p-Divisible Groups

V5A4 – Selected Topics in Algebraic Geometry – p-adic Hodge theory
Masters lecture course, Universität–Bonn,
Winter Semester 2015/16, Wednesday 16.00–18.00, Seminar room 0.007
`http://www.math.uni-bonn.de/people/morrow/WS1516/index.html`

Matthew Morrow (`morrow@math.uni-bonn.de`, office 4.027)

Overview

This course will provide an introduction to p-adic Hodge theory, a major area of arithmetic geometry, through *p-divisible groups* (these are also known as *Barsotti–Tate groups*, since the term "p-divisible group" is so ambiguous). Historically, results and conjectures surrounding p-divisible groups were the main stimulus for the development of p-adic Hodge theory, and they continue to be relevant in modern research.

We will cover the material in John Tate's seminal 1967 paper "p-Divisible Groups", though often with different proofs and providing many more details and examples; this will include affine group schemes, p-divisible groups, Tate–Sen theory, Hodge–Tate decomposition of a p-divisible group, applications to abelian varieties. Then we may do some Dieudonné theory to study p-divisible groups in characteristic p.

Prerequisites: Standard commutative algebra (e.g., tensor products of k-algebras; local rings), the first definitions of category theory (e.g., category, functor), and basic algebraic geometry (e.g., the fact that the category of affine k-schemes is the opposite of the category of k-algebras), will be sufficient for most of the course. The main applications of the theory concern abelian varieties, which require some heavier knowledge of algebraic geometry, but these will not appear until later in the course.

1 Affine group schemes

1.1 Groups

Before giving the first main definition of the course, it will be useful to consider groups from a different (more categorical) point of view. A *commutative group* (in the usual sense) is the data (G, m, e, i) of

(i) a set G,

(ii) functions "multiplication" $m : G \times G \to G$, "unit" $e : \{1\} \to G$, and "inverse" $i : G \to G$,

such that the following diagrams commute:

(I) "Associativity"

$$\begin{tikzcd}
G \times G \times G \arrow[r, "m \times \mathrm{id}_G"] \arrow[d, "\mathrm{id}_G \times m"] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"'] & G
\end{tikzcd}$$

i.e., $m(m(a,b),c) = m(a, m(b,c))$ for all $a, b, c \in G$.

(II) "e(1) is a left unit"

$$\begin{tikzcd}
\{1\} \times G \arrow[r, "e \times \mathrm{id}_G"] \arrow[dr, "="'] & G \times G \arrow[d, "m"] \\
 & G
\end{tikzcd}$$

i.e., $m(e(1), a) = a$ for all $a \in G$.

(III) "Existence of left inverses"

$$\begin{tikzcd}
G \times G \arrow[rr, "i \times \mathrm{id}_G"] & & G \times G \arrow[d, "m"] \\
G \arrow[u, "\mathrm{diag}"] \arrow[dr, "1"'] & & G \\
 & \{1\} \arrow[ur, "e"'] &
\end{tikzcd}$$

i.e., $m(i(a), a) = e(1)$ for all $a \in G$.

(IV) "Commutativity"

$$\begin{tikzcd}
G \times G \arrow[r, "\mathrm{swap}"] \arrow[dr, "m"'] & G \times G \arrow[d, "m"] \\
 & G
\end{tikzcd}$$

i.e., $m(b,a) = m(a,b)$ for all $a, b \in G$.

Similarly, a *commutative topological group* is the data (G, m, e, i) of a topological space G and continuous functions $m : G \times G \to G,\ e : \{1\} \to G,\quad i : G \to G$, such that diagrams (I)–(IV) commute. And a *commutative Lie group* is data (G, m, e, i) of a manifold G, and smooth functions $m : G \times G \to G,\ e : \{1\} \to G,\quad i : G \to G$, such that diagrams (I)–(IV) commute.

In general, if $\mathcal{C}$ is a category with a final object 0 (i.e., each object of $\mathcal{C}$ has a unique morphism to 0) and in which products make sense, then a *commutative group object* in $\mathcal{C}$ is the data (G, m, e, i) of an object $G \in \operatorname{Ob}\mathcal{C}$ and morphisms $m : G \times G \to G$, $e : 0 \to G,\quad i : G \to G$, such that diagrams (I)–(IV) commute in $\mathcal{C}$.

In particular, the above discussion shows that a commutative group is the same thing as a commutative group object in the category of sets.

1.2 Affine groups schemes

Until stated otherwise, k denotes any commutative ring. The category of affine k-schemes is denoted by Aff_k, and we assume the reader is familiar with the anti-equivalence of categories

$$k\text{-alg} \xrightarrow{\simeq} \mathrm{Aff}_k, \quad A \mapsto \operatorname{Spec} A.$$

Note that Aff_k has a zero object, namely $\operatorname{Spec} k$, and a product given by $\times_k$, which corresponds to $\otimes_k$ under the anti-equivalence. The following is the first main definition of the course:

Definition 1.1. A *affine commutative group scheme G over k* is a commutative group object in the category Aff_k. In light of the anti-equivalence $k\text{-alg} \overset{\simeq}{\to} \mathrm{Aff}_k$, this means that $G = \operatorname{Spec} A$, where

(i) A is a k-algebra equipped with

(ii) homomorphisms of k-algebras called the "comultiplication" $\mu : A \to A \otimes_k A$, "counit" $\varepsilon : A \to k$, and "antipode" $\iota : A \to A$,

such that the opposites of diagrams (I)–(IV) commute after replacing $\times$ by $\otimes_k$:

(1) "Coassociativity"

$$\begin{tikzcd}
A \otimes_k A \otimes_k A & A \otimes_k A \arrow[l, "\mu\otimes\mathrm{id}_A"'] \\
A \otimes_k A \arrow[u, "\mathrm{id}_A \otimes\mu"] & A \arrow[l, "\mu"] \arrow[u, "\mu"']
\end{tikzcd}$$

(2) "ε is a left counit"

$$\begin{tikzcd}
k \otimes_k A & A \otimes_k A \arrow[l, "\varepsilon\otimes\mathrm{id}_A"'] \\
 & A \arrow[u, "\mu"] \arrow[ul, "="]
\end{tikzcd}$$

(3) "Existence of left coinverses"

$$\begin{tikzcd}
A\otimes_k A \arrow[d, "\mathrm{mult}"'] & & A\otimes_k A \arrow[ll, "\iota\otimes\mathrm{id}_A"'] \\
A & & A \arrow[u, "\mu"] \arrow[dl, "\varepsilon"] \\
& k \arrow[ul, "e"] &
\end{tikzcd}$$

(4) "Cocommutativity"

$$\begin{tikzcd}
A\otimes_k A & A\otimes_k A \arrow[l, "\mathrm{swap}"'] \\
& A \arrow[u, "\mu"] \arrow[ul, "\mu"]
\end{tikzcd}$$

The data $(A,\mu,\varepsilon,\iota)$ is known as a *cocommutative Hopf algebra over k*.

Thus a commutative affine group scheme G is exactly the same thing as a cocommutative Hopf algebra, but whether the geometric or algebraic point of view is more useful depends on the context. The standard notation for passing between these points of view is as follows:

- Given the group scheme G, the associated Hopf algebra is $(\mathcal{O}(G),\mu_G,\varepsilon_G,\iota_G)$.
- Given the Hopf algebra $(A,\varepsilon,\mu,\iota)$, the associated group scheme is $G=\operatorname{Spec}A$ (with ε,μ,ι suppressed from the notation).

Remark 1.2. (i) If $(A,\mu,\varepsilon,\iota)$ is an cocommutative Hopf algebra, then it easily follows from diagram (4) that "ε is a right counit" and "right coinverses exist", in the sense that the following diagrams commute:

(2')
$$\begin{tikzcd}
k\otimes_k A & A\otimes_k A \arrow[l, "\mathrm{id}_A\otimes\varepsilon"'] \\
& A \arrow[u, "\mu"] \arrow[ul]
\end{tikzcd}$$

(3')
$$\begin{tikzcd}
A\otimes_k A \arrow[d, "\mathrm{mult}"'] & & A\otimes_k A \arrow[ll, "\mathrm{id}_A\otimes\iota"'] \\
A & & A \arrow[u, "\mu"] \arrow[dl, "\varepsilon"] \\
& k \arrow[ul, "e"] &
\end{tikzcd}$$

(ii) If diagrams (1), (2), (2'), (3), and (3') all commute, but not necessarily (4), then G is simply called an *affine group scheme*, or $(A,\mu,\varepsilon,\iota)$ is called a *Hopf algebra, over k* but we do not study them in this course. Hence, for simplicity, we will henceforth always say "affine group scheme" to mean "affine commutative group scheme"; this is a relatively common notational simplification, but you should still be careful when consulting the literature. Similarly, we will say "Hopf algebra" to mean "cocommutative Hopf algebra".

(iii) If $(A,\mu,\varepsilon,\iota)$ is a Hopf algebra, then $\iota^2=\mathrm{id}_A$. This is a helpful exercise, which we will give an easy proof of later in Lemma 1.13 using the language of points.

Now we devote some time to examples:

Example 1.3 (Group algebras)**.** Let Γ be a commutative group, and $k[\Gamma]$ its group algebra, i.e., $k[\Gamma]$ is the free k-module with basis set Γ and convolution product:

$$\sum_{g\in G} a_g g * \sum_{g\in G} b_g g := \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g,$$

where $a_g, b_g \in k$, and all but finitely many of them are zero.

Define functions

$$\begin{aligned} \mu : k[\Gamma] \to k[\Gamma]\otimes_k k[\Gamma], \quad & \sum_{g\in\Gamma} a_g g \mapsto \sum_{g\in\Gamma} a_g (g\otimes g) \\ \varepsilon : k[\Gamma] \to k, \quad & \sum_{g\in\Gamma} a_g g \mapsto \sum_{g\in\Gamma} a_g \\ \iota : k[\Gamma] \to k[\Gamma], \quad & \sum_{g\in\Gamma} a_g g \mapsto \sum_{g\in G} a_{g^{-1}} g \end{aligned}$$

Proposition 1.4. *The data $(k[\Gamma], \varepsilon, \mu, \iota)$ is a Hopf algebra over k.*

Proof. It is an easy exercise that ε, μ, ι are homomorphisms of k-algebras. It remains to check that diagrams (1)–(4) commute; since these diagrams are k-linear and since $k[\Gamma]$ is the free k-module on the set Γ, it is enough to check commutativity on the elements $g \in k[\Gamma]$, for each $g \in \Gamma$.

Diagram (1): $g \otimes g \otimes g = g \otimes g \otimes g$, which is true.

Diagram (2): $1 \otimes g = 1 \otimes g$.

Diagram (3): $\mathrm{mult} \circ (\iota \otimes \mathrm{id}) \circ \mu(g) = \mathrm{mult} \circ (\iota \otimes \mathrm{id})(g \otimes g) = \mathrm{mult}(g^{-1} \otimes g) = 1$.

Diagram (4): $\mathrm{swap} \circ \mu(g) = \mathrm{swap}(g \otimes g) = g \otimes g = \mu(g)$. □

The next two example are special cases of $k[\Gamma]$, which give rise to two of our most important example of affine group schemes, namely $\mathbb{G}_{m,k}$ and $\boldsymbol{\mu}_{n,k}$:

Example 1.5 (The multiplicative group)**.** If Γ is an infinite cyclic group, and we pick a generator of Γ, then there is a resulting isomorphism of k-algebras $k[\Gamma] \cong k[t, t^{-1}]$ (Laurent polynomial algebra) which sends the chosen generator to t; under this identification the maps μ, ε, ι of the previous example are characterised by

$$\mu(t) = t \otimes t, \qquad \varepsilon(t) = 1, \qquad \iota(t) = t^{-1}.$$

The associated affine group scheme $\mathrm{Spec}\, k[t, t^{-1}]$ is known as the *multiplicative group over k* and denoted by $\mathbb{G}_{m,k}$.

Example 1.6 (Roots of unity)**.** If Γ is a cyclic group of order $n \geq 1$, and we pick a generator of Γ, then there is a resulting isomorphism of k-algebras $k[\Gamma] \cong k[t]/(t^n - 1)$ which sends the chosen generator to t; under this identification the maps μ, ε, ι are again characterised by the facts that

$$\mu(t) = t \otimes t, \qquad \varepsilon(t) = 1, \qquad \iota(t) = t^{-1}.$$

The associated affine group scheme $\mathrm{Spec}\, k[t]/(t^n - 1)$ is known as the *group of n^{th} roots of unity over k* and denoted by $\boldsymbol{\mu}_{n,k}$.

Example 1.7 (The additive group)**.** We will equip the ring of polynomials $k[t]$ with the structure of a Hopf algebra, by defining

$$\begin{aligned}\mu : k[t] \to k[t] \otimes_k k[t], &\quad \sum_{n\geq 0} a_n t^n \mapsto \sum_{n\geq 0} a_n(t\otimes 1 + 1\otimes t)^n\\ \varepsilon : k[t] \to k, &\quad f \mapsto f(0)\\ \iota : k[t] \to k[t], &\quad \sum_{n\geq 0} a_n t^n \mapsto \sum_{n\geq 0} (-1)^n a_n t^n\end{aligned}$$

We check in the next proposition that this is indeed a Hopf algebra. The associated affine group scheme $\operatorname{Spec} k[t]$ is called the *additive group over* k and denoted by $\mathbb{G}_{a,k}$.

Proposition 1.8. *The data* $(k[t], \mu, \varepsilon, \iota)$ *is a Hopf algebra over* k*.*

Proof. It is again an easy exercise that μ, ε, ι are homomorphisms of k-algebras. Hence all the maps in diagrams (1)–(4) are maps of k-algebras, and so it is enough to check commutativity on the element $t \in k[t]$.

Diagram (1): Both routes around the diagram give $t\otimes 1\otimes 1 + 1\otimes t\otimes t + 1\otimes 1\otimes t$.

Diagram (2): Both routes around the diagram give $1 \otimes t$.

Diagrams (3), (4): left to the reader. □

Example 1.9. (A stranger example: $G_{(a,b),k}$) Fix elements $a, b \in k$ satisfying $ab = 2$, and put $A := k[t]/(t^2 + at)$. Then the element

$$(t\otimes 1 + 1\otimes t + bt\otimes t)^2 + a(t\otimes 1 + 1\otimes t + bt\otimes t)$$

of A is zero (Check this!), and so there is a map of k-algebras $\mu : A \to A\otimes_k A$ characterised by $\mu(t) = t\otimes 1 + 1\otimes t + bt\otimes t$. Also set $\varepsilon : A \to k$, $f \mapsto f(0)$, and $\iota = \mathrm{id}_A : A \to A$.

It is not hard to check that $(A, \mu, \varepsilon, \iota)$ is a Hopf algebra over k; the associated affine group scheme $\operatorname{Spec} A$ is sometimes denoted by $G_{(a,b),k}$ (or some variant on this notation).

Example 1.10 (The trivial/zero affine group scheme over k)**.** Let $A = k$, and define

$$\begin{aligned}\mu : k \xrightarrow{\simeq} k\otimes_k k, &\quad a \mapsto a\otimes 1 = 1\otimes a\\ \varepsilon : k \to k, &\quad a \mapsto a\\ \iota : k \to k, &\quad a \mapsto a\end{aligned}$$

These are clearly maps of k-algebras which makes diagrams (1)–(4) commute, and so $(k, \mu, \varepsilon, \iota)$ is a Hopf algebra over k, which we call the *trivial* Hopf algebra. The associated affine group scheme $\operatorname{Spec} k$ is called the *trivial*, or *zero, group scheme over* k and denoted by 0_k (or, later, simply by 0 when it is unlikely to cause confusion).

We finish this introductory section by noting that comultiplication and the antipode are predetermined modulo $\operatorname{Ker}\varepsilon$:

Lemma 1.11. *Let* $(A, \mu, \varepsilon, \iota)$ *be a Hopf algebra over* k*. Then:*

(i) the map $k \oplus \operatorname{Ker}\varepsilon \to A$, $(a, b) \mapsto a + b$ *is an isomorphism of* k*-modules;*

(ii) $\mu(a) \equiv -\varepsilon(a) + a\otimes 1 + 1\otimes a$ *mod* $\operatorname{Ker}\varepsilon \otimes_k \operatorname{Ker}\varepsilon$*;*

(iii) $\iota(a) \equiv -a$ *mod* $(\operatorname{Ker}\varepsilon)^2$ *for any* $a \in \operatorname{Ker}\varepsilon$*.*

Proof. (i): The inverse map $A \to k \oplus \operatorname{Ker}\varepsilon$ is given by $a \mapsto (\varepsilon a, a - \varepsilon(a))$: note that ε satisfies $\varepsilon(a) = a$ for any $a \in k$, since it is a homomorphism of k-algebras.

(ii): Part (i) allows us to write

$$A \otimes_k A = k \oplus (\operatorname{Ker}\varepsilon \otimes_k k) + (k \otimes_k \operatorname{Ker}\varepsilon) + (\operatorname{Ker}\varepsilon \otimes_k \operatorname{Ker}\varepsilon)$$

(the first copy of k really means $k \cdot 1_A \otimes 1_A$). So if $a \in A$ then we may write

$$\mu(a) = b + c \otimes 1 + 1 \otimes d + z$$

where $b \in k$, $c, d \in \operatorname{Ker}\varepsilon$, and $z \in \operatorname{Ker}\varepsilon \otimes_k \operatorname{Ker}\varepsilon$.

Diagram (2) implies that $a = (\varepsilon \otimes \mathrm{id}_A)(b + c \otimes 1 + 1 \otimes d + z) = b1_A + d$. Similarly, diagram (2') implies that $a = b1 + c$. Applying ε shows that $b = \varepsilon(a)$. In conclusion,

$$\mu(a) = \varepsilon(a) + (a - \varepsilon(a)) \otimes 1 + 1 \otimes (a - \varepsilon(a)) + z = -\varepsilon(a) + a \otimes 1 + 1 \otimes a + z,$$

as required.

(iii): Apply diagram (3) to part (ii) – Check this! □

End of Lecture 1

1.3 Points of an affine group scheme

The notion of the points of an affine group scheme with values in a k-algebra is extremely important:

Definition 1.12 (Points in a k-algebra)**.** For any k-algebra R, the functor of points $\operatorname{Hom}_{\mathrm{Aff}_k}(\operatorname{Spec} R, -) : \mathrm{Aff}_k \to \mathrm{Sets}$ is a covariant functor taking $\otimes_k$ to $\times$ and $\operatorname{Spec} k$ to $\{1\}$. Hence it takes an affine group scheme G to a commutative group $G(R)$.[1]

Explicitly, if $G = \operatorname{Spec} A$, then

$$G(R) = \operatorname{Hom}_{\mathrm{Aff}_k}(\operatorname{Spec} R, G) = \operatorname{Hom}_{k\text{-alg}}(A, R),$$

with operations:

- addition $G(R) \times G(R) \to G(R)$ given by

$$(f, g) \mapsto \text{ the composition } A \xrightarrow{\mu} A \otimes_k A \xrightarrow{f \otimes g} R \otimes_k R \xrightarrow{\text{mult}} R$$

- zero element given by $A \xrightarrow{\varepsilon} k \to R$.
- inverse $G(R) \to G(R)$ given by $f \mapsto f \circ \iota$.

N.B., although we typically view $G(R)$ as a group under addition, sometimes it will be more convenient to denote the operator multiplicatively.

[1] This is a general construction: If $F : \mathcal{C} \to \mathcal{D}$ is a functor between categories which takes products to products, and takes a final object $0_{\mathcal{C}}$ to a final object $0_{\mathcal{D}}$, then F can be applied to any group object in $\mathcal{C}$ to yield a group object in $\mathcal{D}$.

In particular, taking $R = A$, the previous construction equips $G(A) = \mathrm{End}_{k\text{-alg}}(A)$ with the structure of a commutative group[2] sometimes called the "universal points" of G. This provides a standard technique to prove results by using knowledge of groups, of which the following is the simplest example:

Lemma 1.13. *If $(A, \mu, \varepsilon, \iota)$ is a Hopf algebra, then $\iota^2 = \mathrm{id}_A$.*

Proof. By the previous definition, $\mathrm{End}_{k\text{-alg}}(A)$ is a commutative group in which the inverse of an element f is $f \circ \iota$; hence $f \circ \iota^2 = f \circ \iota \circ \iota$ is the inverse of the inverse of f, i.e., it is f. Taking $f = \mathrm{id}_A$ proves the claim. □

Now we check how the points look for our standard examples of affine group schemes, justifying their names:

Proposition 1.14. *For any k-algebra R, there are isomorphisms of groups*

$$\mathbb{G}_{m,k}(R) \overset{\simeq}{\to} R^\times, \qquad \boldsymbol{\mu}_{n,k}(R) \overset{\simeq}{\to} \{x \in R^\times : x^n = 1\}, \qquad \mathbb{G}_{a,k}(R) \overset{\simeq}{\to} R^+$$

where $R^\times$ is the group (under multiplication) of invertible elements in R, and R^+ is the underlying additive subgroup of R.

Proof. Recall from Example 1.6 that $\mathbb{G}_{m,k} = \operatorname{Spec} k[t, t^{-1}]$, with Hopf algebra structure given by $\mu(t) = t \otimes t$, $\varepsilon(t) = 1$, and $\iota(t) = t^{-1}$. There is certainly a bijection of sets

$$\mathrm{ev}_t : \mathbb{G}_{m,k}(R) = \mathrm{Hom}_{k\text{-alg}}(k[t, t^{-1}], R) \xrightarrow{\simeq} R^\times, \quad f \mapsto f(t),$$

so we must check that this bijection respect the unit element and product structure on both sides. Firstly, the identity $\mathrm{ev}_t(\varepsilon) = 1$ is easy. Secondly, fixing $f, g \in \mathbb{G}_{m,k}(R)$, recall from the previous definition that their product (this is the main example in which we view $G(R)$ multiplicatively rather than additively!) fg is given by the morphism of k-algebras

$$A \overset{\mu}{\to} A \otimes_k A \xrightarrow{f \otimes g} R \otimes_k R \xrightarrow{\text{mult}} R;$$

hence $\mathrm{ev}_t(fg) = \mathrm{mult}((f \otimes g)(t \otimes t)) = \mathrm{mult}(f(t) \otimes g(t)) = f(t)g(t)$, and so ev_t is a homomorphism of groups. Since ev_t is bijective, we have proved it is an isomorphism of groups.

"Evaluation at t" also defines bijections of sets

$$\boldsymbol{\mu}_{n,k}(R) \overset{\simeq}{\to} \{x \in R^\times : x^n = 1\}, \qquad \mathbb{G}_{a,k}(R) \overset{\simeq}{\to} R^+,$$

but we leave it to the reader as a very important exercise to verify that they are actually isomorphisms of groups. □

Example 1.15. Recall the affine group scheme $G_{(a,b),k}$ from Example 1.9. Then evaluation at t again defines an isomorphism of groups

$$G_{(a,b),k}(R) \xrightarrow{\simeq} \{x \in R : x^2 + ax = 0\},$$

where the right is equipped with addition law $x +_{a,b} y := x + y + bxy$.

[2] In fact, if $(A, \mu, \varepsilon, \iota)$ is the usual data of a Hopf algebra but we do not assume that diagrams (1)–(4) commute, then $G(A)$ being a commutative group under the previous construction is *equivalent* to the commutativity of diagrams (1)–(4). In other words, $G(A)$ being a group is completely characterising that A is a Hopf algebra.

2 The category of affine group schemes

k continues to be any (commutative) ring. In this section we develop enough properties of the category of affine group schemes so that we can manipulate them as though they were honest groups. In particular, we will discuss subgroups, kernels, quotients, exact sequences, and show that the category is additive.[3]

Most importantly, for any affine group scheme G, and $n \geq 0$, we will define the *sub affine group scheme $G[n]$ of n-torsion points*, which is essential in order to define p-divisible groups.

2.1 Sub affine group schemes

Definition 2.1. Let $G = \operatorname{Spec} A$ be an affine group scheme over k. A *sub affine group scheme* $H \subseteq G$ (or just *subgroup*) is an affine group scheme which is a closed subscheme of G compatibly with the product, unit, and inverse. In other words $H = \operatorname{Spec} A/I$, where $I \subseteq A$ is an ideal and $(A/I, \overline{\mu}, \overline{\varepsilon}, \overline{\iota})$ is a quotient Hopf algebra of $(A, \mu, \varepsilon, \iota)$ in the obvious sense, i.e., the following diagrams commute:

$$\begin{tikzcd}
A \arrow[r, "\mu"] \arrow[d] & A \otimes_k A \arrow[d] \\
A/I \arrow[r, "\overline{\mu}"'] & A/I \otimes_k A/I
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\varepsilon"] \arrow[d] & k \\
A/I \arrow[ur, "\overline{\varepsilon}"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[d] & A \arrow[d] \\
A/I \arrow[r, "\overline{\iota}"'] & A/I
\end{tikzcd}$$

It should now be clear that sub affine group schemes of G are in one-to-one correspondence with ideals I of A satisfying the following three conditions:

$$\mu(I) \subseteq \operatorname{Ker}(A \otimes_k A \to A/I \otimes_k A/I), \quad \varepsilon(I) = 0, \quad \iota(I) \subseteq I.$$

Such ideals are called *Hopf ideals* of A.

Example 2.2. The zero group scheme 0_k is the sub affine group scheme of G corresponding to the Hopf ideal $\operatorname{Ker} \varepsilon \subseteq A$. At the other extreme, G is a sub affine group scheme of itself, corresponding to the zero ideal.

Example 2.3. Let Γ be a commutative group, and $\Gamma' \subseteq \Gamma$ a subgroup. Then $k[\Gamma]$ contains a Hopf ideal

$$I := \{\sum_{g \in \Gamma} a_g g \in k[\Gamma] : \sum_{g' \in \Gamma'} a_{g+g'} = 0 \; \forall g \in \Gamma\},$$

and the quotient Hopf algebra $k[\Gamma]/I_{\Gamma'}$ is isomorphic to $k[\Gamma/\Gamma']$.

Example 2.4. Taking $\Gamma' := n\mathbb{Z} \subseteq \Gamma := \mathbb{Z}$ in the previous example, we see that $\boldsymbol{\mu}_{n,k}$ is the sub affine group scheme of $\mathbb{G}_{m,k}$ corresponding to the Hopf ideal $(t^n - 1)$ of $k[t, t^{-1}] = \mathcal{O}(\mathbb{G}_{m,k})$.

The next two results concern sub affine group schemes of $\mathbb{G}_{a,k}$ (see Example 1.7 if you need a reminder on the Hopf algebra structure on $k[t] = \mathcal{O}(\mathbb{G}_{a,k})$):

[3] A category $\mathcal{C}$ is *additive* if and only if each set of morphisms has the structure of an abelian group, in such a way that composition $\operatorname{Hom}(H, F) \times \operatorname{Hom}(G, H) \to \operatorname{Hom}(G, F)$ is bilinear.

Proposition 2.5. *Let $f = \sum_{i=0}^d a_i t^i \in k[t]$ be a monic[4] polynomial $\neq t$. Then the ideal (f) is a Hopf ideal of $k[t]$ if and only if*

(i) there is a prime number $p > 0$ (necessarily unique) which is zero in k,

(ii) and $a_i = 0$ whenever i is not a power of p.

Proof. Recall that (f) is a Hopf ideal if and only if the following three conditions hold:

$$\mu(f) \in \operatorname{Ker}(k[t] \otimes_k k[t] \to k[t]/(f) \otimes_k k[t]/(f)), \quad \varepsilon(f) = 0, \quad \iota(f) \in (f). \qquad (\dagger)$$

The first condition says that $\sum_{i=0}^n a_i(t \otimes 1 + 1 \otimes t)^n$ vanishes in $k[t]/f \otimes_k k[t]/f$. Since the latter ring is a free k-module with basis $t^i \otimes t^j$, $0 \leq i, j < n$, we easily see by a binomial expansion that the vanishing is equivalent to the vanishing in k of $a_i\binom{n}{j} = 0$ for all $0 < j < i \leq n$, which in turn is equivalent to the vanishing of $a_i \gcd_{1<j<i} \binom{n}{j} = 0$ for $0 < i \leq n$.

But it is reasonably well-known that

$$\gcd_{1 \leq j < i} \binom{i}{j} = \begin{cases} p & i = p^r \text{ for some } r \geq 1 \text{ and prime number } p > 0 \\ 1 & \text{else} \end{cases}$$

and so the first condition in (†) is equivalent to the vanishing of the following elements of k: a_i whenever i is not a power of some prime number p, and pa_i whenever i is a power of some prime number p. In particular, since $a_d = 1$, we see that $d = p^n$ for a certain prime number p which is zero in k. All other prime numbers are therefore invertible in k, and so the first condition in (†) is equivalent to having $a_i = 0$ whenever i is not a power of p.

In summary, the first condition appearing in (†) is true if and only if f has the form $f = \sum_{i=0}^n b_i t^{p^i}$ for some $b_i \in k$. Then the other two conditions in (†) are always true: $\varepsilon(f) = f(0) = 0$, and $\iota(f) = \sum_{i=0}^n b_i(-t)^{p^i} = (-1)^p f$. □

Definition 2.6. When a prime number p is zero in k, the sub affine group scheme of $\mathbb{G}_{a,k}$ corresponding to the Hopf ideal $(t^{p^r}) \subseteq k[t]$ is denoted by $\boldsymbol{\alpha}_{p^r,k}$.

Corollary 2.7. *Suppose that k is a field. Then the following affine group scheme over k contains no proper, non-zero sub affine group scheme:*

(i) $\mathbb{G}_{a,k}$, if $\operatorname{char} k = 0$;

(ii) $\boldsymbol{\alpha}_{p,k}$, if $\operatorname{char} k = p > 0$;

Proof. By standard commutative algebra, any ideal of $k[t]$ is generated by a single monic polynomial.

So, if $\operatorname{char} k = 0$, then the previous proposition implies that the only proper sub affine group scheme G of $\mathbb{G}_{a,k}$ corresponds to the Hopf ideal $(t) = \operatorname{Ker} \varepsilon$, so that $G = 0_k$.

On the other hand, if $\operatorname{char} k = p > 0$, then any proper sub affine group scheme G of $\boldsymbol{\alpha}_{p,k}$ corresponds to a Hopf ideal I of $k[t]$ which contains t^p, and then previous proposition again implies that $I = (t)$, whence again $G = 0_k$. □

[4] Exercise: See what happens if we do not assume that f is monic.

Remark 2.8 (Points of a sub affine group scheme)**.** If H is a sub affine group scheme of $G = \operatorname{Spec} A$ corresponding to Hopf ideal $I \subseteq A$, then, for any k-algebra R, the R-points $H(R)$ is a subgroup of $G(R)$, via

$$H(R) = \mathrm{Hom}_{k\text{-alg}}(A/I, R) = \{f \in G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R) : f(I) = 0\} \subseteq G(R).$$

Check this if you are uncertain.

For example, recall from Proposition 1.14 that there is an isomorphism of groups $\mathrm{ev}_t : \mathbb{G}_{a,k}(R) \overset{\cong}{\to} R^+$; under this isomorphism, and assuming that a prime number p is zero in k, the group $\boldsymbol{\alpha}_{p^r,k}(R)$ identifies with the subgroup $\{x \in R^+ : x^{p^r} = 0\}$ of R^+.

2.2 Morphisms of affine groups schemes

Now we study maps between affine group schemes.

Definition 2.9. Let $G = \operatorname{Spec} A$ and $F = \operatorname{Spec} B$ be affine group schemes over k. A *morphism* $\Phi : G \to F$ is a morphism in Aff_k which is compatible with the multiplications, units, and inversions. In other words, it is a homomorphism of k-algebras $\phi : B \to A$ satisfying $\mu\phi = (\phi \otimes \phi)\mu'$, $\varepsilon\phi = \varepsilon'$, and $\iota\phi = \phi\iota'$, which is called a homomorphism of Hopf algebras.

The set of morphisms from G to F is denoted as usual by $\mathrm{Hom}(G, F)$, and the category of affine group schemes will be denoted by AC_k.[5]

Φ is said to be an *isomorphism* if and only if it is an isomorphism of schemes, i.e. ϕ is an isomorphism of k-algebras.

Remark 2.10. If R is a k-algebra, then any morphism $\Phi : G \to F$ induces a homomorphism of groups

$$\Phi_R : G(R) = \mathrm{Hom}_{k\text{-alg}}(A, R) \to F(R) = \mathrm{Hom}_{k\text{-alg}}(B, R), \quad f \mapsto f \circ \phi.$$

In other words, $G \mapsto G(R)$ is a functor from AC_k to the category of abelian groups.[6]

Example 2.11. For any affine group scheme G, there is a unique morphism of affine group schemes $G \to 0_k$ (it is given by the algebra structure map $k \to A$), and a unique morphism $0_k \to G$ (it is given by the counit $\varepsilon : A \to k$). Check both of these. In categorical language, 0_k is the *zero object* of the category AC_k.

If F is another group scheme, the *zero morphism* from G to H is by definition the composition $G \to 0_k \to H$.

Example 2.12. Recall the affine group scheme $G_{(a,b),k}$ from Example 1.9. There is an isomorphism $G_{(a,b),k} \cong G_{(a',b'),k}$ if and only if there exists a unit $u \in A^\times$ such that $a' = ua$ and $b' = u^{-1}b$.

Example 2.13. Suppose that a prime number p is zero in k. Then $\boldsymbol{\mu}_{p,k} = \operatorname{Spec} k[t]/(t^p - 1)$ and $\boldsymbol{\alpha}_{p,k} = \operatorname{Spec} k[t]/(t^p)$ are isomorphic as k-schemes, via the isomorphism of k-algebras

$$k[t]/(t^p) \overset{\cong}{\to} k[t]/(t^p - 1), \quad t \mapsto t - 1$$

(note that $t^p - 1 = (t-1)^p$), but they are not isomorphic as affine group schemes (we will prove this later).

[5] There is no standard notation for this category; the C is to remind us that our affine group scheme are commutative

[6] The categorically inclined reader may to formulate a general statement: any functor between categories induces a functor on the associated categories of group objects.

Example 2.14. For each $n \geq 1$, let's see that $\phi_n : k[t, t^{-1}] \to k[t, t^{-1}]$, $f(t) \mapsto f(t^n)$ is a homomorphism of Hopf algebras (as usual, the Hopf algebra structure on $k[t, t^{-1}]$ is the one defining $\mathbb{G}_{a,k}$). Indeed, for any $f(t) \in k[t, t^{-1}]$, we have

$$(\phi \otimes \phi)(\mu(t)) = (\phi \otimes \phi)(t \otimes t) = t^n \otimes t^n = (t \otimes t)^n = \mu(t)^n = \mu(t^n) = \mu(\phi(t))$$

$$\varepsilon(\phi(f(t))) = \varepsilon(f(t^n)) = f(1^n) = f(1) = \varepsilon(f(t))$$
$$\iota(\phi(f(t))) = \iota(f(t^n)) = f(t^{-n}) = \phi(f(t^{-1})) = \phi(\iota(f(t)))$$

In other words, we have defined a morphism of group schemes $\Phi_n : \mathbb{G}_{m,k} \to \mathbb{G}_{m,k}$. Now suppose that R is a k-algebra. Recall:

- from Remark 2.10 that Φ_n induces a homomorphism $\mathbb{G}_{m,k}(R) \xrightarrow{\Phi_{n,R}} \mathbb{G}_{m,k}(R)$,
- from Proposition 1.14 that there is an isomorphism of groups $\mathrm{ev}_t : \mathbb{G}_{n,k}(R) \overset{\simeq}{\to} R^\times$,

Check, using the definitions of all the maps, that the corresponding homomorphism $R^\times \to R^\times$ is $x \mapsto x^n$.

Our next goal is to construct an analogue of the morphism Φ_n for any affine group scheme G.

End of Lecture 2

To be precise, we want to prove the following:

Theorem 2.15. *Let G be an affine group scheme over k. Then:*

(i) there exists a unique morphism $n = [n] : G \to G$ with the property that the induced homomorphism $n_R : G(R) \to G(R)$, for any k-algebra R, is multiplication by n;

(ii) there exists a unique sub affine group scheme $G[n] \subseteq G$ with the property that, for any k-algebra R, the inclusion $G[n](R) \subseteq G(R)$ identities $G[n](R)$ with the n-torsion $\{x \in G(R) : nx = 0\}$.

Note that we have already proved the theorem in the special case $G = \mathbb{G}_{m,k}$: the morphism n was constructed in the previous example, and the subgroup $\mathbb{G}_{m,k}[n]$ is exactly $\boldsymbol{\mu}_{m,k}$. To be precise, we have not proved uniqueness, but we do this in a moment for general G.)

Definition 2.16. (Pre-definition of p-divisible group) Let p be a prime number. A *p-divisible group*, or *Barsotti–Tate group*, over k is (roughly – we will be more precise later) will be defined to be a sequence of affine groups schemes $G_1, G_2, \dots$ over k such that $G_n = G_{n+1}[p^n]$ for all $i \geq 1$, together with extra conditions on the k-modules $\mathcal{O}(G_n)$.

Example 2.17. The main example is $\boldsymbol{\mu}_{p,k} \subset \boldsymbol{\mu}_{p^2,k} \subset \cdots$

We now mention explicitly the following "shadow of the Yoneda Lemma"; note that parts (i) and (ii) prove the uniqness assertion of the previous theorem:

Lemma 2.18. *(i) If $\Phi, \Psi : G \to F$ are homomorphisms of affine group schemes such that $\Phi_R = \Psi_R$ for all k-algebras R, then $\Phi = \Phi$.*

(ii) If $H, H' \subseteq G$ are sub affine group schemes such that $H(R) = H(R')$ (as subgroups of $G(R)$) for all k-algebras R, then $H = H'$.

(iii) Let $G = \operatorname{Spec} A$ and $F = \operatorname{Spec} B$ be affine group schemes over k, and $\Phi : G \to H$ a homomorphism of k-schemes (not assumed to be a morphism of group schemes!), with corresponding k-algebra homomorphism $\phi : B \to A$ (not assumed to be a homomorphism of Hopf algebras!). Then Φ is a morphism of affine group schemes (i.e., ϕ is a homomorphism of Hopf algebras) if and only if, for every k-algebra R, the induced map from Remark 2.10, i.e.,

$$\Phi_R : G(R) = \operatorname{Hom}_{k\text{-}alg}(A, R) \longrightarrow F(R) = \operatorname{Hom}_{k\text{-}alg}(B, R), \quad f \mapsto f \circ \phi$$

is a homomorphism of groups.

Proof. Let's start with (i), which is very easy. Taking $R = A := \mathcal{O}(G)$, the fact that $\Phi_A(\mathrm{id}_A) = \Psi_A(\mathrm{id}_A)$ in $F(A)$ is exactly the statement that $\Phi = \Psi$.

The proof of (ii) is similar. Let $I, I' \subseteq A = \mathcal{O}(G)$ be the Hopf ideals defining H and H'. Then $H(R) = \{f \in \operatorname{Hom}_{k\text{-}algs}(A, R); f(I) = 0\}$ and similarly for H'. So the assumption says that a k-algebra homomorphism $f : A \to R$ vanishes on I if and only if it vanishes on I'. By taking $R = A/I$ we deduce that $I' \subseteq I$; by taking $R = A/I'$ we deduce that $I \subseteq I'$. So $I = I'$, i.e., $H = H'$.

(iii) is a similar idea but slightly more tedious, since there are three identities to check:

- Take $R = A \otimes_k A$: and consider the two homomorphisms $j_1, j_2 : A \to A \otimes_k A$ given by $j_1(a) := a \otimes 1$ and $j_2(a) := 1 \otimes a$. Their sum, as elements of $G(A \otimes_k A)$, is μ_G. Moreover,

  $$\Phi_{A\otimes_k A}(j_1) = \phi \otimes 1, \qquad \Phi_{A\otimes_k A}(j_2) = 1 \otimes \phi, \qquad \Phi_{A\otimes_k A}(\mu_G) = \mu_G \circ \phi$$

  The sum, as element of $F(A \otimes_k A)$ of these first two elements is $(\phi \otimes \phi) \circ \mu_F$. Since we are assuming that $\Phi_{A\otimes_k A}$ is additive, it follows that $\mu_G \circ \phi = (\phi \otimes \phi) \circ \mu_F$.

- Take $R = k$: the fact that Φ_k sends the identity of $G(k)$ (i.e., ε_G) to the identity of $F(k)$ (i.e., ε_F) is exactly the statement $\phi \circ \varepsilon_F = \varepsilon_G$.

- Take $R = A$: applying the assumption that $\Phi_A : G(A) \to F(A)$ respects inversion shows that $\phi \iota_G = \iota_F \circ \phi$.

□

Now we must define the product of two group schemes and the sum of two morphisms:

Definition 2.19. The product of two affine group schemes $G = \operatorname{Spec} A$ and $G' = \operatorname{Spec} A'$ is by definition $G \times_k G = \operatorname{Spec} A \otimes_k A'$, where the comultiplication, counit, and antipode on $A \otimes_k A'$ are given respectively by

$$A \otimes_k A' \xrightarrow{\mu\otimes\mu'} (A \otimes_k A) \otimes_k (A' \otimes_k A') \quad \overset{\mathrm{id}_A \otimes \mathrm{swap} \otimes \mathrm{id}_{A'}}{\overset{\simeq}{\to}} \quad (A \otimes_k A') \otimes_k (A \otimes_k A')$$

$$A \otimes_k A' \xrightarrow{\varepsilon\otimes\varepsilon'} A \otimes_k A'$$

$$A \otimes_k A' \xrightarrow{\iota\otimes\iota'} A \otimes_k A'$$

By tensoring diagrams (1)–(4) from Section 1.2 for A with those for A', it is very easy to see (Check if in doubt) that this really makes $A \otimes_k A'$ into a Hopf algebra, and hence $G \times_k G$ is a well-defined affine group scheme.

Lemma 2.20. *Let $(A, \mu, \varepsilon, \iota)$ be a Hopf algebra over k. Then the homomorphisms of k-algebras*

$$\mu : A \to A \otimes_k A, \quad \varepsilon : A \to k, \quad \iota : A \to A$$
$$\mathrm{mult} : A \otimes_k A \to A, \quad k \to A, \quad \mathrm{swap} : A \otimes_k A \to A \otimes_k A$$

are actually homomorphisms of Hopf algebras, where $A \otimes_k A$ is equipped with the Hopf algebra structure of the previous definition.

Proof. For any k-algebra R, the six maps of the proposition induce on points the maps

$$\mathrm{mult} : G(R) \times G(R) \to G(R), \quad e : 0_k(R) = \{1\} \to G(R), \quad i = \mathrm{inv} : G(A) \to G(A)$$
$$\mathrm{diag} : G(R) \to G(R) \times G(R), \quad 0 : G(R) \to 0_k(R) = \{1\}, \quad \mathrm{swap} : G(R) \times G(R) \to G(R) \times G(R)$$

These maps are all group homomorphisms by elementary group theory, so the previous lemma implies that the original maps of k-algebras were actually maps of affine group schemes. □

The six morphisms of affine group schemes induced by the previous lemma are usually denoted by

$$m = \mathrm{mult} : G \times_k G \to G, \quad e : 0_k \to A, \quad i : G \to G$$
$$\Delta = \mathrm{diag}\, G \to G \times_k G, \quad 0 : G \to 0_k, \quad \mathrm{swap} : G \times_k G \to G \times_k G.$$

What this means is that (G, m, e, i) is not just a group object in the category Aff_k (by definition), but it is actually a group object in the category AC_k (i.e., diagrams (I)–(IV) from Section 1.1 are commutative diagrams in AC_k).

So, if H is another affine group scheme, then it again follows by functoriality that $\mathrm{Hom}(G, H)$ has the structure of an abelian group such that:

(i) The sum of $\Phi, \Psi : G \to H$ is the composition

$$\Phi + \Psi : G \xrightarrow{\mathrm{diag}} G \times_k G \xrightarrow{\Phi \times_k \Psi} H \times_k H \xrightarrow{m} H.$$

(Note that this is really a morphism of affine group schemes by what we just said.)

(ii) The zero element of $\mathrm{Hom}(G, H)$ is the zero morphism $G \to 0_k \to H$ from an earlier example.

(iii) The inverse of Φ is $\Phi \circ \iota_G$.

It also follows from functoriality that, if R is any k-algebra, then

$$\mathrm{Hom}(G, H) \to \mathrm{Hom}(G(R), H(R)), \quad \Phi \mapsto \Phi_R$$

is a homomorphism of groups. If you are uncertain about anything in the previous two paragraphs, you should try to either check the assertions directly in terms of the definitions of a various group structures, or read more about group objects in general categories to see that this is all functorial "nonsense".

In particular, if $G = H$ then $\mathrm{End}(G) := \mathrm{Hom}(G, G)$ is a commutative group containing id_G, and so for each $n \in \mathbb{Z}$ we define a morphism of affine groups schemes

$$[n] := n\, \mathrm{id}_G = \underbrace{\mathrm{id}_G + \cdots + \mathrm{id}_G}_{n \text{ times}} : G \to G.$$

If R is any k-algebra, then $n_R : G(R) \to G(R)$ is exactly multiplication by n. This proves Theorem 2.15(i).

To prove Theorem 2.15(ii), we want to define $G[n]$ to be the kernel of the morphism $n : G \to G$. But this requires us to define kernels, which is the next section.

2.3 Kernels and injections

Now we define the kernel of a morphism:

Lemma 2.21. *Let $\Phi : G = \operatorname{Spec} A \to F = \operatorname{Spec} B$ be a morphism of affine group schemes over k. Then the ideal $\phi(\operatorname{Ker} \varepsilon_F)A \subseteq A$ is a Hopf ideal of A.*

Proof. Clearly $\phi(\operatorname{Ker} \varepsilon_F)A$ is killed by ε. If $b \in \operatorname{Ker} \varepsilon_F$, then the final lemma from Lecture 1 implies that

$$\mu_G(\phi(b)) = \phi \otimes \phi(\mu_F(b)) \equiv \phi(b) \otimes 1 + 1 \otimes \phi(b) \equiv 0 \mod \phi(\operatorname{Ker} \varepsilon_F)A \otimes_k \phi(\operatorname{Ker} \varepsilon_F)A$$

and

$$\iota_G \phi(b) = \phi(\iota_F(b)) \equiv -\phi(b) \mod \phi(\operatorname{Ker} \varepsilon_F)^2 A$$

which suffices. □

Definition 2.22. Adopt the setting of the previous lemma. The sub affine group scheme of G defined by the Hopf ideal $\phi(\operatorname{Ker} \varepsilon')A$ is called the *kernel of* Φ and denoted by $\operatorname{Ker} \Phi$.

In particular, we the kernel of $n : G \to G$ is denoted by $G[n]$ and called the sub affine group scheme of *n-torsion points*.

Example 2.23. If k is a field of char 0, then we know that $\mathbb{G}_{a,k}$ is simple; so $\mathbb{G}_{a,k}[n] = 0$ for all $n \geq 1$.

Example 2.24. If $p = 0$ in k, then there is a morphism of affine group schemes $F : \mathbb{G}_{a,k} \to \mathbb{G}_{a,k}$ given by the homomorphism of k-algebras $k[t] \mapsto k[t]$, $f \mapsto f^{p^r}$. Since $\operatorname{Ker} \varepsilon = (t)$, we see that $\operatorname{Ker} F$ is the subgroup scheme associated to the Hopf ideal (t^{p^r}), i.e., $\operatorname{Ker} F = \boldsymbol{\alpha}_{p^r,k}$.

Example 2.25. Let's check that $\mathbb{G}_{m,k}[n] = \boldsymbol{\mu}_{n,k}$. Firstly, since we know that the morphism $\Phi_n : \mathbb{G}_{m,k} \to \mathbb{G}_{m,k}$ from Example 2.14 induces multiplication by n on R-valued points for any k-algebra R, the uniqueness part of Theorem 2.15 shows that $\Phi_n = n$. Since $\operatorname{Ker} \varepsilon = (t-1) \subseteq k[t, t^{-1}]$, we see that $\mathbb{G}_{m,k}[n] = \operatorname{Ker} \Phi_n$ is the subgroup associated to the Hopf ideal $(\phi_n(t-1)) = (t^n - 1)$. But we already know this this Hopf ideal defines $\boldsymbol{\mu}_{n,k}$.

It is now convenient to introduce some notation about injections:

Definition 2.26. Φ is said to be an *injection* if and only if it is a closed embedding of schemes, i.e., ϕ is surjective.

The *image* $\operatorname{Im} i$ of an injection $i : H \to G$ is the sub affine group scheme of G defined by the Hopf ideal $\operatorname{Ker}(\mathcal{O}(G) \twoheadrightarrow \mathcal{O}(H)$. Obviously $H \xrightarrow{\sim} \operatorname{Im} i$, we we are not really building anything new, but this is nonetheless a convenient definition.

A sequence of morphisms $0 \to H \xrightarrow{i} G \xrightarrow{\Phi} F$ is called *left exact* if and only if i is an injection with image equal to $\operatorname{Ker} \Phi$. Up to isomorphism, every left exact sequence of course looks like

$$0 \to \operatorname{Ker} \Phi \to G \xrightarrow{\Phi} F,$$

but it is still useful to introduce the notation more generally.

Collect together a large number of results on taking points; but this cannot be done until the abelian structure is in place.

Proposition 2.27. *Let $0 \to H \xrightarrow{i} G \xrightarrow{\Phi} F$ be an sequence of affine group schemes over k. If it is left exact, then the sequence of abelian groups*

$$0 \to H(R) \xrightarrow{i_R} G(R) \xrightarrow{\Phi_R} F(R)$$

is left exact for every k-algebra R. The converse is true if we assume that $\mathcal{O}(H)$ is finitely generated as a $\mathcal{O}(H)$-module.

Corollary 2.28. *Let $i : H \to G$ be a morphism of affine group schemes over k. If i is injective then* $\operatorname{Ker} i = 0_k$*. The converse is true if we assume that $\mathcal{O}(H)$ is finitely generated as a $\mathcal{O}(H)$-module.*

Proof of the Prop. and Corol. Let $A = \mathcal{O}(G)$.

$\Rightarrow$ of Prop: So we are assuming that H is the sub affine group scheme of G associated to $I = \phi(\operatorname{Ker} \varepsilon_F)A$. We have maps of Hopf algebras

$$\mathcal{O}(F) \xrightarrow{\phi} A \xrightarrow{\pi} A/I = \mathcal{O}(H),$$

for any k-algebra R, we must prove that the sequence of abelian groups is exact

$$0 \longrightarrow \operatorname{Hom}_{k\text{-alg}}(A/I, R) \xrightarrow{\circ\pi} \operatorname{Hom}_{k\text{-alg}}(A, R) \xrightarrow{\circ\phi} \operatorname{Hom}_{k\text{-alg}}(\mathcal{O}(F), R)$$

Certainly $\circ\pi$ is injective, so remains to check that if $f : A \to R$ is a k-algebra homomorphism, then f factors through A/I (i.e., $f(I) = 0$) if and only if $f \circ \phi$ equals the zero element of $F(R)$ (i.e., $f \circ \phi(\operatorname{Ker} \varepsilon_F) = 0$, since $\mathcal{O}(F) = k \oplus \operatorname{Ker} \varepsilon_F$). But I is the ideal of A generated by $\phi(\operatorname{Ker} \varepsilon_F)$, so this is clearly true.

$\Rightarrow$ of Corol: The sequence $0 \to \operatorname{Ker} i \to H \xrightarrow{i} G$ is left exact, so we have just proved that $0 \to \operatorname{Ker} i(R) \to H(R) \to G(R)$ is left exact for every k-algebra R. But we are assuming i is injective, so $A \to \mathcal{O}(H)$ is surjective and hence $H(R) \subseteq G(R)$; therefore $\operatorname{Ker} i(R) = 0$ for all R. Taking $R = \mathcal{O}(\operatorname{Ker} i)$ clearly shows that $\operatorname{Ker} i = 0_k$.

$\Leftarrow$ of Corol: We are assuming that $0 \to 0_k \to H \xrightarrow{i} G$ is left exact. Since $0_k(R) = 0$ for all R, the $\Rightarrow$ of Prop proves that $H(R) = \operatorname{Hom}(\mathcal{O}(H), R) \to G(R) = \operatorname{Hom}(A, R)$ is injective for any R. In particular, taking $R = \mathcal{O}(H) \otimes_A \mathcal{O}(H)$ and take $j_1, j_2 : \mathcal{O}(H) \to R$ to be the maps into the two coordinates; this coincide after pull-back to A, so the injectivity implies that they already coincide. This easily forces $\mathcal{O}(H) \otimes_A \mathcal{O}(H) = \mathcal{O}(H)$. If $\mathcal{O}(H)$ is finitely generated over A, then this forces $\mathcal{O}(H) = A$.

$\Leftarrow$ of Prop: By $\Leftarrow$ of Corol we deduce that i is injective, and by assumption we then see that $0 \to \operatorname{Im} H(R) \to G(R) \to F(R)$ is left exact for each R. But $0 \to \operatorname{Ker} \Phi \to G \to F$ is also left exact for each R, and so $\Rightarrow$ of Prop shows that also $0 \to \operatorname{Ker} \Phi(R) \to G(R) \to F(R)$ is also left exact for all R. Hence $\operatorname{Ker} \Phi$ and $\operatorname{Im} H$ have the same points for all R, which forces them to be equal by the first lemma today. □

So, in particular, if G is any affine group scheme, then $0 \to G[n] \to G \xrightarrow{n} G[n]$ is left exact by definition, and so, for any k-algebra R, the sequence of groups $0 \to G[n](R) \to G(R) \xrightarrow{n} G(R)$ is exact, i.e., $G[n](R) = \{x \in G(R) : nx = 0\}$. This proves Theorem 2.15(ii).

End of Lecture 3

3 p-DIVISIBLE GROUPS

In this section k is a Noetherian ring, and $p > 0$ is some fixed prime number.

Definition 3.1. Recall that a k-module M is said to be *finite flat* if and only if it satisfies the following equivalent conditions:

(i) M is finitely generated and flat;

(ii) M is finitely generated and projective;

(iii) M is isomorphic to a direct summand of k^n for some $n \geq 0$.

Letting $\mathfrak{m}$ be an arbitrary maximal ideal of k, the *rank* of M is then defined to be the dimension of $M/\mathfrak{m}M$ as a vector space over the field $k/\mathfrak{m}$. This rank is well-defined as long as $\operatorname{Spec} k$ is connected (i.e., k is not a product of two rings, or equivalently k contains no non-trivial idempotents; this is always true if k is local).

Definition 3.2. An affine group scheme $G = \operatorname{Spec} A$ over k is said to be *finite flat* if and only if A is finite flat as a k-module; the rank of A is called the *order* of G and denoted by a variety of notations: $\#G$, $|G|$, $o(G)$, $\operatorname{ord}(G)$.

If A is a finite étale k-algebra, then G is called finite étale (we may review étale algebras in more detail later; for now, we just need to know that if k is a field, then it means $A \cong \prod_i k_k$, for finitely many finite separable field extensions k_i/k).

Example 3.3. $\boldsymbol{\mu}_{n,k}$, $\boldsymbol{\alpha}_{p^r,k}$, and $G_{(a,b),k}$ are finite flat group schemes of orders n, p^r, and 2 respectively. $\boldsymbol{\mu}_{n,k}$ is finite étale if and only if n is invertible in k.

$\mathbb{G}_{m,k}$ and $\mathbb{G}_{a,k}$ are not finite flat, since the underlying algebras $k[t, t^{-1}]$ and $k[t]$ are not finitely generated as k-modules!

Example 3.4. We have not yet seen many examples of finite étale group schemes, but we will now construct them. Let Γ be a commutative group, usually written additively in this construction, and let k^Γ be the set of functions from Γ to k, under pointwise addition, scaler multiplication, and product:

$$(f+g)(\gamma) := f(\gamma) + g(\gamma), \quad (fg)(\gamma) := f(\gamma)g(\gamma) \quad \forall \gamma \in \Gamma.$$

There is an isomorphism of algebras

$$k^\Gamma \cong \prod_\Gamma k$$
$$f \mapsto (f(\gamma))_{\gamma \in \Gamma}$$

with inverse given by the delta functions δ_γ. Hence k^Γ is a finite étale k-algebra.

Define functions

$$\mu : k^\Gamma \to k^\Gamma \otimes_k k^\Gamma, \quad f \mapsto \sum_{\gamma \in \Gamma} \delta_\gamma \otimes f(\cdot + \gamma)$$
$$\varepsilon : k^\Gamma \to k, \quad f \mapsto f(1)$$
$$\iota : k^\Gamma \to k^\Gamma, \quad f \mapsto f(-\cdot)$$

It is left as an exercise to check that these make k^Γ into a Hopf algebra over k. The associated group scheme $\operatorname{Spec} k^\Gamma$ is called the *constant group scheme* associated to Γ and denoted by $\underline{\Gamma}_k$. In conclusion, $\underline{\Gamma}_k$ is a finite étale group scheme over k, of order $\#\Gamma$.

Thus we have defined a functor[7]

$$\text{finite abelian groups} \longrightarrow \text{finite étale group schemes}, \qquad \Gamma \mapsto \underline{\Gamma}_k$$

which preserves orders. It also preserves subgroups: check that if Γ' is a subgroup of Γ, then $\underline{\Gamma}'_k$ is a sub affine group scheme of $\underline{\Gamma}_k$.

In a moment we will prove the following facts in characteristic zero:

Proposition 3.5 (Cartier)**.** *Suppose k is a field of characteristic 0.*

(i) Every Hopf algebra over k is reduced ("Cartier's Theorem")

(ii) Every finite flat group scheme over k is finite étale.

(iii) If k is algebraically closed then taking k-points is an equivalence of categories

$$\textit{finite flat group schemes over } k \overset{\simeq}{\to} \textit{finite abelian groups}, \qquad G \mapsto G(k)$$

with inverse $\Gamma \mapsto \underline{\Gamma}_k$; orders on each side are the same.

Proof. (ii) Since k is a perfect field, a finite k-algebra is étale if and only if it is reduced. So this follows from (i). We will prove (i) later.

(iii) Now assume k is also algebraically closed, and let $G = \operatorname{Spec} A$ be a finite étale group scheme over k. Since A is finite étale over k, it is isomorphic to a product of a number of copies of k; these copies clearly correspond to the k-algebra homomorphisms $A \to k$. In other words, the homomorphism of k-algebras

$$A \longrightarrow k^{G(k)}, \quad a \mapsto \sum_{f \in G(k)} f(a)\delta_f$$

is an isomorphism. But by the very definition of the Hopf algebra structure on the right, it is also a map of Hopf algebras (Check!), and so $\underline{G(k)}_k \overset{\simeq}{\to} G$. □

Definition 3.6. A *p-divisible group* (or *Barsotti–Tate group*) *of height h* over a Noetherian ring k is a sequence of affine groups schemes $G_1, G_2, G_3, \dots$ over k, together with a morphism $i_n : G_n \to G_{n+1}$ for each $n \geq 1$, satisfying the following for each $n \geq 1$:

(i) G_n is finite flat of order p^{nh};

(ii) the morphism i_n is injective and has image $G_{n+1}[p^n]$.

In other words, up to identifying G_n with its image in G_{n+1}, a p-divisible group is a tower of affine group schemes

$$G_1 \subset G_2 \subset G_3 \subset G_4 \subset \cdots$$

such that $G_n = G_{n+1}[p^n]$ for all $n \geq 1$, together with the condition that G_n is finite flat of order p^{nh}.

Example 3.7. The tower $\boldsymbol{\mu}_{p,k} \subset \boldsymbol{\mu}_{p^2,k} \subset \boldsymbol{\mu}_{p^3,k} \subset \cdots$ is a p-divisible group of height 1.

[7] If k is an algebraically closed field of any characteristic then, as Thomas pointed out, this functor is an equivalence of categories by the proof of part (iii) of the next proposition.

Example 3.8. $\underline{(p^{-1}\mathbb{Z}/\mathbb{Z})^h}_k \subset \underline{(p^{-2}\mathbb{Z}/\mathbb{Z})^h}_k \subset \cdots$ is a p-divisible group of height h, denoted by $\underline{(\mathbb{Q}_p/\mathbb{Z}_p)^h}_k$.

Warning: Up to isomorphism, this p-divisible group can also be written as $\underline{(\mathbb{Z}/p\mathbb{Z})^h}_k \xrightarrow{p} \underline{(\mathbb{Z}/p^2\mathbb{Z})^h}_k \xrightarrow{p} \cdots$, where $i_n = p : \underline{(\mathbb{Z}/p^n\mathbb{Z})^h}_k \to \underline{(\mathbb{Z}/p^{n+1}\mathbb{Z})^h}_k$ is the injection induced by multiplication by $p : \mathbb{Z}/p^n \to \mathbb{Z}/p^{n+1}\mathbb{Z}$. It is easy to get muddled between these two notations.

Important: If k is an algebraically closed field of characteristic 0, then this is (up to isomorphism) the *only* p-divisible group of height h over k. (Proof: by the previous proposition, we must classify towers of honest abelian groups $G_1 \subset G_2 \subset \cdots$ such that $G_n = G_{n+1}[p^n]$ and $\#G_n = p^{nh}$; then elementary group theory shows $G_n \cong (\mathbb{Z}/p^n\mathbb{Z})^h \cong (p^{-n}\mathbb{Z}/\mathbb{Z})^h$ for all n)

Lemma 3.9. *Let $G_1 \subseteq G_2 \subseteq$ be a p-divisible group of height h over k.*

(i) $G_n = G_{n+r}[p^n]$ for any $r \geq 1$ (by a trivial induction on r).

(ii) the multiplication map $p : G_{n+1} \to G_{n+1}$ lands inside $G_{n+1}[p^n] = G_n$; i.e., there exists a map j_n

$$\begin{tikzcd} G_{n+1} \arrow[r, "j_n"] \arrow[rr, bend right, "p"'] & G_n = G_{n+1}[p^n] \subseteq & G_{n+1} \end{tikzcd}$$

Proof. By taking points in every k-algebra R, and using the results from last time that this is sufficient, we may assume that the G_n are honest groups satisfying $G_n = G_{n+1}[p^n]$. Then (i) is a trivial induction on r, and (ii) is obvious. □

Note from part (ii) that associated to G there is also an *inverse* system of finite flat group schemes

$$\cdots \xrightarrow{j_3} G_3 \xrightarrow{j_2} G_2 \xrightarrow{j_1} G_1$$

Definition 3.10. Let G be a p-divisible group over an integral domain $\mathcal{O}$ with field of fractions K having characteristic zero. Then the *Tate module* of G is

$$T_p(G) := \varprojlim_n G_n(K^{\mathrm{alg}})$$

where we take the limit over the j_n maps. The *Tate co-module* is $\Phi_p(G) = \varinjlim_n G_n(K^{\mathrm{alg}})$, where the limit is taken over the inclusions $G_1(K^{\mathrm{alg}}) \subset G_2(K^{\mathrm{alg}}) \subset \cdots$

Lemma 3.11. *The Tate module and co-module have the following properties:*

(i) $T_p(G)$ is a free $\mathbb{Z}_p$-module of rank h, such that $T_p(G)/p^n = G_n(K^{alg})$.

(ii) $\Phi_p(G) \cong T_p(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$, and $\Phi_p(G)[p^n] = G_n(K^{alg})$.

(iii) $T_p(G) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Phi_p(G))$

Proof. $G \otimes_k K$ is a p-divisible group over K of height h (see Remark 6.1 later for some comments on base changing p-divisible groups), hence $\cong \underline{(\mathbb{Q}_p/\mathbb{Z}_p)^h}_{K^{\mathrm{alg}}}$ by the previous example.

It follows that there are compatible isomorphisms $G_n(K^{\mathrm{alg}}) \cong (\mathbb{Z}/p^n\mathbb{Z})^h$; in this description $j_n : G_{n+1}(K^{\mathrm{alg}}) \to G_n(K^{\mathrm{alg}})$ is exactly the usual projection map, and i_n is multiplication by p. So $T_p(G) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^h = \mathbb{Z}_p^h$, and $T_p(G)/p^n = (\mathbb{Z}/p^n\mathbb{Z})^h$.

Similarly, $\Phi_p(G) = \varinjlim_n (\mathbb{Z}/p^n\mathbb{Z})^h = (\mathbb{Q}_p/\mathbb{Z}_p)^h$, and $\Phi_p(G) = (p^{-n}\mathbb{Z}/\mathbb{Z})^h \cong (\mathbb{Z}/p^n\mathbb{Z})^h = G_n(K^{\mathrm{alg}})$. □

Corollary 3.12. *$T_p(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is an h-dimensional p-adic Galois representation of K.*

Proof. More precisely: we mean that $T_p(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is an h-dimensional $\mathbb{Q}_p$-vector space, equipped with a continuous linear action of $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{alg}}/K)$. The first part of the previous lemma shows that it is an h-dimensional $\mathbb{Q}_p$-vector space.

Any K-algebra automorphism $\sigma : K^{\mathrm{alg}} \to K^{\mathrm{alg}}$ induces a group automorphism $\sigma_{K^{\mathrm{alg}}} : G_n(K^{\mathrm{alg}}) \to G_n(K^{\mathrm{alg}})$ for all $n \geq 1$. Taking the limit over n defines a $\mathbb{Z}_p$-linear automorphism $\sigma_{T_p(G)} : T_p(G) \to T_p(G)$. Tensoring by $\mathbb{Q}_p$ defines the action of Gal_K on $T_p(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. □

One of the main results to prove in the course is the following:

Theorem 3.13 (Hodge–Tate decomposition of a p-divisible group)**.** *Suppose that $\mathcal{O}$ is a complete discrete valuation ring of mixed characteristic, with perfect residue field; let K denote the fraction field. Then there is an isomorphism, as finite dimensional $\mathbb{Q}_p$-representations of* Gal_K*,*

$$T_p(G) \otimes_{\mathbb{Z}_p} \widehat{\mathbb{Q}_p^{alg}} \cong \textit{tangent} \oplus \textit{cotangent space of } G,$$

where $\widehat{\mathbb{Q}_p^{alg}}$ denotes the p-adic completion of the algebraically closure of $\mathbb{Q}_p$, and the right side still needs to be defined.

End of Lecture 4

4 The formal group and tangent space of a p-divisible group

Idea: Let G be a p-divisible group over a ring $\mathcal{O}$, and write $G_n = \operatorname{Spec} A_n$ for each $n \geq 1$. Then

$$\cdots \twoheadrightarrow A_2 \twoheadrightarrow A_1$$

is an inverse system, with surjective transition maps, of Hopf algebras over $\mathcal{O}$. The *formal group* associated to G is

$$\mathcal{A} := \varprojlim_n A_n$$

This is a $\mathcal{O}$-algebra equipped operators

$$\mu := \varprojlim \mu_n : \mathcal{A} \to \mathcal{A} \widehat{\otimes}_{\mathcal{O}} \mathcal{A} := \varprojlim_n A_n \otimes_{\mathcal{O}} A_n, \qquad \varepsilon := \varprojlim_n \varepsilon_n : \mathcal{A} \to \mathcal{O}, \qquad \iota := \varprojlim_n \iota_n : \mathcal{A} \to \mathcal{A}$$

which satisfy the axioms for a Hopf-algebra, i.e., it is a type of "continuous Hopf algebra"

To make this part of a satisfactory theory, it is best to assume that all rings occurring are complete, Noetherian, and local.

Remark 4.1 (Reminders on complete local rings)**.** We recall some results about complete, Noetherian, local rings.

Let $\mathcal{O}$ be a Noetherian local ring; recall that $\mathcal{O}$ is said to be *complete* if and only if the canonical map $\mathcal{O} \to \varprojlim_r \mathcal{O}/\mathfrak{m}^r$ is an isomorphism, where $\mathfrak{m} \subseteq \mathcal{O}$ denotes the maximal ideal. If this is true then many other objects associated to $\mathcal{O}$ are also complete:

(i) any finitely generated $\mathcal{O}$-module M is also complete, in the sense that $M \overset{\cong}{\to} \varprojlim_r M/\mathfrak{m}^r M$ (the key to proving this is the Artin–Rees Lemma);

(ii) in particular, if $I \subseteq \mathcal{O}$ is an ideal then $\mathcal{O}/I$ is also a complete Noetherian local ring;

(iii) and the power series ring $\mathcal{O}[[X_1, \ldots, X_d]]$ is also a complete Noetherian local ring, with maximal ideal $\mathfrak{m} + \langle X_1, \ldots, X_d \rangle$.

For simplicity, we will use in this section the non-standard notation $\mathcal{O}$-c. alg to mean the category of complete Noetherian local $\mathcal{O}$-algebras with the same residue field as $\mathcal{O}$ (i.e., the canonical map $\mathcal{O}/\mathfrak{m} \to A/\mathfrak{m}_A$ is an isomorphism; also note that "a local $\mathcal{O}$-algebra C" is not just a $\mathcal{O}$-algebra which is a local ring; the additional property that $\mathfrak{m}C \subseteq \mathfrak{m}_C$ must be satisfied; for example, $\mathbb{Q}_p[[T]]$ is not a local $\mathbb{Z}_p$-algebra!). The main example is $\mathcal{O}[[X_1, \ldots, X_d]]$, or a quotient of this $\mathcal{O}$-algebra.

Now let $\mathcal{O}$ be a complete Noetherian local ring, and let $A, B \in \mathcal{O}$-c. alg. Then we define their *completed tensor product*

$$A \widehat{\otimes}_{\mathcal{O}} B := \varprojlim_r A/\mathfrak{m}_A^r \otimes_{\mathcal{O}} B/\mathfrak{m}_B^r$$

Example 4.2. $\mathcal{O}[[X_1, \ldots, X_c]] \widehat{\otimes}_{\mathcal{O}} \mathcal{O}[[Y_1, \ldots, Y_d]] \cong \mathcal{O}[[X_1, \ldots, X_c, Y_1, \ldots, Y_d]]$.

Lemma 4.3. *$\mathcal{O}$-c. alg is closed under $\widehat{\otimes}_{\mathcal{O}}$.*

Proof. Let A, B be two such $\mathcal{O}$-algebras. Pick generators $x_1, \ldots, x_c$ for the maximal ideal of A, and generators $y_1, \ldots, y_d$ for the maximal ideal of B. Then the $\mathcal{O}$-algebra homomorphisms

$$\mathcal{O}[[X_1, \ldots, X_c]] \to A, \quad X_i \mapsto x_i \qquad \qquad \mathcal{O}[[X_1, \ldots, X_d]] \to A, \quad Y_i \mapsto y_i$$

are surjective since A and B have the same residue field as $\mathcal{O}$. So we obtain surjections

$$\mathcal{O}[[X_1, \ldots, X_c]]/(\mathfrak{m}, X_1, \ldots, X_c)^r \otimes_{\mathcal{O}} \mathcal{O}[[Y_1, \ldots, Y_d]]/(\mathfrak{m}, Y_1, \ldots, Y_d)^r \longrightarrow A/\mathfrak{m}_A^r \otimes_k B/\mathfrak{m}_B^r$$

for each r, and in letting $r \to \infty$ these give a surjection

$$\mathcal{O}[[X_1, \ldots, X_c, Y_1, \ldots, Y_d]] \longrightarrow A \widehat{\otimes}_k B$$

Since the left is a complete Noetherian local $\mathcal{O}$-algebra with the same residue field as A, the same is true of the right side. □

Definition 4.4. A *connected (= local) formal group over $\mathcal{O}$* is a "Hopf algebra in the category $\mathcal{O}$-c. alg". In other words, it is data $(A, \mu, \varepsilon, \iota)$ where A is a complete Noetherian local $\mathcal{O}$-algebra with the same residue field as $\mathcal{O}$, and homomorphisms of $\mathcal{O}$-algebras $\mu : A \to A \widehat{\otimes}_{\mathcal{O}} A$, $\varepsilon : A \to \mathcal{O}$, and $\iota : A \to A$ which satisfy the usual rules for a Hopf algebra after replacing $\otimes_k$ by $\widehat{\otimes}_{\mathcal{O}}$ everywhere.

Example 4.5. The *additive formal group* $\widehat{\mathbb{G}}_{a,\mathcal{O}}$ over $\mathcal{O}$ is $\mathcal{O}[[X]]$, with operators

$$\begin{aligned}
&\mu : \mathcal{O}[[X]] \to \mathcal{O}[[X,Y]] = \mathcal{O}[[X]]\widehat{\otimes}_{\mathcal{O}}\mathcal{O}[[Y]], \qquad X \mapsto X+Y \\
&\varepsilon : \mathcal{O}[[X]] \to \mathcal{O}, \qquad \sum_{i\geq 0} a_n X^n \mapsto a_0 \\
&\iota : \mathcal{O}[[X]] \to \mathcal{O}[[X]], \qquad X \mapsto -X
\end{aligned}$$

Check that the axioms are satisfied! It is exactly the same as for the additive group scheme $\mathbb{G}_a$. Indeed, it is its X-adic completion.

Example 4.6. The *multiplicative formal group* $\widehat{\mathbb{G}}_{m,\mathcal{O}}$ over $\mathcal{O}$ is $\mathcal{O}[[X]]$, with operators

$$\begin{aligned}
&\mu : \mathcal{O}[[X]] \to \mathcal{O}[[X,Y]] = \mathcal{O}[[X]]\widehat{\otimes}_{\mathcal{O}}\mathcal{O}[[Y]], \qquad X \mapsto X+Y-XY \\
&\varepsilon : \mathcal{O}[[X]] \to \mathcal{O}, \qquad \sum_{i\geq 0} a_n X^n \mapsto a_0 \\
&\iota : \mathcal{O}[[X]] \to \mathcal{O}[[X]], \qquad X \mapsto \text{uniquely determined power series } \iota(X) \text{ s.t. } \mu(X,\iota(X)) = X
\end{aligned}$$

i.e., $\iota(X) = 1-(1-X)^{-1}$. Again, check that the axioms are satisfied. After applying the change of variable $X \leftrightarrow t-1$ it is the completion of the multiplicative group scheme.

Example 4.7. If A is a usual Hopf algebra over $\mathcal{O}$ which is local and finitely generated as an $\mathcal{O}$-module, then A is a connected formal group. Indeed, the finite generation hypothesis implies that $A\widehat{\otimes}_{\mathcal{O}}A = A \otimes_{\mathcal{O}} A$.

Almost all the theory we developed for Hopf algebras/affine group schemes works verbatim for connected formal groups over $\mathcal{O}$; in particular:

(i) if $\psi : A \to B$ is a morphism of connected formal groups (i.e., map of $\mathcal{O}$-algebras compatible with μ, ε, ι in the obvious way), then the associated *kernel* is the connected formal Hopf algebra $B/\psi(\operatorname{Ker}\varepsilon_A)B$.

(ii) The set of morphisms $\operatorname{Hom}(A,B)$ is an abelian group, and so there is a multiplication morphism of connected formal groups

$$[n] = n_A := \mathrm{id}_A + \cdots + \mathrm{id}_A : A \to A$$

for each $n \geq 0$, whose associated kernel is $A[n] := A/[n](\operatorname{Ker}\varepsilon_A)A$ is the *n-torsion.*

Definition 4.8. A morphism $\psi : A \to B$ of connected formal groups is called an *isogeny* if and only if it is injective and makes B into a finite free A-module.

A connected formal group A is called *p-divisible* if and only if the multiplication map $[p] : A \to A$ is an isogeny.

Lemma 4.9. *Let $\psi : A \to B$ be an isogeny.*

(i) Then the associated kernel $B/\psi(\operatorname{Ker}\varepsilon_A)B$ is a finite free local Hopf algebra over $\mathcal{O}$, whose $\mathcal{O}$-rank is $\operatorname{rk}_A B$.

(ii) If $\psi' : B \to C$ is another isogeny, then $\psi' \circ \psi : A \to B$ is also an isogeny, and $\operatorname{rk}_A C = \operatorname{rk}_A B \cdot \operatorname{rk}_C B$.

Proof. (i): According to the previous example and comments, $B/\psi(\operatorname{Ker}\varepsilon_A)B$ inherits the structure of a connected formal Hopf algebra, so we only need to show that it is a finite free $\mathcal{O}$-module.

Let $b_1, \dots, b_m$ be a basis for B as a free A-module; we will show that their images $\overline{b}_1, \dots, \overline{b}_m$ in $B/\psi(\operatorname{Ker}\varepsilon)B$ form a basis for $B/\psi(\operatorname{Ker}\varepsilon)B$ as an $\mathcal{O}$-module. This will complete the proof.

Generation: If $b \in B$ then we may write $b = \sum_i \psi(a_i)b_i \equiv \sum_i \psi(\varepsilon(a_i))b_i = \sum_i \varepsilon(a_i)b_i$ for some $a_i \in A$, whence the generation is clear.

Linear independence: If $\sum_i \lambda_i \overline{b}_i = 0$, where $\lambda_i \in \mathcal{O}$, then $\sum_i \lambda_i b_i \in \psi(\operatorname{Ker}\varepsilon)B$, so it easily follows that there exist $a_1, \dots, a_m \in \operatorname{Ker}\varepsilon_A$ such that $\sum_i \lambda_i b_i = \sum_i \psi(a_i)b_i$. Then $\sum_i \psi(\lambda_i - a_i)b_i = 0$, and so from the assumption that b_i is a basis we deduce that $\lambda_i - a_i = 0$ for all i; but $A = \mathcal{O} \oplus \operatorname{Ker}\varepsilon_A$, so $\lambda_i = 0 = a_i$ for all i.

(ii): This is easy algebra: B is a free A-module and C is a free B-module, so C is a free A-module, and taking ranks is multiplicative. □

Instead of starting – but not finishing – the proof of the upcoming proposition as we did in lecture 5, we now jump to the beginning of lecture 6.

Recall the situation from last time: $\mathcal{O}$ is a complete Noetherian local ring, $p > 0$ is a prime number, and we studied *connected formal groups* $(A, \mu, \varepsilon, \iota)$, means that A is a complete Noetherian local $\mathcal{O}$-algebra, and $\mu : A \to A \widehat{\otimes}_{\mathcal{O}} A$, etc., satisfying the usual Hopf algebra rules, always replacing tensor products by completed tensor products. This was called *p-divisible* if and only if the morphism $[p] : A \to A$ is an isogeny (i.e., injective and A is a free module over its image).

We should also introduce the following standard terminology: A finite flat group scheme $H = \operatorname{Spec} B$ over $\mathcal{O}$ is called *connected* if and only if B is a local ring; a p-divisible group $G = (G_1 \subset G_2 \subset \cdots)$ over $\mathcal{O}$ is called *connected* if and only if each G_n is connected.

Given a connected, p-divisible group $G = (G_1 \subset G_2 \subset \cdots)$, we associate to it the connected formal group is $A := \varprojlim_n A_n$, where we have written $G = \operatorname{Spec} A_n$, with A_n being finite flat, local, Hopf algebras over $\mathcal{O}$. (Commutative algebra implies that that A really is a complete Noetherian local $\mathcal{O}$-algebra, while the structure maps $\mu := \varprojlim_n \mu_n$, $\varepsilon := \varprojlim_n \varepsilon_n$, and $\iota := \varprojlim_n \iota_n$ satisfy the Hopf algebra rules since the same is true for each n.)

Definition 4.10. With G a connected, p-divisible group over $\mathcal{O}$, and A as above:

(i) the *dimension* of G is defined to be $\dim A - \dim \mathcal{O}$ (these dims denote Krull dimension).

(ii) For any (probably only finitely generated) $\mathcal{O}$-module M, the *cotangent* and *tangent* spaces of G with values in M are defined to be

$$\mathfrak{t}^*_G(M) := \operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2 \otimes_{\mathcal{O}} M, \qquad \mathfrak{t}_G(M) := \operatorname{Hom}_{\mathcal{O}}(\operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2, M).$$

Note: more explicitly, $\operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2$ is just $\varprojlim_n \operatorname{Ker}\varepsilon_n / \operatorname{Ker}\varepsilon_n^2$.

Example 4.11. Let $\mathcal{O}$ have residue characteristic p, and let $G := \boldsymbol{\mu}_{p^\infty} := (\boldsymbol{\mu}_p \subset \boldsymbol{\mu}_{p^2} \subset \cdots)$, which is a connected p-divisible group of height 1. Then the associated connected formal group is

$$A = \varprojlim_n \mathcal{O}[t]/(t^{p^r} - 1) \cong \varprojlim_n \mathcal{O}[X]/((X+1)^{p^r} - 1) \cong \mathcal{O}[[X]] = \widehat{\mathbb{G}}_{m,\mathcal{O}},$$

where the first isomorphism is the change of variable $t \leftrightarrow X+1$ and the second isomorphism is a well-known isomorphism from commutative algebra (which uses $\mathcal{O}$ having residue characteristic p).

Since $\varepsilon : \mathcal{O}[[X]] \to \mathcal{O}$ is the usual projection, we see that

$$\operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2 = X\mathcal{O}[[X]]/X^2\mathcal{O}[[X]] \cong \mathcal{O};$$

hence, for any $\mathcal{O}$-module M, we have

$$\mathrm{t}^*_G(M) = X\mathcal{O}[[X]]/X^2\mathcal{O}[[X]] \otimes_{\mathcal{O}} M \cong M$$

$$\mathrm{t}_G(M) := \operatorname{Hom}_{\mathcal{O}}(X\mathcal{O}[[X]]/X^2\mathcal{O}[[X]], M) \cong \operatorname{Hom}_{\mathcal{O}}(\mathcal{O}, M) = M$$

The following is the main result of the section, setting up a correspondence between connected p-divisible groups and p-divisible connected formal groups:

Proposition 4.12. *Let $\mathcal{O}$ be a complete Noetherian local ring whose residue field has characteristic p. Then there is a one-to-one correspondence (even an equivalence of categories) between*

connected p-divisible groups $G = (G_1 \subset G_2 \subseteq \cdots)$

and

p-divisible connected formal groups $(A, \mu, \varepsilon, \iota)$

This is given by

$$G \mapsto A := \varprojlim_n A_n$$

and

$$A \mapsto (G_1 \subset G_2 \subset \cdots) \text{ where } G_n := \operatorname{Spec} A/\psi^n(\operatorname{Ker}\varepsilon)A.$$

Proof. $\uparrow$: Let A be a p-divisible connected formal group over $\mathcal{O}$. By inductively applying the previous lemma to $A \xrightarrow{[p]} A \xrightarrow{[p]} \cdots$, we deduce that $A_n := A/[p^n](\operatorname{Ker}\varepsilon_A)A$ is a finite free local $\mathcal{O}$-algebra of rank d^n, where $d := \operatorname{rk}_{\mathcal{O}} A/[p](\operatorname{Ker}\varepsilon_A)A$; since A_1 is a finite flat local Hopf algebra over $\mathcal{O}$, the "Corollary" to Cartier's Theorem (which we prove next time) shows that d is a power of p. Also, the $A_1, A_2, \ldots$ are successive Hopf algebra quotients of A which satisfy, by construction,

$$A_n = A_{n+1}/[p^n](\operatorname{Ker}\varepsilon_{A_{n+1}})A_{n+1}$$

i.e., setting $G_n := \operatorname{Spec} A_n$, we see that $G_1 \subseteq G_2 \subseteq \cdots$ is a tower of finite flat group schemes over $\mathcal{O}$ of ranks d^n satisfying $G_n = G_{n+1}[p^n]$ for all $n \geq 1$, i.e., a p-divisible group!

(Side remark since it is being used repeatedly, in case it wasn't clear: If $H = \operatorname{Spec} B$ is an affine group scheme over some ring, then we defined $H[m] := \operatorname{Ker}[m]$ to be the kernel of the morphism $[m]$; according to the definition of kernels, this means that $H[n] = \operatorname{Spec} B/[n](\operatorname{Ker}\varepsilon_B)B$.)

$\downarrow$: Now we must go in the other direction. Fix a connected p-divisible group G of height h, and write $G_n = \operatorname{Spec} A_n$ (so each A_n is a local, finite flat Hopf algebra over $\mathcal{O}$ of rank p^{nh}). Then $A := \varprojlim_n A_n$ is local, Noetherian, and complete (by standard commutative algebra), and the Hopf algebra structures on each A_n clearly give A the structure of a connected formal group over $\mathcal{O}$, e.g.,

$$\mu = \varprojlim_n \mu_n : A \to \varprojlim_n A_n \otimes_{\mathcal{O}} A_n = \varprojlim_n \varprojlim_r A_n/\mathfrak{m}^r A_n \otimes A_n \mathfrak{m}^r A_n = A \widehat{\otimes}_{\mathcal{O}} A.$$

Now we use that $G_n = G_{n+r}[p^n]$ for all $n, r \geq 1$; in terms of Hopf algebras this means that $A_n = A_{n+r}/[p^n](\operatorname{Ker} \varepsilon_{A_{n+r}})A_{n+r}$, and so by taking the limit over r we deduce

$$A/[p]^n(\operatorname{Ker} \varepsilon)A = A_n$$

i.e., this is inverting the previous construction $A \mapsto G$. However, it remains to check that the connected formal group $A = \varprojlim_n A_n$ is p-divisible; this is perhaps the trickiest part of the proof, but also not so important for us.

We must first show that $[p] : A \to A$ is injective. Recall from the last section the commutative diagram

$$\begin{tikzcd} G_{n+1} \arrow[r, "j_n"] \arrow[rr, bend right, "p"'] & G_n = G_{n+1}[p^n] \subseteq & G_{n+1} \end{tikzcd}$$

This corresponds to a diagram of Hopf algebras:

$$\begin{tikzcd} A_{n+1} & A_n = A_{n+1}/[p^n](\operatorname{Ker} \varepsilon_{n+1})A_{n+1} \arrow[l, "j_n"'] & A_{n+1} \arrow[l, two heads] \arrow[ll, bend left, "{[p]}"] \end{tikzcd}$$

By counting ranks, one can check that $j_n : A_n \to A_{n+1}$ is injective as a map of algebras (this is a little tricky and we are skipping over the details). So $\varprojlim_n j_n : A \to A$ is injective; but the diagram shows that $\varprojlim_n j_n = [p] : A \to A$.

Next we must show that A is a free module over its subring $[p](A)$: the rank will be p^h, where h is the height of G. Let $b_1, \ldots, b_{p^h} \in A$ be elements whose images in $A_1 = A/[p](\operatorname{Ker} \varepsilon)A$ form an $\mathcal{O}$-basis for A_1 (recall this is free of height p^h). We will show that these elements give a basis.

Generation: Given $a \in A$, we may write $a \equiv \sum_i a_i^{(0)} b_i + z$ for some $a_i^{(0)} \in \mathcal{O}$ and $z \in [p](\operatorname{Ker} \varepsilon)A$. Then write $z = \sum_i [p](a_i^{(1)})b_i + z^{(1)}$ for some $a_i^{(1)} \in \operatorname{Ker} \varepsilon$ and $z^1 \in [p](\operatorname{Ker} \varepsilon^2)A$. Repeating the argument, we get $a = \sum_i [p](a_i^{(0)} + a_i^{(1)} + \cdots)b_i$, where the infinite sums converge through completeness.

Linear independence: By taking $\varprojlim_n$, it is enough to show that the images $\overline{b}_1, \ldots, \overline{b}_{p^h}$ in of $b_1, \ldots, b_{p^h}$ in $A_n = A/[p^n](\operatorname{Ker} \varepsilon)A$ are linearly independent over $[p](A_n)$. Note that these elements are generators by the previous paragraph. But $[p](A_n) = j_{n-1}(A_{n-1})$ has rank $p^{h(n-1)}$ since j_{n-1} is injective. Thus any relation among $\overline{b}_1, \ldots, \overline{b}_{p^h}$ would cause the $\mathcal{O}$-rank of A_n to be $< p^n p^{h(n-1)} = p^h n$, which is a contradiction. □

Remark 4.13. (which we may prove at the end of the course): Suppose that A is a connected formal group over $\mathcal{O}$. If $\mathcal{O}$ has residue characteristic p and A is p-divisible, then it can be shown that A is automatically "formally smooth" as a $\mathcal{O}$-algebra, which means concretely that there exists an $\mathcal{O}$-algebra isomorphism $A \cong \mathcal{O}[[X_1, \ldots, X_d]]$.

In particular, if G is a connected p-divisible group over $\mathcal{O}$ and $A := \varprojlim_n A_n$ is its associated connected formal group, then we showed in the previous proposition that A is p-divisible and so we deduce:

(i) $A \cong \mathcal{O}[[X_1, \dots, X_d]]$ where d is the dimension of G;

(ii) $\operatorname{Ker}\varepsilon \cong (X_1, \dots, X_d)$ and so $\operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2$ is a free $\mathcal{O}$-module of rank d, with basis given by the classes of $X_1, \dots, X_d$;

(iii) if M is an $\mathcal{O}$-module, there are therefore non-canonical isomorphisms of $\mathcal{O}$-modules $\mathfrak{t}_G(M) \cong \mathfrak{t}^*_G(M) \cong M^d$.

5 The structure of finite flat group schemes over complete local rings

Over a complete Noetherian local ring, we have now have two important classes of finite-flat group schemes and p-divisible groups:

(i) connected – these can be studied using the previous proposition.

(ii) étale – these are typically easy and explicit, reducing to Galois theory.

The goal of this section is to analyse further these two classes, and show that any finite flat group scheme/p-divisible group can be built out of them.

We start by proving the Cartier isomorphism, which we skipped before:

Proposition 5.1 ("Cartier's Theorem")**.** *Suppose k is a field of characteristic 0. Then every Hopf algebra over k is reduced.*

Proof. We will only prove the result in the case that the Hopf algebra is finite dimensional over k, but it is not too hard to modify the proof to prove the full result. We will actually start by proving some more general statements:

For any Hopf algebra $(A, \mu, \varepsilon, \iota)$ over any ring k, we may define a k-linear map $\rho : A \to \operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2$ by $\rho(a) := a - \varepsilon a \bmod \operatorname{Ker}\varepsilon^2$, and then consider the k-linear map

$$\delta : A \xrightarrow{\mu} A \otimes_k A \xrightarrow{\rho} A \otimes_k \operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2$$

Directly from the axioms of a Hopf algebra, one can check that ∂ is a derivation on the k-algebra A (i.e., it is k-linear and satisfies $\partial(ab) = a\partial(b) + b\partial(a)$ for all $a, b \in A$).

Now suppose that k is a field and that A is Noetherian. Then $\operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2$ is a finite dimension k-vector space, and we pick a basis $\overline{t}_1, \dots, \overline{t}_d$ of it; here $t_1, \dots, t_d \in \operatorname{Ker}\varepsilon$ and the overline denotes mod $\operatorname{Ker}\varepsilon^2$. Let $e_i : \operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2 \to k$ be the k-linear maps which form the dual basis, i.e., $e_i(\overline{t}_j) = \delta_{i,j}$.

Since ∂ is a derivation, so is

$$\partial_i : A \xrightarrow{\partial} A \otimes_k \operatorname{Ker}\varepsilon / \operatorname{Ker}\varepsilon^2 \xrightarrow{\mathrm{id}_A \otimes e_i} A \otimes_k k = A,$$

and one checks directly that $\partial_i(t_j) \equiv \delta_{i,j} \bmod \operatorname{Ker}\varepsilon$. By now repeatedly applying the Leibnitz rule, one checks the following: if $\alpha_1, \dots, \alpha_d$ and $\beta_1, \dots, \beta_d$ are non-negative integers satisfying $\sum_i \alpha_i = \sum_i \beta_i$, then

$$\partial^{\alpha_1} \cdots \partial_d^{\alpha_d}(t_1^{\beta_1} \cdots t_d^{\beta_d}) \equiv \begin{cases} \alpha_1! \cdots \alpha_d! \mod \operatorname{Ker}\varepsilon & \alpha_i = \beta_i \text{ for all } i = 1, \dots, n, \\ 0 \mod \operatorname{Ker}\varepsilon & \text{else} \end{cases}$$

Now we specialise to the case at hand: we will prove that if k is a field of characteristic zero and A is a finite dimensional Hopf algebra over k, then A is reduced (the result holds without assuming that A is finite dimensional, but the proof is a little trickier and we do not need it). After replacing k by k^{alg} and A by $A \otimes_k k^{\mathrm{alg}}$ we may assume k is algebraically closed.

It easily follows from the existence of all these functionals on A that the surjection

$$k[X_1, \ldots, X_d]/(X_1, \ldots, X_d)^n \to A/\operatorname{Ker} \varepsilon^n, \quad X_i \mapsto t_i$$

cannot have any kernel (the coefficients in the relation would be detected by suitable functionals), and so it is an isomorphism for all $n \geq 1$. But since A is finite dimensional over k, then there is no way that the dimension of $A/\ker^n$ can be d^n for all $n \geq 0$, unless it was the case that $d = 0$, i.e., we have concluded that $\operatorname{Ker} \varepsilon = \operatorname{Ker} \varepsilon^2$.

Now we want to use this to show that $\mathfrak{m} = \mathfrak{m}^2$ for every maximal ideal $\mathfrak{m}$ of A. Let $\pi : A \to A/\mathfrak{m} = k$ be the projection, which we can think of as a point $\pi \in G(k)$. Then there is a homomorphism of k-algebras

$$\tau : A \xrightarrow{\mu} A \otimes_k A \xrightarrow{\mathrm{id}_A \otimes \pi} A \otimes_k A/\mathfrak{m} = A,$$

and the induced map $\tau_R : G(R) \to G(R)$ is translation by π for any k-algebra R. Since this is a bijection for any R, it is easy to check that τ is an automorphism of A and that $\tau(\operatorname{Ker} \varepsilon) = \mathfrak{m}$ (since $\operatorname{Ker} \varepsilon$ corresponds to $0 \in G(k)$ and $\mathfrak{m}$ corresponds to $\pi \in G(k)$). Since we have already shown $\operatorname{Ker} \varepsilon = \operatorname{Ker} \varepsilon^2$, we see that also $\mathfrak{m} = \mathfrak{m}^2$.

Many different argument now show that A is reduced. For example, since A is a finite dimensional algebra over k, it is isomorphic to $\prod_i A_i$ for finitely many finite-dimensional local k-algebras A_i. From what we have shown about maximal ideals, it follows that $\mathfrak{m}_i = \mathfrak{m}_i^2$, where $\mathfrak{m}_i$ is the maximal ideal of A_i. By Nakayama therefore $\mathfrak{m}_i = 0$, whence A_i is a field. So A is a product of fields, hence reduced. □

End of lecture 6.

Corollary 5.2. *Let $\mathcal{O}$ be a complete Noetherian local ring and $G = \operatorname{Spec} A$ a connected, finite flat group scheme over $\mathcal{O}$. Then*

(i) If $\mathcal{O}$ has residue characteristic zero then G is trivial, i.e., $= 0_{\mathcal{O}}$.

(ii) If $\mathcal{O}$ has residue characteristic $p > 0$ then the order of G is a power of p.

Proof. Let $k = \mathcal{O}/\mathfrak{m}$, so that $A/\mathfrak{m}A$ is a finite flat Hopf algebra over the field k.

If $\operatorname{char} k = 0$ then we have already seen in an earlier lecture that Cartier's result forces $A/\mathfrak{m}A$ to be étale over k, hence to be a finite product of separable extensions of k. But $A/\mathfrak{m}A$ is local and $k \to A/\mathfrak{m}A$ has a section, so the only option is $A/\mathfrak{m}A = k$. Commutative algebra (e.g., Nakayama's lemma) then implies that $A = \mathcal{O}$.

Next suppose that k has characteristic p. After replacing A by $A/\mathfrak{m}A$ (whose k-rank is the same as the $\mathcal{O}$-rank of A), we may as well suppose that $\mathcal{O} = k$ is a field. Let $\phi : A \to A$ $a \mapsto a^p$ be the absolute Frobenius. It is easy to check that $\phi^n(\operatorname{Ker} \varepsilon)A$ is a Hopf ideal of A, and it has to vanish for $n \gg 0$ since $\operatorname{Ker} \varepsilon$ is nilpotent (since A is a local, finite dimensional algebra). By a non-trivial induction on n (e.g., using existence of quotient group schemes, though a direct argument is also possible), we will restrict ourselves to the case that $\phi^n(\operatorname{Ker} \varepsilon) = 0$. This means that we have a surjection

$$k[X_1, \ldots, X_d]/(X_1^p, \ldots, X_d^p) \longrightarrow A, \quad X_i \mapsto t_i,$$

and the proof will be complete if we show it is an isomorphism. But this easily follows from the existence of the derivations constructed in the previous proof (which required no assumptions on k). □

The next goal is to show that any finite flat group scheme over $\mathcal{O}$ decomposes into an étale piece and a connected piece; to make the notion of "decomposes" precise, we need the following definition:

Definition 5.3. The following definitions really belong to the earlier sections on the general theory of affine group schemes, but we didn't need them until now:

A morphism $G = \operatorname{Spec} A \to F = \operatorname{Spec} B$ of affine group schemes (over any ring) is said to be *surjective* if and only if the corresponding map of rings $B \to A$ is faithfully flat (recall that this means that (1) $A \to B$ is flat and (2) $\mathfrak{p}B \neq B$ for every prime ideal $\mathfrak{p} \subseteq A$, i.e., $G \to F$ is surjective as a map of sets of prime ideals; in particular, a map of local rings is faithfully flat if and only if it is flat.)

A sequence

$$0 \to H \to G \to F \to 0$$

is then said to be *exact* if and only if the sequence $0 \to H \to G \to F$ is left exact (recall we defined this to mean that $H \to G$ is injective and has image $\operatorname{Ker}(G \to F)$) and in addition $G \to F$ is surjective.

The following trick, by counting ranks, is useful: If H, G, F are all finite flat, and $0 \to H \to G \to F$ is left exact, then the following are equivalent:

(i) $G \to F$ is surjective;

(ii) $\#G = \#H \cdot \#F$.

(Idea of proof: let $I = (\operatorname{Ker} \varepsilon_B)A \subseteq A$ be the Hopf ideal defining $\operatorname{Ker}(G \to F)$, so that $H \cong \operatorname{Spec} A/I$, and consider the morphism

$$A \otimes_B A \longrightarrow A \otimes_k A/I, \qquad a_1 \otimes a_2 \mapsto a_1 \mu(a_2) \mod A \otimes_k I.$$

This is an isomorphism if and only if (i) or (ii) holds.)

Example 5.4. If $G = (G_1 \subset G_2 \cdots)$ is a p-divisible group (over any ring), then we constructed $j_n : G_{n+1} \to G_n$ such that the composition $G_{n+1} \xrightarrow{j_n} G_n \subseteq G_{n+1}$ is $[p]$. So the sequence $0 \to G_1 \to G_{n+1} \xrightarrow{j_n} G_n$ is left exact. By counting ranks we deduce that j_n is surjective (which was used in the proof of the main proposition of the last section).

Remark 5.5. First we make some comments from commutative algebra on the structure of $\mathcal{O}$-algebras A which are finitely generated as a module.

(i) A is isomorphic, as an $\mathcal{O}$-algebra, to a finite product $\prod_i A_i$ where each A_i is a complete Noetherian local $\mathcal{O}$-algebra (also finitely generated as a module). More naturally, this decomposition can be written as $A \xrightarrow{\simeq} \prod_{\mathfrak{m}} A_{\mathfrak{m}}$, where $\mathfrak{m}$ runs over the finitely many maximal ideals of A, and $A_{\mathfrak{m}}$ is the localisation of A at $\mathfrak{m}$.

(ii) A is *finite étale* over $\mathcal{O}$ if and only if the following conditions all hold: A is flat over $\mathcal{O}$ and, for each i, the maximal ideal of A_i is $\mathfrak{m}A_i$ and the finite field extension $A/\mathfrak{m}A_i \supseteq \mathcal{O}/\mathfrak{m}$ is separable.

Lemma 5.6. *Let A be a $\mathcal{O}$-algebra which is finite flat; then A contains a unique subalgebra $A^{ét}$ (the "maximal étale subalgebra") with the following properties:*

(i) $A^{ét}$ is finite étale over $\mathcal{O}$;

(ii) if R is an étale $\mathcal{O}$-algebra, then any $\mathcal{O}$-algebra homomorphism $R \to A$ has image inside $A^{ét}$.

Moreover, A is flat over $A^{ét}$ (even faithfully flat), and if $\mathcal{O}$ is a perfect field then the composition $A^{ét} \to A \to A_{red}$ is an isomorphism.

Proof. Using the decomposition $A = \prod_i A_i$, it is easy to reduce to the case that A is local. Then $K := A/\mathfrak{m}_A \supseteq \mathcal{O}/\mathfrak{m} =: k$ is a finite field extension, and we let k^s be the separable closure of k inside K; by standard Galois theory (Thm of the Primitive Element) it is possible to write $k^s = k(\alpha)$ for some $\alpha \in k^s$; let $f(X) \in k[X]$ be its minimal polynomial and note that $f(X)$, $f'(X)$ are coprime (since k^s/k) is a separable extension.

Let $\widetilde{f}(X) \in \mathcal{O}[X]$ be any monic lift of $f(X)$. By Hensel's Lemma, there exists a unique lift $\widetilde{\alpha} \in A$ of α which is a root of $\widetilde{f}(X)$, and so we let $A^{\text{ét}} \cong \mathcal{O}[X]/\widetilde{f}(X)$ be the $\mathcal{O}$-subalgebra of A generated by $\widetilde{\alpha}$. We need to check that this satisfies all the desired properties:

Firstly, $A^{\text{ét}}$ is a free $\mathcal{O}$-algebra satisfying $A^{\text{ét}}/\mathfrak{m}A^{\text{ét}} = k[X]/f(X) = k^s$, so $A^{\text{ét}}$ is finite étale over $\mathcal{O}$.

Let R be any étale $\mathcal{O}$-algebra and $R \to A$ any homomorphism. Then $R/\mathfrak{m}R$ is a finite product of separable field extensions of k, so it is easy to see that the image of $R/\mathfrak{m}R$ inside K lies inside $k^s = A^{\text{ét}}/\mathfrak{m}A^{\text{ét}}$. Follows that the image of R inside A lies in $A^{\text{ét}}$.

Next, some tricky commutative algebra which we omit ("fibral flatness theorem": see the section "Criteria for flatness' in the Stacks Project if you are interested) proves the following: if $\mathcal{O} \to R' \to R''$ are maps of local rings such that $\mathcal{O} \to R''$ and $R'/\mathfrak{m}R' \to R''/\mathfrak{m}R''$ are flat, then $R' \to R''$ is flat; apply this to $R' = A^{\text{ét}}$ and $R = A$ to deduce that $A^{\text{ét}} \to A$ is flat.

Finally, if $\mathcal{O}$ is a perfect field (so $\mathfrak{m} = 0$ and $\mathcal{O} = k$), then we can take $\widetilde{f}(X) = f(X)$, whence $A^{\text{ét}} = k[X]/f(X) = k^s \xrightarrow{\sim} A/\mathfrak{m}_A$ (note that $k^s = A/\mathfrak{m}_A$ since k is perfect).

□

The following proposition defines the "connected–étale sequence" of a finite flat group scheme:

Proposition 5.7. *Let $G = \operatorname{Spec} A$ be a finite flat group scheme over $\mathcal{O}$. Then:*

(i) $A^{ét}$ is a sub Hopf algebra of A; write $G^{ét} := \operatorname{Spec} A^{ét}$ (called "the étale part of G")

(ii) the affine group scheme $G^0 := \operatorname{Ker}(\operatorname{Spec} A \to \operatorname{Spec} A^{ét})$ over $\mathcal{O}$ is finite flat and connected (called "the connected part of G")

(iii) the sequence $0 \to G^0 \to G \to G^{ét} \to 0$ is exact.

(iv) If $\mathcal{O}$ is a perfect field then this sequence naturally splits: $G \cong G^0 \times G^{ét}$

Proof. (i): It is easy to check that $(A \otimes_{\mathcal{O}} A)^{\text{ét}} = A^{\text{ét}} \otimes_{\mathcal{O}} A^{\text{ét}}$. Thus the universal property of the maximal étale subalgebra implies that $A^{\text{ét}}$ is preserved by μ, ι, ε.

(ii): By definition $G^0 = \operatorname{Spec} A/(\operatorname{Ker}\varepsilon \cap A^{\text{ét}})A$. Write $A = \prod_{i=1}^n A_i$ as a finite product of complete local Noetherian $\mathcal{O}$-algebras, and let $e_i \in A$ be the associated idempotents. By construction $A^{\text{ét}} = \prod_i A_i^{\text{ét}}$, and so $e_1 \in A^{\text{ét}}$.

Since $\mathcal{O}$ is local, its only idempotents are zero and 1; since $e_1, \dots, e_n$ is a complete set of idempotents for A, it follows that $\varepsilon(e_i) = 1$ for exactly one index – cal it $i = 1$ –, and vanishes for all others. Thus $\operatorname{Ker}\varepsilon \cap A^{\text{ét}}$ contains all the idempotents except for the index $i = 1$.

In particular, $\operatorname{Ker}\varepsilon \ni e_2, \dots, e_n$; since $A = \mathcal{O} \oplus \operatorname{Ker}\varepsilon$ it follows that $\mathcal{O}$ is a direct summand of A_1, and so A_1 has residue field $\mathcal{O}/\mathfrak{m}$. Therefore $A_1^{\text{ét}} = \mathcal{O}$ and so $\operatorname{Ker}\varepsilon \cap A_1^{\text{ét}} = 0$. This implies that $\operatorname{Ker}\varepsilon \cap A^{\text{ét}} = (e_2, \dots, e_n)$ and so $A/(\operatorname{Ker}\varepsilon \cap A^{\text{ét}})A = A_1$, which is local and finite flat over $\mathcal{O}$, as required.

(iii): Since we proved in the previous lemma that $A^{\text{ét}} \to A$ is faithfully flat, there is nothing more to do to prove this.

(iv): We must find a sub affine group of G which maps isomorphically to $G^{\text{ét}}$, i.e., a Hopf ideal $I \subseteq A$ such that $A^{\text{ét}} \to A \to A/I$ is an isomorphism. By the previous lemma the ideal $I = \prod_i \mathfrak{m}_{A_i}$ (which is clearly a Hopf ideal since it is the nilradical of A) works. □

So, to any finite flat group scheme G over $\mathcal{O}$, we can (functorially) associate new finite flat group schemes G^0, $G^{\text{ét}}$, which are respectively connected and étale. These have the following universal properties:

- any morphism from a connected group scheme to G factors uniquely through G^0;
- any morphism from G to an étale group scheme factors uniquely through $G^{\text{ét}}$.

(These follow from the characterising property of $A^{\text{ét}}$, together with the following easy observation which you may wish to check: the only morphism from a connected group scheme to an étale group scheme is zero.)

Note that if $\mathcal{O}$ has residue characteristic 0 then the earlier corollary to Cartier's theorem implies that $G^{\text{ét}} = G$ and $G^\circ = 0$; so the interesting case really is when $\mathcal{O}$ has residue characteristic $p > 0$.

These functors behaves well with respect to kernels and surjections:

Lemma 5.8. *Let ? denote $\circ$ or ét.*

(i) If $0 \to H \to G \to F$ is a left exact sequence of finite flat group schemes over $\mathcal{O}$, then so is $0 \to H^? \to G^? \to F^?$.

(ii) If $G \to F$ is a surjection of finite flat group schemes over $\mathcal{O}$, then so is $G^? \to F^?$.

(iii) If $0 \to H \to G \to F \to 0$ is an exact sequence of finite flat group schemes over $\mathcal{O}$, then so is $0 \to H^? \to G^? \to F^? \to 0$.

Proof. By definition of an exact sequence, (i)&(ii)⇒(iii).

(ii): Suppose that $G = \operatorname{Spec} A \to F = \operatorname{Spec} B$ is surjective, and let's prove the same about $G^\circ \to F^\circ$. Algebraically we have the following situation: $B = \prod_{j=1}^m B_j \to A = \prod_{i=1}^n A_i$ is faithfully flat, where the A_i and B_j are finite flat local $\mathcal{O}$-algebras, and $G^\circ \to F^\circ$ is represented by $A_1 \to B_1$ (without loss of generality, by reindexing), which we must prove is flat. But this is clear: we may write the faithfully flat A_1-algebra $A_1 \otimes_A B = \prod_{j \in S} B_j$ for some set $S \subseteq \{1, \dots, m\}$ containing 1; thus B_1 is a direct summand of a flat A_1-algebra, hence is flat itself.

With the same surjecitivty situation, we have a faithfully flat map $A^{\text{ét}} \to B^{\text{ét}} \to B$ (since it is equal to $A^{\text{ét}} \hookrightarrow A \hookrightarrow B$, which is a composition of faithfully flat maps hence is faithfully flat) in which the second arrow is faithfully flat; it follows that the first arrow is also faithfully flat.

(i): Now suppose that $0 \to H \to G \to F$ is a left exact sequence of finite flat group schemes over $\mathcal{O}$. Then $H^\circ \to G^\circ$ is injective, and the composition $H^\circ \to G^\circ \to F^\circ$ is zero, so $H^\circ \subseteq \operatorname{Ker}(G^\circ \subseteq F^\circ)$. Conversely, $\operatorname{Ker}(G^\circ \to F^\circ)$ is a connected (since it is a subgroup of the connected G°) sub affine group scheme of H, and hence it is contained in H° (by universal property of H°).

It remains to prove that $0 \to H^{\text{ét}} \to G^{\text{ét}} \to F^{\text{ét}}$ is also left exact; this is the trickiest assertion, and we will only sketch the proof under the additional assumption that $G \to F$ is surjective (so that $0 \to H \to G \to F \to 0$ is exact). Then we have a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & H^\circ \arrow[r] \arrow[d] & G^\circ \arrow[r] \arrow[d] & F^\circ \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & F \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^{\text{ét}} \arrow[r] \arrow[d] & G^{\text{ét}} \arrow[r] \arrow[d] & F^{\text{ét}} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

in which each column is exact (by the connected–étale exact sequence), the central row is exact (by assumption), and the top row is exact (by what we have already proved). By the "3×3 lemma", it follows formally that the bottom row is exact (of course, for this to work we need to know that exact sequence of affine group schemes, as we have defined them, satisfy the same types of formalism as exact sequences of ordinary groups; this essentially follows by taking points in all $\mathcal{O}$-algebras.) □

End of lecture 7.

Last time we introduced the connected and étale parts of a finite flat group scheme over $\mathcal{O}$, and saw that they behaved well under short exact sequences; from this we can deduce that the connected and étale parts of a p-divisible group are well-defined:

Corollary 5.9. *If $G = (G_1 \subset G_2 \subset \cdots)$ is a p-divisible group over $\mathcal{O}$, then so are $G^\circ := (G_1^\circ \subset \cdots)$, and $G^{\acute{e}t} := (G_1^{\acute{e}t} \subset \cdots)$; they are called the connected and étale parts of G.*

Proof. Let ? denote $\circ$ or ét. Firstly, the previous lemma implies that $G^?_{n+1}[p^n] = G_{n+1}[p^n]^? = G^?_n$. Secondly, from the short exact sequence $0 \to G_1 \to G_{n+1} \xrightarrow{j_n} G_n \to 0$ we obtain another short exact sequence $0 \to G^?_1 \to G^?_{n+1} \xrightarrow{j_n} G^?_n \to 0$, whence the multiplicativity of the ranks (and a trivial induction on n) implies that $\#G^?_{n+1} = (\#G^?_1)^n$. Finally, the short exact sequence $0 \to G^\circ_1 \to G_1 \to G^{\text{ét}}_1 \to 0$ shows that $\#G^?_1$ is an order of p. Combining these observations we see that $G^?$ satisfies all the axioms of a p-divisible group. □

6 Points of a p-divisible group

Remark 6.1 (Base change)**.** We now make some side comments on base changing p-divisible groups – this is straightforward, but we will often use it.

If $G = \operatorname{Spec} A$ is an affine group scheme over any ring k, and k' is a k-algebra, then it is very easy to check that $G \otimes_k k' = \operatorname{Spec}(A \otimes_k k')$ is an affine group scheme over k', i.e., $A \otimes_k k'$ is a Hopf-algebra over k'. Base change has the following properties:

(i) If R is a k'-algebra, then $G(R) = (G \otimes_k k')(R)$; this is the standard result from commutative algebra that $\operatorname{Hom}_{k\text{-alg}}(A, R) = \operatorname{Hom}_{k\text{-alg}}(A \otimes_k k', R)$.

(ii) If $0 \to H \to G \to F$ is a left exact sequence of affine group schemes over k, then $0 \to H \otimes_k k' \to G \otimes_k k' \to F \otimes_k k'$ is left exact over k'.

(iii) In particular, it follows that $G[n] \otimes_k k' = (G \otimes_k k')[n]$.

(iv) If G is finite flat (resp. finite étale) over k, then so is $G \otimes_k k'$ over k' and it has the same order.

If $G = (G_1 \subset G_2 \subset \cdots)$ is now a p-divisible group of height h over k, it follows from (iii) and (iv) that $G \otimes_k k' := (G_1 \otimes_k k' \subset G_2 \otimes_k k' \subset \cdots)$ is a p-divisible group of height h over k'.

Now we really begin the section. $\mathcal{O}$ continues to be a complete Noetherian local ring, with maximal ideal $\mathfrak{m}$, and G is a p-divisible group over $\mathcal{O}$.

Definition 6.2. We want to define the *R-points of G*, where R is a complete local $\mathcal{O}$-algebra, in a way which takes topologies into account; for this to be reasonable we need to assume that the set of $\mathfrak{m}R$-adic topological nilpotent elements of R is exactly its maximal ideal $\mathfrak{m}_R$, i.e., that for any $x \in \mathfrak{m}_R$, there exists $r \gg 0$ satisfying $x^r \in \mathfrak{m}_R$ (Note: I made a mistake in class: we do *not* want to assume the existence of a single value of r satisfying $\mathfrak{m}_R^r \subseteq \mathfrak{m}R$ for $r \gg 0$.)

We first put $G(R/\mathfrak{m}^r R) := \varinjlim_n G_n(R/\mathfrak{m}^r R)$ for each $r \geq 1$, and then define the *R-valued points of G* to be

$$G(R) := \varprojlim_r G(R/\mathfrak{m}^r R)$$

Alternatively, writing $G_n := \operatorname{Spec} A_n$ and putting $\mathcal{A} := \varprojlim_n A_n$ (which makes sense even if G is not connected), we see that

$$G(R) = \varprojlim_r \varinjlim_n \operatorname{Hom}_{\mathcal{O}\text{-alg}}(A_n, R/\mathfrak{m}^r R) = \operatorname{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}, R)$$

where R has the $\mathfrak{m}R$-adic topology and $\mathcal{A}$ has the inverse limit topology (with each A_n being given the $\mathfrak{m}A_n$-adic topology).

Lemma 6.3. *Points have the following basic properties:*

(i) $G(R)$ is a $\mathbb{Z}_p$-module.

(ii) The canonical map $\varinjlim_n \varprojlim_r G_n(R/\mathfrak{m}^r R) \to \varprojlim_r \varinjlim_r G_n(R/\mathfrak{m}^r R) = G(R)$ is injective and its image is $G(R)_{tors}$.

(iii) If G is étale then the previous map is an isomorphism, $G(R) = \varinjlim_n G_n(R/\mathfrak{m}_R)$, and this is torsion.

(iv) If $\mathcal{O}$ has residue characteristic p and G is connected, then there exists a (non-canonical) isomorphism of sets (of topological spaces if we are more careful)

$$G(R) \cong \mathfrak{m}_R \oplus \cdots \oplus \mathfrak{m}_R, \qquad (d \text{ copies})$$

where d is the dimension of G.

Proof. (i): Each $G_n(R/\mathfrak{m}^r)$ is a $\mathbb{Z}/p^n\mathbb{Z}$-module since G_n is p^n-torsion. Hence $G(R/\mathfrak{m}^r R)$ and $G(R)$ are $\mathbb{Z}_p$-modules.

(ii): Each transition map $G_n(R/\mathfrak{m}^r) \to G_{n+1}(R/\mathfrak{m}^r)$ is injective since $G_n \subseteq G_{n+1}$; so the canonical map is injective by general formalism of doubly-indexed systems. Regarding torsion, let $s \geq 1$ and recall that the sequence

$$0 \to G_s(R/\mathfrak{m}^r R) \to G_{n+s}(R/\mathfrak{m}^r R) \xrightarrow{p^s} G_{n+s}(R/\mathfrak{m}^r R)$$

is exact. Apply $\varinjlim_n \varprojlim_r$ to deduce that $\varprojlim_r G_s(R/\mathfrak{m}^r R)$ is the p^s-torsion of $G(R)$. Now take $\varinjlim_s$ to prove the assertion.

(iii): Now suppose that G is étale over $\mathcal{O}$. Thus A_n (the $\mathcal{O}$-algebra underlying G_n, as usual) is étale and so the "infinitesimal lifting criterion for étaleness" implies that $\operatorname{Hom}(A_n, R/\mathfrak{m}^{r+1}) \xrightarrow{\simeq} \operatorname{Hom}(A_n, R/\mathfrak{m}^r) \xrightarrow{\simeq} \operatorname{Hom}(A_n, R/\mathfrak{m}_R)$ for all $r \geq 1$. General formalism of doubly-indexed inverse limits then shows that the canonical map in (ii) is an isomorphism, whence $G(R)$ is torsion and has the claimed form.

(iv): If G is connected, then we studied its associated connected formal group $\mathcal{A} := \varprojlim_n A_n$ in some detail in a previous section, and in Remark 4.13 mentioned that there always exists a (non-canonical) isomorphism of $\mathcal{O}$-algebras $\mathcal{A} \cong \mathcal{O}[[X_1, \ldots, X_d]]$. Therefore

$$G(R) \cong \operatorname{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{O}[[X_1, \ldots, X_d]], R) \cong (\mathfrak{m}_R)^d$$

since such a continuous homomorphism is determined by sending $X_1, \ldots, X_d$ to arbitrary topologically nilpotent elements of R, and $\mathfrak{m}_R$ is precisely the set of such elements. □

Example 6.4. Assume $\mathcal{O}$ has residue characteristic p, and let's see the previous lemma explicitly in the case $G = \boldsymbol{\mu}_{p^\infty, \mathcal{O}}$. Then

$$\begin{aligned}\boldsymbol{\mu}_{p^\infty,\mathcal{O}}(R) = \varprojlim_r \varinjlim_n \mu_{p^n,\mathcal{O}}(R/\mathfrak{m}^r R) &= \varprojlim_r \varinjlim_n \{x \in R/\mathfrak{m}^r R^\times : x^{p^n} = 1\} \\ &= \varprojlim_r 1 + \mathfrak{m}_R/\mathfrak{m}^r R \\ &= 1 + \mathfrak{m}_R,\end{aligned}$$

and

$$\begin{aligned}\varinjlim_n \varprojlim_r \boldsymbol{\mu}_{p^\infty,\mathcal{O}}(R/\mathfrak{m}^r R) = \varinjlim_n \varprojlim_r \{x \in R/\mathfrak{m}^r R^\times : x^{p^n} = 1\} &= \varinjlim_n \{x \in R^\times : x^{p^n} = 1\} \\ &= p\text{-power torsion in } R^\times \\ &= p\text{-power torsion in } 1 + \mathfrak{m}_R,\end{aligned}$$

as predicted by the previous lemma.

The main result of the section is that the connected-étale sequence works well with respect to points:

Proposition 6.5. *Suppose that $\mathcal{O}$ has perfect residue field of characteristic p, and let R continue to be a complete local $\mathcal{O}$-algebra as above. Then the sequence of abelian groups*

$$0 \to G^\circ(R) \to G(R) \to G^{ét}(R) \to 0$$

is exact.

Proof. Since $0 \to G_n^\circ \to G_n \to G_n^{\text{ét}} \to 0$ is exact, and since the three operations "taking points of an affine group scheme", $\varprojlim_r$, and $\varinjlim_n$ preserve left exact sequences, the sequence is certainly left exact. The non-trivial part is showing that $G(R) \to G^{\text{ét}}(R)$ is surjective (which is not true at fixed levels n).

As usual, write $G_n = \operatorname{Spec} A_n$, with corresponding étale and connected pieces $A_n^{\text{ét}} \subseteq A_n \twoheadrightarrow A_n^\circ$. Thus

$$\mathcal{A}^{\text{ét}} := \varprojlim_n A_n^{\text{ét}} \subseteq \mathcal{A} := \varprojlim_n A_n \twoheadrightarrow \mathcal{A}^\circ := \varprojlim_n A_n^\circ$$

are the formal groups associated to $G^{\text{ét}}$, G, and G° respectively. We need to prove that

$$\operatorname{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}, R) \to \operatorname{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}^{\text{ét}}, R)$$

is surjective. We will prove that there exists a (non-canonical) isomorphism of $\mathcal{O}$-algebras $\mathcal{A} \cong \mathcal{A}^{\text{ét}}\widehat{\otimes}_{\mathcal{O}}\mathcal{A}^\circ$ (whence there is a splitting $\mathcal{A} \cong \mathcal{A}^{\text{ét}}\widehat{\otimes}_{\mathcal{O}}\mathcal{A}^\circ \xrightarrow{\text{id}\otimes\varepsilon} \mathcal{A}^{\text{ét}}$ of the inclusion $\mathcal{A}^{\text{ét}} \subseteq \mathcal{A}$, and so the surjectivity is clear).

Again using Remark 4.13 to pick an isomorphism $\mathcal{A}^\circ \cong \mathcal{O}[[X_1, \dots, X_d]]$, and picking arbitrary lifts of the variables X_i to $\mathcal{A}$, there is a splitting $\sigma : \mathcal{A}^\circ \cong \mathcal{O}[[X_1, \dots, X_d]] \to \mathcal{A}$ of the surjection $\mathcal{A} \twoheadrightarrow \mathcal{A}^\circ$. Tensoring with $\mathcal{A}^{\text{ét}}$ we obtain

$$\text{inclus.} \otimes \sigma : \mathcal{A}^{\text{ét}}\widehat{\otimes}_{\mathcal{O}}\mathcal{O}[[X_1, \dots, X_d]] \to \mathcal{A}.$$

We must prove this is an isomorphism. Since everything is flat and complete, it is enough to prove it is an isomorphism after applying $\otimes_{\mathcal{O}} k$, where k is the residue field. So from now on we replace $\mathcal{O}$ by k, and we consider

$$\mathcal{A}^{\text{ét}}[[X_1, \dots, X_d]] = \mathcal{A}^{\text{ét}}\widehat{\otimes}_k k[[X_1, \dots, X_d]] \to \mathcal{A}.$$

This is easily checked to be an isomorphism by using the following purely algebraic observations:

(i) the structure map $k \to \mathcal{A}^{\text{ét}}$ has a section $\varepsilon : \mathcal{A}^{\text{ét}} \to k$, and there is a map $\mathcal{A} \to \mathcal{A}^\circ = k[[X_1, \dots, X_d]]$ such that the composition $\mathcal{A}^{\text{ét}}[[X_1, \dots, X_d]] \to \mathcal{A} \to k[[X_1, \dots, X_d]]$ is ε. (This map is by construction of σ.)

(ii) there exists a map $\mathcal{A} \to \mathcal{A}^{\text{ét}}$ such that the composition $\mathcal{A}^{\text{ét}}[[X_1, \dots, X_d]] \to \mathcal{A} \to \mathcal{A}^{\text{ét}}$ is the canonical projection. (This map $\mathcal{A} \to \mathcal{A}^{\text{ét}}$ is given by $\mathcal{A} = \varprojlim_n A_n \to \varprojlim_n A_{n\,\text{red}} \cong \varprojlim_n A_n^{\text{ét}} = \mathcal{A}^{\text{ét}}$, where we use Lemma 5.6.)

□

End of lecture 8

Corollary 6.6. *Under the same conditions as the previous proposition, assume also that R is normal and has algebraically closed fraction field. Then $G(R)$ is a divisible group.*

Proof. By the previous proposition, we may assume that G is either connected or étale.

We will start with the étale case, which is an explicit calculation. We saw in the first lemma of the section that $G(R) = \varinjlim_n G_n(R/\mathfrak{m}_R)$. Writing $R/\mathfrak{m}_R = K$ (which is an algebraically closed field extension of k) and $G'_n = G_n \otimes_k K$, we have $G_n(K) = G'_n(K)$ by our earlier remarks on points. But $G' = (G'_1 \subset G'_2 \subset \cdots)$ is an étale p-divisible group over an algebraically closed field K, hence is isomorphic to $\underline{(\mathbb{Q}_p/\mathbb{Z}_p)^h}_K$, where h is he height of G. So then

$$\varinjlim_n G_n(K) = \varinjlim_n \underline{(p^n\mathbb{Z}/\mathbb{Z})^h}_K(K) = (p^n\mathbb{Z}/\mathbb{Z})^h = (\mathbb{Q}_p/\mathbb{Z}_p)^h,$$

which is certainly a divisible group.

Now suppose instead that G is connected. Let $\mathcal{A}$ be its associated connected formal group, and let $f \in \mathrm{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}, R)$ be an R-valued point of G. We must show that f is divisible by p, i.e., find $f' \in \mathrm{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}, R)$ such that $f = f' \circ [p]$, where $[p] : \mathcal{A} \to \mathcal{A}$ is the multiplication by p map. We proved in the section on formal groups that $[p] : \mathcal{A} \to \mathcal{A}$ is an isogeny, i.e., injective and makes $\mathcal{A}$ into a finite free algebra over itself; therefore $R' := \mathcal{A} \otimes_{[p],\mathcal{A},f} R$ is a finite free algebra extension of R. Since R is normal and has algebraically closed fraction field, the inclusion $R \hookrightarrow R'$ has a section $\sigma : R' \to R$. The composition $\mathcal{A} \xrightarrow{[p]} \mathcal{A} \to R' \xrightarrow{\sigma} R$ has the desired property by construction. □

7 Aside: duality theory

Before proving the main theorem – the Hodge–Tate decomposition –, there is one remaining algebraic topic concerning finite flat group schemes and p-divisible groups: duality.

k is an arbitrary commutative ring in this section. If M is a finite flat k-module, then we write $M^* := \mathrm{Hom}_{k\text{-mod}}(M, k)$ for its dual, which is another finite flat k-module under point-wise multiplication; a morphism $\phi : M \to N$ of k-modules induces a morphism of k-modules $\phi^* : N^* \to M^*$ by the rule $\phi(f)(m) := f(\phi(m))$, where $f \in N^*$ and $m \in M$.

Lemma 7.1. *The evaluation map*

$$M \to M^{**}, \quad m \mapsto \mathrm{ev}_m = \langle M^* \ni f \mapsto f(m) \rangle$$

is an isomorphism of k-modules. If N is another finite flat k-module, then the canonical morphism of k-modules

$$M^* \otimes_k N^* \to (M \otimes_k N)^*, \quad f \otimes g \mapsto \langle M \otimes_k N \ni m \otimes n \mapsto f(m)g(n) \rangle$$

is an isomorphism.

Proof. By localising at each maximal ideal of k we may assume k is local (which is our only case of interest anyway). Then M and N are finite free k-modules, in which case the claims are trivial linear algebra. □

Suppose that $G = \operatorname{Spec} A$ is a finite flat group scheme over k, i.e., A is a finite flat k-module equipped with maps of k-modules $e, m, \mu, \varepsilon, \iota$

$$\begin{tikzcd}
k \arrow[r, bend left, "e"] & A \arrow[l, bend left, "\varepsilon"] \arrow[loop below, "\iota"] \arrow[r, bend right, "\mu"'] & A \otimes_k A \arrow[l, bend right, "m=\text{mult}"']
\end{tikzcd}$$

satisfying the algebra and Hopf-algebra axioms.

Proposition 7.2. *The dual maps*

$$\begin{tikzcd}
k = k^* \arrow[r, bend left, "\varepsilon^*"] & A^* \arrow[l, bend left, "e^*"] \arrow[loop below, "\iota^*"] \arrow[r, bend right, "m^*"'] & A^* \otimes_k A^* = (A \otimes_k A)^* \arrow[l, bend right, "\mu^*"']
\end{tikzcd}$$

also satisfy the algebra and Hopf algebra axioms, thereby giving rise to a finite flat group scheme $G^* := \operatorname{Spec} A^*$, known as the Cartier dual of *G.*

Proof. Tedious algebra shows that the algebra+Hopf algebra axioms are symmetric:

(1) m is associative and μ is coassociative:

$$\begin{tikzcd}
A \otimes_k A \otimes_k A \arrow[r, "m \otimes \mathrm{id}_A"] & A \otimes_k A \\
A \otimes_k A \arrow[u, "\mathrm{id}_A \otimes \mu"] & A \arrow[l, "\mu"] \arrow[u, "\mu"']
\end{tikzcd}
\qquad
\begin{tikzcd}
A \otimes_k A \otimes_k A & A \otimes_k A \arrow[l, "\mu \otimes \mathrm{id}_A"'] \\
A \otimes_k A \arrow[u, "\mathrm{id}_A \otimes \mu"] & A \arrow[l, "\mu"] \arrow[u, "\mu"']
\end{tikzcd}$$

(2) e is a left unit and ε is a left counit:

$$\begin{tikzcd}
k \otimes_k A \arrow[r, "e \otimes \mu"] \arrow[dr, "="'] & A \otimes_k A \arrow[d, "m"] \\
& A
\end{tikzcd}
\qquad
\begin{tikzcd}
k \otimes_k A & A \otimes_k A \arrow[l, "\varepsilon \otimes \mathrm{id}_A"'] \\
& A \arrow[ul, "="] \arrow[u, "\mu"]
\end{tikzcd}$$

(3) Existence of left coinverses

$$\begin{tikzcd}
A \otimes_k A \arrow[d, "\text{mult}"'] & & A \otimes_k A \arrow[ll, "\iota \otimes \mathrm{id}_A"'] \\
A & & A \arrow[dl, "\varepsilon"'] \arrow[u, "\mu"] \\
& k \arrow[ul, "e"] &
\end{tikzcd}$$

(4) Commutativity and cocommutativity

$$\begin{tikzcd}
A \otimes_k A & A \otimes_k A \arrow[l, "\text{swap"'] \\
& A \arrow[ul, "\mu"] \arrow[u, "\mu"]
\end{tikzcd}$$

(5) "μ and ε are homomorphisms of k-algebras"

$$\begin{tikzcd}
A \otimes_k A \arrow[r, "m"] \arrow[d, "\mu\otimes\mu"'] & A \arrow[d, "\mu"] & & A \arrow[r, "\mu"] & A \otimes_k A \\
A \otimes_k A \arrow[r, "m"'] & A & & k \arrow[u, "e"] \arrow[r, "="'] & k \otimes_k k \arrow[u, "e\otimes e"']
\end{tikzcd}$$

(6) "ι is a homomorphism of k-algebras"

□

Example 7.3. If Γ is a finite group over k, then $k[\Gamma]^* = k^\Gamma$. In particular, $\boldsymbol{\mu}_{n,k}^* = \underline{\mathbb{Z}/n\mathbb{Z}}_k$. If k has characteristic p, then $\boldsymbol{\alpha}_{p,k}$ is self-dual.

It is important to identify the points of the Cartier dual G^* in terms of the group of morphisms $\mathrm{Hom}(G, \mathbb{G}_{m,k})$:

Lemma 7.4. *For any k-algebra R, there is a natural identification of groups*

$$G^*(R) = \mathrm{Hom}(G \otimes_k R, \mathbb{G}_{m,R})$$

(where the right denotes the group of morphisms of affine group schemes over R).

Proof. Replacing G by $G\otimes_k R$ and k by R, it is enough to show that $G^*(k) = \mathrm{Hom}(G, \mathbb{G}_{m,k})$.

Since any $f \in G^*(k) = \mathrm{Hom}_{k\text{-alg}}(A^*, k)$ has the form $f = \mathrm{ev}_a$ for some unique $a \in A$, we have an inclusion

$$G^*(k) \hookrightarrow A, \quad \mathrm{ev}_a \mapsto a,$$

whose image we denote by Σ, i.e.,

$$\Sigma = \{a \in A : \mathrm{ev}_a : A^* \to k \text{ is a } k\text{-algebra homomorphism}\}$$

When is ev_a a k-algebra homomorphism? Let $\alpha, \beta \in A^*$; the product $\alpha \cdot \beta$ of α, β in A^* is by definition $(\alpha\otimes\beta)\circ\mu : A \to A\otimes_k A \to k\otimes_k k = k$, and so $\mathrm{ev}_a(\alpha\cdot\beta) = (\alpha\otimes\beta)(\mu(a))$. On the other hand, $\mathrm{ev}_a(\alpha)\,\mathrm{ev}_a(\beta) = \alpha(a)\beta(a) = \alpha \otimes \beta(a \otimes a)$. It follows that ev_a is multiplicative if and only if $\mu(a) = a \otimes a$. A similar argument shows that $\mathrm{ev}_a(1_{A^*})$ if and only if $\varepsilon(a) = 1$.

So $\Sigma := \{a \in A : \mu(a) = a \otimes a \text{ and } \varepsilon(a) = 1\}$. But the set of Hopf algebra homomorphisms $k[t, t^{-1}] \to A$ also corresponds to Σ, via evaluation at t. This gives natural bijections

$$G^*(k) = \Sigma = \mathrm{Hom}(G, \mathbb{G}_{m,k}),$$

which you should check respects the group structures on the left and right sides. □

It can be shown that the Cartier dual of a short exact sequence of finite flat groups schemes $0 \to H \to G \to F \to 0$ is again short exact: $0 \to F^* \to G^* \to H^* \to 0$.

Definition 7.5. If $G = (G_0 \subseteq G_1 \subseteq \cdots)$ is a p-divisible group over k, of height h, then its *Cartier dual* is the p-divisible group

$$G^* = (G_0^* \xrightarrow{j_1^*} G_1^* \xrightarrow{j_2^*} \cdots)$$

(where the transition maps are the duals of the maps in Lemma 3.9). Using the previous fact on short exact sequences, it is easy to check that this is really a p-divisible group.

Example 7.6. $\boldsymbol{\mu}^*_{p^\infty,k} = \underline{\mathbb{Q}_p/\mathbb{Z}_p}_k$.

We quote, but do not prove, the following result about duals of p-divisible groups (the dimension of a p-divisible group G is by definition the dimension of its connected part G° as in Definition 4.10):

Proposition 7.7. *Let G be a p-divisible group over k of height h. Then*

$$\dim G + \dim G^* = h.$$

8 The Hodge–Tate decomposition

Our aim is to soon prove the Hodge–Tate decomposition of a p-divisible group; although some parts of the intermediate theory can be developed in greater generality, from now on we work in the following set-up:

Let K be a complete discrete valuation field; recall this means that K is complete under a norm $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the following properties: $|x| = 0$ if and only if $x = 0$; $|xy| = |x||y|$; $|x+y| \leq \max(|x|,|y|)$; and there exists $\pi \in K^\times$ such that $|\pi|$ generates the group $|K^\times|$ (this is the "discreteness" condition). These assumptions imply that the *ring of integers* $\mathcal{O} := \{x \in K : |x| \leq 1\}$ is a complete discrete valuation ring with maximal ideal $\mathfrak{m} = \pi\mathcal{O}$ (in particular, $\mathcal{O}$ is a complete Noetherian local ring – so the theory we developed in the previous chapters applies).

The norm extends uniquely to the algebraic closure K^{alg} of K (but it will no longer be discrete), and we write $\mathbb{C}_K$ for its topological completion; the norm also extends to $\mathbb{C}_K$, and we set $R := \{x \in \mathbb{C}_K : |x| \leq 1\}$ for its ring of integers. It is a fact (Krasner's Lemma) that $\mathbb{C}_K$ is still algebraically closed.

The action of the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{alg}}/K)$ extends by continuity to $\mathbb{C}_K$, and by functoriality will also act on the various groups of points, tangent spaces, etc. which we will study.

Finally, we assume that K has characteristic zero but that $k := \mathcal{O}/\mathfrak{m}$ is a perfect field of characteristic p.

Example 8.1. $\mathcal{O} = \mathbb{Z}_p \subseteq K = \mathbb{Q}_p$; then $\mathbb{C}_K$ is the completion of the algebraic closure of $\mathbb{Q}_p$, sometimes denoted by $\mathbb{C}_p$.

Let G be a p-divisible group over $\mathcal{O}$. Recall that the goal of Hodge–Tate decomposition is to understand the natural action of Gal_K on the Tate module (and maybe also comodule)

$$T_p(G) = \varprojlim_n G_n(K^{\mathrm{alg}}), \qquad \Phi_p(G) = \varinjlim_n G_n(K^{\mathrm{alg}}).$$

We begin this process by slightly reinterpreting the Tate (co)module:

Lemma 8.2. *If H is any finite flat group scheme over $\mathcal{O}$, then the natural maps*

$$H(K^{alg}) \hookrightarrow H(\mathbb{C}_K) \leftarrow H(R) \to \varprojlim_r H(R/\mathfrak{m}^r R)$$

are all isomorphisms.

Proof. Recall that finite free group schemes over any algebraically field of characteristic zero are equivalent to the category of groups, by taking points: so if $L' \supset L$ is *any* extension of algebraically closed, characteristic zero fields, then $H(L) = H(L')$.

Write $H = \operatorname{Spec} B$. The image of any $\mathcal{O}$-algebra homomorphism $f : B \to \mathbb{C}_K$ is finitely generated over $\mathcal{O}$, hence lies in R (this is not hard to see); so $H(\mathbb{C}_K) = H(R)$.

Finally, R is $\mathfrak{m}R$-adically complete, so

$$H(R) = \operatorname{Hom}_{\mathcal{O}\text{-alg}}(B, R) = \varprojlim_r \operatorname{Hom}_{\mathcal{O}\text{-alg}}(B, R/\mathfrak{m}^r R). \qquad \square$$

Corollary 8.3. *$T_p(G) = \varprojlim_n G_n(\mathbb{C}_K)$ and $\Phi_p(G) = G(R)_{tors}$.*

Proof. First equality is immediate from the lemma. For the second, use

$$\Phi_p(G) = \varinjlim_n G_n(K^{\text{alg}}) = \varinjlim_n \varprojlim_r H(R/\mathfrak{m}^r R) = G(R)_{\text{tors}},$$

where the final equality is from last time. □

Now we define the logarithm map for G. As usual, we write $G_n = \operatorname{Spec} A_n$, and we let $\mathcal{A}^\circ := \varprojlim_n A_n^\circ$ be the connected formal group associated to the connected p-divisible group G°. Also set $I := \operatorname{Ker} \varepsilon \subseteq \mathcal{A}^\circ$.

If M is an $\mathcal{O}$-module, then the *tangent space* of G with values in M is by definition the tangent space of G^0 with values in M (as in Definition 4.10), i.e.,

$$\mathfrak{t}_G(M) := \mathfrak{t}_{G^0}(M) = \operatorname{Hom}_{\mathcal{O}}(I/I^2, M).$$

The logarithm map will be a $\mathbb{Z}_p$-module homomorphism

$$\log_G : G(R) \longrightarrow \mathfrak{t}_G(\mathbb{C}_K),$$

which we now construct. From (the easy left exactness part of) Proposition 6.5, and Lemma 6.3, we know that the inclusion of points $G^\circ(R) \subseteq G(R)$ has torsion quotient. So, if $f \in G(R)$, then $p^i f \in G^\circ(R) = \operatorname{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}^\circ, R)$ for $i \gg 0$, and it makes sense to evaluate it at any $a \in A^\circ$ to get $(p^i f)(a)$; then we can divide by p^i in $\mathbb{C}_K$ to get

$$\frac{(p^i f)(a)}{p^i} \in \mathbb{C}_K$$

(note that $p^i f$ denotes multiplication by p^i in the group of points $G(R)$, while the division by p^i is honest division in the field $\mathbb{C}_K$).

Lemma 8.4. *The limit*

$$\log_G(f)(a) := \lim_{i \to \infty} \frac{(p^i f)(a)}{p^i}$$

exists in $\mathbb{C}_K$ if $a \in I$, and has the following properties:

(i) $\log_G(f)(a) = 0$ *if* $a \in I^2$

(ii) $\log_G(f + g)(a) = \log_G(f)(a) + \log_G(g)(a)$ *if* $f, g \in G(R)$ *and* $a \in I$.

Proof. We define a descending filtration on $G^\circ(R) = \operatorname{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}^\circ, R)$ by the rule

$$F^\lambda G^\circ(R) = \{f : \nu(f(a)) \geq \lambda \ \forall a \in I\}$$

where $\lambda > 0$ is any positive real number. Here, as often in the theory of complete discrete valuation fields, we write $\nu(x) := -\log_p |x|$ for the *valuation* of $x \in \mathbb{C}_K$; note that $|x| = p^{-\nu(x)}$, and so $\nu(x)$ and $|x|$ are equivalent ways of measuring the size of x (but $|x|$ is small when $\nu(x)$ is large!).

If $f \in F^\lambda G^\circ(R)$ and $a \in I$, then $[p]a = pa + z$ for some $z \in I^2$, and so

$$(pf)(a) = f([p]a) = f(pa + z) = pf(a) + g(z),$$

which has valuation $\geq \min(\nu(p)+\lambda, 2\lambda)$. This shows that $pF^\lambda G^\circ(R) \subseteq F^{\lambda+\min(\nu(p),\lambda)}G^\circ(R)$.

Since any $f \in G^\circ(R)$ belongs to $f \in F^\lambda G^\circ(R)$ for some $\lambda > 0$, this shows that for any $\lambda' \gg 0$ (which we may as well assume is $\geq \nu(p)$), we can find $i \gg 0$ such that $p^i f \in F^{\lambda'}G(R)$; but then the previous argument shows that

$$\frac{(p^{i+1}f)(a)}{p^{i+1}} - \frac{(p^i f)(a)}{p^i} = \frac{(p^i f)(z)}{p^{i+1}},$$

which has valuation $\geq 2(\lambda' + i\nu(p)) - (i+1)\nu(p) = 2\lambda' + (i-1)\nu(p) \to \infty$ as $i \to \infty$. This shows that the sequence $\frac{(p^i f)(a)}{p^i}$ is Cauchy as $i \to \infty$, and so it converges in$\mathbb{C}_K$.

This has also shown that for any $z \in I^2$, the sequence $\frac{(p^i f)(z)}{p^i}$ tends to zero as $i \to \infty$, proving (i).

For (ii), write $\mu(a) = a \otimes 1 + 1 \otimes a + z$ for some $z \in I\widehat{\otimes}_{\mathcal{O}}I$, so that $(f+g)(a) \equiv f(a) + g(z) \mod f(I)g(I)$ and use the same estimates. □

The previous lemma shows that the logarithm

$$\log_G : G(R) \to \mathfrak{t}_G(\mathbb{C}_K)$$

is a well-defined $\mathbb{Z}_p$-module homomorphism.

Corollary 8.5. $\log_G$ *has the following properties:*

(i) it is a local homeomorphism: if $\lambda > \nu(p)/(p-1)$ *then*

$$\log_G : F^\lambda G^\circ(R) \overset{\cong}{\to} \{\tau \in \mathfrak{t}_G(\mathbb{C}_K) : \nu(\tau(a)) \geq \lambda \, \forall a \in I/I^2\}$$

(ii) it is surjective and has kernel $G(R)_{tors}$.

Proof. (i): Pick a non-canonical isomorphism $\mathcal{A}^\circ \cong \mathcal{O}[[X_1, \dots, X_n]]$, so that I/I^2 is the free $\mathcal{O}$-module with basis $X_1, \dots, X_n$; then check that the inverse is given by

$$\tau \mapsto \text{the unique } f \in \mathrm{ContHom}_{\mathcal{O}\text{-alg}}(\mathcal{A}^\circ, R) \text{ satisfying } f(X_i) = \tau(X_i)\ \forall i$$

(ii): Certainly $\mathrm{Ker}\log_G \subseteq G(R)_{\mathrm{tors}}$ since $\mathfrak{t}_G(\mathbb{C}_K)$ is torsion-free. In the other direction, if $f \in \mathrm{Ker}\log_G$ then $p^i \in \mathrm{Ker}\log_G$ for all $i \geq 1$: by picking $i \gg 0$ we may arrange that $p^i f \in F^\lambda G^\circ(R)$ for λ sufficiently large that $\log_G$ is a local homeomorphism (in particular injective) on $F^\lambda G^\circ(R)$, by the previous corollary. This implies $p^i f = 0$ for $i \gg 0$, so f is torsion.

Finally, if $\tau \in \mathfrak{t}_G(\mathbb{C}_K)$ then $p^i\tau$ is in the RHS of i for $i \gg 0$; thus $p^i\tau$ is in the image of $\log_G$. But we proved in Corollary 6.6 that $G(R)$ is divisible, whence it easily follows that τ is also in the image (this is the key application of Corollary 6.6.) □

We now have a short exact sequence

$$0 \longrightarrow G(R)_{\mathrm{tors}} \longrightarrow G(R) \xrightarrow{\log_G} \mathfrak{t}_G(\mathbb{C}_K) \longrightarrow 0$$

in which all maps are Γ_K-equivariant (automatically).

Example 8.6. Suppose that $G = \boldsymbol{\mu}_{p^\infty,\mathcal{O}}$. Then we saw last time that $G(R) = 1 + \mathfrak{m}_R$, and so $G(R)_{\text{tors}}$ is the group of (necessarily p-power) roots of unity μ_{p^∞} in $1+\mathfrak{m}_R$. Thus we have an exact sequence

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow 1 + \mathfrak{m}_R \xrightarrow{\log_G} \mathbb{C}_K \longrightarrow 0,$$

and it can be directly checked that $\log_G$ is the usual p-adic logarithm $\log(1 + x) = \sum_{i=}^{\infty}(-1)^{n+1}x^n/n!$

The next step is to relate the logarithm on G to the previous example using duality. For each n we apply Lemma 7.4 to write

$$G_n^*(R) \cong \mathrm{Hom}(G_n \otimes_{\mathcal{O}} R, \mathbb{G}_{m,R}) = \mathrm{Hom}(G_n \otimes_{\mathcal{O}} R, \boldsymbol{\mu}_{p^n,R})$$

(the second equality is an easy consequence of the fact that G_n is killed by p^n, so any homomorphism to $\mathbb{G}_n$ lands in $\boldsymbol{\mu}_{p^n}$). Letting $n \to \infty$ gives

$$T_p(G^*) = \varprojlim_n G_n(R) \cong \mathrm{Hom}(G \otimes_{\mathcal{O}} R, \boldsymbol{\mu}_{p^\infty,R}),$$

where the right sides denotes morphism of p-divisible groups over R. By functoriality any map of p-divisible groups induces a map on the points and the tangent spaces, meaning that we have maps of groups

$$\begin{tikzcd}
 & \mathrm{Hom}(G \otimes_{\mathcal{O}} R, \boldsymbol{\mu}_{p^\infty,R}) \arrow[dl] \arrow[dr] & \\
\mathrm{Hom}_{\mathbb{Z}_p}(G(R), \boldsymbol{\mu}_{p^\infty,\mathcal{O}}(R)) & & \mathrm{Hom}_{\mathbb{C}_K}(\mathfrak{t}_G(\mathbb{C}_K)), \mathfrak{t}_{\boldsymbol{\mu}_{p^\infty,\mathcal{O}}}(\mathbb{C}_K))
\end{tikzcd}$$

By evaluating in the usual way (i.e., a map of abelian groups $A \to \mathrm{Hom}(B, C)$ induces $B \to \mathrm{Hom}(A, C)$ by evaluation) we finally arrive at maps of $\mathbb{Z}_p$-modules

$$\alpha : G(R) \to \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), 1 + \mathfrak{m}_R)$$

(which restricts to torsion points) and

$$d\alpha : \mathfrak{t}_G(\mathbb{C}_K) \to \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), \mathbb{C}_K)$$

In conclusion we obtain a commutative diagram of $\mathbb{Z}_p$-modules, with exact rows, where Gal_K acts on everything compatibly:

$$\begin{tikzcd}
0 \arrow[r] & G(R)_{\text{tors}} \arrow[r] \arrow[d, "\alpha_0"'] & G(R) \arrow[r, "\log_G"] \arrow[d, "\alpha"'] & \mathfrak{t}_G(\mathbb{C}_K) \arrow[r] \arrow[d, "d\alpha"'] & 0 \\
0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), \mu_{p^\infty}) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), 1 + \mathfrak{m}_R) \arrow[r, "\log"'] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), \mathbb{C}_K) \arrow[r] & 0
\end{tikzcd}$$

Proposition 8.7. *α_0 is an isomorphism, and α and $d\alpha$ are injective.*

Theorem 8.8. *(i) Taking Gal_K-fixed points, the induced maps*

$$\alpha_{\mathcal{O}} : G(\mathcal{O}) \to \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), 1 + \mathfrak{m}_R)$$

and

$$d\alpha_{\mathcal{O}} : \mathfrak{t}_G(K) \to \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), \mathbb{C}_K)$$

are isomorphisms. (Here $\mathrm{Hom}_{\mathrm{Gal}_K}$ denotes Gal_K-equivariant homomorphisms of $\mathbb{Z}_p$-modules).

(ii) Hodge–Tate decomposition: There is a Gal_K*-equivariant isomorphism of* $\mathbb{C}_K$*-vector spaces*

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_p(G),\mathbb{C}_K)\cong\mathfrak{t}_{G^*}(\mathbb{C}_K)\oplus(\mathfrak{t}_G(\mathbb{C}_K)\otimes_{\mathbb{C}_K}\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1),\mathbb{C}_K))$$

Although the above statement of the Hodge–Tate decomposition is the usual one, it may look nicer to take $\mathbb{C}_K$-duals of it, i.e., $\mathrm{Hom}_{\mathbb{C}_K}(-,\mathbb{C}_K)$ everywhere, and to remember that $\mathfrak{t}(\mathbb{C}_K)=\mathfrak{t}(K)\otimes_K\mathbb{C}_K$, to finally obtain a Gal_K-equivariant isomorphism of $\mathbb{C}_K$-vector spaces

$$T_p(G)\otimes_{\mathbb{Z}_p}\mathbb{C}_K\cong(\mathfrak{t}^*_{G*}(K)\otimes_K\mathbb{C}_K)\oplus(\mathfrak{t}_G(K)\otimes_K\mathbb{C}_K\otimes_{\mathbb{Z}_p}\mathbb{Z}_p(1))$$

where the first term involves the cotangent space of G^*, i.e., $\mathfrak{t}^*_{G^*}(K):=\mathrm{Hom}_K(\mathfrak{t}_{G^*}(K),K)$.

Remark 8.9 (Tate twists)**.** The rank one free $\mathbb{Z}_p$-module

$$T_p(\boldsymbol{\mu}_{p^\infty,\mathcal{O}})=\varprojlim_n\mu_{p^n}$$

(where the transition maps in the inverse system are given by raising to the power of p) is known as a *Tate twist* and denoted by $\mathbb{Z}_p(1)$. A choice of basis element e corresponds to a choice of a sequence of p-power roots of unity $\zeta_p,\zeta_p^2,\dots\in K^{\mathrm{alg}}$.

Although $\mathbb{Z}_p(1)$ is a free $\mathbb{Z}_p$-module of rank one, the action of Gal_K on $\mathbb{Z}_p(1)$ (induced by the actions on each μ_{p^n}) is interesting. Specifically, if we do chose a basis element $e=(\zeta_p,\zeta_{p^2},\dots)$ as above, then the action is given by

$$\sigma(e)=\chi(\sigma)e,$$

where $\chi(\sigma)\in\mathbb{Z}_p^\times$ is the unique p-adic unit satisfying $\sigma(\zeta_{p^r})=\zeta_{p^r}^{\chi(\sigma)}$ for all $r\geq1$. The homomorphism $\chi:\mathrm{Gal}_K\to\mathbb{Z}_p^\times$ is known as the *cyclotomic character.*

One typically writes $\mathbb{Z}_p(-1)=\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1),\mathbb{Z}_p)$ for its dual, which is again a rank one free $\mathbb{Z}_p$-module, on which the action of Gal_K is related to the inverse of the cyclotomic character.

Remark 8.10 (Tate–Sen theory)**.** In the theorem and proposition we need some results of Tate and Sen concerning the action of Gal_K, the absolute Galois group of K, on $\mathbb{C}_K$. The first of these is the surprising hard to prove fact that the only elements of $\mathbb{C}_K$ fixed by the action are the elements of K, i.e., $\mathbb{C}_K^{\mathrm{Gal}_K}=K$. The second is that, on the other hand, $\mathbb{C}\otimes_{\mathbb{Z}_p}\mathbb{Z}_p(1)$ has no non-zero element fixed by Gal_K; more explicitly, using the cyclotomic character of the previous remark, this means that if $x\in\mathbb{C}_K$ satisfies $\sigma(x)=\chi(\sigma)x$ for all $\sigma\in\mathrm{Gal}_K$, then $x=0$.

Proof of Theorem, assuming Proposition. Firstly, we add to the above diagram what we know from the Proposition:

$$\begin{tikzcd}
0 \arrow[r] & G(R)_{\mathrm{tors}} \arrow[r] \arrow[d, "\alpha_0"', "\cong"] & G(R) \arrow[r, "\log_G"] \arrow[d, hook, "\alpha"'] & \mathfrak{t}_G(\mathbb{C}_K) \arrow[r] \arrow[d, hook, "d\alpha"'] & 0 \\
0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*),\mu_{p^\infty}) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*),1+\mathfrak{m}_R) \arrow[r, "\log"'] \arrow[d] & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*),\mathbb{C}_K) \arrow[r] \arrow[d] & 0 \\
 & & \mathrm{coker}\,\alpha \arrow[r, "\cong"] & \mathrm{coker}\,d\alpha &
\end{tikzcd}$$

(The isomorphism between the kernels is a formal consequence, through a diagram chase, of the left vertical isomorphism.) Taking Gal_K-fixed points of the central and vertical columns gives short exact sequences

$$0 \longrightarrow G(\mathcal{O}) \xrightarrow{\alpha_{\mathcal{O}}} \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), 1+\mathfrak{m}_R) \longrightarrow (\operatorname{coker}\alpha)^{\mathrm{Gal}_K}$$

and

$$0 \longrightarrow \mathfrak{t}_G(K) \xrightarrow{d\alpha_{\mathcal{O}}} \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), \mathbb{C}_K) \longrightarrow (\operatorname{coker} d\alpha)^{\mathrm{Gal}_K}$$

It follows that the map

$$\operatorname{coker}\alpha_{\mathcal{O}} \longrightarrow \operatorname{coker} d\alpha_{\mathcal{O}}$$

(induced by the logarithms) is injective. Therefore, for (i), it is enough to show that the injection $d\alpha_{\mathcal{O}}$ is surjective. Since the domain and codomain of $d\alpha_{\mathcal{O}}$ are K-vector spaces of dimensions $\dim G$ and $n^* := \dim_K \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), \mathbb{C}_K)$, we know that $\dim G \leq n^* := \dim_K \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), \mathbb{C}_K)$, and to prove surjectivity it is equivalent to show this is an equality.

But swapping G and G^*, we also know $\dim G^* \leq n := \dim_K \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G), \mathbb{C}_K)$. Since $\dim G + \dim G^* = h$ (quoted in the duality section), it becomes equivalent to show $n + n^* \leq h$, and this is what we will do. The key (also to proving (ii)) will be defining a certain pairing.

We have

$$G_n^*(\mathbb{C}_K) = \mathrm{Hom}(G_n \otimes_{\mathcal{O}} \mathbb{C}_K, \boldsymbol{\mu}_{p^n,\mathbb{C}_K}) = \mathrm{Hom}_{\mathbb{Z}_p}(G_n(\mathbb{C}_K), \mu_{p^n}),$$

where the first equality is by duality, and the second equality is by identifying the category of finite flat group schemes over $\mathbb{C}_K$ with the category of finite abelian groups. Then take limit over n to get a Gal_K-equivariant identification $T_p(G^*) = \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G), \mathbb{Z}_p(1))$, where $\mathbb{Z}_p(1)$ is the rank one free $\mathbb{Z}_p$-module $T_p(\boldsymbol{\mu}_{p^\infty,\mathcal{O}}) = \varprojlim_n \mu_{p^n}$ (i.e., the Tate twist). The same is true swapping G and G^*, which amounts to the statement that we have a perfect pairing between free, rank-h $\mathbb{Z}_p$-modules

$$T_p(G) \times T_p(G^*) \to \mathbb{Z}_p(1)$$

This induces a perfect pairing between h-dimensional $\mathbb{C}_K$-vector spaces

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_p(G), \mathbb{C}_K) \times \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), \mathbb{C}_K) \to \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1), \mathbb{C}_K), \tag{†}$$

and taking Galois invariants induces a pairing

$$\mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G), \mathbb{C}_K) \times \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), \mathbb{C}_K) \to \mathrm{Hom}_{\mathrm{Gal}_K}(\mathbb{Z}_p(1), \mathbb{C}_K) = 0$$

where the vanishing is by the second part of Tate–Sen theory. It follows that

$$\mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G), \mathbb{C}_K) \otimes_K \mathbb{C}_K \qquad \text{and} \qquad \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), \mathbb{C}_K) \otimes_K \mathbb{C}_K$$

are orthogonal under the pairing (†), and hence the sum of their dims is $\leq h$, as required to complete the proof of (i).

It follows that actually $n + n^* = h$, and so the $\mathbb{C}_K$-vector spaces of the previous lines are not merely orthogonal, but even orthogonal complements of each other under pairing (†). This means there is a natural Gal_K-equivariant identification

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_p(G), \mathbb{C}_K)/(\mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G), \mathbb{C}_K) \otimes_K \mathbb{C}_K) \cong \mathrm{Hom}_{\mathrm{Gal}_K}(T_p(G^*), \mathbb{C}_K) \otimes_K \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1), \mathbb{C}_K)$$

By the isomorphisms of (i), this may be rewritten as

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_p(G),\mathbb{C}_K)/\mathfrak{t}_G(\mathbb{C}_K)\cong\mathfrak{t}_{G^*}(\mathbb{C}_K)\otimes_{\mathbb{C}_K}\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1),\mathbb{C}_K)$$

All that remains in (ii) is to show that this description of $\mathrm{Hom}_{\mathbb{Z}_p}(T_p(G),\mathbb{C}_K)$ admits a Gal_K-equivariant splitting. Unfortunately this is another piece of Tate–Sen theory which we must skip. (The idea is that the Gal_K-actions on $\mathfrak{t}_G(\mathbb{C}_K)$ and the right side are too incompatible for their extension $\mathrm{Hom}_{\mathbb{Z}_p}(T_p(G),\mathbb{C}_K)$ to not be split.) □

Proof of Proposition. Step 1: α_0 is an isomorphism. As we already pointed out in the proof of the theorem, we have $G(\mathbb{C}_K)=\mathrm{Hom}_{\mathbb{Z}_p}(G_n^*(\mathbb{C}_K),\mu_{p^n})$; taking the limit over n (in a different direction to the previous theorem) yields an isomorphism

$$G(R)_{\mathrm{tors}}=\varinjlim_n G_n(\mathbb{C}_K)\xrightarrow{\simeq}\mathrm{Hom}_{\mathbb{Z}_p}(\varprojlim_n G_n^*(\mathbb{C}_K),\mu_{p^n})=\mathrm{Hom}_{\mathbb{Z}_p}(T_p(G_n^*),\mu_{p^n})$$

(where the equalities follow from the lemma and corollary at the start of the section).

Step 2: The kernel and cokernel of α are $\mathbb{Q}_p$-vector spaces (a priori they are only $\mathbb{Z}_p$-modules). Indeed, by Step 1 it follows by the snake lemma, or a similar diagram chase, that the maps $\mathrm{Ker}\,\alpha\to\mathrm{Ker}\,d\alpha$ and $\mathrm{coker}\,\alpha\to\mathrm{coker}\,d\alpha$, induced by the logarithm, are isomorphisms of $\mathbb{Z}_p$-modules. Since $d\alpha$ is a map between $\mathbb{Q}_p$-vector spaces, it follows that its kernel and cokernel are $\mathbb{Q}_p$-vector spaces.

Step 3: $G(R)^{\mathrm{Gal}_K}=G(\mathcal{O})$ (which was already implicitly used in the theorem). From the short exact sequence of Proposition 6.5, it is enough to prove this separately for G° and $G^{\text{ét}}$. In the first case, we have

$$G^\circ(R)^{\mathrm{Gal}_K}=\mathrm{ContHom}(\mathcal{A}^\circ,R)^{\mathrm{Gal}_K}=\mathrm{ContHom}(\mathcal{A}^\circ,R^{\mathrm{Gal}_K})=\mathrm{ContHom}(\mathcal{A}^\circ,\mathcal{O}),$$

where the middle equality is tautological, but the second equality if a consequence of Tate–Sen theory stating that $\mathbb{C}_K^{\mathrm{Gal}_K}=K$ (and so, restricting to elements of absolute value ≤ 1, we have $R^{\mathrm{Gal}_K}=\mathcal{O}$). Next, in the étale case, we use Lemma 6.3 to write $G^{\text{ét}}(R)=\varinjlim_n G_n(k^{\mathrm{alg}})$ and $G^{\text{ét}}(\mathcal{O})=\varinjlim_n G_n(k)$, where $k^{\mathrm{alg}}=R/\mathfrak{m}_R$ is an algebraic closure of $k=\mathcal{O}/\mathfrak{m}$. But for each group scheme $H=G_n$ over $\mathcal{O}$, we have $H(k^{\mathrm{alg}})^{\mathrm{Gal}_K}=H((k^{\mathrm{alg}})^{\mathrm{Gal}_K})=H(k)$, from which the result follows.

Step 3.5: $\mathfrak{t}_G(\mathbb{C}_K)^{\mathrm{Gal}_K}=\mathfrak{t}_G(K)$. By the same argument as Step 3.

Step 4: α is injective on $G(\mathcal{O})$. Since $G(\mathcal{O})=G(R)^{\mathrm{Gal}_K}$, the kernel of α restricted to $G(\mathcal{O})$ is $(\mathrm{Ker}\,\alpha)^{\mathrm{Gal}_K}$, which is a $\mathbb{Q}_p$-vector space. By decomposing G into its connected and étale piece (this reduction to the connected and étale pieces is not entirely trivial: it uses the fact that $T_p(G^{\circ *})\twoheadrightarrow T_p(G^*)$), it is sufficient to show that the $\mathbb{Z}_p$-modules $G^\circ(\mathcal{O})$ and $G^{\text{ét}}(\mathcal{O})$ contain no non-zero $\mathbb{Q}_p$-vector spaces. This is easy for $G^{\text{ét}}(\mathcal{O})$ since it is torsion by Lemma 6.3. On the other hand $G^\circ(\mathcal{O})=\mathrm{ContHom}(\mathcal{A}^\circ,\mathcal{O})$: by the same filtration argument as used when proving convergence of the logarithm, we see by an easy induction that if $f:\mathcal{A}^\circ\to\mathcal{O}$ is any function, then $([p]^r f)(I)\subseteq\mathfrak{m}^r$; thus an element f of $G^\circ(R)$ which is infinitely p-divisible sends I to $\bigcup_{r\ge1}\mathfrak{m}^r=0$, and so f is the zero element of $G^\circ(R)$.

Step 5: The restriction of $d\alpha$ to $\mathfrak{t}_G(K)\subseteq\mathfrak{t}_G(\mathbb{C}_K)$ is injective. From Step 4 it follows (using Step 1 to make a diagram chase) that $d\alpha$ is injective on the $\mathbb{Z}_p$-submodule $\log_G(G(\mathcal{O}))\subseteq\mathfrak{t}_G(\mathbb{C}_K)$, therefore also injective on the $\mathbb{Q}_p$-vector subspace it generates; but this $\mathbb{Q}_p$-vector subspace is exactly $\mathfrak{t}_G(K)$ (by an easy modification of the proof of Corollary 8.5(ii)).

Step 6: $d\alpha$ is injective. We factor the map as

$$\mathfrak{t}_G(\mathbb{C}_K) = \mathfrak{t}_K(K) \otimes_K \mathbb{C}_K \to \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), \mathbb{C}_K)^{\mathrm{Gal}_K} \otimes_K \mathbb{C}_K \to \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^*), \mathbb{C}_K),$$

where the first arrow is injective by Step 5. The second arrow is injective by the general linear algebra result.

Step 7: α is injective. As noted in Step 2, we have $\operatorname{Ker}\alpha \xrightarrow{\cong} \operatorname{Ker} d\alpha$, which we have just shown is zero. □