r \in \mathbb{Z}$ with $1 < n_1 < n_2 < \ldots < n_r < p-1$ and $n_{m+1} - n_m \geqslant 2$ for each $m = 1, \ldots, r-1$. Then $(p-2)!/(n_1 \cdot n_2 \cdots n_r) = a(l_1, l_2, \ldots, l_{p-2r-2})$ for a unique $(l_1, \ldots, l_{p-2r-2}) \in \mathbb{Z}^{p-2r-2}$, with $1 \leqslant l_1 < l_2 < \ldots < l_{p-2r-2} \leqslant p-r-2$. We conclude that

$$\tilde{\lambda}_{r+1,p-2r-1} = (-1)^r \sum_{\substack{1 < n_1 < n_2 < \ldots < n_r < p-1 \\ n_{m+1} - n_m \geqslant 2}} \frac{(p-2)!}{n_1 \cdot n_2 \cdots n_r} \quad \in \mathbb{Z}\,.$$

As $\lambda_{r+1,p-2r-1} \equiv \tilde{\lambda}_{r+1,p-2r-1} \mod p$, and $(p-2)! \equiv 1 \mod p$, this completes the proof. $\square$

Via Propositions 4.17 and 4.18, we have translated Conjecture 4.11 into a number-theoretic hypothesis, which we shall include here for completion.

Conjecture 4.19. *For every prime number $p \geqslant 5$, the following is true:*

$$\sum_{\substack{1<n_1<n_2<\ldots<n_r<p-1 \\ n_{m+1}-n_m \geqslant 2}} \frac{1}{n_1 \cdot n_2 \cdots n_r} \equiv 0 \mod p \qquad \text{for } r = 1, \ldots, \frac{p-3}{2}.$$

We can summarise the results obtained in Section 4.3 in the following proposition.

Proposition 4.20. *Conjecture 4.19 holds if and only if Conjecture 4.11 holds. In particular, Conjecture 4.19 implies Conjecture 4.8.* □

We shall finish Section 4.3 by presenting some results in favour of Conjecture 4.19.

Proposition 4.21. *Conjecture 4.19 holds for the odd values of r, and for $r = 2$ if $p \geqslant 7$.*

Proof. First suppose r is odd. Define a set $S \subset \mathbb{Z}^r$ as

$$S = \{(n_1, n_2, \ldots, n_r) \in \mathbb{Z}^r : 1 < n_1 < \ldots < n_r < p-1 \text{ and } n_{m+1}-n_m \geqslant 2 \text{ for } m = 1, \ldots, r-1\}.$$

Consider the map

$$\sigma : S \to S,$$
$$\sigma(n_1, n_2, \ldots, n_r) = ((p-n_r), (p-n_{r-1}), \ldots, (p-n_1)).$$

Remark that σ well-defined involution on S, and that $\sigma(x) \neq x$ for each $x \in S$. Indeed, $\sigma(n_1, n_2, \ldots, n_r) = (n_1, n_2, \ldots, n_r) \in S$ would imply that $n_{(r-1)/2} = p - n_{(r-1)/2}$, which contradicts the fact that p is prime. This gives a decomposition $S = S_1 \sqcup S_2$, with for each $x \in S$, $\sigma(x) \in S_2$ if and only if $x \in S_1$. But for such $(n_1, \ldots, n_r), (k_1, \ldots, k_r) \in S$ with $\sigma(n_1, \ldots, n_r) = (k_1, \ldots, k_r)$, one has $1/(n_1 \cdot n_2 \cdots n_r) + 1/(k_1 \cdot k_2 \cdots k_r) \equiv 0 \mod p$. Therefore

$$\sum_{\substack{1<n_1<n_2<\ldots<n_r<p-1 \\ n_{m+1}-n_m \geqslant 2}} \frac{1}{n_1 \cdot n_2 \cdots n_r} = \sum_{(n_1,\ldots,n_r)\in S_1} \frac{1}{n_1 \cdot n_2 \cdots n_r} + \sum_{(n_1,\ldots,n_r)\in S_2} \frac{1}{n_1 \cdot n_2 \cdots n_r} \equiv 0.$$

This finishes the proof of Conjecture 4.19 for r odd.

To prove the second claim, suppose $p \geqslant 7$. In the remaining, our index sets are subset of $\mathbb{Z}$ or $\mathbb{Z}^2$, whereas our equalities are equalities in $\mathbb{F}_p$. First of all, we have

$$2 \cdot \sum_{\substack{1<n<m<p-1 \\ m-n \geqslant 2}} \frac{1}{n \cdot m} = \sum_{\substack{1<n,m<p-1 \\ |m-n| \geqslant 2}} \frac{1}{n \cdot m} = \sum_{1<n,m<p-1} \frac{1}{n \cdot m} - \sum_{\substack{1<n,m<p-1 \\ |m-n| \leqslant 1}} \frac{1}{n \cdot m} = -\sum_{\substack{1<n,m<p-1 \\ |m-n| \leqslant 1}} \frac{1}{n \cdot m}.$$

Indeed:

$$\sum_{1<n,m<p-1} \frac{1}{n \cdot m} = \left(\sum_{\mathbb{F}_p\, 1<n<p-1} \frac{1}{n} \right)^2 = \left(\sum_{x \in \mathbb{F}_p^*} x^{-1} - 1 - \frac{1}{p-1} \right)^2 = \left(\sum_{x \in \mathbb{F}_p^*} x \right)^2 = 0.$$

Furthermore,

$$\sum_{\substack{1<n,m<p-1\\|m-n|\leqslant 1}} \frac{1}{n\cdot m} = \sum_{1<n<p-1} \frac{1}{n^2} + \sum_{\substack{1<n,m<p-1\\|m-n|=1}} \frac{1}{n\cdot m} = \sum_{1<n<p-1} \frac{1}{n^2} + 2\cdot \sum_{2\leqslant n\leqslant p-3} \frac{1}{n(n+1)}.$$

We have $\sum_{1<n<p-1} \frac{1}{n^2} = \sigma - 2$ where $\sigma = \sum_{\mathbb{F}_p^*} x^2$. Because $p>2$, the generator α of the cyclic group $\mathbb{F}_p^*$ satisfies $\alpha^2 \neq 1$. Observe that

$$\alpha^2\sigma = \alpha^2 \sum_{x\in\mathbb{F}_p^*} x^2 = \sum_{x\in\mathbb{F}_p^*} (\alpha x)^2 = \sum_{x\in(\mathbb{F}_p)^*} x^2 = \sigma.$$

We conclude that $(\alpha^2-1)\sigma = 0$, and because $\alpha^2 \neq 1$ and $\mathbb{F}_p$ is a field, we must have $\sigma = 0$. Therefore $\sum_{1<n<p-1} \frac{1}{n^2} = -2$. Finally, remark that

$$\sum_{2\leqslant n\leqslant p-3} \frac{1}{n(n+1)} = \sum_{1\leqslant n\leqslant p-2} \frac{1}{n(n+1)} - \frac{1}{1\cdot 2} - \frac{1}{(p-2)(p-1)} = \sum_{1\leqslant n\leqslant p-2} \frac{1}{n(n+1)} - 1,$$

with

$$\sum_{1\leqslant n\leqslant p-2} \frac{1}{n(n+1)} = \sum_{1\leqslant n\leqslant p-2} \left(\frac{1}{n} - \frac{1}{n+1}\right) = 2.$$

We conclude that

$$\sum_{\substack{1<n<m<p-1\\m-n\geqslant 2}} \frac{1}{n\cdot m} = -2^{-1} \sum_{\substack{1<n,m<p-1\\|m-n|\leqslant 1}} \frac{1}{n\cdot m} = -2^{-1}\left(-2 + 2\cdot \sum_{2\leqslant n\leqslant p-3} \frac{1}{n(n+1)}\right) = 0.$$

□

Popular summary

In mathematics, one often wants to describe a certain construction in the terminology of another construction. The two constructions can exist in seemingly very different mathematical worlds, or *categories* as we call them, and therefore the discovery of a relation between the two can often come as a surprise. And not only that: such relations can prove to be very useful! For example, the category of real matrices is equivalent to the category of finite dimensional real vector spaces, and the category of locally compact Hausdorff topological spaces is equivalent to the category of commutative C^*-algebras with unit. Take the first example: it tells us that the language of linear transformations between finite-dimensional real vector spaces is equivalent to the language of matrices. Therefore, we can translate problems of matrices to problems of vector spaces and back, using whatever description we find most convenient. Up to isomorphism, nothing is lost in the process. Category theory came up in the 1940's, and we use it in our proofs.

Let us make some definitions. Let G be an abelian group, X a set, and $p \geqslant 5$ a prime number. An *action* of G on X is a map of sets $\mu : G \times X \to X$ such that $\mu(g, \mu(h, x)) = \mu(gh, x)$ and $\mu(e, x) = x$ for all $g, h \in G$ and $x \in X$. Then X is a *torsor* under the action μ by G if for every $x, y \in X$ there exists a unique $g \in G$ such that $f(g, x) = y$. A *co-commutative Hopf algebra over* $\mathbb{F}_p(t)$ can be seen as a generalisation of an abelian group - informally, one could say that it is a $\mathbb{F}_p(t)$-algebra A satisfying the following condition: for every $\mathbb{F}_p(t)$-algebra R, the set of $\mathbb{F}_p(t)$-algebra morphisms $A \to R$ carries an abelian group structure, compatible with morphisms of $\mathbb{F}_p(t)$-algebras $R \to R'$. There is an analogue of the definition of a *Hopf algebra action* of A on an $\mathbb{F}_p(t)$-algebra B, and also of B being a *torsor under* A by such an action.

With these definitions in place, we can explain the aim of this thesis. We show that the category of finite co-commutative Hopf algebras over $\mathbb{F}_p(t)$ is equivalent to the category of finite dimensional $\mathbb{F}_p(t)$-vector spaces V that are equipped with a map $\varphi : V \to V$ satisfying $\varphi(\lambda x) = \lambda^p \varphi(x)$ for every $\lambda \in \mathbb{F}_p(t)$ and $x \in V$. We deduce that finite rank p co-commutative Hopf algebras (up to isomorphism) correspond to elements in $\mathbb{F}_p(t)$ (up to multiplication by non-zero elements in $\mathbb{F}_p(t)^{p-1}$). This allows us to prove the following statement. Let $c \in \mathbb{F}_p(t)$, and let $\partial : \mathbb{F}_p(t)[x] \to \mathbb{F}_p(t)[x]$ the $\mathbb{F}_p(t)$-linear map $\partial = (cx^{p-1} - 1)d/dx$. If the following is true:

$$\sum_{\substack{1<n_1<n_2<\ldots<n_r<p-1 \\ n_{m+1}-n_m \geqslant 2}} \frac{1}{n_1 \cdot n_2 \cdots n_r} \equiv 0 \mod p \qquad \text{for } r = 1, \ldots, \frac{p-3}{2}, \tag{22}$$

then the equality $\partial^p = c \cdot \partial$ would hold, and therefore $\mathbb{F}_p(t^{1/p})$ would be a torsor under every rank p co-commutative Hopf algebra over $\mathbb{F}_p(t)$. Can you prove that (22) is true?

References

[1] Bourbaki, N. (1972). *Groupes et algèbres de Lie, Chapitre 1.* Éléments de Mathématique. Springer Berlin Heidelberg New York, first édition.

[2] Brion, M. (2018). Notes on automorphism groups of projective varieties.

[3] Chase, S. U. (1972). On the automorphism scheme of a purely inseparable field extension.

[4] Chase, S. U. (1976). Infinitesimal group scheme actions on finite field extensions. *American Journal of Mathematics*, 98(2):441–480.

[5] de Jong, J. A. (1993). Finite locally free group schemes in characteristic *p*. *Inventiones mathematicae*, 114(1):89–137.

[6] Deligne, P. et Rapoport, M. (1972). Les schémas de modules de courbes elliptiques. *International Summer School on Modular Functions*, 1(1):189–192.

[7] Edixhoven, B., Geer, G. et Moonen, B. (1). *Abelian Varieties.* Preliminary version of the first chapters.

[8] Gortz, U. et Wedhorn, T. (2010). *Algebraic Geometry I.* Springer.

[9] Grothendieck, A. (1960). Technique de descente et théorèmes d'existence en géométrie algébrique. i. généralités. descente par morphismes fidèlement plats. *Séminaire N. Bourbaki*, 5(talk:190):299–327.

[10] Grothendieck, A. (1966). Le groupe de brauer : I. algèbres d'azumaya et interprétations diverses. *Séminaire N. Bourbaki*, 290(1):199–219.

[11] Grothendieck, A. et Demazure, M. (1971). *SGA 3, Schémas en Groupes.* Numéro 151, 152, 153 de Lecture Notes in Mathematics. Springer.

[12] Jacobson, N. (1941). Restricted lie algebras of characteristic *p*. *Transactions of the American Mathematical Society*, 50(1):15–25.

[13] Jacobson, N. (1994). *Lectures in Abstract Algebra, Vol. III.* The University Series. Van Nostrand, Princeton, first édition.

[14] Katz, N. M. et Mazur, B. (1985). *Arithmetic Moduli of Elliptic Curves. (AM-108).* 1. Princeton University Press, first édition.

[15] Poonen, B. (2017). *Rational points on varieties.* Graduate Studies in Mathematics; 186. American Mathematical Society.

[16] Raynaud, M. (1967). Passage au quotient par une relation d'équivalence plate. *Proceedings of a conference on local fields*, 1(1):78–85.

[17] Shen, M. (2018). Lecture notes on abelian varieties.

[18] Silverman, J. H. (1986). *The Arithmetic of Elliptic Curves*, volume 106 de *Graduate Texts in Mathematics*. Springer.

[19] Stacks Project Authors (2018). *Stacks Project*. `https://stacks.math.columbia.edu`.

[20] Sweedler, M. E. (1968). Structure of inseparable extensions. *Annals of Mathematics*, 87(3):401–410.

[21] Tate, J. (1997). Finite flat group schemes. *Modular Forms and Fermat's Last Theorem*, 1(1):121–154.

[22] Weil, A. (1956). The field of definition of a variety. *American Journal of Mathematics*, 78(3):509–524.