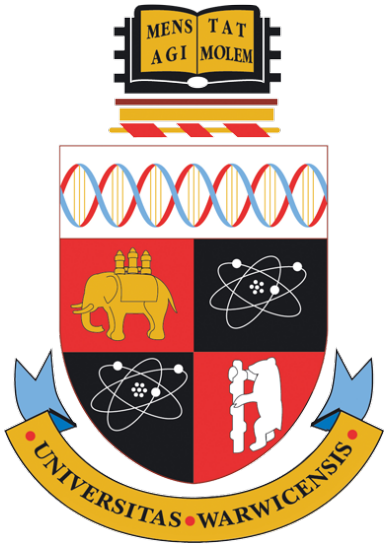
WARWICK
THE UNIVERSITY OF WARWICK



Families of group schemes of prime power order

by

Vladimir Eremichev

Thesis

Submitted to the University of Warwick

in partial fulfilment of the requirements

for admission to the degree of

Doctor of Philosophy

Department of Mathematics

March 2020

Contents

Acknowledgments

First of all, I would like to express my sincere gratitude to my research supervisor Professor Miles Reid for his advice, brilliance, encouragement, and sharing with me his immense knowledge and enthusiasm for algebraic geometry. I could not have imagined a better advisor and mentor for my Ph.D studies.

My sincere thanks also goes to Professor Gregory Sankaran, Professor Balázs Szendrői, and Professor Gavin Brown for helpful discussions. I would also like to thank Dr Marco Schlichting and Professor Diane Maclagan for their helpful comments on earlier drafts of this thesis.

A very special thank you to my examiners, Professor Nicholas Shepherd-Barron and Dr. Dmitriy Rumynin for conducting a most pleasant and enjoyable viva.

Finally, I wish to thank my family, and especially my wife Julia for her support and patience. I would not be here without you.

Declarations

I declare that, to the best of my knowledge, the material in this thesis is the original work of the author except where stated explicitly in the text.

The material in this thesis is submitted for the degree of Ph.D. to the University of Warwick only.

Abstract

In this thesis we study families of group schemes of prime power order, in particular, of order p^2. We show that these group schemes can be put into deformation families and we investigate the associated invariant theory, including actions and quotient varieties.

Preface

This thesis consists of four chapters. In Chapter 1 we recall the main aspects of finite flat group schemes over a ring and in particular the decomposition

$$G \cong G_{rr} \times G_{lr} \times G_{rl} \times G_{ll}, \tag{1}$$

for G a finite group scheme over a perfect field k. In Chapter 2 we study Dieudonné correspondences and use them to construct a parameter space for primitively generated finite group schemes. We also set up the Dieudonné correspondence which is used to classify local-local group schemes of prime power order in Chapter 3. Finally, in Chapter 4 we put group schemes in deformation families and consider their representation and invariant theory, with the goal towards constructing nonclassical Godeaux surfaces in positive characteristic.

Chapter 1

Group schemes

This chapter is a reminder of the basics of group schemes of prime power order and, in particular, the decomposition

$$G \simeq G_{\mathrm{rr}} \times_k G_{\mathrm{rl}} \times_k G_{\mathrm{lr}} \times_k G_{\mathrm{ll}}, \tag{1.1}$$

where G is an affine group scheme over a perfect field k. Our main references are [Wat79], [Pin], and [DG80].

1.1 Group schemes: definitions and main examples

In this section we will be working over a commutative base ring S which is not assumed to be a field.

Definition 1.1.1. An **affine group scheme** over S is a representable functor

$$G : \mathrm{Alg}_S \to \mathrm{Grp}, \tag{1.2}$$

from the category of S-algebras to the category of groups. The representing object A of G is called the **representing algebra** of G. All group schemes in this thesis are assumed to be commutative unless stated otherwise.

For an affine group scheme G there is, by definition, a natural transformation

$$G \simeq h_A. \tag{1.3}$$

The functor h_A is defined by

$$h_A : \mathrm{Alg}_S \to \mathrm{Grp}, \tag{1.4}$$

$$R \mapsto \mathrm{Hom}_S(A, R) \tag{1.5}$$

for some S-algebra A. Since G lands in the category of groups, there are natural transformations

$$m : G \times_S G \to G, \tag{1.6}$$

$$^{-1} : G \to G, \tag{1.7}$$

$$1 : \operatorname{Spec} S \to G, \tag{1.8}$$

corresponding to group multiplication, inversion, and identity element respectively. Taking the global sections functor, we see that the S-algebra A is equipped with the maps

$$\Delta : A \to A \otimes_S A, \tag{1.9}$$

$$S : A \to A, \tag{1.10}$$

$$\epsilon : A \to S, \tag{1.11}$$

called the **comultiplication**, the **antipode**, and the **augmentation** respectively, such that certain diagrams commute (see p.8 of [Wat79]). An S-algebra A with maps Δ, S, ϵ satisfying these conditions is called a **Hopf algebra** over S. Alternative names for Hopf algebras include commutative and cocommutative augmented algebras, bialgebras, bigebras with antipode etc.
A group scheme is called **commutative** if its essential image lies in the subcategory of commutative groups. Most of the group schemes we consider will be commutative, with the sole exception of Example 1.1.9.

Theorem 1.1.2. *[Wat79, 1.4 Theorem] There is an equivalence of categories*

$$\{\textit{Commutative affine group schemes over } \operatorname{Spec} S\} \simeq \{\textit{Hopf algebras over } S\}. \tag{1.12}$$

Just like it is enough to specify only a group law in order to define a group, it is enough to specify a comultiplication in order to define a Hopf algebra. This principle holds in greater generality by Yoneda lemma.

Example 1.1.3 (The additive group scheme)**.** The additive group scheme is defined as

$$\mathbb{G}_a : \operatorname{Alg}_S \to \operatorname{Grp}, \tag{1.13}$$

$$R \mapsto (R, +) \tag{1.14}$$

and is represented by $S[x]$. The comultiplication is

$$x \mapsto 1 \otimes x + x \otimes 1. \tag{1.15}$$

Example 1.1.4 (The multiplicative group scheme)**.** The multiplicative group scheme is defined as

$$\mathbb{G}_m : \mathrm{Alg}_S \to \mathrm{Grp}, \tag{1.16}$$

$$R \mapsto (R^*, \times). \tag{1.17}$$

This group scheme is represented by $S[x, x^{-1}] = S[x, y]/(xy - 1)$ with comultiplication

$$x \mapsto x \otimes x. \tag{1.18}$$

Definition 1.1.5. An S-group scheme G is called **finite** if its representing algebra is finite over S. The dimension of A over S is called the **order** of G.

Example 1.1.6 ($\boldsymbol{\alpha}_{p^n}$)**.** Let k be a field of positive characteristic p and n a positive integer. The group scheme $\boldsymbol{\alpha}_{p^n}$ is defined as

$$\boldsymbol{\alpha}_{p^n} : \mathrm{Alg}_k \to \mathrm{Grp}, \tag{1.19}$$

$$R \mapsto \{r \in R : r^{p^n} = 0\}. \tag{1.20}$$

This is an absolute *Frobenius kernel* of $\mathbb{G}_a$. Its representing algebra is $k[x]/(x^{p^n})$ with comultiplication

$$x \mapsto x \otimes 1 + 1 \otimes x. \tag{1.21}$$

It is clear that $\boldsymbol{\alpha}_{p^n}$ is a finite group scheme of order p^n.

Example 1.1.7 ($\boldsymbol{\mu}_{n,S}$)**.** The group scheme $\boldsymbol{\mu}_{n,S}$ is a Frobenius kernel of $\mathbb{G}_m$, namely,

$$\boldsymbol{\mu}_{n,S} : \mathrm{Alg}_S \to \mathrm{Grp}, \tag{1.22}$$

$$R \mapsto \{r \in R : r^n = 1\}. \tag{1.23}$$

Example 1.1.8 (Finite constant group schemes)**.** Let Γ be a finite group in a group-theoretic sense. Let $A = S^\Gamma = \mathrm{Hom}_{\mathrm{Set}}(\Gamma, S)$. For each $\sigma \in \Gamma$ define $e_\sigma \in A$ to be 1 on σ and 0 otherwise. Then $\{e_\sigma\}_{\sigma\in\Gamma}$ is an S-basis of A. The Hopf algebra structure on A is given by

$$\Delta(e_\sigma) = \sum_{\rho\tau=\sigma} e_\rho \otimes e_\tau. \tag{1.24}$$

Such a group scheme is denoted by $\underline{\Gamma}_S$ or just Γ if no confusion is likely to arise. We call such group schemes **finite constant group schemes**.

If Γ is a constant group scheme of order p^2 for p prime then it is either

$(\mathbb{Z}/p)^2$ or $\mathbb{Z}/p^2$ and is commutative in both cases. This is not the case for group schemes, as the following example shows.

Example 1.1.9 (A noncommutative group scheme of order p^2, A.3.6 in [Gor02])**.** Let k be a ring of characteristic p. Consider the functor

$$G : \mathrm{Alg}_k \to \mathrm{Grp}, \tag{1.25}$$

$$R \mapsto \left\{ \begin{pmatrix} m & a \\ 0 & 1 \end{pmatrix} : m \in \boldsymbol{\mu}_p(R), a \in \boldsymbol{\alpha}_p(R) \right\} \tag{1.26}$$

This is a subfunctor of GL_2. It is easy to see that this functor G is represented by $A = k[x, y]/(x^p - 1, y^p)$ with Hopf algebra structure induced from that of GL_2:

$$\boldsymbol{\mu} : A \otimes_k A \to A, \tag{1.27}$$

$$x \mapsto x \otimes x, \tag{1.28}$$

$$y \mapsto x \otimes y + y, \tag{1.29}$$

$$\epsilon : A \to k, \tag{1.30}$$

$$x \mapsto 1, \tag{1.31}$$

$$y \mapsto 0, \tag{1.32}$$

$$S : A \to A, \tag{1.33}$$

$$x \mapsto x^{-1}, \tag{1.34}$$

$$y \mapsto -x^{-1} \otimes y. \tag{1.35}$$

Let A, B be two matrices in $G(R)$ for some k-algebra R, i.e.,

$$A = \begin{pmatrix} m & a \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} n & b \\ 0 & 1 \end{pmatrix}. \tag{1.36}$$

Then, in general,

$$AB = \begin{pmatrix} mn & mb+a \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} mn & na+b \\ 0 & 1 \end{pmatrix} = BA, \tag{1.37}$$

since $mb + a \neq na + b$. This shows that G is not commutative. A basis of A is given by $\{x^i y^j\}_{0 \leq i,j \leq p-1}$, so the order is p^2.
Here is another way to look at G: $\boldsymbol{\mu}_p$ acts on $\boldsymbol{\alpha}_p$ by multiplication:

$$\boldsymbol{\mu}_p(R) \times \boldsymbol{\alpha}_p(R) \to \boldsymbol{\alpha}_p(R), \tag{1.38}$$

$$(m, a) \mapsto ma, \tag{1.39}$$

with $(ma)^p = 0$. This makes G into a *semidirect product* of $\boldsymbol{\alpha}_p$ and $\boldsymbol{\mu}_p$.

Definition 1.1.10. Let N, G be group schemes over a base S. Consider the automorphism functor of N

$$\mathrm{Aut}(N) : \mathrm{Sch}/S \to \mathrm{Grp}, \tag{1.40}$$

$$T \mapsto \mathrm{Aut}(N_T) \tag{1.41}$$

and an action of G on N

$$\rho : G \to \mathrm{Aut}(N). \tag{1.42}$$

The **semidirect product group scheme** $N \rtimes_\rho G$ is the representable functor

$$N \rtimes_\rho G : \mathrm{Sch}/S \to \mathrm{Grp}, \tag{1.43}$$

$$T \mapsto N(T) \rtimes_{\rho_T} G(T). \tag{1.44}$$

While we mostly work with finite flat group schemes over a field, where flatness is automatic, we will also work with finite flat group schemes over general rings. The kernel of a morphism of finite flat group schemes over a field is a finite flat group scheme. Moreover, the category of commutative finite group schemes over a field is abelian (see [Stacks, Lemma 03CN]). However, this does not hold over rings as the next example shows.

Example 1.1.11. Consider the group scheme

$$\mathrm{Alg}_{\mathbb{Z}} \to \mathrm{Grp}, \tag{1.45}$$

$$B \mapsto \{b \in B : b^2 = b\}, \tag{1.46}$$

i.e., the functor sending a ring to its set of idempotents. The group law is

$$(x, y) \mapsto x + y - 2xy = x(1 - y) + y(1 - x). \tag{1.47}$$

The reason for this composition law is that if x and y are idempotents in a commutative ring, then $xy, x(1-y), y(1-x)$, and $(1-x)(1-y)$ are orthogonal idempotents, so any sum of these is an idempotent as well. This functor is in fact represented by $\mathbb{Z}[x]/(x^2 - x)$, i.e., this is the constant group scheme $\mathbb{Z}/2$. Define the morphism

$$\mathbb{Z}/2 \to \boldsymbol{\mu}_2, \tag{1.48}$$

$$\mathbb{Z}/2(B) \to \boldsymbol{\mu}_2(B), \tag{1.49}$$

$$e \mapsto 1 - 2e. \tag{1.50}$$

The kernel of this morphism is represented by $\mathbb{Z}[x]/(x^2 - x, 2x)$, which is finite, but has torsion, to it cannot be a flat module.

1.2 Group schemes of rank two over a local ring

Classification of group schemes over general rings is quite difficult. We can get full results over low ranks. Let R be a commutative local ring. Following Tate and Oort ([Tat97] and [TO70]), we will show how to classify group schemes of order 2 over R. Let A be the representing Hopf algebra of such a group scheme. We have the short exact sequence

$$0 \to I \to A \xrightarrow{\epsilon} R \to 0, \tag{1.51}$$

which is split because R is projective over itself. More precisely, the splitting is given by the structure map $R \to A$. Recall that for any R-modules M, N there is a canonical isomorphism

$$\bigwedge^n M \oplus N \cong \bigoplus_{i+j=n} \bigwedge^i M \otimes \bigwedge^j N. \tag{1.52}$$

Now, A is an R-module of rank 2 by assumption. We have

$$0 = \bigwedge^3 A = \bigwedge^3 \ker \epsilon \oplus \bigwedge^2 \ker \epsilon, \tag{1.53}$$

which implies $\bigwedge^3 \ker\epsilon = \bigwedge^2 \ker\epsilon = 0$. It follows that

$$R = \bigwedge^2 A = \bigwedge^2 \ker\epsilon \oplus \bigwedge^1 \ker\epsilon = \bigwedge^1 \ker\epsilon = \ker\epsilon. \tag{1.54}$$

We have shown that for a group scheme of rank 2 the augmentation ideal has rank 1. This does not generalise: if $k \oplus I = k^n$ for $n \geq 3$ then $\ker\epsilon$ is not necessarily free, but it does hold over fields.
Now let $\{x\}$ be an R-basis of I, so that $I = Rx$. Then A is spanned by $\{1, x\}$, so $A \otimes A$ is spanned by $\{1\otimes 1, x\otimes 1, 1\otimes x, x\otimes x\}$. There exist scalars a_1, a_2, a_3, and b in R such that

$$\Delta(x) = a_1(1\otimes 1) + a_2(x\otimes 1) + a_3(1\otimes x) + b(x\otimes x). \tag{1.55}$$

In a Hopf algebra we must have

$$(\epsilon \otimes \mathrm{id}) \circ \Delta = \mathrm{id}_A\,. \tag{1.56}$$

Applying these to x we get

$$(\epsilon\otimes\mathrm{id})(a_1(1\otimes 1) + a_2(x\otimes 1) + a_3(1\otimes x) + b(x\otimes x)) = a_1 + a_2 x = x, \tag{1.57}$$

which implies $a_1 = 0$ and $a_2 = 1$. By symmetry, we must also have $a_3 = 1$. The comultiplication law is then

$$\Delta(x) = x\otimes 1 + 1\otimes x + b(x\otimes x). \tag{1.58}$$

The augmentation module I is an ideal, so $x^2 \in I$, which means that there is $a \in R$ such that $x^2 = -ax$ and $x^2 + ax = 0$. It follows that

$$A = R[X]/(X^2 + aX) \tag{1.59}$$

as R-algebras.
Let us now look at the antipode map. We have

$$S(x) = u + cx, \tag{1.60}$$

for $u, c \in R$. Note that

$$(S, \mathrm{id}) \circ \Delta = \epsilon, \tag{1.61}$$

which corresponds to $g \times g^{-1} = 1$ in abstract group theory. Applying both sides to x we get

$$u + cx + x + bux + bcx^2 = 0, \tag{1.62}$$

from which it follows that $u = 0$. Note that it is not possible to conclude that $c = -1$ from the above since $x^2 = ax$. We now know that $S(x) = cx$. But $S^2 = \mathrm{id}$, so $c^2 x = x$ and $c^2 = 1$. By expanding both sides of

$$\Delta(x^2) = \Delta(-ax), \tag{1.63}$$

we can show that $ab = 2$ (look at the coefficient of $x \otimes x$). From the above, we get

$$cx + x - bcax = 0, \tag{1.64}$$

i.e.,

$$c + 1 - abc = 0, \tag{1.65}$$

$$c + 1 - 2c = 0, \tag{1.66}$$

$$c = 1. \tag{1.67}$$

Conversely, given $a, b \in R$ with $ab = 2$, we can define the affine group scheme

$$G_{a,b}(A) = \{y \in A : y^2 + ay = 0\} \tag{1.68}$$

with the group operation

$$(y_1, y_2) \mapsto y_1 + y_2 + by_1y_2. \tag{1.69}$$

Define an equivalence relation on R^2 by declaring $(a_1, b_1) \sim (a_2, b_2)$ if and only if there is $u \in R^*$ such that $a_1 = ua_2$ and $b_1 = u^{-1}b_2$. Then

$$G_{a_1,b_1} \cong G_{a_2,b_2} \tag{1.70}$$

if and only if $(a_1, b_1) \sim (a_2, b_2)$. The Hopf algebra isomorphism is given by

$$G_{a_1,b_1} \to G_{a_2,b_2}, \tag{1.71}$$

$$x \mapsto ux \tag{1.72}$$

with the inverse

$$x \mapsto u^{-1}x. \tag{1.73}$$

Conversely, every isomorphism of Hopf algebras of rank 2 is of this form – for the proof it is crucial that $ab = 2$.
We have already seen examples of $G_{a,b}$. For example, if k is a field then we have $G_{1,2}$ corresponding to $k[x]/(x^2+x)$ which is $\mathbb{Z}/2$ and $G_{2,1} = k[x]/(x^2+1) = \boldsymbol{\mu}_2$.

Furthermore, if $0 = 2$ in k then $G_{0,0}$ is $\boldsymbol{\alpha}_2$. Cartier duality (see the next section) swaps a and b:

$$G_{a,b}^D = G_{b,a}. \tag{1.74}$$

1.3 Cartier duality for finite group schemes.

Let G be a commutative finite flat group scheme over S and let A be its representing algebra. The S-linear dual algebra of A

$$A^D := \mathrm{Hom}_S(A, S) \tag{1.75}$$

is also a Hopf algebra. Indeed, let m, S, i denote the multiplication, the antipode, and the S-algebra structure map for A. Then

$$m^D : A^D \to A^D \otimes_S A^D, \tag{1.76}$$
$$S^D : A^D \to A^D, \tag{1.77}$$
$$i^D : A^D \to S^D \simeq S \tag{1.78}$$
$$\tag{1.79}$$

give A the structure of a Hopf algebra. Let G^D be the group scheme corresponding to A^D. We call G^D the **Cartier dual** of G.

Theorem 1.3.1. *[Wat79, p. 17] The Cartier dual functor is a duality theory for the category of finite commutative group schemes, i.e., there is an isomorphism of functors*

$$\mathrm{id} \simeq (-)^{D^2}. \tag{1.80}$$

There is a duality pairing

$$G \times_S G^D \to \mathbb{G}_{m,S}, \tag{1.81}$$

$$(g, \phi) \mapsto \phi(g). \tag{1.82}$$

Furthermore, for any S-algebra B,

$$G^D(B) = \mathrm{Hom}_B(G_B, \mathbb{G}_{m,B}) \cong \mathrm{Hom}_B(B[T^{\pm 1}, A \otimes_S B]). \tag{1.83}$$

In other words, on the level of group schemes, the Cartier dual behaves like the Hom-sheaf $\mathcal{H}\mathrm{om}(-, \mathbb{G}_m)$ and this can be made precise by working in the fppf-topology (see Section 021L in [Stacks] and Chapter 5 of [Ols16]).

Example 1.3.2 ($\boldsymbol{\mu}_n \cong \mathbb{Z}/n^D$)**.** The dual of $\boldsymbol{\mu}_n$ is represented by

$$\mathrm{Hom}_S(S[t^{\pm 1}, S[x]/(x^n - 1)]). \tag{1.84}$$

Take $\phi : S[t^{\pm 1}] \to S[x]/(x^n - 1)]$ and let $\phi(t) = p(x) = \sum_{i=0}^{n-1} a_i x^i$. Note that $p(fg) = p(f)p(g)$ for f, g polynomials, so

$$\sum a_i (fg)^i \equiv \sum a_i (f)^i \sum a_i (g)^i \mod (f^n - 1, g^n - 1). \tag{1.85}$$

Comparing the terms above we see $a_i a_j = 0$ if $i \neq j$ and $a_i^2 = 1$. Also note that $\sum a_i = 1$, so the a_i are orthogonal idempotents. Each a_i corresponds to a point in $\mathbb{Z}/n$, the constant group scheme with base S, which is the Cartier dual of $\boldsymbol{\mu}_n$.

We can also see the duality in more explicit terms. The constant group scheme $\mathbb{Z}/n$ has an S-basis $\{e_0, ..., e_{p-1}\}$ with maps

$$\Delta : e_i \mapsto \sum_{j+k=i} e_j \otimes e_k, \tag{1.86}$$

$$\epsilon : e_0 \mapsto 1, e_{i\neq 0} \mapsto 0, \tag{1.87}$$

$$S : e_i \mapsto e_{-i}, \tag{1.88}$$

$$i : s \mapsto s, \tag{1.89}$$

$$\nabla : e_i \otimes e_j \mapsto \delta_{i,j} e_i. \tag{1.90}$$

Let the dual group scheme $\mathbb{Z}/n^D$ have the dual basis $\{e^0, ..., e^{p-1}\}$, with maps

$$\nabla^D : e^i \mapsto e^i \otimes e^i, \tag{1.91}$$

$$i^D : e^i \mapsto 1, \tag{1.92}$$

$$S^D : e^i \mapsto e^{-i}, \tag{1.93}$$

$$\epsilon^D : s \mapsto s, \tag{1.94}$$

$$\Delta^D : e^i \otimes e^j \mapsto e^{i+j}, \tag{1.95}$$

which are the maps defining the Hopf algebra structure on $S[x]/(x^n - 1)$, the representing algebra of $\boldsymbol{\mu}_{n,S}$.

Now assume S has positive characteristic p. We can write down the Cartier pairing for the pair $(\boldsymbol{\mu}_p, \mathbb{Z}/p)$. It is a function

$$S[t^{\pm 1}] \to S[x]/(x^p - x) \otimes_S S[y]/(y^p - 1), \tag{1.96}$$

where $S[x]/(x^p - x)$ represents $\mathbb{Z}/p$. Let $\{1, x, ..., x^{p-1}\}$ be an S-basis of $S[x]/(x^p - 1)$ and let $f_0, ..., f_{p-1}$ be its dual basis. Then

$$f_i = \frac{f_1^i}{i!}. \tag{1.97}$$

Denote by $\exp_p$ the truncated exponential

$$\exp_p(a) = 1 + a + \frac{a^2}{2} + ... + \frac{a^{p-1}}{(p-1)!}. \tag{1.98}$$

Hence $y = \exp_p(f_1)$. The Cartier pairing is

$$S[t^{\pm 1}] \to S[x]/(x^p - x) \otimes_S S[y]/(y^p - 1), \tag{1.99}$$

$$t \mapsto \exp_p(x \otimes \log(y)). \tag{1.100}$$

Example 1.3.3. The additive finite group scheme $\boldsymbol{\alpha}_p$ is self-dual: $\boldsymbol{\alpha}_p^D \cong \boldsymbol{\alpha}_p$, with the dual basis given by divided powers.

1.4 The canonical decomposition

In this section we will recall how every finite commutative algebraic group over a perfect field admits a canonical decomposition as a direct sum of four components. For the more precise statement, see Prop 1.4.8.
Let $G = \operatorname{Spec} A$ be a finite commutative algebraic group scheme and $T_{G,0}$ the Zariski tangent space at the origin. The point $0 \in G$ is the image of $\operatorname{Spec} k \to G$ which comes from the counit Hopf algebra map $\epsilon : A \to k$.

Proposition 1.4.1. *There is an isomorphism of k-vector spaces*

$$T_{G,0} \cong \operatorname{Hom}(G^D, \mathbb{G}_a), \tag{1.101}$$

where the k-action on the right hand side is induced from the k-action of $\mathbb{G}_a$.

Proof. The tangent space $T_{G,0}$ is naturally isomorphic to the kernel of the map

$$G(k[t]/(t^2)) \to G(k). \tag{1.102}$$

This corresponds to the kernel of the restriction map of k-algebras

$$\operatorname{Hom}(A, k[t]/(t^2)) \to \operatorname{Hom}(A, k). \tag{1.103}$$

A map $f : A \to k[t]/(t^2) = k \oplus tk$ has two components and the first component has to be the counit map. So $f = \epsilon + t\lambda$, where $\lambda : A \to k$ is a linear map. Define

$$\widetilde{f} : k[t] \to A^D \tag{1.104}$$

$$t \mapsto \lambda. \tag{1.105}$$

This gives an element of $\mathrm{Hom}(G^D, \mathbb{G}_A)$ by taking $\mathrm{Spec}\, \widetilde{f}$.
Conversely, given $\psi : k[t] \to A^D$, let $\lambda = \psi(t)$ and define

$$\overline{\psi} : A \to k[t]/(t^2) \tag{1.106}$$

$$a \mapsto \epsilon(a) + t\lambda(a). \tag{1.107}$$

It is clear that we do get a linear bijection between these vector spaces. □

Proposition 1.4.2. *If k is a field of characteristic 0, then any finite commutative group scheme over k is étale.*

Proof. Let G be a finite group scheme over k. We can assume that k is algebraically closed. The translation action of $G(k)$ on G is transitive, hence it is enough to show that G is étale at the origin. By the previous proposition, it is enough to show that any map $G^D \to \mathbb{G}_a$ is zero. The image of G^D under this map is a finite subgroup scheme of $\mathbb{G}_a$. We will show that $\mathbb{G}_a$ has no finite subgroup schemes. Let $H \subset \mathbb{G}_a$ be a finite subgroup scheme. Then $H(k) \subset \mathbb{G}_a(k) = k^+$ is a finite subgroup. But k^+ is a $\mathbb{Q}$-vector space, in particular, it has no finite subgroups. Hence $H(k) = 0$ and it follows that H is of the form $k[x]/(x^n)$ for some n. The comultiplication

$$x \mapsto 1 \otimes x + x \otimes 1 \tag{1.108}$$

of $\mathbb{G}_a$ must restrict to H as well. Therefore,

$$(x \otimes 1 + 1 \otimes x)^n = \sum_{i=1}^{n} \binom{n}{i} x^{n-i} \otimes x^i \tag{1.109}$$

must be in the ideal generated by $x^n \otimes 1, 1 \otimes x^n$. Since the characteristic of k is zero, all the binomial coefficients in the formula above are nonzero. Hence $n = 1$ and $H = 0$. □

Using a similar argument, we can show that if $\mathrm{char}\, k = p$, then $\boldsymbol{\alpha}_p$ is simple. Indeed, let $H \subset \boldsymbol{\alpha}_p$ be a subgroup scheme. Then it is of the form $\mathrm{Spec}\, k[x]/(x^n)$ for $n < p$. So all the binomial coefficients are again nonzero and $n = 1$, so $H = 0$.

Remark. For our proof it was essential that G is commutative because we are using Cartier duality. However, the result holds without the commutativity assumption, see [Wat79, §11.4].

Proposition 1.4.3. *Let G be a finite commutative algebraic group over a field k. The following are equivalent:*

(i) $G_{k^{\mathrm{sep}}}$ *is constant.*

(ii) G *is étale.*

(iii) F_G *is an isomorphism.*

Proof. Let us show that (i) is equivalent to (ii). By definition, an étale morphism is a smooth morphism of relative dimension zero, i.e., flat, finite type, with vanishing sheaf of differentials. Since k is a field, G is étale if and only if $\Omega_{G/k} = 0$. Formation of the sheaf of relative differentials is invariant under base change, so $\Omega_{G/k} = 0$ is equivalent to $\Omega_{G_{k^{\mathrm{sep}}}/k^{\mathrm{sep}}} = 0$. This means that $G_{k^{\mathrm{sep}}}$ is reduced and all its residue fields are separable over k^{sep}. But k^{sep} is separably closed, so

$$G_{k^{\mathrm{sep}}} \cong \sqcup \operatorname{Spec} k^{\mathrm{sep}} \tag{1.110}$$

as a scheme. The group structure on $G_{k^{\mathrm{sep}}}$ corresponds to the group structure on $G(k^{\mathrm{sep}})$, yielding

$$G_{k^{\mathrm{sep}}} \cong \underline{G(k^{\mathrm{sep}})}. \tag{1.111}$$

Now let us see that (ii) is equivalent to (iii). The group G is étale if and only if the tangent space at the identity is trivial. The absolute Frobenius σ and the relative Frobenius F_G are both zero at this tangent space, so the étaleness of G is equivalent to F_G being an infinitesimal isomorphism. But F_G is bijective on points, so this is equivalent to F_G being an isomorphism. □

Definition 1.4.4. Let G be a finite commutative group scheme over a field. Let $F_G : G \to G^{(p)}$ be the relative Frobenius morphism. It induces a homomorphism

$$F_{G^D} : G^D \to (G^D)^{(p)} \cong (G^{(p)})^D. \tag{1.112}$$

The **Verschiebung morphism** V_G (also denoted by V if there is no confusion about G) is defined as the dual of F_{G^D}:

$$V_G = F_{G^D}^D : G^{(p)} \to G. \tag{1.113}$$

Taking the Cartier dual of the previous proposition gives us

Proposition 1.4.5. *The following are equivalent:*

(i) $G_{k^{\mathrm{sep}}} \cong \bigoplus_{i=1}^{k} \boldsymbol{\mu}_{n_i,k^{\mathrm{sep}}}$ *for some positive integers* n_i.

(ii) G^D *is étale.*

(iii) V_G *is an isomorphism.*

Now let $G^{\mathrm{red}} \subset G$ be the underlying reduced subscheme of G. In general, G^{red} does not have a natural group scheme structure making it a subgroup

scheme of G. However, if k is a perfect field, then G^{red} is naturally a closed subgroup of G. Since G^{red} is reduced, it is smooth ([SGA3]), hence it is geometrically reduced ([SGA3]). By [EGA4, Volume IV 4.6.1] $G^{\mathrm{red}} \times_k G^{\mathrm{red}}$ is reduced and hence the restriction of the multiplication map

$$G \times_k G \to G \tag{1.114}$$

to $G^{\mathrm{red}} \times_k G^{\mathrm{red}}$ factors through G^{red}, making it a subgroup scheme of G. In general, for G noncommutative, $G^{\mathrm{red}} \subset G$ is not normal.
Denote by $G^0 \subset G$ the connected component of the identity. It is a group subscheme of G by [Wat79, p. 51].

Proposition 1.4.6. *Let G be a finite group scheme over a perfect field k. Then there is a canonical isomorphism of group schemes*

$$G \cong G^0 \oplus G^{\mathrm{red}}. \tag{1.115}$$

Proof. We will show that the natural map

$$G^{\mathrm{red}} \to G/G^0 \tag{1.116}$$

is an isomorphism. The formation of G^{red} and G^0 is compatible with base change, so without the loss of generality we may assume that k is separably closed. Then $G^{\mathrm{red}} \to G/G^0$ is a bijective morphism between constant group schemes, i.e., an isomorphism. □

Remark. It is crucial that k is a perfect field in the above proposition, as there are counterexamples for fields which are not perfect.

Definition 1.4.7. A finite commutative group scheme G is **local** if $G = G^0$ and **reduced** if $G = G^{\mathrm{red}}$. A group scheme G is of *a*-*b* **type** if G is of type a and G^D is of type b. Such a group scheme is called a **group scheme of pure type**.

The previous definition implies that there are four possibilities for a finite commutative group scheme G: reduced-reduced, reduced-local, local-reduced, and local-local. Every group splits into the direct sum of four groups of these types.

Proposition 1.4.8. *Let G be a finite commutative group scheme over a perfect field k. There is a unique and functorial decomposition of G*

$$G \cong G_{\mathrm{rr}} \oplus G_{\mathrm{rl}} \oplus G_{\mathrm{lr}} \oplus G_{\mathrm{ll}}, \tag{1.117}$$

with $G_{\mathrm{rr}}, G_{\mathrm{rl}}, G_{\mathrm{lr}}, G_{\mathrm{ll}}$ of reduced-reduced, reduced-local, local-reduced, local-local types respectively.

Proof. The decomposition $G = G^0 \oplus G^{\mathrm{red}}$ is functorial in G. Take the Cartier dual

$$G^D = (G^0 \oplus G^{\mathrm{red}})^D = (G^0)^D \oplus (G^{\mathrm{red}})^D \tag{1.118}$$

and apply the decomposition to each factor, so

$$G^D = ((G^0)^D)^0 \oplus ((G^0)^D)^{\mathrm{red}} \oplus ((G^{\mathrm{red}})^D)^0 \oplus ((G^{\mathrm{red}})^D)^{\mathrm{red}}. \tag{1.119}$$

Apply the Cartier duality functor again to get

$$\begin{aligned} G &= (G^D)^D && (1.120)\\ &= (((G^0)^D)^0 \oplus ((G^0)^D)^{\mathrm{red}} \oplus ((G^{\mathrm{red}})^D)^0 \oplus ((G^{\mathrm{red}})^D)^{\mathrm{red}})^D && (1.121)\\ &= G_{\mathrm{ll}} \oplus G_{\mathrm{lr}} \oplus G_{\mathrm{rl}} \oplus G_{\mathrm{rr}}. && (1.122) \end{aligned}$$

□

Note that, in particular, there are no homomorphisms between groups of different types.

Proposition 1.4.9. *Let G, H be finite algebraic groups over k with G local and H reduced. Then*

$$\mathrm{Hom}(G, H) = \mathrm{Hom}(H, G) = 0. \tag{1.123}$$

Proof. Let $A = \mathcal{O}(G), B = \mathcal{O}(H)$, i.e., A is local and B is reduced. It is clear that there are no k-algebra homomorphisms $A \to B$ – the maximal ideal of A is nilpotent since A is artinian, hence any homomorphism maps the maximal ideal it to zero. But $A = m_e \oplus k$, hence $\mathrm{Hom}(A, B) = 0$.
Recall that a local ring has only two idempotents, 0 and 1. Indeed, if $x = x^2$ then $x(x-1) = 0$. If x is in the maximal ideal, then $x-1$ is invertible and $x = 0$. If x is not in the maximal ideal, then it is invertible and $x = 1$. Also recall a theorem by Dedekind: if B is a reduced artinian ring, then B decomposes as a finite product of fields

$$B = k_1 \times ... \times k_n. \tag{1.124}$$

Let $e_1, ..., e_n$ be idempotents in B (e_i is the row of zeros except for 1 in the ith place). Because $\epsilon_B i_B = \mathrm{id}_k$, we may assume that $\epsilon_B(e_1) = 1$, i.e., $k_1 = k$. Since $e_1 e_i = 0$ for all $i \geq 2$ we have $\epsilon_B(e_i) = 0$. Let $f : B \to A$ be a morphism of algebras. We must have $\epsilon_A = \epsilon_B \circ f$, so $f(e_1) = 1$ and $f(e_i) = 0$ for all $i \geq 2$. But this implies $f = i_B \circ \epsilon_A$, so $f = 0$ as required. □

In fact, we can replace Hom by Ext^1 in the proposition. If we are working over a ring, nonsplit extensions are possible.

Example 1.4.10. Let $R = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}] = \mathbb{Z}[a]$ be the base ring. Notice that $a\overline{a} = 2$. By Section 1.2, there are 4 group schemes of order 2 over R. These are $\mathbb{Z}/2, \boldsymbol{\mu}_2, G_a = \operatorname{Spec} R[x]/(x^2 - ax)$, and $G_{\overline{a}} = \operatorname{Spec} R[y]/(y^2 - \overline{a}y)$. Define an inclusion

$$0 \to \mathbb{Z}/2 \to G_a \times G_{\overline{a}} \tag{1.125}$$

by

$$x \mapsto at, \tag{1.126}$$

$$y \mapsto \overline{a}t, \tag{1.127}$$

where t is a co-ordinate on $\mathcal{O}(\mathbb{Z}/2)$. The cokernel is a representable sheaf and is isomorphic to $\boldsymbol{\mu}_2$. The resulting short exact sequence

$$0 \to \mathbb{Z}/2 \to G_a \times_R G_{\overline{a}} \to \boldsymbol{\mu}_2 \to 0 \tag{1.128}$$

is not split. This can be checked by looking at its étale and connected parts.

Proposition 1.4.11. *Let G be a commutative finite group scheme of pure type. Then*

(i) G is reduced-reduced if and only if F, V are both isomorphisms.

(ii) G is reduced-local if and only if F is an isomorphism and V is nilpotent.

(iii) G is local-reduced if and only if F is nilpotent and V is an isomorphism.

(iv) G is local-local if and only if F, V are both nilpotent.

Proof. Suppose that G is local, i.e., $G = G^0$. The maximal ideal of G^0 corresponding to the group identity element is nilpotent, so it is annihilated by some power of the absolute Frobenius. Hence it must be annihilated by some power of the relative Frobenius as well. Hence F is nilpotent on G. On the other hand, if G is reduced, then by 1.4.3 we know that F is an isomorphism. Applying the same argument to the case of G reduced and then to G^D yields the result. □

Theorem 1.4.12. *The assignment*

$$G \mapsto G(k^s) \tag{1.129}$$

defines an equivalence between the category of finite étale group schemes over a field k and the category of continuous finite $\mathbb{Z}[\mathrm{Gal}(k^s/k)]$-modules.

Sketch of proof. Let Γ be a finite abelian group with a continuous action of G_k, the absolute Galois group of k. An action is continuous if each $\gamma \in \Gamma$ is

fixed by some G_L for a field extension L/k. Define the corresponding group scheme $A(\Gamma)$ as follows. As a k-vector space, $A(\Gamma)$ consists of maps

$$f : \Gamma \to \overline{k} \tag{1.130}$$

which commute with the action of G_k:

$$f(g\gamma) = \gamma f(g). \tag{1.131}$$

Let L/k be a finite extension such that G_L acts trivially. Every f in $A(\Gamma)$ then lands in L and $A(\Gamma)$ is finite dimensional over k. In fact, $\dim_k A(\Gamma) = |\Gamma|$. The ring structure on $A(\Gamma)$ is defined pointwise:

$$fg(\gamma) = f(\gamma)g(\gamma). \tag{1.132}$$

The Hopf algebra structure is

$$\Delta(f)(\gamma, \delta) = f(\gamma + \delta), \tag{1.133}$$

$$S(f)(g) = f(-g), \tag{1.134}$$

$$\epsilon(f)(g) = f(0). \tag{1.135}$$

The algebra $A(\Gamma)$ is a finite étale Hopf algebra, i.e., it is isomorphic to a finite direct sum of finite field extensions of k. □

The theorem implies that the study of G_{rr}, G_{rl} and, by Cartier duality, G_{lr} is essentially Galois theory. In particular, the case of k algebraically closed, gives an equivalence with finite abelian groups. On the other hand, the group schemes of local-local type are very different and need further tools.

1.5 Finite groups schemes of local-local type

Let G be a local-local group scheme over an algebraically closed field. We know that Frobenius and Verschiebung are both nilpotent. We start with the case $F = V = 0$.

Proposition 1.5.1. *If $F_G = V_G = 0$ then $G \cong \boldsymbol{\alpha}_p^{\oplus n}$, where $n = \dim_k T_{G,0}$.*

Proof. Consider the short exact sequence of k-modules

$$0 \to I \to A \xrightarrow{\epsilon} k \to 0, \tag{1.136}$$

where ϵ is the counit map. Since k is projective, the sequence splits and $A \cong I \oplus k$. Recall that $T_{G,0} \cong (I/I^2)^\vee$, so I is generated by n elements. But $F = 0$, so $a^p = 0$ for all $a \in I$. Hence I is nilpotent and its n generators generate A as a k-algebra. Write $A = k[x_1, ..., x_n]/J$, $I = (x_1, ..., x_n)/J$ for some ideal J. Then $x_i^p \in J$ for all i. Hence A must be a quotient of $k[x_1, ..., x_n]/(x_1^p, ..., x_n^p)$. It follows that $\dim_k A \leq p^n$. By 1.4.1, we can work with morphisms $G^D \to \mathbb{G}_a$ instead of tangent vectors. Let

$$\phi : G^D \to \mathbb{G}_a \tag{1.137}$$

be a morphism. Then, using $V = 0$ and functoriality of F,

$$F_{\mathbb{G}_a} \circ \phi = \phi^{(p)} \circ F_{G^D} = \phi^{(p)} \circ V_G^D = 0. \tag{1.138}$$

Therefore, ϕ factors through the kernel of $F_{\mathbb{G}_a}$, which is $\boldsymbol{\alpha}_p$.

□

Chapter 2

Dieudonné modules and Hopf algebras

2.1 Classification of primitively generated Hopf algebras

In this section we classify Hopf algebras which are primitively generated. Fix a base ring S, which is an $\mathbb{F}_p$-algebra. Let H be a finite flat Hopf algebra over S. An element $a \in H$ is **primitive** if

$$\Delta(a) = 1 \otimes a + a \otimes 1. \tag{2.1}$$

For example, $x \in S[x]/(x^p) = \mathcal{O}(\boldsymbol{\alpha}_p)$ is primitive. Let $P(H) \subset H$ denote the subset of primitive elements. A Hopf algebra H is **primitively generated** if the smallest Hopf subalgebra of H which contains $P(H)$ is H itself.

Example 2.1.1. Let $H = \mathcal{O}(\boldsymbol{\alpha}_p) = S[x]/(x^p)$. Then

$$P(H) = Sx, \tag{2.2}$$

since for other powers x^i of x we will have

$$\Delta(x^i) = \Delta(x)^i = (1 \otimes x + x \otimes 1)^i \neq 1 \otimes x^i + x^i \otimes 1, \tag{2.3}$$

because there will be mixed terms with coefficients not dividing p, unless $i = p$. If $H = S[x]/(x^{p^n})$ and H corresponds to the algebraic group $\boldsymbol{\alpha}_{p^n}$ then

$$P(H) = Sx \oplus Sx^p \oplus Sx^{p^2} ... \oplus Sx^{p^{n-1}}. \tag{2.4}$$

Let $\mathbb{Z}/p$ denote the constant group scheme, then $P(\mathbb{Z}/p) = Sx$. The multiplicative group scheme $\boldsymbol{\mu}_p$, represented by $S[t]/(x^p - 1)$ with comultiplication $\Delta(x) = x \otimes x$ is primitive-free: $P(\boldsymbol{\mu}_p) = 0$.

Example 2.1.2. The p-torsion group scheme $\mathcal{M}_{p^2}$ of a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ is not primitively generated since it admits a quotient isomorphic to $\boldsymbol{\alpha}_p$ which corresponds to a proper Hopf subalgebra containing all the primitive elements. Indeed, we have a nonsplit extension

$$0 \to \boldsymbol{\alpha}_p \to \mathcal{M}_{p^2} \to \boldsymbol{\alpha}_p \to 0 \tag{2.5}$$

in the category of *commutative* group schemes.

Proposition 2.1.3. *Let H be a Hopf algebra and $P(H)$ the set of primitive elements. Then $P(H)$ has the following properties:*

1. *$P(H) \cap S = 0$,*
2. *$P(H)$ is an S-module.*
3. *If S is a PID then $P(H)$ is free over S.*
4. *$t \in P(H)$ implies $t^p \in P(H)$.*

Proof. The proofs are immediate, for example, for 1, let $a \in P(H) \cap S$, then

$$\Delta(a) = a\Delta(1) = a \otimes 1, \tag{2.6}$$

on the other hand,

$$\Delta(a) = a \otimes 1 + 1 \otimes a, \tag{2.7}$$

so that

$$a = a(1 \otimes 1) = 1 \otimes a = 0, \tag{2.8}$$

since $1 \otimes 1 \in H \otimes H$ is 1. □

The last property implies that the Frobenius map restricts to primitive elements, i.e., we can define

$$P(H) \to P(H) \tag{2.9}$$

$$t \to t^p. \tag{2.10}$$

Example 2.1.4. Take $\boldsymbol{\alpha}_p$, which is represented by $H = S[x]/(x^p)$ with x primitive. We know that $P(H) = Sx$ and $F(x) = 0$.

Example 2.1.5. Consider $\boldsymbol{\alpha}_{p^n}$, which is represented by $H = S[x]/(x^{p^n})$ with x primitive. Then

$$P(H) = Sx \oplus Sx^p \oplus Sx^{p^2} ... \oplus Sx^{p^{n-1}} \tag{2.11}$$

and $F(x^{p^i}) = x^{p^{i+1}}$.

Example 2.1.6. If $\mathbb{Z}/p$ is the constant group scheme with $P(\mathbb{Z}/p) = Sx$ then $F(x) = x$.

Define $S\{F\}$ to be the noncommutative ring of polynomials with single variable F and $Fs = s^pF$. This is the baby version of the Dieudonné ring, but this will work for the primitively generated case.

Proposition 2.1.7 (Dieudonné correspondence for primitively generated Hopf algebras)**.** *Let S be an $\mathbb{F}_p$-algebra and a principal ideal domain. There is an equivalence of categories*

$$\{\textit{Finitely generated free primitively generated Hopf algebras over } S\} \tag{2.12}$$

$$\simeq$$

$$\{\textit{Modules of finite type over } S\{F\}\textit{, free over } S.\} \tag{2.13}$$

We call the modules on the right hand side of the equivalence **primitive Dieudonné modules**.

Proof. For any H, the module of primitive elements $P(H)$ is free over S and the action of F on H restricts to $P(H)$, so it is indeed an $S\{F\}$-module. For a Hopf algebra morphism

$$\phi : H_1 \to H_2 \tag{2.14}$$

the restricted map $\phi|_{P(H_1)}$ lands in $P(H_2)$, so we do get a functor between categories.
On the other hand, consider an $S\{F\}$-module M of finite type free over S. Let $\{e_1, ..., e_n\}$ be an S-basis of M. Then

$$Fe_i = \sum_{j=1}^{n} a_{ji} e_j \tag{2.15}$$

for some $a_{ji} \in S$. Define

$$H = S[x_1, ..., x_n]/(\{x_i^p - \sum_j a_{ji} x_j\}_{i=1,...,n}) \tag{2.16}$$

with the x_i primitive. Then H is a primitively generated Hopf algebra which corresponds to M. □

Definition 2.1.8. A **morphism** of primitive Dieudonné moddules M_1 and M_2 is an S-linear map

$$M_1 \to M_2 \tag{2.17}$$

which respects the F-action.

Remark. Taking just the functor

$$\{S\text{-Hopf algebras}\} \to \{S\{F\}\text{-modules}\} \tag{2.18}$$

$$H \mapsto P(H) \tag{2.19}$$

does not give us an equivalence. For example, $P(\mathbb{Z}/p^2) \cong P((\mathbb{Z}/p)^2)$ and $S\{F\}[X]$ with X commuting variable is not in the image of $P(-)$.

Remark. The functor $P(-)$ is a contravariant Dieudonné module theory in the sense of [DG80].

Example 2.1.9. Let $G = \boldsymbol{\alpha}_p$, then we know that it corresponds to the module Se with $Fe = 0$.

Example 2.1.10. Let $G = \boldsymbol{\alpha}_{p^n}$. This algebraic group corresponds to $\bigoplus_{i=1}^{n} Se_i$ with $Fe_i = e_{i+1}$ if $i \neq n$ and $Fe_n = 0$. We can work backwards from the module to recover the algebraic group.

Example 2.1.11. The finite group scheme $\mathbb{Z}/p$ corresponds to Se with $Fe = e$.

Example 2.1.12. Take $M = Se_1 \oplus Se_2$ and let F swap e_1 and e_2. The corresponding Hopf algebra is

$$S[x_1, x_2]/(x_1^p - x_2, x_2^p - x_1) \cong S[x]/(x^{p^2} - x), \tag{2.20}$$

where x is primitive. This Hopf algebra corresponds to $\mathbb{Z}/p^2$.

2.2 The parameter space for primitively generated Hopf algebras

Take a finite free S-module M and let $\{e_1, ..., e_n\}$ be its S-basis. For an arbitrary matrix $A \in \mathrm{M}_n(S)$ define the action of $F \in S\{F\}$:

$$Fe_i := Ae_i. \tag{2.21}$$

There is a primitively generated Hopf algebra H associated to the pair (n, A). On the other hand, every primitively generated Hopf algebra H defines a matrix – the corresponding primitive Dieudonné module is finite over S and the Fe_i define an S-linear map. We need to know when two matrices define the same Hopf algebra.

Proposition 2.2.1. *Two matrices A and B in $\mathrm{M}_n(S)$ define isomorphic Hopf algebras if and only if there is an invertible matrix $Q \in \mathrm{M}_n(S)^*$ such that*

$$QA = BQ^{(p)}, \tag{2.22}$$

where $Q^{(p)}$ is obtained from Q by raising every entry to the power of p.

Proof. Assume that A and B define free R-modules M_A, M_B of rank n over S. Fix an S-isomorphism $M_A \cong M_B$ and an S-basis $\{e_1, ..., e_n\}$ for both of these modules. Let

$$Q : M_A \to M_B \tag{2.23}$$

be a map of $S\{F\}$-modules, i.e., a map of primitive Dieudonné modules. Then $QF = FQ$, which we can write out using the basis:

$$\begin{aligned} FQ(e_1) =& F(q_{11}e_1 + q_{21}e_2 + ... + q_{n1}e_n) && (2.24)\\ =& (q_{11}^p b_{11} + ... + q_{n1}^p b_{1n})e_1 && (2.25)\\ & (q_{11}^p b_{21} + ... + q_{n1}^p b_{2n})e_2 + && (2.26)\\ & \vdots && (2.27)\\ & (q_{11}^p b_{n1} + ... + q_{n1}^p b_{nn})e_n && (2.28) \end{aligned}$$

and, on the other hand,

$$\begin{aligned} QF(e_1) =& Q(a_{11}e_1 + a_{21}e_2 + ... + a_{n1}e_n) && (2.29)\\ =& (a_{11}q_{11} + a_{21}q_{12} + ... + a_{n1}q_{1n})e_1 + && (2.30)\\ & (a_{11}q_{21} + a_{21}q_{22} + ... + a_{n1}q_{2n})e_1 + && (2.31)\\ & \vdots && (2.32)\\ & (a_{11}q_{n1} + a_{21}q_{n2} + ... + a_{n1}q_{nn})e_n. && (2.33) \end{aligned}$$

Repeating the above calculation for all e_i, we conclude $QA = BQ^{(p)}$, where the (i, j)-th entry of $Q^{(p)}$ is q_{ij}^p. The modules M_A and M_B are isomorphic if and only if there is an inverse to Q, i.e., $Q \in M_n(S)^*$ □

2.3 Primitively generated Hopf algebras of low rank

We consider primitively generated Hopf algebras of p-rank n over various finite rings.

Example 2.3.1. Let $S = \mathbb{F}_p$ and $n = 1$. We already know about $\boldsymbol{\alpha}_p$, represented by $\mathbb{F}_p[x]/(x^p)$. The parameter space is $\mathbb{F}_p/\sim$, where $\lambda_1 \sim \lambda_2$ if and only if $a^p\lambda_1 = a\lambda_2$. By Fermat's little theorem this implies $\lambda_1 = \lambda_2$, so there are p isomorphism classes given by $\{\mathbb{F}_p[x]/(x^p - \lambda x)\}_{\lambda \in \mathbb{F}_p}$.

Example 2.3.2. Let $S = \mathbb{F}_2$ and $n = 2$. We use the code from Appendix B to calculate the parameter space, which in this case is the quotient stack over $\mathbb{F}_p$ modulo twisted conjugation. Calling `MatrixConjClass(FiniteField(2),2);` we

get the list

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}, \tag{2.34}$$

$$\left\{\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix}\right\}, \tag{2.35}$$

$$\left\{\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}, \tag{2.36}$$

$$\left\{\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\}, \tag{2.37}$$

$$\left\{\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}1&1\\1&1\end{pmatrix},\right\}, \tag{2.38}$$

$$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\} \tag{2.39}$$

The corresponding Hopf algebras are given by calling

```
[PrimGenHopfAlg(C[1]): C in L];
```

which returns

```
[
    Affine Algebra of rank 2 over GF(2)
    Lexicographical Order
    Variables: x_1, x_2
    Quotient relations:
    [
        x_1^2 + x_1,
        x_2^2 + x_2
    ],
    Affine Algebra of rank 2 over GF(2)
    Lexicographical Order
    Variables: x_1, x_2
    Quotient relations:
    [
        x_1^2,
        x_2^2 + x_2
    ],
    Affine Algebra of rank 2 over GF(2)
    Lexicographical Order
    Variables: x_1, x_2
    Quotient relations:
    [
        x_1^2 + x_1 + x_2,
        x_1 + x_2^2
```

```
    ],
    Affine Algebra of rank 2 over GF(2)
    Lexicographical Order
    Variables: x_1, x_2
    Quotient relations:
    [
        x_1^2 + x_2,
        x_1 + x_2^2
    ],
    Affine Algebra of rank 2 over GF(2)
    Lexicographical Order
    Variables: x_1, x_2
    Quotient relations:
    [
        x_1^2 + x_2,
        x_2^2
    ],
    Affine Algebra of rank 2 over GF(2)
    Lexicographical Order
    Variables: x_1, x_2
    Quotient relations:
    [
        x_1^2,
        x_2^2
    ]
]
```

The comultiplication in these algebras is particularly simple – all the x_i are primitive.

Example 2.3.3. We can also consider $S = \mathbb{F}_p$ for various primes p and $n = 3, 4, 5$. The number of isomorphism classes grows quite fast.

2-rank	# of classes	3-rank	# of classes	4-rank	# of classes	5-rank	# of classes
1	2	1	3	1	2	1	5
2	6	2	12	2	6	2	30
3	14	3	39	3	14	3	155
4	34	4	129	4	34	4	?
5	74	5	?	5	74	5	?

2.4 Primitive extensions of Hopf algebas

Using the classical Dieudonné module theory in the sense of [Gro74, Chapitre II], the group $\mathbb{G}_a$, represented by $S[x]$ corresponds to the 1-dimensional module $S\{F\}$. This is a projective object in the category of $S\{F\}$-modules and can be

used to construct projective resolutions. For example, consider $\boldsymbol{\alpha}_p$ and let M be the corresponding Dieudonné module. Then we have a short exact sequence

$$0 \to S\{F\} \xrightarrow{F} S\{F\} \to M \to 0 \tag{2.40}$$

which is a projective resolution of M *in the category of modules of finite type over* $S\{F\}$*, free over* S. We have

$$0 \to \mathrm{Hom}_{S\{F\}}(S\{F\}, M) \to \mathrm{Hom}_{S\{F\}}(S\{F\}, M) \to \mathrm{Ext}^1_{S\{F\}}(M, M) \to 0. \tag{2.41}$$

Note that $\mathrm{Hom}_{S\{F\}}(S\{F\}, M) \cong M$ via $f \mapsto f(1)$. So we get the sequence

$$0 \to M \xrightarrow{0} M \to \mathrm{Ext}^1_{S\{F\}}(M, M), \tag{2.42}$$

since the Frobenius is 0 on M. We conclude that $\mathrm{Ext}^1_{S\{F\}}(M, M) \cong M$. But note that this Ext group only classifies extensions which give primitively generated Hopf algebras. For example, the group scheme $\mathcal{M}_{p^2}$ constructed in Section 3.2 does not arise this way.

2.5 Witt vectors

In this section we will define the ring of Witt vectors and show that it is an affine group scheme, i.e., it represents a certain functor. The canonical reference for this material is [Ser79, Section II.6] and this is what I am following, but I hope to be more down to earth in my treatment.

Basic idea: W allows us to build $\mathbb{Z}_p$ from $\mathbb{F}_p$ without any prior knowledge of $\mathbb{Z}_p$. Remarkably, we construct an integral domain of characteristic zero from a field of characteristic p. The construction is related to the fact that while the additive group of the power series ring $k[[t]]$ in characteristic p has p-torsion, the multiplicative group $1 + tk[[t]]$ is torsion-free. This means that some aspect of characteristic zero is preserved in positive characteristic.

Pick a prime p and define **Witt polynomials** by

$$\Phi_n \in \mathbb{Z}[x_0, ..., x_n], \tag{2.43}$$

$$\Phi_n(x_0, ..., x_n) = x_0^{p^n} + px_1^{p^{n-1}} + ... + p^n x_n. \tag{2.44}$$

Now define **Witt addition and multiplication polynomials** $S_n, P_n \in \mathbb{Z}[x_0, ..., x_n, y_0, ..., y_n]$ implicitly by

$$\Phi_n(S_0, ..., S_n) = \Phi_n(x_0, ..., x_n) + \Phi_n(y_0, ..., y_n), \tag{2.45}$$

$$\Phi_n(P_0, ..., P_n) = \Phi_n(x_0, ..., x_n) \cdot \Phi_n(y_0, ..., y_n). \tag{2.46}$$

For example, the first few of these are

$$S_0(x_0, y_0) = x_0 + y_0, \tag{2.47}$$

$$P_0(x_0, y_0) = x_0 y_0, \tag{2.48}$$

$$S_1(x_0, x_1, y_0, y_1) = x_1 + y_1 - \frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} x_0^i y_0^{p-i}. \tag{2.49}$$

These become rather cumbersome to write down even for small values of n, so it is better to think of these conceptually.

Definition 2.5.1. The **Witt ring scheme** is a representable functor defined by

$$W : \mathrm{Alg}_{\mathbb{Z}} \to \mathrm{Ring}, \tag{2.50}$$

$$A \mapsto \prod_{i=0}^{\infty} A. \tag{2.51}$$

The addition and multiplication on $W(A)$ are defined using the Witt addition and multiplication polynomials:

$$(w_0, w_1, ...) + (v_0, v_1, ...) = (S_0(w_0, v_0), S_1(w_0, w_1, v_0, v_1), ...), \tag{2.52}$$

$$(w_0, w_1, ...) \cdot (v_0, v_1, ...) = (P_0(w_0, v_0), P_1(w_0, w_1, v_0, v_1), ...). \tag{2.53}$$

The **truncated ring of Witt vectors** is the quotient $W_n(A) = W(A)/p^n W(A)$.

We can also define the Frobenius and the Verschiebung operators on $W(A)$:

$$F : W(A) \to W(A), \tag{2.54}$$

$$(a_0, a_1, ...) \mapsto (a_0^p, a_1^p, ...), \tag{2.55}$$

$$V : W(A) \to W(A), \tag{2.56}$$

$$(a_0, a_1, ...) \mapsto (0, a_0, a_1, ...). \tag{2.57}$$

These satisfy $VF = FV = p$, i.e., their composition acts as multiplication by

p. Both F and V descend to operations on the truncated Witt ring $W_n(A)$.

Proposition 2.5.2. *Let k be a field of characteristic p and $W = W(k)$ its corresponding Witt ring. Then W is an integral domain of characteristic zero, with multiplicative identity $(1, 0, 0, ...)$.*

Example 2.5.3. $W(\mathbb{F}_p) \cong \mathbb{Z}_p$. Note that in particular we have $W_n(F_p) = \mathbb{Z}/p^n$ and $W(\mathbb{F}_p)$ is obtained as the limit of the $W_n(F_p)$.

Example 2.5.4. $W(\mathbb{F}_{p^n})$ is the unique degree n unramified extension of $\mathbb{Z}_p$.

We can now define the Dieudonné ring. We use the following notation: for a commutative ring A, the ring $A\{x_1, x_2\}$ denotes the noncommutative ring with variables x_1 and x_2 which do not necessarily commute between themselves or with elements of A. The notation $A[x_1, x_2]$ always denotes the commutative polynomial ring over A.

Definition 2.5.5. Let A be a ring and $W = W(A)$ its corresponding Witt ring. The **Dieudonné ring** is defined as

$$\mathcal{D} = W\{F, V\}/(FV - p, VF - p, Fw - \sigma(w)F, wV - V\sigma(w)), \tag{2.58}$$

where $\sigma : W \to W$ is the automorphism induced by the absolute Frobenius map on A.

Note that $\mathcal{D}$ is a noncommutative ring in general, with the only exception $\mathcal{D}(F_p)$.
Define the Frobenius kernels on W_n by

$$W_n^m(A) = \{(a_0, ..., a_{n-1}) : a_i^{p^m} = 0, 0 \leq i \leq n-1\}. \tag{2.59}$$

The operators F and V restrict to

$$F : W_n^m(A) \to W_n^m(A), \tag{2.60}$$

$$V : W_n^m(A) \to W_n^m(A). \tag{2.61}$$

2.6 Dieudonné correspondence

Now we arrive to the main theorem for Dieudonné theory for local-local group schemes.

Theorem 2.6.1 (Théorème 4.2, [Gro74] and Chapitre V [DG80])**.** *Let k be a*

perfect field. There is a categorical equivalence

$$D^*: \{\textit{Local-local commutative algebraic group schemes of rank } p^n \textit{ over a field } k\}$$

$$\simeq$$

$$\{\textit{Dieudonné modules of length } n \textit{ over } W_k\textit{, killed by powers of } F \textit{ and } V.\}$$

The functor D^* is constructed as follows. Let G be a local-local group scheme of prime power order, then

$$D^*(G) = \mathrm{Hom}(\varinjlim_{m,n} W_n^m, G) \tag{2.62}$$

The actions of F and V on the W_n^m induce actions on their injective limit, so we get an action of F and V on $D^*(G)$, making it a Dieudonné module. We will also need the 'quasi-inverse' to D^*, as outlined in Annexe 6 of [Gro74].

Definition 2.6.2. Let M be a Dieudonné module of length n over W, killed by powers of F and V. Choose N large enough so that $V^{N+1} = 0$ on M. Let A_M be the quotient of the free k-algebra $k[T_x : x \in M]$ by the ideal generated by the following elements:

1. $T_{Fx} - T_x^p$ for all $x \in M$;
2. $T_{x+y} - S_N(T_{V^N x}, ..., T_x, T_{V^N y}, ..., T_y)$ for all $x, y \in M$;
3. $T_{\lambda x} - P_N(\lambda_1^{p^{-N}}, \lambda_2^{p^{-N}}, ..., \lambda_{N+1}^{p^{-N}}, T_{V^N x}, ..., T_x)$ for $\lambda \in E, x \in M$.

Proposition 2.6.3. *[Gro74, §6.2] A_M is a local-local Hopf algebra with comultiplication*

$$\Delta(T_m) = S_N(T_{V^N m} \otimes 1, T_{V^{N-1} m} \otimes 1, ..., T_m \otimes 1, 1 \otimes T_{V^N m}, ..., 1 \otimes T_m), \tag{2.63}$$

Proposition 2.6.4. *[Gro74, §6. Annexe] There exists a left adjoint functor E^* to D^*. For every Dieudonné module M the functor $E^*(M)$ is representable and its representing object is* $\mathrm{Spec}\, A_M$.

Example 2.6.5. Let M be the quotient of $\mathcal{D}$ by (F, V). Then $N = 0$. Let $\{m\}$ be an $\mathcal{D}$-basis for M. Then the corresponding Hopf algebra H is generated by T_m over k. The comultiplication is

$$\Delta(T_m) = S_0(T_m \otimes 1, 1 \otimes T_m) = T_m \otimes 1 + 1 \otimes T_m. \tag{2.64}$$

Note that

$$T_m^p = T_{Fm} = T_0 = 0. \tag{2.65}$$

We conclude that H is isomorphic to $k[t]/(t^p)$ with t primitive, i.e., H represents the group scheme $\boldsymbol{\alpha}_p$.

Example 2.6.6. Let M be the quotient of $\mathcal{D}$ by (F^m, V^n). Then we have an k-basis $\{T_{ij}\}_{1\leq i\leq m, 1\leq j\leq n}$ for the Hopf algebra H of M. Note that $FT_{ij} = T_{i+1,j}$, so we may relabel the T_{ij} as $t_j^{p^i}$. The comultiplication is

$$\Delta(t_j^{p^i}) = S_N(T_{V^N m}\otimes 1, T_{V^{N-1}m}\otimes 1, ..., T_m\otimes 1, 1\otimes T_{V^N m}, ..., 1\otimes T_m), \quad (2.66)$$

which we recognise as the comultiplication for the Frobenius kernel W_n^m. We conclude that

$$H = k[t_1, ..., t_n]/(t_1^{p^m}, ..., t_n^{p^m}). \quad (2.67)$$

Example 2.6.7. Given a Hopf algebra H, we may also work backwards to find the corresponding module over $\mathcal{D}$. For example. let H be $k[t]/(t^{p^5})$ with

$$\Delta(t) = t\otimes 1 + 1\otimes t + \sum_{i=1}^{p-1} \frac{1}{i!(p-i)!} t^{p^3 i}\otimes t^{p^4 - p^3 i}. \quad (2.68)$$

Let M be the corresponding Dieudonné module and let $m\in M$ correspond to t, i.e., $T_m = t$. Then

$$(T_m)^5 = T_{F^5 m} = 0, \quad (2.69)$$

so $F^5 M = 0$, but $F^4 M \neq 0$ because $F^4 m \neq 0$. The comultiplication is given by

$$\begin{aligned}\Delta(t) &= S_1(T_m^{p^3}\otimes 1, T_m\otimes 1, 1\otimes T_m^{p^3}, 1\otimes T_m), &(2.70)\\ &= S_1(T_{F^3 m}\otimes 1, T_m\otimes 1, 1\otimes T_{F^3 m}, 1\otimes T_m), &(2.71)\\ &= S_1(T_{Vm}\otimes 1, T_m\otimes 1, 1\otimes T_{Vm}, 1\otimes T_m). &(2.72)\end{aligned}$$

It follows that $V = F^3$ and $V^2 = 0$. Therefore, M is the quotient of $\mathcal{D}$ by $(F^5, F^3 - V, V^2)$ or $(F^5, F^3 - V)$.

Example 2.6.8. Let $H = k[t_1, t_2]/(t_1^{p^2}, t_2^{p^2})$ with t_1 primitive and

$$\Delta(t_2) = t_2\otimes 1 + 1\otimes t_2 + \sum_{i=1}^{p-1} \frac{1}{i!(p-i)!} t_1^{pi}\otimes t_1^{p^2 - pi}. \quad (2.73)$$

Let M be the corresponding Dieudonné module and say it is generated by x_1, x_2 which correspond to t_1, t_2, i.e., $t_1 = T_{x_1}, t_2 = T_{x_2}$. Notice that

$$t_1^2 = T_{x_1}^2 = T_{F^2 x_1} = 0 = T_0, \quad (2.74)$$

so $F^2 x_1 = F^2 x_2 = 0$, while $Fx_1 \neq 0, Fx_2 \neq 0$. Recall the polynomial S_1:

$$S_1(X_0, X_1, Y_0, Y_1) = X_1 + Y_1 - \frac{1}{p}\sum_{i=1}^{p-1} \binom{p}{i} X_0^i Y_0^{p-i}. \quad (2.75)$$

Then we can write

$$\Delta(t_1) = S_0(T_{x_1} \otimes 1, 1 \otimes T_{x_1}), \tag{2.76}$$
$$= S_1(0 \otimes 1, T_{x_1} \otimes 1, 1 \otimes 0, 1 \otimes T_{x_1}), \tag{2.77}$$
$$= S_1(T_{Vx_1} \otimes 1, T_{x_1} \otimes 1, 1 \otimes T_{Vx_1}, 1 \otimes T_{x_1}), \tag{2.78}$$

so it follows that $Vx_1 = 0$. On the other hand,

$$\Delta(t_2) = S_1(T_{x_1}^p \otimes 1, T_x \otimes 1, 1 \otimes T_{x_1}^p, 1 \otimes T_x) \tag{2.79}$$
$$= S_1(T_{Fx_1} \otimes 1, T_{x_2} \otimes 1, 1 \otimes T_{Fx_1}, 1 \otimes T_{x_2}), \tag{2.80}$$
$$= S_1(T_{Vx_2} \otimes 1, T_{x_2} \otimes 1, 1 \otimes T_{Vx_2}, 1 \otimes T_{x_2}), \tag{2.81}$$

so $Fx_1 = Vx_2$. We get a module M generated by x_1, x_2, subject to $F^2M = 0, V^2M = 0, Vx_1 = 0, Fx_1 = Vx_2$.

Dieudonné modules can also be used to describe the local structure of group schemes.

Proposition 2.6.9. *Let G be a finite group scheme over k. There is a canonical isomorphism of k-vector spaces*

$$T_{G,0} \cong (M(G)/FM(G))^\vee. \tag{2.82}$$

Proof. By definition,

$$T_{G,0} = \ker(G(k[\epsilon]) \to G(k)) \cong \mathrm{Hom}(G^D, \mathbb{G}_a) = \mathrm{Hom}(G^D, W_1). \tag{2.83}$$

Notice that $W_1 = \ker V$, so that

$$\mathrm{Hom}(G^D, W_1) = \ker V|_{M(G^D)} = \ker V|_{M(G)^D} = \mathrm{coker}(F|_{M(G)})^\vee. \tag{2.84}$$

□

Remark. If A is an abelian variety over k, there is an exact sequence

$$0 \to H^0(A, \Omega_A^1) \to H^1_{\mathrm{dr}}(A) \to H^1(A, \mathcal{O}_A) \to 0. \tag{2.85}$$

It was shown by Oda in [Oda69] that there is a canonical isomorphism

$$H^1_{\mathrm{dR}}(A) \cong M(A[p]). \tag{2.86}$$

Moreover, the Hodge filtration $H^0(A, \Omega_A^1) \subset H^1_{\mathrm{dR}}(A)$ can be identified with

$$\ker F|_{M(A[p])} = VM(A[p]) \subset M(A[p]). \tag{2.87}$$

The exact sequence can be written as

$$0 \to V(M(A[p])) \to M(A[p]) \to T_{[\mathcal{O}_A]} \operatorname{Pic}^0 A \to 0 \tag{2.88}$$

Chapter 3

Group schemes of order p^2 and p^3

3.1 The p-torsion group scheme $A[p]$

Fix a Noetherian scheme S. Let $\pi\colon A \to S$ be an abelian scheme of relative dimension g. For a natural number n, denote by $[n]\colon A \to A$ the multiplication by n map. It is a proper flat morphism and its kernel $A[n]$ is a finite flat group scheme of order n^{2g}. Let $S_0 \subset S$ be the open subscheme where all the primes dividing n are invertible. The kernel $A[n]$ is étale over S_0 and S_0 is the maximal S-scheme with such property. Therefore, if A/k is an abelian variety and k is a field of characteristic p, then $A[p]$ is never étale over k. Let i be the order of the largest étale quotient of $A[p]$. Then $i \leq p^g$ and in the case of equality A is called an **ordinary abelian variety**.

Example 3.1.1 (g=1, Example A.3.14 in [Gor02])**.** Let E be an elliptic curve. Recall the construction of the Hasse invariant: the absolute Frobenius

$$F\colon E \to E \tag{3.1}$$

induces the morphism

$$F^*\colon H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E) \tag{3.2}$$

on cohomology which is not linear, but *p-linear*, i.e., $F^*(\lambda a) = \lambda^p F^*(a)$ for $\lambda \in k, a \in H^1(E, \mathcal{O}_E)$. The curve E has genus 1, so $h^1(\mathcal{O}_E) = 1$, therefore, F^* is either the zero map or a bijection. In the former case, we say that E has Hasse invariant 0 or E is **ordinary**, in the latter case, we say that E has Hasse invariant 1 or E is **supersingular**. Note that E is always nonsingular as a k-variety.

Every elliptic curve is principally polarised and hence $E[p]$ is self-dual. The

group scheme $E[p]$ is affine of order p^2. There are two cases corresponding to the two values of the Hasse invariant. We list the corresponding cases along with their canonical filtrations (see [Oor05]) and Dieudonné modules in local-local cases.

(i) E is an ordinary elliptic curve. Assume that E is defined over an algebraically closed field. Then we have a split exact sequence

$$0 \to \boldsymbol{\mu}_p \to E[p] \to \mathbb{Z}/p \to 0. \tag{3.3}$$

The Cartier duality for $E[p]$ swaps the two factors: $\boldsymbol{\mu}_p^D = \mathbb{Z}/p$ and $\mathbb{Z}/p^D = \boldsymbol{\mu}_p$. The kernel of the Frobenius is $\boldsymbol{\mu}_p$ and the canonical filtration is

$$0 \subset \boldsymbol{\mu}_p \subset E[p]. \tag{3.4}$$

Note that this filtration cannot be refined: $\boldsymbol{\mu}_p$ is a simple object and does not admit any subgroup schemes, on the other side, the ranks of $\boldsymbol{\mu}_p$ and $E[p]$ are p and p^2 respectively, so if H is a group scheme such that $\boldsymbol{\mu}_p \subset H \subset E[p]$, then $H = \boldsymbol{\mu}_p$ or $E[p]$.

(ii) E is supersingular. Then there is a non-split exact sequence

$$0 \to \boldsymbol{\alpha}_p \to E[p] \to \boldsymbol{\alpha}_p \to 0, \tag{3.5}$$

where the image of $\boldsymbol{\alpha}_p \to E[p]$ is unique and is the kernel of both Frobenius and Verschiebung. If k is algebraically closed and E_1, E_2 are supersingular elliptic curves over k, then $E_1[p] = E_2[p]$. The canonical filtration is

$$0 \subset \boldsymbol{\alpha}_p \subset E[p], \tag{3.6}$$

with $\boldsymbol{\alpha}_p$ simple of order p, $E[p]$ of order p^2. Note that $E[p]$ is not simple in the category of finite group schemes, but it is simple in the category of BT_1 group schemes, see [Oor05, p. 277]. We will study $E[p]$ in more detail in Section 3.2 – it is the self-dual local-local group scheme $\mathcal{M}_{p^2}$.

Example 3.1.2 ($g = 2$, Example A.3.15 in [Gor02])**.** Let A be a principally polarised abelian surface over an algebraically closed field, so that $A[p]$ is self-dual. There are four possibilities:

(i) A is ordinary. Then we have

$$A[p] \cong (\boldsymbol{\mu}_p \times \mathbb{Z}/p)^2. \tag{3.7}$$

Here $\boldsymbol{\mu}_p^2$ is the kernel of Frobenius and $(\mathbb{Z}/p)^2$ is the kernel of Verschiebung.

(ii) A has étale part of order p. Then

$$A[p] \cong E[p] \times \boldsymbol{\mu}_p \times \mathbb{Z}/p, \tag{3.8}$$

where $E[p]$ is the p-torsion of a supersingular elliptic curve E. By the previous part, $A[p]$ contains a unique embedded $\boldsymbol{\alpha}_p$. The kernel of Frobenius is $\boldsymbol{\alpha}_p \times \boldsymbol{\mu}_p$ and the kernel of Verschiebung is $\boldsymbol{\alpha}_p \times \mathbb{Z}/p$.

(iii) A has no étale part. Then A is supersingular[1] and there are two further cases:

(iiia) A is **superspecial**, which means that A is the product of two supersingular elliptic curves E_1, E_2. Then

$$A[p] \cong E_1[p] \times E_2[p], \tag{3.9}$$

and if k is algebraically closed, then $E_1[p] \cong E_2[p]$ and

$$A[p] \cong E_1[p]^2. \tag{3.10}$$

(iiib) A is not superspecial. Then there is a filtration $\boldsymbol{\alpha}_p \subset G \subset A[p]$, where G fits into non-split short exact sequences

$$0 \to \boldsymbol{\alpha}_p \to G \to \boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_p \to 0 \tag{3.11}$$

and

$$0 \to G \to A[p] \to \boldsymbol{\alpha}_p \to 0. \tag{3.12}$$

The kernel of the Frobenius on G is isomorphic to $\boldsymbol{\alpha}_{p^2}^D$ and we show in Section 3.2.1 that it has Dieudonné module with $F = V^2 = 0$, while the kernel of the Verschiebung is isomorphic to $\boldsymbol{\alpha}_{p^2}$ and has $F^2 = V = 0$.These two kernels are dual to each other. In general, Frobenius and Verschiebung are swapped by Cartier duality, this follows from 1.4.4. There is a non-split exact sequence

$$0 \to \boldsymbol{\alpha}_p \to \boldsymbol{\alpha}_{p^2} \times \boldsymbol{\alpha}_{p^2}^D \to G \to 0. \tag{3.13}$$

Note that neither of $\boldsymbol{\alpha}_{p^2}, \boldsymbol{\alpha}_{p^2}^D$ can be realized as the p-torsion of a supersingular elliptic curve.

[1] Note that for $g \geq 3$ supersingularity implies having no physical torsion but the converse is false.

3.2 Classification over $\overline{\mathbb{F}}_p$

3.2.1 Group schemes of order p^2

Let k be an algerbaically closed field of characteristic p. We want to classify group schemes of order p^2 over k. Note that a similar classification is done in [Wan13], using purely algebraic techniques and without invoking Dieudonné modules. We treat all the cases where a group scheme or its Cartier dual is etalé using Galois theory, as in 1.4.12. In the case of an algebraically closed field the classification is reduced to that of constant commutative group schemes of order p^2. In the local-local case we can use Dieudonné theory as outlined in Chapter 2.
Altogether, we get three types of group schemes:

1. Products of group schemes of order p, i.e., split extensions $\{\mathbb{Z}/p, \boldsymbol{\alpha}_p, \boldsymbol{\mu}_p\} \times \{\mathbb{Z}/p, \boldsymbol{\alpha}_p, \boldsymbol{\mu}_p\}$.

2. Nonsplit extensions of $\boldsymbol{\mu}_p$ by itself and $\mathbb{Z}/p$ by itself. There is only one nonsplit extension of $\mathbb{Z}/p$ by $\mathbb{Z}/p$, namely $\mathbb{Z}/p^2$ and if we are working over an algebraically closed field this corresponds to a unique nonsplit extension of $\boldsymbol{\mu}_p$ by $\boldsymbol{\mu}_p$, which will be the Cartier dual of $\mathbb{Z}/p^2$ and is isomorphic to $\boldsymbol{\mu}_{p^2}$.

3. Nonsplit extensions of $\boldsymbol{\alpha}_p$ by itself. There are three of those and we now classify them.

Local-local nonsplit group schemes correspond to simple Dieudonne modules. A local-local group scheme of order p^2 is neccessarily killed by p – this can be seen by writing down F and V in co-ordinates as matrices, hence its Dieudonné module is a vector space over k. Let M be such a module, i.e., a two-dimensional vector space over k equipped with Frobenius and Verschiebung. Since we are in the local-local setting, both Frobenius and Verschiebung are nilpotent. Up to a change of basis, there are three options:

1. $F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, V = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$;

2. $F = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$;

3. $F = V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

One of the above modules corresponds to $\boldsymbol{\alpha}_{p^2}$. Unlike $\boldsymbol{\alpha}_p$, it is not self-dual.

Proposition 3.2.1. *The group scheme $\boldsymbol{\alpha}_{p^2}$ is not self-dual.*

Proof. The representing k-algebra of $\boldsymbol{\alpha}_{p^2}$ is $A = k[x]/(x^{p^2})$. Let $\{1, x, ..., x^{p^2-1}\}$ be its basis. The Hopf algebra structure on A is given by the following maps (all tensor products over k).

$$\begin{aligned}
\Delta\colon A &\to A \otimes A, && (3.14)\\
x &\mapsto x \otimes 1 + 1 \otimes x, && (3.15)\\
\epsilon\colon A &\to k, && (3.16)\\
x &\mapsto 0, && (3.17)\\
S\colon A &\to A, && (3.18)\\
x &\mapsto -x, && (3.19)\\
m\colon A \otimes A &\to A, && (3.20)\\
x^i \otimes x^j &\mapsto x^{i+j}, && (3.21)\\
\iota\colon k &\to A. && (3.22)
\end{aligned}$$

Let $\{e_0, ..., e_{p^2-1}\}$ be the basis of A^D dual to $\{1, x, ..., x^{p^2}\}$. The multiplication in A^D is given by the map

$$\Delta^D\colon A^D \otimes A^D \to A^D. \tag{3.23}$$

The value $\Delta^D(e_i \otimes e_j)(x^k)$ is calculated as

$$\begin{aligned}
(e_i \otimes e_j)(\Delta(x^k)) &= (e_i \otimes e_j)\Big(\sum_{q=0}^{k} \binom{k}{q} x^q \otimes x^{k-q}\Big) && (3.24)\\
&= \binom{i+j}{i} && (3.25)\\
&= \binom{i+j}{i} e_{i+j}(x^{i+j}) && (3.26)
\end{aligned}$$

and hence

$$e_i e_j = \binom{i+j}{i} e_{i+j}. \tag{3.27}$$

Note that $i+j > p^2$ implies $\binom{i+j}{i} = 0$ in k, so the multiplication formula above makes sense for all $0 \le i, j \le p^2 - 1$. More precisely, if $i + j \ge p^2$, then e_i and e_j are orthogonal. This multiplication makes e_0 the unit element. For $i > 0$ we have

$$\begin{aligned}
e_i^p = \binom{2i}{i} e_{2i} e_i^{p-2} = \binom{2i}{i}\binom{3i}{i} e_{3i} e_i^{p-3} &= \frac{(2i)!}{i!i!}\frac{(3i)!}{i!(2i!)} e_{3i} e_i^{p-3}\\
&= \frac{(3i)!}{(i!)^3} e_{3i} e_i^{p-3} = \cdots = \frac{(pi)!}{(i!)^p} e_{pi}. \qquad (3.28)
\end{aligned}$$

If $p \le i < p^2 - 1$, then $ip \ge p^2$, so $e_{pi} = 0$. If $i < p$, then $p \nmid (i!)^p$, but the

numerator of $\frac{(pi)!}{i!^p}$ has a factor of p, so $\frac{(pi)!}{i!^p} = 0$. We conclude that for all $i > 0$ $e_i^p = 0$. Pick an arbitrary element

$$b = \lambda_0 e_0 + \lambda_1 e_1 + \cdots + \lambda_{p^2-1} e_{p^2-1} \in A^D. \tag{3.29}$$

Taking the pth power and remembering that we are over characteristic p, obtain

$$b^p = \lambda_0^p e_0. \tag{3.30}$$

So $b \in A^D$ is nilpotent if $\lambda_0 = 0$ and is a unit otherwise. We conclude that A^D is isomorphic to $k[x,y]/(x^p, y^p)$. So $A \ncong A^D$, because, for example, in the latter ring the maximal ideal is killed by raising to the power p. In particular, the algebraic group schemes $\boldsymbol{\alpha}_{p^2}$ and $\boldsymbol{\alpha}_{p^2}^D$ are not isomorphic. □

We know that $\boldsymbol{\alpha}_{p^2}$ is not $\boldsymbol{\alpha}_{p^2}^D$, but which module does it correspond to? The ring $k[x]/(x^{p^2})$ is local with the maximal ideal $m = (x)$ and $\dim_k m/m^2 = 1$. Hence $\dim_k M/FM = 1$ and F is not zero, therefore $V = 0$ for $\boldsymbol{\alpha}_{p^2}$. On the other hand, $\boldsymbol{\alpha}_{p^2}^D$ must then have $F = 0$ and V nonzero.
It is also possible to approach the problem of classification directly with modules. Let M be a 2-dimensional Dieudonné module with F, V nilpotent. We start with the easy case when $F = V = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Let $\{t_1, t_2\}$ be a basis. Recall from that 2.6.2 that the corresponding Hopf algebra is generated by $x = T_{t_1}, y = T_{t_2}$ with comultiplication

$$\Delta(T_{t_1}) = S_0(T_{t_1} \otimes 1, 1 \otimes T_{t_1}) = x \otimes 1 + 1 \otimes x, \tag{3.31}$$

$$\Delta(T_{t_2}) = S_0(T_{t_2} \otimes 1, 1 \otimes T_{t_2}) = y \otimes 1 + 1 \otimes y. \tag{3.32}$$

Also note that $T_{Ft_1} = (T_{t_1})^p = 0$ and $T_{Ft_2} = (T_{t_2})^p = 0$. So we get the algebra

$$k[x,y]/(x^p, y^p), \tag{3.33}$$

where both x and y are primitive. This is the group scheme $\boldsymbol{\alpha}_p^2$.
Now let us consider the case when $F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, V = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. We can guess that it will correspond to $\boldsymbol{\alpha}_{p^2}$ because the Frobenius action on this group scheme is nontrivial. Indeed, let $\{t_1, t_2\}$ be a basis, then

$$Vt_1 = Vt_2 = Ft_1 = 0, Ft_2 = t_1. \tag{3.34}$$

The comultiplication is

$$\Delta(T_{t_1}) = S_0(T_{t_1} \otimes 1, 1 \otimes T_{t_1}) = T_{t_1} \otimes 1 + 1 \otimes T_{t_1}, \tag{3.35}$$

$$\Delta(T_{t_2}) = S_0(T_{t_2} \otimes 1, 1 \otimes T_{t_2}) = T_{t_2} \otimes 1 + 1 \otimes T_{t_2}. \tag{3.36}$$

Note that $T_{t_1} = T_{Ft_2} = T_{t_2}^p$, so the algebra is generated by $T_{t_2} = x$. We get the algebra $k[x]/(x^{p^2})$ with x primitive. In other words, we get the group scheme $\boldsymbol{\alpha}_{p^2}$.

We can now recover the dual of $\boldsymbol{\alpha}_{p^2}$ through Dieudonné modules. This will correspond to $V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, F = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so the action is

$$Ft_1 = Ft_2 = 0 = Vt_1 = 0, Vt_2 = t_1. \tag{3.37}$$

The comultiplication is now

$$\begin{aligned}
\Delta(T_1) &= S_1(T_{Vt_1} \otimes 1, T_{t_1} \otimes 1, 1 \otimes T_{Vt_1}, 1 \otimes T_{t_1}), && (3.38)\\
&= S_1(0 \otimes 1, T_{t_1} \otimes 1, 1 \otimes 0, 1 \otimes T_{t_1}), && (3.39)\\
&= T_1 \otimes 1 + 1 \otimes T_1. && (3.40)\\
\Delta(T_2) &= S_1(T_{t_1} \otimes 1, T_{t_2} \otimes 1, 1 \otimes T_{t_1}, 1 \otimes T_{t_2}), && (3.41)\\
&= T_{t_2} \otimes 1 + 1 \otimes T_{t_2} - \frac{1}{p}\sum_{i=1}^{p-1} \binom{p}{i} T_1^{p-i} \otimes T_1^i && (3.42)
\end{aligned}$$

Relabel $T_1 = x, T_2 = y$, $F = 0$ tells us that there is no algebraic relationship between x and y. The Hopf algebra is $k[x, y]/(x^p, y^p)$ with x primitive and

$$\Delta(y) = y \otimes 1 + 1 \otimes y - \frac{1}{p}\sum_{i=1}^{p-1} \binom{p}{i} x^{p-i} \otimes x^i. \tag{3.43}$$

3.2.2 The self-dual local-local group scheme of order p^2.

Finally, we have the local-local self-dual group scheme of order p^2. This group scheme has

$$F = V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \tag{3.44}$$

If $y = T_{t_1}, x = T_{t_2}$ then $Fy = x, Fx = 0, Vy = x, Vx = 0$, so we do get the Hopf algebra $k[z]/(z^{p^2})$, where we identify $y = z, x = z^p$. The comultiplication

is given by

$$\Delta(z) = S_1(z^p \otimes 1, z \otimes 1, 1 \otimes z^p, 1 \otimes z) \tag{3.45}$$

$$= z \otimes 1 + 1 \otimes z - \frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} z^{p^2-pi} \otimes z^{pi} \tag{3.46}$$

We denote this group $\mathcal{M}_{p^2}$. For example $p = 2$ gives

$$x \mapsto x \otimes 1 + 1 \otimes x - x^2 \otimes x^2 \tag{3.47}$$

and $p = 3$ gives

$$x \mapsto x \otimes 1 + 1 \otimes x - x^6 \otimes x^3 - x^3 \otimes x^6. \tag{3.48}$$

Note that $\mathcal{M}_{p^2}$ is isomorphic to $E[p]$, where E is a supersingular elliptic curve over k.

Proposition 3.2.2. *Write the group law as*

$$xy = x + y - f_p(x, y), \tag{3.49}$$

where $f_p(x, y)$ is a polynomial depending on the prime p. Then

$$f_p(x, y) \equiv \frac{\binom{p^2}{p}}{p} x^p y^{p^2-p} + \frac{\binom{p^2}{2p}}{p} x^{2p} y^{p^2-2p} + ... + \frac{\binom{p^2}{p}}{p} x^{p^2-p} y^p \mod p, \tag{3.50}$$

i.e., only $x^i y^j$-terms with $p \mid i$ and $p \mid j$ survive.

Proof. Write $f_p(x, y)$ as

$$f_p(x, y) = \sum_{i=1}^{p^2-1} \frac{\binom{p}{i}}{p} x^i y^{p^2-i} \tag{3.51}$$

and denote $\frac{\binom{p}{i}}{p} =: F_i$. We claim that $F_i \equiv 0 \mod p$ if and only if p divides i. Suppose $i = pj$ for some $0 < j < p$. Then

$$F_i = \frac{\binom{p^2}{pj}}{p} = \frac{p^2!}{(pj)!(p^2 - pj)!p} \tag{3.52}$$

$$= \frac{p^2(p^2-1)...(p^2-p)...(p^2-2p)...(p^2-p(j+1))...(p^2-pj)...}{pj(pj-1)...(pj-p)...(pj-2p)...(p^2-pj)...p} \tag{3.53}$$

$$= \frac{p^2(p^2-1)...(p^2-p)...(p^2-p(j+1))...}{p^2 j(pj-1)...(pj-p)...(p^2-p(j+1)...} \tag{3.54}$$

In the last expression, every factor of p in the numerator comes from $p^2 - pk$ for $1 \leq k \leq j+1$ and it is cancelled by p from $pj - pk$ in the denominator. We

are left with a fraction expression for an integer where both numerator and denominator are not divisible by p, so F_i itself is not divisible by p.
Now assume that p does not divide i. The expression for F_i now reads

$$F_i = \frac{p^2!}{p(i!)(p^2-i)!} \tag{3.55}$$

$$= \frac{p^2(p^2-1)...(p^2-i+1)(p^2-i)...}{pi(i-1)...(p^2-i)...} \tag{3.56}$$

$$= \frac{p(p^2-1)...(p^2-i+1)}{i(i-1)...} \tag{3.57}$$

If $i < p$ then p does not divide $i!$ and the numerator has a factor of p, even of p^2, so $F_i \equiv 0 \mod p$. If $i \geq p$, let n be the biggest natural number such that $i > pn$, so that $i < p(n+1)$. Then

$$F_i = \frac{p(p^2-1)(p^2-2)...(p^2-p)...(p^2-2p)...(p^2-pn)...(p^2-i+1)}{i(i-1)...pn...p(n-1)...p...} \tag{3.58}$$

Altogether there are $n+1$ factors of p in the numerator, coming from $p^2 - jp$ for $1 \leq j \leq n$ and p at the beginning. In the denominator, there are n factors of p, coming from $p, 2p, ..., np$. So F_i is divisible by p. and $F_i \equiv 0 \mod p$. $\square$

3.2.3 Group schemes of order p^3 killed by p.

In a manner similar to the previous section, we only need to consider local-local group schemes of order p^3. We will have the underlying assumption that the group schemes we consider are killed by p. This implies that the underlying Dieudonné modules are vector spaces over $\mathbb{F}_p$, equipped with F, V nilpotent of length at most three. By basic linear algebra, any nilpotent matrix is similar to a direct sum $\bigoplus_{i=1}^{n} S_i$, where each S_i is a canonical nilpotent matrix. The **canonical n-by-n nilpotent matrix** is the matrix that has 1s on the superdiagonal and 0s elsewhere. Hence, up to linear isomorphism, F and V come from the list

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}. \tag{3.59}$$

We need to make sure that $FV = p = 0$ so that the module is a vector space. These correspond to the cases with $F^n = V^m = 0$ and $1 \leq m, n \leq 3$, except for the case $m = n = 3$, for which $FV \neq 0$.
This gives us 9 classes of local-local group schemes. We will also need

$S_2(X_0, X_1, X_2, Y_0, Y_1, Y_2)$, which is equal to

$$X_2+Y_2+\frac{1}{p}(X_1^p+Y_1^p)-\frac{1}{p^2}\left(\sum_{i=1}^{p^2-1}\binom{p^2}{i}X_0^iY_0^{p^2-i}\right)-\frac{1}{p}\left(X_1+Y_1-\frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}X_0^iY_0^{p-i}\right)^p \tag{3.60}$$

Note that

$$S_2(0,0,X_2,0,0,Y_2) = S_0(X_2,Y_2) \tag{3.61}$$

and

$$S_2(0,X_1,X_2,0,Y_1,Y_2) = S_1(X_1,X_2,Y_1,Y_2). \tag{3.62}$$

- Class 1 is $V = F = 0$ and it corresponds to $k[x]/(x^{p^3})$ with x primitive, i.e., $\boldsymbol{\alpha}_p^3$.

- Class 2 is $F^2 \neq 0, F^3 = 0, V = 0$. This is the group scheme $\boldsymbol{\alpha}_{p^3}$, represented by $k[x]/(x^9)$ and x primitive.

- Class 3 is $V^2 \neq 0, V^3 = 0, F = 0$, which is the dual of $\boldsymbol{\alpha}_{p^3}$. This is a group scheme with algebra generated by 3 elements, so $k[x,y,z]/(x^p, y^p, z^p)$. To write out the comultiplication, consider the action of V:

$$Vx = 0, \tag{3.63}$$

$$Vy = x, \tag{3.64}$$

$$Vz = y. \tag{3.65}$$

  Then the comultiplication is

$$\begin{aligned}
\Delta(x) &= S_2(V^2x\otimes 1, Vx\otimes 1, x\otimes 1, 1\otimes V^2x, 1\otimes Vx, 1\otimes x) && (3.66)\\
&= S_2(0\otimes 1, 0\otimes 1, x\otimes 1, 1\otimes 0, 1\otimes 0, 1\otimes x) && (3.67)\\
&= x\otimes 1 + 1\otimes x && (3.68)\\
\Delta(y) &= S_2(V^2y\otimes 1, Vy\otimes 1, y\otimes 1, 1\otimes V^2y, 1\otimes Vy, 1\otimes y) && (3.69)\\
&= S_2(0\otimes 1, x\otimes 1, y\otimes 1, 1\otimes 0, 1\otimes x, 1\otimes y) && (3.70)\\
&= S_1(x\otimes 1, y\otimes 1, 1\otimes x, 1\otimes y) && (3.71)\\
\Delta(z) &= S_2(x\otimes 1, y\otimes 1, z\otimes 1, 1\otimes x, 1\otimes y, 1\otimes z). && (3.72)
\end{aligned}$$

- Class 4 is $F^2 = 0, V = 0$, i.e.,

$$Ft_1 = 0, Ft_2 = t_1, Ft_3 = 0 \tag{3.73}$$

where t_1, t_2, t_3 is a basis of M. The Hopf algebra will have a relation $T_{t_2}^p = T_{t_1}$, so it is generated by $T_{t_1} = x$ and $T_{t_3} = y$ with the algebra structure

$$k[x, y]/(x^{p^2}, y^p) \tag{3.74}$$

and x, y both primitive. We can recognise this class as $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_{p^2}$.

- Class 5 is the dual of class 4, i.e., $V^2 = 0, F = 0$. This gives the Hopf algebra $k[x, y, z]/(x^p, y^p, z^p)$. Let $\{t_1, t_2, t_3\}$ be the corresponding basis of the Dieudonné module, then

$$Vt_1 = 0, Vt_2 = t_1, Vt_3 = 0. \tag{3.75}$$

The comultiplication is

$$\begin{aligned}
\Delta(x) &= S_1(T_{Vt_1} \otimes 1, T_{t_1} \otimes 1, 1 \otimes T_{Vt_1}, 1 \otimes T_{t_1}) && (3.76)\\
&= S_1(0 \otimes 1, x \otimes 1, 1 \otimes 0, 1 \otimes x) && (3.77)\\
&= x \otimes 1 + 1 \otimes x && (3.78)\\
\Delta(y) &= S_1(TVt_2 \otimes 1, T_{t_2} \otimes 1, 1 \otimes T_{Vt_2}, 1 \otimes T_{t_2}) && (3.79)\\
&= S_1(T_{t_1} \otimes 1, T_{t_2} \otimes 1, 1 \otimes T_{t_1}, 1 \otimes T_{t_2}) && (3.80)\\
&= y \otimes 1 + 1 \otimes y + \frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i} && (3.81)\\
\Delta(z) &= S_1(T_{Vt_3} \otimes 1, T_{t_3} \otimes 1, 1 \otimes T_{Vt_3}, 1 \otimes T_{t_3}) && (3.82)\\
&= S_1(0 \otimes 1, z \otimes 1, 1 \otimes 0, 1 \otimes z) && (3.83)\\
&= z \otimes 1 + 1 \otimes z && (3.84)\\
& && (3.85)
\end{aligned}$$

This class is $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_{p^2}^D$.

- Class 6 is the class corresponding to $\boldsymbol{\alpha}_p \times \mathcal{M}_{p^2}$ and is self-dual.

- Class 7 is the first class which gives a 'new' type of a group scheme. Let $F^3 = 0$ and $V^2 = 0$ with basis $\{t_1, t_2, t_3\}$. As always with $F^3 = 0$ the Hopf algebra is $k[x]/(x^{p^3})$, where x corresponds to T_{t_3}. Consequently, we only need the comultiplication for x, which is

$$\begin{aligned}
\Delta(x) &= S_1(x^p \otimes 1, x \otimes 1, 1 \otimes x^p, 1 \otimes x) && (3.86)\\
&= x \otimes 1 + 1 \otimes x + \frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} (x^p)^{p-i} \otimes (x^p)^i && (3.87)
\end{aligned}$$

- Class 8 is the dual of Class 7 with $F^2 = 0, V^3 = 0$. This gives the Hopf algebra $k[x,y]/(x^{p^2}, y^p)$. The action of V is

$$Vt_1 = 0, Vt_2 = t_1, Vt_3 = t_1. \tag{3.88}$$

- Class 9 is self-dual with $F^3 = V^3 = 0$. Its Hopf algebra is $k[x]/(x^{p^3})$ and the comultiplication is

$$\Delta(x) = S_2(x^{p^2} \otimes 1, x^p \otimes 1, x \otimes 1, 1 \otimes x^{p^2}, 1 \otimes x^p, 1 \otimes x). \tag{3.89}$$

Remark. Note that the classification of local-local group schemes of order p^n killed by p is equivalent to classifying pairs of nilpotent linear transformations which multiply to 0. When $n = 1, 2$, or 3 this is particularly easy because a nilpotent matrix in each of these cases is determined by its order. This is no longer the case when $n \geq 4$ For example, we have matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{3.90}$$

which both square to zero but which are not equivalent.

3.3 Local-local group schemes in families.

From the previous section, we know that the local-local group schemes of order p^2 are $\boldsymbol{\alpha}_p^2, \boldsymbol{\alpha}_{p^2}, \boldsymbol{\alpha}_{p^2}^D$, and $\mathcal{M}_{p^2}$. It is possible to put them into a single deformation family, which will be an *unfolding* of $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_p$.

Proposition 3.3.1. *Let $B = \mathbb{Z}[t_1, t_2]$ be the base ring. The algebra $A =$*

$B[x,y]/(x^p, y^p - t_1 x)$ is a Hopf algebra with operations

$$\Delta\colon A \to A \otimes_B A, \tag{3.91}$$
$$x \mapsto x \otimes 1 + 1 \otimes x, \tag{3.92}$$
$$y \mapsto y \otimes 1 + 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i}, \tag{3.93}$$
$$S\colon A \to A, \tag{3.94}$$
$$x \mapsto -x, \tag{3.95}$$
$$y \mapsto -y, \tag{3.96}$$
$$\epsilon\colon A \to B, \tag{3.97}$$
$$x \mapsto 0, \tag{3.98}$$
$$y \mapsto 0. \tag{3.99}$$

Proof. We need to show that three *group-like* axioms hold.
Associativity is encoded in the commutativity of

$$\begin{array}{ccc} A \otimes_B A \otimes_B A & \xleftarrow{id \otimes \Delta} & A \otimes_B A \\ \uparrow{\scriptstyle \Delta \otimes \mathrm{id}} & & \uparrow{\scriptstyle \Delta} \\ A \otimes_B A & \xleftarrow[\Delta]{} & A \end{array}$$

We only need to check this on algebra generators and it is obvious that associativity holds for x, since $\Delta(x)$ represents the operation of addition. So

we need to check it for y:

$$\Delta \otimes \mathrm{id}(\Delta(y)) = \Delta \otimes \mathrm{id}(y \otimes 1 + 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i}) \tag{3.100}$$

$$= (y \otimes 1 + 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-1}) \otimes 1 + 1 \otimes 1 \otimes y \tag{3.101}$$

$$- \frac{t_2^2}{p} \sum_{i=1}^{p-i} \binom{p}{i} \left(\sum_{j=0}^{i} \binom{i}{j} x^{i-j} \otimes x^j \right) \otimes x^{p-i} \tag{3.102}$$

$$= y \otimes 1 \otimes 1 + 1 \otimes y \otimes 1 - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i} \otimes 1 + 1 \otimes 1 \otimes y \tag{3.103}$$

$$- \frac{t_2^2}{p} \sum_{i=1}^{p-1} \sum_{j=0}^{i} \binom{p}{i} \binom{i}{j} x^{i-j} \otimes x^j \otimes x^{p-i} \tag{3.104}$$

$$= y \otimes 1 \otimes 1 + 1 \otimes y \otimes 1 + 1 \otimes 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p} \sum_{j=0}^{i} \binom{p}{i} \binom{i}{j} x^{i-j} \otimes x^j \otimes x^{p-i} \tag{3.105}$$

On the other hand,

$$\mathrm{id} \otimes \Delta(\Delta(y)) = \mathrm{id} \otimes \Delta(y \otimes 1 + 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i}) \tag{3.106}$$

$$= y \otimes 1 \otimes 1 + 1 \otimes (y \otimes 1 + 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i}) \tag{3.107}$$

$$- \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes \Delta(x^{p-i}) \tag{3.108}$$

$$= y \otimes 1 \otimes 1 + 1 \otimes y \otimes 1 + 1 \otimes 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} 1 \otimes x^i \otimes x^{p-i} \tag{3.109}$$

$$- \frac{t_2^2}{p} \sum_{i=1}^{p-1} \sum_{j=0}^{p-i} \binom{p}{i} \binom{p-i}{j} x^i \otimes x^{p-i-j} \otimes x^j \tag{3.110}$$

$$= y \otimes 1 \otimes 1 + 1 \otimes y \otimes 1 + 1 \otimes 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p} \sum_{j=0}^{p-i} \binom{p}{i} \binom{p-i}{j} x^i \otimes x^{p-i-j} \otimes x^j \tag{3.111}$$

The two polynomials

$$\frac{t_2^2}{p}\sum_{i=1}^{p}\sum_{j=0}^{i}\binom{p}{i}\binom{i}{j}x^{i-j}\otimes x^j\otimes x^{p-i} \tag{3.112}$$

and

$$\frac{t_2^2}{p}\sum_{i=1}^{p}\sum_{j=0}^{p-i}\binom{p}{i}\binom{p-i}{j}x^{i}\otimes x^{p-i-j}\otimes x^j \tag{3.113}$$

are equal. Indeed, the (i,j)-summand of the first one is

$$\binom{p}{i}\binom{i}{j}x^{i-j}\otimes x^j\otimes x^{p-i}, \tag{3.114}$$

whereas the $(j,p-i)$-summand of the second one is

$$\binom{p}{j}\binom{p-j}{p-i}x^{i-j}\otimes x^j\otimes x^{p-i}, \tag{3.115}$$

with

$$\binom{p}{i}\binom{i}{j}=\binom{p}{j}\binom{p-j}{p-i} \tag{3.116}$$

which is the Subset-of-a-subset identity for binomial coefficients.
The existence of an identity corresponds to the commutativity of

$$\begin{array}{ccc} B\otimes_B A & \xleftarrow{\epsilon\otimes \mathrm{id}} & A\otimes_B A \\ \cong\uparrow & & \uparrow\Delta \\ A & \xleftarrow[=]{} & A \end{array}$$

We need to look at what happens to y only:

$$\epsilon\otimes\mathrm{id}(\Delta(y))=\epsilon\otimes\mathrm{id}(y\otimes 1+1\otimes y-\frac{t_2^2}{p}\sum_{i=1}^{p-1}\binom{p}{i}x^i\otimes x^{p-i})=1\otimes y, \tag{3.117}$$

which is where y gets sent under the isomorphism

$$A\to B\otimes_B A, \tag{3.118}$$

$$a\mapsto 1\otimes a. \tag{3.119}$$

Finally, we need

$$\begin{array}{ccc} A & \xleftarrow{(S,\mathrm{id})} & A \otimes_B A \\ \uparrow & & \uparrow{\scriptstyle \Delta} \\ B & \xleftarrow[\epsilon]{} & A \end{array}$$

to be commutative. We have

$$(S,\mathrm{id})(\Delta(y)) = (S,\mathrm{id})(y\otimes 1+1\otimes y-\frac{t_2^2}{p}\sum_{i=1}^{p-1}\binom{p}{i}x^i\otimes x^{p-i}) = -y+y-\frac{t_2^2}{p}\sum_{i=1}^{p-1}\binom{p}{i}(-1)^i x^p = 0 \tag{3.120}$$

and

$$\epsilon(y) = 0. \tag{3.121}$$

□

We can reduce the coefficients of the group scheme above mod p, so that we get a family over $\mathbb{F}_p[t_1, t_2]$.

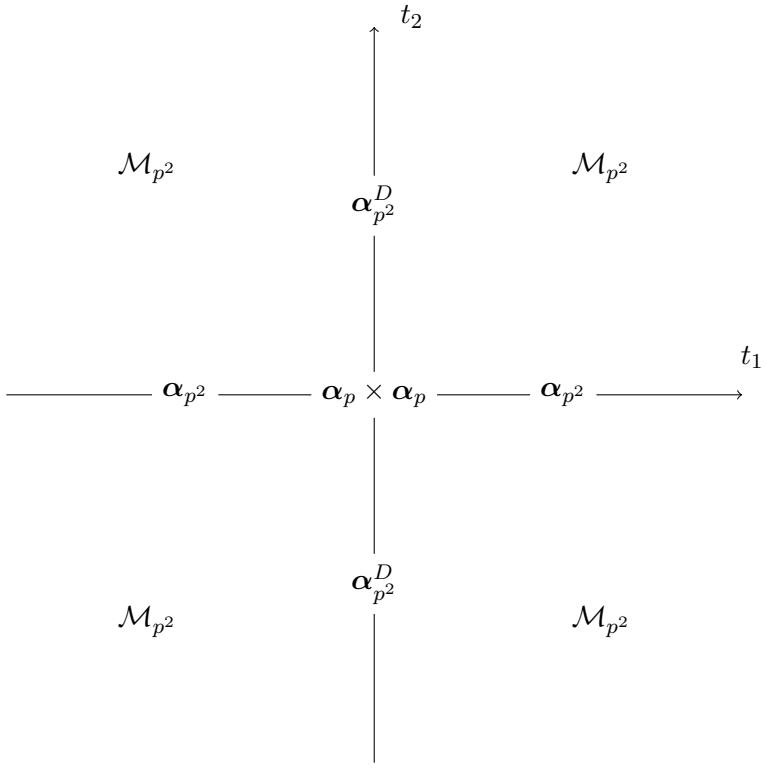


Figure 3.1: An unfolding of $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_p$

Proposition 3.3.2. *Let k be an algebraically closed field of characteristic p. The group scheme* $\operatorname{Spec} k[x, y, t_1, t_2]/(x^p, y^p - t_1 x)$ *is a family of group schemes*

of local-local type over $\operatorname{Spec} k[t_1, t_2] = \mathbb{A}^2_k$. *The affine plane is stratified into four components:*

1. *Over the locus where* t_1 *and* t_2 *are both invertible, the geometric fibres are isomorphic to* $\mathcal{M}_{p^2}$.
2. *Over the locus where* $t_2 = 0$ *and* t_1 *is invertible, the geometric fibres are isomorphic to* $\boldsymbol{\alpha}_{p^2}$.
3. *Over the locus where* $t_1 = 0$ *and* t_2 *is invertible, the geometric fibres are isomorphic to* $\boldsymbol{\alpha}^D_{p^2}$.
4. *Over the point* $t_1 = t_2 = 0$ *the geometric fibre is isomorphic to* $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_p$.

We call this group scheme the **local-local Tate-Oort group scheme of order** p^2 *and denote it by* $\mathbb{TO}^{ll}_{p^2}$.

Proof. Recall that the comultiplication is

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \tag{3.122}$$

$$\Delta(y) = y \otimes 1 + 1 \otimes y - \frac{t_2^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i}. \tag{3.123}$$

With t_1, t_2 both invertible, we have $y^p = t_1 x$, so the group scheme is isomorphic to $\mathbb{F}_p[y]/(y^{p^2})$ with comultiplication making it into a copy of $\mathcal{M}_{p^2}$. The other cases are similar. □

Corollary 3.3.3. *Fix* $(t_1, t_2) \in \mathbb{A}^2_k$ *and consider the corresponding finite flat group scheme* G_{t_1,t_2}. *The Cartier dual of this group scheme is given by*

$$G^D_{t_1,t_2} = G_{t_2,t_1}, \tag{3.124}$$

i.e., the dual of G_{t_1,t_2} *is the group scheme represented by* $k[x, y, t_1, t_2]/(x^p, y^p - t_2 x)$ *and comultiplilcation where* x *is primitive and*

$$\Delta(y) = y \otimes 1 + 1 \otimes y - \frac{t_1^2}{p} \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i}. \tag{3.125}$$

It follows that the Cartier duality action on these group schemes induces the action on the plane $\mathbb{A}^2_k$ *which is given by the matrix* $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

3.4 Small Tate-Oort scheme of order p^2.

We start with this case to prepare for the more complicated case of the deformation family of all group schemes of order p^2. The small Tate-Oort

group scheme $\mathbb{TO}^s_{p^2}$ will be a deformation family of the groups $\boldsymbol{\alpha}_{p^2}$ and $\boldsymbol{\mu}_{p^2}$. This construction closely follows the construction of Reid in [Rei19].
The group schemes $\boldsymbol{\alpha}_{p^2}$ and $\mathbb{Z}/p^2$ are closed subschemes of $\mathbb{G}_a$, while $\boldsymbol{\mu}_{p^2}$ is a closed subscheme of $\mathbb{G}_m$. Reid defines a hybrid additive-multiplicative group scheme $\mathbb{G}$ as $\operatorname{Spec} A$, where $A = B[x, \frac{1}{1+tx}]$, for B any base ring and $t \in B$ arbitrary. The Hopf algebra structure on A is given by

$$\Delta(x) = x \otimes 1 + 1 \otimes x + tx \otimes x. \tag{3.126}$$

The scheme $\operatorname{Spec} B$ is stratified into two components

$$\operatorname{Spec} B = D(t) \cup V(t) = \operatorname{Spec} B_t \cup \operatorname{Spec} B/t \tag{3.127}$$

and above the open subscheme $D(t)$ the scheme $\mathbb{G}$ is isomorphic to $\mathbb{G}_m$ via $x \mapsto 1 + tx$ and above the closed subscheme $V(t)$ the scheme $\mathbb{G}$ is isomorphic to $\mathbb{G}_a$.
Define the **given representation** of $\mathbb{G}$ to be

$$\rho_{\text{giv}}(R) \colon \mathbb{G}(R) \to \mathrm{GL}_2(R), \tag{3.128}$$

$$x \mapsto \begin{pmatrix} 1 & 0 \\ x & 1+tx \end{pmatrix}, \tag{3.129}$$

where R is a B-algebra.

Definition 3.4.1. Let p be a prime number and $B = \mathbb{Z}[S,t]/(St^{p^2-1} + p)$ a base ring. The **small Tate-Oort group scheme** $\mathbb{TO}^s_{p^2}$ of order p^2 is defined as the subscheme of $\operatorname{Spec} B[x]$ cut out by

$$x^{p^2} - Sg_p(t,x), \tag{3.130}$$

where

$$g_p(t,x) = \frac{(1+tx)^p - 1 - t^p x^p}{pt}. \tag{3.131}$$

Proposition 3.4.2. *Inside the co-ordinate ring of $\mathbb{TO}^s_{p^2}$ we have the relation.*

$$(1+tx)^p = 1. \tag{3.132}$$

3.5 Tate-Oort group scheme $\mathbb{TO}^l_{p^2}$

The group scheme $\mathbb{TO}^l_{p^2}$ is a deformation family that includes local group schemes of order p^2. Let

$$B = \mathbb{Z}[w_1, w_2]/(w_1 w_2^{p^2-1} + p) \tag{3.133}$$

be the base ring. Consider the scheme

$$\mathbb{G}_{B,t_1,t_2} = \operatorname{Spec} B[x_1, x_2, \frac{1}{1+w_1x}, \frac{1}{1+w_2y}, t_1, t_2] \tag{3.134}$$

The **Tate-Oort group scheme** $\mathbb{TO}^l_{p^2}$ is defined as the closed subscheme of $\mathbb{G}_{B,t_1,t_2}$ with ideal generated by

$$x^p.y^p - t_1x \tag{3.135}$$

The Hopf algebra structure on the function ring A of $\mathbb{TO}^l_{p^2}$ is defined as:

$$\Delta : A \to A \otimes A, \tag{3.136}$$

$$x \mapsto x \otimes 1 + 1 \otimes x + w_2x \otimes x, \tag{3.137}$$

$$y \mapsto y \otimes 1 + 1 \otimes y + w_1y \otimes y - \frac{t_2^2}{p}\sum_{i=1}^{p-1}\binom{p}{i}x^i \otimes x^{p-i}, \tag{3.138}$$

$$S : R \to R, \tag{3.139}$$

$$x \mapsto \frac{-x}{1+w_1x}, \tag{3.140}$$

$$y \mapsto \frac{-y}{1+w_2y}, \tag{3.141}$$

$$\epsilon : R \to B, \tag{3.142}$$

$$x \mapsto 0, \tag{3.143}$$

$$y \mapsto 0 \tag{3.144}$$

Proposition 3.5.1. *The group scheme $\mathbb{TO}^l_{p^2}$ is a deformation family that includes all local group schemes of order p^2 over k that exist:*

- *Setting $t_1 = t_2 = 0$ gives $\mathbb{TO}^l_p \times \mathbb{TO}^l_p$, which contains split extensions of local group schemes of order p, i.e., $s = t = 0$ gives $\boldsymbol{\alpha}_p^2$, w_1 invertible $w_2 = 0$ gives $\boldsymbol{\mu}_p \times \boldsymbol{\alpha}_p$, $w_1 = 0$ w_2 invertible gives $\boldsymbol{\alpha}_p \times \boldsymbol{\mu}_p$ and w_1, w_2 invertible gives $\boldsymbol{\mu}_p^2$.*
- *Over the locus where t_1 is invertible and $t_2 = 0$ we can have w_1, w_2 both invertible, so that geometric fibres are isomorphic to $\boldsymbol{\mu}_p^2$ and over the point $w_1 = w_2 = 0$ the fibre is $\boldsymbol{\alpha}_{p^2}$.*
- *Over the locus where $t_1 = 0, t_2$ invertible, the only possibility is $w_1 = w_2 = 0$, so the fibre is $\boldsymbol{\alpha}^D_{p^2}$.*
- *Over the locus where t_1, t_2 are both invertible, the only possibility is $w_1 = w_2 = 0$ so the fibre is isomorphic to $\mathcal{M}_{p^2}$.*

The group scheme $\mathbb{TO}^l_{p^2}$ has a representation theory similar to that of $\mathbb{TO}_p$ – we can figure out invariants of action by considering multiplicative group

schemes like $\boldsymbol{\mu}_{p^2}$ or $\boldsymbol{\mu}_p^2$ and then this should give invariants for all other group schemes in the family. The only difference is that we do not include the étale group schemes $\mathbb{Z}/p^2$ and $\mathbb{Z}/p \times \mathbb{Z}/p$, so there is no description of how Cartier duality works in this case. Note however that setting $s = t = 0$ allows us to recover the unfolding of $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_p$ from Figure 3.1.

Chapter 4

Invariant theory of Tate-Oort group schemes and geometric applications

4.1 Actions of $\mathbb{TO}_p$

This section introduces the Tate-Oort group schemes which is an example of a group scheme discovered by Reid in [Rei19]. Recall that over an algebraically closed field k of positive characteristic p, there are three isomorphism classes of group schemes of order p:

$$\boldsymbol{\alpha}_p, \boldsymbol{\mu}_p, \mathbb{Z}/p. \tag{4.1}$$

The Tate-Oort group scheme puts them into a single deformation family. Note that $\boldsymbol{\alpha}_p$ and $\boldsymbol{\mu}_p$ are isomorphic as schemes over k and that $\boldsymbol{\alpha}_p$ and $\mathbb{Z}/p$ share the same multiplication law, i.e., they are both subgroup schemes of $\mathbb{G}_a$, whereas $\boldsymbol{\mu}_p$ is a subgroup scheme of $\mathbb{G}_m$.
In the first step, we put $\mathbb{G}_{a,\mathbb{Z}}$ and $\mathbb{G}_{m,\mathbb{Z}}$ into a family over $\operatorname{Spec}\mathbb{Z}$. Choose $t \in \mathbb{Z}$ and let $A = \mathbb{Z}[x, \frac{1}{1+tx}]$. We put a Hopf algebra structure on A by defining

$$\begin{aligned}
\Delta : A &\to A \otimes_{\mathbb{Z}} A, && (4.2)\\
x &\mapsto x \otimes 1 + 1 \otimes x + tx \otimes x, && (4.3)\\
S : A &\to A, && (4.4)\\
x &\mapsto \frac{-1}{1+tx}, && (4.5)\\
\epsilon : A &\to B, && (4.6)\\
x &\mapsto 0. && (4.7)
\end{aligned}$$

The group scheme $\mathbb{G} = \operatorname{Spec} A$ is isomorphic to $\mathbb{G}_m$ over the locus where t is invertible, i.e., over $\operatorname{Spec} \mathbb{Z}[t, t^{-1}]$ and is isomorphic to $\mathbb{G}_a$ over the locus where $t = 0$, i.e., over $\operatorname{Spec} \mathbb{Z}/(t)$. The group scheme is defined over $\mathbb{Z}$, hence it can be defined over any base ring B.

Definition 4.1.1. The **given representation** M of $\mathbb{G}$ is defined as

$$\mathbb{G} = \left\{ \begin{pmatrix} 1 & 0 \\ x & 1+tx \end{pmatrix} \right\} \subset \operatorname{GL}_2 \mathbb{Z}. \tag{4.8}$$

The group scheme $\mathbb{TO}_p$ is defined as a p-torsion subgroup scheme of $\mathbb{G}$. It comes in two flavours: characteristic p and mixed characteristic. We will focus on mixed characteristic case here. Let the base be $B = \mathbb{Z}[S, t]/(P)$, where $P = St^{p-1} + p$. Define $\mathbb{TO}_p$ by $(F = 0) \subset \mathbb{G}$, where $F = x^p - Sf_p(t, x)$ and

$$f_p(t, x) = \frac{(1+tx)^p - 1 - t^p x^p}{pt}. \tag{4.9}$$

For example, $p = 2$ gives $F = x^2 - Sx$, $p = 3$ gives $F = x^3 - S(tx^2 + x)$ and so on. The main property and the point of these polynomials is that

$$(1+tx)^p \equiv 1 \mod (F, P). \tag{4.10}$$

This allows us to search for $\mathbb{TO}_p$-invariant polynomials.

Example 4.1.2. [5.3 Rei19] Consider $\mathbb{P}^2_{B\langle u_0,u_1,u_2\rangle}$, the projective plane over B with the u_i homogeneous generators of the co-ordinate ring. Let $\mathbb{TO}_3$ act on $\mathbb{P}^2_{B\langle u_0,u_1,u_2\rangle}$ by $\operatorname{Sym}^2 M$, where M is the given representation. On the level of algebras the action is given by

$$B[u_0, u_1, u_2] \to B[u_0, u_1, u_2] \otimes_B B[x, \frac{1}{1+tx}]/(P, F), \tag{4.11}$$

$$(u_0, u_1, u_2) \mapsto (u_0, u_1, u_2) \begin{pmatrix} 1 & 0 & 0 \\ x & 1+tx & 0 \\ x^2 & 2x(1+tx) & (1+tx)^2 \end{pmatrix}. \tag{4.12}$$

More precisely,

$$u_0 \mapsto u_0 + xu_1 + x^2 u_2, \tag{4.13}$$

$$u_1 \mapsto (1+tx)u_1 + 2x(1+tx)u_2, \tag{4.14}$$

$$u_2 \mapsto (1+tx)^2 u_2. \tag{4.15}$$

The action diagonalises over $\operatorname{Spec} B[\frac{1}{t}]$ with eigenvectors

$$v_0 = u_0, \tag{4.16}$$

$$v_1 = u_0 + tu_1, \tag{4.17}$$

$$v_2 = u_0 + 2tu_1 + t^2u_2, \tag{4.18}$$

corresponding to eigenvalues $1, (1+tx), (1+tx)^2$ respectively.
Denote $1 + tx = \tau$. We will now calculate the ring of invariants with respect to this $\mathbb{TO}_3$-action. We first work with various bases of monomials in the v_i and then move to monomial bases in the u_i.
In degree 1 the action is given by $\mathrm{diag}(1, \tau, \tau^2)$, which gives the only invariant linear form $v_0 = u_0$. In degree 2 the action is $\mathrm{diag}(1, \tau, \tau^2, \tau^2, 1, \tau)$ which has two corresponding monomials: $v_0^2 = u_0^2$ and v_1v_2. We write out v_1v_2 in terms of the u_i to get

$$\begin{aligned} v_1v_2 - v_0^2 &= (u_0 + tu_1)(u_0 + 2tu_1 + t^2u_2) && (4.19)\\ &= 3tu_0u_1 + t^2u_0u_2 + 2t^2u_1^2 + t^3u_1u_2 && (4.20) \end{aligned}$$

Substitute $3 \mapsto -St^2$ to get

$$-St^2u_0u_1 + t^2u_0u_2 + 2t^2u_1^2 + t^3u_1u_2 \tag{4.21}$$

and cancel t^2 to get an invariant

$$(u_0u_2 + 2u_1^2) + tu_1u_2 - Su_0u_1. \tag{4.22}$$

The action on cubic forms is given by

$$\mathrm{Sym}^3 \mathrm{diag}(1, \tau, \tau^2) = \mathrm{diag}(1, \tau, \tau^2, \tau^2, 1, \tau^2, 1, \tau, \tau^2, 1). \tag{4.23}$$

We can now read off invariant cubics – these correspond to 1's on the diagonal, so we get $v_0^3, v_0v_1v_2, v_1^3, v_2^3$.

Remark. We implicitly order monomials by degree with $v_0 > v_1 > v_2$, but of course any other ordering of the monomials would give us the same invariant cubics.

Now we need to write down the invariant cubics in terms of the original basis. We have

$$v_0^3 = u_0^3 = f_0, \tag{4.24}$$

which gives us the first invariant cubic. For the second invariant cubic consider

$$\begin{aligned} v_0v_1v_2 - v_0^3 &= 3tu_0^2u_1 + t^2u_0^2u_2 + 2t^2u_0u_1^2 + t^3u_0u_1u_2 && (4.25)\\ &= -St^3u_0^2u_1 + t^2u_0^2u_2 + 2t^2u_0u_1^2 + t^3u_0u_1u_2 && (4.26)\\ & && (4.27)\end{aligned}$$

where replace $3 \mapsto -St^2$ which is the relation given by $P = St^2 - 3$. Now cancel t^2 to get the second invariant

$$f_1 = (2u_0u_1^2 + u_0^2u_2) + tu_0u_1u_2 - Stu_0^2u1 \tag{4.28}$$

We get the third invariant cubic in a similar fashion:

$$\begin{aligned} v_1^3 - v_0^3 &= (u_0 + tu_1)^3 - u_0^3 && (4.29)\\ &= 3tu_0^2u_1 + 3t^2u_0u_1^2 + t^3u_1 && (4.30)\\ &= -St^3u_0^2u_1 - St^4u_0u_1^2 + t^3u_1^3 && (4.31)\end{aligned}$$

and cancel t^3 to get

$$f_2 = u_1^3 - S(u_0^2u_1 + tu_0u_1^2). \tag{4.32}$$

Finally, the last invariant is obtained from starting with

$$\begin{aligned} v_2^3 - v_0^3 =&(u_0 + 2tu_1 + t^2u_2)^3 - u_0^3 && (4.33)\\ =&t^6u_2^3 + 6t^5u_1u_2^2 + 3t^4u_0u_2^2 + 12t^4u_1^2u_2 + 8t^3u_1^3 && (4.34)\\ &+ 12t^4u_1^2u_2 + 8t^3u_1^3 + 12t^3u_0u_1u_2 + 12t^2u_0u_1^2 + 3t^2u_0^2u_2 + 6tu_0^2u_1 && (4.35)\\ =&t^6u_2^3 - 2St^7u_1u_2^2 - St^6u_0u_2^2 - 4St^6u_1^2u_2 + 8t^3u_1^3 && (4.36)\\ &- 4St^5u_0u_1u_2 - 4St^4u_0u_1^2 - St^4u_0^2u_2 - 2St^3u_0^2u_1 && (4.37)\end{aligned}$$

We want to cancel the factor of t^6, but some summands only have factors of lower powers of t. To get rid of those, we consider

$$v_2^3 - v_0^3 - 8(v_1^3 - v_0^3) + 6(v_0v_1v_2 - v_0^3) = t^6u_2^3 + 6t^5u_1u_2^2 + 3t^4u_0u_2^2 + 12t^4u_1^2u_2 + 18t^3u_0u_1u_2 + 9t^2u_0^2u_2. \tag{4.38}$$

Now we can substitute $3 \mapsto -St^3$ and get the last invariant

$$f_3 = u_2^3 - S(u_0u_2^2 + 4u_1^2u_2 + 2tu_1u_2^2) + S^2(u_0^2u_2 + 2tu_0u_1u_2). \tag{4.39}$$

We can consider a relative elliptic curve

$$E\colon (f_0 + f_1 + f_2 + f_3 = 0) \subset \mathbb{P}^2_B. \tag{4.40}$$

In characteristic 0 E is the Hesse cubic and in characteristic 3 we get a supersingular elliptic curve.
Altogether, over the fibre $S = t = 3 = 0$ the invariant ring has the following generators in degrees up to 3:

Degree	Generators
1	u_0
2	$u_0^2, u_0u_2 + 2u_1^2$
3	$u_0^3, u_0^2u_2 + 2u_0u_1^2, u_1^3, u_2^3$

Example 4.1.3. [5.3 Rei19] We start with $\mathbb{TO}_2$ and we try to produce an action on $\mathbb{P}(1,1,2)_{(u_0,u_1,w)}$. The action on linear terms is given by

$$\begin{pmatrix} 1 & 0 \\ x & 1+tx \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \tag{4.41}$$

and the action on quadratic terms is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ x & 1+tx & 0 & 0 \\ x^2 & 2x(1+tx) & (1+tx)^2 & 0 \\ x^3 & 3x^2(1+tx) & 3x(1+tx)^2 & (1+tx)^3 \end{pmatrix} \begin{pmatrix} u_0^2 \\ u_0u_1 \\ u_1^2 \\ w \end{pmatrix} \tag{4.42}$$

which we need to specify because of the presence of w. We act on the graded ring $A = \mathbb{Z}[u_0, u_1, v]$ and want to figure out the subring $A^{\mathbb{TO}_2}$ of invariants of this action.
Define polynomials

$$v_0 = u_0, \tag{4.43}$$

$$v_1 = u_0 + tu_1, \tag{4.44}$$

$$q = u_0^2 + 3tu_0u_1 + 3t^2u_1^2 + t^3w. \tag{4.45}$$

These polynomials and their products will diagonalise the group action in various degrees.
We start with degree 1. In the basis $\{v_0, v_1\}$, the group action diagonalises as $\mathrm{diag}(1, \tau)$, which gives us the only invariant linear form $v_0 = u_0$.
In degree 2, we have eigenforms $(v_0^2, v_0v_1, v_1^2, q)$ which diagonalise the action to $\mathrm{diag}(1, \tau, \tau^2, \tau^3)$, with τ^2 corresponding to v_1^2 and giving us the new invariant

in degree 2:

$$v_1^2 - v_0^2 = (u_0 + tu_1)^2 \tag{4.46}$$
$$= 2tu_0u_1 + t^2u_1^2 \tag{4.47}$$
$$= -St^2u_0u_1 + t^2u_1^2 \tag{4.48}$$

Cancel t^2 to get

$$u_1^2 - Su_0u_1. \tag{4.49}$$

In degree 3 we act on the basis $(v_0^3, v_0^2v_1, v_0v_1^2, v_1^3, v_0w, v_1w)$ by the matrix $\mathrm{diag}(1, \tau, \tau^2, \tau^3, \tau^3, \tau^4)$. The only new invariant, i.e., not the product of invariants of degrees 1 and 2, is u_1w. We write it out:

$$v_1w - v_0^3 = (u_0 + tu_1)(u_0^2 + 3tu_0u_1 + 3t^2u_1^2 + t^3w) \tag{4.50}$$
$$= t^4u_1w + t^3u_02 + 3t^3u_1^3 + 6t^2u_0u_1^2 + 4tu_0^2u_1 \tag{4.51}$$
$$= t^4u_1w + t^3u_02 + 3t^3u_1^3 - 3St^3u_0u_1^2 + S^2t^3u_0^2u_1 \tag{4.52}$$

Cancel t^3 to get

$$(u_0w + 3u_1^3) + tu_1w - 3Su_0u_1^2 + S^2u_0^2u_1. \tag{4.53}$$

In degree 4 we have eigenforms $(v_0^4, v_0^3v_1, v_0^2v_1^2, v_0v_1^3, q^2, v_0^2q, v_0v_1q, v_1^2q)$ on which the group acts as $\mathrm{diag}(1, \tau, \tau^2, \tau^3, \tau^4, \tau^6, \tau^3, \tau^4, \tau^5)$. This gives us only one new invariant, corresponding to the eigenvalue $\tau^6 = 1$, namely q^2. We have

$$q^2 - u_0^4 = (u_0^2 + 3tu_0u_1 + 3t^2u_1^2 + t^3w)^2 \tag{4.54}$$
$$= t^6w^2 + 6t^5u_1^2w + 6t^4u_0u_1w + 9t^4u_1^4 + 2t^3u_0^2w + 18t^3u_0u_1^3 + 15t^2u_0^2u_1^2 + 6tu_0^3u_1 \tag{4.55}$$

and in order to proceed, we need to add linear multiples of other invariant forms – this is because we want to cancel as high power of t as possible. We want to add integer multiples of other invariant quartics, these are:

$$v_0^4, v_1^4, v_0^2v_1^2, v_0v_1^3, v_0v_1q \tag{4.56}$$

In order to proceed, we will write out these polynomials in a table:

	q^2	v_0v_1q	v_1^4	$v_0v_1^3$	$v_0^2v_1^2$
w^2	t^6				
u_1^2w	$6t^5$				
u_0u_1w	$6t^4$	t^4			
u_1^4	$9t^4$		t^4		
u_0^2w	$2t^3$	t^3			
$u_0u_1^3$	$18t^3$	$3t^3$	$4t^3$	t^3	
$u_0^2u_1^2$	$15t^2$	$6t^2$	$6t^2$	$3t^2$	t^2
$u_0^3u_1$	$6t$	$4t$	$4t$	$3t$	$2t$

Now we need to do a balancing exercise – increase the degree (in t) of each coefficient of q^2 until it is 6, or as high as possible if 6 cannot be achieved. We start with u_0u_1w, which has coefficient $6t^4$ and which can only be modified by adding an integer multiple of v_0v_1q. One choice is to do $q^2 - 2v_0v_1q$ to get

	$q^2 - 2v_0v_1q$	v_0v_1q	v_1^4	$v_0v_1^3$	$v_0^2v_1^2$
w^2	t^6				
u_1^2w	$6t^5$				
u_0u_1w	$4t^4$	t^4			
u_1^4	$9t^4$		t^4		
u_0^2w		t^3			
$u_0u_1^3$	$12t^3$	$3t^3$	$4t^3$	t^3	
$u_0^2u_1^2$	$3t^2$	$6t^2$	$6t^2$	$3t^2$	t^2
$u_0^3u_1$	$-2t$	$4t$	$4t$	$3t$	$2t$

Next we look at u_1^4 and its coefficient $9t^4$, which we want to make into $8t^4$. This can be achieved by subtracting v_1^4:

	$q^2 - 2v_0v_1q - v_1^4$	v_0v_1q	v_1^4	$v_0v_1^3$	$v_0^2v_1^2$
w^2	t^6				
u_1^2w	$6t^5$				
u_0u_1w	$4t^4$	t^4			
u_1^4	$8t^4$		t^4		
u_0^2w		t^3			
$u_0u_1^3$	$8t^3$	$3t^3$	$4t^3$	t^3	
$u_0^2u_1^2$	$-3t^2$	$6t^2$	$6t^2$	$3t^2$	t^2
$u_0^3u_1$	$-6t$	$4t$	$4t$	$3t$	$2t$

Finally, we balance $-3t^2$ and $-6t$, the coefficients or $u_0^2u_1^2$ and $u_0^3u_1$ respectively, by adding $3v_0^2v_1^2$:

	$q^2-2v_0v_1q-v_1^4+3v_0^2v_1^2$	v_0v_1q	v_1^4	$v_0v_1^3$	$v_0^2v_1^2$
w^2	t^6				
u_1^2w	$6t^5$				
u_0u_1w	$4t^4$	t^4			
u_1^4	$8t^4$		t^4		
u_0^2w		t^3			
$u_0u_1^3$	$8t^3$	$3t^3$	$4t^3$	t^3	
$u_0^2u_1^2$		$6t^2$	$6t^2$	$3t^2$	t^2
$u_0^3u_1$		$4t$	$4t$	$3t$	$2t$

We are left with

$$q^2-2v_0v_1q-v_1^4+3v_0^2v_1^2 = t^6w^2+6t^5u_1^2w+4t^4u_0u_1w+8t^4u_1^4+8t^3u_0u_1^3. \quad (4.57)$$

We can substitute $2=-St, 4=S^2t^2, 8=-S^3t^3$ and cancel t^6 to get the last invariant

$$w^2-3Su_1^2w+S^2u_0u_1w-S^3(tu_1^4+u_0u_1^3). \quad (4.58)$$

The fibre over $S=t=2$ is $\boldsymbol{\alpha}_2$ and the invariant ring with respect to this group scheme has generators u_0, u_1^2, u_0v, v^2 in degrees 1,2,3,4 respectively.

4.2 Actions of $\mathbb{TO}^s_{p^2}$.

Example 4.2.1. Consider $\mathbb{P}^3_{[u_0,u_1,u_2,u_3]}$, the projective space over the ring $B=\mathbb{Z}[S,t]/(St^3-2)$. We will act by $\mathbb{TO}^s_4$. Recall the given representation

$$\begin{pmatrix} 1 & 0 \\ x & 1+tx \end{pmatrix}. \quad (4.59)$$

We act on linear forms by the symmetric fourth power of the given representation, i.e., by

$$\mathrm{Sym}^4(M) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x & 1+tx & 0 & 0 \\ x^2 & 2x(1+tx) & (1+tx)^2 & 0 \\ x^3 & 3x^2(1+tx) & 3x(1+tx)^2 & (1+tx)^3 \end{pmatrix} \quad (4.60)$$

The calculation will proceed with some help from computer algebra, see Appendix B for the MAGMA code. One function that we will repeatedly use is

```
inv_mon(n,L)
```

which takes a diagonalised action in form of a list L and an integer $n \geq 1$ and outputs invariant monomials of degree n. We want to figure out what

the invariant ring $B[u_0, u_1, u_2, u_3]^{\mathbb{TO}_4}$ is. The action is diagonalised to $D = \mathrm{diag}(1, \tau, \tau^2, \tau^3)$ (where $\tau = 1 + tx$) with respect to the basis

$$v_0 = u_0, \tag{4.61}$$

$$v_1 = u_0 + tu_1, \tag{4.62}$$

$$v_2 = u_0 + 2tu_1 + t^2u_2, \tag{4.63}$$

$$v_3 = u_0 + 3tu_1 + 3t^2u_2 + t^3u_3. \tag{4.64}$$

There is only one linear invariant form, that is $v_0 = u_0$.
In degree 2 the action is $\mathrm{Sym}^2(D)$. We call

```
R<t>:=PolynomialRing(Rationals());
R<t>:=quo<R | t^4-1>;
inv_mon(2,L);
```

which gives us the output

```
[
    v_0^2,
    v_1*v_3,
    v_2^2
]
```

The last two polynomials are written out in a table – this way makes it easier to cancel powers of t. The rows are labelled monomials in u_i and the columns are labeled by invariant polynomials in v_i.

	$v_1v_3 - v_0^2$	$v_2^2 - v_0^2$
u_1u_3	t^4	
u_2^2		t^4
u_1u_2	$3t^3$	$4t^3$
u_0u_3	t^3	
u_1^2	$3t^2$	$4t^2$
u_0u_2	$3t^2$	$2t^2$
u_0u_1	$4t$	$4t$

We cannot cancel t^3 starting with v_1v_3 because of the monomial u_0u_3 – it is not present in $v_2^2 - v_0^2$. But we can cancel t^2 by substituting $4 = S^2t^6$. However,

we can cancel t^4 in $v_2^2 - v_0^2$. Altogether, we get two invariant quadratics

$$v_0^2 = u_0^2 \tag{4.65}$$

$$v_1 v_3 = 3(u_1^2 + u_0 u_2) + 3t u_1 u_2 + t u_0 u_3 + t^2 u_1 u_3 + S^2 t^6 u_0 u_1, \tag{4.66}$$

$$v_2^2 = u_2^2 - S t u_0 u_2 + S^2(t^5 u_1 u_2 + t^4 u_1^2 + t^3 u_0 u_1) \tag{4.67}$$

In degree 3 the representation will be $\mathrm{Sym}^3(D)$, which contains a copy of $\mathrm{Sym}^2(D)$ via the map $\mathrm{Sym}^2(D) \mapsto v_0 \,\mathrm{Sym}^2(D)$. The invariant cubics in the v_i are obtained by calling

```
inv_mon(3,L);
```

We get

```
[
  v_0^3,
  v_0*v_1*v_3,
  v_0*v_2^2,
  v_1^2*v_2,
  v_2*v_3^2
]
```

with the monomials starting with v_0 known to us beforehand – these monomials are obtained as products of v_0 with degree 2 invariants. There are two new invariant monomials: $v_1^2 v_2$ and $v_2 v_3^2$. We put all the cubic invariants into a table. We shall start with $v_1^2 v_2$ as it has a smaller number of monomials.

	$v_1^2 v_2 - v_0^3$	$v_0 v_1 v_3 - v_0^3$	$v_0 v_2^2 - v_0^3$
$u_1^2 u_2$	t^4		
$u_0 u_1 u_3$		t^4	
$u_0 u_2^2$			t^4
u_1^3	$2t^3$		
$u_0^2 u_3$		t^3	
$u_0 u_1 u_2$	$2t^3$	$3t^3$	$4t^3$
$u_0 u_1^2$	$5t^2$	$3t^2$	$4t^2$
$u_0^2 u_2$	t^2	$3t^2$	$2t^2$
$u_0^2 u_1$	$4t$	$4t$	$4t$

What we need to do is to cancel as high power of t as possible. We allow to modify an invariant polynomial by scaling it and adding a $\mathbb{Z}$-linear combination of other invariant polynomials. We look at the column corresponding to $v_1^2 v_2 - v_0^3$ and compute pseudovaluations of the entries. These are $4, 6, 6, 2, 2, 4$ top to bottom. In order to cancel t^4, we need to modify monomials $5t^2 u_0 u_1^2$ and $t^2 u_0^2 u_2$. More precisely, we are looking at coefficients $5t^2$ and t^2 and we want to modify them so that the integral part is even in both cases. This can only be

achieved by summing it with something odd, which leaves us only one option – $v_0v_1v_3 - v_0^3$, since the corresponding coefficients in $v_0v_2^2 - v_0^3$ are even. So we want to consider $(v_1^2v_2 - v_0^3) + n(v_0v_1v_3 - v_0^3)$, where n must be an odd integer. This introduces the monomial $nt^3u_0^2u_3$ which will have pseudovaluation 3 (n is odd) and which cannot be further modified since this monomial is not present in any other invariant polynomials. This shows that we cannot cancel t^4. Note however that we can cancel t^3 by considering $v_1^2v_2 - v_0v_1v_3$:

	$v_1^2v_2 - v_0^3$	$v_0v_1v_3 - v_0^3$	$v_0v_2^2 - v_0^3$	$v_1^2v_2 - v_0v_1v_3$
$u_1^2u_2$	t^4			t^4
$u_0u_1u_3$		t^4		$-t^4$
$u_0u_2^2$			t^4	
u_1^3	$2t^3$			$2t^3 = -St^6$
$u_0^2u_3$		t^3		$-t^3$
$u_0u_1u_2$	$2t^3$	$3t^3$	$4t^3$	$-t^3$
$u_0u_1^2$	$5t^2$	$3t^2$	$4t^2$	$2t^2 = -St^5$
$u_0^2u_2$	t^2	$3t^2$	$2t^2$	$-2t^2 = St^5$
$u_0^2u_1$	$4t$	$4t$	$4t$	

We cancel t^3 and multiply by -1 to get the new invariant form

$$v_0v_1v_3 - v_1^2v_2 = u_0^2u_3 + u_0u_1u_2 + t(u_0u_1u_3 - u_1^2u_2) + S(t^3u_1^3 + t^2u_0u_1^2 - t^2u_0^2u_2). \tag{4.68}$$

The next invariant polynomial is $v_2v_3^2$, which has a bigger number of monomials in u_i, but the technique is the same.

	$v_2v_3^2 - v_0^3$	$v_0v_2^2 - v_0^3$	$v_v^2v_2 - v_0^3$
$u_2u_3^2$	t^8		
$u_1u_3^2$	$2t^7$		
$u_2^2u_3$	$6t^7$		
u_2^3	$9t^6$		
$u_0u_3^2$	t^6		
$u_1u_2u_3$	$18t^6$		
$u_1u_2^2$	$36t^5$		
$u_1^2u_3$	$12t^5$		
$u_0u_2u_3$	$8t^5$		
$u_0u_2^2$	$15t^4$	t^4	
$u_1^2u_2$	$45t^4$		t^4
$u_0u_1u_3$	$10t^4$		
u_1^3	$18t^3$		$2t^3$
$u_0u_1u_2$	$36t^3$	$4t^2$	$2t^3$
$u_0^2u_3$	$2t^3$		
$u_0u_1^2$	$21t^2$	$4t^2$	$5t^2$
$u_0^2u_2$	$7t^2$	$2t^2$	t^2
$u_0^2u_1$	$8t$	$4t$	$4t$

Suppose that we want to cancel t^8, but because the term $9t^6u_2^3$ is only present in one invariant monomial we cannot modify it. But we can cancel t^6 – there is no canonical choice here, but one choice that works is to take $v_2v_3^2-v_0^3+v_0v_2^2-v_1^2v_2$:

	$v_2v_3^2 - v_0^3$	$v_0v_2^2 - v_0^3$	$v_v^2v_2 - v_0^3$	$v_2v_3^2 - v_0^3 + v_0v_2^2 - v_1^2v_2$
$u_2u_3^2$	t^8			t^8
$u_1u_3^2$	$2t^7$			$2t^7 = -St^{10}$
$u_2^2u_3$	$6t^7$			$6t^7 = -3St^{10}$
u_2^3	$9t^6$			$9t^6$
$u_0u_3^2$	t^6			t^6
$u_1u_2u_3$	$18t^6$			$18t^6 = -9St^9$
$u_1u_2^2$	$36t^5$			$36t^5 = 9S^2t^{11}$
$u_1^2u_3$	$12t^5$			$12t^5 = 3S^2t^{11}$
$u_0u_2u_3$	$8t^5$			$8t^5 = -S^3t^{14}$
$u_0u_2^2$	$15t^4$	t^4		$16t^4 = S^4t^{16}$
$u_1^2u_2$	$45t^4$		t^4	$44t^4 = -11St^7$
$u_0u_1u_3$	$10t^4$			$10t^4 = -5St^7$
u_1^3	$18t^3$		$2t^3$	$16t^3 = S^4t^{15}$
$u_0u_1u_2$	$36t^3$	$4t^2$	$2t^3$	$38t^3 = -19St^6$
$u_0^2u_3$	$2t^3$			$2t^3 = -St^6$
$u_0u_1^2$	$21t^2$	$4t^2$	$5t^2$	$20t^2 = 5S^2t^8$
$u_0^2u_2$	$7t^2$	$2t^2$	t^2	$8t^2 = -S^3t^{11}$
$u_0^2u_1$	$8t$	$4t$	$4t$	$8t = -S^3t^{10}$

Cancel t^6 to get the invariant polynomial

$$v_2v_3^2 - v_0^3 + v_0v_2^2 - v_1^2v_2 = 9u_2^3 + u_0u_3^2 + t^2u_2u_3^2 \tag{4.69}$$

$$- S(t^4u_1u_3^2 + 3t^4u_2^2u_3 + 9t^3u_1u_2u_3 + 11tu_1^2u_2 + 5tu_0u_1u_3) \tag{4.70}$$

$$+ S^2(9t^5u_1u_2^2 + 3t^5u_1^2u_3 + 5t^2u_0u_1^2) \tag{4.71}$$

$$- S^3(t^8u_0u_2u_3 + t^5u_0^2u_2 + t^4u_0^2u_1) + S^4(t^{10}u_0u_2^2 + t^9u_1^3) \tag{4.72}$$

In degree 4 the MAGMA output is

```
[
    v_0^4,
    v_0^2*v_1*v_3,
    v_0^2*v_2^2,
    v_0*v_1^2*v_2,
    v_0*v_2*v_3^2,
    v_1^4,
    v_1^2*v_3^2,
    v_1*v_2^2*v_3,
    v_2^4,
    v_3^4
]
```

There are only two new invariant polynomials – v_1^4 and v_3^4. We don't need to modify v_1^4:

$$v_1^4 - u_0^4 = t^4u_1^4 + 4t^3u_1^3u_0 + 6t^2u_0^2u_1^2 + 4tu_0^2u_1 \tag{4.73}$$
$$= t^4u_1^4 + S^2t^9u_0u_1^3 - 3St^5u_0^2u_1^2 + S^2t^7u_0^2u_1 \tag{4.74}$$

and we can cancel t^4 to get the invariant

$$v_1^4 - v_0^4 = u_1^4 - 3Stu_0^2u_1^2 + S^2(t^5u_0u_1^3 + t^3u_0^3u_1) \tag{4.75}$$

The invariant quartic v_3^4 will be rather large:

$$\begin{aligned}
v_3^4 =& t^{12}u_3^4 + 12t^{11}u_2u_3^3 + 12t^{10}u_1u_3^3 + 54t^{10}u_2^2u_3^2 + 4t^9u_0u_3^3 && (4.76)\\
&+ 108t^9u_1u_2u_3^2 + 108t^9u_2^3u_3 + 81t^8u + 2^4 + 54t^8u_1^2u_3^2 && (4.77)\\
&+ 36t^8u_0u_2u_3^2 + 324t^8u_1u_2^2u_3 + 324t^7u_1u_2^3 + 36t^7u_0u_1u_3^2 && (4.78)\\
&+ 108t^7u_0u_2^2u_3 + 324t^7u_1^2u_2u_3 + 108t^6u_0u_2^3 + 486t^6u_1^2u_2^2 && (4.79)\\
&+ 6t^6u_0^2u_3^2 + 108t^6u_1^3u_3 + 216t^6u_0u_1u_2u_3 + 324 + t^6u_0u_1u_2^2 && (4.80)\\
&+ 324t^5u_1^3u_2 + 108t^5u_0u_1^2u_3 + 36t^5u_0^2u_2u_3 + 81t^4u_1^4 + 54t^4u_0^2u_2^2 && (4.81)\\
&+ 324t^4u_0u_1^2u_2 + 36t^4u_0^2u_1u_3 + 108t^3u_0u_1^3 + 108t^3u_0^2u_1u_2 + 4t^3u_0^3u_3 && (4.82)\\
&+ 54t^2u_0^2u_1^2 + 12t^2u_0^3u_2 + 12tu_0^3u_1 + u_0^4. && (4.83)
\end{aligned}$$

We will try to cancel t^{12}. Note that the coefficients of the terms starting with $u_2u_3^3$ to $u_2^3u_3$ are even and have a power of t which is at least 9. Moreover, these terms are not summands of any other invariant polynomials, so we will ignore them in subsequent tables. We will consider three tables altogether. In the first table we will have only summands in the u_i which have powers of t in their coefficients of at least 6 – this is so that we only need to make sure that the integral part is divisible by $4 = S^2t^6$ in each case, so that we can cancel t^{12}.

	v_3^4	v_2^4	$v_1^2v_3^2$
u_2^4	$\underline{81t^8}$	t^8	
$u_1^2u_3^2$	$\underline{54t^8}$		t^8
$u_1u_2^3$	$324t^7$	$8t^7$	
$u_0u_1u_3^2$	$36t^7$		$6t^7$
$u_0u_2^3$	$108t^6$	$4t^6$	
$u_1^2u_2^2$	$\underline{486t^6}$	$24t^6$	$9t^6$
$u_0^2u_3^2$	$\underline{6t^6}$		t^6
$u_1^3u_3$	$108t^6$		t^6
$u_0u_1u_2u_3$	$216t^6$		$12t^6$

Note that we skipped the monomials in the u_i which were already divisible by

4 and which were not summands in either v_2^4 or $v_1^2v_3^2$. The coefficients where integral part is not divisible by 4 are underlined. We can get rid of $81t^8$ by subtracting $81v_2^4$ and we can double $54t^8$ by adding $54v_1^2v_3^2$. In order to keep the integral coefficients as small as possible, we reduce 81 and 54 modulo 16, so that it won't affect the calculations in the next two tables.

	v_3^4	v_2^4	$v_1^2v_3^2$	$v_3^4 - v_2^4 + 6v_1^2v_3^2$
u_2^4	$\underline{81t^8}$	t^8		$80t^8$
$u_1^2u_3^2$	$\underline{54t^8}$		t^8	$60t^8$
$u_1u_2^3$	$324t^7$	$8t^7$		$316t^7$
$u_0u_1u_3^2$	$36t^7$		$6t^7$	$72t^7$
$u_0u_2^3$	$108t^6$	$4t^6$		$104t^6$
$u_1^2u_2^2$	$\underline{486t^6}$	$24t^6$	$9t^6$	$516t^6$
$u_0^2u_3^2$	$\underline{6t^6}$		t^6	$12t^6$
$u_1^3u_3$	$108t^6$		$6t^6$	$144t^6$
$u_0u_1u_2u_3$	$216t^6$		$12t^6$	$288t^6$

In the last column all of the integral coefficients are now divisible by 4.
In the next table we look at the rows which have powers of t of between 3 and 5 and we want to make the integral part divisible by $8 = -S^3t^9$.

	$v_3^4 - v_2^4 + 6v_1^2v_2^2$	v_1^4	$v_0^2v_1^2$
$u_0u_1u_2^2$	$408t^5$		
$u_1^3u_2$	$400t^5$		
$u_0u_1^2u_3$	$192t^5$		
$u_0^2u_2u_3$	$72t^5$		
u_1^4	$\underline{119t^4}$	t^4	
$u_0^2u_2^2$	$\underline{102t^4}$		t^4
$u_0u_1^2u_2$	$528t^4$		
$u_0^2u_1u_3$	$96t^4$		
$u_0u_1^3$	$\underline{220t^3}$	$4t^3$	
$u_0^2u_1u_2$	$264t^3$		$4t^3$
$u_0^3u_3$	$16t^3$		

The coefficients with integral parts not divisible by 8 are underlined. One way to proceed is to add[1] $9v_1^4 + 2v_0^2v_2^2$:

[1] we could have added $v_1^4+2v_0^2v_2^2$ to balance this table, but then we would not get divisibility by 16 in the last table.

	$v_3^4 - v_2^4 + 6v_1^2v_2^2$	v_1^4	$v_0^2v_1^2$	$v_3^4 - v_2^4 + 6v_1^2v_2^2 + 9v_1^4 + 2v_0^2v_2^2$
$u_0u_1u_2^2$	$408t^5$			$408t^5$
$u_1^3u_2$	$400t^5$			$400t^5$
$u_0u_1^2u_3$	$192t^5$			$192t^5$
$u_0^2u_2u_3$	$72t^5$			$72t^5$
u_1^4	$\underline{119t^4}$	t^4		$128t^4$
$u_0^2u_2^2$	$\underline{102t^4}$		t^4	$104t^4$
$u_0u_1^2u_2$	$528t^4$			$528t^4$
$u_0^2u_1u_3$	$96t^4$			$96t^4$
$u_0u_1^3$	$\underline{220t^3}$	$4t^3$		$256t^3$
$u_0^2u_1u_2$	$264t^3$		$4t^3$	$272t^3$
$u_0^3u_3$	$16t^3$			$16t^3$

In the last column all of the integral coefficients are now divisible by 8.
We now look at the last tables, which consists of those rows which have powers of t 1 and 2. We want to make integral parts divisible by 16, but they already are:

	$v_3^4 - v_2^4 + 6v_1^2v_2^2 + 9v_1^4 + 2v_0^2v_2^2$
$u_0^2u_1^2$	$224t^2$
$u_0^3u_2$	$48t^2$
$u_0^3u_1$	$96t$

We can replace powers of 2 by powers of $-St^3$ and cancel t^{12} to get the invariant form

$$v_3^4 - v_0^4 = u_3^4 - 27Stu_2^2u_3^2 \tag{4.84}$$
$$+ S^2(3t^5u_2u_3^3 + 3t^4u_1u_3^3 + t^3u_0u_3^3 + 27t^3u_1u_2u_3^2 + 27t^3u_2^3u_3 + 9t^2u_0u_2u_3^2 \tag{4.85}$$
$$+ 27tu_0u_2^2u_3 + 15t^2u_1^2u_3^2 + 79tu_1u_2^3 + 129t^3u_0u_2^3 + 3u_0^2u_3^2) \tag{4.86}$$
$$- S^3(9t^4u_0u_1u_3^2 + 13t^3u_0u_2^3 + 51t^2u_0u_1u_2^2 + 9t^2u_0^2u_2u_3 + 13tu_0^2u_2) \tag{4.87}$$
$$+ S^4(5t^8u_2^4 + 9t^6u_1^3u_3 + 25t^5u_1^3u_2 + 33t^4u_0u_1^2u_2 + 17t^3u_0^2u_1u_2 + t^3u_0^3u_3) \tag{4.88}$$
$$- S^5(9t^9u_0u_1u_2u_3 + 3t^7u_0^2u_1u_3) + 3S^6t^{11}u_0u_1^2u_3 - S^7t^9u_1^4 + S^8t^{12}u_0u_1^3 \tag{4.89}$$

The invariant ring is generated in degrees 1,2,3,4. There are no generators in higher degrees because of the relation $\tau^4 = 1$.

4.3 Numerical Godeaux surfaces

All surfaces in this section are smooth and projective unless stated otherwise. Let X be a minimal surface of general type. The smallest possible invariants for X are $\chi(\mathcal{O}_X) = K_X^2 = 1$ and $p_g = q = 0$. The first example of such a surface was given by Godeaux in [God31]. After almost 90 years since the first example, there is still no complete classification or understanding of this type of surfaces.

Definition 4.3.1. A minimal surface X of general type with $K_X^2 = 1$ is called a **numerical Godeaux surface**.

Numerical Godeaux surfaces over $\mathbb{C}$ with an involution were classified by Calabri, Ciliberto, and Mendes Lopes in [CCML07].

Example 4.3.2. Let us construct a numerical Godeaux surface over $\mathbb{C}$. Let x_0, x_1, x_2, x_3 be co-ordinates on $\mathbb{P}^3_{\mathbb{C}}$. Take $G = \mathbb{Z}/5$ and let it act on $\mathbb{P}^3$ by $\frac{1}{5}(0,1,2,3)$, i.e., we take the following representation of $\mathbb{Z}/5$:

$$\mathbb{Z}/5 \to \mathrm{GL}_4, \tag{4.90}$$

$$1 \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \epsilon & 0 & 0 \\ 0 & 0 & \epsilon^2 & 0 \\ 0 & 0 & 0 & \epsilon^3 \end{pmatrix} = A, \tag{4.91}$$

where ϵ is a primitive fifth root of unity. Then A acts on the column vector $(x_0, x_1, x_2, x_3)^T$. The action has four fixed points: $[1:0:0:0], [0:1:0:0], [0:0:1:0]$, and $[0:0:0:1]$. The Fermat quintic surface X defined by $x_0^5 + x_1^5 + x_2^5 + x_3^5 = 0$ does not pass through any of the fixed points of this action. Furthermore, the defining polynomial is G-invariant, so the quotient $Y = X/G$ is a smooth surface. By [Bar+04, Proposition V.2.1], we have $\pi_1(X) = 0$, so $\pi_1(Y) \cong G$ and $q_Y = 0$.

Proposition 4.3.3. *[Lie09, Proposition 1.1] Let X be a minimal surface of general type with $K_X^2 = 1$. Then the following hold:*

$$b_1(X) = 0, \tag{4.92}$$

$$|\pi_1(X)| \leq 6, \tag{4.93}$$

$$p_g(X) \leq 2, \tag{4.94}$$

$$h^{01}(X) = h^1(X, \mathcal{O}_X) \leq 1. \tag{4.95}$$

In particular, if $h^{01}(X) = 1$ then X has a non-reduced Picard scheme, which can only happen in positive characteristic.

In characteristic 0, the only possibilities for $G = \mathrm{Tors}(X)$ are

$$0, \mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/4, \mathbb{Z}/2 \times \mathbb{Z}/2, \mathbb{Z}/5. \tag{4.96}$$

By [Rei78, Theorem 2.1] the case $\mathbb{Z}/2 \times \mathbb{Z}/2$ is excluded. We have already seen the case $\mathbb{Z}/5$ and all the other cyclic groups are also possible by the works of Barlow [Bar84; Bar85] ($G = 0, \mathbb{Z}/2$) and Reid [Rei78] ($G = \mathbb{Z}/3, \mathbb{Z}/4$).
In positive characteristic, numerical Godeaux surfaces are further subdivided into three classes.

Definition 4.3.4. Let X be a numerical Godeaux surface. If $h^1(\mathcal{O}_X) = 0$, then X is called a **classical Godeaux surface**. If $h^1(\mathcal{O}_X) = 1$ the surface X is called a **nonclassical Godeaux surface**. These are further subdivided into two cases depending on the action of the Frobenius $F\colon H^1(\mathcal{O}_X) \to H^1(\mathcal{O}_X)$. If F is an isomorphism, X is called a **singular Godeaux surface**. If F acts as zero, X is called a **supersingular Godeaux surface**.

Nonclassical Godeaux surfaces exist only if the characteristic of the field is low enough, as shown in the following theorem by Liedtke.

Proposition 4.3.5. *[Lie09, Theorem 2.1 and Theorem 2.4] Nonclassical Godeaux surfaces can exist in characteristic* $2, 3,$ *and* 5 *only.*

Liedtke specialises to the case $p = 5$ in [Lie09].

Proposition 4.3.6. *[Lie09, p. 4] and [Proposition I.1.7 Eke88] Let X be a smooth surface over an algebraically closed field of characteristic $p > 0$ and $\pi\colon Y \to X$ a nontrivial $\boldsymbol{\mu}_p$- or $\boldsymbol{\alpha}_p$-torsor. Then we have the equalities*

$$\chi(\mathcal{O}_Y) = p\chi(\mathcal{O}_X) \tag{4.97}$$

and

$$K_Y^2 = pK_X^2. \tag{4.98}$$

Proposition 4.3.7. *[Proposition 2.3 Lie09] Let X be a minimal surface of general type and $\pi\colon Y \to X$ a nontrivial $\boldsymbol{\alpha}_p$- or $\boldsymbol{\mu}_p$-torsor. Then Noether's inequality*

$$K_Y^2 \geq 2h^0(\omega_Y) - 4 \tag{4.99}$$

holds.

Proposition 4.3.8. *Let $p = 3$ and X a supersingular Godeaux surface. Asuume that the torsor corresponding to $\mathrm{Pic}^0 X$ is normal, so that Liedtke's version of Noether's inequality can be applied. Then the only possibilities for $\mathrm{Pic}^0 X$ are $\boldsymbol{\alpha}_3, \boldsymbol{\alpha}_9$, and M_9, with $\boldsymbol{\alpha}_9^D$ not possible.*

Proof. Suppose that X is supersingular. Then the action of F on $H^1(\mathcal{O}_X)$ gives an embedding

$$\boldsymbol{\alpha}_3 \hookrightarrow \operatorname{Pic}^0 X. \tag{4.100}$$

Note that $\boldsymbol{\mu}_p \hookrightarrow \operatorname{Pic}^0 X$ is not possible because the Frobenius is not bijective on $H^1(\mathcal{O}_X)$. The embedding gives rise to an $\boldsymbol{\alpha}_3^D$-torsor

$$Y \to X. \tag{4.101}$$

Consider the corresponding exact sequence of group schemes

$$0 \to \boldsymbol{\alpha}_3 \to \operatorname{Pic}^0 X \to G \to 0. \tag{4.102}$$

Suppose that G is nontrivial, then there is an embedding $\boldsymbol{\alpha}_3 \hookrightarrow G$ giving rise to an $\boldsymbol{\alpha}_3^D$-torsor above Y. In particular, $h^1(\mathcal{O}_Y) \neq 0$ – if it is zero, then $\operatorname{Pic} Y$ is an étale group scheme. By 4.3.6, we have

$$K_Y^2 = 3K_X^2 = 3, \tag{4.103}$$

so that

$$3 = h^0(\mathcal{O}_Y) - h^1(\mathcal{O}_Y) + h^2(\mathcal{O}_Y), \tag{4.104}$$

from which it follows that

$$h^2(\mathcal{O}_Y) = 2 + h^1(\mathcal{O}_Y) \geq 3. \tag{4.105}$$

On the other hand, Noether's inequality 4.3.7 gives

$$3 \geq 2h^0(\omega_Y) - 4, \tag{4.106}$$

from which it follows that

$$h^2(\mathcal{O}_Y) \leq 3.5 \tag{4.107}$$

and hence we get

$$h^2(\mathcal{O}_Y) = 3, \tag{4.108}$$

$$h^1(\mathcal{O}_Y) = 1. \tag{4.109}$$

Recall that $\boldsymbol{\alpha}_3 \cong \boldsymbol{\alpha}_3^D$ and now look at the $\boldsymbol{\alpha}_3$-torsor above Y, say

$$Z \to Y. \tag{4.110}$$

Consider the corresponding exact sequence

$$0 \to \boldsymbol{\alpha}_3 \to \operatorname{Pic}^0 Y \to H \to 0 \tag{4.111}$$

We know that $K_Z^2 = 3K_Y^2 = 9$ and hence

$$h^2(\mathcal{O}_Z) = 8 + h^1(\mathcal{O}_Z) \geq 9. \tag{4.112}$$

On the other hand, by Noether's inequality,

$$9 \geq 2h^0(\omega_Z) - 4, \tag{4.113}$$

$$h^0(\omega_Z) \leq 6.5, \tag{4.114}$$

so $H = 0$ and $\mathrm{Pic}^0 Y = \boldsymbol{\alpha}_3$. Hence $\mathrm{Pic}^0 X \in \mathrm{Ext}^1(\boldsymbol{\alpha}_3, \boldsymbol{\alpha}_3)$ and so it must be one of $\boldsymbol{\alpha}_3 \times \boldsymbol{\alpha}_3, \boldsymbol{\alpha}_9, \boldsymbol{\alpha}_9^D, M_9$, but because $h^1(\mathcal{O}_X) = 1$ we cannot have group schemes with tangent space of dimension 2. This leaves $\boldsymbol{\alpha}_9$ and M_9 as the other two possibilities, in addition to $\boldsymbol{\alpha}_3$ corresponding to $G = 0$. □

Remark. It should be possible to perform a similar analysis for the case $p = 2$, but we would need to consider group schemes of order $2^3 = 8$ as well. These were classified in Section 3.2.3.

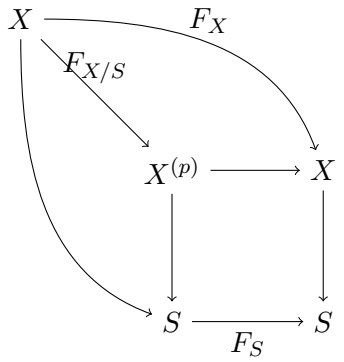
4.4 Further directions

As we saw in the previous section, classical Godeaux surfaces were constructed in all characteristics. Nonclassical Godeaux surfaces can only exist in characteristic 2,3, or 5. In characteristic 5 these were constructed by Lang in [Lan81] (étale case), Miranda in [Mir84] (singular case), and Liedtke in [Lie09] (supersingular case). Kim and Reid give a unified treatment of these surfaces in characteristic 5 [KR], using the Tate-Oort group scheme $\mathbb{TO}_p$ from [Rei19]. We have shown that in characteristic 3 the only possibilities for $\mathrm{Pic}^0 X$ are $\boldsymbol{\alpha}_3, \boldsymbol{\alpha}_9$, or M_9 in the supersingular case. It should be possible to deal with characteristics 2 and 3 and put nonclassical Godeaux surfaces into a single deformation family, using the group schemes $\mathbb{TO}_{p^2}^{ll}$ and $\mathbb{TO}_{p^2}^{l}$.

Appendix A

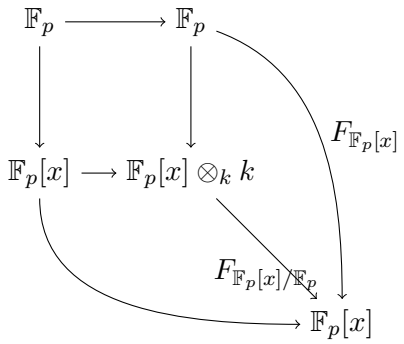
Frobenius morphisms

Let X be a scheme of characteristic p, i.e., $p\mathcal{O}_X = 0$. Note that p must be unique, unless X is trivial. Equivalently, we say that X of characteristic p if the structure morphism $\operatorname{Spec}\mathbb{Z}$ factors uniquely through $\operatorname{Spec}\mathbb{F}_p$.
The **absolute Frobenius** morphism of X is defined as the identity on the topological space and $x \mapsto x^p$ on the structure sheaf – this map is indeed a morphism of sheaves of rings because $(a+b)^p = a^p + b^p$ in characteristic p.
If instead of $\operatorname{Spec}\mathbb{F}_p$ we have another scheme S of characteristic p as our base scheme, then there is a relative version of Frobenius which is $\mathcal{O}_S$-linear.



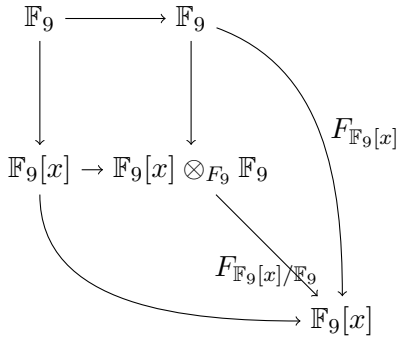
The square in the diagram is a pullback square in the category of $\mathbb{F}_p$-schemes (or $\mathbb{Z}$-schemes) and defines $X^{(p)}$. The morphism $F_{X/S}\colon X \to X^{(p)}$ is defined uniquely by the property of the pullback square and is $\mathcal{O}_S$-linear.

Example A.0.1. Let $A = \mathbb{F}_p[x]$, then we have the pushforward square of $\mathbb{F}_p$-algebras



Note that $x^p = x$ in $\mathbb{F}_p$, so everything in sight is $\mathbb{F}_p$-linear and there is no need for relative Frobenius.

Example A.0.2. Take $k = \mathbb{F}_9 = \mathbb{F}_3[i]$ and $A = \mathbb{F}_9[x]$. The absolute Frobenius is no longer the identity, e.g., i maps to $2i$. We have the diagram



The map $\mathbb{F}_9[x] \to \mathbb{F}_9[x] \otimes_{\mathbb{F}_9} F_9 \cong \mathbb{F}_9[x]$ is given by

$$ax \mapsto x \otimes a^p, \tag{A.1}$$

so that the relative Frobenius is given by

$$F_{\mathbb{F}_9[x]/\mathbb{F}_9} \colon \mathbb{F}_9[x] \to \mathbb{F}_9[x], \tag{A.2}$$

$$ax \mapsto ax^p. \tag{A.3}$$

In general, if A is an $\mathbb{F}_p$-algebra of finite type, say, $A = \mathbb{F}_p[x_1, ..., x_n]/(f_1, ..., f_m)$, then $A^{(p)} = \mathbb{F}_p[x_1, ..., x_n]/(f_1^{(p)}, ..., f_m^{(p)})$. Here, $f^{(p)}$ is obtained from f be raising all coefficients of f to the pth power. The relative Frobenius in this case is given by $ax_i \mapsto ax^p$ on generators.

Appendix B

MAGMA code

All of calculations for this thesis were done in MAGMA Computational Algebra System [BCP97].

```
// The default FrobeniusImage function of MAGMA takes a matrix
    defined over a finite field and computes its Frobenius image. It
    does not work with matrices defined over algebras of positive
    characteristic. The function below does.

function FrobeniusImageRing(M,n)
return
    Matrix(NumberOfRows(M),NumberOfColumns(M),[M[j,i]^(Characteristic(Parent(M))^n):
    i in [1..NumberOfRows(M)], j in [1..NumberOfRows(M)]]);
end function;

// The purpose of MatrixRingList is to get the list of elements of
    the matrix ring M_n(R). Just calling Set(MatrixRing(R,n)) is not
    good, because if R is a finite ring which is not a field then it
    is not possible to iterate over MatrixRing(R,n) -- MAGMA gives a
    mistake even if R is a ring of order 4.

function MatrixRingList(R,n)
m:=#R^(n^2);
C:=CartesianPower(R,n^2);
L:=[i: i in Set(C)];
P:=[];
for i in [1..m] do
  P[i]:=Matrix(R,n,n, [j: j in L[i]]);
end for;
return P,#P;
end function;

// Our function takes in a finite ring R and an integer n and outputs
```

```
    p-conjugates of matrices in M_n(R)]

function MatrixConjClass(R,n)
M:=MatrixRing(R,n);
L:={@ x: x in Set(M)@};
G:={@ x: x in L | IsInvertible(x) @};
P:={@ @};
while #L ne 0 do
    for x in L do
        K:={@ FrobeniusImageRing(y,1)*x*y^-1 : y in G @};
        P:=Include(P,K);
        L:= L diff K;
    end for;
end while;
return P;
end function;

// This function takes two matrices and outputs true if their
    corresponding primitively generated Hopf algebras are isomorphic
    and false otherwise
function MatrixIsoHopfAlg(A,B)
M:=MatrixRing(Parent(A[1,1]),NumberOfRows(A));
L:={@ x: x in Set(M)@};
G:={@ x: x in L | IsInvertible(x) @};
K:={@ FrobeniusImageRing(y,1)*A*y^-1 : y in G @};
if B in K then return true;
else return false;
end if;
end function;

// This function takes a representation of a group (in diagonal form)
    and outputs invariant monomials of degree n
function inv_mon(n,L)
L:=[R!L[i]: i in [1..#L]];
M:=DiagonalMatrix(Parent(L[1]),#L,L);
P:=PolynomialRing(Integers(),#L);
K:=[];
O:=[];
AssignNames(~P, ["v_" cat IntegerToString(k) : k in [0..#L-1]] );
N:=[R!SymmetricPower(M,n)[i,i]: i in
    [1..NumberOfRows(SymmetricPower(M,n))]];
  for i in N do
    if i eq 1 then Append(~K, Index(N,i));
    N[Index(N,i)]:=0;
    end if;
  end for;
```

```
G:=MonomialsOfDegree(P,n);
  for i in K do
    Append(~O,G[i]);
  end for;
return O;
end function;


// Our function takes in a finite ring R and an integer n and outputs
    p-conjugates of matrices in M_n(R)]

function MatrixConjClass(R,n)
M:=MatrixRing(R,n);
L:={@ x: x in Set(M)@};
// We create a copy of L so that we can iterate over L and remove
    elements from L1 -- it is not recommended to change the list we
    are iterating over
L1:= L;
G:={@g : g in L | IsInvertible(g) @};
// G:=GeneralLinearGroup(n,R);
P:={@ @};
    for x in L do
        if #L1 eq 0 then break;
        end if;
        if x notin L1 then continue;
        end if;
        K:={@ FrobeniusImage(y,1)*x*y^-1 : y in G @};
        P:=Include(P,K);
        L1:= L1 diff K;
// This part is optional: uncomment to see the progress in real time
        printf "The size of L1 is now ";
        #L1;
    end for;
return P;
end function;


// This function takes two matrices and outputs true if their
    corresponding primitively generated Hopf algebras are isomorphic
    and false otherwise
function MatrixIsoHopfAlg(A,B)
M:=MatrixRing(Parent(A[1,1]),NumberOfRows(A));
L:={@ x: x in Set(M)@};
G:={@ x: x in L | IsInvertible(x) @};
K:={@ FrobeniusImageRing(y,1)*A*y^-1 : y in G @};
if B in K then return true;
```

```
else return false;
end if;
end function;




// This function takes a matrix M with entries in an F_p-algebra and
    outputs the corresponding primitively generated Hopf algebra H
function PrimGenHopfAlg(M)
n:=NumberOfRows(M);
p:=Characteristic(Parent(M[1,1]));
P:=PolynomialRing(Parent(M[1,1]), n);
// This step is needed to make the output more readable -- the
    variables will have names x_1, x_2 etc.
AssignNames(~P, ["x_" cat IntegerToString(k) : k in [1..n]] );
// Define the ideal of relations for the Hopf algebra
L:=[P.i^p-(&+[Transpose(M)[i,j]*P.j : j in [1..n]]): i in [1..n]];
H:=quo<P | L>;
return H;
end function;




// Setting up the group scheme
K<t>:=FunctionField(Rationals());
A<x>:=PolynomialRing(K);
S:=-2/t^3;
RR<x,u_0,u_1,u_2,u_3, y_1, y_3>:=PolynomialRing(K,7);
Phi:=x^4-S*(2*t^2*x^3+3*t*x^2+2*x);
R:=quo<RR|Phi>;
tau:=1+t*x;
// specifying the given representation, same as in TO_p case:
A:=Matrix(R,2,2,[1,0,x,tau]);
// specifying the action on linear terms, i.e., u_0, u_1, u_2, u_3
B:=SymmetricPower(A,3);
// this will give us the action on quadratic terms, i.e., Sym^2 (u_i)
    + (y_1, y_3).
C:=SymmetricPower(B,3);
// we only need the following 12*12 submatrix:
Act:=Matrix(R,12,12,[C[i,j]: i in [1..12], j in [1..12]]);
Act:=Transpose(Act);
// the diagonal helps us find invariant terms
[Act[i,i]: i in [1..12]];
```

```
L:=[1,t,t^2,t^3];
R<t>:=PolynomialRing(Rationals()); R<t>:=quo<R | t^4-1>;
// This function takes a representation of a group (in diagonal form)
    and outputs invariant monomials of degree n
function inv_mon(n,L)
R:=Parent(L[1]);
L:=[R!L[i]: i in [1..#L]];
M:=DiagonalMatrix(Parent(L[1]),#L,L);
P:=PolynomialRing(Integers(),#L);
K:=[];
O:=[];
AssignNames(~P, ["v_" cat IntegerToString(k) : k in [0..#L-1]] );
N:=[R!SymmetricPower(M,n)[i,i]: i in
    [1..NumberOfRows(SymmetricPower(M,n))]];
  for i in N do
    if i eq 1 then Append(~K, Index(N,i));
    N[Index(N,i)]:=0;
    end if;
  end for;
G:=MonomialsOfDegree(P,n);
  for i in K do
    Append(~O,G[i]);
  end for;
return O;
end function;
```

Bibliography

[Bar+04] Wolf P. Barth et al. *Compact complex surfaces*. Second. Vol. 4. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]. Springer-Verlag, Berlin, 2004, pp. xii+436.

[Bar84] Rebecca Barlow. "Some new surfaces with $p_g = 0$". In: *Duke Math. J.* 51.4 (1984), pp. 889–904.

[Bar85] Rebecca Barlow. "A simply connected surface of general type with $p_g = 0$". In: *Invent. Math.* 79.2 (1985), pp. 293–301.

[BCP97] Wieb Bosma, John Cannon and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[CCML07] Alberto Calabri, Ciro Ciliberto and Margarida Mendes Lopes. "Numerical Godeaux surfaces with an involution". In: *Trans. Amer. Math. Soc.* 359.4 (2007), pp. 1605–1632.

[DG80] Michel Demazure and Peter Gabriel. *Introduction to algebraic geometry and algebraic groups*. Vol. 39. North-Holland Mathematics Studies. Translated from the French by J. Bell. North-Holland Publishing Co., Amsterdam-New York, 1980, pp. xiv+357.

[EGA4] A. Grothendieck. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV". In: *Inst. Hautes Études Sci. Publ. Math.* 32 (1967), p. 361.

[Eke88] Torsten Ekedahl. "Canonical models of surfaces of general type in positive characteristic". In: *Inst. Hautes Études Sci. Publ. Math.* 67 (1988), pp. 97–144.

[God31] Lucien Godeaux. "Sur une surface algébrique de genres zéro et bigenre deux". In: *Atti Accad. naz. Lincei, Rend.* 14.6 (1931), pp. 479–481.

[Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*. Vol. 14. CRM Monograph Series. With the assistance of Marc-Hubert Nicole. American Mathematical Society, Providence, RI, 2002, pp. x+270.

[Gro74] Alexandre Grothendieck. *Groupes de Barsotti-Tate et cristaux de Dieudonné*. Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970). Les Presses de l'Université de Montréal, Montreal, Que., 1974, p. 155.

[KR] Soonyoung Kim and Miles Reid. "The Tate–Oort group of order p and Godeaux surfaces". In preparation. URL: `http://homepages.warwick.ac.uk/~masda/TOp/`.

[Lan81] William E. Lang. "Classical Godeaux surface in characteristic P". In: *Math. Ann.* 256.4 (1981), pp. 419–427.

[Lie09] Christian Liedtke. "Non-classical Godeaux surfaces". In: *Math. Ann.* 343.3 (2009), pp. 623–637.

[Mir84] Rick Miranda. "Nonclassical Godeaux surfaces in characteristic five". In: *Proc. Amer. Math. Soc.* 91.1 (1984), pp. 9–11.

[Oda69] Tadao Oda. "The first de Rham cohomology group and Dieudonné modules". In: *Ann. Sci. École Norm. Sup. (4)* 2 (1969), pp. 63–135.

[Ols16] Martin Olsson. *Algebraic spaces and stacks*. Vol. 62. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 2016, pp. xi+298.

[Oor05] Frans Oort. "Simple p-kernels of p-divisible groups". In: *Adv. Math.* 198.1 (2005), pp. 275–310.

[Pin] Richard Pink. "Finite Group Schemes". Course Notes. URL: `https://people.math.ethz.ch/~pink/ftp/FGS/CompleteNotes.pdf`.

[Rei19] Miles Reid. "The Tate-Oort Group Scheme $\mathbb{TO}_p$". In: vol. 307. Proceedings of the Steklov Institute of Mathematics. Pleiades Publishing, 2019, pp. 245–266.

[Rei78] Miles Reid. "Surfaces with $p_g = 0$, $K^2 = 1$". In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 25.1 (1978), pp. 75–92.

[Ser79] Jean-Pierre Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979, pp. viii+241.

[SGA3] Philippe Gille and Patrick Polo, eds. *Schémas en groupes (SGA 3). Tome III. Structure des schémas en groupes réductifs*. Vol. 8. Documents Mathématiques (Paris) [Mathematical Documents (Paris)]. Séminaire de Géométrie Algébrique du Bois Marie 1962–64. [Algebraic Geometry Seminar of Bois Marie 1962–64], A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre, Revised and annotated edition of the 1970 French original. Société Mathématique de France, Paris, 2011, pp. lvi+337.

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

[Tat97] John Tate. "Finite flat group schemes". In: *Modular forms and Fermat's last theorem (Boston, MA, 1995)*. Springer, New York, 1997, pp. 121–154.

[TO70] John Tate and Frans Oort. "Group schemes of prime order". In: *Ann. Sci. École Norm. Sup. (4)* 3 (1970), pp. 1–21.

[Wan13] Xingting Wang. "Connected Hopf algebras of dimension p^2". In: *J. Algebra* 391 (2013), pp. 93–113.

[Wat79] William C. Waterhouse. *Introduction to affine group schemes*. Vol. 66. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1979, pp. xi+164.