
Finite Group Schemes and p -Divisible Groups

by Frans Oort*

Introduction

In mathematics we profit from the method of assigning an *algebraic object* (such as a number, a group, a ring, and so on) to a *geometric object*. Many proofs in geometry are unthinkable without this technique. Every reader will know examples (the fundamental group of a topological space, cohomology theories, and discrete invariants like dimension, genus or whatever). Classification often starts by fixing an “invariant”. For objects moving in families we can study “moduli” or the behavior of “jumps” of invariants considered.

This little survey note introduces (a particular and small) part of this story: we see how the algebraic object, the “invariant”, can be a *finite group scheme*, or a *p -divisible group* (or, in special cases, a Galois representation given by a group scheme). We will define and discuss these notions. We will see the way this gives access to the definition and study of new phenomena: in mathematics one wants to discover the structure underlying objects, questions and conjectures considered.

Methods described are particularly useful in geometry over fields of positive characteristic or in geometry and number theory over a number field. There we cannot use analysis and topology in the classical vein. These new methods show a rich vocabulary of new structures that, in a sense, replace our familiar characteristic zero tools. Quite unexpected invariants, stratifications and foliations appear; these have been studied in some detail, and we can enjoy the beauty of these new geometric objects.

* Mathematical Institute, University of Utrecht, The Netherlands
E-mail: f.oort@uu.nl

Early roots we have already seen in work by Gauss and in the belief of Weil that objects in positive characteristic should be treated as geometric objects (and not as algebraic objects obtained from characteristic zero phenomena reduced mod p). Foundations were laid, then Grothendieck and many others carried on in a breathtaking way. Manin started the search for typical positive characteristic structures in the study of moduli spaces of abelian varieties. Tate showed how Tate ℓ -groups and p -divisible groups replace the use of the fundamental group in cases where the classical topology is not anymore present. Many modern proofs in algebraic geometry and in number theory use these new tools. Part of this we describe in this little survey.

A remark on terminology. In this survey we will use theory of schemes; a small part of the first two chapters of the book [30] will suffice; also see [84]. However, if you are not familiar with this terminology, already over a base field you can follow most of the theory below; if we say “over a base scheme” you may restrict to a base ring (commutative, with $1 \neq 0$); already over base rings the theory of finite group schemes offers beautiful results and intriguing questions and problems.

If you want to stick to classical terminology, you can see “an abelian scheme $A \rightarrow S$ ” as a family of abelian varieties parametrized by S ; in this classical language many results have been proved; scheme theory simplifies and gives new insight. In Definition 3 we see that (in most cases) you can treat finite group schemes as algebraic objects (with quite a lot of structure). I am not saying that this makes insight easy, but sometimes direct computations can be done making use of such an algebraic description. – You will be convinced that theory explained below is difficult to

grasp and to describe using only the language of varieties.

Notation. We write K for an arbitrary field, κ for a field, in most cases of positive characteristic, and k for an algebraically closed field. Any base ring R will be commutative, and usually we assume $0 \neq 1$ in R . For a ring R an element $x \in R$ is called nilpotent if there exists $n \in \mathbb{Z}_{>0}$ with $x^n = 0$; in a (commutative) ring the nilpotent elements form an ideal, sometimes denoted by $\sqrt{(0)}$; if there are no nilpotents $x \neq 0$, i.e. if $\sqrt{(0)}$ is the zero-ideal, we say that R is *reduced*; for any R the ring $R/\sqrt{(0)}$ is reduced. For a scheme S nilpotents in the structure sheaf \mathcal{O}_S define a sheaf \mathcal{I} of ideals, and its subscheme of zeros, with structure sheaf $\mathcal{O}_S/\mathcal{I}$, is denoted by $S_{\text{red}} \subset S$; see 1.14. The symbols p and ℓ will be used for prime numbers.

We use the concept “variety” in the following way; a scheme S over a field K is called a variety if for every field extension $K \subset L$ after base change $S \otimes_K L$ we obtain a reduced, irreducible scheme, i.e. S/K is *geometrically reduced and irreducible*.

Suppose X is a scheme over S , e.g. a variety V over a field K . For a morphism $T \rightarrow S$ we write $X_T = X \times_S T$; e.g. if $K \subset L$ we write $V_L = V \otimes_K L$. Classical language often uses the same symbol for V , a variety over K , and for V_L ; however the “variety V over K ” and the “variety V over L ” are “different objects” and should be distinguished in notation.

We will write $\mathcal{A}_g = \cup_d \mathcal{A}_{g,d}$ for the moduli space of polarized abelian varieties, and $\mathcal{A}_{g,1}$ for the moduli space of principally polarized abelian varieties. If working in characteristic p we tend to write $\mathcal{A}_{g,1}$ instead of $\mathcal{A}_{g,1} \otimes \mathbb{F}_p$.

1. (Finite) Group Schemes

1.1. Group Schemes. Here is a short definition:

Definition 1. Consider a base scheme S and consider the category Sch_S of all schemes over S . A *group object* $G \rightarrow S$ in this category is called an *S -group scheme*. This means that for every $X \rightarrow S$ the set $\text{Mor}_S(X, G) = G(X)$ is a group in a functorial way.

This may sound a bit abstract. We discuss the definition and soon we will give many examples, to make you familiar with this concept. As in the category Sch_S of schemes over S (fibered) products exist, and as S with the identity map to S is a final object, i.e. $\text{Mor}_S(X, S)$ consists of one element for every $X \in \text{Sch}_S$ we can rephrase the definition:

Definition 2. There exist morphisms

$$m_G = m : G \times_S G \rightarrow G, \quad i_G = i : G \rightarrow G, \quad e : S \rightarrow G$$

satisfying the usual group axioms.

Definition 3 (Affine group schemes). If $S = \text{Spec}(R)$ is affine, where R is a commutative ring, and $G = \text{Spec}(B) \rightarrow S$ is affine, the R -algebra structure on the commutative R -algebra B ; if G is an S -group scheme the group axioms on $\text{Spec}(B)$ translate into the following homomorphisms

$$\times : B \otimes_R B \rightarrow B \qquad s = s_B : B \rightarrow B \otimes_R B$$

$$\iota = \iota_B : B \rightarrow B$$

$$\eta_B : R \rightarrow B$$

$$\varepsilon_B : B \rightarrow R$$

Here \times and η_B come from the R -algebra structure on B and s_B, ι_B and ε_B define the group structure on $G = \text{Spec}(B) \rightarrow S$:

- the multiplication $m : G \times_S G \rightarrow G$ gives the “co-multiplication” s_B ,
- the inverse in the group object gives the antipode $\iota = \iota_B : B \rightarrow B$ and
- the unit element $e \in G(S)$ gives the augmentation ε_B .

I suggest you spell out the various properties of these maps, obtained from the group axioms, and the way the two definitions group object versus bialgebra agree in case of affine group schemes; for examples see [63], 1.1. Also see [84], Chapter 5.

A commutative R -algebra with this structure is called a *R -bialgebra*. A commutative R -algebra coming from an affine, non necessarily commutative group scheme, is called a *R -Hopf algebra*. Note that the multiplication in \times in the ring B is assumed to be commutative, however the multiplication m on G need not be commutative, respectively the co-multiplication s_B need not be co-commutative.

If $G = \text{Spec}(B) \rightarrow S = \text{Spec}(R)$, and B is finite flat over R of constant rank n we say n is the *order* of G/S .

For a group G or a group scheme G/S and $N \in \mathbb{Z}_{>0}$ we define a map $[N] : G \rightarrow G$, respectively a morphism $[N] : G \rightarrow G$ by $[N](x) = x^N$; for a group scheme G/S with multiplication $m : G \times G \rightarrow G$ this is defined as

$$[N] = \left(G \xrightarrow{\Delta_N} \underbrace{G \times \cdots \times G}_m \xrightarrow{m^N} G \right).$$

1.2. A linear group, or an affine group variety, is a group scheme $G = \text{Spec}(E)$ over a field K such that E is a finite type K -Hopf algebra such that $E \otimes k$ is a domain (no zero-divisors) for any field k containing K . The notions “linear” and “affine” amount to the same here, e.g. see [84], Th. 5.3.1.

An example is $GL_{n,K}$ and any affine group variety can be embedded into an appropriate GL_n . Examples:

$$\mathbb{G}_a = \text{Spec}(K[T]), \quad s(T) = T_1 + T_2, \quad \iota(T) = -T, \quad \varepsilon(T) = 0,$$

the additive group of dimension one, and the multiplicative group of dimension one:

$$GL_1 = \mathbb{G}_m = \text{Spec}(K[T, T^{-1}]), \quad sT = T \otimes T, \\ \iota(T) = T^{-1}, \quad \varepsilon(T) = 1.$$

these group schemes are defined over a prime field, and we use the same notation over any base ring if no confusion can occur.

1.3. Example/Exercise (Tate). To give you a taste of this topic let us discuss the case (“group schemes of order 2”) that in the R -Hopf algebra $E \supset I = \text{Ker}(\varepsilon) \cong R \cdot x$ is *free of rank one over R* ; here a complete classification can be given, and I suggest you prove all details of the following exercise. We see in [109] this is a special case of the classification of group schemes of prime order (over quite general rings, for restrictions see that paper).

- (1) There exists $a \in R$ such that $x^2 = ax$.
- (2) There exists $b \in R$ such that $s(x) = x_1 + x_2 + b(x \otimes x)$ where $x_1 = x \otimes 1$ and $x_2 = 1 \otimes x$. Conclude that the comultiplication s is cocommutative (i.e. G is a commutative group scheme).
- (3) Using $as(x) = s(ax) = s(x^2) = (s(x))^2$ conclude that

$$(ab + 1)(ab + 2) = 0.$$

- (4) Write $\iota(x) = \gamma \cdot x$. Using that ι is the coinverse show

$$\gamma \cdot x + x + b\gamma ax = 0; \text{ hence } 1 + ba \text{ is a unit in } R.$$

- (5) Conclude that $ab = -2 \in R$.
- (6) Conversely, suppose given any ring R (commutative with $0 \neq 1 \in R$) and suppose given $a, b \in R$ with $ab = -2 \in R$. Formulas given above define a group scheme G , that is commutative with I free of R -rank one. Note that choosing $I = R \cdot y$ with $y = ux$, where U is a unit in R gives the structure constants $y^2 = (ua)y$ and $s(y) = y_1 + y_2 + (bu^{-1})(y \otimes y)$; the pairs (a, b) and $(ua, u^{-1}b)$ define isomorphic group schemes.

Conclusion. Group schemes of order 2 over an arbitrary base ring are classified by a choice (a, b) with $ab = -2 \in R$ up to the equivalence described above. For $a, b \in R$ with $ab = -2$ in R , and G is given by:

$$G = G_{a,b} = \text{Spec}(B), \quad B = R[x]/(x^2 - ax),$$

and the group structure (the bi-algebra structure) is given by

$$\varepsilon(x) = 0, \quad s(x) = x \otimes 1 + 1 \otimes x + bx \otimes x, \quad \iota(x) = x.$$

See [109]; [108], 3.2; [3], Section 5; [88], Proposition on page 10.

The classification for $p = 2$ as described above can be generalized to any group scheme of prime order. A classification over an arbitrary base ring can be found in [109], Theorem 2 on page 12. A little warning: some authors define a by $x^p = -ax$; this would give $x^2 = -ax$ and $ab = 2$ in the small example above, just a matter of taste and notation.

Over the base ring $\kappa = \mathbb{F}_p$ we define $\alpha_p = \text{Ker}(F : \mathbb{G}_a \rightarrow \mathbb{G}_a)$, where F denotes the Frobenius morphism. For any $R \supset \mathbb{F}_p$ we use the same notation, instead of $\alpha_p \otimes R$ if no confusion can occur.

Remark/Exercise. Write out the bialgebra for α_p . We see that $\alpha_p = G_{0,0}$ for any base ring.

Explicit cases. $G_{0,0} \cong \alpha_2$ with $\mathbb{F}_p \subset R$, and $G_{-2,1} \cong \mu_{2,R}$, $G_{1,-2} \cong \underline{\mathbb{Z}/2}_R$.

In [109] the case of arbitrary prime order p flat finite group schemes of order p over a quite general ring is treated.

Remark. In particular *any finite group scheme of prime order is commutative*. We have seen in 1.10.2 a non-commutative group scheme of order p^2 over a field. Note a difference: any finite group of order p^2 is commutative, but we see the analogous statement is not correct for group schemes.

1.4. Example. For $k \supset \mathbb{F}_p$ any group scheme N over k of order p is in one of the following isomorphism classes:

- [(loc, et)]

$$N \cong \mu_{p,k},$$

- [(loc, loc)]

$$N \cong \alpha_p,$$

- [(et, et)]

$$N \cong \underline{\mathbb{Z}/p\mathbb{Z}}_k.$$

For a perfect field $\kappa \supset \mathbb{F}_p$ any N_1 with $N_1 \otimes k \cong \mu_{p,k}$ determines and is determined by a Galois representation $\text{Gal}(k/\kappa) \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$,

for any N_1 with $N_1 \otimes k \cong \alpha_p$ we have $N_1 \cong \alpha_p$, any N_1 with $N_1 \otimes k \cong \underline{\mathbb{Z}/p\mathbb{Z}}_k$ determines and is determined by a Galois representation $\text{Gal}(k/\kappa) \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$.

This can be showed using [109]; also see 1.10.

1.5. Structure. Over a field we have a good insight what kind of group schemes exist. We a morphism $T \rightarrow \text{Spec}(K)$ is algebraic, we say T is an algebraic scheme over K , if this morphism is of finite type.

An algebraic group scheme G over a field K (algebraic means of finite type) can be one of the following types:

- (f). *Finite group schemes*: $\text{Spec}(B)$ as above, with $\dim_K(B) < \infty$.
- (lin). *Linear group schemes*: a closed (irreducible, reduced) subgroup scheme of a the linear group $\text{GL}_{n,K}$.
- (AV). *Abelian varieties*. We say A is an abelian variety if A is a group scheme over a field K , the structure sheaf of $A \otimes k$ has no nilpotents, A is connected and A is a projective scheme. This implies that the group law on A is commutative. The name comes from the fact that Niels Henrik Abel constructed such varieties for computing values of “abelian integrals” on Riemann surfaces.

In each of these three categories we see interesting structures and many applications.

We will see that every group scheme of finite type after a base field extension admits a filtration with every subquotients contained in one of these three categories.

1.5.1. Although we use schemes you might be interested using more classical terminology.

- Over an arbitrary field K , a *variety* V is a separated scheme of finite type such that $V \otimes k$ is reduced and irreducible for any algebraically closed $k \supset K$. Example: if $K \subsetneq L$ is a field extension, $\text{Spec}(L)$ is a scheme over $\text{Spec}(K)$ but is it not a variety over K ; see 1.14.
- For a group scheme G of finite type over a field K such that $G \otimes_K k$ is reduced and irreducible for any algebraically closed $k \supset K$ we will use the terminology *group variety*.
- For a group variety over K that can be embedded into some $\text{GL}_{n,K}$ we use *linear algebraic group*.
- An abelian scheme over a field will be called an abelian variety; this is a group variety over a field that is complete (proper over K).

1.5.2. A Structure Theorem by Chevalley, see [13]; for a survey see [14]. Suppose G is a group scheme of finite type over a *perfect field* P . Then:

the connected component $(G^0)_{\text{red}}$ of the unit element is a normal, closed subgroup scheme, $(G^0)_{\text{red}}$ is a group variety and $G/(G^0)_{\text{red}}$ is a finite group scheme.

Moreover

Theorem (Chevalley). *For any group variety G over a perfect field P there is a unique maximal linear subgroup variety $H \subset G$, this is a normal subgroup variety and G/H is an abelian variety.*

Corollary. *Suppose G is an algebraic group scheme over a field K . There exists a finite extension $K \subset L$ and a filtration*

$$H \subset ((G_L)^0)_{\text{red}} \subset G_L$$

such that $H \subset ((G_L)^0)_{\text{red}}$ is a linear subgroup variety over L , and $((G_L)^0)_{\text{red}}/H$ is an abelian variety and $G_L/((G_L)^0)_{\text{red}}$ is a finite group scheme, all over L .

We will see that commutative finite group schemes will be crucial in a better understanding of abelian varieties. That is the essence of this note.

In general a connected, reduced group scheme over a field is not a group variety; $\text{Spec}(\mathbb{Q}(\sqrt{-3})) = \mu_{3,\mathbb{Q}}/\text{Spec}(\mathbb{Q})$ is a scheme consisting of one point, but $\mu_{3,L}$ is reducible for any $L \supset \mathbb{Q}(\sqrt{-3})$.

A reduced subscheme of a group scheme need not be a subgroup scheme (over a non-perfect field), see 1.15.4.

1.6. We note that for any homomorphism $f : G_1 \rightarrow G_2$ on S -group schemes $\text{Ker}(f) \subset G_1$ does exist as a closed subgroup scheme, namely by the cartesian diagram (defined as a fibered product):

$$\begin{array}{ccc} \text{Ker}(f) \hookrightarrow & G_1 & \\ \downarrow & & \downarrow f \\ S & \xrightarrow{e} & G_2. \end{array}$$

We do not discuss the notion of quotients and resulting theorems.

Let $G \rightarrow \text{Spec}(K)$ be an algebraic group scheme, and $e \in G(K)$ the identity element for the group operation. We write G^0 for the connected component of $e \in G(K)$, called the identity component of G . We know that G^0 is geometrically irreducible, in particular for any $K \subset K'$ we have $(G^0)_{K'} = (G_{K'})^0$; e.g. see [26]², 4.5.14.

We know that the following phenomenon can happen: an irreducible zero-set becomes reducible after extension of base field. For example $X^2 + Y^2 \in \mathbb{R}[X, Y]$ defines an irreducible zero-set, which however becomes reducible over \mathbb{C} as $X^2 + Y^2 = (X + \sqrt{-1} \cdot Y)(X - \sqrt{-1} \cdot Y) \in \mathbb{R}[X, Y]$. As we see, this does not happen for algebraic group varieties, but it can happen for algebraic group schemes.

1.7. Some Examples. We give examples over \mathbb{Z} , base-changed to any ring.

1.7.1. We write $\mathbb{G}_{m,\mathbb{Z}}$ for the *multiplicative group*; it is given by the algebra $\mathbb{Z}[T, 1/T]$ with comultiplication $s(T) = T \otimes T$ and antipode $\iota T = T^{-1}$.

Suppose $n \in \mathbb{Z}_{>1}$. We define the finite group scheme of “ n -the roots of unity by

$$\begin{aligned} E &= \mathbb{Z}[T, 1/T]/(T^n - 1), \\ \mu_{n,\mathbb{Z}} &= \text{Spec}(\mathbb{Z}[T, 1/T]/(T^n - 1)) \subset \mathbb{G}_{m,\mathbb{Z}}, \end{aligned}$$

or, $\mu_{n,\mathbb{Z}} = \mathbb{G}_{m,\mathbb{Z}}[n]$. Note that $\mu_{n,\mathbb{Z}}$ is etale after base change to $\mathbb{Z}[1/n] \rightarrow \mathbb{Z}$. However for every prime number p dividing n the group scheme μ_{n,\mathbb{F}_p} is not etale; μ_{p,\mathbb{F}_p} is a local group scheme of order p , consisting as a scheme of one point.

1.7.2. For every $n \geq 1$ we write $\mathrm{GL}_{n,\mathbb{Z}}$ for the *General Linear group*, the group scheme that associates to every ring B the multiplicative group $\mathrm{GL}_n(B)$ of invertible $n \times n$ matrices with entries in B , i.e. such matrices with determinant a unit in B . We see that $\mathbb{G}_m = \mathrm{GL}_1$, and $\mathbb{G}_a \hookrightarrow \mathrm{GL}_2$ as matrices

$$\mathbb{G}_a(B) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \subset \mathrm{GL}_2(B), \quad t \in B.$$

1.7.3. Constant Group Schemes. Let H be a (an abstract) finite group. Let S be base scheme. We write \underline{H}_S for the constant group scheme over S with fibers equal to H ; That is, for $T \rightarrow S$ with T connected, $\underline{H}_S(T) = H$. For example, for $S = \mathrm{Spec}(R)$ we have $\underline{H}_S = \mathrm{Spec}(R^H)$ and the group law on H gives the comultiplication on $R^H \cong R^{\#(H)}$.

If K is a field, $n \in \mathbb{Z}_{>1}$ and $\mathrm{char}(K)$ does not divide n and $T^n - 1 \in K[T]$ factors in linear factors, “all n -th roots of unity are in K ”, a choice $\zeta_n \in K$ gives an isomorphism

$$\underline{\mathbb{Z}/n}_K \cong \mu_{n,K}.$$

1.8. Cartier Duality. Let $N \rightarrow S$ be a commutative, finite flat group scheme. In this case Cartier defined N^D/S , and $N = N^{DD}/S$. Here is the definition in case $S = \mathrm{Spec}(R)$ and $N = \mathrm{Spec}(B)$: we define $N^D = \mathrm{Spec}(\mathrm{Hom}_R(B, R))$; one easily shows

the bialgebra maps produce the structure of an R -bialgebra on $B^D := \mathrm{Hom}_R(B, R)$,

e.g. see [63], 1.2. For an arbitrary base scheme S constructions locally on S paste to the desired $N^D \rightarrow S$. The reader can work out interesting details, such as the fact that the multiplication in the ring B induces the comultiplication on B^D , etc. Examples:

$$(\underline{\mathbb{Z}/n}_S)^D = \mu_{n,S} \text{ and } (\alpha_{p,\kappa})^D \cong \alpha_{p,\kappa} \text{ for any } \kappa \supset \mathbb{F}_p.$$

Note that Cartier duality for a non-commutative group scheme would produce an algebra with non-commutative multiplication; such rings however are not considered in present algebraic geometry.

1.9. Frobenius and Verschiebung. See [25], I, Exp. VIIA.4. In this subsection all rings and schemes are over \mathbb{F}_p . For an \mathbb{F}_p -algebra B the *absolute Frobenius* is denoted by

$$\mathrm{Frob} : B \rightarrow B, \quad x \mapsto x^p.$$

For a scheme $T \rightarrow S$ we define $T^{(p/S)}$, called the Frobenius twist. It is defined by the commutative, cartesian

diagram

$$\begin{array}{ccc} T^{(p/S)} & \longrightarrow & T \\ \downarrow & \mathrm{Frob} & \downarrow \\ S & \longrightarrow & S. \end{array}$$

Here is a down-to-earth definition. If $T \rightarrow S = \mathrm{Spec}(R)$ and an affine chart of T is given by polynomials

$$\sum_{\alpha} a_{i,\alpha} X^{\alpha}$$

in multi-index notation $X^{\alpha} = X_1^{\alpha_1} \times \dots \times X_m^{\alpha_m}$, then $T^{(p/S)}$ is defined by the polynomials

$$\sum_{\alpha} a_{i,\alpha}^p X^{\alpha}.$$

We define an S -morphism $F : T^{(p/S)} \rightarrow T$ by the diagram

$$\begin{array}{ccc} T & & \\ \downarrow & \mathrm{Frob} & \downarrow \\ T^{(p/S)} & \longrightarrow & T \\ \downarrow & \mathrm{Frob} & \downarrow \\ S & \longrightarrow & S. \end{array}$$

(A dashed arrow labeled F points from T to $T^{(p/S)}$ in the above diagram.)

In down-to-earth terms: a point (x_1, \dots, x_m) on a local chart of T maps to (x_1^p, \dots, x_m^p) . This makes sense because

$$\sum_{\alpha} a_{i,\alpha}^p (X^{\alpha})^p = \left(\sum_{\alpha} a_{i,\alpha} X^{\alpha} \right)^p.$$

Note that for any group scheme $G \rightarrow S$ the relative Frobenius $F : G^{(p/S)} \rightarrow G$ is a homomorphism.

For a *commutative, flat* $G \rightarrow S$ one can define $V : G \rightarrow G^{(p/S)}$; we refer to [25], I, Exp. VIIA.4.3 for the construction. Note that

$$(G^{(p/S)} \xrightarrow{V} G \xrightarrow{F} G^{(p/S)}) = [p], \quad (G \xrightarrow{F} G^{(p/S)} \xrightarrow{V} G) = [p].$$

1.10. Some Finite Group Schemes in Positive Characteristic. Later in this note we will explain a difference between group schemes in characteristic zero on the one hand and in positive characteristic on the other hand, e.g. see 1.16. At first we give some examples. All fields in this section are in characteristic $p > 0$: $\kappa \supset \mathbb{F}_p$.

1.10.1. For any κ we write $\alpha_p = \mathrm{Ker}(F : \mathbb{G}_a \rightarrow \mathbb{G}_a)$. This is the same as: $\alpha_p = \kappa[\tau]$ with $\tau^p = 1$ and $s(\tau) = \tau \otimes 1 + 1 \otimes \tau$, $\iota(\tau) = -\tau$. Note that if $\kappa \subset k$, and N is a finite group scheme over κ with $N \cong \otimes k \cong \alpha_{p,\kappa} \otimes k$ then $N \cong \alpha_{p,\kappa}$. Hence we write α_p without mentioning the base field; however with this notation $\mathrm{Hom}(\alpha_p, \alpha_p)$ is ambiguous.

Over $k \supset \mathbb{F}_p$ we see three (isomorphism classes of a) finite group scheme(s) of order p , see 1.4:

$$\mu_{p,k} \quad \alpha_p, \quad \underline{\mathbb{Z}/p}_k.$$

Using Dieudonné module theory is easily seen that these are the only ones of order p . Moreover, for any base Cartier duality gives $(\alpha_p)^D \cong \alpha_p$. For any base in any characteristic $(\mu_{p,S})^D \cong \mathbb{Z}/p_S$.

1.10.2. Here is an example of a non-commutative finite group scheme. We define G over $R \supset \mathbb{F}_p$ by

$$G(C) = \begin{pmatrix} \rho & \tau \\ 0 & 1 \end{pmatrix}, \quad \rho^p = 1, \quad \tau^p = 0$$

for any commutative R -algebra C . We can easily write out the coordinate ring of G , and the group axioms (the maps defining this bialgebra). Note that $\text{rank}(G/\text{Spec}(R)) = p^2$.

1.11. Dieudonné Modules. In this subsection all rings and schemes are over \mathbb{F}_p and group schemes are finite and *commutative*. For a *perfect* field $\kappa \supset \mathbb{F}_p$ we write $\Lambda = \Lambda_\kappa$ for the ring of infinite Witt vectors; W_∞ is the usual notation, but we will use the letter W later; we write $\sigma : \Lambda \rightarrow \Lambda$ for the lift of the Frobenius on κ . The Dieudonné ring R_κ is the ring $R_\kappa = \Lambda_\kappa[\mathcal{F}, \mathcal{V}]$ with relations

$$\mathcal{F}\mathcal{V} = p = \mathcal{V}\mathcal{F}, \quad \mathcal{F}\beta = \beta^\sigma \mathcal{F}, \quad \mathcal{V}\beta^\sigma = \beta \mathcal{V}, \quad \beta \in \Lambda.$$

A left R_κ -module is called a Dieudonné module. Note that R_κ is a commutative ring if and only if $\kappa = \mathbb{F}_p$.

There is an (covariant) equivalence $\mathbb{D}(N) = M$ between on the one hand

the category of finite, commutative group schemes N over κ .

and on the other hand

the category of left modules M of finite length over R_κ .

In [47] the contravariant theory is proved; also see [15]; that theory with Cartier duality gives the covariant theory.

A remark on notation. The homomorphism $F : N \rightarrow N^{(p)}$ in the *covariant* theory is transformed into \mathcal{V} and $V : N^{(p)} \rightarrow N$ into \mathcal{F} ; for this reason we distinguish F (on schemes) and \mathcal{F} (on Dieudonné modules) and V and \mathcal{V} .

There are many generalizations of the above theorem; it would take a lot of space to discuss these. and we will not do so here. See [8], Section 4. For the case of finite group schemes annihilated by F over an arbitrary (not necessarily perfect) field $\kappa \supset \mathbb{F}_p$ see [16], II.7.4.2.

1.11.1. We see that

$$\mathbb{D}(\alpha_p) \cong \kappa, \text{ with } \mathcal{F} \text{ and } \mathcal{V} \text{ acting as zero on } \mathbb{D}(\alpha_p),$$

$$\mathbb{D}(\alpha_p) = R_\kappa/R_\kappa(\mathcal{F}, \mathcal{V})$$

$\mathbb{D}(\mu_{p,\kappa}) \cong \kappa$ with \mathcal{F} acting as zero and \mathcal{V} acting as $\mathcal{V}\beta^\sigma = \beta\mathcal{V}$,

$$\mathbb{D}(\mu_{p,\kappa}) = R_\kappa/R_\kappa(\mathcal{F}, \mathcal{V} - 1),$$

and $\mathbb{D}(\mathbb{Z}/n_\kappa) \cong \kappa$ with $\mathcal{F}\beta = \beta^\sigma \mathcal{F}$ and \mathcal{V} acting as zero

$$\mathbb{D}(\mathbb{Z}/n_\kappa) = R_\kappa/R_\kappa(\mathcal{F} - 1, \mathcal{V}).$$

Many more examples can be made along these lines. We will see many applications later.

1.12. Local and Etale Group Schemes. A finite group scheme $N = \text{Spec}(B)$ over a field K is called local, if B is a local ring; for $K \supset \mathbb{F}_p$ this is equivalent to the condition $F^n = 0$ on N for $n \gg 0$.

1.12.1. An etale morphism in algebraic geometry is the analogue of a finite unramified cover in topology; however in the algebraic context also we have to take care also of algebraic phenomena like inseparability. For a definition see [24], I.4 and III.1.2. Also see [26], IV.4.17, e.g. Corollaire 17.6.2. An etale morphism locally of finite presentation $T \rightarrow S$ is flat and unramified, and this can be taken as a definition, see [26], 17.6.1. A morphism is etale if and only if it is smooth and of relative dimension zero. We will say a ring extension $R \hookrightarrow B$ is etale if $\text{Spec}(R) \leftarrow \text{Spec}(B)$ is etale.

1.12.2. Here are some examples of etale ring extensions.

- (1) $R = K$, a field, and $B = K_1 \times \cdots \times K_n$ and every $K \subset K_i$ is a finite, separable extension; these are all etale ring extensions of a field.
- (2) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-1})$; $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-1}, 1/2]$;
- (3) Let $T \rightarrow S$ be etale, and $U \subset T$ a dense open subscheme; then $U \rightarrow S$ is etale (being etale is a property locally on T). E.g. $\mathbb{Q}[X] \subset \mathbb{Q}[X, Y]/XY - 1$ is etale although above the prime ideal $(X) \subset \mathbb{Q}[X]$ there is no prime ideal in $\mathbb{Q}[X, Y]/XY - 1$.
- (4) Let $R \rightarrow B$, and $P \subset B$ a prime ideal and $P' = P \cap R$. The inclusion is etale at P if and only if $P' \cdot B_P$ equal the maximal ideal of the local ring B_P , and the extension of residue class fields $R_{P'}/P'R_{P'} \subset B_P/PB_P$ is separable.

Here are some examples of ring extensions that are not etale.

- (5) $\mathbb{F}_p(t) \subset \mathbb{F}_p(\sqrt[p]{t})$;
- (6) $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-1}]$;
- (7) $\mathbb{Z} \subset \mathbb{Z}[T]$;
- (8) $\mathbb{Q}[X, Y] \subset \mathbb{Q}[X, Y, T]/(X - YT)$.
- (9) Any purely inseparable extension $K \subsetneq K'$ is not etale.

1.12.3. We say a finite group scheme $N \rightarrow S$ is etale if N/S is flat of finite presentation and N/S is etale.

Note. Suppose $S = \text{Spec}(K) \leftarrow N = \text{Spec}(B)$. We see N/S is a finite etale group scheme if B is as in (1) above. If moreover K is perfect, this is the case if and only if every $K \subset K_i$ is a finite extension.

An aside. Suppose $T \rightarrow S$ is a finite etale morphism, and S is connected with a marked point $s \in S$. In this situation $T \rightarrow S$ defines a continuous representation $\pi_1^{\text{et}}(S, s)$ in a finite set (a geometric fiber of T/S and every T/S as above is obtained in this way. - This shows etale finite group schemes over a field are given by a Galois representation $\text{Gal}(K^{\text{sep}}/K)$.

1.12.4. We will see examples of a finite group scheme N over a non-perfect field K such that N is a reduced scheme, but $N \otimes K'$ is not reduced for some extension $K \subset K'$, see 1.15.

However if N is finite etale over K , then N is reduced if and only if $N \otimes K'$ is reduced for every extension $K \subset K'$. Over a perfect field finite etale is the same as finite reduced.

Moreover, over any field K a finite etale group scheme N is of the form

$$N \cong \text{Spec}(B), \quad B = K_1 \times \cdots \times K_n$$

where every $K \subset K_i$ is a finite, separable extension.

1.12.5. We will say that N/K is local-etale if $N = \text{Spec}(B)$, where B is a local ring, and the Cartier dual $N^D = \text{Spec}B^D$ is etale.

In the same way we define local-local, etale-local and etale-etale finite group schemes over a field.

For any finite group scheme N over a field we have $N^{(0)}/K$, the connected component of the identity element. We will see that in general

$$1 \rightarrow N^{(0)} \rightarrow N \rightarrow N/N^{(0)} \rightarrow 1$$

does not split; this is the starting point of “Serre-Tate parameters”, see 8.11. However over a perfect field the extension does split, and we obtain the following

1.12.6. Structure Theorem. *Any finite, commutative group scheme over a perfect field κ has the following subgroup schemes*

$$N_{\text{loc,et}}, N_{\text{loc,loc}}, N_{\text{et,loc}}, N_{\text{et,et}} \subset N,$$

with $N_{\text{loc,et}}$ of local-etale type, etc, and

$$N = N_{\text{loc,et}} \times N_{\text{loc,loc}} \times N_{\text{et,loc}} \times N_{\text{et,et}}.$$

E.g. see [63], I.2.

Examples. Over a field κ of characteristic p we have:

- μ_p is local-etale,
- α_p is local-local,
- \mathbb{Z}/p_κ is etale-local;

moreover

N is etale-etale if and only if its order is prime to the characteristic of κ .

1.13. Lifting. Suppose G_0 is a group scheme over $\kappa \supset \mathbb{F}_p$. We say a group scheme $G \rightarrow \text{Spec}(B)$ is a lifting to characteristic zero if B is an integral domain in characteristic zero and

$$B \rightarrow \kappa, \quad G \otimes_B \kappa \cong G_0.$$

Just two examples:

1.13.1. The group scheme in 1.7.2 does not admit any lifting to characteristic zero; indeed, one can show that G after going to an algebraic closure of the field of fractions of B would be a constant group scheme of order p^2 , hence commutative by easy group theory; this would imply G and G_0 are commutative, a contradiction.

1.13.2. The group scheme α_p over a perfect field $\kappa \supset \mathbb{F}_p$ does not lift to the ring of infinite Witt vectors $\Lambda_\kappa \rightarrow \kappa$ (we need ramification), but α_p does lift to $\Lambda_\kappa[\sqrt{p}] \rightarrow \kappa$. This can easily be deduced from the classification in [109].

1.13.3. This is a particular case of the fact that any finite commutative group scheme does admit a lifting to characteristic zero, see [80]. For more information see [66], [7].

Remark. The topic of lifting to characteristic zero has many aspects and interesting cases, such as varieties of arbitrary dimension, curves with an automorphism, CM abelian varieties, and much more. This rich field is not treated here.

1.14. The Reduced Underlying Scheme. For any scheme T the sheaf of nilpotents elements (with the element 0) form an ideal; dividing out this ideal in the structure sheaf gives a subscheme denoted by $T_{\text{red}} \subset T$.

If G is a group scheme over a perfect field the subscheme $G_{\text{red}} \subset G$ is a sub group scheme. However, if k is non-perfect this need not be the case. We will see examples.

1.15. Hidden Nilpotents. We have seen that an irreducible algebraic group scheme over a field stays irreducible after base change. However as reduced group scheme need not stay reduced after extension of the base field.

Definition. We say a scheme $X \rightarrow S$ has *hidden nilpotents* if there exists $T \rightarrow S$ such that

$$(X \times_S T)_{\text{red}} \subsetneq X_{\text{red}} \times_S T,$$

i.e. if new nilpotents show up after base change.

Already in classic al situations these can appear, e.g. in ramified situations:

$$(\mathbb{Z}[\sqrt{-1}] \otimes_{\mathbb{Z}} \mathbb{F}_2)_{\text{red}} = \mathbb{F}_2 \subsetneq \mathbb{F}_2[\varepsilon]/(\varepsilon^2) = (\mathbb{Z}[\sqrt{-1}] \otimes_{\mathbb{Z}} \mathbb{F}_2).$$

Or in families with “multiple fibers:

$$\begin{aligned} & (K[X, Y, t]/(Y^2 - tX) \otimes_K k[t])_{\text{red}} \\ & \subsetneq K[X, Y, t]/(Y^2 - tX) \otimes_K k[t] \quad t \mapsto 0. \end{aligned}$$

If $\mathbb{Q} \subset K \subset L$ and R is a reduced K -algebra, then $R \otimes_K L$ is reduced. However in positive characteristic this does not hold.

1.15.1. Here is an easy example: $\kappa[X, Y]/(X^p - aY^p)$ with $a \notin \kappa^p$ where p is the characteristic of κ .

1.15.2. Example. See [11], 3.10. Consider $K = \mathbb{F}_2(t)$, a transcendental extension of \mathbb{F}_2 . Let $E \subset \mathbb{P}_K^2$ be given as

$$E = \mathcal{Z}(Y^2Z + XYZ + X^3 + tZ^3).$$

This is a non-singular curve of genus one. As is usual, we take the point whose projective coordinates are $[x = 0 : y = 1 : z = 0]$ as the unity element for the group law, and we obtain an elliptic curve E . As a group scheme we can consider $E[2]$, the 2-torsion on this abelian variety of dimension one. It is the scheme-theoretic kernel of the endomorphism $[2]_E : E \rightarrow E$, multiplication by 2 for the group law of E . We see that as a scheme $E[2]$ is a *disjoint* union $\mu_2 \sqcup T$, where $\mu_2 \cong \text{Spec}(K[\tau]/\tau^2)$ and $T \subset E$ is a *reduced* subscheme (reduced means its structure sheaf has no nilpotents), with $T \cong \text{Spec}(K[Y]/(Y^2 + t))$. However $T \times_{\text{Spec}(K)} \text{Spec}(K[\sqrt{t}]) \cong \text{Spec}(K[\sqrt{t}][Y]/((Y + \sqrt{t})^2))$: after base change nilpotents show up.

1.15.3. The previous example works for every prime number; we just took $p = 2$ in order to have simpler equations. Consider E_0 an ordinary elliptic curve over $\kappa = \mathbb{F}_p$ and the equal characteristic deformation space $\mathcal{E} \rightarrow \text{Spf}(\kappa[[t]])$. The elliptic curve \mathcal{E}_η over $K := \kappa((t))$ has hidden nilpotents, just as before.

We could also consider an arbitrary principally polarized, ordinary abelian variety (A_0, λ_0) and $(A, \lambda)/K$ the formal equal characteristic universal deformation; for this case $A_\eta[p]$ is reduced, with hidden nilpotents, and $A[p]_{\text{red}} \subset A[p]$ is not a subgroup scheme, quite analogous to the example above.

1.15.4. Example. See [18]: an exercise in 3.1. Let $a \in \kappa$, and $a \notin \kappa^p$, where p is the characteristic of κ . Consider $\mathbb{G}_a = \text{Spec}(\kappa[T])$. Let

$$\mathbb{G}_a \supset N = \text{Spec}(\kappa[T]/(T^{p^2} + aT^p)).$$

Then: $N \subset \mathbb{G}_a$ is a subgroup scheme, as topological space N consists of p points, N^0 is not reduced, $N \setminus N^0$ consists of the disjoint union of $p - 1$ reduced subschemes, N_{red} is not a subgroup scheme of \mathbb{G}_a .

Conclusion. Group schemes over non-perfect base schemes should be handled with some extra care, not necessary over perfect fields (such as characteristic zero fields).

1.16. Group Schemes in Characteristic Zero Are Reduced. Cartier proved that

over a field K of characteristic zero an algebraic group scheme is etale,

hence reduced, [4], page 109. For an easy proof for algebraic group schemes, see [64]; also see [112], 11.3, Theorem; see [49], Th. 9.3, see [103], 2.4; see [101], 38.8.3 for the general case.

As a corollary: any finite flat group scheme $N \rightarrow S$ such that *the order of N/S is invertible in the sheaf of local rings on S* is etale. This reduces the case of finite group schemes in this case to representations of the fundamental group, in particular to representations of the Galois group if we work over a field.

From now on group schemes considered will be *commutative*, and any finite group scheme $N \rightarrow S$ is moreover supposed to be *of finite presentation and flat* over S .

Here is some literature that can be used: [8], [14], [15], [16], [47], [49], [80], [64], [63], [83], [88], [103], [108], [109], [112].

2. Tate ℓ -Groups

In this section ℓ is a prime number.

2.1. Definition. Fix $h \in \mathbb{Z}_{>0}$. Choose a base scheme S . A Tate ℓ -group of rank h over S is projective system $\{N_j \mid j \in \mathbb{Z}_{>0}\}$, such that N_j/S is an *etale* group scheme of height ℓ^{hj} , we have $N_{j+1} \rightarrow N_j$ and every geometric fiber over $s \in S(\Omega)$ of N_j/S is isomorphic with the constant group scheme $(\mathbb{Z}/\ell^j_{\Omega})^h$.

Note that giving a Tate ℓ -group of rank h is the same as giving a continuous representation of $\pi_1(S)$ on \mathbb{Z}_ℓ^h . Here \mathbb{Z}_ℓ is the additive group of ℓ -adic numbers. In case $S = \text{Spec}(K)$ this a continuous representation of $\text{Gal}(K^{\text{sep}}/K)$.

2.2. Example. For any S such that ℓ is invertible on S the projective system

$$T_\ell(\mathbb{G}_{m,S}) = \{\mathbb{G}_{m,S}[\ell^j] \mid j\}$$

is a Tate ℓ -group of height 1.

2.3. Basic Example. Suppose ℓ is invertible on S , let $A \rightarrow S$ be an abelian scheme of relative dimension g . The projective system

$$T_\ell(A) = \{A[\ell^j] \mid j\}$$

is a Tate ℓ -group of rank $2g$.

Suppose A is an abelian variety over \mathbb{C} , and let

$$0 \rightarrow \Lambda \rightarrow \mathbb{C}^g \rightarrow \mathbb{C}^g/\Lambda \cong A(\mathbb{C}) \rightarrow 0$$

be the complex uniformization with lattice $\pi_1^{\text{top}}(A(\mathbb{C}), 0) \cong \Lambda \cong \mathbb{Z}^{2g}$, the topological fundamental group. In this case we have

$$T_\ell(A) = \varprojlim \Lambda/\ell^j \cdot \Lambda = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell.$$

We see that for an abelian variety B over a field $K \subset \mathbb{C}$ the Tate ℓ -module $T_\ell(B)$ is determined by a Galois action on the ℓ -adic version of the fundamental group of $A = B \otimes \mathbb{C}$.

Note that the Grothendieck fundamental group $\pi_1^{\text{et}}(A, 0)$ admits the comparison between its profinite completion and the topological fundamental group

$$\pi_1^{\text{et}}(A, 0)^\wedge \cong \pi_1^{\text{top}}(A(\mathbb{C}), 0)$$

for an abelian variety over \mathbb{C} .

For an abelian variety B over a field $K \subset \mathbb{C}$, and $k = \overline{K}$, we obtain an exact sequence

$$0 \rightarrow \pi_1(B_k, 0) \rightarrow \pi_1(B, 0) \rightarrow \pi_1(\text{Spec}(K)) \cong \text{Gal}(k/K) \rightarrow 0$$

with $\pi_1(B_k, 0) \cong \pi_1^{\text{top}}(B(\mathbb{C}), 0)$.

We see a bridge between arithmetic and topology: for an abelian variety over a field $K \subset \mathbb{C}$ it was the wonderful idea of Tate, the Tate conjecture, that replacing $\pi_1(A(\mathbb{C})) \cong \Lambda$ by the Galois module $T_\ell(B)$ gives access to arithmetic properties of B/K . This tool has been of decisive use in work by Tate, Faltings, Wiles and many others.

Tate ℓ -modules as Galois representations are of important use as long as ℓ is invertible on S . However in case the characteristic of the base scheme is equal to ℓ this causes problems. Some authors then use the “physical” Tate module. However, then there is a problem. We give two examples showing this difficulty.

2.3.1. Suppose you have a family of elliptic curves $E \rightarrow S$ over a base in characteristic p , and points $0, \eta \in S$ such that

$$E_{\kappa(\eta)}[p](\overline{\kappa(\eta)}) \cong \mathbb{Z}/p, \quad \text{and} \quad E_{\kappa(0)}[p](\overline{\kappa(0)}) = 0.$$

This is the example where the generic fiber is ordinary and a special fiber is supersingular. For example any “universal” elliptic curve in positive characteristic has this property. The collection of geometric p^j -torsion points do not fit into a flat (constant rank) group scheme.

Still you can apply this method for abelian schemes where the p -rank is constant.

2.3.2. The same problem arises in mixed characteristic. Suppose you have an abelian scheme over a domain R in mixed characteristic, the field of fractions

had characteristic zero, and a residue field $R \rightarrow \kappa \supset \mathbb{F}_p$ has characteristic p . Also here the collection of geometric p^j -torsion points inside A/S do not fit into a flat (constant rank) group scheme over R .

One can use “ ℓ -adic methods” in characteristic p , or if the residue characteristic equals p as long as $\ell \neq p$. However for the case $\ell = p$ another concept had to be developed.

3. p -Divisible Groups

In this section p is a prime number, and no restriction is made on p in relation with a base scheme used. Unimportant detail: in the previous section projective limit were used; for the concept of p -divisible groups discussed here inductive limits (unions) are used; this turns out to be somewhat easier to handle, but there is no essential difference between the setup using either projective or inductive limits. In the literature you will find “Barsotti-Tate groups” for the equivalent notion of p -divisible groups.

3.1. Definition. Suppose $h \in \mathbb{Z}_{>0}$. Let S be a base scheme. A p -divisible group of height h is an inductive system

$$\{G_i \mid G_i \hookrightarrow G_{i+1}, i \geq 1\}, G_i \rightarrow S$$

is finite, commutative, locally free of order p^{ih} , G_i is annihilated by p^i and for every i and j the multiplication $[p_i] : G_{i+j} \rightarrow G_{i+j}$ factors as the composition of a faithfully flat $G_{i+j} \rightarrow G_j$ and an inclusion $G_j \hookrightarrow G_{i+j}$; we obtain the following exact sequence

$$0 \rightarrow G_i \rightarrow G_{i+j} \xrightarrow{[p^i]} G_j \rightarrow 0.$$

Observe that $G_i = G[p^i]$. We can write $G = \cup G_i = \varinjlim G_i$. As $[p] : G \rightarrow G$ is epimorphic, in an appropriate sense, these objects are called “ p -divisible”. For more information see [105], [34]. Note that $G_{i+j}/G_i = G_j$; in particular $G_{i+1}/G_i = G_1$, i.e. a p -divisible group is a tower with building blocks (successive quotients) equal to G_1 .

We say that a p -divisible group X over a field is *simple* if every sub- p -divisible group is either zero or equal to X ; note that a non-zero simple p -divisible groups does contain many subgroup schemes. Later in this note we shall discuss the question whether G_1 determines G , see § 7.

3.2. Examples.

(1) We write $\mathbb{G}_m[p^\infty]$, or μ_{p^∞} , for the inductive system

$$\mu_{p^\infty} = \{\mu_{p^i} \hookrightarrow \mu_{p^{i+1}} \mid i\}$$

(over any base); here $h = 1$.

(2) Over any base scheme S we write $\underline{\mathbb{Q}}_p/\underline{\mathbb{Z}}_{p_S}$ for the inductive system

$$G = \{\dots \underline{\mathbb{Z}}/p^i_S \hookrightarrow \underline{\mathbb{Z}}/p^{i+1}_S \dots\}; \quad h = 1.$$

(3) Let $A \rightarrow S$ be an abelian scheme of relative dimension g . Then

$$A[p^\infty] = \{\dots A[p^i] \hookrightarrow A[p^{i+1}] \dots\}$$

is a p -divisible group of height $h = 2g$. Reminder: $A[n] = \text{Ker}(\times n : A \rightarrow A)$.

3.3. The Serre Dual. For a p -divisible group $G = \cup_i G_i$ the exact sequence

$$0 \rightarrow G_i \rightarrow G_{i+j} \rightarrow G_j \rightarrow 0$$

under Cartier duality produces the exact sequence

$$0 \rightarrow G_j^D \rightarrow G_{i+j}^D \rightarrow G_i^D \rightarrow 0;$$

we define

$$G^t = \{\dots G_j^D \hookrightarrow G_{j+1}^D \dots\}, \quad \text{the Serre dual of } G.$$

3.4. The Duality Theorem. Let A, B be abelian schemes over an arbitrary base scheme S . Suppose $\varphi : A \rightarrow B$ is an S -isogeny (i.e. a homomorphism with finite kernel; it follows this kernel is flat over S), i.e. we have an exact sequence

$$0 \rightarrow N := \text{Ker}(\varphi) \rightarrow A \xrightarrow{\varphi} B \rightarrow 0.$$

This gives rise naturally to an exact sequence

$$0 \rightarrow N^D = \text{Ker}(\varphi^t) \rightarrow B^t \xrightarrow{\varphi^t} A^t \rightarrow 0.$$

See [63], Th. 19.1

3.5. Elliptic Curves Over \mathbb{Z} ?

Theorem (Tate). *There is no elliptic curve over \mathbb{Q} with good reduction everywhere.* See [62].

This turned out to be a special case of:

Theorem (Fontaine, [23]). *There is no abelian scheme $A \rightarrow \text{Spec}(\mathbb{Z})$ of relative dimension $g > 0$.*

The proof of this theorem is quite non-trivial. However suppose we would have a positive answer to Question 9.2 then this theorem of Fontaine would follow easily. Indeed, suppose $A \rightarrow \text{Spec}(\mathbb{Z})$ is an abelian scheme; choose a prime number p ; if 9.2 has a positive answer we would know that

$$A[p^\infty] \cong (\mu_{p, \infty, \mathbb{Z}})^a \times (\underline{\mathbb{Q}}_p/\underline{\mathbb{Z}}_{p_{\mathbb{Z}}})^b.$$

Using duality and a polarization $A \rightarrow A^t$, and [63], 18.1, we see that $a = g = b$. We would conclude $\#((A \bmod p)[p^n](\mathbb{F}_p)) = p^{ng}$; however $\#((A \bmod p)(\mathbb{F}_p)) \leq 2g\sqrt{p}$, and for large n we derive a contradiction. Hence we see that (9.2 is true) would imply this result by Fontaine.

3.6. Remark. Does it suffice to assume that the fundamental group of the base is trivial? Note the analogy. Let k be an algebraically closed field of characteristic zero, and $S = \mathbb{P}_k^1$. Any p -divisible group over S is of the form $(\underline{\mathbb{Q}}_p/\underline{\mathbb{Z}}_{p_S})^b$.

Proof. For $G \rightarrow \mathbb{P}_k^1$ we know $G_i \rightarrow S$ is etale for every i , see 1.16. Note that $\pi_1(\mathbb{P}_k^1)$ is trivial; hence $G_i \rightarrow S$ is constant for every i . \square

Note that any abelian scheme $A \rightarrow \mathbb{P}_k^1$ in characteristic zero has mutually isomorphic geometric fibers.

However in positive characteristic there are many non-constant p -divisible groups over $S = \mathbb{P}_k^1$, and there are many abelian schemes over $S = \mathbb{P}_k^1$ with an infinite set of fibers in different isomorphism classes; we will see many examples.

Maybe the question 9.2 has a positive answer, here for base ring \mathbb{Z} . However for the ring of integers of other number field the situation is different in general. We will observe some examples, but it seems hard to give general results.

3.6.1. Example, $\sqrt{7}$. We see that $\varepsilon = 8 + 3\sqrt{7}$ is a fundamental unit in $\mathcal{O}_L \subset L = \mathbb{Q}(\sqrt{7})$. One shows that the discriminant of

$$E : Y^2 + XY = X^3 - 2\varepsilon X^2 + \varepsilon^2 X \quad \text{equals } \Delta = -\varepsilon^6.$$

Over this ring of integers with class number equal to $h(L) = 1$ we have an elliptic curve with everywhere good reduction.

3.6.2. Example, $\sqrt{29}$ (Tate). Let $L = \mathbb{Q}(\sqrt{29})$. We see that $\varepsilon = (5 + \sqrt{29})/2$ is a fundamental unit, and

$$E : Y^2 + XY + \varepsilon Y = X^3 \quad \Delta = -\varepsilon^{10}$$

and here also $h(\mathbb{Q}(\sqrt{29})) = 1$; see [95], page 320.

3.6.3. Example, $\sqrt{41}$ (FO). We see $\varepsilon = (32 + 5\sqrt{41})/2$ is a fundamental unit in $\mathbb{Z}[(1 + \sqrt{41})/2]$ with $h(\mathbb{Q}(\sqrt{41})) = 1$ and

$$Y^2 + XY = X^3 - \varepsilon X, \quad \Delta = \varepsilon^4,$$

see [102], 2.1.3.3.

Many more examples can be given, for examples see [1], [90], [91], [92], [110].

3.6.4. More generally,

for every g there are infinitely many pairs (A, K) , where A is an abelian variety of dimension g over a number field $[K : \mathbb{Q}] < \infty$ such that A has good reduction at every non-archimedean prime of K

(hence A extends to an abelian scheme over the ring of integers of K). This can be seen as follows. Take any CM abelian variety A'' over \mathbb{C} . We know (as Shimura already proved long ago) that it can be descended to an abelian variety A' over a number field K' having

sufficiently many CM over K' by [97]. we know A'/K' has potentially good reduction, i.e. there exists a finite extension $K' \subset K$ such that $A' \otimes K =: A/K$ has good reduction everywhere.

3.7. Schemes in Characteristic p . For any commutative ring $R \supset \mathbb{F}_p$ the map $x \mapsto x^p$ is a ring homomorphism. Hence for a schemes T over \mathbb{F}_p we obtain a morphism $\text{Frob} : T \rightarrow T$ (the absolute Frobenius). The *relative Frobenius* $F : T \rightarrow T^{(p)}$ is given by the commutative diagram as in 1.9. If G is a group scheme, $F : G \rightarrow G^{(p)}$ is a homomorphism. This morphism is functorial in G/S .

For a *commutative*, flat group scheme G/S over a characteristic p base scheme one can define the *Verschiebung homomorphism* $V : G^{(p)} \rightarrow G$; moreover

$$F \cdot V = [p]_{G^{(p)}}, \quad V \cdot F = [p]_G.$$

For this construction, and much more information see SGAD: [25] Vol. I, Exp. VII_A.

3.8. An Example. Suppose E is an elliptic curve over a finite field $\kappa = \mathbb{F}_q$ with $q = p^n$. How to compute the number of rational points $\#(E(\mathbb{F}_q))$? This was already studied by Gauss in various disguises. Emil Artin noted in his PhD-thesis, 1921, the analogy with the classical Riemann Hypothesis RH; Artin formulated a conjecture (that I like to indicate by) pRH for elliptic curves over a finite field. For some time mathematicians thought this was as hard as the classical RH. However for elliptic curves this was proved: Hasse and many others contributed, and Weil generalized this into a vast complex of conjectures, proved by Grothendieck, Deligne with input from many others; for surveys of this fascinating story in mathematics, see [81], [51].

We indicate aspects of the proof started by Hasse, and completed later. Duality on E , giving the Rosatti involution on $D = \text{End}(E)$, “is complex conjugation” for every element of D . Moreover one shows that $F^t = V$ and $V^t = F$ in the correct interpretation. Write

$$\pi = \underbrace{(F_{E^{(p^{n-1})}}) \cdots (F_E)}_n : E \longrightarrow E^{(p^n)} = E,$$

and using $FV = p$, we derive that $\pi \bar{\pi} = q$, hence the complex absolute value equals

$$|\pi| = \sqrt{q}, \quad \text{part of the Weil conjectures.}$$

As $E(\mathbb{F}_q)$ is the set of fixed points in $E(k)$ of the map $\text{Frob} : x \mapsto x^q$ on k , this is the easiest part of the proof,

$$E(\mathbb{F}_q) = E(k)^{\text{Frob}},$$

and using the fact that the order of $E[1 - \pi]$ equals the norm of $1 - \pi$, we deduce that

$$\#(E(\mathbb{F}_q)) = (1 - \pi)(1 - \bar{\pi}) = 1 - \text{Trace}(\pi) + q.$$

This was predicted by Gauss in a special case, see [76], conjectured by Emil Artin and vastly generalized by Weil later.

See [35] for a description of part of the history of the development of p -divisible groups. Some further references: [2], [8], [11], [7], [15], [22], [23], [28], [34] [47], [48], [51], [71], [72], [81].

4. Dieudonné Modules and Newton Polygons

In this section we mention a classification of finite commutative group schemes, and of p -divisible groups over a *perfect* field $\kappa \supset \mathbb{F}_p$.

4.1. For a perfect field κ we write $\Gamma = \Gamma_\kappa = \text{Witt}_\infty(\kappa)$ for the ring of infinite Witt vectors over κ . Example: for $\kappa = \mathbb{F}_p$ we obtain $\Gamma_{\mathbb{F}_p} = \mathbb{Z}_p$.

Discussion. The usual notation is W_κ ; however the symbol W will be reserved for Newton polygon strata; hence we change notation. We write $\sigma : \Gamma \rightarrow \Gamma$ for the unique ring homomorphism lifting $x_0 \mapsto x_0^p$ in κ .

We write $\mathcal{R}_\kappa = \Gamma[\mathcal{F}, \mathcal{V}]$ for the ring of finite expressions with coefficients in Γ and \mathcal{F}^i and \mathcal{V}^j with relations

$$x \cdot \mathcal{V} = \mathcal{V} \cdot x^\sigma, \quad \mathcal{F} \cdot x = x^\sigma \cdot \mathcal{F}, \quad \forall x \in \Gamma, \quad \mathcal{F} \cdot \mathcal{V} = p = \mathcal{V} \cdot \mathcal{F}.$$

Note that \mathcal{R}_κ is commutative if and only if $\kappa = \mathbb{F}_p$.

Discussion. We will describe covariant Dieudonné theory. Then F on a group scheme will be transformed into \mathcal{V} on its Dieudonné module and V into \mathcal{F} ; see [68], 15.3; for this reason we avoid using F and V for Dieudonné modules, instead we use \mathcal{F} and \mathcal{V} .

4.2. Theorem. Assume $\kappa \supset \mathbb{F}_p$ is a perfect field. There is a covariant equivalence $N \mapsto \mathbb{D}(N)$ between

the category of commutative, finite group schemes N of p -power rank over κ

and

left \mathcal{R}_κ -modules of finite length over \mathcal{R}_κ .

Under this equivalence for $\text{rank}(N) = p^d$ we obtain a module of length d ; note that $F : N \rightarrow N^{(p)}$ “corresponds” with left multiplication by \mathcal{V} , and $V : N^{(p)} \rightarrow N$ “corresponds” with left multiplication by \mathcal{F} .

4.3. Theorem. There is a covariant equivalence $X \mapsto \mathbb{D}(X)$ between the category of p -divisible groups over κ into the category of left \mathcal{R}_κ -modules that are free as Γ -modules. Under this equivalence for a p -divisible group of height h we obtain a module that is free of rank h over Γ . Also here F transforms into \mathcal{V} and V into \mathcal{F} .

Note that an isogeny $f : X \rightarrow Y$ results into an exact sequence

$$0 \rightarrow \mathbb{D}(X) \rightarrow \mathbb{D}(Y) \rightarrow \mathbb{D}(\text{Ker}(f)) \rightarrow 0$$

of \mathcal{R} -modules.

Note that a p -divisible group of dimension $\dim(X) = d$ has the property that $X[F] := \text{Ker}(F : X \rightarrow X^{(p)})$ is a group scheme of order p^d and $\mathbb{D}(X)/\mathcal{V}\cdot\mathbb{D}(X)$ is a κ vector space of dimension d . We write $c = c(X) := \text{height}(X) - d$. With this notation $\mathbb{D}(X)/\mathcal{F}\cdot\mathbb{D}(X)$ is a κ vector space of dimension c . Note that $d(X) = c(X')$ and $c(X) = d(X')$.

4.4. There is a vast literature for generalizations of Dieudonné modules over an arbitrary base. For p -divisible groups the notion of displays as invented by Mumford, later generalized by Zink has many applications. For finite group schemes we mention only one, very useful result:

For a finite groups scheme G over a field $K \supset \mathbb{F}_p$ (not necessarily perfect) with $G = \text{Ker}(F : G \rightarrow G^{(p)})$ one can construct a p -Lie algebra and obtain an equivalence of categories, see [16], II.7.4.2.

4.5. Notation (a). Suppose $m, n \in \mathbb{Z}_{\geq 0}$ are coprime integers. We define a p -divisible group $G_{m,n}$ over \mathbb{F}_p by

$$\mathbb{D}(G_{m,n}) = \mathcal{R}_{\mathbb{F}_p}/\mathcal{R}_{\mathbb{F}_p} \cdot (\mathcal{V}^m - \mathcal{F}^n).$$

Note that $d(G_{m,n}) = m$ and $c(G_{m,n}) = n$. For every $K \supset \mathbb{F}_p$ we will write $G_{m,n}$ instead of $G_{m,n} \otimes K$ is no confusion is possible. Note that $G_{m,n} \otimes K$ is a simple p -divisible group. Examples: $G_{1,0} \cong \mathbb{G}_m[p^\infty]$ and $G_{0,1} \cong \underline{\mathbb{Q}}_p/\underline{\mathbb{Z}}_p$. Note that $(G_{m,n})^f \cong G_{n,m}$.

For a supersingular elliptic curve E over $k = \overline{\mathbb{F}}_p$ we have $E[p^\infty] \cong G_{1,1} \otimes k$.

(b). For $G_{m,n}$ we define its Newton polygon $\mathcal{N}(G_{m,n})$ as the straight line segment starting at $(0,0)$ and ending at $(m+n, m)$; this line has slope $m/(m+n)$, an isoclinic Newton Polygon. This gives “the Frobenius slope” of $G_{m,n}$. More generally, a Newton polygon related to dimension d and height h is a *lower convex polygon* starting at $(0,0)$ and ending at d/h , and *having break-points with integral coordinates*.

(c). Theorem/Notation (Manin). Any p -divisible group X over an algebraically closed field k is isogenous with a product

$$X \sim_k \prod_i G_{m_i, n_i}, \quad \gcd(m_i, n_i) = 1.$$

Notation. The Newton polygon $\mathcal{N}(X)$ in this case is the lower convex polygon consisting of slopes $m_i/(m_i + n_i)$ with multiplicities $m_i + n_i$ arranged in non-decreasing order. We write (m, n) for a pair of coprime non-negative integers, and this stands for the slope $m/(m+n)$ with multiplicity $m+n$.

We obtain a bijective map

$$\{X \mid d(X) = d, h(X) = h\} / \sim_k \xrightarrow{\sim} \{\text{NP} \mid d(\mathcal{N}) = d, h(\mathcal{N}) = h\}.$$

For a p -divisible group Y over a field $K \supset \mathbb{F}_p$ we define $\mathcal{N}(Y)$ as the Newton polygon of $K \otimes k$ for any $k \supset K$. We say a Newton Polygon is *isoclinic* if all slopes are equal, i.e. the polygon is straight line segment.

(d). For an abelian scheme $A \rightarrow S$ one can define the dual abelian scheme $A^t \rightarrow S$, e.g. see [57], Chapter 6. An abelian variety A does admit a polarization $A \rightarrow A^t$; hence A and A^t are isogenous. The duality theorem, see 3.4, implies that $A^t[p^\infty] \cong (A[p^\infty])^t$.

We say a Newton polygon ξ is *symmetric* if and only if the slopes λ and $1 - \lambda$ appear with the same multiplicity in ξ .

We conclude that *for any abelian variety A over $K \supset \mathbb{F}_p$ its Newton Polygon $\mathcal{N}(A)$ is symmetric*.

A conjecture by Manin. *Conversely, for any symmetric Newton polygon ξ there exists an abelian variety A with $\mathcal{N}(A) = \xi$; see [47], page 76; this was proved by Serre (unpublished) and by Honda in the Honda-Tate theory, see [106], page 98; for another proof see [67], Section 5.*

(e). Supersingular. An elliptic curve E defined over a field $K \supset \mathbb{F}_p$ is said to be supersingular if and only if $E[p](k) = 0$. This is the case if and only if $E[p^\infty] \otimes k \cong G_{1,1}$, if and only if $E[p]$ is a local-local group scheme, if and only if $\mathcal{N}(E)$ is isoclinic of constant slope $1/2$. For higher dimension we have the following equivalent properties: *Let A be an abelian variety over a field $K \supset \mathbb{F}_p$; suppose $\dim(A) := g > 1$; fix a supersingular elliptic curve E ; the following are equivalent:*

Definition.

- $\mathcal{N}(A)$ is isoclinic of all slopes equal to $1/2$;
- there is an isogeny $A[p^\infty] \otimes k \sim_k (G_{1,1})^g$;
- there is an isogeny $A \otimes k \sim_k E^g \otimes k$;

Note the curious aspect that every supersingular abelian variety of dimension at least two is not absolutely simple; however for any non-isoclinic symmetric Newton polygon there exists an abelian variety that is geometrically simple having that Newton Polygon; see [45]; see [9], Section 5.

For a group scheme G over $K \supset \mathbb{F}_p$ we write

$$a(G) := \dim_\kappa(\text{Hom}(\alpha_p, G \otimes \kappa))$$

for a perfect field containing K .

Examples. We see $a(G_{m,n}) = 1$, and $a(H_{m,n}) = \min(m, n)$ (see below);

The following properties are equivalent for an abelian variety of $\dim(A) = g > 1$:

- There is an isomorphism $A[p^\infty] \otimes k \cong_k (G_{1,1})^g$;
- there is an isomorphism $A \otimes k \cong_k E^g \otimes k$;
- $a(A) = g$.

Definition. A is *superspecial*.

(f). For later use, see § 7, we define particular p -divisible groups. Suppose given coprime integers $m, n \in \mathbb{Z}_{\geq 0}$. We define a Dieudonné module with free Γ -base $\{e_0, e_1, \dots, e_{m+n-1}\}$. Moreover we write $e_{j+m+n} := p \cdot e_j$, and $\mathcal{F}e_j = e_{j+n}$ and $\mathcal{V}e_j = e_{j+m}$ for all $j \geq 0$. We obtain a Dieudonné module $M(m, n)$ of height $m+n$ and dimension m . We define the p -divisible group over \mathbb{F}_p by $\mathbb{D}(H_{m,n}) = M(m, n)$. Note that $H_{m,n} \sim_{\mathbb{F}_p} G_{m,n}$. For every $K \supset \mathbb{F}_p$ we will write $H_{m,n}$ instead of $H_{m,n} \otimes K$ is no confusion is possible.

Note that for $n \leq 1$ and/or $m \leq 1$ we have $G_{m,n} = H_{m,n}$; for all other cases $G_{m,n} \not\cong H_{m,n}$; proof: $a(G_{m,n}) = 1$ and $a(H_{m,n}) = \min(m, n)$.

Warning. $a(X) = \min(m, n)$ and $X \sim G_{m,n}$ does not imply $X \cong H_{m,n}$; indeed, take $m = 2, n = 5$, and consider the Dieudonné module generated M by e_0 and e_3 inside $\sum_{0 \leq j \leq 6} \Gamma \cdot e_j$ as above. This gives a p -divisible group X with $\mathbb{D}(X) = M$, an isogeny $X \rightarrow X/\alpha_p \cong H_{2,5}$ and we have $a(X) = 2 = a(H_{2,5})$. For easy combinatorics behind such questions see [37], Section 6: Appendix, and see [72].

Property/characterization. Note that $H_{m,n}$ is simple. Hence $\text{End}^0(H_{m,n} \otimes K)$ is a division algebra over \mathbb{Q} for every K . The division algebra $\text{End}^0(H_{m,n} \otimes k)$ is well understood.

For a p -divisible group X over k we have $X \cong H_{m,n} \otimes k$ if and only if $X \sim_k G_{m,n} \otimes k$ and $\text{End}(X)$ is a maximal order in $\text{End}^0(X) = \text{End}^0(G_{m,n} \otimes k)$; see [37].

For a Newton polygon $\zeta = \{(m_j, n_j) \mid j\}$ we write $H(\zeta) := \sum_j H_{m_j, n_j}$.

(g). A partial ordering. We write $\zeta \prec \zeta'$ if these Newton Polygons have the same end point, i.e. the same height and dimension, and every point on ζ is on or above ζ' ; in this case we say “ ζ is above ζ' ”. For $d(\zeta) = d$ and $c(\zeta) = c$ the isoclinic Newton Polygon of slope $d/(d+c)$ is the minimal in this ordering. For symmetric Newton Polygons the supersingular $\sigma = \sigma_g = \mathcal{N}((G_{1,1})^g) = g \cdot (1, 1)$, isoclinic of slope $1/2$, is the minimal one appearing for abelian varieties of dimension g . Note: for every symmetric ξ we have:

$\mathcal{N}(A) \sim \sigma_g \Leftrightarrow A$ is supersingular, and $\sigma_g \prec \xi$,
 A is ordinary $\Leftrightarrow \mathcal{N}(A) = g \cdot (1, 0) + g \cdot (0, 1) =: \rho_g$, and
 $\xi \prec \rho_g$.

(h). Theorem (Grothendieck, Katz). *If $\mathcal{X} \rightarrow S$ is a p -divisible group over an irreducible scheme S/\mathbb{F}_p , with $0 \in S$ and generic point $\eta \in S$. Then*

$$\mathcal{N}(\mathcal{X}_0) \prec \mathcal{N}(\mathcal{X}_\eta),$$

i.e. “Newton Polygons go up under specialization”; see [28], page 150; [41], Th. 2.3.1, page 143.

Grothendieck asked whether the converse holds:

In order to consider this problem we first showed that “Purity” holds for NP strata:

4.6. Theorem (Purity). *Let $S \rightarrow \text{Spec}(\mathbb{F}_p)$ be an irreducible noetherian base scheme in characteristic p . Let $X \rightarrow S$ be a p -divisible group, or let $A \rightarrow S$ be an abelian scheme. The locus where the Newton Polygon differs from that of the generic fiber is in pure codimension one. See [37].*

4.7. A Conjecture by Grothendieck.

Conjecture/Theorem. *Work in characteristic p . Suppose given a p -divisible group X_0/κ with Newton Polygon $\mathcal{N}(X_0) = \zeta$ and suppose given a Newton Polygon $\xi \succ \zeta$, i.e. ζ is “above” ξ , there exists a p -divisible group over an irreducible scheme S/\mathbb{F}_p , with $0 \in S$ and generic point $\eta \in S$ with $\mathcal{X}_0 = X_0$ and $\mathcal{N}(\mathcal{X}_\eta) = \xi$, i.e. the partial ordering is realized by a deformation of X_0 .*

See [37], [67], [69]. An analogous result for principally polarized p -divisible groups or principally polarized abelian varieties holds. A systematic way of finding counterexamples in the non-principally polarized cases is described in [74].

Remark. The proof I know for this theorem is quite involved. Does there exist a “pure thought proof”?

Corollary. Consider $\mathcal{A}_g = \mathcal{A}_{g,1} \otimes \mathbb{F}_p$, the moduli space of principally polarized abelian varieties in characteristic p . For a Newton polygon ξ write $W_\xi \subset \mathcal{A}_g$ for the locus where the Newton Polygon equals ξ .

The Grothendieck conjecture in this case amounts to the fact that

$$\partial(W_\xi) := (W_\xi)^{\text{Zar}} \setminus W_\xi \subset \mathcal{A}_g$$

is the union of all smaller NP strata.

Some literature: especially [47]; further: [8], [15], [27], [28], [34], [37], [63], [67], [69], [68], [71], [74], [75], [82], [106], [104], [105], [111], [112], [113].

5. Kraft Cycles

In this section we work over an algebraically closed field $k \supset \mathbb{F}_p$. We will see that in general the set of isomorphism classes of finite group schemes over k of fixed rank is infinite, see 5.5. However a wonderful theorem by Kraft, see [43], classifies all finite commutative group schemes *annihilated by p* ; in particular in that case the number of isomorphism classes of finite commutative group schemes over k of fixed order is finite. We define finite group schemes P_u and Q_w ; we will see that these are the simple building blocks of any finite commutative group scheme annihilated by p over k .

5.1. Lin: *Linear words, Kraft words.* Consider a word $u = L_1 \cdots L_{h-1}$ with $h \in \mathbb{Z}_{\geq 1}$. We define a finite group scheme P_u by constructing its Dieudonné module $\mathbb{D}(P_u) = M_u$. We write $z_1 L_1 z_2 \cdots z_{h-1} L_{h-1} z_h$ and on $M_u := \sum_{1 \leq i \leq h} k \cdot z_i$ we give the structure of a Dieudonné module of dimension h over k by:

$$\begin{aligned} \mathcal{V}z_1 = 0; \quad L_i = \mathcal{F} \text{ then } \mathcal{F}z_i = z_{i+1}, \text{ and } \mathcal{V}z_{i+1} = 0; \\ L_i = \mathcal{V} \text{ then } \mathcal{V}z_{i+1} = z_i, \text{ and } \mathcal{F}z_i = 0; \quad \mathcal{F}z_h = 0. \end{aligned}$$

I.e. we visualize:

$$0 \xleftarrow{\mathcal{V}} z_1; \quad z_i \xrightarrow{\mathcal{F}} z_{i+1}; \quad z_i \xleftarrow{\mathcal{V}} z_{i+1}; \quad z_h \xrightarrow{\mathcal{F}} 0.$$

Note that this defines the image of any base vector under \mathcal{F} and under \mathcal{V} . The empty word $h = 1$ defines $P_\emptyset \cong \alpha_p$. For example

$$z_1 \xleftarrow{\mathcal{V}} z_2 \xleftarrow{\mathcal{V}} z_3 \text{ defines } P_u \cong \mathbb{G}_a[F^3].$$

Note that any P_u is indecomposable, annihilated by p , with $\mathcal{F}M_u \subsetneq M_u[\mathcal{V}]$ and $\mathcal{V}M_u \subsetneq M_u[\mathcal{F}]$.

Any $G = P_u$ has the property $\text{Ker}(F) \subsetneq VG$ and $\text{Ker}(V) \subsetneq FG$. It is a finite group scheme over \mathbb{F}_p annihilated by p of rank p^h .

Circ: *Circular words, Kraft cycles.* Consider a word $w = L_1 \cdots L_h$ with $h \in \mathbb{Z}_{\geq 1}$. Here we only consider such a K-cycle in a cyclic way: we introduce an (a cyclic) equivalence relation generated by $L_1 \cdots L_{h-1} L_h \sim L_h L_1 \cdots L_{h-1}$. The equivalence class of $L_1 \cdots L_h$ is denoted by $[L_1 \cdots L_h]$ or by $\Gamma = [L_1 \cdots L_h]$. From a K-cycle w we construct a Dieudonné module Q_w ; this module is associated with a BT_1 group scheme N_w over κ by $\mathbb{D}(N_w) = Q_w$. The construction $w \mapsto Q_w$ is given by:

$$\begin{aligned} N_w = \sum_{1 \leq j \leq h} \kappa \cdot z_j, \quad \text{write } z_1 L_1 z_2 \cdots z_h L_h z_1 \\ L_j = \mathcal{F} \implies \mathcal{F} \cdot z_j = z_{j+1}, \quad 0 = \mathcal{V} \cdot z_{j+1}, \\ L_j = \mathcal{V} \implies \mathcal{V} \cdot z_{j+1} = z_j, \quad 0 = \mathcal{F} \cdot z_j. \end{aligned}$$

We write $v_{\mathcal{F}}(w) := \#\{i \mid L_i = \mathcal{F}\}$ and $v_{\mathcal{V}}(w) := \#\{i \mid L_i = \mathcal{V}\}$. We say that a circular word w is *indecomposable* if $w = (w')^\mu$ implies $\mu = 1$.

Note that Q_w is indecomposable if and only if the circular word w is indecomposable. We see that Q_w is annihilated by p , with $\mathcal{F}N_w = N_w[\mathcal{V}]$ and $\mathcal{V}N_w = N_w[\mathcal{F}]$. For any circular word w the group scheme Q_w is a BT_1 group scheme (see below).

Any $G = Q_w$ has the property $\text{Ker}(F) = VG$ and $\text{Ker}(V) = FG$. It is a finite group scheme over \mathbb{F}_p annihilated by p .

Although P_u and Q_w are defined over \mathbb{F}_p we will use the same notation over any field K containing \mathbb{F}_p , i.e. we write P_u instead of $P_u \otimes K$, if no confusion is possible.

5.2. Definition. An object $T \neq 0$ in an abelian category is called *indecomposable* if $T = T_1 \oplus T_2$ implies $T_1 = 0$ or $T_2 = 0$. A basic tool:

Theorem (Krull-Remak-Schmidt). *Let R be a ring, and consider the category \mathcal{C} of artinian and noetherian left R -modules. For every indecomposable $T \in \mathcal{C}$ the ring $\text{End}_R(T)$ is a local ring. In \mathcal{C} every non-zero object is a direct sum of indecomposable modules, and this decomposition is unique up to an isomorphism and permutation of the factors. See [44], Prop. X.7.4, and Theorem X.7.5. See [36], page 115.*

5.3. Theorem (Kraft). *Over an algebraically closed field $k \supset \mathbb{F}_p$ any commutative group scheme G annihilated by p can be written as a direct sum of group schemes P_{w_i} and indecomposable Q_{w_j} ,*

$$G \cong \sum_i P_{w_i} \oplus \sum_j Q_{w_j},$$

and this way of writing is unique up to isomorphism and permutation of the factors. See [43]; see [12], Chapter 2.

5.4. Corollary. *Over an algebraically closed field $k \supset \mathbb{F}_p$ and for a fixed n the set of isomorphism classes of finite group schemes of order p^n over k annihilated by p is finite.*

5.5. Remark/Example. The condition “annihilated by p ” is essential in the preceding two results. We show that (without this condition)

the set of isomorphism classes of group schemes of rank p^n over k with $n \geq 3$ is *not finite*.

For any $\beta \in k^* = k \setminus \{0\}$ we define the Dieudonné module $M_\beta = M_{\beta, e, x}$ defined by generators e and x with the following relations:

$$\mathcal{F} \cdot e = \mathcal{V} \cdot e, \quad \mathcal{F}^2 \cdot e = \mathcal{V}^2 \cdot e = p \cdot e = 0,$$

and

$$\mathcal{F} \cdot x = \beta \cdot e, \quad \mathcal{V} \cdot x = e.$$

We see that the length of M_β equals p^3 ; hence this is the Dieudonné module of a finite group scheme of order p^3 .

Claim. *We have*

$$(\{M_\beta \mid \beta \in k^*\} / \cong) \cong k^* / (\mathbb{F}_{p^2})^*;$$

hence the set

$$\#\{(\{M_\beta \mid \beta \in k^*\} / \cong) = \infty$$

in an infinite set.

Proof. Suppose $M_\gamma = M_{\gamma,f,y}$ has generators f and y with relations as above and suppose that $M_\beta \cong M_\gamma$. We see that

$$\{u \in M_\beta \mid pu = 0\} = R \cdot e \cong R \cdot f;$$

this isomorphism is given by $e \mapsto b \cdot f + c \cdot \mathcal{F} \cdot f$ with $b \in \mathbb{F}_{p^2}$ and $c \in k$. Further

$$x \mapsto \delta \cdot y + \varepsilon \cdot f, \quad \delta, \varepsilon \in R.$$

Using $\mathcal{V} \cdot x = e$ and $\mathcal{V} \cdot y = f$ we see that $b = \delta \pmod{p}$, and we conclude $M_\beta \cong M_\gamma$ if and only if $\beta/\gamma \in \mathbb{F}_{p^2}$. \square

5.6. An Example with an Explication. Consider extensions over k given as

$$0 \rightarrow \alpha_p \rightarrow N \rightarrow \alpha_p \rightarrow 0.$$

The group $\text{Ext}(\alpha_p, \alpha_p)$ is infinite; for a description see [63], 15.5. However, if we consider such group schemes N up to isomorphism over k , without fixing coordinates on the embedded $\alpha_p \subset N$ and on the cokernel $N \rightarrow \alpha_p$, the number of such isomorphism classes is four, the possibilities are:

- α_p^2 (the split extension), and
- $\mathbb{G}_a[F^2]$ given by the linear Kraft word \mathcal{V} ,
- its dual given by the linear Kraft word \mathcal{F} , and
- $E[p]$, where E is a supersingular elliptic curve; this last finite group scheme $N \cong N_{\mathcal{F}\mathcal{V}}$ is given by the circular Kraft cycle $\mathcal{F}\mathcal{V}$.

For concepts in this section, see [12], [43], [52], [54], [63], [68], 2.5.

6. Mixed Characteristics and Lifting Questions

For an early survey, see [66]. Suppose you have an object X_0 over a field $\kappa \supset \mathbb{F}_p$ (we give more precise cases soon). We say $\mathcal{X} \rightarrow \text{Spec}(\Gamma)$ is a *lifting to characteristic zero*, if there exists an integral domain Γ , with given $\Gamma \rightarrow \kappa$, and fraction field $Q(\Gamma) = K \supset \mathbb{Q}$ and \mathcal{X} over Γ (with extra conditions, depending on the situation); usually we write $X = \mathcal{X} \otimes_\Gamma K$ for the generic and $X_0 = \mathcal{X} \otimes_\Gamma \kappa$ for the special fiber. Sometimes we impose extra conditions on κ , e.g. a perfect field, or an algebraically closed field. Sometimes we can impose extra conditions on Γ , e.g. the ring being local, the ring being unramified relative to $\Gamma \rightarrow \kappa$ and we should impose conditions on \mathcal{X}/Γ to be specified in every concrete situation. See 9.5.

6.1. Examples and Some Results on Liftings.

6.1.1. Finite Group Schemes. In general a finite group scheme N_0/κ does not admit a lifting to characteristic zero:

Any non-commutative group scheme N_0 of rank p^2 , e.g. see 1.7.2, does not admit a lifting to a flat \mathcal{N}/Γ . In fact any such lifting would define a non-commutative, constant $\mathcal{N} \otimes \bar{K}$; by group theory we know any group of order p^2 is commutative.

Theorem. *Any commutative group scheme N_0 over $k \supset \kappa$ does admit a lifting to characteristic zero, see [80].*

The group scheme α_p does admit a lifting, as we already see by [109]; it does admit a lifting to an appropriate ramified $\Gamma \rightarrow \kappa$, but not to an unramified Γ .

6.1.2. Algebraic Curves. Any smooth complete algebraic curve C_0 can be lifted to a flat, smooth algebraic curve in mixed characteristic.

6.1.3. Algebraic Varieties. There exist varieties of dimension at least two in positive characteristic that cannot be lifted to characteristic zero, as was proved by Serre, see [94], also see the appendix in [78].

6.1.4. Polarized Abelian Varieties. Any abelian variety in characteristic p can be lifted to a *formal abelian scheme* over a complete Noetherian local domain. However in order to decide whether this formal abelian scheme can be algebraized we like to lift a polarization along. For principally polarized abelian varieties we know a lifting does exist, even to an unramified situation (as was proved by Grothendieck and Mumford).

Theorem (Mumford; Norman and Oort). *Any polarized abelian variety (A, λ) over a perfect field κ can be lifted to a polarized abelian scheme, and there do exist examples that cannot be lifted to an unramified situation (an example was given by Ogus); see [60], [59].*

6.1.5. Curves with Automorphisms. Suppose C_0 is an algebraic curve over κ and a subgroup $G \subset \text{Aut}(C_0)$; in general the pair (C_0, G) cannot be lifted to characteristic zero: the Hurwitz bound easily provides us with examples; for other examples see [66]. However for a cyclic G liftability was a conjecture for some time (1995), and that has been proved now:

Theorem (F. Pop; Obus and Wewers). *Let (C_0, φ) be a smooth, complete algebraic curve with an automorphism $\varphi \in \text{Aut}(C_0)$ over an algebraically closed field $k \supset \mathbb{F}_p$; this pair can be lifted to characteristic zero.*

See [61], [85]; see 6.2.4. For a discussion and references see A. Obus - *Lifting curves with automorphisms* in [77], Chapter 2.

6.1.6. p -Divisible Groups. Any p -divisible group over a perfect κ admits a lifting to an unramified mixed characteristic domain.

6.1.7. CM-Liftings. Suppose A_0 is an abelian variety over a finite field. We know by Tate that A_0 is a CM

abelian variety, see [104]. We can ask whether a CM-lifting does exist. It turns out that one has to formulate this question in various ways, with various answers. For a full account of this interesting field, see [7].

6.2. A Method in Deformation Theory. See [80], [79]. Suppose we study a problem in lifting theory, or we want a deformation with specific properties of a generic fibre. If the universal deformation theory exists, as in [87], which is the case in many situations, it seems the problem is (almost) solved: just inspect properties of all fibers; in several cases this works well. However in more difficult problems we can encounter situations not easily solved in this way. We discuss a method that worked well in several cases. This method consists of two steps:

- (I) deform N_0 to a “better” situation M_0 ; we have to define what better means, and we have to make a usually non-canonical choice of such a deformation; in most cases this is the hard part of the proof.
- (II) apply general theory to solve the problem at hand for this “good” situation.

We explain this method in the various situations.

Serre once communicated to me: “*About theorems being proved by general methods or by tricks. The word trick is pejorative. But one should keep in mind that a ‘trick’ in year N often becomes a ‘theory’ in year $N + 20$.*”

6.2.1. Lifting Finite Commutative Group Schemes.

Step I. After rigidifying finite commutative group schemes it is proved that the equi-characteristic- p deformation space is irreducible, [80], Theorem 3.1. As usual, Step I is the hard part. In particular any finite commutative N_0 admits a deformation with geometric generic fiber $M_0 = \mathcal{N}_{\bar{\eta}}$ a direct sum of a local-etale and an etale-local group scheme.

Step II. Clearly M_0 can be lifted to characteristic zero (the easy part of the argument), and [80] Lemma 2.1 finishes the proof that *any finite commutative group scheme can be lifted to characteristic zero.*

6.2.2. Lifting Polarized Abelian Varieties.

Step I. Consider a polarized abelian variety (A_0, μ) over $\kappa \supset \mathbb{F}_p$. Using the theory of displays (enabling us to write down deformation of p -divisible groups explicitly) we prove that (A_0, μ) can be deformed with geometric generic fiber an ordinary (B_0, μ) , see [60], Th. 2.2 and Th. 3.1. In this part and in the next step a theorem by Serre and Tate that infinitesimal deformations of (polarized) p -divisible group and of (polarized) abelian schemes is an equivalence of categories in a precise sense.

Step II. Clearly an ordinary polarized p -divisible group can be lifted, and the Serre-Tate equivalence shows (B_0, μ) can be lifted to characteristic zero, and [80] Lemma 2.1 finishes the proof that *any polarized abelian varieties can be lifted to characteristic zero*, see [60], Coroll. 3.2. For a different proof see [59].

6.2.3. Deformations of p -Divisible Groups with Prescribed Generic Newton Polygon.

Step I. For a p -divisible group X_0 over a perfect $\kappa \supset \mathbb{F}_p$ we define

$$a(X_0) = \dim_{\kappa}(\mathrm{Hom}(\alpha_p, X_0)).$$

Note that $a(X_0) = 0$ if and only if X_0 is ordinary. Suppose X_0 is non-ordinary; we show there exists an equi-characteristic- p deformation of X_0 with geometric generic fiber Y_0 such that $\mathcal{N}(X_0) = \mathcal{N}(Y_0)$ and $a(Y_0) = 1$; see [37], Th. 5.11 and Coroll. 5.12.

Step II. For p -divisible groups with $a(-) = 1$ a method in linear algebra generalizing the well-known *Cayley-Hamilton theorem* describes precisely all Newton Polygon strata in $\mathrm{Def}(Y_0)$, see [67], Th. 3.4, see [69], Th. 2.1, showing that any p -divisible group X_0 can be deformed to a p -divisible group with prescribed Newton Polygon, exactly as Grothendieck had asked for, see [28], page 150 in the Appendix.

Remark. The method described here can be generalized to the situation of principally polarized p -divisible groups, and hence to principally polarized abelian varieties; see [69], Th. 3.1. There one can start with any principally polarized supersingular abelian variety, and apply (I) and (II), or we can start with a principally polarized supersingular abelian variety with $a(A_0) = 1$, existence assured by [46], Th. 4.9(iii) and apply (II).

Remark. The method described here shows that for any symmetric Newton Polygon ξ the Newton Polygon stratum $W_{\xi} \subset \mathcal{A}_{g,1} = \mathcal{A}_{g,1} \otimes \mathbb{F}_p$ in the moduli space of principally polarized abelian varieties in characteristic p , is non-empty. As a corollary this proves the conjecture by Manin, see [47] page 76, that any symmetric Newton Polygon appears for an abelian variety of that dimension in that characteristic, see [67], Section 5. This conjecture was earlier proved by Serre (unpublished) and by Honda in the Honda-Tate theory, see [106], page 98.

Remark. For non-principally polarized abelian varieties there do exist Newton Polygon strata where $a(-) > 1$ for all points. Step (I) does not hold in such situations. There are many counterexamples to the generalization of the Grothendieck Conjecture to polarized p -divisible groups, and to polarized abelian varieties; in [74] there is a systematic way to find such examples.

6.2.4. Lifting a Cyclic Cover of an Algebraic Curve.

Step II. In [61], Th. 1.4 we find a criterion for a cyclic cover in positive characteristic ensuring the lifting problem has a solution.

Step I. In [85] we find a deformation argument showing that any cyclic cover in positive characteristic can be deformed to a cyclic cover as in [61], Th. 1.4.

Combining the two (quite non-trivial steps) we arrive at:

Theorem. *Any cyclic cover $C \rightarrow D$ over $k \supset \mathbb{F}_p$ can be lifted to a mixed characteristic domain. See [85], Th. 1.1.*

6.3. Suppose we have an object X_0 over $\kappa \supset \mathbb{F}_p$ such that $X_0 \otimes k$ can be lifted to characteristic zero for some $k \supset \mathbb{F}_p$. Suppose the deformation theory of X_0 is prorepresentable. Then we see that X_0 can be lifted to some mixed characteristic domain $\Gamma \rightarrow \kappa$. However normalizing Γ might extend the residue class field. Hence only the information given here does not answer the question whether N_0 can be lifted to some mixed characteristic *normal* domain. For questions see 9.5.

7. Minimal p -Divisible Groups

In this section we work over an algebraically closed field $k \supset \mathbb{F}_p$. For a p -divisible group X we consider $X[p] = G_1 = \text{Ker}([p] : X \rightarrow X)$. We can consider how far the structure of $X[p]$ determines the isomorphism class of X . This was a question in a letter 5 January 1970 of Grothendieck to Mumford, see [58], pp. 744–745: “*I wonder ... assume k algebraically closed, and G and H BT groups, and assume $G(1)$ and $H(1)$ are isomorphic. Are G and H isomorphic?*” As an answer, Mumford wrote counterexamples. I think neither Grothendieck nor Mumford ever pursued this question.

Completely independent of this, not knowing at that moment this correspondence, I wondered what conditions on $X[p] \cong Y[p]$ would imply $X \cong Y$ for p -divisible groups over an algebraically closed field. In this section we describe this necessary and sufficient condition.

7.1. BT_1 group schemes. *A finite, commutative flat group $\mathcal{N} \rightarrow S$ is called a BT_1 group scheme over S if \mathcal{N}/S is annihilated by p , and $\mathcal{N}^{(p)}[V]$ is flat over S and equal to the image of $F : \mathcal{N} \rightarrow \mathcal{N}^{(p)}$. See [34], 1.1.*

The following conditions are equivalent for a finite commutative group scheme N over a perfect field κ :

- N/κ is a BT_1 group scheme;
- there exists a p -divisible group X with $X[p] \cong N$; see [34], 1.7;

- $FN = N^{(p)}[V]$ and $VN^{(p)}N = N[F]$ (hence N is annihilated by p);
- there exist a set of circular Kraft cycles $\{w_j \mid j\}$ such that $N \otimes k \cong \sum_j Q_{w_j}$.

7.2. An Example. Suppose

$$\iota = (x, y) : \alpha_p \rightarrow (\alpha_p)^2 \subset (G_{1,1})^2; \text{ define } Z_{[x,y]} = (G_{1,1})^2 / \iota(\alpha_p).$$

It is easy to see that $x \notin \mathbb{F}_{p^2}$ and $y \notin \mathbb{F}_{p^2}$ if and only if $a(Z_{[x,y]}) = 1$; in this case $Z_{[x,y]}[p] \otimes k \cong Q_w$ for the circular word $w = \mathcal{F}\mathcal{F}\mathcal{V}\mathcal{V}$; in particular these BT_1 's are mutually isomorphic. However,

$$\begin{aligned} & (\{Z_x \mid x \in k, x \notin \mathbb{F}_{p^2}, Z_x = (G_{1,1})^2 / (x, 1)(\alpha_p)\} / \cong) \\ & = k^* / (\mathbb{F}_{p^2})^*; \end{aligned}$$

we see that $Q_{\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{V}}$ is a BT_1 such that there are infinitely many isomorphism classes of p -divisible groups Z with $Z[p] \cong Q_{\mathcal{F}\mathcal{F}\mathcal{V}\mathcal{V}}$.

Proof. We work over k . For $a(Z) = 1$ we have $a(Z')$ and $Z \sim (G_{1,1})^2$. The unique $\alpha_p \subset Z'$ gives $Z'/\alpha_p \cong (G_{1,1})^2$. By duality this gives functorially an exact sequence

$$0 \rightarrow \alpha_p^D \cong \alpha_p \rightarrow ((G_{1,1})^2)^t \cong (G_{1,1})^2 \rightarrow Z^t = Z \rightarrow 0.$$

For $Z_x \cong Z_y$ we obtain a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \alpha_p & \longrightarrow & (G_{1,1})^2 & \longrightarrow & Z_x \longrightarrow 0 \\ & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ 0 & \longrightarrow & \alpha_p & \longrightarrow & (G_{1,1})^2 & \longrightarrow & Z_y \longrightarrow 0. \end{array}$$

The action of $\text{End}((G_{1,1})^2)$ on $(\alpha_p)^2 = (G_{1,1})^2[F]$ is via $\text{Mat}(2, \mathbb{F}_{p^2})$ and the result follows. \square

Conclusion. There is a BT_1 group scheme N of order p^4 and infinitely many k -isomorphism classes of a p -divisible groups X with $X[p] \cong N$.

Variante. Take any $n \in \mathbb{Z}_{>1}$, and $(x, y) : \alpha_p \rightarrow G_{1,n} \times G_{n,1}$ with $Z_x = (G_{1,n} \times G_{n,1}) / (x, 1)(\alpha_p)$. For $x \neq 0$ and $y \neq 0$ we have $a(Z_{[x,y]}) = 1$, and the set of such isomorphism classes is $k^* / \mathbb{F}_{p^{1+n}}$.

We could also consider $(x, y) : \alpha_p \rightarrow G_{1,n} \times G_{m,1}$, etc.

7.3. Remark. *Note that for a BT_1 group scheme N over k we can have p -divisible groups X and Y such that $X[p] \cong N \cong Y[p]$ such that $\mathcal{N}(X) \neq \mathcal{N}(Y)$.*

For example, take the circular Kraft cycle $w = \mathcal{F}^n \mathcal{V}^n$ for some $n > 1$. Any symmetric Newton Polygon ξ for $g = n$ with no slopes equal to 0 and no slopes equal to one 1 (“the p -rank is zero”) admits a p -divisible group X of height $h = 2n$ with $\mathcal{N}(X) = \xi$ and $X[p] \cong N_w$. For any $n > 1$ we have at least two different symmetric Newton Polygons with p -rank zero and we obtain examples as in the remark above.

7.4. Definition. A p -divisible group X is called minimal if there exists a Newton polygon ζ with

$$X[p] \otimes k \cong H(\zeta)$$

in the notation of 4.5.f. Note that we do not make a priori any connection between $\mathcal{N}(X)$ and ζ .

7.5. Theorem. Suppose X and Y are minimal p -divisible groups over k . Then

$$X[p] \cong Y[p] \iff X \cong Y;$$

in this case $\mathcal{N}(X) = \zeta = \mathcal{N}(Y)$ with $X[p] \cong H(\zeta)p \cong Y[p]$. See [71].

Note that the minimal p -divisible groups are precisely those for which the answer to the question by Grothendieck is affirmative. Moreover, in every k -isogeny class there is a unique minimal one.

7.6. Example. We consider $k = \bar{k} \supset \mathbb{F}_p$ and $g = 3$. We see that we have the following possible Newton Polygons. We write $f = f(-)$ for the p -rank: $G[p](k) \cong (\mathbb{Z}/p)^{f(G)}$ for any commutative group scheme.

- (ss) $\xi = \sigma_3$; X is minimal if and only if $a(X) = 3$, the superspecial case;
- ($f = 0$) for $\xi = (2, 1) + (1, 2)$ we see X is minimal if and only if $a(X) = 2$;
- ($f = 1$) for $\xi = (1, 0) + 2 \cdot (1, 1) + (0, 1)$ we see X is minimal if and only if $a(X) = 2$;
- ($f = 2$) any X with $\mathcal{N}(X) = \xi = 2 \cdot (1, 0) + (1, 1) + 2 \cdot (0, 1)$ is minimal;
- ($f = 3$) any ordinary p -divisible group is minimal.

As 7.5 allows us to describe explicitly all possible minimal p -divisible groups, such examples can be explicitly given for any g .

Here is another characterization of minimal p -divisible groups.

7.7. Theorem. A p -divisible group X is minimal if in the direct summand $X[p] \otimes k \cong \sum_j Q_{w_j}$ every Q_{w_j} is simple as object in the category of BT_1 group schemes. See [72], 0.1.

Remark. Note that “simple as object in the category of BT_1 group schemes” is much stronger than the concept “simple”. For example $N = N_{\mathcal{FV}}$ has a non-trivial proper subgroup but N is simple as BT_1 group scheme.

For example $Q_{\mathcal{FV}}$ is not simple as BT_1 group scheme: it contains a subgroup scheme isomorphic with $Q_{\mathcal{FV}}$. Using 7.4 and 7.5 one can explicitly determine all circular Kraft cycles that give a simple BT_1 group scheme.

Remark. For any p -divisible group X such that $X[p]$ is local-local and $d(X) > 1$ and $c(X) > 1$ there

exist infinitely many $Y \sim X$ that are not minimal. Grothendieck had examples in mind for which his question has an affirmative answer; p -divisible groups of dimension 1 or of codimension 1 indeed are minimal, but in other cases many examples of non-minimal p -divisible groups are present.

8. Stratifications and Foliations

Here we come to an application as promised in the introduction: fix “an invariant” and study the space of all objects having that invariant. The moduli space of polarized abelian varieties has been studied (certainly since Abel) and geometric, topological and analytic tools give a wealth of information on such spaces over \mathbb{C} . It seems we are at loss as these tools are not available in positive characteristic. We show there are other, powerful tools available in that situation.

We consider $\mathcal{A}_g = \mathcal{A}_{g,1} \otimes \mathbb{F}_p$, the moduli space of g -dimensional principally polarized abelian varieties defined over some field in characteristic p . We construct two stratifications and foliations of these spaces. Properties have been well established by now, and we can harvest the fruits. (We have also studied the cases of arbitrary degree of polarization, interesting but not discussed here.)

8.1. (NP) Newton Polygons. The invariant: $A[p^\infty] \bmod \sim$

Consider a symmetric Newton Polygon ξ and define the open Newton polygon stratum

$$\mathcal{W}_\xi(\mathcal{A}_g) = \{[(A, \mu)] \in \mathcal{A}_g \mid \mathcal{N}(A[p^\infty]) = \xi\}.$$

By Grothendieck and Katz we know $\mathcal{W}_\xi(\mathcal{A}_g) \subset \mathcal{A}_g$ is locally closed, see [28], page 150; [41] Th. 2.3.1, page 143. We obtain a finite union $\mathcal{A}_g = \sqcup \mathcal{W}_\xi(\mathcal{A}_g)$.

8.2. (EO) EO Strata. The invariant: $(A, \lambda)[p] \bmod \cong$

Consider a BT_1 group scheme N , with a non-degenerate alternating pairing $\langle -, - \rangle$; for details see [68], Section 9. A principally polarized abelian variety (A, λ) defines such a pair by

$$(A, \lambda)[p] = (N, \langle -, - \rangle).$$

Denote its isomorphism type by

$$\varphi = ((N, \langle -, - \rangle) \bmod \cong).$$

For a classification of such pairs over k see [68], Theorem 9.4. Define

$$S_\varphi = \{[(A, \mu)] \in \mathcal{A}_g \mid A[p] \otimes \Omega \cong N\}.$$

Here Ω is some algebraically closed field. The set $S_\varphi \subset \mathcal{A}_g$ is locally closed. Using Section 5 we can prove that the number of such isomorphism types is finite; hence we obtain a finite union $\mathcal{A}_g = \sqcup S_\varphi$.

8.3. (Fol) Foliations: Central Leaves. The invariant:

$$(A, \mu)[p^\infty] \bmod \cong$$

Consider the moduli point of a polarized abelian variety $x = [(A, \lambda)]$ and consider

$$\mathcal{C}(x) = \{[(B, \mu)] \in \mathcal{A}_g \mid (B, \mu) \otimes \Omega \cong (A, \lambda) \otimes \Omega\}.$$

This set is locally closed in the Newton polygon stratum $\mathcal{W}_\xi(\mathcal{A}_g)$ with $\xi := \mathcal{N}(A)$, and this inclusion is locally closed, hence $\mathcal{C}(x) \subset \mathcal{A}_g$ is locally closed. See [70].

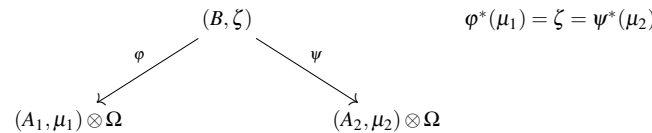
8.4. A Discussion, Some Properties. In all three cases we have defined these sets as sets of points, and over a perfect field we consider the scheme structure as a reduced scheme. This seems a method not fitting very well in Grothendieck’s philosophy.

For (NP) we do not know a good scheme theoretic definition, see 8.1. This seems a serious obstacle in further developments.

For (EO) there is a nice, functorial description of these strata, see [20].

For (Fol) initially a set-theoretic definition was given in [70]; now a functorial description is available by the notion of *sustained p -divisible groups*, see [77], Chapter 7, [12]. It is known that over a perfect base field $\mathcal{C}(x)$ is non-singular (in both definitions).

8.5. Hecke Orbits. Suppose given a polarized abelian variety (A, μ) over a field. Write $x = [(A, \mu)]$ for its moduli point; its Hecke orbit $\mathcal{H}(x)$ is defined as the isogeny class of (A, μ) . Explicitly: $[(A_2, \mu_2)] \in \mathcal{H}([(A_1, \mu_1)])$ if there exists a field Ω , and (B, ζ) over Ω and isogenies



Easy. For abelian varieties over \mathbb{C} any Hecke orbit is dense everywhere in the moduli space (dense in the classical topology and dense in the Zariski topology).

Example. The Hecke orbit of a *supersingular elliptic curve* over $k \supset \mathbb{F}_p$ has only finitely many points in $\mathcal{A}_{g,1}$ and we see the Hecke orbit is not dense in this case.

We suggest an exercise to the reader: show the Hecke orbit of an *ordinary elliptic curve* is everywhere dense in the moduli space.

What do these results suggest?

Theorem (Chai). *For an ordinary (A, μ) over $k \supset \mathbb{F}_p$ its Hecke orbit is every where dense in the moduli space $\mathcal{A}_g \otimes \mathbb{F}_p$. See [5].*

Theorem (Chai-Oort). *For any (A, μ) over $k \supset \mathbb{F}_p$, with $\mathcal{N}(A) = \xi$, its Hecke orbit is everywhere dense in the Newton Polygon stratum given by ξ . To be published in [12].*

Hecke correspondences in positive characteristic can blow up and down. Here is an easy example. Consider the supersingular locus $S \subset \mathcal{A}_{2,1}$ of principally polarized abelian surfaces, and $S' \subset \mathcal{A}_{2,p}$ of abelian surfaces with a polarization of degree p^2 ; we know S is a union of rational curves, also S' is a union of rational curves. Intersection points of components of S blow up to a component of S' and components of S blow down to intersection points of components of S' under Hecke- p -correspondences. For other Newton Polygons, especially for higher g much more complicated patterns appear.

As a consequence we see that different components in $\mathcal{W}_\xi(\mathcal{A}_g)$, the locus in $\cup_d \mathcal{A}_{g,d}$ where ξ is realized, can have different dimensions. This behavior is well understood by now; see [74]. However components in $\mathcal{W}_\xi(\mathcal{A}_{g,1})$ all have the same dimension; this is completely understood, e.g. see [69], [67]; an easy combinatorial pattern computes the dimension of NP strata in the *principally polarized case*.

8.6. It is hard to (define and to) describe EO strata in \mathcal{A}_g . However in $\mathcal{A}_{g,1}$ the situation is clear. See [68] for a complete and precise description.

For a given symmetric Newton Polygon all central leaves in $\mathcal{W}_\xi(\mathcal{A}_g)$ have the same dimension. It feels that central leaves have “the same properties” as the moduli space $\mathcal{A}_g \otimes \mathbb{Q}$ of polarized abelian varieties in characteristic zero. This insight is supported by the Hecke Orbit problem: any Hecke orbit is dense in $\mathcal{A}_g \otimes \mathbb{Q}$ on the one hand, and any prime-to- p Hecke orbit is dense in $\mathcal{A}_g \otimes \mathbb{F}_p$, the main theorem in [12].

Boundaries. We study inclusions after taking Zariski closures. For a locally closed subset $T \subset \mathcal{A}_g$ we define

$$\partial(T) := T^{\text{Zar}} - T \subset \mathcal{A}_g.$$

We know (solution of the Grothendieck conjecture) that $\partial(\mathcal{W}_\xi(\mathcal{A}_{g,1}))$ is the union of all NP strata as given by the partial ordering of Newton Polygons; however for non-principally polarized abelian varieties this is no longer true, and the inclusion pattern is complicated; see [74].

For EO strata we know that $\partial(S_\varphi)$ is the union of smaller strata in $\mathcal{A}_{g,1}$. However in the non-principally polarized case this pattern is hard to understand; see [74].

For central leaves we know $\partial(\mathcal{C}(x))$ is a union of leaves. It seems a hard and unsolved problem to determine for a given $\mathcal{C}(x) \subset \mathcal{W}_\xi(\mathcal{A}_g)$ which leaves appear in its boundary, see 9.4.

8.7. Structures described above have many applications.

For any g the moduli space $\mathcal{A}_{g,1} = \mathcal{A}_{g,1} \otimes \mathbb{F}_p$ is *geometrically irreducible*, as was proved by Faltings and by Chai (for $p > 2$); their proof uses the analogous fact

in characteristic zero, reduction mod p , and a careful study along the locus of degenerate abelian varieties.

By (EO) we have a pure characteristic p proof, see [68], 1.4: for any $S_\varphi \subset \mathcal{A}_{g,1}$ we know $\partial(S_\varphi)$ is the union of smaller EO strata, see [68], 1.3; Ekedahl proved that the Zariski closure of the unique one-dimensional EO stratum is connected, [68], Section 7, in particular 7.3; hence $\mathcal{A}_{g,1}$ is geometrically connected, and irreducibility follows. We note the interesting fact that we do not specialize to the boundary of $\mathcal{A}_{g,1}$, say in the Satake compactification, but that we specialize to smaller strata inside $\mathcal{A}_{g,1}$.

For another application, a proof of the Manin conjecture, see [67], Section 5.

8.8. Irreducibility. This story started with a theorem proved by Eichler, Deuring and Igusa, computing the number of supersingular elliptic curves as a class number, see [19], [17], [33]: the number of supersingular j -values, isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, is asymptotically $p/12$ for $p \rightarrow \infty$.

For $g > 1$ an analogous result holds, see [38], [39], [31], [46] 4.9. We see that (for p large)

the supersingular locus inside $\mathcal{A}_{g,1}$ is *reducible*.

Then we saw that supersingular strata and leaves on the one hand and non-supersingular strata and leaves on the other hand behave very differently as far as (ir)reducibility is concerned. Results:

- (NP) *Non-supersingular NP strata inside $\mathcal{A}_{g,1}$ are irreducible*, see [10], Th. A; see 8.9.
- (EO) *For any EO stratum S_φ inside $\mathcal{A}_{g,1}$ not contained in the supersingular locus Ekedahl and Van der Geer showed that S_φ is geometrically irreducible*, see [20], Th. 11.5 and [75], Th. 10.14.
- (Fol) *Any central leaf not contained in the supersingular locus is irreducible*, see [10], Th. B.

8.9. We give a (very brief) sketch of the proof of the geometric irreducibility of non-supersingular $W_\xi \subset \mathcal{A}_{g,1}$, see [6], [10] and [77], Chapter 5. We will see that this is a combination of beautiful geometric arguments and an elegant result on monodromy groups. For an algebraic variety (or an algebraic scheme) T we write $\Pi_0(T)$ for the set of irreducible components of $T \otimes k$.

(1). Using ideas and results by Raynaud [86], Th 5 on page 62, Moret-Bailly [55], XI.5 on page 237, we conclude that every EO stratum $S_\varphi \subset \mathcal{A}_{g,1}$ is quasi-affine, see [68], 1.2.

(2). Using this and using that Hecke prime-to- p orbits and Hecke ℓ -orbits outside the supersingular locus are infinite we show that for any irreducible component $T \subset W_\xi$ its boundary $\partial(T)$ contains an irreducible component of the supersingular locus $W_\sigma \subset \mathcal{A}_{g,1}$; for details see [77], Chapter 5, 6.4.2.

(3). In [46] we find a description of the set of irreducible components of $W_\sigma \otimes k$.

Remark. We see that for any $x \in W_\sigma$ the Hecke p -orbit $\mathcal{H}_p(x)$ is dense in at least one component, and for any prime $\ell \neq p$ the ℓ -Hecke orbit \mathcal{H}_ℓ acts transitively on $\Pi_0(W_\sigma)$.

(4). Using geometric arguments such as purity [37], the Grothendieck conjecture, see 4.7, the Cayley-Hamilton method as in [67], we show that the \mathcal{H}_ℓ -equivariant map $\Pi_0(W_\sigma) \rightarrow \Pi_0(W_\xi)$ is surjective; hence transitivity of \mathcal{H}_ℓ on $\Pi_0(W_\xi)$.

(5). A beautiful group theoretic argument, see [6], 4.4 shows the transitivity of \mathcal{H}_ℓ on $\Pi_0(W_\xi)$ finishes the proof of irreducibility of $W_\xi \otimes k$.

8.10. An Explicit Example. From the definitions it is clear that different NP strata do not intersect and different EO strata do not intersect. It turns out that the same is true for different central leaves.

For an ordinary NP, i.e. $\xi = g \cdot (1,0) + g \cdot (0,1)$ a NP stratum and a central leaf coincide; the same holds of the “almost ordinary NP” $(g-1) \cdot (1,0) + (1,1) + (g-1) \cdot (0,1)$; for all other Newton Polygons the number of central leaves in a NP stratum is infinite. A central leaf is zero-dimensional if and only if we work on the supersingular locus.

Here we illustrate the notion of leaves in a special case: principally polarized abelian varieties of dimension 3 and p -rank zero. There are two possible symmetric Newton Polygons in this case: $\xi = (2,1) + (1,2)$ and $g \cdot (1,1)$. We describe leaves in the first case. Here $W = W_\xi = \mathcal{W}_\xi(\mathcal{A}_{3,1})$ is irreducible and of dimension 3. Suppose $[(A, \lambda)] = x \in W$ such that $A[p^\infty]$ is *minimal*; in this case the central leaf $\mathcal{C}(x) = \mathcal{Z}$ is called the *central stream* of W_ξ ; we know all leaves in W_ξ are irreducible. Moreover it can be proved that in this case $\mathcal{Z} \subset W_\xi$ is the singular locus of W_ξ (as a stack, or after adding enough level structure). Moreover every central leaf in this W_ξ has dimension equal to 2. For any $y \in W_\xi - \mathcal{Z}$ the leaf $\mathcal{C}(y)$ is 2-dimensional and non-singular and contains only non-singular points of W_ξ ; every two different leaves do not intersect, and the whole situation can be seen as “parallel” surfaces in a 3-fold. The structure of W_ξ in this particular case is well-understood. For a more general case the picture of a foliation of a NP stratum looks very much the same.

It can be proved (but this seems particular for this choice of NP) that $\partial(\mathcal{C}(z))$ for any $z \in W_\xi$ is the 1-dimensional locus of supersingular abelian 3-folds with $a \geq 2$. For a more general case it seems hard to describe the boundary of a central leaf, see 9.4.

8.11. Serre-Tate Parameters. Let X_0 be an ordinary p -divisible group over a perfect field $\kappa \supset \mathbb{F}_p$, i.e. the Frobenius slopes are only 0 and 1. For this case the deformation space (equal characteristic p , or unequal characteristic $p=0$) are well-understood; see [96], [42], [53]. It is a beautiful example of families of p -divisible groups that are not constant, but where the geomet-

ric fibers are mutually isomorphic; indeed, this is an example of a leaf in a foliation.

One can wonder whether the notion of Serre-Tate parameters can be generalized to non-ordinary p -divisible groups; by now we know what the limitations are and what the correct generalization is; see Section 8 of C.-L. Chai and F. Oort – *Moduli of abelian varieties* in [77], Chapter 5: in general we have a notion of “generalized Serre-Tate parameters” on a central leaf in characteristic p . Beyond a central leaf this structure in general cannot be extended, not in characteristic p , not in mixed characteristics.

In order to understand families of p -divisible groups over a leaf as in 8.3 a new concept has been developed and rather well understood: *sustained p -divisible groups*. We will not discuss this concept here, but just refer to Chapter 7: C.-L. Chai and F. Oort – *Sustained p -divisible groups: a foliation re-traced* in [77], and to [12]. We use the terminology “sustained” as in music: a voice can remain constant, although the underlying harmony changes; in a sustained family of p -divisible groups fibers are mutually geometrically isomorphic, but the family need not be constant, even in general cannot be made constant by a faithfully flat base change.

For some literature, see: [6], [7], [8], [10], [12], [20], [52], [54], [67], [68], [69], [70], [71], [71], [75], [86], [113].

9. Some Questions

9.1. Suppose $N \rightarrow S$ is a finite presentation flat group scheme of constant order $n = \text{rank}(N/S)$. Is N/S annihilated by $[n]$, i.e. is

$$([n] : N \rightarrow N) \stackrel{?}{=} (N \rightarrow S \xrightarrow{e} N) ?$$

We know this is true for commutative group schemes by a theorem by Deligne, [109], page 4, [108], 3.8; we know this is true for a group scheme over a field, see [93], Coroll. 2.2. It suffices to show (or to have a counter example) for a finite flat local group scheme of order a power of p over a local Artin ring R with residue field $R \twoheadrightarrow \kappa = \bar{\kappa}$ an algebraically closed field of characteristic p . For more information see [25], Exp. VIII, Remarque 7.3.1; for a survey see [93].

9.2. Question (Tate, [105], Question on page 162). We know p -divisible groups over \mathbb{Z} :

$$\mu_{p,\infty,\mathbb{Z}} \quad \text{and} \quad \underline{\mathbb{Q}_p/\mathbb{Z}_p}_{\mathbb{Z}}.$$

Is every p -divisible group over \mathbb{Z} a product of copies of these?

9.3. As Manin conjectured, for every prime number p and every symmetric Newton Polygon ξ there exists

an abelian variety A over $\overline{\mathbb{F}_p}$ with $\mathcal{N}(A) = \xi$. [47], page 76, [106], page 98, [67], Section 5. However,

does there exist for every p and ξ an irreducible algebraic curve C over $\overline{\mathbb{F}_p}$ with $\mathcal{N}(\text{Jac}(C)) = \xi$?

Some special cases are known. The general case is unsolved, and this seems a hard problem. It might even be true that for a given ξ the answer for different prime numbers p can be different. E.g. see R. Preis – *Current results on Newton Polygons of curves*, [77], Chapter 6.

9.4. Question. We have seen that central leaves in one fixed NP stratum are “parallel” they do not intersect inside W_ξ . However many examples show that the Zariski closure of different central leaves meet in $(W_\xi)^{\text{Zar}}$.

Describe for every central leaf the “boundary” $\partial(\mathcal{C}(x)) = (\mathcal{C}(x))^{\text{Zar}} \setminus \mathcal{C}(x)$.

See [29].

9.5. Question. We have seen that any pair (C_0, φ) as in 6.1.5 can be lifted to a domain in characteristic zero. Can it be lifted to a *normal* domain in characteristic zero?

Remark. For an analogous problem, lifting CM abelian varieties, we have seen that lifting is possible (after applying an isogeny), but there are cases where no lifting is possible to a *normal* domain in characteristic zero; see the notion of the *residual reflex condition* in [7], 2.1.5.

9.6. NP Strata. Find a functorial description of NP strata. Determine which NP strata with this correct scheme structure are reduced.

An Afterthought. We have seen that p -divisible groups over a field, and p -divisible groups over a base scheme in characteristic p are rather well-understood; for applications in characteristic p geometry this has been a crucial tool.

However, we also said that p -divisible groups are not finite type (etc.) objects in algebraic geometry, and we have already seen particular care has to be taken in considerations in case the (arbitrary) base is not a field. In equal characteristic p this seems to be well-understood by now.

We did not discuss p -divisible groups in mixed characteristic; fascinating developments and applications are being developing recently. See:

- M. Rapoport and Th. Zink – *Period spaces for p -divisible groups*. Annals of Mathematics Studies, 141. Princeton University Press, Princeton, NJ, 1996.
- P. Scholze – *p -adic geometry*. <https://arxiv.org/abs/1712.03708>

- P. Scholze and J. Weinstein – *Moduli of p -divisible groups*. Cambridge J. Math. **1** (2013), 145–237. Also see <https://arxiv.org/pdf/1211.6357.pdf>
- L. Fargues and J.-M. Fontaine – *Courbes et fibrés vectoriels en théorie de Hodge p -adique*.
- The paper Courbe.df in: <https://webusers.imj-prg.fr/~laurent.fargues/Prepublications.html>

References

- [1] V. Abrashkin – *Projective varieties with bad semi-stable reduction at 3 only*. Doc. Math. **18** (2013), 547–619.
- [2] I. Barsotti – *Analytic methods for abelian varieties in positive characteristic*. Coll. Théorie des Groupes Algébriques (Bruxelles, 1962), pp. 77–85. Gauthier-Villars, 1962.
- [3] K. Buzzard – *Finite flat group schemes course*. Notes, 2012. http://www.imperial.ac.uk/~buzzard/maths/research/notes/finite_flat_group_schemes_course.pdf
- [4] P. Cartier – *Groupes algébriques et groupes formels*. Colloq. Théorie des groupes algébriques (Bruxelles, 1962), pp. 87–111. Librairie Universitaire, Louvain.
- [5] C.-L. Chai – *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*. Invent. Math. **121** (1995), 439–479.
- [6] C.-L. Chai – *Monodromy of Hecke-invariant subvarieties*. Pure Appl. Math. Q. **1** (2005). Special Issue: In memory of Armand Borel. Part 1, 291–303.
- [7] C.-L. Chai, B. Conrad and F. Oort – *Complex multiplication and lifting problems*. AMS series Mathematical Surveys and Monographs **195**. AMS, 2014. <http://www.ams.org/bookstore-getitem/item=surv-195>. <http://www.ams.org/publications/authors/books/postpub/surv-195>.
- [8] C.-L. Chai and F. Oort – *Moduli of abelian varieties and p -divisible groups*. Clay Mathematics Proceedings **8**. Arithmetic geometry, Clay Mathematics Institute Summer School, Göttingen 2006 (Ed. H. Darmon, D. Ellwood, B. Hassett and Y. Tschinkel), pp. 441–536. AMS, Clay Math. Inst., 2009. <http://www.math.rice.edu/~hassett/conferences/Clay2006/cmi-index.html>.
- [9] C.-L. Chai and F. Oort – *Hypersymmetric abelian varieties*. Pure Appl. Math. Q. **2** (2006). Special Issue: In honor of John H. Coates. Part 1, 1–27.
- [10] C.-L. Chai and F. Oort – *Monodromy and irreducibility of leaves*. Ann. Math. **173** (2011), 1359–1396. <http://annals.math.princeton.edu/2011/173-3/p03>.
- [11] C.-L. Chai and F. Oort – *Life and work of Alexander Grothendieck*. Notices of the ICCM **5** (2017), 22–50.
- [12] C.-L. Chai and F. Oort – *Hecke orbits*. [Book. In preparation.]
- [13] C. Chevalley – *Une démonstration d'un théorème sur les groupes algébriques*. J. Math. Pures et Appl. **39** (1960), 307–317.
- [14] B. Conrad – *A modern proof of Chevalley's theorem on algebraic groups*. <http://math.stanford.edu/~conrad/papers/chev.pdf>.
- [15] M. Demazure – *Lectures on p -divisible groups*. Lecture Notes in Math. **302**. Springer, Berlin, 1972.
- [16] M. Demazure and P. Gabriel – *Groupes algébriques*. Tome I: Géométrie algébrique, généralités, groupes commutatifs. With an appendix *Corps de classes local* by M. Hazewinkel. Masson & Cie, Éditeur, Paris, North-Holland Publishing Co., Amsterdam, 1970.
- [17] M. Deuring – *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*. Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
- [18] S. Edixhoven, G van der Geer and B. Moonen – *Abelian varieties*. [Book in preparation.] <https://www.math.ru.nl/~bmoonen/research.html#bookabvar>.
- [19] M. Eichler – *Über die Idealklassenzahl total definiter Quaternionenalgebren*. Math. Z. **43** (1938), 102–109.
- [20] T. Ekedahl and G. van der Geer – *Cycle classes of the E - O stratification on the moduli of abelian varieties*. Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I, Progr. Math. **269**, pp. 567–636. Birkhäuser Boston, Inc., Boston, MA, 2009.
- [21] G. Faltings and C.-L. Chai – *Degeneration of abelian varieties*. With an appendix by David Mumford. Ergebnisse der Mathematik und ihrer Grenzgebiete **22**. Springer-Verlag, Berlin, 1990.
- [22] J.-M. Fontaine – *Groupes p -divisibles sur les corps locaux*. Astérisque, No. 47–48. Société Mathématique de France, Paris, 1977.
- [23] J.-M. Fontaine – *Il n'y a pas de variété abélienne sur \mathbb{Z}* . Invent. Math. **81** (1985), 515–538.
- [24] A. Grothendieck – *Revêtements étales et groupe fondamental*. SGA1. Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, 1960/61. Lect. Notes Math. **224**. Springer-Verlag, 1971.
- [25] M. Demazure and A. Grothendieck – *Schémas en groupes*. SGA3. Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, 1962/64. Lect. Notes Math. **151**, **152**, **153**. Springer-Verlag, 1970.
- [26] A. Grothendieck – *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas*. Inst. Hautes Études Sci. Publ. Math. In 4 volumes:
 - [26]¹ No. 20, 1964.
 - [26]² No. 24, 1965.
 - [26]³ No. 28, 1966.
 - [26]⁴ No. 32, 1967.
- [27] A. Grothendieck – *Groupes de Barsotti-Tate et cristaux*. Actes du Congr. Internat. Math. (Nice, 1970), Tome 1, pp. 431–436.
- [28] A. Grothendieck – *Groupes de Barsotti-Tate et cristaux de Dieudonné*. Séminaire de Mathématiques Supérieures, No. 45 (Summer 1970). Les Presses de l'Université de Montréal, Montréal, 1974.
- [29] S. Harashita – *Questions on families of p -divisible groups*. In [77], Appendix 4.
- [30] R. Hartshorne – *Algebraic geometry*. Graduate Texts in Mathematics **52**. Springer-Verlag, New York-Heidelberg, 1977.
- [31] T. Ibukiyama, T. Katsura and F. Oort – *Supersingular curves of genus two and class numbers*. Compos. Math. **57** (1986), 127–152.
- [32] J.-I. Igusa – *On the algebraic theory of elliptic modular functions*. J. Math. Soc. Japan **20** (1968), 96–106.
- [33] J.-I. Igusa – *Class number of a definite quaternion with prime discriminant*. Proc. Nat. Acad. Sci. U.S.A. **44** (1958), 312–314.
- [34] L. Illusie – *Déformations de groupes de Barsotti-Tate*, d'après A. Grothendieck. In: Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell, Lucien Szpiro, Astérisque **127**, pp. 151–198. SMF, 1985.
- [35] L. Illusie – *Grothendieck at Pisa: crystals and Barsotti-Tate groups*. Talk at the Colloquium De Giorgi, Pisa, 2013. <https://www.math.u-psud.fr/~illusie/Illusie-Pisa5.pdf>.
- [36] N. Jacobson – *Basic algebra II*. W.H. Freeman & Co., 1989.

- [37] J. de Jong and F. Oort - *Purity of the stratification by Newton polygons*. J. Amer. Math. Soc. **13** (2000), 209-241.
- [38] T. Katsura and F. Oort - *Families of supersingular abelian surfaces*. Compositio Math. **62** (1987), 107-167.
- [39] T. Katsura and F. Oort - *Supersingular abelian varieties of dimension two or three and class numbers*. Algebraic geometry, Sendai, 1985, Adv. Stud. Pure Math. **10**, pp. 253-281. North-Holland, Amsterdam, 1987.
- [40] N. Katz - *p -adic properties of modular schemes and modular forms*. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Mathematics **350**, pp. 69-190. Springer, Berlin, 1973.
- [41] N. Katz - *Slope filtration of F -crystals*. Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, Astérisque **63**, pp. 113-163. Soc. Math. France, Paris, 1979.
- [42] N. Katz - *Serre-Tate local moduli*. Surfaces Algébriques (Ed. J. Giraud, L. Illusie, and M. Raynaud). Lecture Notes in Mathematics **868**, pp. 138-202. Springer Verlag, 1981. <https://link.springer.com/chapter/10.1007%2FBFb0090648>.
- [43] H.-P. Kraft - *Kommutative algebraische p -Gruppen (mit Anwendungen auf p -divisible Gruppen und abelsche Varietäten)*. Sonderforsch. Bereich Bonn, September 1975. Ms. 86 pp.
- [44] S. Lang - *Algebra* (revised 3rd ed.). Graduate Texts in Math. **211**. Springer-Verlag, 2002.
- [45] H. Lenstra and F. Oort - *Simple abelian varieties having a prescribed formal isogeny type*. J. Pure Appl. Algebra **4** (1974), 47-53.
- [46] K.-Z. Li and F. Oort - *Moduli of supersingular abelian varieties*. Lecture Notes in Mathematics **1680**. Springer-Verlag, Berlin, 1998.
- [47] Ju.I. Manin - *Theory of commutative formal groups over fields of finite characteristic*. Uspehi Mat. Nauk **18** 1963 (114), 3-90.
- [48] W. Messing - *The crystals associated to Barsotti-Tate groups: with applications to Abelian schemes*. Lecture Notes in Math. **264**, Springer, Berlin, 1972.
- [49] J. Milne - *Basic theory of affine group schemes*. Notes, 2012. <https://www.jmilne.org/math/CourseNotes/AGS.pdf>.
- [50] J. Milne - *Algebraic groups. The theory of group schemes of finite type over a field*. Cambridge Studies in Advanced Mathematics **170**. Cambridge University Press, Cambridge, 2017.
- [51] J. Milne - *The Riemann Hypothesis over finite fields from Weil to the present day*. The legacy of Bernhard Riemann after one hundred and fifty years. Vol. II, Advanced Lectures in Mathematics (ALM) **35.2**, pp. 14-52. Int. Press, Somerville, MA, 2016.
- [52] B. Moonen - *Group schemes with additional structures and Weyl group cosets*. In: *Moduli of abelian varieties* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. **195**, pp. 255-298. Birkhäuser Verlag, 2001.
- [53] B. Moonen - *Serre-Tate theory for moduli spaces of PEL type*. Ann. Sci. École Norm. Sup. **37** (2004), 223-269.
- [54] B. Moonen and T. Wedhorn - *Discrete invariants of varieties in positive characteristic*. Int. Math. Res. Not. **72** (2004), 3855-3903.
- [55] L. Moret-Bailly - *Pinceaux de variétés abéliennes*. Astérisque **129** (1985).
- [56] D. Mumford - *Abelian varieties*. Tata Inst. Fund. Res. Studies in Mathematics **5**. Published for the Tata Institute of Fundamental Research, Bombay. Oxford University Press, London, 1970.
- D. Mumford - *Abelian varieties*. With appendices by C.P. Ramanujam and Yuri Manin. Corrected reprint of the second (1974) edition. By Hindustan Book Agency, New Delhi, 2008.
- [57] D. Mumford - *Geometric invariant theory*. Ergebn. Math., Neue Folge, Band 34. Springer-Verlag, Berlin-New York, 1965.
- D. Mumford and J. Fogarty - *Geometric invariant theory*. Second edition. Springer-Verlag, Berlin, 1982.
- D. Mumford, J. Fogarty and F. Kirwan - *Geometric invariant theory*. Third edition. Springer-Verlag, Berlin, 1994.
- [58] D. Mumford - *Selected papers*, Volume II. On algebraic geometry, including correspondence with Grothendieck (Ed. Ching-Li Chai, Amnon Neeman and Takahiro Shiota). Springer, New York, 2010.
- [59] P. Norman - *Lifting abelian varieties*. Invent. Math. **64** (1981), 431-443.
- [60] P. Norman and F. Oort - *Moduli of abelian varieties*. Ann. of Math. **112** (1980), 413-439.
- [61] A. Obus and S. Wewers - *Cyclic extensions and the local lifting problem*. Ann. Math. **180** (2014), 233-284.
- [62] A. Ogg - *Abelian curves of 2-power conductor*. Proc. Cambridge Philos. Soc. **62** (1966), 143-148.
- [63] F. Oort - *Commutative group schemes*. Lecture Notes in Mathematics **15**. Springer-Verlag, Berlin-New York, 1966.
- [64] F. Oort - *Algebraic group schemes in characteristic zero are reduced*. Invent. Math. **2** (1966), 79-80.
- [65] F. Oort - *Finite group schemes, local moduli for abelian varieties, and lifting problems*. Compos. Math. **23** (1971), 265-296.
- [66] F. Oort - *Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero*. Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math. **46**, Part 2, pp. 165-195. Amer. Math. Soc., Providence, RI, 1987.
- [67] F. Oort - *Newton polygons and formal groups: conjectures by Manin and Grothendieck*. Ann. of Math. **152** (2000), 183-206.
- [68] F. Oort - *A stratification of a moduli space of abelian varieties*. In: *Moduli of abelian varieties*. (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. **195**, pp. 345-416. Birkhäuser Verlag, 2001.
- [69] F. Oort - *Newton polygon strata in the moduli space of abelian varieties*. In: *Moduli of abelian varieties*. (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. **195**, pp. 417-440. Birkhäuser Verlag, 2001.
- [70] F. Oort - *Foliations in moduli spaces of abelian varieties*. J. Amer. Math. Soc. **17** (2004), 267-296.
- [71] F. Oort - *Minimal p -divisible groups*. Ann. of Math. **161** (2005), 1021-1036.
- [72] F. Oort - *Simple p -kernels of p -divisible groups*. Adv. Math. **198** (2005), 275-310.
- [73] F. Oort - *Abelian varieties over finite fields*. Summer School on "Varieties over finite fields", Göttingen, 2007. Higher-dimensional geometry over finite fields. Proceedings of the NATO Advanced Study Institute 2007 (Ed. Dmitry Kaledin, Yuri Tschinkel), pp. 123-188. IOS Press, 2008. <http://www.math.nyu.edu/~tschinke/books/finite-fields/finite.html>. http://www.math.nyu.edu/~tschinke/books/finite-fields/final/05_oort.pdf.
- [74] F. Oort - *Foliations in moduli spaces of abelian varieties and dimension of leaves*. Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. II, Progr. Math. **270**, pp. 465-501. Birkhäuser Boston, Inc., Boston, MA, 2009.
- [75] F. Oort - *Moduli of abelian varieties in mixed and*

- in positive characteristic*. Handbook of moduli. Vol. III, Adv. Lect. Math. (ALM) **26**, pp. 75–134. Int. Press, Somerville, MA, 2013.
- [76] F. Oort – *Gauss: the last entry*. Notices of the ICCM **4** (2016), 29–39.
- [77] F. Oort – *Open problems in arithmetic algebraic geometry*. With contributions by R. Schoof, A. Obus, J. Tsimerman, C.-L. Chai and R. Preis. Advanced Lectures in Mathematics (ALM) **46**, International Press and Higher Education Press of China, 2019.
- [78] F. Oort – *CM Jacobians*. Motives and complex multiplications (Ed. Javier Fresán and Peter Jossen), Summer School Ascona, 2016. [To appear.]
- [79] F. Oort – *A method in deformation theory*. [To appear.]
- [80] F. Oort and D. Mumford – *Deformations and liftings of finite, commutative group schemes*. Invent. Math. **5** (1968), 317–334.
- [81] F. Oort and N. Schappacher – *Early history of the Riemann hypothesis in positive characteristic*. The legacy of Bernhard Riemann after one hundred and fifty years. Vol. II, Advanced Lectures in Mathematics (ALM) **35.2**, pp. 595–631. Int. Press, Somerville, MA, 2016.
- [82] F. Oort and T. Zink – *Families of p -divisible groups with constant Newton polygon*. Doc. Math. **7** (2002), 183–201.
- [83] R. Pink – *Finite group schemes*. Lecture course in WS 2004/05, ETH Zürich. <ftp://ftp.math.ethz.ch/users/pink/FGS/CompleteNotes.pdf>.
- [84] B. Poonen – *Rational points on varieties*. Graduate Studies in Mathematics **186**. American Mathematical Society, Providence, RI, 2017.
- [85] F. Pop – *The Oort conjecture on lifting covers of curves*. Ann. of Math. **180** (2014), 285–322.
- [86] L. Szpiro – *Propriétés numériques du faisceau dualisant relatif*. Séminaire sur les pinceaux de courbes de genre au moins deux. École Normale Supérieure, Paris, 1983–1984 (Ed. L. Szpiro). Astérisque **86** (1981), 44–78.
- [87] M. Schlessinger – *Functors of Artin rings*. Trans. Amer. Math. Soc. **130** (1968), 208–222.
- [88] R. Schoof – *Introduction to finite group schemes*. Notes taken by John Voight, 2000. <https://math.dartmouth.edu/~jvoight/notes/274-Schoof.pdf>.
- [89] R. Schoof – *Finite flat group schemes over local Artin rings*. Compos. Math. **128** (2001), 1–15.
- [90] R. Schoof – *Abelian varieties over the field of the 20th roots of unity that have good reduction everywhere*. Applications of algebraic geometry to coding theory, physics and computation (Eilat, 2001), NATO Sci. Ser. II Math. Phys. Chem. **36**, pp. 291–296. Kluwer Acad. Publ., Dordrecht, 2001.
- [91] R. Schoof – *Abelian varieties over $\mathbb{Q}(\sqrt{6})$ with good reduction everywhere*. Class field theory, its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math. **30**, pp. 287–306. Math. Soc. Japan, Tokyo, 2001.
- [92] R. Schoof – *Abelian varieties over cyclotomic fields with good reduction everywhere*. Math. Ann. **325** (2003), 413–448.
- [93] R. Schoof – *Is a finite locally free group scheme killed by its order?* Chapter 1 in [77].
- [94] J.-P. Serre – *Exemples de variétés projectives en caractéristique p non relevable en caractéristique zéro*. Proc. Nat. Acad. Sc. USA **47** (1961), 108–109.
- [95] J.-P. Serre – *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), 259–331.
- [96] J. Lubin, J.-P. Serre and J. Tate – *Elliptic curves and formal groups*. Summer Institute on Algebraic Geometry, Woods Hole, 1964. <http://www.ma.utexas.edu/users/voloch/1st.html>.
- [97] J.-P. Serre and J. Tate – *Good reduction of abelian varieties*. Ann. of Math. **88** (1968), 492–517.
- [98] *Correspondance Serre-Tate*. Volume I (1956–1973) & Volume II (1973–2000). Edited, and with notes and commentaries by Pierre Colmez and Jean-Pierre Serre. Documents Mathématiques **13** & **14**. Société Mathématique de France, 2015.
- [99] I. Shafarevich – *Algebraic number fields*. Proceedings of the International Congress of Mathematicians (Stockholm, 1962), pp. 163–176. Inst. Mittag-Leffler, Djursholm, 1963. Amer. Math. Soc. Transl. **31** (1963), 25–39.
- [100] J. Silverman – *The arithmetic of elliptic curves*. Graduate Texts in Mathematics **106**. Springer-Verlag, New York, 1986.
- [101] *The stacks project*. <https://stacks.math.columbia.edu/>.
- [102] R. Stroeker – *Elliptic curves defined over imaginary quadratic number fields*. A Diophantine approach. Ph.D. Thesis. Universiteit van Amsterdam, Amsterdam, 1975.
- [103] J. Stix – *A course on finite flat group schemes and p -divisible groups*. https://www.uni-frankfurt.de/52288632/Stix_finflat_Grpschemes.pdf.
- [104] J. Tate – *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2** (1966), 134–144.
- [105] J. Tate – *p -divisible groups*. Proc. Conf. Local Fields (Driebergen, 1966), pp. 158–183. Springer, 1967.
- [106] J. Tate – *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*. Sémin. Bourbaki. 1968/69: Exposés 347–363; Exp. 352, Lecture Notes in Math. **175**, pp. 95–110. Springer, Berlin, 1971.
- [107] J. Tate – *The arithmetic of elliptic curves*. Invent. Math. **23** (1974), 179–206. <http://www.fen.bilkent.edu.tr/~franz/ta/tate.pdf>.
- [108] J. Tate – *Finite flat group schemes*. Modular forms and Fermat's last theorem (Boston, MA, 1995), pp. 121–154. Springer, New York, 1997.
- [109] J. Tate and F. Oort – *Group schemes of prime order*. Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.
- [110] H. Verhoeck – *Modularity of abelian varieties over \mathbb{Q} with bad reduction in one prime only*. J. Number Theory **133** (2013), 3065–3098.
- [111] W. Waterhouse – *Abelian varieties over finite fields*. Ann. Sci. École Norm. Sup. **2** (1969), 521–560.
- [112] W. Waterhouse – *Introduction to affine group schemes*. Graduate Texts in Mathematics **66**. Springer-Verlag, New York-Berlin, 1979.
- [113] T. Zink – *On the slope filtration*. Duke Math. J. **109** (2001), 79–95.