Updated October 30, 2014

CONNECTED p-DIVISIBLE GROUPS

SPEAKER: ADITYA KARNATAKI

Note: our convention is that all group schemes today are commutative and and mostly all (formal) schemes are affine.

We will talk about the Serre-Tate equivalence. This is a handy tool that gives us a handle on the connected part of a p-divisible group. In particular, it does two things for us : (1) It enables us to define 'dimension' of a p-divisible group, which will play a role in proving the main theorem about generic fibers; and (2) It helps us prove a similar theorem about special fibers.

Let R be a complete noetherian local ring with residue field k of characteristic p. The equivalence is an equivalence

$$\{\text{divisible commutative formal Lie groups over } R\} \longleftrightarrow \{\text{connected } p\text{-divisible groups over } R\}.$$

We have to define what all these terms mean.

1. Formal groups

Definition. *A (affine) formal group over R is a group object Γ in the category of affine formal schemes over R.*

Let's do an example. This works for any group scheme but we work with $\mathbf{G}_m$ over $\mathbf{F}_p$. It is affine. We can complete along the identity section. At the level of rings, $\mathbf{G}_m = \operatorname{Spec}(\mathbf{F}_p[T, T^{-1}])$. The ideal corresponding to the identity section $\operatorname{Spec} \mathbf{F}_p \to \mathbf{G}_m$ is the ideal $(T-1)$ inside that ring. The completion along the identity is

$$\operatorname{Spf}(\varprojlim_n \mathbf{F}_p[T, T^{-1}]/(T-1)^n)$$

and this is a formal group. The group law is given at the finite levels

$$\mathbf{F}_p[T, T^{-1}]/I^n \to \mathbf{F}_p[u, u^{-1}, v, v^{-1}]/((u-1)^n, (v-1)^n)$$
$$t \mapsto uv.$$

At the level of the inverse limit we see formal power series rings

$$\mathbf{F}_p[[x]] \to \mathbf{F}_p[[y, z]]$$

with $x = t-1$, $y = u-1$ and $z = v-1$. Thus $x \mapsto (y+1)(z+1) - 1 = y + z + yz$. We call this completion $\widehat{\mathbf{G}}_m$. It is a one-dimensional formal group. (Here dimension refers to the number of variables.) It is formally smooth, so it is an example of a formal Lie group.

Remark: It is worth noting how the group law can be read off at finite levels, on 'small Artinian points'. We refer the reader to Michael Lipnowski's notes [1] where this concept is explained in detail in full generality. This is a crucial observation that allows us to infer functoriality of constructions that follow.

Definition. *A formal Lie group over R is a formally smooth formal group over R.*

Let $\mathscr{A} = R[[x_1, \ldots, x_n]]$. Then a formal Lie group (by definition) is given by $e : \mathscr{A} \to R$ and $m : \mathscr{A} \to \mathscr{A} \widehat{\otimes}_R \mathscr{A}$. Thus m is the same as $f(Y, Z) = (f_i(Y, Z))$ of n power series in $2n$ variables. It satisfies the following axioms :

(a) $X = f(X, 0) = f(0, X)$
(b) $f(X, f(Y, Z)) = f(f(X, Y), Z)$
(c) $f(X, Y) = f(Y, X)$

The first point implies that $f(X, Y) = X + Y +$ higher terms. We denote the group law $X * Y = f(X, Y)$ and multiplication by p given by $[p]_\Gamma(X) = X * X * \cdots * X$.

Definition. Γ *is divisible if $[p]_\Gamma^* : \mathscr{A} \to \mathscr{A}$ is finite free, i.e. $\mathscr{A}$ is a free module of finite rank over itself through this map.*

At the group level, this corresponds to multiplication by p being an isogeny.

2. One side to the other

We have defined all the terms appearing in the statement of our equivalence. Let's go from one side of the equivalence to the other, i.e. start with a divisible formal Lie group Γ and define a connected p-divisible group.

Let $I = (X_1, \dots, X_n)$ be the augmentation ideal of $\mathscr{A} \to R$. Let $A_v = \mathscr{A}/[p^v]^*_\Gamma(I)$. Check: if we define $\Gamma_{p^v} = \mathrm{Spec}(A_v)$ then Γ_{p^v} is a group scheme induced by the comultiplication m. Each A_v is a local ring so each Γ_{p^v} is connected. Thus, order of Γ_{p^v} is a power of p.

We need to know that these powers are compatible, i.e. we should have

$$\text{Order of } \Gamma_{p^v} = (\text{Order of } \Gamma_p)^v$$

This follows from the fact that any finite free map $\phi : \mathscr{A} \to \mathscr{A}$ has rank equal to $\mathrm{rank}_R\, A/\phi(I)$. Let p^h be the order of Γ_p. Then, order of Γ_{p^v} is p^{hv}. Thus h will be the height of our p-divisible group. Note that there is no direct relation between the dimension n and the height h. Later on, we'll see that there is a subtle relation that binds these quantities together.

In fact, from the definition of Γ_{p^v}, it follows that it represents the p^v-torsion of Γ. Thus, the inclusion $\Gamma[p^v] \subset \Gamma[p^{v+1}]$ gives an inclusion $i_v : \Gamma_{p^v} \to \Gamma_{p^{v+1}}$, which is also the kernel of $[p^v] : \Gamma_{p^{v+1}} \to \Gamma_{p^{v+1}}$. These maps form a compatible system, and thus we get a connected p-divisible group (Γ_{p^v}, i_v). We denote this group by $\Gamma(p)$. The association $\Gamma \mapsto \Gamma(p)$ is functorial. This follows from the 'small artinian points' viewpoint.

Thus, we have produced a functor from the category of divisible formal Lie groups to the category of connected p-divisible groups. The main theorem says that this is in fact an equivalence.

3. Serre-Tate Equivalence

Theorem 1 (Serre-Tate)**.** *Let R be a complete local noetherian ring whose residue field k has characteristic $p > 0$. Then $\Gamma \mapsto \Gamma(p)$ is an equivalence of categories between the category of divisible formal Lie groups over R and the category of connected p-divisible groups over R.*

Sketch of proof. (1) Fully faithfulness : This is the easy part. Unraveling the definitions (of a p-divisible group and a formal Lie group), it can be seen that we need to recover the coordinate ring $\mathscr{A} = R[[x_1, \dots, x_n]]$ from $\Gamma(p)$, if we know ahead of time that we come from Γ.

Thus, we are given a connected p-divisible group $\Gamma(p) = (\Gamma_{p^v}, i_v)$ where $\Gamma_{p^v} = \mathrm{Spec}\, \mathscr{A}/[p^v]^*_\Gamma(I)$. Full faithfulness is the statement that

$$\mathscr{A} \simeq \varprojlim_v \mathscr{A}/[p^v]^*_\Gamma(I)$$

as *topological rings*. Let m be the maximal ideal of R and let $M = m\mathscr{A} + I$ denote the maximal ideal of $\mathscr{A}$. Then it suffices to prove that the ideals $\{m^v\mathscr{A} + [p^v]^*_\Gamma(I)\}$ form a system of neighbourhoods of 0 in the M-adic topology on $\mathscr{A}$. We refer the reader to Tate's paper [2, Lemma 0] for more details.

(2) Essential surjectivity : This is the hard part. In the previous case, since each $A_v := \mathscr{A}/[p^v]^*_\Gamma(I)$ was explicitly known to us as a quotient of $\mathscr{A}$, it was easier to show that $\mathscr{A} \simeq \varprojlim_v A_v$. But in this case, we do not know ahead of time, that the connected p-divisible group $G := (G_v, i_v)$ that we'll be starting with, comes from a formal Lie group. As it will be clear from the proof, it is easy to show that G corresponds to a formal group, but it is hard to prove that this formal group is actually a formal *Lie* group. We prove essential surjectivity in two parts.

(a) First one reduces to the case where $R = k$. Let $G = (G_v = \mathrm{Spec}\, A_v, \iota_v)$ be a connected p-divisible group and let $\overline{G} = (\overline{G}_v = \mathrm{Spec}\, \overline{A}_v, \iota_v)$ be the base change to k. Let $\overline{A} = \varprojlim \overline{A}_v$ and $A = \varprojlim A_v$. Suppose we know the essential surjectivity to be true for $\overline{G}$, i.e. $\overline{A} \simeq k[[x_1, \dots, x_n]]$ for some n. Then we need to show[1] that A is a power series ring in R. One considers

$$\begin{array}{ccc} R[[x_1,\dots,x_n]] & & A_v \\ \downarrow & \searrow & \downarrow \\ k[[x_1,\dots,x_n]] & \twoheadrightarrow & \overline{A}_v \end{array}$$

A_v is a finite free R-module, so that by Nakayama's Lemma, a lifting π_v of $\overline{\pi}_v : k[[x_1,\dots,x_n]] \to \overline{A}_v$ to $\pi_v : R[[x_1,\dots,x_n]] \to A_v$ is surjective. Since $A_{v+1} \twoheadrightarrow A_v$ is surjective between finite free modules, we can arrange for compatible liftings $\{\pi_v\}$. Doing so, we get a map $\psi : R[[x_1,\dots,x_n]] \to A$. By a topological argument which uses the fact that the surjections $A_{v+1} \twoheadrightarrow A_v$ admit R-module splittings because of the finite freeness, we get that ψ is a surjective map. Then it can be seen using Nakayama's Lemma, that ker ψ is trivial. Thus, ψ is an isomorphism. It is in fact a *topological* isomorphism, which allows us to transfer the group law from the p-divisible group G to the ring $R[[x_1,\dots,x_n]]$ at finite levels, so that we have a formal Lie group Γ, that corresponds to G under the correspondence we constructed in the previous section. We again refer the reader to [1] for more details.

(b) Now assume that $R = k$ and remember that k is of characteristic $p > 0$. If X is a k-scheme denote by $X^{(p)}$ the base change of X corresponding to $x \to x^p$. It comes with a map $Frob : X \to X^{(p)}$. In fact, by base changing at each finite level, we can base change a p-divisible group $G \to G^{(p)}$. The group law at each finite level remains the same, but the counit changes when we base change. Thus we have the following facts:

1) There is a Frobenius map $F : G \to G^{(p)}$, which arises from the $Frob$ maps. There is also the Verschiebung $V : G^{(p)} \to G$ coming from each finite level. (The $ver : G^{(p)} \to G$ at each finite level arises via Cartier duality from $Frob$, at least for commutative group schemes.) They satisfy $VF = [p]_G$ and $FV = [p]_{G^{(p)}}$.
2) If G has height h then $G^{(p)}$ also has height h and F, V are surjective with finite kernel of order $\leq p^h$.

Looking back at the earlier notation, we want to show that $\varprojlim A_v \simeq k[[x_1,\dots,x_n]]$. We'll use the map F to create another collection of objects $\{B_v\}$ such that $\varprojlim_v A_v = \varprojlim_v B_v$[2] and we have a better handle on B_v.

Let Spec $B_v := H_v := \ker(G \xrightarrow{F^v} G^{(p^v)})$. It is a fact that $\varprojlim A_v = \varprojlim B_v$, because $H_v \subset G_v$ and also $G_v \subset H_N$ for some large enough N, as every finite flat group scheme is killed by a sufficiently large power of Frobenius. Thus $\varprojlim A_v = \varprojlim B_v =: \mathscr{A}$, say. Let I_v be the maximal ideal of B_v. Then $I := \varprojlim I_v$ is the maximal ideal of $\mathscr{A}$.

Let $a_1,\dots,a_n$ be elements of I whose images form a k-basis for I_1/I_1^2. Then it can be checked that these also form a k-basis for I_v/I_v^2. Thus, by Nakayama's Lemma, the maps

$$u_v : k[[x_1,\dots,x_n]] \to B_v \ , \ x_i \to a_i$$

are surjective. The kernel of u_v contains $J_v := (x_1^{p^v},\dots,x_n^{p^v})$, since by definition, H_v is the kernel of F^v. But, it can be shown that rank $B_v = p^{nv}$ and codimension of J_v in $k[[x_1,\dots,x_n]]$ is p^{nv}. Thus, we see that

$$u_v : k[[x_1,\dots,x_n]]/J_v \simeq B_v$$

is an isomorphism, and taking inverse limits, we see that

$$\varprojlim u_v : k[[x_1,\dots,x_n]] \to \varprojlim B_v$$

is the required isomorphism. (With the right topology)

□

We conclude with a definition that arises from the theorem:

Definition. *Dimension of a p-divisible group G is defined to be the dimension of the divisible formal Lie group associated to* G^0.

Example 2. Working out $\widehat{\mathbf{G}}_m(p)$ versus (μ_{p^∞}).

[1] This is one of the two important aspects of the proof.
[2] This is the second major aspect of the proof.

We expect that (μ_{p^∞}) is the p-divisible group corresponding to $\widehat{\mathbf{G}}_m$ via this equivalence. Let's consider these over $R = \mathbf{Z}_p$ and $k = \mathbf{F}_p$. We know that, at each finite level, $\mu_{p^v} =$ Spec $R[x]/(x^{p^v} - 1)$. Over $k = \mathbf{F}_p$, we have μ_{p^v} Spec $k[x]/(x^{p^v} - 1) =$ Spec $k[x]/(x-1)^{p^v}$.

Thus, over k, $A_v = k[x]/(x-1)^{p^v}$. What is B_v? The kernel of $(Frob)^v$ on μ_{p^v} should be all of Spec A_v, so that $B_v = A_v$. By a coordinate change $x \to 1 + T$, we see that B_v is indeed isomorphic to $k[T]/T^{p^v}$. It is also clear that $\varprojlim A_v = \varprojlim B_v = k[[T]]$ and that the group law, transferred from the group laws on μ_{p^v}, is the same as the group law on $\widehat{\mathbf{G}}_m$.

The situation is not immediate for R, since $R[x]/(x^{p^v} - 1)$ is not isomorphic to $R[x]/(x-1)^{p^v}$. It is still true and classically known, that $\varprojlim_v R[x]/(x^{p^v} - 1) \simeq R[[T]]$. So that in this special case, the correspondence can be checked. Tate's proof gives us a general argument working for all cases, and in particular it shows us how to go from the preceding paragraph about k to this paragraph about R completely generally, without using any particular structure on R.

References

[1] M. Liponowski. p-divisible groups. *Online*, 2010. `http://dl.dropbox.com/u/1589321/Faltings seminar/L09.pdf`.

[2] J. T. Tate. p-divisible groups. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.