p-divisible groups

Michael Lipnowski

Introduction

We'd like to understand abelian schemes A over an arbitrary base S, or at least over rings of integers and localizations and completions thereof. That's very difficult. As a first step, we consider its associated torsion group schemes. Let $G_v = \ker(A \xrightarrow{p^v} A)$; we'll justify later that these are commutative finite flat groups schemes over S. They fit in an exact sequence

$$0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1},$$

where $G_v \xrightarrow{i_v} G_{v+1}$ is the natural inclusion. Furthermore, the order of G_v, as a group scheme over S, is p^{2gv}, where g is the relative dimension of A over S. These are the characterizing properties of a p-divisible groups over S of height $2g$. This write up is devoted to some basic but important aspects of the structure theory of p-divisible groups. The most exciting thing discused will be the relation between connected p-divisible groups and divisible formal Lie groups over R.

Connection with Faltings' Proof

This section is *very* rough and intended for motivation only. Please take it with a grain of salt, since I don't properly understand the contents myself. Large parts might even be wrong.

The main goals of our seminar are proving (for a number field K):

- *Weak Tate Conjecture.* The map

  $$\{\text{Abelian varieties of dimension } g/K\} \xrightarrow{t} \{\text{Galois representations } G_K \to GL_{2g}(\mathbb{Q}_p)\}$$

  has fibers consisting of isogeny classes.
- Isogeny classes are finite.

The key will be a careful analysis of Faltings height $\hat{h}$, namely that "Faltings height doesn't change much under isogeny". Though we haven't defined Faltings height yet, it will be roughly $volume(A(K \otimes_Q \mathbb{C}))^{-1}$, where this volume is normalized by a basis of Neron differentials (an integral structure on the 1-forms of A). It will turn out that this height is controlled by discriminants of various p-divisible groups of A.

Consider an abelian varieties A/K of fixed dimension g with good reduction outside a fixed finite set Σ of places of K. By semi-stable reduction, there is a fixed finite field extension K'/K, depending only on g and Σ so that $A \otimes_K K'$ has semi-stable reduction at places of bad reduction (a theorem to be discussed in the winter).

The change in height under isogenies $f : A \to A'$ between *semistable* abelian varieties is therefore the main focus. Assume A has good reduction at v, an l-adic place of K, and f is an l-isogeny. Raynaud's computation of the Galois action on $det(\ker(f))/K'$ for l-torsion groups over l-adic integer rings gives an explicit expression for the change in Faltings height, when $e(v) \leq l - 1$. So while Raynaud's calculation of the discriminant applies for large l, relative to the absolute ramification of $K'/\mathbb{Q}$, it won't suffice for small l, in particular for small l of bad reduction. Tate's computation of the discriminant of constitutents of a p-divisible groups over a complete, local, noetherian ring will be crucial to bypass this problem.

Definitions

A *p-divisible group of height h over a scheme S* is an inductive system $G = (\{G_v\}, G_v \xrightarrow{i_v} G_{v+1})_{v \geq 1}$ of group schemes over S satisfying the following:

(i) G_v is a finite locally free commutative group scheme over S of order p^{hv}.

(ii) $0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1}$ is an exact sequence of group schemes.

For ordinary abelian groups, these axioms imply that
$G_v \cong (\mathbb{Z}/p^v\mathbb{Z})^h$ and $\varinjlim G_v = (\mathbb{Q}_p/\mathbb{Z}_p)^h$.
A *homomorphism of p-divisible groups* $f : G = (G_v, i_v) \to H = (H_v, i'_v)$ is a system of homomorphisms of group schemes $f_v : G_v \to H_v$ which are compatible with the structure maps: $i'_v f_v = f_{v+1} i_v$.
Let $i_{v,m} : G_v \to G_{m+v}$ denote the closed immersion $i_{v+m-1} \circ ... \circ i_{v+1} \circ i_v$.
A diagram chase shows that $G_{m+v} \xrightarrow{p^m} G_{m+v}$ can be factored uniquely through $i_{v,m}$ via a map $j_{m,v} : G_{m+v} \to G_v$ (so $i_{m,v} \circ j_{m,v} = p^m$) and furthermore that

$$0 \to G_m \xrightarrow{i_{v,m}} G_{m+v} \xrightarrow{j_{m,v}} G_v$$

is exact. But since orders are multiplicative in exact sequences, a consideration of orders shows that

$$0 \to G_m \xrightarrow{i_{v,m}} G_{m+v} \xrightarrow{j_{m,v}} G_v \to 0$$

is exact (i.e. the closed immersion $coker(i_{v,m}) \to G_v$ is an isomorphism).
Here are some examples of p-divisible groups.

(a) The simplest p-divisible group over S of height h is the constant group:

$$(\mathbb{Q}_p/\mathbb{Z}_p)^h = ((\mathbb{Z}/p^v)^h \xrightarrow{i_v} (\mathbb{Z}/p^{v+1})^h)$$

with i_v the natural inclusion (using multiplication by p).

(b) The p-divisible group of the multiplicative group $\mathbb{G}_m/S$ is

$$\mathbb{G}_m(p) = (\mathbb{G}_m[p^v] \xrightarrow{i_v} \mathbb{G}_m[p^{v+1}])$$

where $\mathbb{G}_m[p^v]$ is the p^v-torsion subgroup scheme of $\mathbb{G}_m$ and the i_v are the natural inclusions. To be precise, the inclusions

$$\mathbb{G}_m[p^v](T) = \{f \in \mathcal{O}(T) : f^{p^v} = 1\} \to \{f \in \mathcal{O}(T) : f^{p^{v+1}} = 1\} = \mathbb{G}_m[p^{v+1}](T)$$

are functorial in S-schemes T and so defines a map $i_v : \mathbb{G}_m[p^v] \to \mathbb{G}_m[p^{v+1}]$.

- Over an affine $\mathrm{Spec}R \subset S, \mathbb{G}_m[p^v]/R$ is just $\mathrm{Spec}R[x]/(x^{p^v} - 1)$, which is free over R of rank p^v. Hence, $\mathbb{G}_m[p^v]$ is finite flat over S of order p^v.
-

$$\begin{aligned} \ker(\mathbb{G}_m[p^{v+1}] \xrightarrow{p^v} \mathbb{G}_m[p^{v+1}])(T) &= \{f \in \mathcal{O}(T) : f^{p^{v+1}} = 1 \text{ with } f^{p^v} = 1\} \\ &= \text{image}\{\mathbb{G}_m[p^{v+1}](T) \xrightarrow{i_v(T)} \mathbb{G}_m[p^{v+1}]\} \end{aligned}$$

  functorially in S-schemes T. Thus, i_v is the kernel of $\mathbb{G}_m[p^{v+1}] \xrightarrow{p^v} \mathbb{G}_m[p^{v+1}]$.

It follows that $\mathbb{G}_m(p)$ is a p-divisible group of height 1 over S.

(c) What follows is the most important example, alluded to in the introduction.
Let A/S be an abelian scheme of relative dimension g. That is, A is a proper, smooth group scheme over S whose geometric fibers are connected of dimension g. The hypotheses imply that A has commutative multiplication.
Let $[n] : A \to A$ denote multiplication by $n \in \mathbb{Z} - \{0\}$.

- For any geometric point $s : \mathrm{Spec}\Omega \to A$, the fiber $[n]_s : A_s \to A_s$ is a finite map. Thus, $[n]$ is quasifinite and proper, and thus is finite. In particular, $A[n]/S$ is finite.
- The structure map $A \to S$ is flat and for any geometric point $s, [n]_s : A_s \to A_s$ is flat. Thus, by the fibral flatness theorem, $[n]$ is flat. In particular, $A[n]/S$ is flat.

Thus, $A[n]/S$ is a finite flat group scheme. It is also finitely presented since A/S is, and so it is locally free over S.
Because all of its geometric fibers have order n^{2g}, by theory for abelian varieties over an algebraically closed field, $A[n]/S$ has order n^{2g}.

Also, as explained for $\mathbb{G}_m$, the natural inclusion $i_v : A[p^v] \to A[p^{v+1}]$ is the kernel of $A[p^{v+1}] \xrightarrow{p^v} A[p^{v+1}]$.
Thus, $A(p) = (A[p^v], i_v)$ is a p-divisible group of height $2g$ over S.

Etale and Connected Groups

In topology, we know that for reasonable connected spaces S and a choice of base point $\alpha \in S$, there is a functorial bijection between coverings of S and actions of $\pi_1(S, \alpha)$ on finite sets realized through the deck transformation action on the fiber over α. Remarkably, the same correspondence often carries over algebraically.

Let S be connected and locally noetherian with geometric point $\alpha : \mathrm{Spec}\Omega \to S$.
Let $\mathbf{Fet}/S$ denote the category of finite etale coverings of S.

There is a functor

$$D : \mathbf{Fet}/S \to \mathbf{Sets}$$
$$Y \mapsto Y(\alpha)$$

where $Y(\alpha)$ denotes the set of geometric points of a finite etale covering $Y \to S$ lying over α. This functor has an automorphism group $\pi = \pi_1(S, \alpha)$, the fundamental group of S with basepoint α. It is naturally a profinite group.
Let $\mathbf{F}\pi$**-Sets** denote the category of finite sets with a continuous action of π. By construction, each $Y(\alpha)$ carries an action of π. Thus, we can view D as a functor

$$D : \mathbf{Fet}/S \to \mathbf{F}\pi\textbf{-Sets}.$$

D has two good properties: it commutes with products and disjoint unions. This is especially useful in light of

Theorem (Grothendieck). *$D : \boldsymbol{Fet}/S \to \boldsymbol{F\pi}$-$\boldsymbol{Sets}$ is an equivalence of categories.*

We can describe the inverse equivalence in certain cases of interest.

- If $S = \mathrm{Spec}(k)$ for a field k, then a geometric point is an embedding $\alpha : k \to \Omega$. $Aut_k(\Omega)$ acts on $Y(\alpha) = Hom_S(\mathrm{Spec}\Omega, Y)$. This action gives a map $Aut_k(\Omega) \to \pi$ which factors through $Gal(k^s/k)$. The induced map $Gal(k^s/k) \to \pi$ is an isomorphism. The reverse equivalence is given by

$$X \mapsto \mathrm{Spec}(Maps_\pi(X, k^s)).$$

- If $S = \mathrm{Spec}R$ is local henselian with closed point s, then $Y \mapsto Y_s$ is an equivalence of categories

$$\mathbf{FEt/S} \to \mathbf{FEt/s}.$$

  Thus, we have the exact same description of the inverse equivalence in this case:

$$X \mapsto \mathrm{Spec}(Maps_\pi(X, R^{sh})),$$

  where R^{sh} is the strict henselization of R which is compatible with our choice of k^s/k.

We can restrict this equivalence to the subcategory $\mathbf{FGet}/S$ of finite etale group schemes with maps of groups between them.
Let G/S be a group scheme with m, e, i denoting the multiplication, inversion, and identity morphisms respectively. $G(\alpha)$ is a group whose underlying set carries an action of π. But we say much more! $G \times_S G$ is also finite etale over S. Thus, π acts through the automorphism group of $G(\alpha)$. We denote $\mathbf{F}\pi$**-Gps** the category of finite groups with a continuous action of π.

Also, if we let D' denote the inverse equivalence to D, then $H = D'(G(\alpha))$ is a finite etale group scheme over S. Indeed, because D commutes with products and is full, there is a morphism m lifting the multiplication of $G(\alpha)$. Similarly, there are morphisms e and i lifting inversion and the identity. They satisfy the appropriate commutativity because D is faithful. It follows that by restricting D to $\mathbf{FGet}/S$ gives an equivalence of categories

$$\overline{D} : \mathbf{FGet}/S \to \mathbf{F}\pi\mathbf{\text{-}Gps}.$$

This equivalence gives us a fairly completely understanding of finite etale S-groups. As a toy example, we can use this equivalence to prove that the only connected etale group is trivial. Because D is an equivalence of categories which commutes with disjoint unions, connected finite etale S-schemes Y are exactly those for which π acts transitively on $Y(\alpha)$. But as explained above, for G a finite etale group scheme, π acts on $G(\alpha)$ as group automorphisms. In particular, it preserves the identity of $G(\alpha)$. Thus, π permutes $G(\alpha)$ transitively iff $G(\alpha)$ is a singleton, which implies that G is trivial.

Now let $S = \mathrm{Spec}R$, where R is a Henselian local ring. That way, the connected component G^0 of the identity section lifts the identity component of the special fiber, so its formation commutes with products (and local henselian base change) and hence it is a finite flat group scheme over S. For any finite flat group scheme G, define $G^{et} = G/G^0$. Because its identity section is an open immersion, it is an etale group scheme. Further, if $f : G \to H$ is any map with H etale, then G^0 factors through H^0, which is trivial by our above discussion. Thus, we have the exact sequence

$$0 \to G^0 \xrightarrow{i} G \xrightarrow{j} G^{et} \to 0.$$

with $G^0 \xrightarrow{i} G, G \xrightarrow{j} G^{et}$ characterized by the following universal properties:

- If $f : H \to G$ is any map from a connected finite flat group scheme over S, then f factors uniquely through i.
- If $f : G \to H$ is any map to a finite etale group scheme over S, then f factors uniquely through j.

Thus, $G \mapsto G^0, G \mapsto G^{et}$ are actually a functors on finite flat commutative S-group schemes. Over a field, we can prove that these functors are exact as follows.
Suppose $0 \to K \xrightarrow{i} G \xrightarrow{j} H \to 0$ is an exact sequence of finite flat commutative groups over R. Then we have the following short exact triple of complexes:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K^0 & \xrightarrow{i^0} & G^0 & \xrightarrow{j^0} & H^0 & \longrightarrow & 0\ (A^\bullet) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{j} & H & \longrightarrow & 0\ (B^\bullet) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K^{et} & \xrightarrow{i^{et}} & G^{et} & \xrightarrow{j^{et}} & H^{et} & \longrightarrow & 0\ (C^\bullet)
\end{array}$$

We readily check that i^0 is the kernel of j^0 and that j^{et} is the cokernel of i^{et}.

Let α be a closed geometric point of S. Note that since $K \xrightarrow{i} G$ is the functorial kernel of $G \xrightarrow{j} H$, we have that $0 \to K(\alpha) \to G(\alpha) \to H(\alpha)$ is exact. But $A(\alpha) = A^{et}(\alpha)$ for any finite flat commutative group scheme A. Thus, by the equivalence of categories, $K^{et} \xrightarrow{i^{et}} G^{et}$ is the kernel of $G^{et} \xrightarrow{j^{et}} H^{et}$ in the category of etale groups over S. But any map from a finite group A to the etale group G^{et} which is killed by j^{et} must factor uniquely through A^{et} and so uniquely through K^{et}. It follows that the bottom sequence is exact. By a comparison of orders, the top row must be left exact too.

- In general, any left exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{f} C$ is a left exact sequence of finite flat commutative group schemes over R with $\text{order}(B) = \text{order}(A)\text{order}(C)$ is exact.
  The induced map $\overline{f} : B/A \to C$ has kernel 0. Indeed, $B \xrightarrow{q} B/A$ is faithfully flat, so if $x \in \ker(\overline{f})(T)$, then $\tilde{x}$, the base change of x via some faithfully flat $T' \to T$, has a preimage $y \in B(T')$. But then $y \in \ker(f)(T') = A(T')$, whence $\tilde{x} = 0$ since the composition $A \xrightarrow{i} B \xrightarrow{q} B/A$ is zero. This implies that $x = 0$.
  Hence, the homomorphism $\overline{f}$ is a closed immersion between two finite flat R-groups of the same order, and so is an isomorphism. Thus, $f = \overline{f} \circ q$ is faithfully flat.

In conclusion, we see that $G \mapsto G^0, G \mapsto G^{et}$ are exact functors.

Now let $G = (G_v, i_v)$ be a p-divisible group. By the exactness proved above,
$G^0 := (G_v^0, i_v^0), G^{et} := (G_v^{et}, i_v^{et})$ are p-divisible groups. The connected etale sequence at finite level

$$0 \to G_v^0 \to G_v \to G_v^{et} \to 0$$

leads to the exact sequence of p-divisible groups

$$0 \to G^0 \to G \to G^{et} \to 0$$

For finite groups G over a perfect field k of characteristic p, the connected etale sequence

$$0 \to G^0 \to G \to G^{et} \to 0.$$

is particularly nice. The map $G \to G^{et}$ admits a section. Indeed, over such k, G^{red} is etale over k. Thus, $G^{red} \times G^{red}$ is reduced, and so multiplication $G^{red} \times G^{red} \to G$ factors through G^{red}, whence G^{red} is a closed subgroup scheme of G. Since $G^{red}(\alpha) = G(\alpha) = G^{et}(\alpha)$ for a geometric point α, we conclude $G^{red} = G^{et}$. The closed immersion $G^{red} \to G$ is a section.
For finite groups over a general henselian local base, $G \to G^{et}$ does not admit a section. But this much is true:
Call a p-divisible group G *ordinary* if the finite level terms of G^0 are multiplicative, i.e. have etale Cartier duals.

Theorem. *Let G be a p-divisible group over a perfect field k of characteristic p. Let R be any henselian local ring with residue field k. Then G admits a unique lift $\tilde{G}$ to R with split connected-etale sequence (necessarily lifting the connected-etale sequence of G).*

This plays an important role in the deformation theory of abelian varieties.

Etale p-divisible groups

At this point, it seems worthwhile to mention that this equivalence of categories extends to etale p-divisible groups over a henselian local ring R with closed geometric point α.
Suppose we have an etale p-divisible group $G = (G_v, i_v)$ of height h over R. Each $G_v(\alpha)$ is isomorphic to $\mathbb{Z}/p^v\mathbb{Z}$. We can form the inverse limit over multiplication by p maps

$$G(\alpha) := \varprojlim G_v(a).$$

The multiplication by p maps are compatible with the action of $\pi_1(R,\alpha)$. Thus, $G(\alpha)$ still carries a continuous action of $\pi_1(R,\alpha)$. Furthermore, since $G_v(\alpha) \cong (\mathbb{Z}/p^v\mathbb{Z})^h$, it follows that $G(\alpha)$ is a free $\mathbb{Z}_p$ module of rank h.

Furthermore, suppose M is a free $\mathbb{Z}_p$ module of rank h with a continuous action of π. Then the quotient M/p^vM is a group of order p^{vh} with a continuous action of π on it. Thus, by the equivalence of categories, there is an etale group over R, say G_v, corresponding to it. The Galois compatible multiplication map $M/p^{v+1}M \xrightarrow{p^v} M/pM$, which is induced by $G_{v+1} \xrightarrow{p^v} G_1$, has kernel $M/p^vM \xrightarrow{i_v} M/p^{v+1}M$. By the equivalence of categories, there is a corresponding map $G_v \xrightarrow{i_v} G_{v+1}$. Thus, $G = (G_v, i_v)$ is an etale p-divisible group.
As a consequence of the above, we conclude

Theorem. *Let p**divEt**$/R$ be the category of etale p-divisible groups of over R, and let **Free-π Mod**$/\mathbb{Z}_p$ denote the category of free $\mathbb{Z}_p$ modules with a continuous action of π. The functor $G \mapsto G(\alpha)$ is an equivalence of categories*

$$p\textbf{divEt}/R \to \textbf{Free-}\pi\ \textbf{Mod}/\mathbb{Z}_p(h).$$

carrying height to $\mathbb{Z}_p$ rank.

As usual, the most important instance of this is for abelian schemes.

- Let A/R be an abelian scheme. Then if $l \neq p, A(l)$ is an etale l-divisible group. The corresponding $\mathbb{Z}_l$ module is none other than $T_l(A)$ with action of $\pi_1(R,\alpha)$.

Then enter Grothendieck, who proved an amazing result.

Theorem (Grothendieck). *Let R be a henselian dvr with fraction field K, and let l be a rational prime. An abelian variety A/K extends to an abelian scheme $/R$ iff $A(l)$ extends to an l-divisible group over R.*

This is proven through the theory of Neron models and the semi-stable reduction theorem. The deepest case is when l is the residue characteristic.

As an example of the power of this result, note that we can recover the classical Neron-Ogg-Shafarevic criterion.

Theorem. *Let p be the residue characteristic of R. Choose any $l \neq p$ be a prime, A an abelian variety over K. Then A has good reduction at l iff the Galois representation on $T_l(A)$ is unramified at l.*

Proof. If $A(l)$ admits a prolongation to R, then it is etale since each $A[l^n]$ has order a power of l, which is prime to the residue characteristic. But by the equivalence of categories for etale l-divisible groups, $A(l)$ admits a prolongation iff the action of $\pi_1(K,\alpha)$ on the corresponding $\mathbb{Z}_l$-module, which is none other than $T_l(A)$, factors through $\pi_1(R,\alpha)$, i.e. iff the Galois action on $T_l(A)$ is unramified. □

Serre-Tate Equivalence for Connected p-divisible groups and Divisible Formal Groups

Let R be a complete, noetherian, local ring with residue field k of characteristic $p > 0$. And let $\mathcal{A} = R[[X_1, ..., X_n]]$ be the power series ring over R in n variables.

Definition. *An n dimensional commutative formal Lie group Γ over R is a pair of maps $m : \mathcal{A} \to \mathcal{A}\hat{\otimes}_R\mathcal{A}$ (the completed tensor product being given the max-adic topology), $e : \mathcal{A} \to R$ such that m is coassociative and cocommutative with e as a counit. Concretely, e is given by $X_i \mapsto 0$ and m is given by a family $f(Y, Z) = (f_i(Y, Z))$ of n power series in $2n$ variables such that*

(i) $X = f(X, 0) = f(0, X)$.

(ii) $f(X, f(Y, Z)) = f(f(X, Y), Z)$.

(iii) $f(X, Y) = f(Y, X)$.

There is a much more functorial interpretation of formal Lie groups over R which is convenient for many purposes. Namely, a *formal group over R* is a group object in the category of formal schemes over R and a *formal Lie group over R* is formally smooth formal group over R. In other words, a formal group is a "pro-representable" functor $F : \textbf{Profinite Artinian}/R \to \textbf{Gps}$, and a a formal Lie group is one for which $F(B) \to F(B/I)$ is surjective for any finite artinian R-algebra B and any square zero ideal $I \subset B$. It's a non-trivial fact that the latter condition implies that the pro-representing object is a power series ring over R. Some interesting examples:

- Let G be an algebraic group over a field k with identity e.
  Let T be a finite artinian k-scheme. Call $x \in G(T)$ *small* if x is supported at e. The small T-points form a subgroup of $G(T)$ because $e \cdot e = e, e^{-1} = e$. Thus, restricting G to small points determines a functor

  $$\widehat{G} : \textbf{Profinite Artinian/k} \to \textbf{Gps}.$$

  Also, any small point factors through an artinian quotient of $\mathrm{Spec}(\mathcal{O}_{G,e})$. Thus, $\widehat{G}$ is pro-represented by $Spf_k(\widehat{\mathcal{O}_{G,e}})$.
  In the case where G is smooth over k, one can see that $\widehat{\mathcal{O}_{G,e}}$ is a power series ring in $n = \dim G$-variables and so is formally smooth, i.e. $\widehat{G}$ is a formal Lie group.

- We show how to recover the formal group law, as originally defined, from the functor on small artinian points. Take $G = \mathbb{G}_m$, for concreteness.
  We simply take the canonical inclusion $i_n : \mathrm{Spec}(\mathcal{O}_{G,e}/m_e^n) \times_k \mathrm{Spec}(\mathcal{O}_{G,e}/m_e^n) \subset G \times_k G$, compose with the two projection maps, and multiply the two of them together using the functor $\widehat{G}$.
  Knowing abstractly that the formal group multiplication is given by a power series, the result of the above computation of $proj_1 \circ i_n * proj_2 \circ i_n$, $*$ denoting multiplication in $G(G \times_k G)$, tells us what the coefficients are up to order n. In the case of $\mathbb{G}_m = \mathrm{Spec}\ k[Z, Z^{-1}]$, reparameterizing with $Z = 1 + T$, (so that $X \mapsto 0$ is the counit) we get

  $$f(X, Y) = X + Y + XY + \geq n\text{th powers}.$$

  Similarly, we can recover the inversion.

Back to the original set up, as in the first defintion of formal Lie groups. Let
$X * Y := f(X, Y) = X + Y +$ higher powers.
Define $[p]_\Gamma(X) = X * ... * X$ (p times), the homomorphism corresponding to multiplication by p in Γ. We call Γ *divisible* if $[p]^* : \mathcal{A} \to \mathcal{A}$ is finite free.

Let $I = (X_1, ..., X_n)$ be the augmentation ideal of $\mathcal{A}$.
Consider $A_v = \mathcal{A}/[p^v]^*_\Gamma(I)$. This is a finite flat R module. Thus, since $\mathcal{A}$ satisfies the Hopf algebra axioms "at finite level", each $\Gamma_{p^v} = \mathrm{Spec}(A_v)$ is a group scheme with multiplication induced by m. We claim that any finite (locally) free map $\phi : \mathcal{A} \to \mathcal{A}$ has rank $= \mathrm{rank}_R \mathcal{A}/\phi(I)$.

- Indeed, let $a_1, ..., a_n$ be a basis for $\mathcal{A}$ over itself via ϕ. We can even assume that $a_1 = 1$. Let $\overline{a_i} = a_i \bmod \phi(I)$.
  - If we can find a relation,

    $$r_1\overline{a_1} + ... + r_n\overline{a_n} = 0 \bmod \phi(I)$$

    for some $r_i \in \mathcal{A}$, then

    $$\phi(r_1)a_1 + ... + \phi(r_n)a_n = \phi(i) \implies \phi(r_1 - i)a_1 + ... + \phi(r_n)a_n = 0$$

    for some $i \in I$ (remember that ϕ is an R-algebra map). This implies that $r_1 = i \in I \cap R = \{0\}, r_2 = ... = r_n = 0$ because the a_i form a basis for $\mathcal{A}_\phi$. Thus, the $\overline{a_i}$ are linearly independent over R.
  - By assumption, we can express any $a \in A$ as

    $$a = \phi(b_1)a_1 + ... + \phi(b_n)a_n$$

    for some $b_i \in \mathcal{A}$. Write each $b_* = r_* + i_*$ for $r_* \in R, i_* \in I$. Then

    $$\overline{a} = r_1\overline{a_1} + ... + r_n\overline{a_n}.$$

    Thus, the $\overline{a_i}$ also generate $\mathcal{A}/\phi(I)$ as an R-module.

  Our claim is thus true: ϕ has rank $= \mathrm{rank}_R \mathcal{A}/\phi(I)$.

In particular, since "free over itself of degree ? " is multiplicative in ? with respect to composition of maps,

$$\mathrm{rank}_R \mathcal{A}/[p^v](I) = (\mathrm{rank}_R \mathcal{A}/[p](I))^v.$$

But each $A_v = \mathcal{A}/\psi^v(I)$ is a local ring. Thus, each Γ_{p^v} is connected and so has order a power of p. Let p^h be the order of Γ_p. Then by the above, Γ_{p^v} has order p^{hv}.
But Γ_{p^v} represents $\Gamma[p^v]$, the p^v-torsion functor of Γ. Thus, the canonical inclusion $i_v : \Gamma_{p^v} \to \Gamma_{p^{v+1}}$, realized through Yoneda via the functorial inclusion $\Gamma[p^v] \subset \Gamma[p^{v+1}]$ is the kernel of $\Gamma_{p^{v+1}} \xrightarrow{[p^v]} \Gamma_{p^{v+1}}$.

Thus, $\Gamma(p) = (\Gamma_{p^v}, i_v)$ is a *connected* p-divisible group. Thought of in terms of the functor of small artinian points, it is clear that the association $\Gamma \mapsto \Gamma(p)$ is functorial. The following remarkable fact is true:

Theorem. *Let R be a complete, local, noetherian ring with maximal ideal m and residue field $k = R/m$ of characteristic $p > 0$. Then $\Gamma \mapsto \Gamma(p)$ is an equivalence between the category of divisible commutative formal Lie groups and the category of connected p-divisible groups.*

Proof. (Tate)
Step 1: Full Faithfulness
Let Γ be a divisible formal Lie group over R. It's coordinate ring $\mathcal{A} = R[[X_1, ..., X_n]]$ has maximal ideal $M = m\mathcal{A} + I$, where $I = (X_1, ..., X_n)$. As above, we let $[p] : \mathcal{A} \to \mathcal{A}$ correspond to multiplication by p in Γ.
First, note that the ideals $m^v\mathcal{A} + [p^v](I)$ form a neighbourhood base of 0 in $\mathcal{A}$:

- $\mathcal{A}/(m^v\mathcal{A} + [p^v](I)) = A_v/m^vA_v$ is artinian. Thus, each $m^v\mathcal{A} + [p^v](I)$ is open.
- $[p](X_i) = pX_i +$ higher order. Thus, $[p](I) \subset pI + I^2 \subset (m\mathcal{A} + I)I = MI$. So

$$[p^v](I) \subset M^vI,$$

and these neighbourhoods are arbitrarily small.

Thus,

$$\mathcal{A} = \varprojlim \mathcal{A}/[p^v](I)$$

and so the functor is fully faithful.

Step 2: Reduction to $R = k$
Let $G = (G_v = \mathrm{Spec}(A_v), i_v)$ be our connected p-divisible group with base change $\overline{G} = (\overline{G_v} = \mathrm{Spec}(\overline{A_v})), \overline{i_v})$ to k. Let $A = \varprojlim A_v, \overline{A} = \varprojlim \overline{A_v}$.
Choose an augmented topological isomorphism $\overline{A} \simeq k[[X_1, ..., X_n]]$. Pick liftings $R[[X_1, ..., X_n]] \to A_v$ of the quotient maps $k[[X_1, ..., X_n]] \twoheadrightarrow \overline{A_v}$, and arrange these choices to be compatible with change in v. This can be arranged because $A_{v+1} \to A_v$ is a surjection between *finite free* R-modules.
By Nakayama's Lemma, the mapping $R[[X_1, ..., X_n]] \to A_v$ to a finite free R-module target is surjective, whence due to R-module splittings of the surjections $A_{v+1} \twoheadrightarrow A_v$ we get two conclusions:
(i) $\varprojlim A_v$ is topologically isomorphic as an R-module to a product of countably many copies of R,
and (ii) the natural map $R[[X_1, ..., X_n]] \xrightarrow{f} \varprojlim A_v$ is *surjective* and splits in the sense of R-modules. By the construction of the countable product decomposition in (i) for the inverse limit as an R-module, it follows that the formation of the module splitting in (ii) is compatible with passage to the quotient modulo m. By the result assumed over the residue field, $\ker(f) \otimes_R k = 0$, i.e. $m \ker(f) = \ker(f)$. Since $R[[X_1, ..., X_n]]$ is a noetherian, $\ker(f)$ is a finitely generated $R[[X_1, ..., X_n]]$-module with $M \ker(f) = (mR[[X_1, ..., X_n]] + I) \ker(f) = \ker(f)$. Thus by Nakayama, $\ker(f) = 0$.
Hence, our map of R-algebras

$$R[[X_1, ..., X_n]] \to \varprojlim A_v$$

is an isomorphism. This is even a topological isomorphism: its formation commutes with passage to quotients modulo any m^N $(N \geq 1)$, and for artinian R the ideals $a_v = \ker(R[[X_1, ..., X_n]] \twoheadrightarrow A_v)$

are a system of *open* ideals (as each A_v has finite length), so a beautiful theorem of Chevalley [Matsumura, Exercise 8.7] (see hint in the back of the book!) gives the cofinality of the a_v's. This is the desired topological aspect for the isomorphism.
As a consequence of the topological nature of the isomorphism, artinian points can be "read off" from the inverse limit description, and so we get a *functorial* formal group law on $R[[X_1, ..., X_n]]$ (via the group laws on the G_v's), with the formation of this group law commuting with passage to the residue field. Hence, $[p]^*$ is *finite flat* (as this is assumed known after reduction over the residue field, and can be pulled up by m-adic completeness and the local flatness theorem). We likewise see that G_v is the p^v-torsion on our formal group law over R because this is true on the level of artinian points (by *construction* of the formal group law on the inverse limit). Consequently, taking $v = 1$ shows that the finite flat map $[p]^*$ has degree p^h, completing the argument over R (granting the results over the residue field).
Thus, it suffices to prove the result for p-divisible groups over k, which is characteristic p.

Step 3: Proof when $R = k$
The key is to use Frobenius F and Verschiebung V.
Consider the category of fppf sheaves of abelian groups over k, which contains finite groups and p-divisible groups as full subcategories. p-divisible groups can be characterized as those sheaves G for which $G(B)$ is p-power torsion for all k-algebras B, $[p]$ is surjective, and each $G[p^v]$ is representable by a finite commutative groups schemes over k.
The the functor $G \mapsto G^{(p)}$ makes sense for finite groups, but also for p-divisible groups. This is because:

- $*^{(p)}$ is exact.
- It preserves the orders of objects represented by finite flat commutative group schemes objects.

In particular, for any p-divisible group $G, G^{(p)} = (G_v^{(p)}, i_v^{(p)})$ is a p-divisible group. We also get maps of p-divisible groups $F : G \to G^{(p)}$ and $V : G^{(p)} \to G$ defined by the usual Frob and Ver maps at finite level. These satisfy $VF = [p]_G, FV = [p]_{G^{(p)}}$. Since $[p] : G \to G$ is a surjective map of fppf sheaves of abelian groups, if G has height h, then so does $G^{(p)}$ and F and V are both surjective with finite kernel of order $\leq p^h$.

Let $H_v = \ker(G \xrightarrow{F^v} G^{(p^v)}) = \mathrm{Spec}(B_v)$. $H_v \subset G_v$ and $G_v \subset H_N$ for some large N, since any finite connected group is killed by a sufficiently high power of Frobenius. Thus,

$$\mathcal{A} = \lim_{\leftarrow} A_v = \lim_{\leftarrow} B_v.$$

Let I_v be the maximal ideal of B_v. Then $I = \lim_{\leftarrow} I_v$ is the maximal ideal of $\mathcal{A}$.
Suppose that $x_1, ..., x_n$ are elements of I whose images form a k basis for I_1/I_1^2. These elements also form a k basis for I_v/I_v^2.

- Indeed, $H_1 \subset H_v$ is the kernel of F on H_v. Thus, $I_v \to I_1$ is a surjective k map with kernel $I_v^{(p)}$, the ideal generated by pth powers of elements of I_v. Thus,

$$I_v/I_v^2 \cong I_v/(I_v^{(p)} + I_v^2) \cong I_1/I_1^2.$$

Consider the maps

$$u_v : k[X_1, ..., X_n] \to B_v; X_i \mapsto x_i.$$

By the above, these maps are surjective. The kernel contains $(X_1^{p^v}, ..., X_n^{p^v})$ because F^v kills H_v. Thus, the homomorphism

$$u_v : k[X_1, ..., X_n]/(X_1^{p^v}, ..., X_n^{p^v}) \to B_v$$

is surjective.
But we can actually compute the dimension of B_v as a k-vector space! Indeed, we claim that the sequences

$$0 \to H_1 \xrightarrow{i} H_{v+1} \xrightarrow{F} H_v^{(p)} \to 0.$$

are exact. That i is the kernel of $H_{v+1} \xrightarrow{F} H_v^{(p)}$ is clear. Also, the identity $FV = [p]_{G^{(p)}}$ implies that $F : G \to G^{(p)}$ is surjective in the sense of fppf abelian sheaves (as this holds for $[p]$ on the p-divisible group $G^{(p)}$), so $H_{v+1} \xrightarrow{F} H_v^{(p)}$ is surjective in that sheaf sense by pullback. But we know that for finite commutative k-groups, a homomorphism is faithfully flat iff it is surjective in the sheaf sense. Thus, $H_{v+1} \xrightarrow{F} H_v^{(p)}$ is faithfully flat and so the above sequence is exact, as claimed. In particular, it follows that

$$\text{order}(H_v) = (\text{order}(H_1))^v.$$

But H_1 is a finite group killed by F with an n dimensional lie algebra. We digress to discuss its structure.

Lemma. *Let $H = Spec(R)$ be a finite commutative group scheme over k killed by F with n dimensional Lie algebra. Then as a scheme,*

$$H = Spec(k[X_1, ..., X_n]/(X_1^p, ..., X_n^p)).$$

Proof. (Mumford, p. 139) Choose $x_1, ..., x_n \in m_e$ which generate the cotangent space m_e/m_e^2. Then the map

$$k[X_1, ..., X_n]/(X_1^p, ..., X_n^p) \to R; X_i \mapsto x_i$$

is surjective.
On the other hand, because it is a group scheme, $R = \Gamma(\mathcal{O}_H)$ admits derivations D_i so that $D_i(x_j) = 1 \bmod m_e$ (the proof of the existence of "enough invariant differentials" for not necessarily smooth finite flat group schemes is given in [Neron Models, p.100]). Then expanding monomials $X_1^{a_1}...X_n^{a_n}, 0 \leq a_i < p$ by the Leibnitz rule, it is straightforward to see that there can be no lower order linear dependences over k (since $\text{char}(k) = p$.) The claim follows. □

It follows that $\text{order}(H_v) = p^{nv}$. On the other hand, $k[X_1, ..., X_n]/(X_1^{p^v}, ..., X_n^{p^v})$ is p^{nv}-dimensional. Thus, u_v is an isomorphism. Passing to the limit, we get

$$k[[X_1, ..., X_n]] \to \overline{A}$$

is an isomorphism, as desired. □

We interpret the Serre-Tate equivalence in more concrete terms for an abelian variety X/k, where k is a field of characteristic p. The formal Lie group corresponding to $X(p)^0$ is none other than the formal group of X/k!

- X/k is smooth. Thus, $\hat{X}$, the completion of X along the identity section is a power series ring over k.
  Recall that we defined $\widehat{X}$ to be the restriction of the functor X to small artinian local k-algebras. $\widehat{X}[p^v]$ is tautologically isomorphic to

  $$T \mapsto X(T)[p^v] = X[p^v](T).$$

  But any small artinian point lies of $X[p^v]$ automatically lies in $X[p^v]^0$ because it is supported at the identity. Thus, $\widehat{X}[p^v]$ and $X[p^v]^0$ are canonically isomorphic. Since any small artinian point is p^v-torsion for some v, we get the functor isomorphism

  $$\widehat{X} = \varinjlim \widehat{X}[p^v] \cong \varinjlim X[p^v]^0.$$

  Hence, $\hat{X}$ corresponds to $X(p)^0$ via the Serre-Tate equivalence.

Life is better with the Serre-Tate equivalence in hand.
We define the *dimension* of G to be the dimension of the divisible formal Lie group associated to G^0.

We digress to discuss a cool result. It's a nice illustration of how to use the connected etale sequence.

Claim. *If (R, m) is a local noetherian ring with residue characteristic $p > 0$, then the "special fiber" functor from p-divisible groups over R to p-divisible groups over the residue field is faithful.*

The noetherian hypothesis is necessary here. Indeed, for the non-noetherian valuation ring $R = \mathbb{Z}_p[\zeta_{p^\infty}]$, there's the map $\mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{G}_m(p)$ given by $1/p^n \mapsto \zeta_{p^n}$ (for a p-power compatible system of choices of ζ_{p^n}'s), and this map is an isomorphism on generic fibers but vanishes on the special fiber.

Proof. (Brian)
Let G and H be p-divisible groups over R, and $f : G \to H$ a map whose special fiber $f_0 : G_0 \to H_0$ vanishes. We want to prove that $f = 0$.
We start off knowing that $f \otimes_R R/m = 0$. Suppose that for any artinian quotient A of R that whenever $I \subset A$ is an ideal with $mI = 0$ and that $f \otimes_R A/I = 0$ then $f \otimes_R A = 0$ $(*)$. If we assume by induction that $f \otimes_R R/m^n = 0$, then applying $(*)$ with
$A = R/m^{n+1}, I = m^n \subset R/m^{n+1}, A/I = R/m^n$ shows that $f \otimes_R R/m^{n+1} = 0$. But
$f_v : G_v = \mathrm{Spec}(A) \to H_v = \mathrm{Spec}(B)$ is the zero map precisely when the corresponding R-Hopf algebra map $B \xrightarrow{f_v^*} A$ factors through $B/J, J$ the augmentation ideal of B. By assumption, $J \subset \ker(f_v^*) + m^n B$ for each n. By Krull's intersection theorem, this implies that f_v^* factors through B/J, i.e. that $f_v = 0$.
Since now we only need to prove the inductive step $(*)$, we can assume for an ideal I in R killed by m that $f \ mod \ I$ vanishes. I will prove that $f \circ [p] = 0$, so then $f = 0$ (that this suffices uses

that $[p]$ is surjective, which is only true at the level of p-divisible groups, not for finite flat group schemes).

Functoriality of the connected-etale sequence leads us to first consider the etale and connected cases separately, and then we'll be reduced to proving that there's no nonzero map from an etale p-divisible group over R to a connected one (which is false without a noetherian condition, by the above example).
The case of etale G and H is trivial. Indeed, the equivalence of categories for etale p-divisible groups says that any map $f : G \to H$ corresponds to a $\pi_1(R, \alpha)$-equivariant map $\tilde{f}$ of free $\mathbb{Z}_p$-modules with a continuous linear actions. But $\tilde{f}_0$ is the same underlying map of $\mathbb{Z}_p$-modules (the difference being the Galois action, given through the isomorphism $\pi_1(k, \overline{\alpha}) \to \pi_1(R, \alpha)$). So

$$f_0 = 0 \implies \tilde{f}_0 = 0 \implies \tilde{f} = 0 \implies f = 0.$$

For the connected case, we switch viewpoint to that of formal Lie groups, so f corresponds to a map of augmented R-algebras

$$f^* : R[[x_1, ..., x_n]] \to R[[y_1, ..., y_N]]$$

such that $f^*(x_j)$ has all coefficients in I (since $f \ mod \ I = 0$) with constant term 0. But then

$$(f \circ [p])^*(x_j) = [p]^*(f^*(x_j)) = [p]^*(\text{stuff with } I\text{-coefficients with constant term } 0),$$

yet every $[p]^*(x_i)$ has linear terms with coefficient p. So, if we plug into it anything with I-coefficients (and no constant term!) then we get zero since $pI = 0$ and $I^2 = 0$ (as I is killed by the maximal ideal of R).

So, the map $f : G \to H$ factors uniquely through $G \xrightarrow{j_G} G^{et}$, the cokernel of $G^0 \xrightarrow{i_G} G$, say through $f' : G^{et} \to H$. Since $j_H \circ f' = f^{et} \circ j_G = 0$, f' factors through i_H, the kernel of j_H. Say $i_H \circ f'' = f'$. It clearly suffices to prove that $f'' = 0$. Thus, we are reduced to prove that $f = 0$ if G is etale and H is connected, and can assume $f \ mod \ I = 0$.

By replacing the artin local R with a strict henselization, we can assume G is constant, and then that $G = \mathbb{Q}_p/\mathbb{Z}_p$. Thus, f corresponds to a sequence of p-power compatible elements in the groups $\ker(H_n(R) \to H_n(R/I))$. By viewing each coordinate ring $\mathcal{O}_{H_n}$ as a quotient of the formal power series ring $\mathcal{O}_H$, it is clear that the kernel of each map $H_n(R) \to H_n(R/I)$ is killed by $[p]$. □

Another fundamental quantity associated with finite group schemes $H = \mathrm{Spec}(B)$ is the *discriminant*: $\mathrm{disc}(H)$ is defined to be the ideal $\mathrm{disc}(B) \subset R$ of the finite free R-algebra B.

Lemma. *Let $0 \to H' \to H \to H'' \to 0$ be an exact sequence of finite flat R-groups of respective orders m', m, m''. Then*

$$disc(H) = (disc(H'))^{m''}(disc(H''))^{m'}.$$

Proof. See Rebecca's notes. □

Our next immediate goal will be to prove the following theorem:

Theorem. *Let $G = (G_v, i_v)$ be a p-divisible group of height h and dimension n over a complete local noetherian ring R with residue characteristic p. Then*

$$disc(G_v) = (p^{nvp^{hv}}).$$

Proof. The preceeding lemma allows us to simplify our computation of the discriminant in two ways:

- From the definition of p-divisible groups, we have an exact sequence

  $$0 \to G_1 \xrightarrow{i} G_{v+1} \xrightarrow{j} G_v \to 0.$$

  Thus, it suffices to compute the discriminant of G_1.

- If H is a finite etale group scheme, then $\text{disc}(H) = 1$. Thus, by the connected-etale sequence, our computation is reduced to the case of connected p-divisible groups.

So, if Γ is the divisible formal Lie group, with coordinate ring $\mathcal{A}$, associated to G, then $G_1 = \text{Spec}(\mathcal{A}/[p]^*(I))$.
But by an earlier discussion, if $a_1, ..., a_n$ denotes a basis for $\mathcal{A}$, viewed as a module over itself via another copy $\mathcal{A}'$ of itself through $[p]$, then $\overline{a_1}, ..., \overline{a_n}$ is an R-basis for $\mathcal{A}/[p](I)$. Since the discriminant is computed by the determinant of a matrix of traces, it is compatible with reduction. Thus, it will suffice to compute $\text{disc}_{\mathcal{A}'/\mathcal{A}}$.

Let Ω, Ω' be the modules of formal differentials of $\mathcal{A}, \mathcal{A}'$ respectively. They are R-linearly spanned by the dX_i, dX_i' respectively.
The map $[p] : \mathcal{A}' \to \mathcal{A}$ induces $d[p] : \Omega' \to \Omega$. A choice of bases for $\mathcal{A}$ (resp. $\mathcal{A}'$) determines generators θ (resp. θ') of $\wedge^n\Omega$ (resp. $\wedge^n\Omega'$). Thus, $\wedge^n d\psi(\theta') = a\theta$ for some $a \in \mathcal{A}$.

In the appendix, we show that

$$\text{disc}_{\mathcal{A}/\mathcal{A}'} = N_{\mathcal{A}/\mathcal{A}'}(a).$$

Grant this fact for now. Choose a basis ω_i of "translation invariant differentials". The existence of such a basis is proven in [Conrad, Leiblich, p. 73], which follows a similar line of reasoning to [Neron Models, p. 100]. For our purposes, it will suffice to note that any invariant differential ω satisfies the property that $d\mu(\omega) = \omega \oplus \omega$. Since $[p]$ corresponds to multiplication by p in Γ,

$$d[p](\omega_i') = p\omega_i.$$

Using this particular basis of differentials to determine θ, it follows that a, from above, equals p^n. Thus, from above, it follows that

$$\text{disc}_{\mathcal{A}/\mathcal{A}'} = N_{\mathcal{A}/\mathcal{A}'}(a) = (p^n)^{\text{rank}_{A'}A} = (p^{np^h}).$$

□

Duality for p-divisible Groups

As explained earlier, for any p-divisible group $G = (G_v, i_v)$ of height h over a commutative ring R, we have an exact sequence

$$0 \to G_1 \xrightarrow{i_{1,v}} G_{v+1} \xrightarrow{j_{1,v}} G_v \to 0.$$

Taking Cartier duals gives the dual exact sequence

$$0 \to G_v^\vee \xrightarrow{j_{1,v}^\vee} G_{v+1}^\vee \xrightarrow{i_{1,v}^\vee} \check{G}_1 \to 0.$$

The maps $j_{1,v}^\vee$ are the kernels of $G_{v+1}^\vee \xrightarrow{p^v} G_{v+1}^\vee$. Also, since duality preserves the order of finite objects, we get that $G^\vee = (G_v^\vee, j_{1,v}^\vee)$ is a p-divisible group of the same height h. We have the following important theorem relating G and $G^\vee$.

Theorem. *Let R be a complete, local, noetherian ring with residue field k of characteristic p. Let $n, n^\vee$ denote the dimensions of $G, G^\vee$. Then*

$$n + n^\vee = h.$$

Proof. The dimensions and heights of $G, G^\vee$ are the same as the dimensions and heights of $G_k, G_k^\vee$. Thus, we are reduced to the case where R is a field of characteristic p.
In the abelian category of fppf abelian group sheaves over k, we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker F & \longrightarrow & G & \xrightarrow{F} & G^{(p)} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle p} & & {\scriptstyle V}\downarrow & & \\ 0 & \longrightarrow & 0 & \longrightarrow & G & \xrightarrow{id} & G & \longrightarrow & 0 \end{array}$$

with exact rows. The snake lemma then yields the exact sequence

$$0 \longrightarrow \ker F \longrightarrow \ker p \longrightarrow \ker V \longrightarrow 0. \ (*)$$

But we can compute the orders of each term in the exact sequence:

- $\ker p = G_1$ has order p^h.
- As explained in the proof of the Serre-Tate equivalence, $\ker F$ (called H_1 in that proof) has order p^n.
- By definition, V is the dual map to F. Thus, because duality is exact, the kernel of V is the dual of the cokernel of

  $$F : G_1^\vee \to (G_1^{(p)})^\vee.$$

  Since $G_1^\vee$ and $(G_1^{(p)})^\vee$ have the same order, and since orders are multiplicative in exact sequences, the cokernel of F the above map has the same order as its kernel, namely $p^{\check{n}}$.

By multiplicativity or orders applied to (*), it follows that $n + n^\vee = h$, as claimed. □

Here are some basic instances of this great result.

- $\mathbb{G}_m(p)$ has height 1 and dimension 1. It's dual is $\mathbb{Q}_p/\mathbb{Z}_p$, which has height 1 and dimension 0.
- Consideran abelian scheme X of dimension g over R. A couple well known facts over fields are, remarkably, true over any base whatsoever (Faltings-Chai):
  - The dual abelian scheme X'/R *always* exists.
  - Duality of abelian schemes is compatible with Cartier duality, i.e.

    $$X(p)^\vee = X'(p).$$

    Composing this natural isomorphism with the Cartier duality pairing

    $$X[p^v] \times X'[p^v] \xrightarrow{\sim} X[p^v] \times X[p^v]^\vee \to \mu_{p^v}.$$

    gives the usual Weil pairing.

  Via a generalization of the fact proved earlier about abelian varieties, the formal Lie group corresponding to $X(p)^0$ under the Serre-Tate equivalence is $\widehat{X}$, the formal Lie group of X.

  In particular, it follows that $X(p), X'(p)$ both have height $2g$ and dimension g.
  The height of $X(p)^0$ thus assumes values between g to $2g$. (It turns out that it can assume all of them.) For example, if X/R is an elliptic curve, then the height is 2 if the elliptic curve has supersingular reduction over the special fiber and 1 if it has ordinary reduction.

Appendix

Using the notation from our partial proof of Tate's discriminant calculation, we want to prove that

$$\mathrm{disc}_{\mathcal{A}/\mathcal{A}'} = N_{\mathcal{A}/\mathcal{A}'}(a).$$

The reference that Tate gives for this fact is inadequate. So during the Wiles Seminars for FLT, Brian devised a proof on his own. I include it here for completeness.

Suppose we have an $\mathcal{A}$-module isomorphism $Tr : \mathcal{A} \cong Hom_{\mathcal{A}'}(\mathcal{A}, \mathcal{A}')$, so $Tr_{\mathcal{A}/\mathcal{A}'}(x) = Tr(dx)$ for some $d \in \mathcal{A}$ unique up to unit multiple (and independent of choice of Tr too).
We wish to compute (d). If $f_i(X_1, ..., X_n) = [p](X_i) \in R[[X_1, ..., X_n]]$, $[p]$ gives an isomorphism of $\mathcal{A}'$ algebras

$$\mathcal{A} \cong \mathcal{A}'[[X_1, ..., X_n]]/(F_i),$$

where $F_i = f_i(X_1, ..., X_n) - X_i'$ and $\partial F_i/\partial X_j = \partial f_i/\partial X_j$.

Claim 2.
- $(d) = (det(\partial f_i/\partial X_j))$.
- $disc_{\mathcal{A}/\mathcal{A}'} = (N_{\mathcal{A}/\mathcal{A}'}(det(\partial f_i/\partial X_j))$.

If θ denotes the $\mathcal{A}'$-module generator $dX_1 \wedge ... \wedge dX_n$ of Ω (resp. θ' denotes the $\mathcal{A}'$-module generator $dX_1' \wedge ... \wedge dX_n'$ of Ω'), then

$$\wedge^n d[p] : \wedge^n \Omega' \to \wedge^n \Omega; \theta' \mapsto det(\partial f_i/\partial X_j)\theta,$$

so $(a) = (det(\partial f_i/\partial X_j))$.
By claim 2(i), it follows that

$$\mathrm{disc}_{\mathcal{A}/\mathcal{A}'} = (N_{\mathcal{A}/\mathcal{A}'}(a)) = ((p^{vn})^{p^{vh}}) = (p^{vnp^{vh}})$$

where the second last equality folows by choosing a basis of Ω' consisting of invariant differentials to compute that a and p^{vn} differ by an $\mathcal{A}^\times$-multiple.

Claim 2(ii) falls into a more general framework.

Claim 2″. *Let A be a ring, R an A-algebra which is finite an free as an R-module. Assume $Hom_A(R, A) \cong R$ as R-mods, and let $Tr_{R/A} \to \tau \in R$ under such an isomorphism (so τ is well defined up to $R^\times$). Then*

$$disc_{R/A} = (N_{R/A}(\tau)).$$

Proof. Say $R = \oplus_{i=1}^n Ae_i$ with π_i the ith coordinate projection. By definition, $\mathrm{disc}_{R/A}$ is generated by $det(Tr_{R/A}(e_ie_j))$. Let $Hom_A(R, A) \cong R$ take f_0 to 1, and choose $r_i \in R$ such that $\pi_i \leftrightarrow r_i$ so that $\pi_i(x) = f_0(r_ix)$. Thus,

$$\begin{aligned} N_{R/A}(\tau) &= det(\pi_j(\tau e_i)) \\ &= det(f_0(r_j\tau e_i)) \\ &= det(f_0(\tau(r_je_i))) \\ &= det(Tr_{R/A}(r_je_i)). \end{aligned}$$

But $\{r_i\}$ forms an A-basis of R because $\{\pi_i\}$ forms an A-basis of $Hom_A(R, A)$. Thus, $r_j = \sum_l a_{jl}e_l$ for some $(a_{ij}) \in GL_n(A)$. Then

$$(Tr_{R/A}(r_je_i)) = (\sum_l a_{jl}Tr_{R/A}(e_le_i)) = (a_{jl})(Tr_{R/A}(e_le_i)).$$

Therefore, $N_{R/A}(\tau) = \text{unit} \cdot det(Tr_{R/A}(e_ie_j))$, as desired. □

Finally, claim 2(i), and our original assumption that $\mathcal{A} \cong Hom_{\mathcal{A}'}(\mathcal{A}, \mathcal{A}')$, are special cases of the next result, where we first observe that $\{F_i\}$ is a regular sequence in $\mathcal{A}'[[X_1, ..., X_n]]$.

Claim 2′. *Let $\mathcal{O}$ be a complete local noetherian ring,*

$$\mathcal{O}' = \mathcal{O}[[T_1, ..., T_n]]/(f_1, ..., f_n)$$

non-zero with $\{f_i\}$ a regular sequence in $\mathcal{O}[[T_1, ..., T_n]]$. Then one has an isomorphism

$$Hom_{\mathcal{O}}(\mathcal{O}', \mathcal{O}) \cong \mathcal{O}'$$

as $\mathcal{O}'$-modules where $Tr_{\mathcal{O}'/\mathcal{O}} \mapsto \overline{det(\partial f_i/\partial T_j)}$.

Proof. For this, we use Tate's results in appendix 3 to Mazzur-Roberts (see references). His theorem A.3 there (with $R = \mathcal{O}, A = \mathcal{O}[[T_1, ..., T_n]], f_i = f_i, C = \mathcal{O}'$) gives an explicit isomorphism $Hom_{\mathcal{O}}(\mathcal{O}', \mathcal{O})$ as $\mathcal{O}'$-modules with $Tr_{\mathcal{O}'/\mathcal{O}} \mapsto \beta(d)$ where

$$\beta : \mathcal{O}'[[T_1, ..., T_n]] \mapsto \mathcal{O}'; T_i \mapsto \overline{T_i}$$

and $f_i(T_1, ..., T_n) = \sum_j b_{ij}(T_j - \overline{T_j}), d = det(b_{ij})$.
But $b_{ij} = \partial f_i/\partial T_j = \sum (T_l - \overline{T_l}) \cdot$ stuff, so

$$\beta(d) = det(\partial f_i/\partial T_j)(\overline{T_1}, ..., \overline{T_n}) = \overline{det(\partial f_i/\partial T_j)}.$$

□

References

- Bosch, Lutkebohmert, Raynaud. *Neron Models.* (1990)
- Conrad, B. *Different Formulations of Gorenstein and Complete Intersection Conditions.* Wiles Seminar (1994).
- Conrad, B. *Shimura-Taniyama Formula.*
- Conrad, B., Leiblich. *Galois Representations Arising from p-divisible groups.*
- Matsumura. *Commutative Ring Theory.*
- Mazur, Roberts. *Local Euler Characteristics.* Inventiones math. 9, 201-234 (1970).
- Mumford. *Abelian Varieties.*
- Tate. *Finite Flat Group Schemes*, in "Modular Forms and Fermat's Last Theorem" (1995).
- Tate. *p-divisible Groups.*