GROUP SCHEMES

MATTHEW HASE-LIU AND KENZ KALLAL

Contents

Introduction

These notes are the result of a reading course we did in Spring 2020, generously supervised by Professor Barry Mazur. During the first month, we read about the general theory of abelian varieties from Mumford's book [8]. That material is not present in these notes. Instead, these notes are about what we read in March, April, and May 2020 about group schemes, especially finite flat group schemes over an affine base. We started by reading the expository notes of Voight [17] and Tate's article [13] in the Cornell–Silverman–Stevens

E-mail address: kenzkallal@college.harvard.edu, matthewhaseliu@college.harvard.edu.

Date: September 13, 2020.

volume on Fermat's last theorem. Then, we read three foundational papers in the field: Oort–Tate's classification of group schemes of prime order over certain bases [14], Fontaine's bound [4] on the ramification of an extension formed by adjoining points of a finite flat group scheme (which he used to prove his theorem on nonexistence of abelian varieties of $\mathbf{Z}$, generalizing an earlier result of Tate), and Tate's paper [12] on p-divisible groups, which A. Abbes told us is the paper that gave birth to p-adic Hodge theory. Towards the end of the process of writing these notes, we came across J. Stix's useful notes [11], from which many of our explanations beyond the original source material are taken, especially for the exposition on p-divisible groups.

Our goal for these notes is not to repeat the arguments in the standard literature on this topic, although we do a lot of that. Instead, the goal is to explain in detail some of the most important arguments, filling in missing steps which were not originally obvious to us.

1. Generalities

1.1. **Yoneda lemma for group objects.**

At some point, we only had an ad-hoc way to prove this for group schemes, but actually it is an easy exercise that holds in general for group objects in an arbitrary category.

Lemma 1.1. *Let $\mathcal{C}$ be a small category with finite products and a final object Z, and $\mathsf{Grp}_{\mathcal{C}}$ the category of group objects in $\mathcal{C}$. Then for all $X \in \mathsf{Grp}_{\mathcal{C}}$, the functor of points*

$$h_X : \mathcal{C} \to \mathsf{Set},$$

namely

$$A \mapsto \mathrm{Hom}_{\mathcal{C}}(A, X)$$

factors through the forgetful functor $\mathsf{Grp} \to \mathsf{Set}$. The resulting functor

$$Y : \mathsf{Grp}_{\mathcal{C}} \to \mathsf{Func}(\mathcal{C}^{\mathrm{op}}, \mathsf{Grp})$$

given by $X \mapsto h_X$ is fully faithful.

Proof. The group structure on $\mathrm{Hom}_{\mathcal{C}}(A, X)$ is given by the identity element $A \to Z \xrightarrow{\epsilon} X$, composition law $a \circ b = m \circ (a \times b)$, and inverse $a^{-1} = i \circ a$. For any morphism $d : A \to B$, the induced morphism

$$h_X(d) : \mathrm{Hom}_{\mathcal{C}}(B, X) \to \mathrm{Hom}_{\mathcal{C}}(A, X)$$

given by precomposition by d is a group homomorphism (an easy consequence of the universal property of $X \times X$). Combined with the fact that h_X is already a functor to Set, this shows that it can be considered as a functor to Grp instead (one which composes with the forgetful functor to Set to give the original h_X). If $f : X \to X'$ is a group object morphism, then $Y(f) : h_X \to h_{X'}$ is given on objects by postcomposition by f. That map $f \circ - : h_X(A) \to h_{X'}(A)$ is a group homomorphism because f is a group object morphism, and by the usual arguments it is clear that $Y(f)$ is a natural transformation of contravariant functors from $\mathcal{C}$ to Grp and that Y is indeed a functor.

It remains to show that Y is fully faithful. The fact that Y is faithful is immediate from the ordinary Yoneda lemma. In particular, if F, G are in the image of Y so that $F = h_X$ and $G = h_{X'}$, and $\tau : F \to G$ is a natural transformation, then for all $A \in \mathcal{C}$, the group homomorphism $\tau_A : \mathrm{Hom}_{\mathcal{C}}(A, X) \to \mathrm{Hom}_{\mathcal{C}}(A, X')$ is given as a map of sets by postcomposition by $\tau_X(\mathrm{id})$, and this is the unique way of writing it in the form $f \circ -$ for some fixed morphism $f : X \to X'$ (this is the Yoneda lemma). To show that Y is full, we just need to show that $\tau_X(\mathrm{id}) : X \to X'$ is a homomorphism of group objects (a priori it is just a morphism in $\mathcal{C}$), so that τ_A is indeed induced by a morphism in $\mathsf{Grp}_{\mathcal{C}}$. To do that, we need to use the fact that τ is a natural transformation between F and G, not only as functors to Set but also Grp. In other words, the diagram

$$\begin{tikzcd} h_{X\times X} \arrow[r, "m\circ-"] \arrow[d, "\tau\times\tau"] & h_X \arrow[d, "\tau"] \\ h_{X'\times X'} \arrow[r, "m'\circ-"] & h_{X'} \end{tikzcd}$$

in the category $\mathsf{Func}(\mathcal{C}, \mathsf{Set})$ commutes. The vertical natural transformation $\tau \times \tau : h_{X\times X} \to h_{X'\times X'}$ is defined using the natural isomorphism $h_{X\times X} \cong h_X \times h_X$ (the universal property of the product). By the ordinary Yoneda lemma, this diagram is obtained by applying the Yoneda embedding to the diagram

$$\begin{tikzcd} X \times X \arrow[r, "m"] \arrow[d, "\tau_X(\mathrm{id})\times\tau_X(\mathrm{id})"] & X \arrow[d, "\tau_X(\mathrm{id})"] \\ X' \times X' \arrow[r, "m'"] & X' \end{tikzcd}$$

which also commutes (by the Yoneda lemma). This proves that $\tau_X(\mathrm{id})$ is a group object homomorphism, as desired. □

One special case of Lemma 1.1 is

Corollary 1.2. *If two functors $\mathcal{C}^{\mathrm{op}} \to \mathsf{Grp}$ in the image of Y are naturally isomorphic, then they are represented by group objects in $\mathcal{C}$ which are isomorphic as group objects. In particular, a group object in $\mathcal{C}$ is determined up to isomorphism (as a group object) by its functor of points.*

Remark 1.3. Moreover, it is easy to directly recover the group object structure of the group object corresponding to such a representable functor, if we know X as an object in $\mathcal{C}$ and h_X as a functor to Grp.

(1) To recover $m : X \to X \to X$, consider it as an element of the group $h_X(X \times X)$. By the definition of the group structure of $h_X(X \times X)$ we state earlier in this proof, m can be recovered as the product in that group of the two canonical projections onto each copy of X.
(2) To recover $i : X \to X$, consider it as an element of the group $h_X(X)$. It can be recovered by taking the inverse of the identity morphism $X \to X$ in that group.
(3) To recover $\epsilon : Z \to X$, consider it as an element of the group $h_X(Z)$, where we know it is the identity element.

This principle also leads to an improvement to Lemma 1.1,

Lemma 1.4. *Let $F \in \mathsf{Func}(\mathcal{C}^{\mathrm{op}}, \mathsf{Grp})$ such that* $\mathrm{Forget} \circ F \in \mathsf{Func}(\mathcal{C}^{\mathrm{op}}, \mathsf{Set})$ *is representable by $X \in \mathcal{C}$. Then there is a unique group object structure on X such that $F = Y(X)$.*

Proof. The uniqueness part is taken care of by Lemma 1.1 at least up to isomorphism, and by Remark 1.3 in terms of equality. It just remains to show that the construction of the group object morphisms in the remark provide a bona fide group object structure on X, and that the functor to Grp induced by that group object agrees with F. For the second one, we need to check that for $a, b \in \operatorname{Hom}_{\mathcal{C}}(A, X)$, we have

$$a \cdot b = (\pi_1 \cdot \pi_2) \circ (a \times b)$$

where π_1, π_2 are the projections $X \times X \to X$. This amounts to the fact that precomposition by $a \times b$ is a group homomorphism

$$\operatorname{Hom}_{\mathcal{C}}(X \times X, X) \to \operatorname{Hom}_{\mathcal{C}}(A, X),$$

which is true because of the functoriality of $h_X : \mathcal{C}^{\mathrm{op}} \to \mathsf{Grp}$. Indeed, the fact that this is a group homomorphism applied to the two morphisms $\pi_1, \pi_2 \in \operatorname{Hom}_{\mathcal{C}}(X \times X, X)$ shows that

$$(\pi_1 \cdot \pi_2) \cdot (a \times b) = (\pi_1 \cdot (a \times b)) \cdot (\pi_2 \cdot (a \times b)) = a \cdot b.$$

The first one (checking that the structure given in Remark 1.3 yields a bona fide group scheme structure on X) amounts to the commutativity of some collection of diagrams, which are mapped under the Yoneda embedding to diagrams in the category $\mathsf{Func}(\mathcal{C}^{\mathrm{op}}, \mathsf{Set})$ whose commutativity amounts to the fact that $F \in \mathsf{Func}(\mathcal{C}^{\mathrm{op}}, \mathsf{Grp})$. □

This provides a convenient way of constructing group schemes: by first constructing the scheme, and then assigning in a functorial way the group structure on the S-points of the scheme for all schemes S.

This is indicative of a general principle of checking properties on points. For instance, we have

Lemma 1.5. *A group object $(X, m, \epsilon, i) \in \mathcal{C}$ is commutative if and only if $h_X(A)$ is commutative for all $A \in \mathcal{C}$.*

Proof. One direction is obvious: if X is commutative, then by definition of the group structure of $h_X(A)$, that is commutative also. On the other hand, $h_X(A)$ being commutative for all A means that the diagram

$$\begin{tikzcd} h_{X \times X} \arrow[r, "m\circ -"] \arrow[d] & h_X \arrow[d, "i\circ -"] \\ h_{X \times X} \arrow[r, "m\circ -"] & h_X \end{tikzcd}$$

in $\mathsf{Func}(\mathcal{C}^{\mathrm{op}}, \mathsf{Set})$ is commutative, where the left vertical morphism is given by identifying $h_{X \times X} \cong h_X \times h_X$ and applying $i \circ -$ to each factor. This diagram is induced under the Yoneda embedding by

$$\begin{tikzcd} X \times X \arrow[r, "m"] \arrow[d, "i\times i"] & X \arrow[d, "i"] \\ X \times X \arrow[r, "m"] & X \end{tikzcd}$$

which is commutative as a result. But the commutativity of this diagram is equivalent to X being a commutative group object. □

So far, we have not used the Yoneda lemma in the form we proved in Lemma 1.1, only the standard version for functors into Set. Still, Lemma 1.1 will be useful for us, for instance for writing down isomorphisms between group schemes in terms of their functors of points. On the other hand, Lemma 1.4 will be useful mostly for specifying group scheme structure on a given scheme.

1.2. **Direct products, base change, and kernels.** Suppose that fiber products exist in $\mathcal{C}$. Then the category $\mathsf{Grp}_{\mathcal{C}}$ has finite direct products. In particular, for two group objects (X, m, ϵ, i) and (X', m', ϵ', i'), there is an obvious group scheme structure on $X \times X' = X \times_Z X'$. For instance, the multiplication morphism

$$(X \times X') \times (X \times X') \to X \times X'$$

is defined using the universal property of $X \times X'$ by mapping into the X-ccordinate via the composition

$$(X \times X') \times (X \times X') \xrightarrow{\pi_X \times \pi_X} X \times X \xrightarrow{m} X$$

and similarly for the X'-coordinate. The same type of analogy with products of actual groups can be used to define the inverse and identity morphisms, and it is simple to check that together they define a group object structure on $X \times X'$. Under this group object structure, one can also check as usual that the morphisms $X \times X' \to X$ and $X \times X' \to X'$ are group object homomorphisms, and that $X \times X'$ satisfies the universal property for the direct product in the category of group objects in $\mathcal{C}$. Also, the morphism $m : X \times X \to X$ can be checked either by direct manipulation with morphisms or by looking at points and applying Lemma 1.1 to be a homomorphism of group objects.

Now, let S be a scheme, and $\mathsf{Sch}_{/S}$ the category of schemes over S. The category of group objects in this category is the category of S-*group schemes.* In this setting, for any S-scheme T and S-group scheme G, it is natural to consider the base change $G \times_S T$, which is at least a T-scheme. Since T is the final object in $\mathsf{Sch}_{/T}$, for any T-scheme T', we have a natural bijection of sets

$$h_{G \times_S T}(T') \cong h_G(T).$$

This means that $h_{G \times_S T}$ factors through the forgetful functor from Grp, and by Lemma 1.4, this allows us to put a natural T-group scheme structure on $G \times_S T$.

Definition 1.6. The *kernel* of a morphism of group objects $f : G \to G'$, if it exists, is a morphism $\varphi : H \to G$ characterized by the following universal property: any morphism $X \to G$ such that the composition $X \to G \xrightarrow{f} G'$ equals $X \to Z \xrightarrow{\epsilon'} G'$ factors uniquely through φ.

Kernels of maps of group schemes (and really of group objects in general) are easy to write down. In particular, the universal property of the kernel is the same as the universal property of the fiber product

$$\begin{tikzcd}
G \times_{G'} Z \arrow[r] \arrow[d, "\varphi"] & Z \arrow[d, "\epsilon'"] \\
G \arrow[r, "f"] & G'
\end{tikzcd}$$

So, we have

Lemma 1.7. *If finite fiber products exist in $\mathcal{C}$, then kernels of group-object morphisms exist.*

When $\mathcal{C} = \mathsf{Sch}_{/S}$, we have $Z = S$, and $G \times_{G'} S$ is an S-group scheme, with $\varphi : G \times_{G'} S \to G$ a morphism of S-schemes.

Lemma 1.8. *$\varphi : G \times_{G'} S \to G$ is a morphism of S-group schemes.*

Proof. φ induces a natural transformation of functors to the category of sets $h_{G\times_{G'}S}\to h_G$. By Lemma 1.1, it suffices, to check that this is also a natural transformation of functors to the category of groups, i.e. that it gives group homomorphisms on points. This is easy to check using the fact that

$$\begin{tikzcd}
(G\times_{G'}S)(T) \arrow[r] \arrow[d, "\varphi(T)"] & S(T) \arrow[d, "\epsilon'(T)"] \\
G(T) \arrow[r, "f(T)"] & G'(T)
\end{tikzcd}$$

is a pullback square, and $f(T)$ is a group homomorphism (and as we have already used, $S(T)$ is the set with one element where $\epsilon'(T)$ maps that element to the identity in the group $G'(T)$). □

Taking this analysis to its logical conclusion gives a convenient description of the kernel as the group-theoretic kernel on points.

Lemma 1.9. *For all S-schemes T, $\varphi(T)$ is injective, and embeds $(G\times'_G S)(T)$ into $G(T)$ as the kernel of $f(T):G(T)\to G'(T)$.*

Proof. Using the standard description of the fiber product of sets and the fact that, we have

$$(G\times'_G S)(T)=\{(a,b)\in G(T)\times S(T):(f(T))(a)=1\}$$

and φ is the canonical projection to $G(T)$, from which the lemma is clear. □

1.3. **Cartier duality.** Let R be a noetherian ring and $G=\operatorname{Spec}A$ be a commutative affine R-group scheme, so that A is a commutative Hopf algebra over R. Assume further that G is finite flat, i.e. that A is a finite flat R-module. Only remembering the R-module structure of A, the additional Hopf algebra structure consists of

- The ring multiplication morphism $A\otimes_R A\to A$, only required to be an R-module homomorphism.
- The R-algebra structure morphism $R\to A$, a ring homomorphism
- The comultiplication morphism $A\to A\otimes_R A$, an R-algebra homomorphism.
- The inverse morphism $A\to A$, an R-algebra homomorphism.
- The identity morphism $A\to R$, an R-algebra homomorphism.

The commutative Hopf algebra structure of A also enforces some properties on these morphisms, of course. Taking the dual $A^\vee=\operatorname{Hom}_{\mathsf{Mod}_R}(A,R)$, the five morphisms above dualize to R-module homomorphisms.

Theorem 1.10. *The five dual morphisms provide $A^\vee$ with the structure of a commutative Hopf R-algebra.*

Proof. The fact that A is finite and flat over R means it is locally free of finite rank[1], so we have an isomorphism

$$A_{\mathfrak{p}}^\vee\otimes_{R_{\mathfrak{p}}}A_{\mathfrak{p}}^\vee\cong(A_{\mathfrak{p}}\otimes_{R_{\mathfrak{p}}}A_{\mathfrak{p}})^\vee$$

[1] This uses the fact that R is Noetherian: every finitely-generated module over a noetherian ring is finitely-presented; finitely-presented and flat implies projective; and projective modules over local rings are free.

for all prime ideals $\mathfrak{p}$ in R, given on pure tensors by taking $f \otimes g$ to the element of $(A_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} A_{\mathfrak{p}})^\vee$ given on pure tensors by $a \otimes b \mapsto f(a)g(b)$. Commuting the localization with the tensor products and duals[2], we get a local isomorphism for all primes, and thus the map

$$(A \otimes_R A)^\vee \to A^\vee \otimes_R A^\vee$$

given by the same formula as above is an isomorphism (it localizes to an isomorphism at each prime). The comultiplication morphism $A \to A \otimes_R A$ dualizes to an R-module homomorphism $A^\vee \otimes A^\vee \to A^\vee$. The fact that A is a commutative Hopf algebra implies that this homomorphism provides $A^\vee$ with the structure of a ring without unit. The counit morphism $A \to R$ dualizes to an R-module homomorphism $R \to A^\vee$. The fact that A is a Hopf algebra implies that this is a ring homomorphism, and thus provides $A^\vee$ with R-algebra structure (and also with a unit element in $A^\vee$). The axiom that guarantees this is the commutativity of the diagram

$$\begin{tikzcd}
\operatorname{Spec} R \times \operatorname{Spec} R \arrow[r, "\sim"] \arrow[d, "\epsilon\times\epsilon"'] & \operatorname{Spec} R \arrow[r, "\epsilon"] & G \\
G \times G \arrow[urr, "m"] & &
\end{tikzcd}$$

which dualizes (once in the sense of categories and once in the sense of taking the dual R-modules) to a diagram which expresses precisely the fact that $R \to A^\vee$ respects multiplication under the ring structure on $A^\vee$ induced by comultiplication. This map also provides a unit element in $A^\vee$ (the image of 1), so together we have shown that dualizing the comultiplication and counit provides a unital R-algebra structure on $A^\vee$. In fact, one can check that this algebra is also commutative, as a result of the assumption that G is commutative as a group scheme (the point of this is that the map $A^\vee \otimes A^\vee \to A^\vee \otimes A^\vee$ that switches the two coordinates is dual to the coordinate-switching morphism $A \otimes A \to A \otimes A$, which corresponds via Spec to the switching morphism $G \times G \to G \times G$, so the commutativity of the diagram

$$\begin{tikzcd}
G \times G \arrow[r, "m"] & G \\
G \times G \arrow[u] \arrow[ur, "m"] &
\end{tikzcd}$$

where the vertical map is the coordinate-switching morphism proves that $A^\vee$ is commutative as a ring).

The ring multiplication $A \otimes_R A \to A$ dualizes to a candidate comultiplication morphism $A^\vee \to A^\vee \otimes_R A^\vee$; the R-algebra structure morphism $R \to A$ dualizes to a candidate counit morphism $A^\vee \to R$; and the coinverse morphism $A \to A$ dualizes to a candidate coinverse morphism $A^\vee \to A^\vee$. One checks directly that these are all ring homomorphisms, and that they provide bona fide commutative Hopf algebra structure on $A^\vee$. Note that the assumption that G is commutative is needed here also, in order to establish the fact that the coinverse morphism dualizes to a ring homomorphism (commutativity of G is equivalent to the coinverse morphism being a group homomorphism). The commutative Hopf algebra axioms are obviously true, because the diagrams that express the fact that G is a commutative group scheme dualize (first in the sense of diagrams involving A, then $A^\vee$ as before) to diagrams

[2] That localization commutes with tensor products is a general fact. It also commutes with taking the dual, which is okay under our hypotheses because A is finitely-presented over R due to being finitely-generated and the fact that R is assumed Noetherian.

expressing what we need, which look exactly the same as the original ones for G except with G replaced with $A^\vee$. For proving that the candidate morphisms are really ring homomorphisms, one example is given above already (the one that proves that the dual map $R \to A^\vee$ is a ring homomorphism). Here is another example: the candidate counit morphism $A^\vee \to R$ is a ring homomorphism because it sends the identity element $\epsilon \in A^\vee$ to

$$(\epsilon \circ (R \to A))(1),$$

which is 1 because $\epsilon : A \to R$ is a ring homomorphism and so is $R \to A$; and because the commutative diagram

$$\begin{tikzcd}
G \times G \arrow[r, "m"] \arrow[d] & G \arrow[r] & \operatorname{Spec} R \\
\operatorname{Spec} R \times \operatorname{Spec} R \arrow[urr, "\sim"] & &
\end{tikzcd}$$

proves the multiplicativity. The candidate coinverse morphism $A^\vee \to A^\vee$ is a ring homomorphism because it sends the identity $\epsilon \in A^\vee$ to $\epsilon \circ (A \to A)$, which is again ϵ because ϵ is the identity element when considered as a $\operatorname{Spec} R$-point of G, and composition with the inverse morphism takes the identity element to itself; the multiplicativity comes from the commutativity of the diagram

$$\begin{tikzcd}
G \times G \arrow[r, "m"] \arrow[d, "i \times i"] & G \arrow[d, "i"] \\
G \times G \arrow[r, "m"] & G
\end{tikzcd}$$

(this is the second place where we use the fact that G is commutative; one way to see this is equivalent to the commutativity of G is to use Lemma 1.5). Finally, the fact that the candidate comultiplication morphism $A^\vee \to A^\vee \otimes A^\vee$ is a ring homomorphism is due to the fact that it takes the identity element ϵ to $(\epsilon \circ (A \otimes A \to A)$, which is $\epsilon \otimes \epsilon$ because $A \otimes A \to A$ corresponds under Spec to the diagonal map $G \to G \times G$. The multiplicativity comes from the commutativity of the diagram

$$\begin{tikzcd}
G \times G \arrow[r, "\Delta \times \Delta"] \arrow[d, "m"] & (G \times G) \times (G \times G) \arrow[d, "m_{G \times G}"] \\
G \arrow[r, "\Delta"] & G \times G
\end{tikzcd}$$

which is tautological. □

So now we have access to a new affine R-group scheme $G^\vee$ which as a scheme is $\operatorname{Spec} A^\vee$, where $A^\vee$ has the R-algebra structure described in Theorem 1.10 (the group object structure is given by the three Hopf algebra structure morphisms also described in Theorem 1.10). This group scheme $G^\vee$ is dual to G in the following sense:

Theorem 1.11 (Cartier duality)**.** *Let $G = \operatorname{Spec} A$ be a finite flat affine commutative group scheme over a Noetherian ring R. The functors $\mathsf{Alg}_R \to \mathsf{Grp}$ given by $h_{G^\vee}$ and*

$$\operatorname{Hom}_{\mathsf{AffGrpSch}_\mathsf{R}}(G \times_R \operatorname{Spec} -, \mathbf{G}_{m,R} \times_R \operatorname{Spec} -)$$

are naturally isomorphic.

Proof. The functor

$$\mathrm{Hom}_{\mathsf{AffGrpSch_R}}(G \times_R \operatorname{Spec} -, \mathbf{G}_{m,R} \times_R \operatorname{Spec} -)$$

takes an R-algebra S to the group

$$\mathrm{Hom}_{\mathsf{AffGrpSch_R}}(G \times_R \operatorname{Spec} S, \mathbf{G}_{m,R} \times_R \operatorname{Spec} S).$$

We haven't justified that this really is a functor. First, the group structure on this hom set is induced by the group structure on the $G \times_R \operatorname{Spec} S$-points of $\mathbf{G}_{m,R} \times_R \operatorname{Spec} S = \mathbf{G}_{m,S}$ (this equality is easily checked by the definition of the group-scheme structure of the base change in the remarks at the beginning of Section 1.2). Indeed, multiplying two group-object morphisms always results in a group-object morphism, since $\mathbf{G}_{m,S}$ is always commutative. The functor is given on morphisms by taking a map of R-algebras $S' \to S$ to the group homomorphism

$$\mathrm{Hom}_{\mathsf{GrpSch}_S}(G \times_R \operatorname{Spec} S, \mathbf{G}_{m,R} \times_R \operatorname{Spec} S) \to \mathrm{Hom}_{\mathsf{GrpSch}_{S'}}(G \times_R \operatorname{Spec} S', \mathbf{G}_{m,R} \times_R \operatorname{Spec} S')$$

given by applying the functor $- \times_S \operatorname{Spec} S'$. One needs to check that on these sets of morphisms, $- \times_S \operatorname{Spec} S'$ indeed takes S-group scheme homs to S'-group scheme homs and is a group homomorphism (the rest of the statement that this is an actual functor is obvious). Without loss of generality, we may assume $R = S$. One easy way to do both of these is to look at points: By the Yoneda lemma, it suffices to show that $f \times \operatorname{Spec} S'$ is a group homomorphism on points, when f is, and that on points it takes pointwise products to pointwise products. Both of these are obvious by the commutativity of the diagram

$$\begin{tikzcd}
G(T) \arrow[r, "f(T)"] \arrow[d] & \mathbf{G}_m(T) \arrow[d] \\
(G \times_S \operatorname{Spec} S')(T) \arrow[r, "(f \times S')(T)"] & \mathbf{G}_{m,S'}(T)
\end{tikzcd}$$

For all S'-schemes T. At least now we have verified (more or less) that the objects in the statement in the theorem are well-defined. It remains to show that for all R-algebras S, we have a natural-in-S isomorphism

$$\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, S) \cong \mathrm{Hom}_{\mathsf{HopfAlg}_S}(S[T, T^{-1}], A \otimes_R S).$$

First, we make the left hand side nicer by noticing that there is a natural isomorphism of S-algebras

$$A^\vee \otimes_R S \cong (A \otimes S)^\vee,$$

where the S-algebra structure of the right hand side comes from the natural finite flat S-Hopf algebra structure on $A \otimes S$ (the dual on the left hand side is over R, and on the right it is over S). We arrive at this isomorphism by starting with the natural extension-restriction adjunction

$$(A \otimes S)^\vee := \mathrm{Hom}_{\mathsf{Mod}_S}(A \otimes S, S) \cong \mathrm{Hom}_{\mathsf{Mod}_R}(A, S),$$

then (abusing the Noetherian hypothesis on R once again to commute localizations with homs and also see that A is locally free) observing that the natural map

$$\mathrm{Hom}_{\mathsf{Mod}_R}(A, R) \otimes_R S \to \mathrm{Hom}_{\mathsf{Mod}_R}(A, S)$$

localizes at each prime $\mathfrak{p}$ of R to an isomorphism and is therefore an isomorphism itself. Then one checks directly that the resulting bijection

$$A^\vee \otimes_R S \to (A \otimes S)^\vee,$$

which we know is given by $f \otimes s \mapsto [a \otimes s' \mapsto ss'f(a)]$ is a homomorphism of not only R-modules, but also S-algebras (using the definition of the algebra structure in terms of the Hopf algebra structure of A). As a result of the fact that the tensor product over R is the coproduct in the category of R-algebras, we have a natural isomorphism

$$\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee \otimes_R S, S) \cong \mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, S) \times \mathrm{Hom}_{\mathsf{Alg}_R}(S, S),$$

and on the right hand side the homs which are furthermore S-algebra homomorphisms are identified with those where the second coordinate is the identity morphism. Hence, we have natural isomorphisms

$$\mathrm{Hom}_{\mathsf{Alg}_S}((A \otimes_R S)^\vee, S) \cong \mathrm{Hom}_{\mathsf{Alg}_S}(A^\vee \otimes_R S, S) \cong \mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, S)$$

and therefore the statement we are looking for is equivalent to

$$\mathrm{Hom}_{\mathsf{Alg}_S}((A \otimes_R S)^\vee, S) \cong \mathrm{Hom}_{\mathsf{HopfAlg}_S}(S[T, T^{-1}], A \otimes_R S).$$

The key point is that the only Hopf algebra appearing here is $A \otimes_R S$, so we can assume that $S = R$ for now and think later about why the isomorphism is natural. The right hand side is naturally identified with the set of units $a \in A^\times$ such that the R-algebra homomorphism $R[T, T^{-1}] \to A$ given by $T \mapsto a$ is moreover a Hopf algebra morphism. This condition is equivalent to the commutativity of the diagram

$$\begin{tikzcd}
\mathbf{G}_m \times \mathbf{G}_m \arrow[r] \arrow[d] & G \times G \arrow[d] \\
\mathbf{G}_m & G \arrow[l]
\end{tikzcd}$$

and thus also to the commutativity of

$$\begin{tikzcd}
R[T_1, T_1^{-1}, T_2, T_2^{-1}] \arrow[r, "T_1 \mapsto a \otimes 1, T_2 \mapsto 1 \otimes a"] & A \otimes A \\
R[T, T^{-1}] \arrow[u, "T \mapsto T_1 T_2"] \arrow[r, "T \mapsto a"] & A \arrow[u, "c"']
\end{tikzcd}$$

where $c : A \to A \otimes A$ is the comultiplication morphism of A, which means that the right hand side is identified (so far only as a set) with

$$\{a \in A^\times : c(a) = a \otimes a\}.$$

On the left hand side, the approach is to view $\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, R)$ as a subset of $\mathrm{Hom}_{\mathsf{Mod}_R}(A^\vee, R) = A^{\vee\vee}$, which is canonically identified with A. In particular, $\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, R)$ is canonically identified with the set of all $a \in A$ such that the map $A^\vee \to R$ given by $f \mapsto f(a)$ is a ring homomorphism. So this means remembering what the ring structure on $A^\vee$ is from Theorem 1.10. The multiplication is obtained by dualizing the comultiplication on A, which means that for $f, g \in A^\vee$,

$$(f \cdot g)(a) = (f \otimes g)(c(a))$$

($f \otimes g$ defined via the fact that $\otimes_R$ is the coproduct in Alg_R). So $f \mapsto f(a)$ is multiplicative if and only if

$$f(a)g(a) = (f \otimes g)(c(a))$$

for all $f, g \in A^\vee$. Note that this is definitely true if $c(a) = a \otimes a$. In fact, the converse is also true, since f and g are allowed to range over all of $A^\vee$ and thus the $f \otimes g$ span all of $(A \otimes A)^\vee$; if $c(a) \neq a \otimes a$, then there exist $f, g \in A^\vee$ such that $(f \otimes g)(c(a)) \neq a \otimes a$

(this is the injectivity part of the statement that the evaluation map $A \otimes A \to (A \otimes A)^{\vee\vee}$ is bijective). It remains to check what $f \mapsto f(a)$ preserving the identity element means in terms of a. From Theorem 1.10, we recall that the identity element in $A^\vee$ is the image of 1 under the morphism $R \to A^\vee$ which is the dual of the counit map $\epsilon : A \to R$, i.e. the identity element is precisely $\epsilon \in A^\vee$. If a already satisfied $c(a) = a \otimes a$, the requirement that $\epsilon(a) = 1$ is equivalent to $ai(a) = 1$, because of the commutativity of

$$\begin{tikzcd} G \arrow[r, "\Delta"] \arrow[d] & G \times G \arrow[r, "\mathrm{id} \times i"] & G \times G \arrow[d, "m"] \\ \operatorname{Spec} R \arrow[rr, "\epsilon"] & & G \end{tikzcd}$$

and the fact that $\Delta : G \to G \times G$ is dual to the multiplication map $A \otimes A \to A$. Thus, $\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, R)$ is identified with the set of all $a \in A^\times$ such that $c(a) = a \otimes a$ and $\epsilon(a) = ai(a) = 1$. In fact, by the commutativity of

$$\begin{tikzcd} G \times_R \operatorname{Spec} R \arrow[r, "\mathrm{id} \times \epsilon"] \arrow[dr, "\sim"] & G \times_R G \arrow[d] \\ & G \end{tikzcd},$$

if $a \in A^\times$ such that $c(a) = a \otimes a$, then $a\epsilon(a) = a$, and thus $\epsilon(a) = 1$, which means that $\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, R)$ is identified with the same subset of $A^\times$ as the right hand side of Cartier duality is. The main content of the theorem is already proved, but it still remains to check two things:

(1) These identifications are isomorphisms of groups.
(2) The resulting map produces a natural isomorphism of functors.

For (1), we need to show that the map $\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, R) \to A$ given by $\mathrm{ev}_a \mapsto a$, and the map $\mathrm{ev}_T : \mathrm{Hom}_{\mathsf{HopfAlg}_R}(R[T, T^{-1}], A) \to A$ are both multiplicative. For the first one, suppose that $a, b \in A^\times$ such that $c(a) = a \otimes a$ and $c(b) = b \otimes b$. Then recall that the group structure on $\mathrm{Hom}_{\mathsf{HopfAlg}_R}(R[T, T^{-1}], A)$ comes from the group structure of $G^\vee(R)$, i.e. $\mathrm{ev}_a \cdot \mathrm{ev}_b$ is given by $(\mathrm{ev}_a \otimes \mathrm{ev}_b) \circ m^\vee$. In particular, for $f \in A^\vee$,

$$\begin{aligned} (\mathrm{ev}_a \cdot \mathrm{ev}_b)(f) &= ((\mathrm{ev}_a \otimes \mathrm{ev}_b))(f \circ m) \\ &= (f \circ m)(a \otimes b) \\ &= f(ab) \\ &= \mathrm{ev}_{ab}(f) \end{aligned}$$

where here $m : A \otimes A \to A$ stands for the ring multiplication map. For the second one, the idea is very similar. For $a, b \in A$ and $\phi \in R[T, T^{-1}]$, we have by definition of the group structure on $\mathrm{Hom}_{\mathsf{HopfAlg}_R}(R[T, T^{-1}], A)$ as a subgroup of $\mathbf{G}_m(G)$ that

$$(\mathrm{ev}_a \cdot \mathrm{ev}_b)(f) = (\mathrm{ev}_a \otimes \mathrm{ev}_b)(f(T_1 T_2)) = f(ab) = \mathrm{ev}_{ab}(f)$$

which completes the verification of (1). By replacing R with S and A with $A \otimes_R S$ everywhere above, we therefore have isomorphisms of groups

$$\mathrm{Hom}_{\mathsf{Alg}_S}((A \otimes_R S)^\vee, S) \cong \{a \in (A \otimes S)^\times : c(a) = a \otimes a\} \cong \mathrm{Hom}_{\mathsf{HopfAlg}_S}(S[T, T^{-1}], A \otimes_R S)$$

and to finish off (2) we just need to check that these isomorphisms are natural in S. But this is obvious from the proofs, since the diagrams

$$\begin{tikzcd}
\mathrm{Hom}_{\mathsf{HopfAlg}_S}(S[T,T^{-1}], A \otimes_R S) \arrow[r, "\mathrm{ev}_T"] & A \otimes S \\
\mathrm{Hom}_{\mathsf{HopfAlg}_R}(R[T,T'], A) \arrow[r, "\mathrm{ev}_T"] \arrow[u] & A \arrow[u]
\end{tikzcd}$$

and

$$\begin{tikzcd}
\mathrm{Hom}_{\mathsf{Alg}_S}((A \otimes_R S)^\vee, S) \arrow[r, "\mathrm{ev}_{x \mapsto x}"] & A \otimes S \\
\mathrm{Hom}_{\mathsf{Alg}_R}(A^\vee, R) \arrow[r, "\mathrm{ev}_{a \mapsto a}"] \arrow[u] & A \arrow[u]
\end{tikzcd}$$

commute (one can replace R with any S' with a ring map to S and A with $A \otimes_R S'$). □

1.4. **Commutative group schemes are killed by their order.** Recall from classical group theory that any finite group is killed by its order. Taking a finite flat S-group scheme G of order n, one can ask whether the n-th power map

$$n : G \xrightarrow{\Delta} G^n \xrightarrow{m} G$$

is the identity (i.e. factors through the unit map $S \to G$). This is unknown in general, but was settled by Deligne in the commutative case by exploiting Cartier duality to great effect.

Theorem 1.12 (Deligne)**.** *Let G be a finite flat commutative affine group scheme of order n over a Noetherian ring R. Then G is killed by n.*

Proof. Since a map is zero locally if and only if it is zero globally, we may localize and assume that R is a Noetherian local ring. In particular, the localization of G at a prime $\mathfrak{p}$ of R is just the base change $G \times_R \mathrm{Spec}\, R_{\mathfrak{p}}$, which has a natural group scheme structure, induced from that on G; and essentially by definition the m-th power map $[m]_{\mathfrak{p}} : G \times_R \mathrm{Spec}\, R_{\mathfrak{p}} \to G \times_R \mathrm{Spec}\, R_{\mathfrak{p}}$ is the one induced by $[m]$.

Deligne's trick is a familiar one: it is to consider the map $G \to G$ induced by translating by some R-point of G, and to show that this map is trivial once applied $n = |G|$ times. The key analogy is to the proof in finite group theory where you take the product of all elements of G and use the fact that multiplying by an n-th power just permutes the factors. Since the S-points of G don't always have the same size, this will not work in our case. Instead, we will consider the identity map $G \to G$ (dual to the identity $A \to A$), and instead of multiplying everything together, we will consider its *norm* as defined below. The key point is that this norm doesn't change when you postcompose by multiplication by any point of G.

Now recall that $G(R)$ is naturally a subset of $\mathrm{Hom}_{\mathsf{Mod}_R}(A, R) = A^\vee$, which we have given a ring structure in Theorem 1.10. And since (by the local assumption) A is free over R, $G(G)$ is naturally a subset of $\mathrm{Hom}_{\mathsf{Mod}_R}(A, A) = A^\vee \otimes A$, which naturally has the structure of a finite free $A^\vee$-algebra. So there is a map

$$N : A^\vee \otimes A \to A^\vee$$

given by taking x to the determinant of multiplication by x. This map clearly respects multiplication (a general fact about the norm map for an arbitrary finite free algebra over a ring). The central technical observation that must be made to justify Deligne's argument is that N takes $G(G)$ to $G(R)$. Luckily this is straightforward using the definition of the ring structure of $A^\vee$ from Theorem 1.10. An arbitrary element of $\mathrm{Hom}_{\mathsf{Mod}_R}(A, A)$ is given by an R-linear combination of maps of the form $a \cdot f$, where $a \in A$ and $f \in A^\vee$. But this follows from the characterization of $G(S)$ as a subset of $A^\vee \otimes S$ (apply the proof of Theorem 1.11 to $G^\vee$), namely the set of all $f \in (A^\vee \otimes S)^\times$ such that $c(f) = f \otimes f$, where $c = c_{G^\vee \times_R \operatorname{Spec} S} : A^\vee \otimes S \to (A^\vee \otimes S)^{\otimes 2}$ is the comultiplication for $G^\vee \times_R S = (G \times_R S)^\vee$. Since N is multiplicative, it takes units to units. So we just need to check that for $f \in G(G)$, we have $c_{G^\vee}(N(f)) = N(f) \otimes N(f)$. The fact that $c_{G^\vee} : A^\vee \to A^\vee \otimes A^\vee$ is a ring homomorphism and $c_{G^\vee \times_R A}$ is induced by $c_{G^\vee}$ by tensoring up by A means that the diagram

$$\begin{tikzcd}
A^\vee \otimes A \arrow[r, "c_{G^\vee} \otimes \mathrm{id}_A"] \arrow[d, "N"] & (A^\vee \otimes A^\vee) \otimes A \arrow[r, phantom, "="] & (A^\vee \otimes A) \otimes (A^\vee \otimes A) \arrow[d, "N"] \\
A^\vee \arrow[rr, "c_{G^\vee}"] & & A^\vee \otimes A^\vee
\end{tikzcd}$$

commutes (purely a fact about finite free algebras, where $c_{G^\vee}$ could be replaced by an arbitrary ring homomorphism), and thus

$$c_{G^\vee}(N(f)) = N(c_{G^\vee}(f)) = N(f \otimes f) = N(f) \otimes N(f).$$

Here the first equality comes from the commutativity of the diagram above, and the second comes from the fact that $f \in G(G)$. The last one we haven't yet justified, but it can be checked either directly or in a slightly more abstract but really equivalent way by using the same fact from commutative algebra as above, applied to the diagram

$$\begin{tikzcd}
A^\vee \otimes A \arrow[r, "\mathrm{id}_{A^\vee \otimes A} \otimes 1_{A^\vee \otimes A}"] \arrow[d, "N"] & (A^\vee \otimes A) \otimes (A^\vee \otimes A) \arrow[d, "N"] \\
A^\vee \arrow[r, "\mathrm{id}_{A^\vee} \otimes 1_{A^\vee}"] & A^\vee \otimes A^\vee
\end{tikzcd}$$

(the upstairs horizontal map is equal to the induced map of the bottom one under tensoring by $A^\vee \otimes A$ via the isomorphism of the top-right corner with $A^\vee \otimes A^\vee \otimes A$), so that indeed

$$N(f \otimes f) = N(f \otimes 1)N(1 \otimes f) = (N(f) \otimes 1)(1 \otimes N(f)) = N(f) \otimes N(f)$$

as desired. So we have proved that the norm $N : A^\vee \otimes A \to A^\vee$ induces a map of the subsets $N : G(G) \to G(R)$.

Let $u \in G(R)$. It suffices to show that u^n is trivial in $G(R)$, since the same statement applied to $G \times_R \operatorname{Spec} S$ shows that the n-th power map kills $G(S)$ for all S and thus by Yoneda kills G. Consider the morphism $\tau : A \to A$ given by translation by u. This is an isomorphism of R-algebras because (using the axioms of a group object) it has an inverse given by translation by u. Postcomposition by τ provides an automorphism of $\mathrm{Hom}_{\mathsf{Mod}_R}(A, A)$, which translates to an automorphism of $A^\vee \otimes A$ which takes $f \otimes a$ to $f \otimes \tau(a)$. The fact that $\tau : A \to A$ is an automorphism means that this implies $N(x) = N(\tau(x))$ for all $x \in A^\vee \otimes A$. But for $x \in G(G)$, postcomposing by τ is the same thing as multiplication by $u \in G(R) \to G(G)$, and $N : G(G) \to G(R)$ is a group homomorphism, so we have

$$N(x) = N(\tau(x)) = N(u \cdot x) = N(u)N(x) = u^n N(x).$$

So as long as $x \in G(G)$ (such an x exists, since we can just take it to be the identity) we know that $N(x)$ is in $G(R)$ and is therefore invertible, and thus $u^n = 1$ in $G(R)$ as desired. □

Remark 1.13. I don't think it is necessary to actually prove that N restricts to a map $G(G) \to G(R)$. As long as we know that the inclusions $G(S) \to A^\vee \otimes S$ preserve multiplication (which we used anyway when we used the fact that $N : G(G) \to G(R)$ is a group homomorphism), we can still take $x = \mathrm{id}_G$ and justify the equality

$$N(x) = u^n N(x)$$

in the ring $A^\vee$, where we know that $N(x) \in (A^\vee)^\times$ and therefore u^n is the identity element of $A^\vee$, which we know (also from Theorem 1.10) is the identity element of $G(R)$.

Remark 1.14. The affineness assumption that we have been making here is not very serious. First, any finite scheme over an affine base is affine, since finite morphisms are affine. In the context of arithmetic, it is almost always the case that the base is affine (e.g. the group schemes we care about are the n-torsion points of an abelian variety over $\mathbf{Z}_p$). Even so, the theorems of this section (Cartier duality, Deligne's theorem) are still true without the affine hypothesis, and the proofs are essentially unchanged – one simply does the same arguments replacing A with the structure sheaf of G.

2. Examples

Example 2.1 ($\mathbf{G}_m$)**.** The *multiplicative group* $\mathbf{G}_m$, which we already used in Theorem 1.11, is an affine group scheme which can be defined via its functor of points

$$\mathbf{G}_{m,R}(S) = S^\times$$

for any R-algebra S. This is clearly representable (as a functor to Grp) by $R[T, T^{-1}]$, so as a scheme we have

$$\mathbf{G}_m = \mathrm{Spec}(R[T, T^{-1}])$$

and one checks that the comultiplication is given by $T \mapsto T_1 T_2$, coinverse by $T \mapsto T^{-1}$, and counit by $T \mapsto 1$.

Example 2.2 ($\mathbf{G}_a$)**.** The *additive group* $\mathbf{G}_a$ is an affine group scheme which can be defined via its functor of points

$$\mathbf{G}_{a,R}(S) = (S, +)$$

for any R-algebra S. This is clearly representable (as a functor to Grp) by $R[T]$, so as a scheme we have

$$\mathbf{G}_m = \mathrm{Spec}(R[T])$$

and one checks that the comultiplication is given by $T \mapsto T_1 + T_2$, coinverse by $T \mapsto -T$, and counit by $T \mapsto 0$.

Example 2.3 (Constant group scheme)**.** For any finite group G and ring R, we define the *constant group scheme*[3] G_R. As a scheme, G_R is a disjoint union of copies of $\mathrm{Spec}\, R$ indexed by the elements of G. The multiplication morphism on G is defined by applying the canonical isomorphism $(\mathrm{Spec}\, R) \times (\mathrm{Spec}\, R) \to \mathrm{Spec}\, R$ to get a map

$$(\mathrm{Spec}\, R)_g \times (\mathrm{Spec}\, R)_h \to (\mathrm{Spec}\, R)_{gh}$$

[3] Unless G is trivial, the functor of points of the constant group scheme is NOT the constant function to G; this is an easy mistake to make because of the name and because it is true on connected schemes. In fact, that constant functor is NOT representable, because it must take products to products.

for all $g, h \in G$ which patches together to give the desired map

$$\left(\bigsqcup_{g\in G}(\operatorname{Spec} R)_g\right) \times \left(\bigsqcup_{h\in G}(\operatorname{Spec} R)_h\right) = \bigsqcup_{g,h\in G}(\operatorname{Spec} R)_g \times (\operatorname{Spec} R)_h \to \bigsqcup_{\gamma\in G}(\operatorname{Spec} R)_\gamma.$$

The inverse morphism is just the isomorphism given on the components by the identity map $(\operatorname{Spec} R)_g \to (\operatorname{Spec} R)_{g^{-1}}$ and the identity morphism is the identity map $\operatorname{Spec} R \to (\operatorname{Spec} R)_e$. In terms of Hopf algebras,

$$G_R = \operatorname{Spec} \prod_G R,$$

which we think of as being the ring of functions $G \to R$. The comultiplication sends a map $f : G \to R$ to the map $c(f) : G \times G \to R$ taking (g_1, g_2) to $f(g_1g_2)$. In the language of the product ring, this means the comultiplication

$$\prod_{g\in G} R_g \to \left(\prod_{g\in G} R_g\right)^{\otimes 2}$$

is given by $1_g \mapsto \sum_{h\in G} 1_h \otimes 1_{h^{-1}g}$, the coinverse by $1_g \mapsto 1_{g^{-1}}$, and the counit given by killing all the coordinates other than the one corresponding to $g = 1_G$. By Lemma 1.4, it is automatic that these morphisms are compatible in the sense that they give a valid Hopf algebra structure on $\prod_G R$.

Another convenient way of writing this is by thinking of the 1_g's as a system of orthogonal idempotents for $\prod R_g$, and writing the Hopf algebra as

$$R[\{X_g\}_{g\in G}]/(X_g^2 - X_g, X_gX_h)_{g\neq h}.$$

The functor of points of G_R takes a scheme S to

$$\operatorname{Hom}(S, \sqcup_{g\in G} \operatorname{Spec} R).$$

when S is connected, this is clearly isomorphic to G as a group. In general, one can think of this as the set of locally constant functions $S \to G$. If S is a disjoint union of connected components, then $G_R(S)$ is the product, indexed over those components, of copies of G.

Note that in the case of constant group schemes, commutative or not, Theorem 1.12 is obvious from the theorem for abstract groups.

Example 2.4 (Diagonal group schemes)**.** Let R be a ring and Γ a finite abelian group. The corresponding *diagonal group scheme* is defined as the Cartier dual of Γ_R, i.e. with functor of points

$$D_R^\Gamma(S) = \operatorname{Hom}_{\mathsf{Grp}}(\Gamma, S^\times).$$

This is representable by Theorem 1.10 and Theorem 1.11, and is indeed the Cartier dual of Γ_R, because of the isomorphism of functors $\mathsf{Alg}_R \to \mathsf{Grp}$

$$\operatorname{Hom}_{\mathsf{Grp}}(\Gamma, -^\times) \cong \operatorname{Hom}_{\mathsf{GrpSch}_-}(\Gamma_-, \mathbf{G}_{m,-}).$$

The point of this isomorphism is that for any R-algebra S, the subset

$$\operatorname{Hom}_{\mathsf{GrpSch}_S}(\Gamma_S, \mathbf{G}_{m,S}) \subset \operatorname{Hom}_{\mathsf{Sch}_S}(\Gamma_S, \mathbf{G}_{m,S}) = \operatorname{Hom}_{\mathsf{Sch}_S}(\sqcup_G \operatorname{Spec} S, \mathbf{G}_{m,S}) = \prod_{g\in G} S^\times$$

is canonically identified with

$$\{(s_g)_{g\in G} \in \prod_{g\in G} S^\times : s_{gh} = s_g s_h\}$$

(this follows from the definition of a group object morphism). Note that commutativity of Γ is necessary in order to ensure commutativity of Γ_R as a group scheme and justify the use of Cartier duality Theorem 1.11 as well as the representability of the Cartier dual Theorem 1.10. In terms of Hopf algebra, this provides us with the scheme structure

$$D_R^\Gamma = \mathrm{Spec}(R[\Gamma])$$

with comultiplication $R[\Gamma] \to R[\Gamma] \otimes R[\Gamma]$ given by

$$\gamma \mapsto \gamma \otimes \gamma$$

since the product of two points $f_1, f_2 \in \mathrm{Hom}_{\mathsf{Grp}}(\Gamma, S^\times)$ is the composition

$$R[\Gamma] \overset{c}{\to} R[\Gamma \times \Gamma] = R[\Gamma] \otimes R[\Gamma] \overset{f_1 \times f_2}{\to} S$$

so the diagonal comultiplication indeed gets us the pointwise multiplication group structure on $\mathrm{Hom}_{\mathsf{Grp}}(\Gamma, S^\times)$. The coinverse $R[\Gamma] \to R[\Gamma]$ is just given by $\gamma \mapsto \gamma^{-1}$, and the counit $R[\Gamma] \to R$ sends $\gamma \mapsto 1$. Another way to write this is as the Hopf algebra

$$R[\{X_g\}_{g\in G}]/(X_g X_h - X_{gh})_{g,h\in\Gamma}.$$

with comultiplication $X_g \mapsto X_g \otimes X_g$.

Example 2.5 (Roots of unity)**.** Let R be a ring and $n \geq 1$. Define $\mu_{n,R}$ to be the kernel of $[n] : \mathbf{G}_{m,R} \to \mathbf{G}_{m,R}$. From our definitions in Section 1.2, this means that $\mu_{n,R}(S)$ is the group of n-th roots of unity in S, and in terms of Hopf algebras it is given by

$$R[X]/(X^n - 1)$$

with Hopf algebra structure induced from that of $\mathbf{G}_{m,R}$ (N.B. there is no need to include X^{-1} once we have quotiented by $X^n - 1$).

Example 2.6. (α_p) Let R be a ring of characteristic p. Then we can define a multiplicative p-th power map $[p]_m : \mathbf{G}_{a,R}$ via the Hopf algebra map $R[T] \to R[T]$ given by $T \mapsto T^p$. In particular, for any R-algebra S, the kernel of the p-th power map $S \to S$ (an additive group homomorphism) is a well-defined additive subgroup of S, and thus we have a well-defined subgroup scheme $\alpha_{p,R}$ of $\mathbf{G}_{a,R}$ given by the kernel. The corresponding Hopf algebra is $R[T]/(T^p)$. In particular, it is isomorphic as a scheme to $\mu_{p,R}$, but they are not isomorphic as group schemes (this we will see in the following subsection).

These examples are related to each other in various ways. For instance, from the definition we already know that a constant group scheme is the Cartier dual of the corresponding diagonalizable one. Specializing to a cyclic group of order n, there is another easy connection, this time with the n-th roots of unity.

Lemma 2.7. *Let R be a ring. Then $D_R^{\mathbf{Z}/n\mathbf{Z}} \cong \mu_{n,R}$ as R-group schemes. In other words, $(\mathbf{Z}/n\mathbf{Z})_R$ and $\mu_{n,R}$ are Cartier duals.*

First proof. One way is to exhibit a natural isomorphism between the respective functors of points (this suffices by Lemma 1.1 applied to the category of affine schemes). For an R-algebra S, we have

$$D_R^{\mathbf{Z}/n\mathbf{Z}}(S) = \mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, S^\times) \cong \{x \in S^\times : x^n = 1\} = \mu_{n,R}(S)$$

where the isomorphism is given by a choice of where to send a generator of $\mathbf{Z}/n\mathbf{Z}$. We need to check that this isomorphism is a natural isomorphism of functors, i.e. that for any map of R-algebras $S \to S'$, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathsf{Grp}}(\mathbf{Z}/n\mathbf{Z}, S^\times) \arrow[r, "\mathrm{ev}_1"] \arrow[d] & \{x \in S^\times : x^n = 1\} \arrow[d] \\
\mathrm{Hom}_{\mathsf{Grp}}(\mathbf{Z}/n\mathbf{Z}, S'^\times) \arrow[r, "\mathrm{ev}_1"] & \{x \in S'^\times : x^n = 1\}
\end{tikzcd}$$

commutes. This is clear from the definitions of the vertical maps. □

Alternative proof. By Cartier duality, the S-points of the dual of $\mu_{n,R}$ are in bijection with

$$\mathrm{Hom}_{\mathsf{GrpSch}_S}(\mu_{n,S}, \mathbf{G}_{m,S})$$

which is the set of S-Hopf algebra homomorphisms from $S[T, T^{-1}]$ to $S[T]/(T^n - 1)$. Such a homomorphism is determined by a choice of polynomial $p(T) \in S[T]/(T^n - 1)$, subject to the constraint that $p(T_1T_2) = p(T_1)p(T_2)$ in $S[T_1, T_2]/(T_i^n - 1)$. Note that this automatically enforces the condition that $p(T)$ is invertible (as $p(1) = 1$), and thus we have no problems defining the image of T^{-1}. Such a p has a unique representative in $S[T]$ of the form $\sum_{i=0}^{n-1} a_iT^i$. The condition $p(T_1)p(T_2) = p(T_1T_2)$ in $S[T_1, T_2]/(T_i^n - 1)$ is equivalent to $a_ia_j = 0$ for $i \neq j$ and $a_i^2 = a_i$, so the a_i's are a system of n orthogonal idempotents for S. From this one can explicitly deduce that there is a natural isomorphism of functors with $(\mathbf{Z}/n\mathbf{Z})_R$. □

Under the hood, both proofs of Lemma 2.7 are making crucial use of the functorial isomorphism $D_R^G(S) = \mathcal{H}om(G, S^\times)$ (even the alternative proof, which omits some details at the end which should work out essentially to this).

The dual group schemes G_R and D_R^G are both finite flat of order $|G|$. The group scheme $\alpha_{p,R}$ has order p, and $\mu_{n,R}$ has order n.

From the duality between $(\mathbf{Z}/n\mathbf{Z})_R$ and $\mu_{n,R}$, we can ask whether $(\mathbf{Z}/n\mathbf{Z})_R$ is self-dual, i.e. if $(\mathbf{Z}/n\mathbf{Z})_R \cong \mu_{n,R}$ as R-group schemes. This is easy to answer when R is a field, but I do not know the answer in general.

Lemma 2.8. *Let k be a field with characteristic not dividing n. Then $(\mathbf{Z}/n\mathbf{Z})_k$ is self-dual if and only if k contains n distinct n-th roots of unity.*

Proof. Suppose that k does not contain n distinct n-th roots of unity. Since $\operatorname{Spec} k$ is connected, we know that $|(\mathbf{Z}/n\mathbf{Z})_k(k)| = n$, but $|\mu_{n,k}(k)| \neq n$, and thus there cannot exist such an isomorphism, even as schemes. On the other hand, if k does contain n distinct roots of unity, then $T^n - 1$ splits into n distinct linear factors, and by the Chinese remainder theorem, we have an isomorphism of R-algebras

$$k[X]/(T^n - 1) \cong \prod_{i=1}^{n} k[X]/(T - \zeta_n^i) \cong \prod_{i=1}^{n} k$$

and it is easy to check directly that this isomorphism respects the Hopf algebra structures. □

Remark 2.9. Kevin Chang pointed out to us that Lemma 2.8 can generalize essentially in its current form to the case where R is a general ring, by looking carefully at the functor of points. But the assumption that the characteristic doesn't divide n is still crucial, of course. For example, if $R = \mathbf{Z}/4\mathbf{Z}$ and $n = 2$, there is no isomorphism, even of schemes, between μ_n and $\mathbf{Z}/n\mathbf{Z}$, since the second one has two connected components, and the first only has one (e.g. by looking at idempotents in the corresponding Hopf algebras). Of course, in Lemma 2.8, that assumption is unnecessary, since $X^p - 1 = (X-1)^p$ over characteristic p, so it holds vacuously given we want $X^p - 1$ to split completely.

Bringing the two finite flat group schemes $D_R^{\mathbf{Z}/p\mathbf{Z}}$, $(\mathbf{Z}/p\mathbf{Z})_R$, $\mu_{p,R}$ into contact with $\alpha_{p,R}$ brings us into the territory of finite flat group schemes of order p.

2.1. **Group schemes of prime order.** Let $p > 0$ be a rational prime, and R a ring. We have come up with four ways to construct a group scheme of order p over R:

(1) The constant group scheme $(\mathbf{Z}/p\mathbf{Z})_R$
(2) The diagonal group scheme $D_R^{\mathbf{Z}/p\mathbf{Z}}$
(3) The roots of unity $\mu_{p,R}$
(4) If R has characteristic p, $\alpha_{p,R}$.

Indeed, if we ask that our group scheme has order p, these are the only examples we can extract from what we have constructed so far (note that they are all commutative). We know (Lemma 2.7) that (2) and (3) are isomorphic and equal to the Cartier dual of (1). It is possible that all of these are the same group scheme, i.e. that $(\mathbf{Z}/p\mathbf{Z})_R$ is self-dual, which we know is equivalent to R containing a primitive n-th root of unity when R is a field by Lemma 2.8. What about (4)? First, we study the Cartier dual $\alpha_{p,R}^\vee$.

Lemma 2.10. *Let R be an arbitrary ring of characteristic p. The finite flat group scheme $\alpha_{p,R}$ is self-dual.*

Proof. This is the same method as the alternative proof to Lemma 2.7. By Cartier duality Theorem 1.11, we have

$$\mathrm{Hom}_{\mathsf{GrpSch}_S}(\alpha_{p,S}, \mathbf{G}_{m,S}) \cong \alpha_{p,R}^\vee(S).$$

So we just need to examine the functor on the left. We have

$$\mathrm{Hom}_{\mathsf{GrpSch}_S}(\alpha_{p,S}, \mathbf{G}_{m,S}) = \mathrm{Hom}_{\mathsf{HopfAlg}_S}(S[T, T^{-1}], S[T]/(T^p)).$$

Such an algebra homomorphism is determined by the image of T, and the condition that it respects the Hopf algebra structure is equivalent to $\phi(X+Y) = \phi(X)\phi(Y)$ where ϕ is the image of T. Note that once ϕ satisfies this, it is automatically invertible in $S[T]/(T^p)$ [because we shall see explicitly that $\phi(0)$ must be 1] so the image of T^{-1} is well-defined. The element $\phi \in S[T]/(T^p)$ has a canonical representative

$$\phi = \sum_{i=0}^{p-1} a_i T^i,$$

and the condition $\phi(X+Y) = \phi(X)\phi(Y)$, by looking at individual terms, forces $a_0 = 1$,

$$a_i = \frac{a_1^i}{i!}$$

for $1 \leq i \leq p-1$, and $a_1^p = 0$. Conversely, any such polynomial, which is really just $\exp(a_1 T)$ for a choice of $a_1 \in S$ such that $a_1^p = 0$, satisfies the desired property. As a result, we have a natural isomorphism

$$\mathrm{Hom}_{\mathsf{GrpSchs}}(\alpha_{p,S}, \mathbf{G}_{m,S}) \to \alpha_{p,R}(S)$$

taking the morphism corresponding to the Hopf algebra morphism $T \mapsto \exp(a_1 T)$ to $a_1 \in \alpha_{p,R}(S)$. □

Does $\alpha_{p,R}$ count for an additional order-p R-group scheme other than $\mu_{p,R}$ and its Cartier dual $(\mathbf{Z}/p\mathbf{Z})_R$? By Lemma 2.8 this is certainly true if R is a field not containing a primitive n-th root of unity. In fact, it is true for any field of characteristic p.

Lemma 2.11. *Let k be a field of characteristic p. Then $\alpha_{p,k}$ is not isomorphic to $(\mathbf{Z}/p\mathbf{Z})_k$ or to $\mu_{p,k}$.*

Proof. The key observation is that $\alpha_{p,k}$ is not reduced, and therefore not étale. So both it and its Cartier dual (since it is self-dual by Lemma 2.10) are not étale. On the other hand, $(\mathbf{Z}/p\mathbf{Z})$ is as a scheme a union of finitely many copies of $\operatorname{Spec} k$, and therefore is étale. So since its Cartier dual is $\mu_{p,k}$ by Lemma 2.7, neither can be isomorphic to $\alpha_{p,k}$. □

Remark 2.12. The proof of Lemma 2.11 goes through without change over an arbitrary ring.

The result of our work so far is the following:

Proposition 2.13. *Let k be an algebraically closed field and p a rational prime. If k has characteristic zero or positive characteristic not equal to p, then there is at least one finite flat group scheme of order p over k, namely $(\mathbf{Z}/p\mathbf{Z})_k$, which we showed is isomorphic to $\mu_{p,k}$ and $D_k^{\mathbf{Z}/p\mathbf{Z}}$. If k has characteristic p, then there are at least three, namely $\mu_{p,k} \cong D_k^{\mathbf{Z}/p\mathbf{Z}}$, $(\mathbf{Z}/p\mathbf{Z})_k$ and $\alpha_{p,k}$.*

Proof. The only thing we haven't checked is that when k has characteristic p, $\mu_{p,k}$ is not isomorphic to $(\mathbf{Z}/p\mathbf{Z})_k$. But this is obvious: the second guy is étale and the first guy is super not reduced, because $X^p - 1 = (X-1)^p$ in $k[X]$. □

It turns out that (for k an algebraically closed field), these are the only finite flat group schemes of order p. But what about over an arbitrary ring? This was partially resolved by Oort–Tate (following up on unpublished work of Artin–Mazur), and we will discuss their result later. For now, we content ourselves with the description for $p = 2$.

Example 2.14 (Group schemes of order 2)**.** Let $G = \operatorname{Spec}(A)$ be a finite free group scheme of rank 2 over a Noetherian local ring R (e.g. the localization of a finite flat group scheme over a Noetherian ring). We begin with some generalities that might more sensibly belong in the section labelled "Generalities", but we put here because of how closely the chain of reasoning of the general classification matches this example. First, the composition

$$R \to A \xrightarrow{\epsilon} R$$

is an R-algebra homomorphism, and is therefore the identity (N.B. this already tells us the structure map $R \to A$ is injective). So the exact sequence of R-modules

$$0 \to I \to A \xrightarrow{\epsilon} R \to 0$$

splits, giving $A \cong R \oplus I$ as R-modules. Because of how the splitting was defined, this direct sum is an internal direct sum using the structure map $R \to A$. Also, the fact that A is free and R is local means that by Nakayama's lemma[4], I is also a free R-module of rank 1. In fact (though we won't use this), I can be generated over R by $\epsilon(e_1)e_2 - \epsilon(e_2)e_1$ where (e_1, e_2) is any choice of basis for A as a rank-2 free R-module. This is because $\epsilon(e_1), \epsilon(e_2)$ generate all of R. This splitting also gets us a decomposition

$$A \otimes A = (R \otimes R) \oplus (I \otimes R) \oplus (R \otimes I) \oplus (I \otimes I) = R \oplus (I \otimes 1) \oplus (1 \otimes I) \oplus (I \otimes)$$

where on the right we are talking about subsets of $A \otimes A$. The comultiplication map

$$m : A \to A \otimes A = R \oplus (I \otimes 1) \oplus (1 \otimes I) \oplus (I \otimes I)$$

has nice properties due to the fact that $(\epsilon \otimes \mathrm{id}) \circ m : A \to A$ is the identity map (since ϵ is the coidentity morphism), so for any $f \in I$, the element

$$m(f) - 1 \otimes f - f \otimes 1$$

is in the kernels of $\epsilon \otimes \mathrm{id}$ and $\mathrm{id} \otimes \epsilon$, and hence in $I \otimes A \cap A \otimes I = I \otimes I$. But in this case, the fact that I is free of rank one tells us even more, namely that

$$m(f) = 1 \otimes f + f \otimes 1 + bf \otimes f$$

for some $b \in R$ not depending on f. Since $A = R \otimes I$ where R is included via the structure map $R \to A$, the comultiplication on A is determined by the constant b (in particular, the comultiplication is R-linear and is the identity on R so we just need to define it on I). By Yoneda, the counit and coinverse morphisms are determined by the comultiplication and therefore by the choice of b. The only thing left is the ring structure of A. Since we have written $A = R \otimes I$ and shown that I is free of rank 1 with some generator $x \in I \subset A$, the ring structure on A depends only what the value of x^2 is. Since $\epsilon(x) = 0$, we know that $\epsilon(x^2) = 0$ as well, and thus

$$x^2 = ax$$

for some $a \in R$. So the Hopf algebra structure on A is completely determined by the two constants a and b. But not every choice of $a, b \in R$ results in a bona fide Hopf algebra structure, which is the question we need to answer next. The ring multiplication being defined by $x^2 = ax$ just means that as a ring, $A = R[T]/(T^2 - aT)$ (the isomorphism given by $T \mapsto x$). So in reality, we just need to make sure that the comultiplication $m : R[T]/(T^2 - aT) \to R[T_1, T_2]/(T_1^2 - aT_1, T_2^2 - aT_2)$ given by $m(T) = T_2 + T_2 + bT_1T_2$ is a well-defined ring homomorphism, and that on points it provides an actual group structure. In order for m to be a well-defined ring map, we just need the image of T^2 and the image of aT to coincide. The first is

$$T_1^2 + T_2^2 + b^2T_1^2T_2^2 + 2T_1T_2 + 2bT_1T_2^2 + 2bT_1^2T_2$$

and the second is

$$aT_1 + aT_2 + abT_1T_2$$

so after applying the equivalence relation in the obvious way, their difference is

$$(ab + 1)(ab + 2)T_1T_2 \in R[T_1, T_2]/(T_1^2 - aT_1, T_2^2 - aT_2)$$

which is zero if and only if

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

[4] Since I is a direct summand of the free R-module A, it is projective. The relevant consequence of Nakayama is that finitely-generated projective modules over a local ring are free.

in R. Here is an interesting observation: if $e_1 = -ab - 1$ and $e_2 = ab + 2$ then $e_1 e_2 = 0$ and $e_1 + e_2 = 1$ and therefore

$$e_1^2 - e_1 = -e_1 e_2 = 0$$

and similarly for e_2, which means e_1, e_2 is a system of orthogonal idempotents for R, and thus

$$R = Re_1 \times Re_2, \qquad \operatorname{Spec} R = \operatorname{Spec}(Re_1) \bigsqcup \operatorname{Spec}(Re_2).$$

Tate claims that this directly implies we can assume without loss of generality that either $ab = -1$ or -2, but I don't see it.

For an R-algebra S, the group of S-points of G is

$$G(S) = \{x \in S : x^2 = ax\}$$

where the candidate group structure is

$$x \cdot y := x + y + bxy.$$

Note that this is automatically associative and has an identity element, namely $0 \in S$, and in particular the counit morphism $\epsilon : R[T]/(T^2 - aT) \to R$ must be given by $T \mapsto 0$. So by the commutativity of the diagram

$$\begin{tikzcd}
G \arrow[r, "\Delta"] \arrow[dr] & G \times G \arrow[r, "\mathrm{id} \times i"] & G \times G \arrow[r, "m"] & G \\
& \operatorname{Spec} R \arrow[urr, "\epsilon"] & &
\end{tikzcd}$$

we have

$$T + r + sT + bT(r + sT) = 0$$

in $R[T]/(T^2 - aT)$, from which we may immediately conclude that $r = 0$ and $(1 + ab)s = -1$, and thus $1 + ab$ is a unit, and the identity $(1 + ab)(2 + ab) = 0$ is equivalent to $ab = -2$. So we see that every finite flat group scheme of order 2 over R is of the form $G_{a,b}$ for some $a, b \in R$.

Now suppose that $G_{a,b} \cong G_{a',b'}$. Then there is an isomorphism of R-algebras $R[T]/(T^2 - aT) \to R[T]/(T^2 - a'T)$. If it is given by $T \mapsto r + sT$ with inverse $T \mapsto r' + s'T$, then $ss' = 1$ and $r = -sr'$. In other words, s must be a unit. In order for this map of rings to be well-defined, we also need

$$(r + sT)^2 - a(r + sT) = 0$$

in $R[T]/(T^2 - a'T)$, which is equivalent to $r(r - a) = 0$ and $s(a's + 2r - a) = 0$. For this isomorphism of R-algebras to be a Hopf algebra homomorphism, it is necessary and sufficient to have

$$r + sT_1 + sT_2 + sb'T_1T_2 = 2r + sT_1 + sT_2 + b(r + sT_1)(r + sT_2)$$

in $A' \otimes A' = R[T_1, T_2]/(T_1^2 - a'T_1, T_2^2 - a'T_2)$. This is equivalent to $r(br + 1) = 0$, $bsr = 0$, and $s(bs - b') = 0$. So taken altogether, we see that $T \mapsto r + sT$ provides a well-defined isomorphism of R-Hopf algebras if and only if s is a unit, and

$$r(r - a) = 0 \tag{2.15}$$

$$s(a's + 2r - a) = 0 \tag{2.16}$$

$$r(br + 1) = 0 \tag{2.17}$$

$$bsr = 0 \tag{2.18}$$

$$s(bs - b') = 0. \tag{2.19}$$

Since s is a unit, the last one is equivalent to $b' = bs$, so the fourth becomes $br = 0$, and the third is $r = 0$, which simplifies everything to $a = a's$ and $b' = bs$ where s is a unit. So we have observed that $G_{a,b} \cong G_{a',b'}$ if and only if there is some unit $s \in R$ such that $a' = as^{-1}$ and $b' = bs$. As Professor Mazur explained to us in his office a few weeks B.Z.[5], this means that as R changes, the range of isomorphism classes of $G_{a,b}$'s changes. When R is a field of characteristic not equal to 2, there is only one possible $G_{a,b}$ up to isomorphism (which might as well be $(\mathbf{Z}/2\mathbf{Z})_R$). This doesn't contradict Lemma 2.8, because any field of characteristic not equal to 2 has a primitive 2-nd root of unity. When R is a field of characteristic 2, there are exactly three up to isomorphism, namely $G_{0,0}, G_{0,1}, G_{1,0}$ (which are α_2, μ_2, $\mathbf{Z}/2\mathbf{Z}$). When $R = \mathbf{Z}_2$, we see that there are exactly two, namely

$$G_{-2,1} = \mu_{2,\mathbf{Z}_2}, G_{1,-2} = (\mathbf{Z}/2\mathbf{Z})_{\mathbf{Z}_2}.$$

It is easy to check these isomorphisms by looking at points, or directly using Hopf algebras. But as you adjoin roots of 2 to $\mathbf{Z}_2$, you get more and more isomorphism classes of finite flat $\mathbf{Z}_2$-group schemes of order 2. For example, consider the totally tamely ramified extension $\mathbf{Q}_2(2^{1/e})/\mathbf{Q}_2$ with valuation ring $\mathbf{Z}_2[2^{1/e}]$. Over this ring, there are $e+1$ isomorphism classes of $G_{a,b}$'s. As might be guessed from the examples above, it is a general fact that $G_{a,b}$ and $G_{b,a}$ are Cartier duals, which is easy to check using Cartier duality Theorem 1.11, or by using the definition of the Cartier dual.

Remark 2.20. This example is the first time where we notice that the data of the order of our group scheme and the characteristic of the (residue) ring (in particular whether they are the same prime) are intimately related to the properties it exhibits. There are some very basic reasons for this, as we will see later as we continue to develop the theory. This theme continues to be present in the next example, where we will consider objects having to do with p-power torsion over characteristic p.

Remark 2.21. The basic strategy of using the augmentation ideal to determine the Hopf algebra structure is key in Oort-Tate's classification of group schemes of order p, though that result requires a few more technical observations to justify. In the example for $p = 2$, we were helped by the fact that I has rank one and therefore the comultiplication and multiplication have a very restricted form on I.

2.2. **Elliptic curves.** One main source of finite flat group schemes in arithmetic is as torsion groups of abelian varieties. In fact, for any abelian scheme A of relative dimension d over a Noetherian base S, then $A[n]$ is a finite flat commutative S-scheme of constant fiber rank n^{2d}. According to a mathoverflow post of B. Conrad, even just this requires serious results in algebraic geometry. When A is an elliptic curve E over a field k of characteristic p, this means $E[p^r]$ is a group scheme of order p^{2r}, and together they form a p-divisible group over k of height 2. When k is algebraically closed, there are only two possibilities for this p-divisible group, depending on whether E/k is supersingular (see [6, Theorem 2.9.3]). In this example, we will focus instead on writing down what the group $E[p]$ is as a group scheme, which of course also only depends on whether E is supersingular.

First, $E[p]$ cannot be étale, since it is killed by p and k has characteristic p (in particular, using the theory of Frobeniuseries [1, exposé $\mathrm{VII}_{\mathrm{A}}$ and $\mathrm{VII}_{\mathrm{B}}$], $[p] = VF$ cannot be an isomorphism, where $F : G \to G^{(p)}$ is the Frobenius and $V : G^{(p)} \to G$ is the Verschiebung, so F can't be an isomorphism, and $E[p]$ cannot be étale). Since k is perfect, $E[p] = E[p]^{\circ} \times E[p]^{\text{ét}}$

[5] B.Z.: Before Zoom

where $E[p]^\circ$ has order p or p^2. If E is ordinary, then $E[p](k)$ is nontrivial, and thus the étale part is of order exactly p. By the classification of group schemes of order p over an algebraically closed field, $E[p]^{\text{ét}} = (\mathbf{Z}/p\mathbf{Z})_k$. And the fact that E is self-dual as an abelian variety (plus the fact that taking kernels commutes with taking duals where the dual of the kernel is in the sense of Cartier duality) means that $E[p]$ is self-dual, and thus $E[p]^\circ$, which is connected of order p and thus is either $\alpha_{p,k}$ or $\mu_{p,k}$, must be $\mu_{p,k}$, and as a result

$$E[p] = \mu_{p,k} \times (\mathbf{Z}/p\mathbf{Z})_k.$$

When E is supersingular, we know that $E[p](k)$ is trivial, and thus $E[p]$ is a connected k-group scheme of order p^2. Again, it is self-dual, so it is a connected group scheme of order p^2 with connected dual, which is killed by p. By computing the Dieudonne module, we could find there is only one such possible group scheme. It fits into an exact sequence

$$0 \to \alpha_{p,k} \to E[p] \to \alpha_{p,k} \to 0,$$

which we could have noticed because $\alpha_{p,k}$ is the only (connected, connected) simple group scheme.

These results are already pretty interesting: The isomorphism class (and thus corresponding Dieudonne module) of $E[p]$ only depends on whether E is supersingular or ordinary. Explicit computations, which we were encouraged to do by stackexchange answers of M. Emerton, B. Conrad, and K. Buzzard, can still be done and are instructive. For instance, consider the supersingular elliptic curve

$$E : x^3 = y + y^2$$

over an algebraically closed field of characteristic 2. In homogenous coordinates, this is the curve in $\mathbf{P}^2 k$ given by

$$X^3 = YZ^2 + Y^2 Z.$$

From the convenient description of the chord-tangent process in characteristic 2 from Silverman's book, the 2-torsion points are precisely those $[x : y : z]$ which are equal to their negative, i.e.

$$[x : y : z] = [x : -y - z : z].$$

In particular, we must have $z = 0$, and therefore the only geometric point is the identity $[0 : 1 : 0]$ (after all, we did say it was supersingular...). To get an affine group scheme out of $E[2]$, we need to change coordinates to put $[0 : 1 : 0]$ in an affine patch. So we take the affine coordinates with the middle coordinate normalized to 1

$$x = \frac{X}{Y}, z = \frac{Z}{Y},$$

in which the map $P \mapsto -P$ is

$$(x, z) \mapsto [x : -1 - z : z] = \left(\frac{x}{-1 - z}, \frac{z}{-1 - z} \right)$$

(taking note that this doesn't really act on this affine patch unless we remove the line $z = 1$, but this is okay since we are only interested in what happens near $[0 : 1 : 0]$). As a result, the 2-torsion is defined by (inside this affine part of E) of

$$\frac{x}{-1 - z} = x, \qquad \frac{z}{-1 - z} = z,$$

so as a finite flat affine k-scheme, we have

$$\begin{aligned} E[2] &= \operatorname{Spec} k[x,z]/(x^3 - z^2 - z, xz, z^2) \\ &= \operatorname{Spec} k[x]/(x^4). \end{aligned}$$

This agrees with our general analysis: there is a single geometric point, but the non-reduced structure makes it so that this still has order 4 as a finite flat k-group scheme. What is the group structure? This is something we can read off the chord-tangent equations for the elliptic curve group law (maybe being careful that we are in characteristic 2 but also not worrying too much because we can trust the statements in Silverman). If one wants to write down the group scheme structure of $E[p]$ for general supersingular E over characteristic p, then this type of approach is still possible (since one has general equations for what supersingular elliptic curves look like), but it is probably more useful to just use Dieudonné theory to look at it as a particular self-extension of α_p.

2.3. **Lubin-Tate formal groups.** Let K be a finite extension of $\mathbf{Q}_p$. From the Lubin-Tate explicit approach to local class field theory, we are familiar with the one-dimensional formal group laws which we now recognize as being a group co-object structure on $\mathcal{O}_K[[X]]$ corresponding to a group object structure on $\mathrm{Spf}\mathcal{O}_K[[X]]$ (a group object in the category of formal $\operatorname{Spec} \mathcal{O}_K$-schemes). From Tate's paper on p-divisible groups, we learned that there is an equivalence of categories between the category of connected p-divisible groups over $\mathcal{O}_K$ and the category of p-divisible commutative formal groups over $\mathcal{O}_K$. So it makes sense to ask:

Question 2.22. *When is a given formal group over $\mathcal{O}_K$ p-divisible? Can you tell just by glancing at the defining power series?*

It turns out that J. Lubin has answered this question for 1-dimensional formal groups in a stackexchange post. The answer is that this kind of question is one of the things that becomes clear once one wields the power of the Weierstrass preparation theorem. I wonder whether one can iterate the Weierstrass preparation argument to prove a simple criterion in n dimensions, but it seems a little bit more complicated. It is still unclear to me whether the complications in n dimensions are superficial or make things significantly harder than in 1, since all my concrete experience is from Lubin–Tate theory.

Proposition 2.23. *A 1-dimensional formal group law over $\mathcal{O}_K$ is p-divisible if and only if it does not reduce mod $\mathfrak{m}_K$ to $X + Y$.*

Proof. Let $F \in \mathcal{O}_K[[X,Y]]$ be a formal group law. If $F \equiv X + Y \mod \mathfrak{m}_K$, then $[p] : \mathcal{O}_K[[X]] \to \mathcal{O}_K[[X]]$ sends X to $f(X) \equiv 0 \mod \mathfrak{m}_K$. This crucially uses the fact that the p involved here is the same as the residue characteristic of K. In this case, $[p]$ is clearly not an isogeny, since if $\mathcal{O}_K[[X]]$ was a direct sum of finitely many copies of the subring $\mathcal{O}_K$, then we could tensor by the $\mathcal{O}_K$-module $\mathcal{O}_K/\mathfrak{m}_K = k$ to get

$$k[[X]] = k \oplus \cdots \oplus k,$$

clearly a contradiction.

For the converse, let F be a formal group law whose reduction mod $\mathfrak{m}_K$ has more terms than just $X + Y$. Then $[p] : \mathcal{O}_K[[X]] \to \mathcal{O}_K[[X]]$ takes X to $f(X)$, where $f \in \mathcal{O}_K[[X]]$ has the important property that monomial terms has a unit (i.e. reducing to something nonzero mod $\mathfrak{m}_K$) coefficient.

Lubin's trick is as follows. $[p]$ embeds $\mathcal{O}_K[[X]]$ as the subring

$$\mathcal{O}_K[[f(X)]] \subset \mathcal{O}_K[[X]].$$

Renaming $f(X) = T$, this is the same as the embedding

$$\mathcal{O}_K[[T]] \to \mathcal{O}_K[[T]][[X]]/(f(X) - T).$$

Since f has some coefficient which is a unit in $\mathcal{O}_K$, we know that $f(X) - T \in \mathcal{O}_K[[T]][[X]]$ has some coefficient which is a unit in $\mathcal{O}_K[[T]]$. That ring satisfies the conditions of the Weierstrass preparation theorem, so by that theorem, we see that

$$f(X) - T = gu,$$

where $g \in \mathcal{O}_K[[T]][X]$ is a monic polynomial, and $u \in \mathcal{O}_K[[T]][[X]]^\times$. As a result, we have a further isomorphism

$$\mathcal{O}_K[[T]] \to \mathcal{O}_K[[T]][[X]]/(f(X) - T) \cong \mathcal{O}_K[[T]][[X]]/(g),$$

where the composite map still sends $T \mapsto T$. But since g is a polynomial, this is automatically finite free. □

3. The category of affine group schemes

In this section, we develop properties about affine group schemes that let us treat them as usual groups. In particular, we'll see that the category of S-affine group schemes is abelian.

3.1. **Sub-affine group schemes.**

Definition 3.1. Let S be a ring and $G = \operatorname{Spec} A$ an S-affine group scheme. Then, a **sub-affine group scheme** $H = \operatorname{Spec}(A/I) \subset G$ is simply a closed subscheme of G compatible with the group operations on G (for instance, the multiplication $A \to A \otimes_S A$ should descend to $A/I \to A/I \otimes_S A/I$ via the canonical projection from $A \to A/I$). Such ideals I are called **Hopf ideals**.

Remark 3.2. From the definition, it's clear that $I \subset A$ is a Hopf ideal iff $\mu(I) \subset \ker(A \otimes_S A \to A/I \otimes_S A/I)$, $\varepsilon(I) = 0$, and $\iota(I) \subset I$.

Remark 3.3. Every S-affine group scheme G has at least two sub-affine group schemes: itself (corresponding to the zero Hopf ideal) and the zero group scheme over S (whose corresponding Hopf ideal is the kernel of ε).

We can also take points of a sub-affine group scheme.

Remark 3.4. Let $H = \operatorname{Spec}(A/I)$ be a sub-affine group scheme of $G = \operatorname{Spec} A$ over S. Then, if R is any S-algebra, the R-points of H are

$$H(R) = \operatorname{Hom}_{S\text{-alg}}(A/I, R) = f \in G(R) : f|_I = 0.$$

To illustrate this, consider the following example.

Example 3.5. As a concrete example, suppose S has characteristic p. Then, $\alpha_{p^r,S}(R)$ is a subgroup of $\mathbb{G}_{a,S}(R)$, given by $\{x \in R^+ : x^{p^r} = 0\}$. Indeed, by definition, $\alpha_{p^r,S}$ is the sub-affine group scheme of $\mathbb{G}_{a,S}$ corresponding to the Hopf ideal generated by $x^{p^r} \in S[t]$.

In fact, if $S = k$ is moreover a field, then $\mathbb{G}_{a,S}$ is "simple," if the characteristic of k is 0, and $\alpha_{p,S}$ is "simple," if the characteristic is p. Here, simple means that there are no proper, non-zero sub-affine group schemes.

Indeed, first note that $k[t]$ is a PID, so any ideal is of the form (f), where $f = \sum_{i=0}^{n} a_i x^t$. Suppose f is not t. Then, one can show easily (by the definition of a Hopf ideal and using the fact that the gcd of $\binom{i}{j}$ over all $1 \leq j \leq i-1$ is equal to p if i is a power of $\mathrm{char}(k)$ and $\mathrm{char}(k)$ is prime) that (f) is a Hopf ideal iff $\mathrm{char}(k)$ is prime and $a_i = 0$ for i not a power of this prime.

Then, it follows that if $\mathrm{char}\, k = 0$, the only proper sub-affine group scheme of $\mathbb{G}_{a,k}$ has corresponding Hopf ideal $\ker \varepsilon$, which is the zero group scheme over k. If $\mathrm{char}(k) = p$, then similarly it follows that any proper sub-affine group scheme of $\alpha_{p,k}$ is just the zero group scheme over k.

3.2. **Morphisms of affine group schemes.**

Definition 3.6. A **morphism** $\Phi : G = \mathrm{Spec}(B) \to H = \mathrm{Spec}(A)$ of S-affine group schemes is a morphism of schemes that is also compatible with the group operations. In the language of S-algebras, it corresponds to a homomorphism $\phi : B \to A$ satisfying $\mu_A \circ \phi = (\phi \otimes \phi) \circ \mu_B$, $\varepsilon_A \circ \phi = \varepsilon_B$, and $\iota_A \circ \phi = \phi \circ \iota_B$.

We will denote by $\mathrm{Hom}(G, H)$ the set of morphisms $G \to H$ and by $\mathrm{AffGrpSch}_S$ the category of S-affine group schemes.

We recall the following general categorical fact.

Lemma 3.7. *Any functor between categories induces a functor on the corresponding categories of group objects.*

Corollary 3.8. *Let R be an S-algebra. Then, any morphism $\Phi : G \to H$ of S-affine group schemes induces a group homomorphism $\Phi_R : G(R) \to H(R)$, given by pre-composition by phi, where ϕ is the corresponding S-algebra homomorphism. Indeed, the previous lemma tells us that $G \to G(R)$ gives a functor* $\mathrm{AffGrpSch}_S \to \mathrm{Ab}$.

Remark 3.9. Note that the category $\mathrm{AffGrpSch}_S$ has a zero object. Indeed, for any $G = \mathrm{Spec}\, A \in \mathrm{AffGrpSch}_S$, the maps to and from the zero group scheme 0_S are induced by S-algebra maps $S \to A$ and $A \to S$ (the structure map and counit).

We can define the product of S-affine group schemes in a straightforward way.

Definition 3.10. The **product** of S-affine group schemes $G = \mathrm{Spec}\, A$ and $G' = \mathrm{Spec}\, A'$ has underlying schematic structure given by the fiber product of schemes, and the comultiplication, counit, and antipode given by tensoring those of G and G'.

Remark 3.11. One can check that by endowing $A \otimes_S A$ with the structure of a Hopf algebra as above, the various Hopf algebra operations are not just S-algebra homomorphisms, but actually S-Hopf algebra homomorphisms.

As a consequence, S-affine group schemes are in fact group objects in the category of S-affine group schemes.

We can now endow $\mathrm{Hom}(G, H)$ with an additive structure.

Definition 3.12. Suppose $G, H \in \mathrm{AffGrpSch}_S$ and $\Phi, \Psi \in \mathrm{Hom}(G, H)$. Then, define the **sum of morphisms**

$$\Phi + \Psi : G \to G \times_S G \to H \times_S H \to H$$

as the composition of morphisms of S-affine group schemes.

Moreover, $\mathrm{Hom}(G,H)$ has the structure of an abelian group, because the zero element is given by the composition $G \to 0_S \to H$ and inverses are given by pre-composition by $iota_G$. Then, by functoriality, we get a group homomorphism $\mathrm{Hom}(G,H) \to \mathrm{Hom}(G(R), H(R))$ by sending Φ to Φ_R.

Example 3.13. An important application of this is the morphism $[n] : G \to G$, where G is an S-affine group scheme and n is some integer. In particular, we define $[n] \in \mathrm{Hom}(G,G)$ to be $n\mathrm{id}_G$. In particular, note that on the level of points, $[n]$ is just multiplication by n.

Proposition 3.14. *Let $G, H, H' \in \mathrm{AffGrpSch}_S$.*

1. *If $\Phi, \Psi : G \to H$ are homomorphisms of S-affine group schemes so that $\Phi_R = \Psi_R$ for all S-algebras R.*
2. *If H, H' are sub-affine group schemes of G so that $H(R)$ and $H'(R)$ are the same as subgroups of $G(R)$, then $H = H'$.*
3. *Let $G = \mathrm{Spec}\, A$ and $H = \mathrm{Spec}\, B$. Suppose $\Phi : G \to H$ is a morphism of S-schemes with corresponding S-algebra morphism $B \to A$. Then, Φ is moreover a morphism of S-affine group schemes iff the induced map $\Phi_R : G(R) \to H(R)$ is a group homomorphism for any S-algebra R.*

Proof. (1) follows by setting R to be the underlying ring of G; in particular, $\Phi_{\mathcal{O}(G)}(\mathrm{id}_{\mathcal{O}(G)}) = \Phi_{\mathcal{O}(G)}(\mathrm{id}_{\mathcal{O}(G)})$ (as elements of $H(\mathcal{O}(G))$) gives us exactly what we want.

For (2), let us first write $H = \mathrm{Spec}(A/I)$ and $H' = Spec(A/I')$ with $A = \mathcal{O}(G)$. Now, by our description of points on sub-affine group schemes, if R is any S-algebra, the R-points of H are $H(R) = \mathrm{Hom}_{S\text{-alg}}(A/I, R) = f \in G(R) : f|_I = 0$ and $H'(R) = \mathrm{Hom}_{S\text{-alg}}(A/I', R) = f \in G(R) : f|_{I'} = 0$. As such, $f \in G(R)$ vanishes on I iff it vanishes on I'. By picking R to be A/I or A/I', the result follows.

Similarly, for (3), we'll use this technique of taking points.

If we set $R = A$, since Φ_A is a group homomorphism (which satisfies inversion), it follows that $\phi \circ \iota_G = \iota_H \circ \phi$.

If we set $R = S$, since Φ_S is a group homomorphism (which sends the identity to the identity), it follows that $\phi \circ \varepsilon_H = \varepsilon_G$.

If we set $R = A \otimes_S A$, the projection maps (of the fiber product to its components, corresponding to the S-algebra case) $p_1, p_2 : A \to A \otimes_S A$, given by mapping $a \mapsto a \otimes 1$ and $a \mapsto 1 \otimes a$, respectively. As elements of $G(A \otimes_S A)$, $j_1 + j_2 = \mu_G$. Since $\Phi_{A \otimes_S A}$ is a homomorphism of groups, it follows that $\mu_G \circ \phi = (\phi \otimes \phi) \circ \mu_H$, noting that $\Phi_{A \otimes_S A}(j_1) + \Phi_{A \otimes_S A}(j_2)$ (viewed inside $H(A \otimes_S A)$) is $(\phi \otimes \phi) \circ \mu_H$. □

3.3. Kernels.

Earlier, in Section 1.2, we defined the kernel of a homomorphism of affine group schemes functorially, namely as having points corresponding to the kernel of the group homomorphism on points. Now, we'll re-define the kernel in a more constructive manner by explicitly specifying a Hopf ideal, and then show the equivalence later.

Lemma 3.15. *Let A be an S-Hopf algebra with comultiplication μ, counit ε, and antipode ι. Then,*

1. *$k \oplus \ker \varepsilon \to A$, sending $(a, b) \mapsto a + b$ is an isomorphism of S-modules.*
2. $\mu(a) \equiv -\varepsilon(a) + a \otimes 1 + 1 \otimes a \pmod{\ker \varepsilon \otimes_S \ker \varepsilon}$
3. *for any $a \in \ker \varepsilon$,* $\iota(a) \equiv -a \pmod{\ker \varepsilon^2}$

Corollary 3.16. *Let $\Phi : G = \operatorname{Spec} A \to H = \operatorname{Spec} B$ be a morphism of S-affine group schemes with ϕ the corresponding S-Hopf algebra homomorphism from $B \to A$. Then, the ideal $\phi(\ker \varepsilon_H)A$ is a Hopf ideal of A.*

Proof. This is an easy check, using (2) and (3) from the previous lemma. □

Definition 3.17. With the same notation of the previous corollary, we define the **kernel** of Φ, denoted by $\ker \Phi$, to be sub-affine group scheme of G corresponding to the Hopf ideal $\phi(\ker \varepsilon_H)A$.

As a special case, later when we want to understand p-divisible group, we will want to define the sub-affine group scheme associated to the n-torsion points.

Definition 3.18. We define $G[n]$ to be the kernel of the map $[n] : G \to G$. This is called the **sub-affine group scheme of n-torsion points of G**.

Example 3.19. Earlier, we saw that $\mathbb{G}_{a,k}$ and $\alpha_{p,k}$ were simple for fields k of characteristic 0 and p, respectively. As such, the $n \geq 1$-torsion points of either of these is the trivial group scheme.

Example 3.20. Consider the Hopf-algebra homomorphism $k[t, t^{-1}] \to k[t, t^{-1}]$ sending $f(t)$ to $f(t^n)$, which on the level of group schemes is simply $[n] : \mathbb{G}_{m,k} \to \mathbb{G}_{m,k}$. As such, $\mathbb{G}_{m,k}[n] = \mu_{n,k}$.

Since we've introduced kernels, it's natural to also discuss injections and images.

Definition 3.21. Let Φ be a map of S-affine group schemes $H \to G$. Then, Φ is an **injection** if it is a closed immersion. Moreover, the **image** of an injection is the sub-affine group scheme of G defined by the Hopf ideal $\ker(\mathcal{O}(G) \to \mathcal{O}(H))$.

For now, to avoid defining exactness in full generality (because the construction of the cokernel is a little ugly), we'll only define left exactness for now.

Definition 3.22. The sequence of maps $0 \to H \to G \to F$ is called **(left) exact** if and only if the first map is an injection and its image is equal to the kernel of the second map.

Lemma 3.23. *Suppose $A \to S$ is a ring map and that S is a finitely generated as a module over A. Then, if the multiplication map $S \otimes_A S \to S$ is an isomorphism, $A \to S$ is a surjection.*

Remark 3.24. Geometrically, this is just saying that finite monomorphisms are equivalent to closed immersions.

Proof. Note that we have an exact sequence $A \to S \to S/A \to 0$. Tensoring this by S over A gives $S \to S \otimes_A S \to S \otimes_A S/A \to 0$, so $S \otimes_A S/A = 0$. Then, we have $S/A \otimes_A S/A = 0$. For the sake of contradiction, suppose S/A is nonzero. Then, since S is finite over A, by taking a filtration, we have some $K \subset S$ containing the image of A so that $S/K = A/I$ for some proper I. Then, $S/K \otimes_A S/K$ is nonzero, and there is a surjection $S/A \otimes_A S/A$ onto $S/K \otimes_A S/K$, so $S/A \otimes_A S/A$ is nonzero, which is a contradiction. Hence, the result follows. □

Proposition 3.25. *Suppose $0 \to H \to G \to F$ be a sequence of maps of S-affine group schemes. If it is left exact, then the induced sequence of R-points (where R is an S-algebra) is also exact (as a sequence of abelian groups). Moreover, the converse holds if we assume that $\mathcal{O}(H)$ is finite over $\mathcal{O}(G)$ (as modules).*

Proof. As an intermediate step (and also as a corollary), we will see that if we are given a morphism of S-affine group schemes $\iota : H \to G$, then injectivity of ι implies triviality of $\ker \iota$. Moreover, the converse holds if we assume $\mathcal{O}(H)$ is finite over $\mathcal{O}(G)$ (as modules).

First, let us prove the forward direction. Suppose $0 \to H \to G \to F$ is left exact and let the maps $H \to G$ and $G \to F$ be ι, Φ, respectively. On the level of Hopf algebras, we have $\mathcal{O}(F) \to \mathcal{O}(G) \to \mathcal{O}(H)$. Let the first map be ϕ and the second map be p. Then, note that $\mathcal{O}(H)$ is simply $\mathcal{O}(G)/I$, where $I = \phi(\ker \varepsilon_F)\mathcal{O}(G)$. We can then view p as the canonical projection.

We want to show that for any S-algebra R, the sequence (of abelian groups) $0 \to \mathrm{Hom}_{S-\mathrm{alg}}(\mathcal{O}(G)/I, R) \to \mathrm{Hom}_{S-\mathrm{alg}}(\mathcal{O}(G), R) \to \mathrm{Hom}_{S-\mathrm{alg}}(\mathcal{O}(F), R)$ is exact. The injectivity of the first map is obvious, so it remains to check injectivity at the third term. Suppose $f : \mathcal{O}(G) \to R$ is an S-algebra homomorphism. Then, we want to show that f factors through $\mathcal{O}(G)/I$ iff f vanishes on I iff $f \circ \phi$ is the zero element of $F(R)$. Since the zero element of $F(R)$ is just the composition $\mathcal{O}(F) \to S \to R$ and $\mathcal{O}(F) \cong R \otimes \ker \varepsilon_F$, it follows that $f \circ \phi$ is the zero element of $F(R)$ iff $f \circ \phi$ vanishes on $\ker \varepsilon_F$. But the image of $\ker \varepsilon$ generates I, so the result follows.

Now, suppose $\iota : H \to G$ is an injection. Since the sequence $0 \to \ker \iota \to H \to G$ is exact, what we've already proved tells us that taking R points will induce an exact sequence as well. Since ι is injective, we have a surjection $\mathcal{O}(G) \to \mathcal{O}(H)$, which implies that $H(R) \subset G(R)$. This implies $\ker \iota(R) = 0$ for every S-algebra R by our exact sequence. This implies (for instance, by plugging in $R = \mathcal{O}(H)$) that $\ker \iota$ is the trivial S-affine group scheme.

We now prove the converse of this intermediate step. Assume $\mathcal{O}(H)$ is finite over $\mathcal{O}(G)$ (as modules) and that $\ker \iota$ is trivial. Then, we have the exact sequence $0 \to 0 \to H \to G$, and we want to show that ι is an injection. By the forward direction of the proposition we proved earlier, $H(R) = \mathrm{Hom}_{S-\mathrm{alg}}(\mathcal{O}(H), R) \to \mathrm{Hom}_{S-\mathrm{alg}}(\mathcal{O}(G), R) = G(R)$ is hence injective as abelian groups. Now, let $R = \mathcal{O}(H) \otimes_{\mathcal{O}} (G)\mathcal{O}(G)$ and consider the two maps from $\mathcal{O}(H)$ to R (to the two coordinates). By pulling back to $\mathcal{O}(G)$, these become the same map, so we conclude that they are the same by injectivity. As such, it follows that the canonical multiplication map $\mathcal{O}(H) \otimes_{\mathcal{O}} (G)\mathcal{O}(H) \to \mathcal{O}(H)$ is an isomorphism. Hence, by the lemma above, it follows that $\mathcal{O}(H)$ is a quotient of $\mathcal{O}(G)$, so it follows that ι is indeed an injection.

Finally, it remains to show the converse of the original proposition. Assume $\mathcal{O}(H)$ is finite over $\mathcal{O}(G)$ (as modules) and that the induced sequence $0 \to H(R) \to G(R) \to F(R)$ is left exact for all S-algebras R. By what we just proved, ι is an injection. Also, by assumption, the sequence $0 \to \mathrm{im}\, \iota(R) \to G(R) \to F(R)$ is left exact for every R. Since the sequence $0 \to \ker \Phi \to G \to F$ is exact, the forward direction of the proposition tells us that taking R points will induce an exact sequence as well. Then, $\ker \Phi(R) = \mathrm{im}\, \iota(R)$ for every R, so by Proposition 3.14, the result follows. □

Corollary 3.26. *Suppose G is an S-affine group scheme and n an integer. Then, $G[n] \subset G$ is the unique sub-affine group scheme of G so that for any S-algebra R, the R-points $G[n](R)$ are identified with the n-torsion points of $G(R)$.*

4. Finite flat group schemes

Definition 4.1. We say that an affine group scheme $G = \mathrm{Spec}\, A$ over R is **finite flat** if A is finite flat as an R-module; that is, A is finitely generated and flat (equivalently, finitely generated and projective). If $\mathrm{Spec}\, R$ is connected (such as when R is local), then if we take any maximal ideal $\mathfrak{m} \subset R$, we can define the **rank** of G (written $|G|$) to be the dimension of $A/\mathfrak{m}A$ as an $R/\mathfrak{m}$-vector space.

Definition 4.2. If A is a finite k-étale algebra (k is a field), then we say that $G = \operatorname{Spec} A$ is finite étale.

Example 4.3. $\mu_{n,R}$ is a finite flat group scheme of order n.

Proposition 4.4. *Suppose k is a field of characteristic 0. Then,*

1. *every k-Hopf algebra is reduced.*
2. *every finite flat k-group scheme is finite étale.*

Proof. (ii) follows easily form (i) since k is perfect and finite étale k-algebras are reduced. We can define a k-linear map $A \to \ker \varepsilon/(\ker \varepsilon)^2$ by sending a to $a - \varepsilon a \bmod \ker \varepsilon^2$. We can then consider the composition $D : A \to A \otimes_k A \to A \otimes_k \ker \varepsilon/(\ker \varepsilon)^2$, which we can check is a derivation. For simplicity, assume the Hopf algebra is finite-dimensional over k. We can then take a basis $v_1, \dots, v_d$ of $\ker \varepsilon/(\ker \varepsilon)^2$, and a dual basis $e_1, e_2, \dots, e_d$. Now, we can define D_i to be D, post-composed with the map to $A \otimes_k k \cong A$, induced the second factor by e_i, which is also a derivation.

Now, it's easy to check that for any nonnegative integers $b_1, \dots, b_d$ that have the same sum as that of another set of nonnegative integers a_i, we have $D_1^{a_1} \cdots D_d^{a_d}(v_1^{b_1} \cdots v_d^{b_2})$ equal $\prod a_i! \bmod \ker \varepsilon$ if $a_i = b_i$ for every i, and $0 \bmod \ker \varepsilon$ otherwise. Since geometrically reduced (base-changing to the algebraic closure) implies reduced, it suffices to show the claim for k algebraically closed.

We have a surjection from $k[X_1, \dots, X_d]/(X_1, \dots, X_d)^n$ to $A/\ker \varepsilon^n$, sending X_i to v_i. By our calculation, it follows that this has no kernel, so dimension considerations force us to have $\ker \varepsilon = \ker \varepsilon^2$. Now, note that the projection $\pi : A \to A/\mathfrak{m} \cong k$ (for any maximal ideal $\mathfrak{m}$) can be viewed as a k-point of $G = \operatorname{Spec} A$. In particular, if we consider the composition $A \to A \otimes_k A \to A \otimes_k A/\mathfrak{m} \cong A$ on the level of R-points (for any k-algebra R), it follows that the induced map is just translation by π, which is hence an automorphism of A. Then, $\ker \varepsilon$ corresponds to the 0 element and $\mathfrak{m}$ corresponds to π in $G(k)$, so it follows that $\mathfrak{m} = \mathfrak{m}^2$. By a standard Nakayama argument (noting that we can split up finite-dimensional k-algebras as products of finite-dimensional local k-algebras), it follows that A is a product of fields and is hence reduced. □

We now expand on our definition of exactness from earlier (in Definition 3.22). Though this is still a little ad-hoc, it reflects the more general situation, which may be explained later.

Definition 4.5. A morphism of affine group schemes $G = \operatorname{Spec} B \to F = \operatorname{Spec} A$ (A and B can be affine group schemes over any base ring, but we'll assume finite flat) is called **surjective** if the corresponding ring morphism is faithfully flat.

Remark 4.6. Saying that $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective with $A \to B$ a flat ring extension is the same as saying that $A \to B$ is faithfully flat; this makes the naming convention above more reasonable.

To see why this is true (because this is a bit of a tangent, we've put this in a remark), we'll assume some equivalent definitions of faithfully flat (so this isn't really self-contained). First, assuming that $A \to B$ is faithfully flat, let $\mathfrak{p} \in \operatorname{Spec} A$; we want to show that $\mathfrak{p}$ is in the image of the map on spectra. Since base change preserves faithful flatness, it follows that we can assume A is an integral domain. Indeed, we have the Cartesian diagram

$$\begin{tikzcd}
\operatorname{Spec} B/\mathfrak{p}B \arrow[r] \arrow[d] & \operatorname{Spec} A/\mathfrak{p} \arrow[d] \\
\operatorname{Spec} B \arrow[r] & \operatorname{Spec} A
\end{tikzcd}$$

so that we have $\mathfrak{p}$ in the image of the lower map iff the zero (prime) ideal is in the image of the top map. We may likewise localize at the zero ideal and assume that A is actually a field. Note that B is a faithfully flat A-algebra, and so it can't be the the zero ring, which means that it has some prime ideal. But then $\operatorname{Spec} A$ is just a single point and it's clear then that $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective. For the other direction, we note that one definition of an R-module M being faithfully flat is that $M \neq \mathfrak{m}M$ for any maximal ideal $\mathfrak{m}$. From the proof of the going up and down theorems, an important step is showing that if we have a ring map $\phi : A \to B$ and $\mathfrak{p} \in \operatorname{Spec} A$, then $\mathfrak{p}$ is in the image of spectra iff $\phi^{-1}(\phi(\mathfrak{p}B)) = \mathfrak{p}$. Then, for each $\mathfrak{p}$, we cannot have $\phi(\mathfrak{p})$ generate all of B, so we're done.

Remark 4.7. The reason why this is in some sense the "right" definition of surjective is because the general construction of cokernels in the category of finite flat group schemes involves fpqc sheaves (i.e. Grothendieck topologies who coverings are faithfully flat and quasicompact morphisms); in particular, we want to consider exactness on the level of fpqc sheaves and not Zariski sheaves, because the naive definition of the cokernel as a functor (on the level of points) is not representable. However, representable fpqc presheaves in this situation are actually fpqc sheaves (i.e. every covering is a universal effective epimorphism).

With this notion of surjectivity, we can define exact sequence as follows.

Definition 4.8. A sequence of finite flat affine group schemes $0 \to H \to G \to F \to 0$ is **exact** iff it is left exact and $G \to F$ is surjective.

Lemma 4.9. *If $H = \operatorname{Spec} C, G = \operatorname{Spec} A, F = \operatorname{Spec} B$ are all finite flat affine S-group schemes and $0 \to H \to G \to F$ is left exact, then TFAE:*

(1) $\#G = \#H \cdot \#F$.
(2) *$G \to F$ is surjective.*

Proof. Consider the Hopf ideal defining $\ker(G \to F)$; we have $I = (\ker \varepsilon_B)A \subset A$. We have $H \cong \operatorname{Spec} A/I$. Now, consider the morphism

$$A \otimes_B A \to A \otimes_S A/I,$$

sending the pure tensor $a \otimes a'$ to $a\mu(a')$ mod $A \otimes_S I$. By localizing everything at a maximal ideal of S, the left hand side has rank $\#G^2/\#F$ and the right hand side has rank $\#G \cdot \#H$. So this shows that if the map is an isomorphism of S-modules, then $\#G = \#H \cdot \#F$. Working locally (localization at a maximal ideal) and assuming the ranks are the same, we easily get a surjection (which must also be a bijection by basic linear algebra), so this shows the other direction as well.

TODO: insert proof that G to F is surjective iff morphism is iso □

Although we could, in theory, continue in this fashion and not appeal to Grothendieck's construction of the cokernel (and in fact define the étale and connected components and associated exact sequence), we'll make it easier for ourselves by citing Grothendieck's big theorem here as a black box and come back to it later.

Theorem 4.10. *Let G be a finite flat S-affine group scheme and let H be a closed finite flat sub-affine group scheme of G. Then, the quotient G/H exists as a finite flat group scheme of order $\#G/\#H$.*

4.1. **Étale and connected components.** We first discuss a useful criteria for étaleness of finite flat group schemes.

Proposition 4.11. *Let $G = \operatorname{Spec} A$ be an S-affine group scheme with augmentation ideal I. Then, $I/I^2 \otimes_S A \cong \Omega_{A/S}$ and $I/I^2 \cong \Omega_{A/S} \otimes_A A/I$.*

Corollary 4.12. *G is étale iff $I = I^2$.*

Proof. Since G is already flat over R, G is étale iff $\Omega_{A/S} = 0$. Then, the proposition allows us to conclude. □

Proof of proposition. First, note that we have a diagram

$$\begin{tikzcd} G \times_S G \arrow[r, "f"] & G \times_S G \\ G \arrow[u, "\Delta"] \arrow[ur, "{(\mathrm{id},e)}"] & \end{tikzcd}$$

Here, the top arrow f is simply $(\mathrm{pr}_1, \mathrm{m}) \circ (\mathrm{id}, \mathrm{i})$, which sends (g, h) to (g, gh^{-1}). Note that this top map is an isomorphism because we write down an inverse (just replace gh^{-1} with $h^{-1}g$). On the level of Hopf algebras, this is a bit more transparent for our purposes:

$$\begin{tikzcd} A \otimes_S A \arrow[d] & A \otimes_S A \arrow[l] \arrow[dl] \\ A & \end{tikzcd}$$

Of course, the down arrow is just the standard multiplication map, the top arrow is the isomorphism (dual to the map f from above), and the down-left arrow is the map sending $x \otimes y$ to $x \cdot \varepsilon(y)$.

Let J be the kernel of this down-left map. Then, by the isomorphism on the top map, we get an isomorphism

$$\Omega_{A/S} \cong J/J^2.$$

It remains to relate J to I. We can decompose $A \otimes_R A$ as $A \otimes_R R \oplus A \otimes_R I$, so that the right map has kernel $A \otimes_R I$. We then get an isomorphism between J and $A \otimes_R I$, and also have $J^2 \cong A \otimes_R I^2$ as a result. We then easily get that

$$\Omega_{A/R} \cong A \otimes_R I/I^2.$$

Tensoring this with A/I over A, we then get I/I^2 again, and we're done (noting that $A/I \cong R$). □

Corollary 4.13. *Let $\operatorname{Spec} A$ be a finite flat group scheme over R with augmentation ideal I. Then, $I = I^2$ iff $\operatorname{Spec} A$ is étale.*

Proof. This follows immediately, noting that unramified and flat is equivalent to étale. □

Corollary 4.14. *Every finite flat constant group scheme is étale.*

Proof. If Γ is a finite group, we can write the associated group scheme as $\operatorname{Spec}\left(\bigoplus_{i\in\Gamma} Re_i\right)$. The augmentation ideal is just $\bigoplus_{i\neq \mathrm{id}} Re_i$, so the result follows from the previous corollary. □

Proposition 4.15. *Let $G = \operatorname{Spec} A$ be a finite flat group scheme over R. Then G is étale iff the image of the unit section is open.*

Theorem 4.16. *Let $G = \operatorname{Spec} A$ be a finite flat group scheme over R. Suppose the order of G is invertible in R. Then, G is étale.*

Corollary 4.17. *A finite flat group scheme over a field of characteristic 0 is étale.*

In particular, when thinking about group schemes of order p over $\mathbf{Z}_\ell$, the most interesting case is when $p = \ell$, since otherwise all of these will be étale. As Professor Mazur explained to us, this is why the work of Oort–Tate (which we explain in detail in Section 6) only considers this case, and is a good further explanation of Remark 2.20.

4.1.1. *The connected-étale sequence.* In this section, we consider finite flat group schemes over Henselian local rings. To that end, we fix R to be a Henselian local ring with residue field k.

Proposition 4.18. *Let G be a finite flat R-group scheme. Define G^0 to be the clopen subscheme of G corresponding to the connected component of G containing the unit section. Then,*

1. *G^0 is the spectrum of a Henselian local R-algebra with residue field k and is a flat closed normal subgroup scheme of G.*
2. *Define $G^{ét}$ to be G/G^0. Then, there is an exact sequence called the **connected-étale sequence** $0 \to G^0 \to G \to G^{ét} \to 0$ so that any $G \to H$ with H finite étale over R factors through $G \to G^{ét}$.*
3. *$G \mapsto G^0$ and $G \mapsto G^{ét}$ are exact in the category of finite flat R-group schemes.*
4. *If R is a perfect field, then $G_{red} \to G \to G^{ét}$ is an isomorphism and the connected-étale sequence splits.*

Proposition 4.19. *Let R be a perfect field of characteristic $p \neq 0$. Then, if $G = \operatorname{Spec} A$ is a connected finite flat R-group scheme, then $A \cong R[x_1, \dots, x_n]/(x_1^{p^{e_1}}, \dots, x_n^{p^{e_n}})$ with the $n \geq 1$ and the $e_i \geq 1$. In particular, connected group schemes have p-power order.*

5. Fontaine's ramification bound

The purpose of this section is to prove Fontaine's ramification bound, which is a key step in the proof that there are no nontrivial abelian schemes over $\mathbf{Z}$.

Definition 5.1. Let K be a valued field with valuation ring $\mathcal{O}_K$. Let $X = \operatorname{Spec} B$ be a finite flat $\mathcal{O}_K$-scheme so that $\Omega_{B/\mathcal{O}_K}$ is annihilated by some element of $\mathcal{O}_K$. Then, $K(X(\overline{K}))$, the field generated by $\overline{K}$-points of X is defined as follows. First, note that $B_K = B \otimes_{\mathcal{O}_K} K$ is finite over K and $\Omega_{B_K/K} \cong \Omega_{B/\mathcal{O}_K} \otimes_{\mathcal{O}_K} K = 0$, which implies that B_K is a finite product of finite separable extension of K. Take the compositum of all these finite separable extensions in a common algebraic closure $\overline{K}$, and we'll denote this by $K(X(\overline{K})$.

We also recall some facts about lower/upper ramification groups. In particular, suppose we have a complete DVR of characteristic 0 and residue field of characteristic p and take

L/K to be a finite extension. Let π_K and π_L be uniformizers of K and L so that $\mathcal{O}_L$ is generated over $\mathcal{O}_K$ by π_L.

Let v_K be the normalized valuation on K and v_L be the extended one (so that $v_L(\pi_L) = 1/e_{L/K}$, where $e_{L/K}$ is the ramification index. We also define $i_{L/K}$ to be a function from $G = \mathrm{Gal}(L/K) \to \mathbf{Z}$, so that $\sigma \mapsto v_L(\sigma(\pi_L) - \pi_L)$. We can also define $\phi_{L/K} : \mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}$ so that $i \mapsto \sum_{\sigma \in G} \min(i, i_{L/K}(\sigma))$ and $\psi_{L/K}$ to be the inverse of this function. We can then define $u_{L/K} = \phi_{L/K} \circ i_{L/K}$. Let $i_{L/K} = \sup i_{L/K}(\sigma)$ and $u_{L/K} = \sup u_{L/K}(\sigma)$, where in both cases σ runs over all non-identity elements σ.

We then define $G_{(i)} = \{\sigma \in G : i_{L/K}(\sigma) \geq i\}$ and $G^{(u)} = \{\sigma \in G : u_{L/K}(\sigma) \geq u\}$. We call the former the **lower ramification group** and the latter the **higher ramification group**. We note that these are not the typical conventions, but are the ones that follow Fontaine's treatment.

Fontaine's theorem is then as follows:

Theorem 5.2. *Suppose K is a local field of characteristic 0 and let $e = v_K(p)$, where v_K is a normalized valuation on K (which is a complete discrete valuation ring with residue field of characteristic p). Also, suppose Γ is a finite flat commutative group scheme over $\mathcal{O}_K$ that is killed by p^n.*

Let $L = K(\Gamma(\overline{K}))$, which is the field generated by $\overline{K}$-points, and $G = \mathrm{Gal}(L/K)$. Then, $G^(u) = 1$ for $u > e(n + 1/(p-1))$ and $v(D_{L/K}) < e(n + 1/(p-1))$, where $D_{L/K}$ is the different of L/K.

Before we get into proving Fontaine's theorem, we first discuss the ramification of complete intersections.

Definition 5.3. For a finite flat $\mathcal{O}_K$-algebra S, an ideal $IofS$ is said to be a **divided power ideal** if for all $x \in I$ and $n \in \mathbf{N}$, we have that $x^n/n!$ is also in I. Moreover, let $I^{[m]}$ be the ideal of S that is generated by products $x_1^{n_1}/n_1!, \ldots, x_s^{n_s}/n_s!$ with $x_1, \ldots, x_s \in I$ and $n_1 + \cdots + n_s \geq m$. If, moreover, the intersection of all of the $I^{[m]}$ is 0, we say that I is **topologically nilpotent**.

Proposition 5.4. *Suppose $A = \mathcal{O}_K[\![x_1, \ldots x_n]\!]/\langle f_1, \ldots, f_n\rangle$. Also, suppose there is a nonzero element $a \in \mathcal{O}_K$ annihilating $\Omega_{A/\mathcal{O}_K}$ so that $\Omega_{A/\mathcal{O}_K}$ is a flat A/aA-module.*

1. *If S is a finite flat $\mathcal{O}_K$-algebra and I is a topologically nilpotent divided power ideal, then $\mathrm{Hom}_{\mathcal{O}_K}(A, S) = \mathrm{im}(\mathrm{Hom}_{\mathcal{O}_K}(A, S/aI \to \mathrm{Hom}_{\mathcal{O}_K}(A, S/I)$.*
2. *If $L = K(Y(\overline{K}))$ with $Y = \mathrm{Spec}\, A$, then $u_{L/K} \leq v_K(a) + e_K/(p-1)$, where $e_K = v(p)$.*

Before we get to the proof of the proposition, consider the following lemma:

Lemma 5.5. $(I^{[n]})^{[2]} \subset I^{[n+1]}$.

Proof. Of course, it suffices to show that for any $x \in I^{[n]}$, we have $x^2/2 \in I^{[n+1]}$. We can moreover take x to be a single term, i.e. of the form $x_1^{a_1} \cdots x_k^{a_k}/(a_1! \cdots a_k!)$ with $x_1, \ldots, x_k \in I, a_1 + \cdots + a_k \geq n$. Then, we have

$$\begin{aligned}\frac{x^2}{2} &= \frac{x_1^{2a_1} \cdots x_k^{2a_k}}{2a_1!^2 \cdots a_k!^2} \\ &= \frac{x_1^{2a_1} \cdots x_k^{2a_k}}{(2a_1)! \cdots (2a_k)!} \binom{2a_1 - 1}{a_1 - 1} \binom{2a_2}{a_2} \cdots \binom{2a_k}{a_k},\end{aligned}$$

which is clearly in $I^{[2n]} \subset I^{[n+1]}$, as desired. □

We now return to the proof of (i) of the proposition above:

Proof of (i) of proposition. Note that A is local and let $\mathfrak{m}$ be its maximal ideal. Also $\Omega_{A/\mathcal{O}_K}$ is a finitely generated flat module over a local, Noetherian ring, so it follows that it is free over A/aA. Let $\partial f_i/\partial x_j = ap_{ij}$ with $p_{ij} \in A$. Note that adx_i can be expressed as linear combinations of the df_is, so it follows that corresponding matrix will give an inverse of the matrix (p_{ij}), so that (p_{ij}) itself is an invertible matrix. The goal is to suppose we have some $\mathcal{O}_K$-homomorphism $\phi : A \to S/aI$ and find a lift from $A \to S$ that is unique. To do this, we'll work inductively, and lift a map $A \to S/aI^{[n]}$ to $A \to S/aI^{[n+1]}$. In particular, take elements $v_1, \dots, v_m \in S$ so that applying f_i to the tuple $(v_1, \dots, v_m)$ is in $aI^{[n]}$. We want to find $\varepsilon_i \in I^{[n]}$ so that the $f_i(v_1 + \varepsilon_1, \dots, v_m + \varepsilon_m)$ lands in $aI^{[n+1]}$. We want this choice of tuple to also be unique modulo $I^{[n+1]}$. To work this out, we use the Taylor expansion, as well as the fact that I is a topologically nilpotent divided power ideal to handle convergence issues:

$$\begin{aligned} f_i(v_1 + \varepsilon_1, \dots, v_m + \varepsilon_m) = f_i(v_1, \dots, v_m) &+ \sum_{j=1}^{m} \frac{\partial f_i}{\partial x_j}(v_1, \dots, v_m)\varepsilon_j \\ &+ \sum_{|r| \geq 2} \frac{\partial^r f_i}{\partial x_r}(v_1, \dots, v_m)\frac{\prod_k \varepsilon_k^{r_k}}{r!}. \end{aligned}$$

Suppose we write $\partial f_i/\partial x_j = a\tilde{p_{ij}} + q_{ij}$, where we lift p_{ij} to $\mathcal{O}_K[\![x_1, \dots x_n]\!]$ and let $q_{ij} \in \langle f_1, \dots, f_n \rangle$. By abuse of notation, we'll just write p_{ij} for the lifts. Plugging in $(v_1, \dots, v_m)$, multiplying by ε_j, and using the lemma above gives that $\partial f_i/\partial x_j(v_1, \dots, v_m)\varepsilon_j$ is equivalent to $ap_{ij}(v_1, \dots, v_m)$ modulo $aI^{[n+1]}$. The same idea shows that the higher older partial derivatives land in $aI^{[n+1]}$. It then follows that the Taylor expansion from earlier becomes:

$$f_i(v_1 + \varepsilon_1, \dots, v_m + \varepsilon_m) \equiv f_i(v_1, \dots, v_m) + a\sum_j p_{ij}(v_1, \dots, v_m)\varepsilon_j \pmod{aI^{[n+1]}}.$$

Noting that $(p_{ij}(v_1, \dots, v_m)) \in \mathrm{GL}_m(S)$, it follows that we can find unique ε_i so that $f_i(v_1 + \varepsilon_1, \dots, v_m + \varepsilon_m) \in aI^{[n+1]}$; we can ensure that the ε_i will live in $I^{[n]}$ because the $f_i(v_1, \dots, v_m) \in aI^{[n]} \subset I^{[n]}$. □

Fontaine's proof of (ii) requires another quick fact that is closely related to Krasner's lemma.

Lemma 5.6 (Converse to Krasner's lemma)**.** *Let K be a finite extension of $\mathbf{Q}_p$ as earlier and E/K be finite Galois. Let $v(\cdot)$ be the extended valuation on K to E and define $\mathfrak{m}_E^t = \{x \in \mathcal{O}_E : v(x) \geq t\}$. Then,*

1. *If $t > u_{L/K}$ (defined earlier), then every $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ lifts to an $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E$.*
2. *Conversely, if there is some $t > 0$ so that any $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ lifts to an $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E$ for every finite Galois extension E/K, then t must be bigger than $u_{L/K} - 1/e_{L/K}$.*

Proof. We start with the "forward" direction of the lemma. Let π_L be a uniformizer of L and $p(x)$ be the minimal polynomial, living in $\mathcal{O}_K[x]$. Since $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, any $\mathcal{O}_K$-homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ is determined by where π_L is sent. Let α be the image of π_L, and note that we must have $v(p(\alpha)) \geq t > u_{L/K}$.

Consider v uniquely extended to the compositum of L and E. Also, let c be an argument of the maximum of $v(\alpha - g\pi_L)$, where g ranges over every element of the finite Galois group $G = \mathrm{Gal}(L/K)$. Obviously, we have $v(\alpha - g\pi_L) = \min(v(\alpha - c\pi_L), v(c(\pi_L - c^{-1}g\pi_L)) = i_{L/K}(c^{-1}g)$ for any $g \in \mathrm{Gal}(L/K)$. Now, by the definition of $\phi_{L/K}$ from earlier and noting that $p(\alpha) = \prod(\alpha - g\pi_L)$, it follows that $v(p(\alpha)) = \phi_{L/K}(\max_{g\in G} v(\alpha - g\pi_L))$.

Since $v(p(\alpha)) \geq t > u_{L/K}$ and $\phi_{L/K}$ is monotonically increasing, we have that $v(\alpha - c\pi_L) = \max_{g\in G} v(\alpha - g\pi_L) > i_{L/K}$. Then, by Krasner's lemma, it follows that $c\pi_L \in K(\alpha) \subset E$, which lets us lift to $\mathcal{O}_L \to \mathcal{O}_E$, as desired.

For the converse, it suffices to consider the case $t = u_{L/K} - 1/e_{L/K}$ and obtain a contradiction; in particular, we need to find an un-liftable map. Let K'/K the maximal unramified subextension of L/K. Base change of an unramified extension is still unramified, so we can write $K' \otimes_K E = \prod_i E_i$, where E_i are finite separable extensions of E. We can, of course, replace E with E_i to get a lift to an $\mathcal{O}'_K$-homomorphism from $\mathcal{O}_L$ to $mathcalO_{E_i}/\mathfrak{m}^t_{E_i}$ with $u_{L/K} = u_{L/K'}$ and $e_{L/K} = e_{L/K'}$, which means that we can reduce to the case where L/K is totally ramified. We can moreover split into two cases, one where L/K is tamely ramified and the other where L/K is wildly ramified.

First, suppose L/K is tamely ramified, which tells us that if $v(g\pi_L - \pi_L) > 1/e_{L/K}$, then $g = 1$ (the identity element of $\mathrm{Gal}(L/K)$). As a result, it follows that $i_{L/K} = 1/e_{L/K}$ (essentially by definition) and hence $u_{L/K} = 1$. Then, we have $t = 1 - 1/e_{L/K}$. Note that there is an $\mathcal{O}_K$-homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\pi_K^t\mathcal{O}_E$, given by sending π_L to π_E (uniformizers of L, E, respectively), since $v(\prod(\pi_E - g\pi_L)) = [L : K]/e_{L/K} = 1$. This does not have any lift $\mathcal{O}_L \to \mathcal{O}_E$, at least for any E/K a totally ramified extension of degree $e_{L/K} - 1$ because we claim there are no $\mathcal{O}_K$-homomorphisms $\mathcal{O}_L \to \mathcal{O}_E$. But this just follows from the fact that we cannot send π_L to anything in $\mathcal{O}_E$ because of the restriction on degree.

Now, for the case where L/K is wildly ramified, by definition, we have for g not the identity, that $i_{L/K} \geq 1/e_{L/K}$, so that $t \geq 1$. We can say even more because $p | [L : K] = e_{L/K}$, namely that $t > 1$, since $u_{L/K} \geq 1 + p/e_{L/K}$ and hence $t \geq 1 + (p-1)/e_{L/K}$. Note that $t \in (1/e_{L/K})\mathbf{Z}$, so we can write $e_{L/K}t = e_{L/K}r + s$, with $0 \leq s < e_{L/K}$, where r, s are whole numbers. Let $f \in \mathcal{O}_K[x]$ be the minimal polynomial of π_L and let $g(x) = f(x) - \pi_K^r x^s$, which is clearly monic. By Eisenstein's criterion (and noting that f is Eisenstein because it is the minimal polynomial of π_L and L/K is totally ramified), it follows that $g(x)$ is also Eisenstein if $s > 0$ or $s = 0, r \geq 2$. Now, let α be a root of $g(x)$ and set $E = K(\alpha)$. It follows that E is totally ramified. We can then define an $\mathcal{O}_K$-homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}^t_E$ sending π_L to α, since $v(f(\alpha)) = v(\pi_K^r \alpha^s) = e_{L/K}r + s = t$, as desired.

To complete the proof, we need to show that there is no lift $\mathcal{O}_L \to \mathcal{O}_E$. If there is, by taking fraction fields, we see that $L \subset E$. Since L, E have the same degree over K, they must be the same. Then, $v(g\pi_L - \alpha) \in (1/e_{L/K})\mathbf{Z}$ for each g. We also know that $v(\prod(g\pi_L - \alpha)) = t$ from our earlier computation, which means that $e_{L/K}\phi^{-1}_{L/K}(t) \in \mathbf{Z}$. Also, the slope of $\phi_{L/K}$ at $i_{L/K}$, say s, is the size of $G_{(i_{L/K})}$, which means that (by definition) $e_{L/K}\phi^{-1}_{L/K}(t) = e_{L/K}i_{L/K} - 1/s \in \mathbf{Z}$, so $s = 1$. But that is a contradiction because L/K is wildly ramified and the result follows. □

With this lemma, we can now complete the proof of the earlier proposition.

Proof of (ii) of proposition. Recall we wanted to show that $u_{L/K} \leq v(a) + e_K/(p-1)$. At the very least, for the case where L/K is tame (by definition), we have $u_{L/K} \leq 1 \leq v(a) \leq v(a) + e_K/(p-1)$. So we can assume that L/K is wild.

For $t > v(a)+e_K/(p-1)$ and a finite Galois extension E/K, we claim that any $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ lifts to $\mathcal{O}_L \to \mathcal{O}_E$.

To see this, note that by definition of L, $Y(\mathcal{O}_L)$ gives us all the points of Y, and we moreover have $|Y(\mathcal{O}_E)| \leq |Y(\mathcal{O}_L|$, with equality iff we can find a morphism from $\mathcal{O}_Y \to \mathcal{O}_E$. So it suffices to show that we have equality, given the assumptions of our claim. Indeed, by an easy computation of the valuation of a factorial, we know that $\mathfrak{m}_E^{t-v(a)}$ is a divided power ideal (since $t - v(a) > e_K/(p-1)$), which is also clearly topologically nilpotent. In addition, we have $\mathfrak{m}_E^t = a\mathfrak{m}_E^{t-v(a)}$. Now, given a map $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$, we can post-compose the projection to $\mathcal{O}_E/\mathfrak{m}_E^{t-v(a)}$. The kernel of this composition is just $\mathfrak{m}_L^{t-v(a)}$ and is similarly a divided power ideal that is topologically nilpotent.

For convenience, we will write Hom for the remainder of the proof to refer to homomorphisms over $\mathcal{O}_K$. Now, the first part of the proposition tells us that $\mathrm{Hom}(A, \mathcal{O}_E) = \mathrm{im}(\mathrm{Hom}(A, \mathcal{O}_E/a\mathfrak{m}_E^{t-v(a)}) \to \mathrm{Hom}(A, \mathcal{O}_E/\mathfrak{m}_E^{t-v(a)})$, along with a similar statement if we replace E with L. Take our morphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$, pre-compose it with an element of $Y(\mathcal{O}_L)$ to get an element of $\mathrm{Hom}(A, \mathcal{O}_E/\mathfrak{m}_E^t)$. Again, note that $\mathfrak{m}_E^t = a\mathfrak{m}_E^{t-v(a)}$, and using the equation from (i) tells us that we can post-compose with the projection and hence get an element of $Y(\mathcal{O}_E)$. Moreover, it is easy to see that this map from $Y(\mathcal{O}_L) \to Y(\mathcal{O}_E)$ is injective using the definition of L (it's just the field generated by the points of A). As a result, it follows immediately from the work earlier that our claim holds.

Now, to complete the proof, recall that we are in the situation where L/K is wild. For $i_{L/K}(g) \in (1/e_{L/K})\mathbf{Z}$ for g not the identity and by properties of higher ramification groups, we know that $|G_(i)|$ is divisible by p. Then, by definition of $u_{L/K}$, it follows that $e_{L/K}u_{L/K}$ is an integer divisible by p. Also, note that $v(a) + e_K/(p-1) \geq u_{L/K} - 1/e_{L/K}$, using the previous lemma and the claim, so we have

$$(p-1)e_{L/K}u_{L/K} \leq (p-1)e_{L/K}v(a) + e_{L/K}e_K + p - 1$$

Note that $p|e_{L/K}$, so actually we end up getting

$$(p-1)e_{L/K}u_{L/K} \leq (p-1)e_{L/K}v(a) + e_{L/K}e_K.$$

Then, rearranging the inequality gives us exactly what we need and the result follows. □

Finally, we can prove Fontaine's ramification bound using this proposition.

Proof of theorem. The fact about differents is a general fact that follows after we prove that $u_{L/K} \leq e_K(n + 1/(p-1))$. Indeed, note that, by definition, we have $v(D_{L/K}) = v(\prod_{g\neq 1}(g\pi_L - \pi_L))$. Then, by definition of $u_{L/K}$, we have the following computation:

$$\begin{aligned} u_{L/K} &= \sum_g \min(i_{L/K}, i_{L/K}(g)) \\ &= i_{L/K} + \sum_{g\neq 1} i_{L/K}(g) \\ &= i_{L/K} + v(\prod_{g\neq 1}(g\pi_L - \pi_L)) \\ &= i_{L/K} + v(D_{L/K}, \end{aligned}$$

from which it follows that $v(D_{L/K}) < e_K(n + 1/(p-1))$, since $i_{L/K} > 0$.

Write $\Gamma = \operatorname{Spec} A$. We first proceed in the case where $\Omega_{A/\mathcal{O}_K}$ is free over A/p^nA. Now, note that K is perfect, so by Proposition 4.18, we have $\Gamma_K \cong \Gamma_K^{\text{ét}} \times \Gamma_K^0$. Using Proposition 4.19, it follows that $A = \prod_i A_i$ with each $A_i \cong \mathcal{O}_{K_i}[\![x_1, \dots, x_l]\!]/(f_{i1}, \dots, f_{il})$, with the K_i/K unramified (by our assumption). As a result, we can finish by (ii) of our proposition.

To reduce to this case, we require the following theorem by Raynaud and embed Γ into an abelian scheme X over $\mathcal{O}_K$ (note that $\mathcal{O}_K$ is a local ring). Recalling the construction of L and also noting that $\Gamma(\overline{K}) \hookrightarrow X[p^n](\overline{K})$, showing the result for the $X[p^n]$ is sufficient. By the results of Section 4, we have an exact sequence $0 \to X[p^n] \to X \to X \to 0$, with the third map being the multiplication-by-p^n map. Then, we see that $\Omega_{X[p^n]/\mathcal{O}_K}$ is the cokernel of the multiplication-by-p^n map on $\Omega_{X/\mathcal{O}_K}$, and is hence a locally free $\mathcal{O}_K/p^n\mathcal{O}_K$-module, since $\Omega_{X/\mathcal{O}_K}$ is a locally free $\mathcal{O}_K$-module. The result follows. □

Theorem 5.7. *Let G be a finite flat commutative S-group scheme with S a local ring. Then, we can find a closed S-immersion $G \hookrightarrow A$, where A is an abelian S-scheme.*

Example 5.8. As a silly example (working in the setup of the Fontaine's ramification bound), consider the case where $K = \mathbf{Q}_p$ and Γ is the roots of p^n unity (i.e. $\operatorname{Spec} A = \operatorname{Spec} \mathbf{Z}_p[X]/(X^{p^n} - 1)$). Then, we have $A \otimes K \cong \mathbf{Q}_p \times \mathbf{Q}_p(\zeta_p) \times \cdots \times \mathbf{Q}_p(\zeta_{p^n})$, so it follows that L is just $\mathbf{Q}_p(\zeta_{p^n})$. By an explicit computation (using Herbrand's theorem), it follows that $u_{L/K} = n$ and $i_{L/K} = 1/(p-1)$. The ramification bound is not tight, but predicts that $u_{L/K} \le n + 1/(p-1)$, which is very good for large p.

6. Group schemes of prime order

One of the first things Professor Mazur told us to look at was the classification of group schemes of order p over an algebraically closed field. We learned about this from the classic paper of Oort and Tate [14], which goes on to provide a classification over pretty general complete local rings of residue characteristic p. This generalizes the example for $p = 2$ we did in Section 2. In this section we will explain the key arguments of both of those classifications of Oort-Tate, following their paper closely.

One of the main outcomes of this classification is the following theorem, originally due to Artin and Mazur:

Theorem 6.1. *The only group schemes of order p over $\mathbf{Z}$ are $\mu_{p,\mathbf{Z}}$ and $(\mathbf{Z}/p\mathbf{Z})_{\mathbf{Z}}$.*

We won't get quite this far, but we will get very close: the main ingredient in Oort–Tate's proof really is the classification over $\mathbf{Z}_p$, which we will do in full detail.

6.1. Over an algebraically closed field.

Let k be an algebraically closed field. The statement of the classification of group schemes of order p over k is that Proposition 2.13 accounts for all of them.

Lemma 6.2. *Let k be an algebraically closed field and p a rational prime. Every k-group scheme of order p is either étale or connected.*

Proof. The crux of the proof is the fact that quotients exist and their orders are what you expect (the technicalities of which we have already discussed). In particular, for any subgroup scheme $H \subset G$, Grothendieck established the existence of a scheme G/H with the property that

$$|G| = |H||G/H|.$$

Applying this to $H = G^\circ$, we see that the order of G° is either 1 or p. If it is p, since k is a field, using the theory of finite-dimensional vector spaces it follows that $G = G^\circ$ and thus G is connected. If $|G^\circ| = 1$, then $G^\circ = \operatorname{Spec} k$ and thus (by the étale-connected exact sequence maybe, where we can even use $G = G^\circ \times G^{\text{ét}}$ to avoid thinking since k is perfect) G is étale. □

Remark 6.3. It might seem like one shouldn't need Grothendieck's machinery to establish something like this, since one is really only using the fact that the order of G° divides the order of G. But as S. Marks pointed out to us, this is unlikely – even in the classical group-theoretic setting, one needs to think very directly about the coset space to show this divisibility.

As we know, the étale k-group schemes are easy to think about. Since k is algebraically closed, $\mathrm{Gal}(\bar{k}/k)$ is trivial, and thus the category of étale k-group schemes of order p is equivalent to the category of groups of order p (in particular an étale k-group scheme is determined by its k-points). So we have proved:

Lemma 6.4. *If k is algebraically closed, the only étale group scheme of order p is $(\mathbf{Z}/p\mathbf{Z})_k$.*

Note that this group scheme is commutative, and its Hopf algebra can be generated as a k-algebra by a single element (recall that this Hopf algebra is as a ring the k-algebra of functions on $\mathbf{Z}/p\mathbf{Z}$, so it can be generated by any function taking on different values at each point because of the general theory of polynomial interpolation; such a function exists because k is algebraically closed and therefore infinite). Now for the connected case, which requires a little more care.

Lemma 6.5. *Let k be an algebraically closed field, and G a connected k-group scheme of order p. Then k has characteristic p and $G = \mu_{p,k}$ or $\alpha_{p,k}$.*

Proof. The basic idea is to separate the cases based on whether the Cartier dual $G^\vee$ is étale (in the case of $\mu_{p,k}$) or connected (in the case of $\alpha_{p,k}$). And the way to understand what $G^\vee$ is is to show that its Hopf algebra $A^\vee$ is generated over k by a single element d, which is an arbitrary choice of derivation on A. Once we have shown this, the abstract properties of G (e.g. the fact that it is connected and of order p, and that G' is of order p and therefore either étale or connected by Lemma 6.2) will allow us to deduce the desired fact about G. The main idea of the proof is in the second step, so we do it first

Step 2: In step 1, we will show that $A^\vee = k[d]$ for some $d \in A^\vee$ with the property that

$$c_{A^\vee}(d) = d \otimes 1 + 1 \otimes d$$

and $d \in I_{G^\vee}$, the augmentation ideal of $A^\vee$. Since $G^\vee$ has order p, by Lemma 6.2, we know that it is either étale or connected. If it is étale, then by Lemma 6.4, we have $G^\vee = (\mathbf{Z}/p\mathbf{Z})_k$, and so by Lemma 2.7, $G = \mu_{p,k}$. And since G is assumed connected, it follows that k has characteristic p, since otherwise $G \cong (\mathbf{Z}/p\mathbf{Z})_k$, which is étale and not connected (see Lemma 2.8). The only remaining case is that $G^\vee$ is connected. In that case, $A^\vee$ is a local k-algebra, and it is also Artinian since it is finite over k. So by the standard fact from commutative algebra (see A-M), the augmentation ideal $I_{G^\vee}$ is nilpotent, and therefore d itself is nilpotent. If n is the least positive integer such that $d^n = 0$, then $k[d] = k[X]/(X^n)$ has rank n over k; this means that $n = p$. In particular, continuing to use the very convenient fact that k is a field[6],

$$\begin{aligned} 0 &= c_{A^\vee}(d^p) \\ &= c_{A^\vee}(d)^p \\ &= (1 \otimes d + d \otimes 1)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} d^i \otimes d^{p-i} \\ &= \sum_{i=1}^{p-1} \binom{p}{i} d^i \otimes d^{p-i} \end{aligned}$$

implies that k has characteristic p. So we have

$$A^\vee = k[X]/X^p$$

with Hopf algebra structure given by $X \mapsto 1 \otimes X + X \otimes 1$, in other words

$$G^\vee \cong \alpha_{p,k}$$

(by Lemma 1.4 the comultiplication is enough to deduce this). By Lemma 2.10, this implies that $G \cong \alpha_{p,k}$ as desired.

Step 1: We just need to justify the technical lemma we used in step 2, namely that $A^\vee$ is generated over k by a single element d in the augmentation ideal of $A^\vee$ with the property that

$$c_{A^\vee}(d) = 1 \otimes d + d \otimes 1.$$

We expect such an element to exist from the examples, I suppose. In fact, the claim is that we may choose d to be any k-derivation on A (and the fact that derivations exist on A and can be interpreted as elements of $A^\vee$ is what makes going between A and $A^\vee$ useful despite the symmetry of the situation). Such a derivation exists because the universal property of $\Omega_{A/k}$ and Proposition 4.11, which together say that

$$\mathrm{Der}_k(A,k) \cong \mathrm{Hom}_{\mathsf{Mod}_A}(\Omega_{A/k},k) \cong \mathrm{Hom}_{\mathsf{Mod}_A}(A \otimes_k I/I^2,k) \cong \mathrm{Hom}_{\mathsf{Mod}_k}(I/I^2,k).$$

Since G is connected, A is a local ring, and since it is a finite k-algebra, it is in fact a local Artinian k-algebra, and its maximal ideal (and thus any proper ideal) is therefore nilpotent. In particular, the augmentation ideal I, which is a nonzero proper ideal (and in fact has rank $p-1$ over k as we saw in Section 2), is nilpotent and therefore has $I^2 \subsetneq I$. It follows that $I/I^2 \neq 0$, and thus (by the analysis above), there exists a nonzero k-derivation $d : A \to k$. In this entire discussion, k is being interpreted as an A-module via the counit morphism $\epsilon : A \to k$ (so in particular what we have said so far actually makes sense). We need to establish the following three facts:

(1) That $d \in A^\vee$ is in the augmentation ideal of $A^\vee$, i.e. that d is in the kernel of the dual of the structure morphism $k \to A$.
(2) That $c_{A^\vee}(d) = 1 \otimes d + d \otimes 1$.
(3) That $A^\vee = k[d]$.

[6] So that in particular $1, \dots, d^{p-1}$ form a basis for $A^\vee$ and $\{d^i \otimes d^j : 1 \leq i,j \leq p-1\}$ is a basis for $A^\vee \otimes A^\vee$

To prove (1), just recall from Theorem 1.10 that $\epsilon_{A^\vee}(d) = d \circ (k \to A) = 0$, since d is a k-derivation and therefore sends $k \subset A$ to zero. For (2), the point is that $c_{A^\vee}$ is the dual of the multiplication map $A \otimes A \to A$, so it takes $d \in A^\vee$ to the element of $(A \otimes A)^\vee$ given on pure tensors by $a \otimes b \mapsto d(ab)$. Since d is a derivation, this is in fact

$$a \otimes b \mapsto adb + bda,$$

which as an element of $(A \otimes A)^\vee = A^\vee \otimes A^\vee$ is $1 \otimes d + d \otimes 1$. (3) follows from (2), in the following sense: $c_{A^\vee}(d) = 1 \otimes d + d \otimes 1 \in k[d] \otimes k[d]$, and therefore $k[d] \subset A^\vee$ is an inclusion of bialgebras. This is not obviously good enough to deduce that $k[d]$ is a Hopf subalgebra (for example, the nonnegative integers contain the identity and are closed under addition in the group $\mathbf{Z}$ but are not closed under taking additive inverses). Luckily, there is a trick. Taking duals, the induced map

$$A \to (k[d])^\vee$$

is a surjective map of bialgebras. Since A has the further structure of a Hopf algebra, one checks that this induces a Hopf algebra structure on $(k[d])^\vee$ (e.g. by checking that the kernel of such a map is a Hopf ideal; the verification is analogous to the fact that the kernel of a multiplicative map from a group to a monoid respects taking inverses)[7]. So we see that $(k[d])^\vee$ is a closed subgroup scheme of A. But G has order p over k, so by Grothendieck's quotient construction, $(k[d])^\vee$ is either $k^\vee = k$ or all of A. Of course, d is not in k since it is in the augmentation ideal of $A^\vee$, so $\dim_k k[d] > 1$, and thus $k[d] = A$, as desired. □

As usual we see that the case where k has characteristic p is very distinguished when talking about groups of order p. Collecting all the lemmas in this section and separating based on the characteristic of k rather than the étaleness or connectedness, we have the following result.

Theorem 6.6. *Let k be an algebraically closed field, and p a rational prime. If k has characteristic not equal to p, then there is only one isomorphism class of group schemes over k of order p, e.g. the class of $(\mathbf{Z}/p\mathbf{Z})_k$. If k has characteristic p, then there exactly three isomorphism classes of k-group schemes of order p, namely $(\mathbf{Z}/p\mathbf{Z})_k, \mu_{p,k}, \alpha_{p,k}$.*

Note that we have already argued that the three group schemes in the characteristic p case of Theorem 6.6 are nonisomorphic in Proposition 2.13. Also, as a consequence of this classification, we have

Corollary 6.7. *Let k be an algebraically closed field and p a rational prime. Then all finite flat k-group schemes of order p are commutative and killed by p. Also, their corresponding Hopf algebras can be generated by a single element over k.*

Proof. This is just a reminder that the commutativity plus the fact they have order p implies they have order p (this is a theorem of Deligne which we proved using Cartier duality in Section 2). □

[7] It's kind of funny how taking the dual situation makes things easier: a monoid inside a group is not necessarily a group, but a monoid admitting a surjective morphism from a group gets a natural group structure. In any event, the reason for taking the dual when making this argument is because of the difference between these two situations.

6.2. **General classification.** Let R be a Noetherian local ring. It turns out that part of Corollary 6.7 is still valid in this context, because one can pass to that situation.

Theorem 6.8. *Any R-group scheme of order p is commutative.*

Proof. First, since R is local Noetherian, we can continue to treat "finite flat" as "free of rank p over R". The basic idea, of course, is to pass to the residue field and apply Theorem 6.6. But this doesn't actually work because R doesn't necessarily have algebraically closed residue field. So one needs to invoke a theorem from commutative algebra, due to Nagata: R injects into its *strict henselianization* R^{sh}, which is a strict henselian ring (the important thing is that it has algebraically closed residue field). For example, if $R = \mathbf{Z}_p$, we have an injection from R to the valuation ring of the maximal unramified extension of $\mathbf{Q}_p$, which we know has residue field $\overline{\mathbf{F}}_p$. In this kind of setting (i.e. where R is the valuation ring of some finite extension of $\mathbf{Q}_p$) we know exactly what to embed R into. So while citing Nagata's result gives us a more general theorem, it is not necessary for the cases we probably care the most about anyway.

Recall from Section 1.2 that the comultiplication morphism for the order-p R^{sh}-group scheme $G \times_R \operatorname{Spec} R^{\mathrm{sh}}$ is by definition the one induced by $A \to A \otimes A$ via tensoring up by R^{sh}, using the isomorphism

$$(A \otimes_R A) \otimes_R R^{\mathrm{sh}} \cong (A \otimes_R R^{\mathrm{sh}}) \otimes_{R^{\mathrm{sh}}} (A \otimes_R R^{\mathrm{sh}}).$$

Moreover, the fact that A (and thus $A \otimes A$ as well) is flat means that the natural maps

$$A \to A \otimes_R R^{\mathrm{sh}}$$

and

$$A \otimes A \to (A \otimes_R A) \otimes_R R^{\mathrm{sh}}$$

are injective (since $R \to R^{\mathrm{sh}}$ is injective). In particular, if we can show that the diagram

$$\begin{tikzcd}
A \otimes R^{\mathrm{sh}} \arrow[r] \arrow[dr] & A \otimes A \otimes R^{\mathrm{sh}} \arrow[d] \\
 & A \otimes A \otimes R^{\mathrm{sh}}
\end{tikzcd}$$

commutes, then we are done because (since the comultiplication on the base change is the one induced from the original one by base change, and one checks the same is true of the coordinate-switching map) the diagram we are interested in (the one expressing the cocommutativity of A) is just the restriction of this one to A and $A \otimes A$. So this shows that it suffices to consider the case where $k = R/\mathfrak{m}_R$ is algebraically closed. N.B.: this reduction also uses the fact that $G \times_R \operatorname{Spec} R^{\mathrm{sh}}$ has the same order over R^{sh} as G does over R, but this is a basic fact from algebra.

Now, using the reduction map $R \to k$, we can take the reduction mod $\mathfrak{m}$ of G, i.e.

$$\tilde{G} := G \times_R \operatorname{Spec} k.$$

Since k is algebraically closed, and $\tilde{G}$ is a group scheme of order p, now we can invoke Theorem 6.6 to see that $\tilde{G}$ is commutative. And therefore so is its Cartier dual, which has Hopf algebra

$$(A \otimes k)^\vee \cong A^\vee \otimes k$$

(this is an isomorphism of k-vector spaces and of noncommutative rings; we did this kind of observation in the proof of Theorem 1.11). So we have a natural Hopf algebra structure on

$A^\vee \otimes k$, even though we don't know $A^\vee$ is commutative yet. In particular, $A^\vee$ is a possibly non-commutative ring, and it is our job to deduce that it is commutative form the fact that $A^\vee \otimes k$ (sounds like a job for Nakayama) is commutative. Once $A^\vee$ is commutative as a ring, we know immediately that G is commutative as a group scheme and we are done.

Since the reduction map $R \to k$ is surjective, and $A^\vee$ is free and therefore flat, the natural map

$$A^\vee \to A^\vee \otimes_R k = (A \otimes k)^\vee$$

is surjective. By Corollary 6.7, $(A \otimes k)^\vee$ is generated as a k-algebra by a single element, so by this surjectivity, there is some $f \in A^\vee$ such that $\tilde{f} \in (A \otimes k)^\vee = A^\vee \otimes k$ generates it as a k-algebra. In particular, the R-submodule $R[f]$ of $A^\vee$ reduces mod $\mathfrak{m}$ to all of $A^\vee/\mathfrak{m}A^\vee = A^\vee \otimes k$, so by Nakayama, $R[f] = A^\vee$, which means that $A^\vee$ is in fact commutative as a ring, as desired. □

Remark 6.9. Since this is clearly local on the base, Theorem 6.8 and its proof generalize directly to group schemes of order p over an arbitrary locally Noetherian base scheme. The classification we are about to do over certain kinds of rings holds without change over schemes defined over a certain fixed ring (see Assumption 6.11), but the proof is the same. So we talk only about affine bases, keeping in mind that the global arguments from Oort–Tate are identical (you just replace the R-modules with $\mathcal{O}_S$-modules and invertible modules with sheaves).

By Theorem 1.12, we now have

Corollary 6.10. *Let R be a locally Noetherian ring of residue characteristic p. Then any R-group scheme of order p is (commutative and) killed by p.*

The point of this is that now we can view the Hopf algebra of a finite R-group scheme G as a $R[\mathbf{F}_p^\times]$-module. In particular, the fact that p kills G means that $n \in \mathbf{F}_p^\times$ acts on A by $[n] : A \to A$. This is very useful, because $R[\mathbf{F}_p^\times]$-modules are easy to control, due to some formal facts which look quite similar to the whole story on Gauss/Jacobi sums. In order for the mechanism to work, we need to make

Assumption 6.11. Assume that R is a Λ_p-algebra, where

$$\Lambda_p = \mathbf{Z}\left[\chi(\mathbf{F}_p), \frac{1}{p(p-1)}\right] \cap \mathbf{Z}_p.$$

Here $\chi : \mathbf{F}_p^\times \to \mathbf{Z}_p^\times$ denotes the Teichmüller character (except we don't make an exception when $p = 2$), extended by 0 to $0 \in \mathbf{F}_p$. We demand that Λ_p contains $(p-1)^{-1}$ in order for the mechanism (explained soon) to work, and the extra $1/p$ is sneaked in (which also forces us to intersect with $\mathbf{Z}_p$ since we don't want p to be invertible in the final product) in order for us to have

$$\Lambda_p \cap p\mathbf{Z}_p = p\Lambda_p.$$

Assumption 6.11 is not so serious: for example, Λ_p is a subring of $\mathbf{Z}_p$ so when R is the valuation ring of a finite extension of $\mathbf{Q}_p$ (the main culprit in situations we care about in arithmetic anyway), this is okay.

Remark 6.12. When $p = 2$, as we saw in Section 2, things are pretty simple. Part of the reason for this is that Assumption 6.11 becomes vacuous: $\chi(\mathbf{F}_2)$ is already contained in $\mathbf{Z}$, and 2 is not invertible in $\mathbf{Z}_2$, so $\Lambda_2 = \mathbf{Z}$.

The crucial formal mechanism takes the form of the following system of orthogonal idempotents in $R[\mathbf{F}_p^\times]$.

Lemma 6.13. *Consider the elements*

$$e_i = \frac{1}{p-1} \sum_{m \in \mathbf{F}_p^\times} \chi^{-i}(m)[m] \in \Lambda_p[\mathbf{F}_p^\times]$$

considered as elements of $R[\mathbf{F}_p^\times]$ via Assumption 6.11, defined for $i \in \mathbf{Z}/(p-1)\mathbf{Z}$, since $\chi(\mathbf{F}_p^\times)$ consists of the $(p-1)$-th roots of unity in $\mathbf{Z}_p$. The elements $\{e_i : 1 \leq i \leq p-1\}$ are a system of orthogonal idemptotents in $R[\mathbf{F}_p^\times]$ with the property that $\sum e_i = 1$.

Proof. There are three properties we must check:

(1) $e_i^2 = e_i$
(2) $e_i e_j = 0$ for $i \neq j$
(3) $\sum e_i = 1$.

For (1), we compute

$$\begin{aligned} e_i^2 &= \frac{1}{(p-1)^2} \left(\sum_{m \in \mathbf{F}_p^\times} \chi^{-i}(m)[m] \right)^2 \\ &= \frac{1}{(p-1)^2} \sum_{m,n \in \mathbf{F}_p^\times} \chi^{-i}(n)\chi^{-i}(m)[m][n] \\ &= \frac{1}{(p-1)^2} \sum_{m,n \in \mathbf{F}_p^\times} \chi^{-i}(nm)[nm] \\ &= \frac{1}{(p-1)^2} \sum_{n,a \in \mathbf{F}_p^\times} \chi^{-i}(a)[a] \\ &= \frac{|\mathbf{F}_p^\times|}{(p-1)^2} \sum_{a \in \mathbf{F}_p^\times} \chi^{-i}(a)[a] \\ &= e_i. \end{aligned}$$

For (2), we assume without loss of generality that $i < j$, and compute

$$\begin{aligned} e_i e_j &= \frac{1}{(p-1)^2} \sum_{m,n \in \mathbf{F}_p^\times} \chi^{-i}(n)\chi^{-j}(m)[m][n] \\ &= \frac{1}{(p-1)^2} \sum_{m,n \in \mathbf{F}_p^\times} \chi^{-i}(nm)\chi^{i-j}(m)[mn] \\ &= \frac{1}{(p-1)^2} \sum_{m \in \mathbf{F}_p^\times} \chi^{i-j}(m) \sum_{n \in \mathbf{F}_p^\times} \chi^{-i}(mn)[mn] \\ &= 0 \end{aligned}$$

because the sum on the inside does not depend on m, and the sum of a nontrivial character on $\mathbf{F}_p^\times$ is zero. For (3), we compute

$$\begin{aligned}\sum_{i=1}^{p-1} e_i &= \frac{1}{p-1}\sum_{i=1}^{p-1}\sum_{m\in\mathbf{F}_p^\times}\chi^{-i}(m)[m]\\ &= \frac{1}{p-1}\sum_{m\in\mathbf{F}_p^\times}\left(\sum_{i=1}^{p-1}\chi^{i}(m)\right)[m]\\ &= 1\end{aligned}$$

since the sum on the inside is equal to $p-1$ when $m=1$ and 0 otherwise (e.g. by considering it as a character sum on the pontryagin dual of $\mathbf{F}_p^\times$). □

Remark 6.14. When $p=2$, this formal mechanism degenerates completely to a single idempotent, namely 1. So these shenanigans were not necessary in Section 2, where the following analysis of the augmentation ideal boils down to the fact that it has rank 1 to begin with.

The point of this mechanism is to decompose the augmentation ideal I_G as a direct sum of rank-1 things (of which the $p=2$ case from Section 2 is a trivial example), which are simultaneous eigenspaces of the commuting operators $[m]$ for $m\in\mathbf{F}_p^\times$. The multiplicative characters $\mathbf{F}_p^\times\to\mathbf{Z}_p^\times$ are precisely the powers of $\chi:\mathbf{F}_p^\times\to\mathbf{Z}_p^\times$, so if such an eigenspace decomposition exists where the eigenvalues are in $\mathbf{Z}_p$, we expect the systems of eigenvalues to be given by powers of χ. The e_i is just an averaging operator that is supposed to project A onto the simultaneous eigenspace whose system of eigenvalues is given by χ^i (at least it is clear that it acts by the identity on χ^i-simultaneous eigenvalues). The two lemmas explain how to deduce that this is actually case. The main input is really Lemma 6.13.

Lemma 6.15. *Let $I_i=e_iI\subset A$. Then $I=\bigoplus_{i=1}^{p-1}I_i$.*

Proof. First, we must show that $I_i=e_iI\subset I$. Since I is an ideal in A, it suffices to show that $[m]$ sends I to I for all $m\in\mathbf{F}_p^\times$. The general case follows from the $m=2$ by induction, which is true because of the commutativity of the diagram

$$\begin{tikzcd}
G & G\times G \arrow[l, "m"'] & G \arrow[l, "\Delta"'] \\
 & & \operatorname{Spec} R \arrow[u, "\epsilon"] \arrow[ull, "\epsilon"]
\end{tikzcd}$$

Also, the sum $\sum_{i=1}^{p-1}I_i$ is direct, because one can recover the I_i-component of an element of this sum by applying e_i (this uses Lemma 6.13), and (also from Lemma 6.13), any $a\in I$ is in $\sum I_i$ since

$$a=\left(\sum_{i=1}^{p-1}e_i\right)a.$$

So we have established both inclusions and the directness of the sum, as desired.

□

Lemma 6.16. *$I_iI_j \subset I_{i+j}$ for all $i, j \in \mathbf{Z}/(p-1)\mathbf{Z}$, and*

$$I_i = \{f \in A : [m]f = \chi^i(m)f \text{ for all } m \in \mathbf{F}_p\}$$

Proof. First, it is clear that the first assertion follows from the second, since

$$[m](fg) = ([m]f)([m]g)$$

(no diagram chasing necessary – this is just the fact that $[m]$ is a ring homomorphism $A \to A$). To prove the second assertion, note first that one inclusion is obvious: for any $f \in A$,

$$e_if = \frac{1}{p-1}\sum_{n\in\mathbf{F}_p^\times} \chi^{-i}(n)([n]f)$$

has the property that

$$[m]e_if = \frac{1}{p-1}\sum_{n\in\mathbf{F}_p^\times} \chi^{-i}(nm^{-1})([n]f) = \chi^i(m)e_if$$

for all $m \in \mathbf{F}_p^\times$. And if $f \in I$ (which implies $e_if \in I$ by Lemma 6.15), then $[0]e_if = \epsilon(e_if) = 0$ (since $[0] : A \xrightarrow{\epsilon} R \to A$ is the definition). In fact, the converse is also clear: if $[0]f = 0$, then $f \in I$ (again this is the definition of $[0]$ and the augmentation ideal). The condition at $m = 0$ is really just expressing the fact that we are in the augmentation ideal – if we want to look at a simultaneous eigenspace decomposition of A then we can do it if we forget $m = 0$.

So at least we have the inclusion $I_i \subset \{f \in A : [m]f = \chi^i(m)f \text{ for all } m \in \mathbf{F}_p\}$. The opposite inclusion comes from the fact that $I = \bigoplus I_i$ from Lemma 6.15, because now each $f \in I$ can be expressed as a sum

$$f = \sum_{i=1}^{p-1} f_i$$

where $[m]f_i = \chi^i(m)f$ for all $m \in \mathbf{F}_p^\times$. So again by Lemma 6.15,

$$[m]f = \sum_{j=1}^{p-1} \chi^j(m)f_j$$

is equal to $\chi^i(m)f = \sum_{j=1}^{p-1} \chi^i(m)f_j$ if and only if

$$\chi^j(m)f_j = \chi^i(m)f_j$$

for each $1 \le j \le p-1$. Since the $\chi^i(m)$ are powers of a primitive $(p-1)$-th root of unity in $\mathbf{Q}_p$, they are all distinct, which means that this implies $f_j = 0$ for all $j \ne i$, and so we have the opposite inclusion. □

Remark 6.17. In these proofs and the ones to come, we say a lot of words about why one can assume that R is local. In real life, R is probably the valuation ring of a finite extension of $\mathbf{Q}_p$, especially since we won't talk about Oort–Tate's extension for global fields. So if this is the only case we care about, these proofs become somewhat shorter.

Proposition 6.18. *Each I_i is invertible (locally free of rank 1) as an R-module, and $I_1^t = I_t$ for $1 \le t \le p-1$.*

Proof. Recall from Section 2 that I is locally free of rank $p-1$, and that the same argument (using Lemma 6.15 and the fact from Nakayama that a finitely-generated projective module over a local ring is free) shows that the I_i's are locally free of rank r_i such that

$$\sum_{i=1}^{p-1} r_i = p-1.$$

Notice that we can assume that R is local: just localize everything at a prime ideal of R, and use the fact that the augmentation ideal is compatible with localization, because localization is exact and the coidentity morphism is compatible with base change (in fact the definition of the coidentity morphism is the one that comes from base change so this is a tautology). The fact that the I_i's are compatible with base change is immediate from this because of how they are defined via the action of $\Lambda_p[\mathbf{F}_p^\times]$. Even for the second part of the statement we are allowed to assume that R is local, because base change preserves products of submodules and because if the induced map $I_1^t \otimes R_\mathfrak{p} \to I_t \otimes R_\mathfrak{p}$ is surjective for all $\mathfrak{p}$ then the original inclusion $I_1^t \to I_t$ must have been surjective to begin with as well.

Now that R is local, the I_i are free of rank r_i. But we aren't done with the base-changing just yet. In fact, the augmentation ideal is compatible with arbitrary base-change, because of the splitting of the exact sequence

$$0 \to I \to A \to R \to 0.$$

So by the same arguments as above, to show that I_i has rank 1, we can assume that R is an algebraically closed field by base changing to the algebraic closure of the residue field. For the part about $I_1^t = I_t$, again since multiplication of submodules is preserved by arbitrary base change, if we want to assume that $R = \overline{k}$ it suffices to show that

$$I_1^t \otimes \overline{k} = I_t \otimes \overline{k} \implies I_1^t = I_t,$$

where $k = R/\mathfrak{m}_R$ is the residue field of R. First of all, by linear algebra (dimension considerations), equality of the base changes to $\overline{k}$ at least implies it for k. So we just need to show

$$I_1^t \otimes k = I_t \otimes k \implies I_1^t = I_t.$$

But this is just Nakayama's lemma.

Now we have reduced to the case where R is an algebraically closed field $k = \overline{k}$. But in this setting, we know that there are only three possibilities, according to Theorem 6.6. So we just need to check that this result holds for $G = (\mathbf{Z}/p\mathbf{Z})_k$ if k has characteristic not equal to p, and for $\alpha_{p,k}, \mu_{p,k}$ if k has characteristic p. The property that all of these have in common is that there exists an $f_1 \in I_1$ such that $f^i \neq 0$ for all $1 \leq i \leq p-1$. Then by dimension considerations and Lemma 6.16, $I_1, \ldots, I_{p-1}$ all have rank at least 1, and since $\sum r_i = p-1$, it implies they have rank exactly one. And since k is a field, the fact that $f^t \neq 0$ would imply also by dimension consderations that $I_1^t = I_t$. In the case of $G = (\mathbf{Z}/p\mathbf{Z})_k$, A is the algebra of k-valued functions on $\mathbf{Z}/p\mathbf{Z}$, and the $\mathbf{F}_p^\times$-action is given by $[m]f(n) = f(nm)$. So χ itself (treated as a function from $\mathbf{F}_p$ to k via Assumption 6.11) is in I_1 (e.g. by Lemma 6.16). And the powers of χ are nonzero functions on $\mathbf{Z}/p\mathbf{Z}$, so this is okay.

Next we do $\alpha_{p,k}$. Its Hopf algebra is $A = k[T]/T^p$, with comultiplication $T \mapsto 1 \otimes T + T \otimes 1$ (see Section 2). The multiplication-by-m is induced by the one on $\mathbf{G}_{a,k}$, i.e.

$$[m]T = mT.$$

Again, the fact that k has characteristic p means that $m = \chi(m)$ in k, since they are congruent[8] modulo p in R by the definition of χ. So by Lemma 6.16, $T \in I_1$. By definition of A, the first $p-1$ powers of T are nonzero (though the p-th one is), so this case is also okay.

The final case $\mu_{p,k}$ is similar to $\alpha_{p,k}$ but is more important because a detailed understanding of this example is necessary to prove the full classification. We have $A = k[T]/(T^p - 1)$, and $[m]$ defined by

$$[m]T = T^m$$

since it is induced by the group structure on $\mathbf{G}_{m,p}$. The counit $A \to R$ is given by $T \mapsto 1$, so the augmentation ideal is

$$I = (T-1) \cdot A.$$

Moreover,

$$[m](T-1) = T^m - 1 = (T-1)(1 + \cdots + T^{m-1}) \equiv m(T-1) \mod (T-1)^2.$$

Again, because of Assumption 6.11, we have $m = \chi(m)$ in k, and therefore

$$\begin{aligned} e_1(T-1) &= \frac{1}{p-1} \sum_{m=1}^{p-1} \chi(m)^{-1}[m](T-1) \\ &\equiv \frac{1}{p-1} \sum_{m=1}^{p-1} \chi(m)^{-1}\chi(m)(T-1) \mod (T-1)^2 \\ &\equiv T-1 \mod (T-1)^2 \end{aligned}$$

is in I_1 and is nonzero due to being congruent to $T-1 \bmod (T-1)^2$. We have $A = k[T-1]/(T-1)^p$ since k has characteristic p, so we can deduce that $e_1(T-1)^t \neq 0$ for $t = 1, \ldots, p-1$ (but no further) and thus the proposition is proved. □

The three examples which are the basis for the proof of Proposition 6.18 are independently interesting on their own as examples of this formal mechanism. The computations are still essentially valid over the more general R (though we probably still want Assumption 6.11).

Example 6.19 (Decomposition of the augmentation ideal for α_p)**.** Let R be a ring of characteristic p satisfying Assumption 6.11, and consider $\alpha_{p,R} = \operatorname{Spec} R[T]/T^p$. The augmentation ideal is the kernel of $\epsilon : T \mapsto 0$, and is therefore generated as an ideal by T. The resulting decomposition

$$I = \bigoplus_{i=1}^{p-1} R \cdot T^i$$

coincides with the decomposition into I_i's, as one can check by explicit computation using the definition of e_i or by checking that these are the appropriate eigenspaces.

The importance of this decomposition of the augmentation ideal is that it allows us to encode the scheme structure of G with very little data:

[8] In in order to conclude that m and $\chi(m)$ differ by a multiple of p in R, we need to use the part of Assumption 6.11 that tells us $p\mathbf{Z}_p \cap \Lambda_p = p\Lambda_p$. This subtle part of the assumption is crucial here, and in the future as we continue to look at things mod p.

Lemma 6.20. *Let G be a group scheme of order p over R, and define the decomposition $I_G = \bigoplus I_i$ as above. Let $\mathrm{Sym}^\bullet I_1$ be the symmetric algebra over R, defined by*

$$\mathrm{Sym}^\bullet I_1 = \bigoplus_{i=0}^{\infty} \mathrm{Sym}^i I_1.$$

The natural map $I_1 \to A$ induces a surjective ring homomorphism $\varphi : \mathrm{Sym}^\bullet I_1 \to A$ with kernel equal to ideal generated by $(a-1)\mathrm{Sym}^p I_1$, where

$$a \in \mathrm{Hom}_{\mathsf{Mod}_R}(\mathrm{Sym}^p I_1, I_1)$$

is the map induced by the ring multiplication of A.

Proof. First, as indicated in the notation of [14], the fact that we are talking about $\mathrm{Sym}^\bullet$ is artificial: the projection

$$I^{\otimes i} \to \mathrm{Sym}^i I$$

is (by Proposition 6.18) locally the isomorphism of free rank-1 $R_{\mathfrak{p}}$-modules

$$R_{\mathfrak{p}}^i \to \mathrm{Sym}^i R_{\mathfrak{p}}$$

(in particular in a free $R_{\mathfrak{p}}$-module of finite rank, pure tensors are clearly invariant under permutations). So the map $I^{\otimes i} \to \mathrm{Sym}^i I$ itself is an isomorphism. Similarly, for $1 \le t \le p-1$, the multiplication map

$$I_1^{\otimes t} \to I_1^t$$

is, by Proposition 6.18, a map of locally free rank-1 R-modules, and it is equal to the restriction of the multiplication map $A \otimes A \to A$. So for any prime $\mathfrak{p}$, it localizes to the the restriction[9] to $I_{1,\mathfrak{p}} \otimes I_{1,\mathfrak{p}}$ of the multiplication map $A_{\mathfrak{p}} \otimes A_{\mathfrak{p}} \to A_{\mathfrak{p}}$. But by Proposition 6.18, this localization is a map of free R-modules of rank 1, and we can choose identifications of $I_{1,\mathfrak{p}}$ with R such that it is the multiplication isomorphism $R \otimes R \to R$. So (only for $1 \le t \le p-1$) the map

$$I_1^{\otimes t} \to I^t = I_t$$

is an isomorphism. The induced map

$$\varphi : \mathrm{Sym}^\bullet I_1 = R \oplus \bigoplus_{t=1}^{\infty} I_1^{\otimes t} \to A = R \oplus \bigoplus_{t=1}^{p-1} I_1^t$$

(here we have used Proposition 6.18 and Lemma 6.15) is given by this isomorphism $I_1^{\otimes t} \to I_1^t$ for $1 \le t \le p-1$ (and we see in particular that φ is surjective). By Lemma 6.16, φ is equal to the direct sum of the identity map $R \mapsto R$ and the multiplication maps

$$\varphi_t : \bigoplus_{\substack{i \ge 1 \\ i \equiv t \pmod{p-1}}} I_1^{\otimes i} \to I_1^t.$$

The fact that $a \in \mathrm{Hom}_{\mathsf{Mod}_R}(I_1^{\otimes p}, I_1)$ in the first place also comes from Lemma 6.16. The elements of $(a-1)I_1^{\otimes p}$ are in the codomain of φ_1 and clearly map to zero under φ_1 (and therefore φ), since $a : I_1^{\otimes p} \to I_1^p \subset I_1$ is the definition of $\varphi_1|_{I_1^{\otimes p}}$. So the ideal generated by $(a-1)I_1^{\otimes p}$ is contained in the kernel of φ. To check the reverse inclusion, it suffices to check

[9] We have no problems thinking about restrictions here, since A and I_1 are flat (since I_1 is invertible).

that $\ker \varphi_t$ is contained in this ideal for all $1 \leq t \leq p-1$. For now, let $t = 1$. For $k \geq 1$, we have $\varphi_1|_{I_1^{\otimes(1+k(p-1))}} = a \circ \sigma_1 \circ \cdots \circ \sigma_{k-1}$, where

$$\sigma_n : I_1^{\otimes(1+(n+1)(p-1))} \to I_1^{\otimes(1+n(p-1))}$$

is defined on pure tensors by the identity on the first $n(p-1)$ coordinates and by a on the next p. In other words, $\sigma_n = I^{\otimes n(p-1)} \otimes a$. So taking the decomposition of an element of $\ker \varphi_1$,

$$z = x + \sum_{k=1}^{N} y_k \in \ker \varphi_1$$

where $x \in I_1$ and $y_k \in I_1^{\otimes(1+k(p-1))}$. That $\varphi_1(z) = 0$ is then equivalent to

$$x = -\sum_{k=1}^{N} a \circ \sigma_1 \circ \cdots \circ \sigma_{k-1} y_k,$$

i.e.

$$z = \sum_{k=1}^{N} y_k - a \circ \sigma_1 \circ \cdots \circ \sigma_{k-1} y_k.$$

So it suffices to show that $y - a \circ \sigma_1 \circ \cdots \circ \sigma_{k-1} y$ is in the ideal generated by $(a-1)I^{\otimes p}$, for any $y \in I_1^{(1+k(p-1))}$. That is because

$$y - a\sigma_1 \cdots \sigma_{k-1} y = \left(\sum_{i=0}^{k-2} \sigma_{k-i} \cdots \sigma_{k-1} y - \sigma_{k-i-1} \cdots \sigma_{k-1} y \right) + \sigma_1 \cdots \sigma_{k-1} y - a\sigma_1 \cdots \sigma_{k-1} y.$$

The last term is a bona fide element of $(a-1)I_1^{\otimes p}$. By looking at pure tensors and the definition of the σ_i's, we also see that the term

$$\sigma_{k-i} \cdots \sigma_{k-1} y - \sigma_{k-i-1} \cdots \sigma_{k-1} y \in I_1^{\otimes(k-i-1)(p-1)} (a-1) I_1^{\otimes p},$$

which proves the desired inclusion

$$\ker \varphi_1 \subset (\mathrm{Sym}^\bullet I_1) \cdot (a-1) I_1^{\otimes p}.$$

But since $\varphi_t = I_1^{\otimes(t-1)} \otimes \varphi_1$, the fact that I_1 is flat (and thus its tensor powers are all flat) means that

$$\ker \varphi_t = I_1^{\otimes(t-1)} \otimes \ker \varphi_1$$

so we are done. □

Remark 6.21. Notice that it isn't necessary for many applications to think as carefully as we just did: instead of explicitly writing own the kernel of φ, we could have just argued that it doesn't depend on anything other than I_1 and α.

Corollary 6.22. *The ring structure of A (and thus the structure of G as an affine R-scheme) is completely determined by the following two pieces of information:*

1. *The invertible R-modules I_1.*
2. *The morphism $a : I_1^{\otimes p} \to I_1$.*

Applying Corollary 6.22 to both G and $G^\vee$, we see that we actually need fewer pieces of information to determine both G and $G^\vee$ as R-schemes. That is because of

Lemma 6.23. *Let $I(G)$ denote the augmentation ideal of A, and $I_i(G)$ denote the invertible R-submodule I_i of A. Then $I(G)^\vee \cong I(G^\vee)$ and $I_i(G)^\vee \cong I_i(G^\vee)$ in the category of R-modules.*

Proof. For the first part, recall from Section 2 that the exact sequence

$$0 \to I \to A \xrightarrow{\epsilon} R \to 0$$

is split via the structure morphism $R \to A$, so we can define another split exact sequence

$$0 \to R \to A \to I \to 0.$$

The fact that this sequence is split means that applying the contravariant functor $(\cdot)^\vee$ preserves exactness, and thus

$$0 \to I^\vee \to A^\vee \to R \to 0$$

is exact. The map $A^\vee \to R$ dual to the structure morphism $R \to A$ is the counit morphism for $A^\vee$, as described in Theorem 1.10, so this shows we have the desired natural isomorphism

$$I^\vee \to I_{G^\vee}.$$

From Lemma 6.15, this means we have an isomorphism

$$\varphi : \bigoplus_{i=1}^{p-1} I_i(G)^\vee \to \bigoplus_{i=1}^{p-1} I_i(G^\vee),$$

and we just need to show that φ takes $I_i(G)^\vee$ to $I_i(G^\vee)$. Here $I_i(G)^\vee$ is included in $I(G)^\vee$ as the set of linear functionals which are zero outside of I_i. By Lemma 6.16, this means that

$$I_i(G)^\vee = \{f \in I(G)^\vee : [m]_G^\vee f = \chi^i(m) f \text{ for all } m \in \mathbf{F}_p^\times\},$$

and thus (also by Lemma 6.16) it suffices to show that the diagram

$$\begin{tikzcd}
I(G)^\vee \arrow[r, "\varphi"] \arrow[d, "{[m]_G^\vee}"] & I(G^\vee) \arrow[d, "{[m]_{G^\vee}}"] \\
I(G)^\vee \arrow[r, "\varphi"] & I(G^\vee)
\end{tikzcd}$$

commutes for all $m \in \mathbf{F}_p^\times$. The point is that (from the definition) φ is given by taking a functional on $I(G)$ and extending it by zero to all of A. So it really suffices to show that the maps $[m]_G^\vee, [m]_{G^\vee} : A^\vee \to A^\vee$ coincide. But this is a fact of life: it follows from the definition of $[m]$ and the group object morphisms attached to $G^\vee$ (see Theorem 1.10). □

Corollary 6.24. *The schemes G and $G^\vee$ are uniquely determined by the following information:*

(1) *The invertible R-module $I_1(G)$*
(2) *The map $a_G : I_1^{\otimes p} \to I_1$*
(2) *The map $a_{G^\vee} : (I_1^\vee)^{\otimes p} \to I_1^\vee$.*

This information doesn't tell us about the group scheme structure of G until we get our hands on the Cartier morphism $G \times G^\vee \to \mathbf{G}_{m,R}$. That morphism factors through $\mu_{p,R}$ due to Corollary 6.10. So we need to understand in more detail the decomposition Lemma 6.15 and Proposition 6.18 in the example of $\mu_{p,R}$.

Let I_{μ_p} be the augmentation ideal of $\mu_{p,R}$. Since $R[T] = R[T-1]$, and the counit map is $\epsilon : T \mapsto 1$, we see that

$$I_{\mu_p} = (T-1) \cdot A$$

as in the proof of Proposition 6.18. In particular, there is a direct sum decomposition

$$I_{\mu_p} = (T-1) \cdot R \oplus \cdots \oplus (T-1)^{p-1} \cdot R.$$

This is to be expected, since we have a unit-section-respecting isomorphism of schemes $\alpha_p \cong \mu_p$. But the hope is that the eigenspace decomposition of the augmentation ideals will be able to distinguish them as group schemes, which is indeed what we saw in the proof of Proposition 6.18: this decomposition of I is not actually the eigenspace decomposition. To construct explicitly the decomposition, we cannot rigorously just take $e_i(T-1)$ and use Nakayama's lemma to deduce that it generates all of $e_i I_{\mu_p}$: this is only valid when R is assumed to be a local ring. Instead, the decomposition above only guarantees that $e_i I$ is generated over R by the powers of $e_i(T-1)$. But we can explicitly check that this is enough[10] by explicitly computing[11] for $i = 1, \ldots, p-1$,

$$\begin{aligned} y_i &:= e_i(T-1) \\ &= \frac{1}{p-1} \sum_{m \in \mathbf{F}_p^\times} \chi^{-i}(m)[m](T-1) \\ &= \frac{1}{p-1} \sum_{m \in \mathbf{F}_p^\times} \chi^{-i}(m)(T^m - 1) \\ &= \frac{1}{p-1} \sum_{m \in \mathbf{F}_p^\times} \chi^{-i}(m) T^m - \sum_{m \in \mathbf{F}_p^\times} \chi^{-i}(m) \\ &= \frac{1}{p-1} \sum_{m \in \mathbf{F}_p^\times} \chi^{-i}(m) T^m - \delta_{i,p-1}(p-1). \end{aligned}$$

The standard trick is that one may recover the quantity $T^m - 1$ as a linear combination of these y_i's, and one can check that

$$T^m - 1 = \sum_{i=1}^{p-1} \chi^{-1}(m) y_i.$$

From the identity $T^m - 1 = (T-1)(1 + \cdots + T^{m-1})$, we know that the elements $\{T^m - 1 : m = 1, \ldots, p-1\}$ span all of $I_{\mu_p} = (T-1)A$, and therefore we have checked explicitly that the $y_i = e_i(T-1)$ span all of I. So by Lemma 6.13, they in fact form a basis, and $I_{\mu_p,i} = R \cdot e_i(T-1)$. So for the special case of μ_p under Assumption 6.11, the simultaneous eigenspaces I_i are not just locally free, but free over R of rank 1.

[10] This is what Oort-Tate does, at least. I would be curious to know if there is a way to prove this by pure thought, but I doubt it because in general these things aren't necessarily free over R despite being invertible.

[11] N.B.: our convention differs from Oort–Tate here by a factor of $p-1$. It doesn't matter because $p-1$ is supposed to be invertible in R.

Also, by the second part of Proposition 6.18, we have $R \cdot e_1(T-1)^t = I_t = R \cdot e_t(T-1)$, so in fact[12]

$$w_t := \frac{y_1^t}{y_t} \in R^\times$$

for all $t = 1, \ldots, p-1$. In fact, this quantity w_t is still defined for larger t, since y_t and I_t only depend on the value of $t \mod p-1$ and thus y_1^t is an R-multiple of y_t (though it won't be a unit for $t \geq p$). Most importantly, we have

$$y_1^p = w_p y_1.$$

The constants w_p live in Λ_p, and can be computed explicitly in terms of Jacobi sums (this is what is done in [14, p. 10-11]). So we have shown

Lemma 6.25. *$A_{\mu_{p,R}} = R[y_1]$, where $y_1 \in A_{\mu_{p,R}}$ satisfies $y_1^p = w_p y_1$.*

The key point is that the information in Corollary 6.24 also determines the Cartier morphism $G \times G^\vee \to \mu_{p,R}$:

Proposition 6.26. *Let*

$$\varphi : R[y_1] \to A \otimes A^\vee$$

be the ring map corresponding to the Cartier duality morphism $G \times G^\vee \to \mu_{p,R}$, using Corollary 6.10 and Lemma 6.25. Also, let $a : I_1^{\otimes p} \to I_1$ and $a' : I_1^{\vee \otimes p} \to I_1^\vee$ be the maps from Corollary 6.24. Then $I_1 \otimes I_1^\vee \subset A \otimes A^\vee$ is a rank-1 free R-module generated by $\varphi(y_1)$, and the map

$$a \otimes a' : (I_1 \otimes I_1^\vee)^{\otimes p} \to I_1 \otimes I_1^\vee$$

is given by

$$(a \otimes a')((\varphi y_1)^{\otimes p}) = w_p \cdot \varphi(y_1)$$

(this determines the map $a \otimes a'$ since $(\varphi y_1)^{\otimes p}$ generates the rank-1 free R-module $(I_1 \otimes I_1^\vee)^{\otimes p}$)

Proof. First, we show that φy_1 actually lands in $I_1 \otimes I_1^\vee$. By Lemma 6.15, we have

$$A \otimes A^\vee = \bigoplus_{0 \leq i,j \leq p-1} I_i \otimes I_j^\vee,$$

where we go by the convention $I_0 = R$. By Lemma 6.16 and Lemma 6.23, $I_i \otimes I_j^\vee$ is the $\chi^i \otimes \chi^j$-simultaneous eigenspace of the action of $\mathbf{F}_p^\times \times \mathbf{F}_p^\times$ on $A \otimes A^\vee$ (in particular, it is the set of $x \in A \otimes A^\vee$ such that $([m] \otimes [n])x = \chi^i(m)\chi^j(n)x$ for all $m, n \in \mathbf{F}_p^\times$). So we just need to check that

$$([m] \otimes [n])\varphi(y_1) = \chi(m)\chi(n)\varphi(y_1).$$

This is true because the Cartier duality morphism $G \times G^\vee \to \mu_{p,R}$ is a pairing of group objects (clear from the construction of this morphism on points via Theorem 1.11), and so the diagram

$$\begin{tikzcd}
G \times G^\vee \arrow[r] \arrow[d, "{[m]_G \times [n]_{G^\vee}}"] & \mu_p \arrow[d, "{[mn]_{\mu_p}}"] \\
G \times G^\vee \arrow[r] & \mu_p
\end{tikzcd}$$

[12] N.B.: Because our convention for the normalization of y_i differs from that of Oort–Tate, our values of w_t are different as well.

commutes. As a result,

$$([m] \otimes [n])\varphi(y_1) = \varphi([mn]y_1) = \chi(mn)\varphi(y_1),$$

as desired, since $y_1 \in I_{1,\mu_p}$ to begin with. The fact that $I_1 \otimes I_1^\vee$ is generated by $\varphi(y)$ is because of the fact that the Cartier pairing is nondegenerate (see Theorem 1.11): since Cartier duality is compatible with base change, it suffices (by the same local to global argument we have already used in this section) to show this in the case where R is a local ring, and (also by compatibility with base change and Nakayama's lemma) in fact we may assume that $R = k$ is a field, and thus $I_1 \otimes I_1^\vee$ is a k-vector space of rank 1. It is therefore reduced to showing that $\varphi(y_1) \neq 0$, which is true because the Cartier duality morphism is nondegenerate (if $\varphi(y_1) = 0$ then the morphism $G \times G^\vee \to \mu_p$ would factor through the identity map $\operatorname{Spec} k \to \mu_p$ which means that the isomorphism $G(S) \to \operatorname{Hom}_{\mathsf{GrpSch}_{/k}}(G^\vee \times S, \mu_{p,S})$ implies $G(S)$ is trivial for all k-algebras S; so G cannot have order $p > 1$).

The second part of the statement, that

$$(a \otimes a')(\varphi(y_1)^{\otimes p}) = w_p\varphi(y_1),$$

is because by Lemma 6.25,

$$w_p\varphi(y_1) = \varphi(y_1^p) = \varphi(y_1)^p = (a \otimes a')(\varphi(y_1)^{\otimes p})$$

by definition of a and a' as the multiplication maps $I_1^{\otimes p} \to I_1$ and $I_1^{\vee\otimes p} \to I_1^\vee$. □

So the key insight is that the maps a and a' give a lot of information about the Cartier duality morphism, and it turns out that this is enough to determine G as a group scheme.

Let $\{G\}$ be the set of isomorphism classes of R-group schemes of order p, and $\{(L, a, b)\}$ the set of isomorphism classes of triples consisting of an invertible R-module L, and R-module maps $a : L^{\otimes p} \to L$, $b : (L^\vee)^{\otimes p} \to L^\vee$, with the property that there exists a generator x of $L \otimes L^\vee = R$ such that $(a \otimes b)x^{\otimes p} = w_p x$. Two triples (L, a, b) and (L, a', b') are considered isomorphic if there is an isomorphism between L and L' that takes a to a' and b to b'. The theory developed so far gives us a map

$$F : \{G\} \to \{(L, a, b)\}$$

taking G to (I_1, a, a').

Theorem 6.27. *F is injective.*

Proof. This comes down to showing that (I_1, a, a') determines the isomorphism class of G as an R-group scheme (i.e. given a triple (I_1, a, a') coming from G we can reconstruct G up to isomorphism). We know (Corollary 6.24) that this data determines G and $G^\vee$ as schemes. The key point is that once we know the morphism $G \times G^\vee \to \mu_{p,R}$, we also know the group structure on G. This is because of the fact that this morphism provides the isomorphisms of groups from Theorem 1.11, namely

$$G(S) \to \operatorname{Hom}_{\mathsf{GrpSch}_R}(G^\vee \times_R S, \mu_{p,S})$$

and in particular knowing the morphism $G \times G^\vee \to \mu_{p,R}$ gives you an inclusion of groups

$$G(S) \to \operatorname{Hom}_{\mathsf{Sch}_R}(G^\vee \times_R S, \mu_{p,S})$$

so it tells you what the functor $G : \mathsf{Sch}_R \to \mathsf{Grp}$ is, which determines G up to isomorphism by Lemma 1.4. So it suffices to determine the Cartier morphism from (I_1, a, a'), which is where Proposition 6.26 comes in. That morphism is determined by $\varphi(y_1)$, which by Proposition 6.26 is a generator of $I_1 \otimes I_1^\vee \subset A \otimes A^\vee$ with the property that $(a \otimes a')(\varphi(y_1)^{\otimes p}) = w_p\varphi(y_1)$. The information we have already means that we know $I_1, I_1^\vee, A, A^\vee, a, a', a \otimes a', y_1$, and w_p. We are looking for a generator x of the free rank-1 R-module $I_1 \otimes I_1^\vee$ with the property that $(a \otimes a')(x^{\otimes p}) = w_p x$. We have shown that $\varphi(y_1)$ is one such a generator. All other generators are of the form $u \cdot \varphi(y_1)$ for some $u \in R^\times$, but if this was also true for $u \cdot \varphi(y_1)$, we would have

$$(a \otimes a')(u^p \varphi(y_1)^{\otimes p}) = u\varphi(y_1),$$

which means u must be a $(p-1)$-th root of unity. In other words, the data (L, a, b) at least determines $\varphi(y_1)$ up to a $(p-1)$-th root of unity. It turns out that this determines G up to isomorphism, because if u is a $(p-1)$-th root of unity there is an isomorphism of group schemes

$$G \times G^\vee \to G \times G^\vee$$

given by the identity on $G^\vee$, and for G, the ring map $A \to A$ given by multiplication by u on I_1, such that we know the composition

$$G \times G^\vee \to G \times G^\vee \to \mu_p.$$

So the information we are given is enough to determine *some* nondegenerate pairing $G \times G^\vee \to \mu_p$, which (by the above argument) is good enough to determine G up to isomorphism as a group scheme. □

Oort–Tate also showed that F is surjective, by exhibiting the preimages explicitly.

The easiest example to think about is the one where all invertible R-modules are free of rank 1. For example R could be a local ring. The most important example to us is $R = \mathbf{Z}_p$ or the valuation ring of a finite extension of $\mathbf{Q}_p$. In this case, there is only one possibility for the R-module L up to isomorphism, namely R, and a and b are just elements of $\mathrm{End}(R) = R$ with the property that $ab = w_p$. The element w_p is determined up to a unit via the choice of generator of L, and changing this generator by a unit u means multiplying a by u^{p-1} and b by u^{1-p}. So in the end we get something which is very similar to what we saw when $p = 2$ in Section 2: the isomorphisms of $\mathbf{Z}_p$-group schemes of order p come as $G_{a,b}$'s, where $ab = p$ (since $v_p(w_p) = p$, as shown in [14]). Since the notion of equivalence is a little bit more coarse than when $p = 2$, we get more group schemes than we did over $\mathbf{Z}_2$, where there were only 2. In particular,

$$[\mathbf{Z}_p^\times : (\mathbf{Z}_p^\times)^{p-1}] = p - 1$$

(see [7, §II.3]) so up to isomorphism there are $2(p-1)$ group schemes of order p over $\mathbf{Z}_p$ (the factor of 2 comes from whether $v_p(a) = 1$ and $v_p(b) = 0$ or vice versa).

7. p-divisible groups

This section is about what we read in Tate's famous paper *p-divisible groups*. Let A be an abelian variety over a local field K of residue characteristic p. The Néron–Ogg–Shavarevich criterion (proved by Serre–Tate [10]) says that if $\ell \neq p$, A has good reduction at p if and only if the ℓ-adic Tate module of A is unramified as a representation of $\mathrm{Gal}(\overline{K}/K)$. But when $\ell = p$, the situation is more complicated. The problem is that one cannot simply look at the geometric points of $A[p^\infty]$, because the group schemes $A[p^n]$ are no longer guaranteed to be étale. For example, if A is a supersingular elliptic curve, then when you base change to the residue field $\mathbf{F}_p$ the p-adic Tate module will be trivial. This is not a proof of anything, but maybe suggests that rather than simply looking at geometric points, one gains information in the $\ell = p$ case by thinking of $A[p^\infty]$ as a p-divisible group, namely the inductive system of commutative group schemes

$$A[p] \to A[p^2] \to \cdots \to A[p^n] \to \cdots ,$$

and by getting a p-adic Galois representation out of that instead. Assume that A has good reduction, so we can assume that A is an abelian scheme over $\mathcal{O}_K$. Recall from Section 2 that $A[p^\infty]$ is a p-divisible group of height $2d$ over $\operatorname{Spec} \mathcal{O}_K$, where d is the relative dimension of A over $\operatorname{Spec} \mathcal{O}_K$. This means that $A[p^i]$ is a finite flat commutative $\mathcal{O}_K$-group scheme of order $p^{ih} = p^{2id}$ included in $A[p^{i+1}]$ as the kernel of p^i (see Section 1.2). That is really the most relevant example of a p-divisible group. Here is another:

Example 7.1. Let $G = \mu_{p^\infty}$, that is the inductive system

$$\mu_p \to \mu_{p^2} \to \cdots .$$

This is a p-divisible group of height 1.

For a p-divisible group $G/\mathcal{O}_K$ given by the inductive system

$$G_1 \to G_2 \to \cdots \to G_i \to \cdots ,$$

we can also produce the projective system that is used in the definition of the Tate module, using the multiplication-by-p maps

$$G_{i+1} \to G_i.$$

Taking the Cartier dual, we get another inductive system

$$G_1^\vee \to G_2^\vee \to \cdots \to G_i^\vee \to \cdots ,$$

which one checks is also a p-divisible group of the same height h. In Section 2, we saw that $\mu_n^\vee \cong \mathbf{Z}/n\mathbf{Z}$, so we have

Example 7.2. The p-divisible group $G = \mu_{p^\infty}$ of height 1 is dual to $G^\vee = \mathbf{Q}_p/\mathbf{Z}_p = \varinjlim \mathbf{Z}/p^n\mathbf{Z}$, also of height 1.

Since the functor taking a finite flat $\mathcal{O}_K$-group scheme to its étale or connected part is exact, there is a well-defined notion of the étale and connected parts of a p-divisible group. The connected part appears to be less familiar: only the information in the étale part is captured by the p-adic Tate module, since it is obtained by taking $\overline{K}$-points in each G_i. Understanding the connected part is where the theory of formal groups comes in. The corresponding formal group is how one writes down the "points" of a p-divisible group, and is how one defines the tangent space. The Hodge–Tate decomposition, which is the main goal of this section of these notes, shows that the extra information of the connected part (namely the tangent and cotangent spaces) determines a decomposition of the rational p-adic Tate module (which we mentioned comes from the étale part of G) as a p-adic Galois representation.

7.1. **Formal groups and connected p-divisible groups.** The category of connected simply-connected n-dimensional Lie groups is nice because it is equivalent to the category of n-dimensional Lie algebras. Unfortunately, in the residue characteristic p setting, the Lie algebra does not contain enough information. Serre and Tate proved that what does contain enough information is the formal group corresponding to G (here G is a connected p-divisible group). Unlike the Lie algebra functor, the most straightforward thing is to construct the connected p-divisible group from the formal group. Given a group scheme on its own, it's natural to take a formal completion at the origin, but this is an inductive limit of group schemes, so one needs to check a bit more in order to see that you can actually recover a formal group from a p-divisible group.

Definition 7.3. Let $\mathscr{A}_n = \mathcal{O}_K[[X_1, \ldots, X_n]]$. A *n-dimensional formal group* over $\mathcal{O}_K$ (i.e. over $\mathrm{Spf}\mathcal{O}_K$) is a ring homomorphism

$$\psi : \mathscr{A}_n \to \mathscr{A}_n \widehat{\otimes}_{\mathcal{O}_K} \mathscr{A}_n = \mathcal{O}_K[\![X_1, \ldots, X_n, Y_1, \ldots, Y_n]\!]$$

satisfying the conditions for a commutative co-group object. In other words, it is the data of a group object in the category of formal $\mathrm{Spf}\mathcal{O}_K$-schemes where the underlying formal scheme is $\mathrm{Spf}\mathscr{A}_n$ with ideal of definition $\mathscr{J}_n = (X_1, \ldots, X_n)$, i.e. the $\mathscr{J}_n$-adic topology. Such a formal group is *p-divisible* if the associated p-th power map

$$[p] : \mathscr{A}_n \to \mathscr{A}_n$$

makes $\mathscr{A}_n$ into a free module of finite rank over itself[13]. That rank is a power of p, and the h such that the rank is p^h is called the *height* of ψ.

The only part of the definition we haven't justified is why the rank is a power of p. The most canonical way of going about this requires some more theory (see [5, §28.2]). At least I do not know how to go about it in general without some Cartier–Dieudonné theory, though in the 1-dimensional case it is much easier.

A p-divisible formal group $\mathscr{G} = (\mathscr{A}_n, \psi)$ yields a bona fide *connected* p-divisible group G via

$$G_i = \ker[p]^i,$$

the scheme-theoretic zero locus of $[p]^i$, which here stands for the map of formal schemes corresponding to the one $\mathscr{A}_n \to \mathscr{A}_n$ mentioned above. More concretely,

$$G_i = \ker[p]^i = \mathrm{Spec}(\mathscr{A}_n/[p]^i(\mathscr{J}_n)\mathscr{A}_n).$$

This forms a p-divisible group of height h, where h is the same as the height of the p-divisible formal group $\mathscr{G}$. In particular, $\mathscr{A}_n/[p](\mathscr{J}_n)\mathscr{A}_n$ is finite flat over $\mathcal{O}_K$ with rank p^h, and $\mathscr{A}_n/[p]^i(\mathscr{J}_n)\mathscr{A}_n$ is finite flat of rank p^{ih}. The reason G_i is connected is simply because $\mathscr{A}_n$, and therefore $\mathscr{A}_n/[p]^i(\mathscr{J}_n)\mathscr{A}_n$, is a local ring.

So we have defined a functor $\mathscr{F}$

$$\{p-\text{divisible formal groups over } \mathcal{O}_K \text{ of height } h\} \to \{p-\text{divisible } \mathcal{O}_K-\text{groups of height } h\}$$

given by

$$\mathscr{G} \mapsto G = \{G_i\}.$$

What about going the other way? In principle, one should be able to recover $\mathscr{G}$ by literally taking the direct limit of group schemes

$$\varinjlim G_i.$$

Example 7.4. Consider the p-divisible group $G = \mathbf{G}_m[p^\infty]$. We have

$$G_i = \mu_{p^i}.$$

The corresponding p-divisible formal group is $\mathbf{G}_m$, which is the 1-dimensional formal group law given by $\psi(X) = X + Y + XY$. The p-th power map is

$$\mathcal{O}_K[\![X]\!] \to \mathcal{O}_K[\![X]\!]$$

[13] In other words, $[p]$ is an isogeny of formal groups

$$X \mapsto (1+X)^p - 1$$

which means that from $\mathscr{G} = \mathbf{G}_m$, applying the functor $\mathscr{F}$ indeed yields

$$G_i = \operatorname{Spec} \mathcal{O}_K[\![X]\!]/((1+X)^{p^i} - 1) \cong \operatorname{Spec} \mathcal{O}_K[X]/((1+X)^{p^i} - 1) \cong \mu_{p^i},$$

i.e. $\mathscr{F}(\mathbf{G}_m) = \mathbf{G}_m[p^\infty]$, where the $\mathbf{G}_m$ on the left is talking about the 1-dimensional p-divisible formal $\mathcal{O}_K$-group, and the $\mathbf{G}_m$ on the right is talking about the abelian scheme. Note, too, that

$$\varprojlim \mathcal{O}_K[X]/((1+X)^{p^i} - 1) \cong \varprojlim \mathcal{O}_K[X]/(X^{p^i}) \cong \mathcal{O}_K[\![X]\!],$$

with compatibility of group laws.

Serre and Tate showed that these observations hold true in general, i.e. that $\mathscr{F}$ is an equivalence of categories. First, the shallower part is

Proposition 7.5. *The functor $\mathscr{F}$ is fully faithful.*

Proof. Recall that $\mathscr{A}_n$ is a local ring with maximal ideal $\mathfrak{m}_{\mathscr{A}} = \mathfrak{m}_K \mathscr{A}_n + \mathscr{J}_n$. The point is really the same as in the end of Example 7.4, but one must prove it in general. The rings that $G = \mathscr{F}(\mathscr{G})$ is made up of are the rings

$$\mathscr{A}_n^{(i)} = \mathscr{A}_n/([p]^i(\mathscr{J}_n)\mathscr{A}_n).$$

The claim is that by taking the inverse limit of these as $i \to \infty$, one recovers $\mathscr{A}_n$. If we can show this, the “full” part of the statement is also obvious, because a morphism of p-divisible groups is defined to respect the maps in the inverse system and therefore induces a map of formal groups (assuming we have proved the claim). But since $\mathscr{A}_n$ is $\mathfrak{m}_{\mathscr{A}}$-adically complete, it suffices to show that the $\mathfrak{m}_{\mathscr{A}}$-adic topology is equivalent to the topology given by the fundamental system of neighborhoods $[p]^i(\mathscr{J})\mathscr{A}_n + \mathfrak{m}_K^j \mathscr{A}_n$, ranging over all $i, j \geq 1$. Once we have that, we are done because

$$\mathscr{A}_n \cong \varprojlim_{(i,j)\in\mathbf{N}\times\mathbf{N}} \mathscr{A}_n/([p]^i(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^j\mathscr{A}_n) \cong \varprojlim_{(i,j)\in\mathbf{N}\times\mathbf{N}} \mathscr{A}_n^{(i)}/\mathfrak{m}_K^j\mathscr{A}_n^{(i)} \cong \varprojlim_{i\in\mathbf{N}} \mathscr{A}_n^{(i)}.$$

The last step is justified by the fact that $\mathscr{A}_n^{(i)}$ is a finite free local $\mathcal{O}_K$-algebra and $\mathcal{O}_K$ is $\mathfrak{m}_K$-adically complete.

First, the ideal $[p]^i(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^j\mathscr{A}_n$ is $\mathfrak{m}_{\mathscr{A}}$-adically open, because

$$\mathscr{A}_n/([p]^i(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^j\mathscr{A}_n) \cong \mathscr{A}_n^{(i)}/\mathfrak{m}_K^j\mathscr{A}_n^{(i)}$$

is a finite k-algebra ($k = \mathcal{O}_K/\mathfrak{m}_K$) and is therefore Artinian, which means that the sequence of ideals $\mathfrak{m}_{\mathscr{A}}^k + ([p]^i(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^j\mathscr{A}_n)$ must stabilize at $[p]^i(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^j\mathscr{A}_n$ for sufficiently large k.

The last thing we need to check is that the $[p]^i(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^j\mathscr{A}_n$ go to zero as $i, j \to \infty$, i.e. that for any $k \in \mathbf{N}$, there exists an i, j such that

$$[p]^i(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^j\mathscr{A}_n \subset \mathfrak{m}_{\mathscr{A}}^k.$$

That one is because $[p](X_i) \equiv pX_i \mod \deg 2$, so since $\mathscr{J}_n = (X_1, \ldots, X_n)$, we have

$$[p](\mathscr{J}_n) \subset p\mathscr{J}_n + \mathscr{J}_n^2 \subset (\mathfrak{m}_K\mathscr{A}_n + \mathscr{J}_n)\mathscr{J}_n \subset \mathfrak{m}_{\mathscr{A}}.$$

Applying $[p]$ again $i-1$ more times, we see by induction that

$$[p]^i(\mathscr{J}_n) \subset (\mathfrak{m}_K\mathscr{A}_n + \mathscr{J}_n)[p]^{i-1}\mathscr{J}_n \subset (\mathfrak{m}_K\mathscr{A}_n + \mathscr{J}_n)^i\mathscr{J}_n \subset \mathfrak{m}_{\mathscr{A}}^i,$$

which shows that

$$[p]^k(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^k\mathscr{A}_n \subset \mathfrak{m}_{\mathscr{A}}^k,$$

as desired. □

The harder part is in showing that the construction $\varprojlim A^{(i)}$ actually does result in some $\mathscr{A}_n$ for the rings $A^{(i)}$ coming from an arbitrary p-divisible group G, i.e.

Proposition 7.6. *The functor $\mathscr{F}$ is essentially surjective.*

Proof. Let $G = \{G_i\}$ be a connected p-divisible $\mathcal{O}_K$-group of height h, where $G_i = \operatorname{Spec}(A_i)$, A_i a finite free local $\mathcal{O}_K$-algebra of rank p^{ih}. The claim is that

$$\mathscr{A} = \varprojlim A_i$$

is actually isomorphic to some $\mathscr{A}_n = \mathcal{O}_K[\![X_1, \ldots, X_n]\!]$. That n is called the *dimension* of G, and is an intrinsic property of G. Using the same kind of compatibility argument as in the proof of Proposition 7.5, this claim suffices to prove the desired result, because the group scheme structure on the G_i's immediately provides a corresponding formal group law structure for $\mathscr{A}_n$, and thus a $\mathscr{G}$ such that $G \cong \mathscr{F}(\mathscr{G})$. Since $\mathscr{F}$ preserves the two notions of height, it will be immediate that G and $\mathscr{G}$ have the same height h.

Also, the ring $\mathscr{A}$ is already guaranteed to be a flat $\mathcal{O}_K$-algebra, because the A_i are free and $A_{i+1} \to A_i$ is assumed to be surjective (so in fact as an $\mathcal{O}_K$-module, $\mathscr{A}$ is a countable direct product of copies of $\mathcal{O}_K$).

The main detail not explained by Tate [12, Proposition 1] is why one can now replace $\mathcal{O}_K$ with its residue field. The reason for this is essentially the usual Nakayama's lemma argument, but some care must be taken because of the direct limits involved. Suppose we have constructed a continuous homomorphism

$$f : \mathcal{O}_K[\![X_1, \ldots, X_n]\!] \to \varprojlim A_i = \mathscr{A}$$

such that the reduction modulo $\mathfrak{m}_K$

$$\overline{f} : k[\![X_1, \ldots, X_n]\!] \to \mathscr{A}/\mathfrak{m}_K\mathscr{A}$$

is an isomorphism. Composing with the projection $\pi_i : \mathscr{A} \to A_i$ and using the fact that

$$\mathscr{A}/\mathfrak{m}_K\mathscr{A} = \varprojlim A_i/\mathfrak{m}_K A_i,$$

we know that $\pi_i \circ f : \mathscr{A}_n \to A_i$ is a continuous homomorphism with the property that

$$\overline{\pi_i} \circ \overline{f} : k[\![X_1, \ldots, X_n]\!] \to A_i/\mathfrak{m}_K A_i$$

is surjective. Since A_i is a finitely generated module over the local ring $\mathcal{O}_K$, Nakayama's lemma applies, and we at least get that $\pi_i \circ f$ is surjective for all $i \in \mathbf{N}$. This does not a priori imply that f is even surjective: think of the example $\mathbf{Z} \subset \mathbf{Z}_p$. In this case though, it is enough, because of the fact that in the short exact sequence of projective systems

$$0 \to (I + \ker(f \circ \pi_i))/I \to \mathscr{A}_n/I \overset{\pi_i \circ f \mod I}{\longrightarrow} A_i/(\pi_i \circ f)(I)A_i \to 0$$

(where i varies over the index category $\mathbf{N}$, and I varies over e.g. the fundamental system of neighborhoods $[p]^a(\mathscr{J}_n)\mathscr{A}_n + \mathfrak{m}_K^b\mathscr{A}_n$ as (a, b) varies over the index category $\mathbf{N}^2$) all three things satisfy the Mittag-Leffler condition (clear from the definition: everything you would ideally want to be surjective is surjective); so taking the inverse limit preserves this short exact sequence, and in particular we see that the induced map

$$\varprojlim_{i,I} \mathscr{A}_n/I \overset{\pi_i\circ f}{\to} \varprojlim_{i,I} A_i/(\pi_i \circ f)(I)A_i,$$

i.e.

$$f : \mathscr{A}_n \to \mathscr{A},$$

is surjective (these are the same arguments as in Proposition 7.5). To check that f is injective, the trick is to apply Nakayama's lemma again, this time using the fact that $\mathscr{A}_n$ is a local ring. By the hypothesis that $\overline{f}$ is an isomorphism, and the fact that $\mathscr{A}$ is flat over $\mathcal{O}_K$,

$$0 = \ker(\overline{f}) = \ker(f)/\mathfrak{m}_K \ker(f),$$

where the right hand side we can think about as an $\mathscr{A}_n$-module. Nakayama's lemma, applied now in two different ways, shows that f is indeed an isomorphism. So now we just need to produce a continuous map $f : \mathscr{A}_n \to \mathscr{A}$ that reduces mod $\mathfrak{m}_K$ to an isomorphism, and in fact just the isomorphism

$$\overline{f} : k[\![X_1, \dots, X_n]\!] \to \mathscr{A}/\mathfrak{m}_K\mathscr{A}$$

is enough, because any such continuous isomorphism may be lifted to $\mathcal{O}_K$. Now that we can replace $\mathcal{O}_K$ with k, the theory of the Frobenius and Verschiebung is accessible. Already, the fact that $F^i \circ V^i = [p]^i$ means that we may consider the closed subscheme

$$H_i := \ker F^i \subset G_i.$$

In fact, any G_i is contained in some H_j, because of the fact that G_i is connected and finite and k has characteristic p (those group schemes are well-understood, and must be of the form $\operatorname{Spec} k[X_1, \dots, X_N]/(X_i^{p^{r_i}})$; so there exists a j such that F^j kills all of G_i). As a result, we can rewrite $\mathscr{A} = \varprojlim A_i$ as $\varprojlim B_i$, where the B_i are the rings representing $H_i = \ker F^i$. The H_i's are also connected, with maximal augmentation ideals $I_i \subset B_i$. Take the cotangent spaces

$$W_i = I_i/I_i^2,$$

finite-dimensional vector spaces over k. In fact, they all have the same dimension, which will be n (the same n the defines the proposed $\mathscr{A}_n$). That is because H_1 is defined as the kernel of $F : H_i \to H_i^{(p)}$, so the kernel of $I_i \to I_1$ is generated by the p-th powers of the elements of I_1, and is therefore contained in I_i^2; it induces an isomorphism of k-vector spaces $I_i/I_i^2 \to I_1/I_1^2$.

We may choose $x_1, \dots, x_n \in \varprojlim_i I_i$ such that their projection to I_i form a basis for the k-vector space I_i/I_i^2. Now define the map

$$\overline{f} : k[\![X_1, \dots, X_n]\!] \to \mathscr{A} = \varprojlim B_i$$

via $X_i \mapsto x_i$. We need to show that this is an isomorphism. At the very least, it is surjective, because $x_1, \dots, x_n$ form a basis for I_i/I_i^2, so together with their powers and k, they generate (in the ring sense) all of B_i for all i. It remains to show that $\overline{f}$ is injective. The kernel of $\pi_i \circ \overline{f}$ contains X^{p^i}, since B_i is the kernel of F^i, so it induces surjective maps

$$\pi_i \circ \overline{f} : k[X_1, \dots, X_n]/(X_1^{p^i}, \dots, X_n^{p^i}) \to B_i.$$

The left hand side has dimension p^{in} over k, so it suffices to show the same is true of B_i. When $i = 1$ at least, this is fine, because H_1 is, by the classification of connected group schemes over k, with the additional restriction of being killed by F, of the form

$$H_1 = \operatorname{Spec}(k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p)).$$

Importantly this n must be the same as n the dimension of G, which is why the dimensions match. To complete the proof for all i, one uses the fact that $F : H_i \to H_{i-1}^{(p)}$ is surjective, and the sequence

$$0 \to H_1 \to H_i \xrightarrow{F} H_{i-1}^{(p)} \to 0$$

exact, so that

$$|H_i| = |H_1||H_{i-1}^{(p)}| = |H_1||H_{i-1}| = |H_1|^i$$

by induction. So B_i has the right dimension over k, and f projects down to an isomorphism

$$k[X_1, \ldots, X_n]/(X_1^{p^i}, \ldots, X_n^{p^i}) \to B_i$$

for all i. Taking the inverse limit over all i yields the desired isomorphism. □

Armed with this equivalence of categories, we may define $n = \dim G = \dim G^\circ$ the *dimension* of the p-divisible group G.

Lemma 7.7. *$\dim G + \dim G^\vee = h$, where h is the height of G (also equal to the height of $G^\vee$ since Cartier duality preserves orders).*

Proof. None of these quantities are affected by change of base, so we may replace $\mathcal{O}_K$ with its residue field. There is an exact sequence

$$0 \to \ker F \to \ker[p] \to \ker V \to 0.$$

The guy in the middle by definition has order p^h. And $\ker F$, as we saw in Proposition 7.6, has order $p^{\dim G}$. Since V is defined dually to F, we have $|\ker V| = p^{\dim G^\vee}$, and thus

$$p^{\dim G + \dim G^\vee} = p^h,$$

as desired. □

7.2. **The Hodge–Tate decomposition.** In this section, we prove a fundamental theorem about p-divisible groups, namely the Hodge-Tate decomposition for Tate modules. This includes better understanding, for a given p-adic field K with absolute Galois group Γ_K, the p-adic Γ_K-representations on the rational Tate module of a p-divisible group. To get to the point quickly, we blackbox some facts from Tate-Sen theory (about the Galois cohomology of the Tate twists of the completed algebraic closure $\mathbf{C}_K$).

First, we need to explain all the words from the previous paragraph.

Definition 7.8. Let K be an extension of $\mathbf{Q}_p$ with nonarchimedean valuation v. Then, we say it is p-adic if it the valuation is discrete and complete with perfect residue field. We also denote by $\mathbf{C}_K$ the completed algebraic closure of K, by which we mean the p-adic completion of the algebraic closure of K.

Remark 7.9. Note that $\mathbf{C}_K$ is not discretely valued.[14]

[14] It is, however, one of the easiest examples of a characteristic 0 perfectoid field.

The action of the absolute Galois group Γ_K on K (uniquely) extends to a continuous action on $\mathbf{C}_K$ and one can also check easily that $\mathbf{C}_K$ is algebraically closed–we do not have to take another algebraic closure. We next recall the definition of the Tate twist.

Definition 7.10. The nth Tate twist of a Γ_K-equivariant $\mathbf{Z}_p$-module M, denoted by $M(n)$, is defined as $M \otimes T_p(\mu_{p^\infty})^{\otimes n}$ for $n \geq 0$ and $\mathrm{Hom}_{\Gamma_K}(T_p(\mu_{p^\infty})^{\otimes -n}, M)$ otherwise.

Remark 7.11. Every p-divisible group G over K gives rise to a p-adic Γ_K-representation $V_p(G)$, defined as tensoring $T_p(G)$ up by $\mathbf{Q}_p$. We call this the rational Tate module of G. More generally, another class of p-adic Γ_K-representations is given by the rational l-adic cohomology (with $l = p$) of a K-variety, denoted by $H^n(X_{\overline{K}}, \mathbf{Q}_p)$.[15]

The main blackboxed tool we will use is the following fact by Tate and Sen:

Theorem 7.12. *$H^i(\Gamma_K, \mathbf{C}_K(n))$ is naturally isomorphic to K if $i = 0, 1$ and $n = 0$ and isomorphic to 0 otherwise. Here, $\mathbf{C}_K(n)$ is the nth Tate twist of $\mathbf{C}_K$.*

We also state without proof a lemma of Serre and Tate.

Lemma 7.13. *Let V be a p-adic Γ_K-representation. Then, there is a natural Γ_K-equivariant, $\mathbf{C}_K$-linear, and injective map*

$$\bigoplus_{n \in \mathbf{Z}} (V \otimes_{\mathbf{Q}_p} \mathbf{C}_K(-n))^{\Gamma_K} \otimes_K \mathbf{C}_K(n) \to V \otimes_{\mathbf{Q}_p} \mathbf{C}_K.$$

Definition 7.14. In the setting of the lemma above, we say that V is Hodge-Tate if the map above is moreover surjective.

We will later describe the Tate module of a p-divisible group through the Hodge-Tate decomposition; on the left hand side, we have the object $\mathrm{Hom}(T_p(G), \mathbf{C}_K)$ and on the right, the tangent and cotangent spaces with values in $\mathbf{C}_K$. More generally, we have the following definition.

Definition 7.15. Let G be a p-divisible group over $\mathcal{O}_K$ of dimension d. Then, recall that $\mu(G)$ is the unique p-divisible formal group law over $\mathcal{O}_K$ so that $\mu(G)[p^\infty] \cong G^\circ$. Let $\mathcal{I}$ be the augmentation ideal of $\mu(G)$. Then, for any $\mathcal{O}_K$-module M, we denote by $t_G(M)$ the tangent space of G with values in M, which we define as $\mathrm{Hom}_{\mathcal{O}_K-\mathrm{mod}}(\mathcal{I}/\mathcal{I}^2, M)$. Similarly, we define the cotangent space of G taking values in M as $t_G^*(M) = \mathcal{I}/\mathcal{I}^2 \otimes_{\mathcal{O}_K} M$.

Remark 7.16. One can check that in this setting, we can define a logarithm map

$$\log_G : G(\mathcal{O}_L) \to t_G(L),$$

so that for any f and x (with lift y to $\mathcal{I}$), we have $\log_G(f)(x) = \lim_{n\to\infty} \frac{p^n f(y)}{p^n}$. We record some important properties that we will use in the proof of the Hodge-Tate decomposition theorem:

(1) $\log_G$ is a (group) homomorphism.
(2) $\ker \log_G$ is $G(\mathcal{O}_L)_{\mathrm{tors}}$ (the torsion subgroup).
(3) $\log_G$ induces an isomorphism between $G(\mathcal{O}_L) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $t_G(L)$.

[15] Note that this is not the étale cohomology with coefficients in $\mathbf{Q}_p$; this notation is a little misleading because $\mathbf{Q}_p$ is neither an étale nor an l-adic sheaf (with $l = p$), but rather tensoring up the l-adic cohomology groups of $X_{\overline{K}}$ (by taking an inverse limit over the cohomology groups with coefficients in $\mathbf{Z}/p^i\mathbf{Z}$) by $\mathbf{Q}_p$ as we did in the construction of the rational Tate module.

Lemma 7.17. *Let G be a p-divisible group over $\mathcal{O}_K$ with components G_v. Then, we have $G_v(\overline{K}) \cong G_v(\mathbf{C}_K) \cong G_v(\mathcal{O}_{\mathbf{C}_K})$.*

Proof. The second isomorphism follows immediately from the valuative criterion. The first isomorphism follows from the fact that $\mathbf{C}_K$ is algberaically closed and because the generic fiber is étale. □

Lemma 7.18. *Let G be a p-divisible group over $\mathcal{O}_{\mathcal{K}}$. Then, $\bigcap_{n=1}^{\infty} p^n G^\circ(\mathcal{O}_K) = 0$.*

Proof. This follows from consider the valuation filtrations of $G^\circ(\mathcal{O}_L)$ (by identifying it with the $\mathcal{O}_K$-continuous maps from $\mathcal{O}_K[\![x_1, \ldots, x_d]\!]$ to $\mathcal{O}_L$)–an analogue of the higher ramification groups. One can show that $p^n G^\circ(\mathcal{O}_K)$ is contained in the $nv(\pi_K)$th filtration, and then note that the intersection over all such filtrations is trivial. □

Lemma 7.19. *Let G be a p-divisible group over $\mathcal{O}_{\mathcal{K}}$. Then, Γ_K-fixed points of $G(\mathcal{O}_{\mathbf{C}_K})$ is precisely $G(\mathcal{O}_K)$. Similarly, we have $t_G(\mathbf{C}_K)^{\Gamma_K} = t_G(K)$.*

Proof. This follows from the observation that Γ_K-invariant elements of $\mathbf{C}_K$ and $\mathcal{O}_{\mathbf{C}_K}$ are K and $\mathcal{O}_K$, respectively. □

Earlier, we talked about Tate modules for p-divisible groups over a field, but here we are working over $\mathcal{O}_K$. In our setting, we define the Tate module and Tate comodule by simply base-changing to the field.

Definition 7.20. If G is a p-divisible group over $\mathcal{O}_K$, we define the Tate module of G as the Tate module of $G \times_{\mathcal{O}_K} K$. As a reminder, this is simply the inverse limit of $G_v(\overline{K})$, where the G_v are the components of G. Similarly, we define the Tate comodule $\Phi_p(G)$ as the direct limit of the $G_v(\overline{K})$.

Proposition 7.21. *Let G be a p-divisible group over $\mathcal{O}_K$. Then, we have Γ_K-equivariant isomorphisms $T_p(G) \cong \operatorname{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mathbf{Z}_p(1))$ and $\Phi_p(G) \cong \operatorname{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mu_{p^\infty}(\overline{K}))$.*

Proof. We first remark that $T_p(\mu_{p^\infty}) = \mathbf{Z}_p(1)$ and that $\Phi(\mu_{p^\infty}) = \mu_{p^\infty}(\overline{K})$. By Cartier duality, we have the following natural isomorphisms:

$$\begin{aligned} G_v(\overline{K}) &\cong (G_v^\vee)^\vee(\overline{K}) \\ &\cong \operatorname{Hom}_{\overline{K}\text{-grp hom}}((G_v^\vee)_{\overline{K}}, (\mu_{p^v})_{\overline{K}}) \\ &\cong \operatorname{Hom}(G_v^\vee(\overline{K}), \mu_{p^v}(\overline{K})). \end{aligned}$$

Now we just use this identification on the component level of our p-divisible group G, commuting the inverse limits properly and using the previous paragraph to conclude that

$$T_p(G) \cong \operatorname{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mathbf{Z}_p(1)).$$

We can do the same for the Tate comodule, noting now that the direct limit will become an inverse limit in the first component, so that we get

$$\Phi(\mu_{p^\infty}) = \mu_{p^\infty}(\overline{K}),$$

as desired. □

We will now prove the existence of a big commutative diagram comparing two exact sequences that will play a crucial role in proving that decomposition theorem; this is essentially the key step to establishing a relationship between the Tate module and the (co)tangent space. And once the commutative diagram is established, we will take Γ_K-invariants, apply our blackboxed knowledge of Tate-Sen theory, and use a bit of linear algebra to obtain the main result of this section.

Proposition 7.22. *Let G be a p-divisible group over $\mathcal{O}_K$. Then, we have the following commutative diagram, where the two rows are exact, and α and $d\alpha$ are injective and Γ_K-equivariant. Also, the leftmost vertical map is an isomorphism.*

$$\begin{tikzcd}
0 \arrow[r] & \Phi_p(G) \arrow[r] \arrow[d] & G(\mathcal{O}_{\mathbf{C}_K}) \arrow[r, "\log_G"] \arrow[d, "\alpha"] & t_G(\mathbf{C}_K) \arrow[r] \arrow[d, "d\alpha"] & 0 \\
0 \arrow[r] & \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mu_{p^\infty}(\overline{K})) \arrow[r] & \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), 1+\mathfrak{m}_{\mathbf{C}_K}) \arrow[r] & \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mathbf{C}_K) \arrow[r] & 0
\end{tikzcd}$$

Proof. First, let us check that the top sequence is actually exact. Using Remark 7.16, it's easy to see that $G(\mathcal{O}_{\mathbf{C}_K})$ is p-divisible and that $\log_G$ is surjective. We also have that (again using Remark 7.16)

$$\begin{aligned}
\Phi_p(G) &= \varinjlim_v G_v(\overline{K}) \\
&\cong \varinjlim_v G_v(\mathcal{O}_{\mathbf{C}_K}) \\
&= \varinjlim_v \varprojlim_n \\
G_v(\mathcal{O}_{\mathbf{C}_K}/\mathfrak{m}^n) &\cong G(\mathcal{O}_{\mathbf{C}_K})_{\mathrm{tors}} \\
&\cong \ker \log_G,
\end{aligned}$$

from which the result follows.

For the specific case where $G = \mu_{p^\infty}$ and taking Homs over $\mathbf{Z}_p$, we get the bottom row of our commutative diagram–exactness follows from the fact that $T_p(G^\vee)$ is a free $\mathbf{Z}_p$-module. The leftmost vertical map is the map from Proposition 7.21, from which we get the isomorphism.

Now, note that we can identify any element of $T_p(G^\vee)$ as a morphism of p-divisible groups $G \times_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_K} \to (\mu_{p^\infty})_{\mathcal{O}_K}$, using Lemma 7.17. Then, we can define the maps α and $d\alpha$ as follows.

Taking a test element $x \in T_p(G^\vee)$, let $\alpha(g)(x)$ be $x'(g)$, where x' is identified with a morphism $G(\mathcal{O}_{\mathbf{C}_K}) \to \mu_{p^\infty}(\mathcal{O}_{\mathbf{C}_K})$ and noting that $\mu_{p^\infty}(\mathcal{O}_{\mathbf{C}_K}) \cong 1 + \mathfrak{m}_{\mathbf{C}_K}$. Similarly, we define $d\alpha$ (this time, we use the fact that $t_{\mu_p^\infty}(\mathbf{C}_K) \cong \mathbf{C}_K$.

Using the snake lemma, it is easy to see that we have $\mathbf{Z}_p$-linear isomorphisms between $\ker \alpha$ and $\ker(d\alpha)$ and also between $\operatorname{coker} \alpha$ and $\operatorname{coker}(d\alpha)$. So we just need to show that $d\alpha$ is injective (and then the injectivity of α will follow). First, we observe that $t_G(\mathbf{C}_K)$ and $\mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mathbf{C}_K)$ are $\mathbf{Q}_p$-linear, which means that the $\mathbf{Z}_p$-linear map $d\alpha$ can be upgraded to be $\mathbf{Q}_p$-linear. It then follows that the two kernels and the two cokernels are $\mathbf{Q}_p$-vector spaces.

Next, restricting to $G(\mathcal{O}_K)$, we will show that α is injective. If not, we can find a non-zero element $x \in \ker \alpha$. Since the kernel is a vector space, it is, in particular, torsion-free, and hence x lives in $G^\circ(\mathcal{O}_K)$. We can define a "restricted" version of α above by replacing G with $G\circ$, and noting that we have a surjective map on the level of Tate modules of the duals (and hence an injective map on the level of duals), we get the following commutative diagram, where the top and bottom arrows are injective.

$$\begin{tikzcd}
G^\circ(\mathcal{O}_{\mathbf{C}_K}) \arrow[r] \arrow[d, "\alpha^\circ"] & G(\mathcal{O}_{\mathbf{C}_K}) \arrow[d, "\alpha"] \\
\mathrm{Hom}_{\mathbf{Z}_p}(T_p((G^\circ)^\vee), 1+\mathfrak{m}_{\mathbf{C}_K}) \arrow[r] & \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), 1+\mathfrak{m}_{\mathbf{C}_K})
\end{tikzcd}$$

By Lemma 7.19, it's easy to see that $\ker(\alpha^\circ)$ and $\ker(\alpha^\circ)\cap G^\circ(\mathcal{O}_K)$ are $\mathbf{Q}_p$-vector spaces, from which it follows that we find $x_n \in \ker(\alpha^\circ)\cap G^\circ(\mathcal{O}_K)$ with $p^n x_n = x$. So this means that $x = 0$ by Lemma 7.18, which is a contradiction.

Using this, we show that $d\alpha$ is injective, which will complete the proof. We can decompose $d\alpha$ as the composition

$$t_G(K)\otimes_K \mathbf{C}_K \to \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee),\mathbf{C}_K)^{\Gamma_K}\otimes_K \mathbf{C}_K \to \mathrm{Hom}_{BZ_p}(T_p(G^\vee),\mathbf{C}_K).$$

Noting that $T_p(G^\vee)$ is free over BZ_p, we can write the third term as $\mathrm{Hom}_{BZ_p}(T_p(G^\vee),K)\otimes_K \mathbf{C}_K$, so the injectivity of the second arrow follows by flatness (these are just vector spaces). For the first map, by the same reason, it suffices to check that $t_G(K)\to\mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee),K)$ is injective.

Note that by Remark 7.16, it suffices to just show injectivity for $\log_G(G(\mathcal{O}_K))$. Like before, pick some $x\in G(\mathcal{O}_K)$ with $\log_G(x)\in\ker(d\alpha)$, and note that because $\ker\alpha$ and $\ker(d\alpha)$ are the same, we can find $x'\in\ker\alpha$ so that $x - x' \in G(\mathcal{O}_{\mathbf{C}_K})_{\mathrm{tors}}$ (using Remark 7.16), which means that we can find some m with $p^m x\in\ker\alpha\cap G(\mathcal{O}_K)$. But we showed earlier that α is injective on $G(\mathcal{O}_K)$, so it follows that $p^n x = 0$ and hence h is torsion. But that means that $\log_G(h) = 0$, as desired. □

Proposition 7.23. *In the setup of the previous proposition, let us restrict α and $d\alpha$ to the Γ_K-invariants. Then, they are both bijective maps.*

Proof. First, we have the following commutative diagram.

$$\begin{tikzcd}
0 \arrow[r] & G(\mathcal{O}_{\mathbf{C}_K}) \arrow[r, "\alpha"] \arrow[d, "\log_G"] & \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), 1+\mathfrak{m}_{\mathbf{C}_K}) \arrow[r] \arrow[d] & \operatorname{coker}\alpha \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & t_G(\mathbf{C}_K) \arrow[r, "d\alpha"] & \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mathbf{C}_K) \arrow[r] & \operatorname{coker}(d\alpha) \arrow[r] & 0
\end{tikzcd}$$

Next, we will take Γ_K-invariants (we write α and $d\alpha$ by a bit of abuse of notation–we only care about the Γ_K-equivariant things now).

$$\begin{tikzcd}
0 \arrow[r] & G(\mathcal{O}_K) \arrow[r, "\alpha"] \arrow[d, "\log_G"] & \mathrm{Hom}_{\mathbf{Z}_p[\Gamma_K]}(T_p(G^\vee), 1+\mathfrak{m}_{\mathbf{C}_K}) \arrow[r] \arrow[d] & (\operatorname{coker}\alpha)^{\Gamma_K} \arrow[d] \\
0 \arrow[r] & t_G(K) \arrow[r, "d\alpha"] & \mathrm{Hom}_{\mathbf{Z}_p[\Gamma_K]}(T_p(G^\vee), \mathbf{C}_K) \arrow[r] & (\operatorname{coker}(d\alpha))^{\Gamma_K}
\end{tikzcd}$$

The rightmost map, (restricted) α, and (restricted) $d\alpha$ are all injective, so it suffices to check surjectivity of the last two (for the rest of this argument, we write α and $d\alpha$ to refer to the restricted versinos). Actually, we get an injective map $\operatorname{coker}\alpha\to\operatorname{coker}(d\alpha)$ (using the exactness at the middle), so we just need to show that $\operatorname{coker}(d\alpha) = 0$ (to show that both α and $d\alpha$ are 0).

Let $V = \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G),\mathbf{C}_K)$ and define V' similarly but for $G^\vee$. If h, d are the height and dimension of G and $d^\vee$ the dimension of $G^\vee$, it follows that V, V' are h-dimensional $\mathbf{C}_K$-vector spaces. Also, using the exact sequences above, we know that $\dim_K(V'^{\Gamma_K}) \geq \dim_K(t_G(K)) =$

d (and surjectivity holds if this is an equality). We'll show soon that the reverse inequality is true as well.

By symmetry, we get $\dim_K(V^{\Gamma_K}) + \dim_K(V'^{\Gamma_K}) \geq d + d^\vee = h$ by Lemma 7.7. Also, the first part of Proposition 7.21 tells us that we have a perfect pairing $T_p(G) \times T_p(G^\vee) \to \mathbf{Z}_p(1)$, which extends (by tensoring with $\mathbf{C}_K$) to a Γ_K-equivariant perfect pairing $V \times V' \to \mathbf{C}_K(-1)$ (the perfectness is because of the freeness of the Tate module). Now, note that the image of $V^{\Gamma_K} \times V'^{\Gamma_K}$ is 0 because of Tate-Sen theory (Lemma 7.13), which means that $V^{\Gamma_K}, V'^{\Gamma_K}$ are orthogonal, and hence $\dim_K(V^{\Gamma_K}) + \dim_K(V'^{\Gamma_K}) \leq h$, since h is also the dimension of V over $\mathbf{C}_K$. So then we have equality and hence surjectivity of $d\alpha$, as desired. □

We now come to the main theorem of this section: the Hodge-Tate decomposition.

Theorem 7.24. *Let G be a p-divisible group over $\mathcal{O}_K$. Then, there is a Γ_K-equivariant $\mathbf{C}_K$-linear isomorphism*

$$\mathrm{Hom}(T_p(G), \mathbf{C}_K) \cong t_{G^\vee}(\mathbf{C}_K) \oplus t_G^*(\mathbf{C}_K)(-1).$$

Proof. Using the previous proposition, we have isomorphisms

$$t_G(\mathbf{C}_K) \cong \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G^\vee), \mathbf{C}_K)^{\Gamma_K} \otimes_K \mathbf{C}_K$$

and

$$t_{G^\vee}(\mathbf{C}_K) \cong \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G), \mathbf{C}_K)^{\Gamma_K} \otimes_K \mathbf{C}_K.$$

Using the perfect pairing described in the proof of the previous proposition, we get an exact sequence $0 \to t_{G^\vee}(\mathbf{C}_K) \to \mathrm{Hom}_{\mathbf{Z}_p}(T_p(G), \mathbf{C}_K) \to t_G^*(\mathbf{C}_K)(-1) \to 0$, noting that $t_G^*(\mathbf{C}_K)$ is the dual of $t_G(\mathbf{C}_K)$.

Now, an easy computation of the first Ext group (corresponding to applying the left exact Γ_K-invariant functor) to the pair $t_G^*(\mathbf{C}_K)(-1)$ and $t_{G^\vee}(\mathbf{C}_K)$ and Tate-Sen theory (Lemma 7.13), it follows that the sequence above splits. We actually get a unique splitting by noting that (in similar vein to the Ext computation) $\mathrm{Hom}_{\mathbf{C}_K[\Gamma_K]}(t_G^*(\mathbf{C}_K)(-1), t_{G^\vee}(\mathbf{C}_K)) \cong H^0(\Gamma_K, \mathbf{C}_K(1))^{\oplus(\dim_{\mathbf{C}_K} t_G(\mathbf{C}_K))(\dim_{\mathbf{C}_K} t_{G^\vee}(\mathbf{C}_K))} = 0$ by Tate-Sen theory again. So the result follows. □

As promised from earlier, we can conclude that the rational Tate module $V_p(G)$ is a Hodge-Tate p-adic Γ_K-representation.

Theorem 7.25. *Let G be a p-divisible group over $\mathcal{O}_K$. Then, $V_p(G)$ is a Hodge-Tate p-adic Γ_K-representation.*

Proof. The Hodge-Tate decomposition implies that $V_p(G) \otimes_{\mathbf{Q}_p} \mathbf{C}_K \cong t_{G^\vee}^*(\mathbf{C}_K) \oplus t_G(\mathbf{C}_K)(1)$ (by taking $\mathbf{C}_K$-duals). Then, the result follows by Tate-Sen theory again, because we get Γ_K-invariants of $V_p(G) \otimes_{\mathbf{Q}_p} \mathbf{C}_K(-n)$ is 0 for $n \geq 2$, $t_G(\mathbf{C}_K)$ for $n = 1$ and $t_{G^\vee}^*(\mathbf{C}_K)$ for $n = 0$. □

Finally, we end with a quick discussion about the complex variant of the Hodge-Tate decomposition, which holds for compact Kahler manifolds; we aim to give some motivation about why the Hodge-Tate decomposition in our situation is really an analogue of the classical statement. First, we state the Hodge decomposition (and provide no explanation of the technical details or definitions).

Theorem 7.26. *Let X be a compact Kahler manifold. Then, for every k, we have an isomorphism*

$$H^k_{sing}(X, \mathbf{C}) \cong \bigoplus_{i+j=k} H^i(X, \Omega^j).$$

Here, the left hand side is singular cohomology and the right hand side is sheaf cohomology of the sheaf of holomorphic differentials.

We can recast this in more algebro-geometric terms using GAGA, and something rather amazing pops out.

Corollary 7.27. *Let $X/\mathbf{C}$ be a smooth projective integral variety. Then, using the fact that X^{an} is a compact Kahler manifold and the GAGA principle, we obtain*

$$H^k_{sing}(X^{an}) \cong \bigoplus_{i+j=k} H^i(X, \Omega^j_{X/\mathbf{C}}).$$

Remark 7.28. This is an incredible result because we are unexpectedly able to relate the singular cohomology of the analytification of X and the sheaf cohomology of (algebraic) differentials–over $\mathbf{C}$, there are numerous cohomology theories when working in algebraic geometry, and there is no particular reason to expect that these two are related in such a simple, elegant way.

We'll now rewrite the Hodge-Tate decomposition theorem from earlier in a similar form, motivated by the fact that l-adic cohomology is an excellent analogue of singular cohomology for algebraic geometry.

Theorem 7.29. *Let A be an abelian variety over K with good reduction*[16]*. Then, there is a natural Γ_K-equivariant isomorphism*

$$H^i_{ét}(A_{\overline{K}}, \mathbf{Q}_p) \otimes_{\mathbf{Q}_p} \mathbf{C}_K \cong \bigoplus_{i+j=n} H^i(A, \Omega^j_{A/K}) \otimes_K \mathbf{C}_K(-j).$$

Sketch. There are canonical identifications $H^0(A, \Omega^1_{A/K}) \cong t^*_{\mathcal{A}[p^\infty]}(K)$ and $H^1(A, \mathcal{O}_A) \cong t_{\mathcal{A}^\vee[p^\infty]}(K)$. Also, there is a canonical isomorphism between the 1st l-adic cohomology group (with $l = p$) of $A_{\overline{K}}$ and $\mathrm{Hom}_{\mathbf{Z}_p}(T_p(A[p^\infty]), \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Finally, we have $H^i(A, \Omega^j) \cong \bigwedge^i H^1(A, \mathcal{O}_A) \otimes \bigwedge^j H^0(A, \Omega^1)$ and $H^n_{\text{ét}}(A_{\overline{K}}, \mathbf{Q}_p) \cong \bigwedge^n H^1_{\text{ét}}(A_{\overline{K}}, \mathbf{Q}_p)$. The result then follows from the variant of the Hodge-Tate decomposition we proved earlier. □

Remark 7.30. The key point here in the proof above is that we really only need to understand the 1-dimensional situation to extend our results to abelian varieties of arbitrary dimension–the higher cohomology groups are nice enough that we can express them very simply in terms of lower degree cohomology groups.

Remark 7.31. Theorem 7.29 is a special case of the more general Hodge–Tate decomposition, which is the same statement extended to all proper smooth K-schemes. It was proved by Faltings [2, 3] using the language of almost mathematics (see also Tsuji's independent work [15, 16]). More recently, Scholze [9] extended Faltings' generalization even further to rigid analytic varieties using his newly developed theory of perfectoid spaces.

[16] The point here is that we can find an abelian scheme $\mathcal{A}/\mathcal{O}_K$ so that $\mathcal{A}_K$ is A.

References

[1] M. Demazure and A. Grothendieck. *Schémas en groupes: séminaire de géométrie algébrique du Bois Marie, 1962/64, SGA 3*, volume 1. Springer, 1970.

[2] G. Faltings. p-adic hodge theory. *Journal of the American Mathematical Society*, 1(1):255–299, 1988.

[3] G. Faltings. Almost étale extensions. *Astérisque*, 279:185–270, 2002.

[4] J.-M. Fontaine. Il n'y a pas de variété abélienne sur $\mathbf{Z}$. *Inventiones mathematicae*, 81(3):515–538, 1985.

[5] M. Hazewinkel. *Formal groups and applications*. 1978.

[6] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, 1985.

[7] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer, 2013.

[8] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay. Oxford university press, Oxford, 2nd edition, 1974.

[9] P. Scholze. Perfectoid spaces: a survey. In *Current developments in mathematics 2012*. International Press, 2013.

[10] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Annals of Mathematics*, pages 492–517, 1968.

[11] J. Stix. A course on finite flat group schemes and p-divisible groups. URL: https://www.math.uni-frankfurt.de/~stix/skripte/STIXfinflatGrpschemes20120918.pdf.

[12] J. Tate. p-divisible groups. In *Proceedings of a conference on Local Fields*, pages 158–183. Springer, 1967.

[13] J. Tate. Finite flat group schemes. In *Modular forms and Fermat's last theorem*, pages 121–154. Springer, 1997.

[14] J. Tate and F. Oort. Group schemes of prime order. *Annales scientifiques de l'École Normale Supérieure*, 3(1):1–21, 1970.

[15] T. Tsuji. p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case. *Inventiones mathematicae*, 137(2):233–411, 1999.

[16] T. Tsuji. Semi-stable conjecture of Fontaine-Jannsen: a survey. *Astérisque*, 279:323–370, 2002.

[17] J. Voight. Introduction to finite group schemes. URL: https://math.dartmouth.edu/~jvoight/notes/274-Schoof.pdf.