LECTURES ON p-DIVISIBLE GROUP

THOMAS ZINK

1. Formal Groups and p-Divisible Groups

Let R be a commutative ring with unit. Let $\mathbf{Nil}_R$ be the category of nilpotent R-algebras. Let $F_i \in R[[X_1, \ldots, X_n, Y_1, \ldots, Y_n]], 1 \leq i \leq n$, be formal power series in $2n$ variables. Take $N \in \mathbf{Nil}_R$. Let $N^{(n)} = N \oplus \cdots \oplus N$ be the direct sum of n copies of N. Given $\underline{x} = (x_1, \ldots, x_n), \underline{y} = (y_1, \ldots, y_n) \in N^{(n)}$, the finite sum

$$F_i(\underline{x}, \underline{y}) = F_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

is a well-defined element of N. Consider the map defined by the n-tuple F,

$$+_F : N^{(n)} \times N^{(n)} \to N^{(n)},$$

$$(\underline{x}, \underline{y}) \mapsto (F_1(\underline{x}, \underline{y}), \ldots, F_n(\underline{x}, \underline{y}))$$

Now suppose $+_F$ is a group law for each $N \in \mathbf{Nil}_R$, with neutral element $\underline{0} = (0, \ldots, 0)$. Then $\underline{0} + \underline{0} = \underline{0}$ implies that $F_i(\underline{0}, \underline{0}) = 0$, so F_i has no constant terms for any i. In this case, the n-tuple $F = (F_i)$ can be considered as a functor

$$\mathbf{Nil}_R \longrightarrow \mathbf{Groups},$$

$$N \mapsto (N^{(n)}, +_F).$$

The composition of F with the forgetful functor $\mathbf{Groups} \to \mathbf{Sets}$ is the functor

$$\mathbf{Nil}_R \to \mathbf{Sets},$$

$$N \mapsto N^{(n)}.$$

This functor will be denoted by $\hat{\mathbb{A}}^n$, i.e.,

$$\hat{\mathbb{A}}^n(N) = N^{(n)}$$

for $N \in \mathbf{Nil}_R$.

Next, we consider how to define a morphism of functors $\hat{\mathbb{A}}^m \to \hat{\mathbb{A}}^m$.

Example: Given $F_i(X_1, \ldots, X_n) \in R[[X_1, \ldots, X_n]], 1 \leq i \leq m$, then

$$\Psi_N : N^n \to N^m \quad N \in \mathbf{Nil}_R,$$

$$\underline{x} \mapsto (F_1(\underline{x}), \ldots, F_m(\underline{x}))$$

defines a morphism $\hat{\mathbb{A}}^n \to \hat{\mathbb{A}}^m$ of functors. Conversely, we have

Proposition 1.1. *Suppose we are given a morphism of functors $\Phi : \hat{\mathbb{A}}^n \to \hat{\mathbb{A}}^m$. Then there are formal power series $F_i \in R[[X_1, \ldots, X_n]], 1 \leq i \leq m$, such that for any $N \in \mathbf{Nil}_R$, the homomorphism $\Phi_N : N^m \to N^n$ is defined by*

$$(x_1, \ldots, x_n) \mapsto (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)).$$

Proof. In $R[[X_1,\dots,X_n]]$, consider the nilpotent algebra

$$N_t = \langle X_1,\dots,X_n\rangle / \langle X_1,\dots,X_n\rangle^t.$$

Then Φ defines

$$\Phi_{N_t} : N_t^{(n)} \to N_t^{(m)}.$$

The homomorphism Φ_{N_t} is determined by

$$\Phi_{N_t}(X_1,\dots,X_n) = (F_1[t],\dots,F_m[t]) \in N_t^{(m)}.$$

If Φ is a morphism of functors, we have the commutative diagram

$$\begin{tikzcd} N_{t+1}^{(n)} \arrow[r, "\Phi_{N_{t+1}}"] \arrow[d] & N_{t+1}^{(m)} \arrow[d] \\ N_t^{(n)} \arrow[r, "\Phi_{N_t}"'] & N_t^{(m)} \end{tikzcd}$$

So there are formal power series $F = (F_i; 1 \le i \le m)$ with $F_i \bmod \deg t = F_i[t]$.

By construction the proposition holds for $N = N_t$. So it is easy to see that the proposition is true for any $N \in \mathbf{Nil}_R$ of the form $N = \oplus_i N_{t_i}$. For any finitely generated nilpotent R-algebra, there is a surjective homomorphism $\oplus_i N_{t_i} \twoheadrightarrow N$. It is easy to see Φ_N is of the given form. Any $N \in \mathbf{Nil}_R$ is a union of finitely generated nilpotent algebras. We are done. □

Thus a morphism of functors $\Phi : \hat{\mathbb{A}}^n \to \hat{\mathbb{A}}^m$ is given by power series. It is an analogue of the fact that the morphism between affine schemes is given by polynomials.

Definition 1.2. *A* ***formal group law*** *is a functor*

$$G : \mathbf{Nil}_R \to \mathbf{Groups}$$

*such that $F \circ G \cong \hat{\mathbb{A}}^n$, where F : **Groups** → **Sets** is the forgetful functor.*

Example: (1) $\hat{\mathbb{G}}_a$, the additive formal group law, is defined by $\hat{\mathbb{G}}_a(N) = (N, +)$.
(2) Let $N \in \mathbf{Nil}_R$. We define a commutative algebra structure on $R \oplus N$ by defining the multiplication by $(r_1, n_1)(r_2, n_2) = (r_1 r_2, r_1 n_2 + r_2 n_1 + n_1 n_2)$. We define the multiplicative formal group law $\hat{\mathbb{G}}_m$ by

$$\hat{\mathbb{G}}_m(N) = (1+N)^\times \subset R \oplus N.$$

Here $(1+N)^\times$ means elements in $R \oplus N$ of the form $1+x, x \in N$ with multiplicative law. As a functor with values in **Sets**, it is clear that $\hat{\mathbb{G}}_m \cong \hat{\mathbb{A}}^1$.

From now on we only consider commutative formal group law. We use **Ab** to denote the category of abelian groups.

Definition 1.3. *A functor*

$$H : \mathbf{Nil}_R \longrightarrow \mathbf{Ab}$$

is called a ***formal group*** *if*
(i) *H is exact, i.e., if $0 \to N_1 \to N_2 \to N_3 \to 0$ is an exact sequence in $\mathbf{Nil}_R$, then*

$$0 \to H(N_1) \to H(N_2) \to H(N_3) \to 0$$

is an exact sequence in **Ab**.
(ii) *If $N \in \mathbf{Nil}_R$ and $N = \cup_{i\in I} N_i$, where N_i are sub-algebras of N and I is a filtered set, (i.e., given any N_i, N_j for $i, j \in I$, there is an $r \in I$ such that $N_i \hookrightarrow N_r, N_j \hookrightarrow N_r$,) then $H(N) = \cup_{i\in I} H(N_i)$.*

As a first example of formal groups, we want to show that given a commutative smooth algebraic group G over R, we can associate to it a formal group. As a preparation, recall the notion of smoothness. There are various equivalent definitions of smoothness. Here we only remark that *smoothness* is equivalent to finite presentation plus formal smoothness. Recall that a morphism between schemes $f : X \to Y$ is called *formally smooth* if for any exact sequence

$$0 \to I \to A \to B \to 0,$$

where A, B are commutative rings over Y (i.e., Spec$A$ and Spec$B$ are schemes over Y) with 1, and I is a *nilpotent* ideal of A, the natural map $X_Y(A) \to X_Y(B)$ is surjective. Here $X_Y(A) = \mathrm{Hom}_Y(\mathrm{Spec}A, X)$.

Lemma 1.4. *Let X be a scheme over R. Let $A_i, i = 1, 2, 3$ be rings over R. Let $\alpha : A_1 \to A_3$ be a surjective homomorphism with nilpotent kernel* Kerα*, and let $\beta : A_2 \to A_3$ be a homomorphism. Form the fiber product $A_1 \times_{A_3} A_2$. Write $X(A) = \mathrm{Hom}_{\mathrm{Spec}R}(\mathrm{Spec}A, X)$ for any R-algebra A. Then we have a bijection*

$$X(A_1) \times_{X(A_3)} X(A_2) \cong X(A_1 \times_{A_3} A_2).$$

Proof. By the universal property of the fiber product, there is a map

$$\Phi : X(A_1 \times_{A_3} A_2) \to X(A_1) \times_{X(A_3)} X(A_2).$$

To show it is a bijection, we first consider the case when $X = \mathrm{Spec}B$ is affine. Then $X(A_i) = \mathrm{Hom}_R(B, A_i)$. We aim to define the inverse map of Φ. Given $(a_1, a_2) \in X(A_1) \times_{X(A_3)} X(A_2) = \mathrm{Hom}(B, A_1) \times_{\mathrm{Hom}(B,A_3)} \mathrm{Hom}(B, A_2)$, which means that we have maps $a_i : B \to A_i$ such that $\alpha a_1 = \beta a_2$, by the universal property of the fiber product again, we define a map $b : B \to A_1 \times_{A_3} A_2$. Define $\Psi((a_1, a_2)) = b$. It is easy to see that Ψ is the inverse of Φ.

Now consider the general case. Since Kerα is nilpotent, Spec$A_1 \cong$ SpecA_3 as a topological space. Hence $\mathrm{Spec}(A_1 \times_{A_3} A_2) \cong \mathrm{Spec}A_2$ as a topological space. Given $(a_1, a_2) \in X(A_1) \times_{X(A_3)} X(A_2)$, for any $x \in \mathrm{Spec}A_2$, there is a basic open affine neighborhood $\mathrm{Spec}(A_2)_f$ of x such that $a_2(\mathrm{Spec}(A_2)_f)$ is contained in an open affine U of X. Since $\alpha : A_1 \to A_3$ is surjective, we can take $g \in A_1$ such that $\alpha(g) = \beta(f) \in A_3$. Then by the affine case considered above there is a morphism

$$b_f : \mathrm{Spec}[(A_1)_g \times_{(A_3)_{\alpha(g)}} (A_2)_f] \to U \to X.$$

Since $\mathrm{Spec}(A_1 \times_{A_3} A_2) \cong \mathrm{Spec}A_2$ as a topological space, when f ranges over a set in A_2 such that $\mathrm{Spec}(A_2)_f$ form a cover of SpecA_2, then $\mathrm{Spec}[(A_1)_g \times_{(A_3)_{\alpha(g)}} (A_2)_f]$ form a cover of $\mathrm{Spec}(A_1 \times_{A_3} A_2)$. So we can glue b_f to get a morphism $b : \mathrm{Spec}(A_1 \times_{A_3} A_2) \to X$. Now define $\Psi((a_1, a_2)) = b$. One can check that Ψ is the inverse of Φ. □

Proposition 1.5. *Now let G be a commutative smooth group scheme over R. We define a functor $\hat{G} : \mathbf{Nil}_R \to \mathbf{Ab}$, named the **completion** of G along the unit, by*

$$\hat{G}(N) = \mathrm{Ker}(G(R \oplus N) \to G(R)).$$

Here $R \oplus N$ is endowed with the commutative ring structure $(r_1, n_1) \cdot (r_2, n_2) = (r_1r_2, r_1n_2 + r_2n_1 + n_1n_2)$, and $R \oplus N \to R$ is the map sending N to 0. The map $G(R \oplus N) \to G(R)$ is induced by the $R \oplus N \to R$. Then the functor $\hat{G}$ is a formal group.

Proof. We first show that $\hat{G}$ is an exact functor. Let

$$\begin{tikzcd} 0 \arrow[r] & N_1 \arrow[r, "f"] & N_2 \arrow[r, "g"] & N_3 \arrow[r] & 0 \end{tikzcd}$$

be an exact sequence of nilpotent algebras. Let $A_i = R \oplus N_i$. We have the natural homomorphisms $A_1 \xrightarrow{f} A_2 \xrightarrow{g} A_3 \xrightarrow{\phi} R$ of commutative R-algebras. Since $g : N_2 \to N_3$ is surjective, so is $g : A_2 \to A_3$. The algebra $\mathrm{Ker}(A_2 \to A_3) = N_1$ is nilpotent. We check

$$\begin{tikzcd} A_1 \arrow[r, "\phi"] \arrow[d, "f"'] & R \arrow[d, "\psi"'] \\ A_2 \arrow[r, "g"'] & A_3 \end{tikzcd}$$

is a fiber product. Here ψ is the structure map, i.e., $\psi(r) = (r, 0)$ and $\phi : A_1 = R \oplus N_1 \to R$ is the natural projection. First the diagram is commutative, since $gf(r, n) = g(r, f(n)) = (r, gf(n)) = (r, 0) = \psi\phi(r, n)$. If $(r, n) \in A_2, r' \in R$ with $g(r, n) = \psi(r')$, i.e., $(r, g(n)) = (r', 0)$, then $r = r', g(n) = 0$, so there is $n_1 \in N_1$ such that $n = f(n_1)$, so we have $(r, n) = f(r, n_1), r = \phi(r, n_1)$. This shows $A_1 \cong A_2 \times_{A_3} R$.

Now we can use Lemma 1.3. Hence we get

$$G(A_1) \cong G(A_2) \times_{G(A_3)} G(R).$$

So we have the following exact sequences

$$\begin{tikzcd} 0 \arrow[r] & G(A_1) \arrow[r] \arrow[d] & G(A_2) \oplus G(R) \arrow[r] \arrow[d] & G(A_3) \arrow[d] & \\ 0 \arrow[r] & G(R) \arrow[r] & G(R) \oplus G(R) \arrow[r] & G(R) \arrow[r] & 0 \end{tikzcd}$$

Then by the snake lemma we have that the sequence of kernels

$$0 \to \hat{G}(N_1) \to \hat{G}(N_2) \to \hat{G}(N_3)$$

is exact. To show the surjectivity of $\hat{G}(N_2) \to \hat{G}(N_3)$ we use the formal smoothness of G. In fact, the formal smoothness of G shows that $G(A_2) \to G(A_3)$ is surjective, then it is easy to see $\hat{G}(N_2) \to \hat{G}(N_3)$ is surjective.

Next we have to show that if $N = \cup_{i \in I} N_i$ is a filtered union, then $\hat{G}(N) = \cup_{i \in I} \hat{G}(N_i)$. If $G = \mathrm{Spec}B$ is affine, then the smoothness of G implies that B is of finite type over R. In this case, we claim that

$$\mathrm{Spec}B(A) = \varinjlim \mathrm{Spec}B(A_i)$$

where $A = R \oplus N$, and $A_i = R \oplus N_i$. In fact, we can write $B = R[X_1, \ldots, X_n]/\mathfrak{a}$, and for $f \in \mathrm{Spec}B(A) = \mathrm{Hom}(B, A)$, f is determined by $a_j = f(x_j) \in A$, where $x_j = X_j + \mathfrak{a}$. Since A_i is filtered, there is an $i \in I$ such that $a_j \in A_i$ for all j, hence the claim. This shows that $\hat{G}(N) = \cup_{i\in I}\hat{G}(N_i)$ if G is affine. For general G, we can reduce it to the affine case. This completes the proof of the proposition. □

Definition 1.6. *A functor $H : \mathbf{Nil}_R \to \mathbf{Sets}$ is called **left exact** if*
(i) $H(0) = \{0\}$*, where* $\{0\}$ *is a given set with one element.*
(ii) H *respects fiber products, i.e., given a fiber product*

$$\begin{tikzcd}
N_1 \times_{N_3} N_2 \arrow[r] \arrow[d] & N_1 \arrow[d] \\
N_2 \arrow[r, "g"'] & N_3
\end{tikzcd}$$

we have $H(N_1 \times_{N_3} N_2) \cong H(N_1) \times_{H(N_3)} H(N_2)$.

Proposition 1.7. *A formal group H is left exact.*

We omit the proof, and just remark that the condition (i) of left exactness of a formal group H follows from the fact that H is an exact functor.

Example. Let X be a scheme over R and $\xi \in X(R)$. Consider the functor $\hat{X} : \mathbf{Nil}_R \to \mathbf{Sets}$

$$\hat{X}(N) = \mathrm{Fiber}_\xi[X(R \oplus N) \to X(R)].$$

The functor $\hat{X}$ is called the **completion** of X along ξ. Then $\hat{X}$ is left exact.

Corollary 1.8. *A formal group H respects fiber products. In particular, we have*

$$H(N_1 \times N_2) \cong H(N_1) \times H(N_2).$$

Next, we turn to another construction.

Let H be a functor $\mathbf{Nil}_R \to \mathbf{Ab}$ such that

$$H(N_1 \times N_2) \cong H(N_1) \times H(N_2) \tag{1.1}$$

for any $N_1, N_2 \in \mathbf{Nil}_R$. A formal group H is such a functor, as we have seen.

Proposition 1.9. *For a functor H satisfying* (1.1)*, there is an R-module structure on $H(N)$ for any $N \in \mathbf{Nil}_R$ with $N^2 = 0$.*

Proof. If $N \in \mathbf{Nil}_R$ and $N^2 = 0$, the addition map $+ : N \oplus N \to N$, which sends (n_1, n_2) to $n_1 + n_2$ (addition law of the algebra structure of N) is a morphism of algebras. Let H be a functor satisfying (1.1). Apply H to the morphism $+$. We get a homomorphism $H(+) : H(N \oplus N) \to H(N)$. By Eq.(1.1) we have $H(N) \times H(N) \cong H(N \oplus N)$. So we have a homomorphism

$$H(N) \times H(N) \to H(N).$$

We can check that this construction gives an abelian group structure on $H(N)$ ($H(N)$ has another abelian group structure as an object of $\mathbf{Ab}$. Later we shall see that the two abelian group structures are the same). The zero element is just $H(0)$.

Next we show that there is an inverse for any $x \in H(N)$. Let $f : N \to N \oplus N$ be the map $f(n) = (n, -n)$. Then f is also a homomorphism of algebras, so we have commutative diagrams

$$\begin{tikzcd}
N \arrow[r, "f"] \arrow[d] & N \oplus N \arrow[d, "+"] \\
0 \arrow[r] & N
\end{tikzcd}
\qquad
\begin{tikzcd}
H(N) \arrow[r, "H(f)"] \arrow[d] & H(N) \times H(N) \arrow[r, "H(p_1)"] \arrow[d] & H(N) \\
H(0) \arrow[r] & H(N) &
\end{tikzcd}$$

where p_1 is the projection $N \times N \to N$ to the first factor. Given $x \in H(N)$, since $H(p_1)H(f) = H(p_1 f) = \mathrm{id}$, we have $H(f)(x) = (x, y)$ for some $y \in H(N)$. It is easy to see that $x + y = 0$.

Let $\lambda \in R$. Then $n \mapsto \lambda n$ induces an algebra homomorphism of N to N. Apply the functor H to get $\lambda : H(N) \to H(N)$. It is not hard to see that these constructions endow $H(N)$ with an R-module structure. □

Definition 1.10. *Let H be a functor satisfying* (1.1). *For any R-module M, we define $M_v \in \mathbf{Nil}_R$ (v stands for vector group) by $M_v = M$ as an abelian group and $M_v^2 = 0$. We define the **tangent functor** t_H of H by*

$$t_H : \mathbf{Mod}_R \to \mathbf{Mod}_R$$

$$M \mapsto H(M_v).$$

Example: Let $(A, \mathfrak{m}, k)$ be a local ring. Let $H : \mathbf{Nil}_k \to \mathbf{Ab}$ be the functor $H(N) = \mathrm{Hom}(\mathfrak{m}, N)$. Then it is not hard to see that $t_H(k) = \mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2, k_v)$, which is the tangent space of Spec$A$ at the closed point. This justifies the name "tangent functor".

For any $M \in \mathbf{Mod}_R, m \in M$, put $c_m : R \to M$ for the map $c_m(a) = am$ and consider the map

$$t_H(R) \otimes_R M \to t_H(M) \tag{1.2}$$

$$\xi \otimes m \mapsto t_H(c_m)(\xi).$$

Lemma 1.11. *If t_H is right exact and commutes with direct sums, then the map* (1.2) *is an isomorphism.*

Proof. If $M = R$, the isomorphism is trivial. If $M = R^{(I)}$ is a free R-module, the isomorphism is also clear, since both sides commute with direct sum. For the general case, M admits a presentation

$$R^{(J)} \to R^{(I)} \to M \to 0.$$

So we have

$$\begin{tikzcd}
t_H(R) \otimes R^{(J)} \arrow[r] \arrow[d] & t_H(R) \otimes R^{(I)} \arrow[r] \arrow[d] & t_H(R) \otimes M \arrow[r] \arrow[d] & 0 \\
t_H(R^{(J)}) \arrow[r] & t_H(R^{(I)}) \arrow[r] & t_H(M) \arrow[r] & 0
\end{tikzcd}$$

Since the first two vertical arrows are isomorphisms by the above discussion, so is the one on the right. □

Lemma 1.12. *Let H be a formal group. Let $N_i \in \mathbf{Nil}_R, i \in I$. Assume there is $t \in \mathbb{N}^+$ such that $N_i^t = 0$ for all $i \in I$. Then $N = \oplus_{i\in I} N_i \in \mathbf{Nil}_R$. Hence $H(N)$ is well-defined. We have*

$$H(\oplus_{i\in I} N_i) \cong \oplus_{i\in I} H(N_i).$$

Proof. The map $\oplus_{i\in I} N_i \to N_i$ induces $H(\oplus_{i\in I} N_i) \to H(N_i)$, so we have a natural map

$$H(\oplus_{i\in I} N_i) \to \prod_{i\in I} H(N_i).$$

We want to show that this map induces an isomorphism $H(\oplus_{i\in I} N_i) \to \oplus_{i\in I} H(N_i)$. If $|I| = 2$, this is Corollary 1.7. By induction, we know this is an isomorphism for any finite set I. For general I, let J be a finite subset of I. We have an isomorphism $H(\oplus_{i\in J} N_i) \cong \oplus_{i\in J} H(N_i)$. Since

$$H(\oplus_{i\in I} N_i) = H(\cup_J \oplus_{j\in J} N_j) = \cup_J H(\oplus_{j\in J} N_j),$$

the lemma follows. □

Since a formal group H is exact, t_H satisfies the condition of Lemma 1.11. We get

Corollary 1.13. *Let H be a formal group. Then we have the isomorphism* (1.2)

$$t_H(R) \otimes_R M \to t_H(M).$$

In particular, since t_H is exact, $t_H(R)$ is a flat R-module.

Now we turn to the relations between the two notions: the formal group law defined in Lecture 1, and the formal group defined in Lecture 2.

Theorem 1.14. *Let H be a formal group. If $t_H(R)$ is a finitely generated free R-module, then H is a formal group law defined in Lecture 1. More precisely, if $t_H(R) \cong R^d$, then $H \cong \hat{\mathbb{A}}^d$ as functors with values in* **Sets***.*

The aim of this lecture is to prove Theorem 1.14.
We begin with some general remarks.

Let $\mathcal{C}$ be a category, N is an object in $\mathcal{C}$. We define a functor

$$h_N : \mathcal{C} \longrightarrow \mathbf{Sets}$$

by $h_N(M) = \mathrm{Hom}(N, M)$. Let $F : \mathcal{C} \to \mathbf{Sets}$ be any other functor. We have a natural map

$$Y : \mathrm{Hom}(h_N, F) \to F(N),$$

which is defined as follows. Given $\Phi : h_N \to F$, then Φ_N is a morphism $h_N(N) = \mathrm{Hom}(N, N) \to F(N)$. Define $Y(\Phi) = \Phi_N(\mathrm{id}_N)$.

Lemma 1.15 (Yoneda's Lemma)**.** *The map Y is a bijection.*

Proof. In fact, we can construct the inverse map of Y as follows. Given $\alpha \in F(N)$, we need to construct a map $\Phi_M : h_N(M) \to F(M)$ for any object M in $\mathcal{C}$. Given $f : N \to M$, define $\Phi_M(f) = F(f)(\alpha)$. It is not hard to see this gives an inverse of Y. □

Definition 1.16. *Let G be a group, which acts on a set M. The set M is called a **principal homogeneous space** over G, if the map*

$$G \times M \longrightarrow M \times M$$
$$(g, m) \mapsto (gm, m)$$

is bijective.

The case of $M = \emptyset$ is possible. Let $\phi : M_1 \to M_2$ be a G-morphism of principal homogeneous space over G. Then ϕ is bijective if and only if $M_1 \neq \emptyset$.

Definition 1.17. *A **small surjection** is a surjective map $\alpha : M \twoheadrightarrow N$ in the category $\mathbf{Nil}_R$ such that* $\mathrm{Ker}\alpha \cdot M = 0$*.*

Let $M \to N$ be a small surjection with kernel K. Then $+ : K \oplus M \to M$ is a homomorphism in $\mathbf{Nil}_R$, and

$$\begin{tikzcd}
K \oplus M \arrow[r, "+"] \arrow[d, "\mathrm{p}_2"'] & M \arrow[d] \\
M \arrow[r] & N
\end{tikzcd}$$

is a fiber product. Let $G : \mathbf{Nil}_R \to \mathbf{Ab}$ be a left exact functor, so G respect the fiber product. We can apply G to the above fiber product to get

$$\begin{tikzcd}
G(K) \oplus G(M) \arrow[r, "G(+)"] \arrow[d, "\mathrm{p}_2"'] & G(M) \arrow[d] \\
G(M) \arrow[r] & G(N)
\end{tikzcd}$$

For $\eta \in G(N)$, put

$$G_\eta(M) = \text{ Fiber}_\eta[G(M) \to G(N)].$$

Then $G(K) \times G_\eta(M) \cong G_\eta(M) \times G_\eta(M)$, i.e., $G_\eta(M)$ is a principal homogeneous $G(K)$-space.

Lemma 1.18 (Jacobi Inversion Theorem)**.** *Let $F, H : \mathbf{Nil}_R \to$ **Sets** be two left exact functors, and $\alpha : F \to H$ a natural transformation. Assume*
(i) *α induces an isomorphism of the tangent functors, i.e.,*

$$\alpha_N : F(N) \to H(N)$$

is bijective for any $N \in \mathbf{Nil}_R$ with $N^2 = 0$;
(ii) *F is smooth, i.e., for any $M \to N$ surjective, $F(M) \to F(N)$ is also surjective. Then F is an isomorphism of functors.*

Remark: In the Jacobi Inversion Theorem, take $F = H = \hat{\mathbb{A}}^d$. These two functors are left exact. Let $\alpha = (F_1, \ldots, F_d)$, where F_i are formal power series. Then on the tangent spaces, the map

$$R^d = \hat{\mathbb{A}}^d(R_v) \longrightarrow \hat{\mathbb{A}}^d(R_v) = R^d$$

is defined by the Jacobian matrix $\mathrm{Jac}(F_1, \ldots, F_d) = (\frac{\partial F_i}{\partial X_j})$. The Jacobi Inversion Theorem says that if $\mathrm{Jac}(F_1, \ldots, F_d)$ is invertible, so is $\alpha = (F_1, \ldots, F_d)$. This is an analogue of the Jacobi Inversion Theorem in calculus.

Proof of Lemma 1.18. Let $0 \to K \to M \to N \to 0$ be a small surjection in $\mathbf{Nil}_R$.

Claim: if α_N is a bijection, then α_M is a bijection, in the diagram

$$\begin{tikzcd} F(M) \arrow[r] \arrow[d, "\alpha_M"'] & F(N) \arrow[d, "\alpha_N"] \\ H(M) \arrow[r] & H(N) \end{tikzcd}$$

Let $\xi \in F(N), \eta = \alpha_N(\xi) \in H(N)$. By assumption (ii), each of the maps $F(M) \to F(N)$ and $H(M) \to H(N)$ is surjective. Since α_N is bijective, it suffice to show $F_\xi(M) \to H_\eta(N)$ is bijective for any $\xi \in F(N)$. Because $K^2 \subset K \cdot M = 0$, and by (i), we see $F(K) \cong H(K)$. Denote this group by G. By the remark before Lemma (1.18), we see that both $F_\xi(M)$ and $H_\eta(M)$ are principal homogeneous G-spaces. Since $F_\xi(M) \neq \emptyset$ by assumption (ii), we see $F_\xi(M) \to H_\eta(M)$ is bijective. The claim follows.

Now let N be any object in $\mathbf{Nil}_R$. Then there is an n such that $N^n = 0$. So we have the small surjections

$$0 \to N^{n-1} \to N \to N/N^{n-1} \to 0,$$
$$0 \to N^{n-2}/N^{n-1} \to N/N^{n-1} \to N/N^{n-2} \to 0,$$
$$\cdots$$
$$0 \to N^2/N^3 \to N/N^3 \to N/N^2 \to 0$$

and $(N/N^2)^2 = 0$. So α_{N/N^2} is bijective. By induction, we get the lemma. □

Now we are ready to prove Theorem 1.14.

Proof of Theorem 1.14. For any $M \in \mathbf{Mod}_R$ we have

$$H(M_v) \cong t_H(R) \otimes_R M \cong \mathrm{Hom}_R(t_H(R)^\vee, M), \tag{1.3}$$

where $t_H(R)^\vee$ is the dual module of $t_H(R)$. Write $T = t_H(R)^\vee$. Let η_1 be the element of $H(T_v)$ corresponding to id_T in the isomorphism (1.3). By Yoneda's Lemma, $\mathrm{Hom}(h_{T_v}, H) \cong H(T_v)$. Hence η_1 induces a natural transformation $h_{T_v} \to H$. Moreover (1.3) shows that, if $N \in \mathbf{Nil}_R$ with $N^2 = 0$ then $h_{T_v}(N) \to H(N)$ is bijective (just take $N = M_v$ for some $M \in \mathbf{Mod}_R$).

Now in $\mathcal{S}[X] = R[X_1, \ldots, X_d]$, let $\mathcal{S}[X]^+ = (X_1, \ldots, X_d)$ be the ideal generated by $X_1, \ldots, X_d$. Take

$$T_n = \mathcal{S}[X]^+/(\mathcal{S}[X]^+)^{n+1}.$$

The freeness of $t_H(R)$ shows that $T_1 \cong T$ as an R-module. Since H is exact, we have surjective morphisms

$$H(T_{i+1}) \to H(T_i).$$

So we can lift $\eta \in H(T_1)$ to $\eta_i \in H(T_i)$, such that $\eta_{i+1} \mapsto \eta_i$ under the surjection $H(T_{i+1}) \to H(T_i)$. Yoneda's Lemma gives $\eta_i : h_{T_i} \to H$, and $\{\eta_i\}$ forms an inductive system by our construction (note that the functor $T \mapsto h_T$ is contravariant). Define

$$F = \varinjlim h_{T_i},$$

and

$$\eta = \varinjlim \eta_i : F \longrightarrow H.$$

Next we check that $F \cong \hat{\mathbb{A}}^d$. For any $N \in \mathbf{Nil}_R$, it is easy to see that

$$\operatorname{Hom}(T_i, N) = \left\{(n_1, \ldots, n_d) \in N | n_1^{k_1} \cdots n_d^{k_d} = 0, \text{ for } k_1 + \cdots k_d \geq i+1\right\}.$$

Hence

$$F(N) = \varinjlim \operatorname{Hom}(T_i, N) = N^{(d)}.$$

So $F \cong \hat{\mathbb{A}}^d$. In particular F is also smooth (terminology as in Lemma 1.18 (ii)). The morphism η induces an isomorphism on the tangent functors by the above discussion, and both F and H are smooth. So we see that η is an isomorphism by Jacobi Inversion Theorem. We are done. □

Lemma 1.19. *If $N \in \mathbf{Nil}_R$ with $N^2 = 0$, and $H : \mathbf{Nil}_R \to \mathbf{Ab}$ is a formal group, then the two abelian group structures defined in Lecture* 3 *coincide.*

Proof. We use $+_\tau : H(N) \times H(N) \to H(N)$ to denote the addition law of $H(N)$ as an object in $\mathbf{Ab}$, and $+$ the addition law on $H(N)$ defined by $H(+)$, where $+ : N \times N \to N$ is the addition of N. Apply H to $\{0\} \hookrightarrow N$. We get $H(\{0\}) \to H(N)$. Let 0_N be the image of $H(0)$. We have seen in Lecture 3, that 0_N is the zero for $+$. Now H is functorial, so for any $N_1 \to N_2$, $N_1, N_2 \in \mathbf{Nil}_R$, $(H(N_1), +_\tau) \to (H(N_2), +\tau)$ is a homomorphism of abelian groups. In the special case $\{0\} \hookrightarrow N$, $H(\{0\})$ has only one element, which is the identity of $H(\{0\})$. Since H preserves the identity element, 0_N is the zero element of $(H(N), +_\tau)$ by functoriality.

To show that $+ = +_\tau$, we note that $+ : H \times H \to H$ is a morphism of functors. So

$$+ : (H(N) \times H(N), +_\tau) \to (H(N), +_\tau)$$

is a homomorphism of abelian groups. Take $(x_1, x_2), (y_1, y_2) \in H(N) \times H(N)$. We have

$$(x_1, x_2) +_\tau (y_1, y_2) = (x_1 +_\tau y_1, x_2 +_\tau y_2).$$

Since $+$ is a homomorphism of abelian groups, applying H we get

$$(x_1 + x_2) +_\tau (y_1 + y_2) = (x_1 +_\tau y_1) + (x_2 +_\tau y_2).$$

Now take $x_1 = y_2 = 0$. We get

$$y_1 +_\tau x_2 = x_2 +_\tau y_1 = y_1 + x_2.$$

This shows the two addition laws are the same. □

Now we consider base change of formal groups.

Definition 1.20. (i) *Let $f : R \to S$ be a homomorphism of rings. If $N \in \mathbf{Nil}_S$, we can view N as an R-algebra via f. We denote $N_{[f]}$ the corresponding R-algebra.*
(ii) *Let $F : \mathbf{Nil}_R \longrightarrow \mathbf{Sets}$ be a functor. We define $f_\bullet F : \mathbf{Nil}_S \longrightarrow \mathbf{Sets}$ by $(f_\bullet F)(N) = F(N_{[f]})$.*

It is easy to see that $f_\bullet(\hat{\mathbb{A}}^d_R) = \hat{\mathbb{A}}^d_S$. If F is a formal group, so is $f_\bullet F$. Then we get a functor $f_\bullet : \mathbf{FG}_R \to \mathbf{FG}_S$, where $\mathbf{FG}_R$ denotes the category of formal groups over R.

Theorem 1.21 (Lazard, 1955)**.** *Let $f : R \twoheadrightarrow S$ be a surjective homomorphism of rings. Let G be a formal group over S such that $G \cong \hat{\mathbb{A}}^d_S$. Then there is a formal group F over R such that $F = \hat{\mathbb{A}}^d_R$ and $f_\bullet F = G$.*

The proof can be found in [Z].

Lazard's Theorem shows that, under some conditions, a formal group of the form $\hat{\mathbb{A}}^d$ can be lifted. How about the morphism? More precisely, let G_1, G_2 be two formal groups over S and F_1, F_2 two formal groups over R such that $f_\bullet F_i = G_i$. Let $\alpha : G_1 \to G_2$ be a homomorphism of formal groups. Does α lift to $F_1 \to F_2$?

The answer is no in general. Let us consider the following example.

Example: Consider $\hat{\mathbb{G}}_a$ over R. As a functor, $\hat{\mathbb{G}}_a(N) = (N, +)$. A homomorphism $f : \hat{\mathbb{G}}_a \to \hat{\mathbb{G}}_a$ is given by a formal power series $f(X) \in R[[X]]$ such that $f_N : N \to N$ is a homomorphism for all $N \in \mathbf{Nil}_R$. So f is a homomorphism if and only if

$$f(S+T) = f(S) + f(T) \tag{1.4}$$

in $R[[S,T]]$. Write $f = \sum a_n X^n, f_n = a_n X^n$. The equation (1.4) is equivalent to

$$a_n(T+S)^n = a_n T^n + a_n S^n, \qquad \forall n \geq 0.$$

So $a_0 = 0$. If R is torsion free, it is easy to see that $a_n = 0, n \geq 2$. If R is p torsion, then $a_n = 0$ for all n such that n is not a power of p. So we get

Proposition 1.22. (1) *If R is torsion free, then* $\operatorname{End}(\hat{\mathbb{G}}_a) = R$.
(2) *If $p \cdot R = 0$ for a prime p, let $\varphi : R \to R$ be the Frobenius, i.e., $\varphi(r) = r^p$. Then* $\operatorname{End}\hat{\mathbb{G}}_a \cong R_\varphi[[T]]$*, where $R_\varphi[[T]]$ is an algebra defined as follows: $R_\varphi[[T]]$ is $R[[T]]$ as an R-module and the multiplication is defined by*

$$r_m T^m \cdot r_n T^n = r_m \varphi^m(r_n) T^{m+n}.$$

Proof. (1) As we have seen, f is a homomorphism if and only if f is defined by $f(X) = rX$. Now associating Φ to r defines the isomorphism $\operatorname{End}(\hat{\mathbb{G}}_a) \to R$.
(2) We have $f \in \operatorname{End}(\hat{\mathbb{G}}_a)$ if and only if f is defined by $f(X) = \sum_i a_i X^{p^i}$. Associating f to the formal power series $\sum_i a_i T^i$ defines a bijection $\operatorname{End}(\hat{\mathbb{G}}_a) \cong R_\varphi[[T]]$. It is easy to see this map preserves the multiplication. □

Now consider the ring homomorphism $f : \mathbb{Z} \to \mathbb{F}_p$. It is easy to see that $f_\bullet(\hat{\mathbb{G}}_a)_{\mathbb{Z}} = (\hat{\mathbb{G}}_a)_{\mathbb{F}_p}$. By the above proposition, there are many homomorphisms $\Phi : (\hat{\mathbb{G}}_a)_{\mathbb{F}_p} \to (\hat{\mathbb{G}}_a)_{\mathbb{F}_p}$ which cannot be lifted.

We have a weaker partial solution to the above problem.

Proposition 1.23. *Let $f : S \twoheadrightarrow R$ be a surjective homomorphism of rings with kernel $\mathfrak{a}$ such that $\mathfrak{a}^2 = 0$. Assume $l\mathfrak{a} = 0$ for some $l \in \mathbb{N}$. Let $F, G : \mathbf{Nil}_S \to \mathbf{Ab}$ be two functors and G is a formal group. Assume $\alpha : f_\bullet F \to f_\bullet G$ is a homomorphism. Then there exists $\alpha' : F \to G$ such that $f_\bullet \alpha' = l\alpha$.*

Proof. Given $N \in \mathbf{Nil}_S$, we have to define $\alpha'_N : F(N) \to G(N)$. Given $\xi \in F(N)$. Let $\bar{\xi}$ be the image of ξ under the map $F(N) \to F(N/\mathfrak{a}N)$. Note that $N/\mathfrak{a}N$ is in fact an R-algebra. So $F(N/\mathfrak{a}N) = f_\bullet F(N/\mathfrak{a}N)$. We get a homomorphism

$\alpha_{N/\alpha N} : F(N/\mathfrak{a}N) \to G(N/\mathfrak{a}N)$. Let $\bar{\eta}$ be the image of $\bar{\xi}$ under this map. Since G is a formal group, we have the following exact sequence:

$$0 \longrightarrow G(\mathfrak{a}N) \longrightarrow G(N) \longrightarrow G(N/\mathfrak{a}N) \longrightarrow 0.$$

Let $\eta, \eta' \in G(N)$ be two lifts of $\bar{\eta}$. Then $\eta - \eta' \in G(\mathfrak{a}N)$. Since $\mathfrak{a}^2 = 0$, we have $G(\mathfrak{a}N) = \mathfrak{a}N \otimes_S t_G(S)$. Since $l\mathfrak{a} = 0$, we see $l\eta = l\eta'$. Now we define $\alpha'_N(\xi) = l\eta$. By the above discussion, α'_N is well-defined and satisfies $f_\bullet \alpha' = l\alpha$. □

Definition 1.24. *Let R be a commutative ring with 1. Let us be given a pair (C, ε), where C is an R-algebra with structure morphism $i : R \to C$ and ε is an R-algebra homomorphism $C \to R$. The pair (C, ε) is called an augmented algebra if $\varepsilon \circ i = \mathrm{id}_R$. If (C, ε) is an augmented algebra, we call $C^+ = \mathrm{Ker}\varepsilon$ the augmentation ideal. We have $C = R \oplus C^+$. A homomorphism of augmented algebras $f : A \to B$ is a homomorphism of R-algebras and $\varepsilon_A = \varepsilon_B \circ f$.*

Notations. We give a list of the notations which will be used later. Let A, B be two R-modules (R-algebras, R-augmented algebras or unitary R-algebras). We denote

$\mathrm{Hom}_R(A, B)$	the set of R-module homomorphisms.
$\mathrm{Hom}_a(A, B)$	the set of R-algebra homomorphisms, i.e., maps preserving the R-module structure and multiplicative structure.
$\mathrm{Hom}_{ua}(A, B)$	the set of homomorphisms of unitary rings, i.e., maps which not only preserve the algebra structure but also preserve 1.
$\mathrm{Hom}_{aa}(A, B)$	the set of homomorphisms of augmented algebras.

It is easy to see that $\mathrm{Hom}_{aa}(A, B) = \mathrm{Hom}_{ua}(A, B)$. If we consider topological rings, we add a "c" in the subscript to denote the continuous homomorphisms. For example, if A, B are two topological R-algebras, $\mathrm{Hom}_{ca}(A, B)$ will denote the set of continuous algebra homomorphisms from A to B.

Given $N \in \mathbf{Nil}_R$, we can form an augmented algebra A. As the R-module $A = R \oplus N$ with multiplication defined by: $(r, n)(r', n') = (rr', rn' + r'n + nn')$, See the Example after Definition 1.1. Let $\varepsilon : A \to R$ be the projection map. Then the augmentation ideal A^+ is N. For any other nilpotent algebra M, we have

$$\mathrm{Hom}_a(N, M) = \mathrm{Hom}_{aa}(A, R \oplus M) = \mathrm{Hom}_{ua}(A, R \oplus M).$$

Let $\mathbf{Augn}_R$ denote the category of augmented algebras with nilpotent augmentation ideals. The above discussion shows that we established an equivalence

$$\mathbf{Augn}_R \to \mathbf{Nil}_R$$

$$A \mapsto A^+$$

with inverse $N \mapsto R \oplus N$.

Since

$$\mathrm{Spec}A \times \mathrm{Spec}B = \mathrm{Spec}(A \otimes B),$$

we can see that

$$h_{A^+} \times h_{B^+} = h_{R\otimes B^+ + A^+\otimes R + A^+\otimes B^+},$$

where $h_N : \mathbf{Nil}_R \to \mathbf{Sets}$ is the functor defined by $h_N(M) = \mathrm{Hom}_a(N, M)$.

Definition 1.25. *Let (C, ε) be an augmented R-algebra given with a chain of ideals*

$$\mathfrak{c}_0 \supset \mathfrak{c}_1 \supset \mathfrak{c}_2 \supset \mathfrak{c}_3 \cdots , \qquad \mathfrak{c}_i \subset C^+,$$

such that $C/\mathfrak{c}_i$ is a nilpotent augmented algebra. We define a functor $\mathrm{Spf} C : \mathbf{Nil}_R \to \mathbf{Sets}$ *by*

$$\mathrm{Spf} C(N) = \varinjlim_{t \in \mathbb{N}} \mathrm{Hom}_a(C^+/\mathfrak{c}_t, N) \tag{1.5}$$

We endow C with the linear topology defined by the ideals $\mathfrak{c}_t$. Then an element of 1.5 is just a continuous algebra homomorphism $C^+ \to N$, where we give N the discrete topology. Indeed $\varphi : C^+ \to N$ continuous means that there is a number t such the $\varphi|_{\mathfrak{c}_t} = 0$. We will write:

$$\mathrm{Spf} C(N) = \mathrm{Hom}_{ca}(C^+, N).$$

We use $\mathrm{Spf}(C, \{\mathfrak{c}_t\})$ to denote the functor if we want to emphasize that $\mathrm{Spf} C$ is defined by the ideals $\mathfrak{c}_t$.

Example: Let $C = R[[X_1, \dots, X_n]], \mathfrak{c}_t = (X_1, \dots, X_n)^t$. Then $\mathrm{Spf} C = \hat{\mathbb{A}}^n_R$.

Definition 1.26. *The functor* $\mathrm{Spf} C$ *is called* ***strictly pro-representable*** *if*
(1) *$C^+/\mathfrak{c}_t$ is finitely generated R-module for any $t \geq 0$;*
(2) *for every $t \geq 0$, there is a sub-R-module $u_t \subset C^+$ such that C^+/u_t is a finitely generated projective R-module, such that the two sequences $\{u_t\}$ and $\{\mathfrak{c}_t\}$ of submodules of C are cofinal.*

Note that in the definition (1.26), the functor $\mathrm{Spf}(C, \{\mathfrak{c}_t\})$ is the same as $\mathrm{Spf}(C, \{u_t\})$ by the cofinality condition in (2).

Notations as above, put $\hat{C} = \varprojlim C/\mathfrak{c}_t$. We have a surjective homomorphism $\hat{C} \twoheadrightarrow C/\mathfrak{c}_s$. Denote the kernel by $\hat{\mathfrak{c}}_s$, we have isomorphisms $\hat{C}/\hat{\mathfrak{c}}_s \cong C/\mathfrak{c}_s$. Then $\mathrm{Spf}(\hat{C}, \{\hat{\mathfrak{c}}_t\}) = \mathrm{Spf}(C, \{\mathfrak{c}_t\})$.

Definition 1.27. *Let $G = \mathrm{Spf} C : \mathbf{Nil}_R \to \mathbf{Ab}$ be a strictly pro-representable functor, i.e., that $F \circ G$ is a strictly pro-representable functor, where $F : \mathbf{Ab} \to \mathbf{Sets}$ is the forgetful functor. Define the* ***hyperalgebra*** *H_G of G by*

$$H_G = \mathrm{Hom}_{cR}(C, R).$$

Lemma 1.28. *There is an augmented algebra structure on H_G.*

Proof. Given $f \in H_G, r \in R$, define $(rf)(x) = rf(x)$. This gives a natural R-module structure on H_G.

The group law $X \times X \to X$ gives a homomorphism $m^* : C \to C \hat{\otimes} C$, where $C \hat{\otimes} C = (C \otimes C, \mathfrak{c}_t \otimes C + C \otimes \mathfrak{c}_t)$, i.e., as an augmented algebra, $C \hat{\otimes} C$ is just $C \otimes C$, and the chain of the ideals is defined by $\{\mathfrak{c}_t \otimes C + C \otimes \mathfrak{c}_t\}$. The multiplication of H_G is defined as follows. Given $\xi, \eta \in H_G$, put $\xi \cdot \eta = (\xi \otimes \eta) \circ m^*$,

$$\begin{tikzcd} C \arrow[r, "m^*"] & C \otimes C \arrow[r, "\xi \otimes \eta"] & R \otimes R = R . \end{tikzcd}$$

This gives an algebra structure on H_G.

For $r \in R$, define $f_r : R \oplus C^+ \to R$ by $f_r|_R(x) = rx$ and $f_r|_{C^+} = 0$. This gives the map $i : R \to H_G$. Define $\varepsilon : H_G \to R$ as follows. Since $C = R \oplus C^+$, any $f \in H_G$ can be written as $f = f_1 \oplus f_2$, where $f_1 : R \to R, f_2 : C^+ \to R$. Define $\epsilon(f) = f_1(1)$. It is easy to see that $\varepsilon \circ i = \mathrm{id}_R$. Hence we get an augmented algebra structure on H_G. It is easy to check that $H_G^+ = \mathrm{Hom}_{cR}(C^+, R)$. □

Definition 1.29. *Define a functor* $(\mathbb{G}_m H_G)^\wedge : \mathbf{Nil}_R \to \mathbf{Ab}$ *by*

$$(\mathbb{G}_m H_G)^\wedge(N) = (1 + H_G^+ \otimes_R N)^\times.$$

As in the definition of $\mathbb{G}_m$, $(1 + H_G^+ \otimes_R N)^\times$ *means the units in* $R \oplus (H_G^+ \otimes_R N) \subset H_G \otimes A$ *of the form* $1 + x, x \in H_G^+ \otimes_R N$, *where* $A = R \oplus N$.

Lemma 1.30. *The functor* $(\mathbb{G}_m H_G)^\wedge$ *is a formal group.*

Proof. Since $H_G^+ = \varinjlim \mathrm{Hom}_R(C/u_t, R)$, and C/u_t is finitely generated projective R-module, H_G^+ is a flat R-module. So the functor $(\mathbb{G}_m H_G)^\wedge$ is exact. The second condition of formal groups is easy to verify. □

Recall that $G = \mathrm{Spf} C$, where $C = R \oplus C^+$. Given $N \in \mathbf{Nil}_R$, we have

$$G(N) = \mathrm{Hom}_{ca}(C^+, N) = \varinjlim_t \mathrm{Hom}_a(C^+/\mathfrak{c}_t, N)$$

$$\subset \varinjlim_t \mathrm{Hom}_R(C^+/\mathfrak{c}_t, N) = \varinjlim_t \mathrm{Hom}_R(C^+/u_t, N).$$

Since C^+/u_t is a finitely generated projective module, we have $\mathrm{Hom}_R(C^+/u_t, N) \cong \mathrm{Hom}_R(C^+/u_t, R) \otimes N$ [1].

So we have

$$X(N) \subset \varinjlim(\mathrm{Hom}_R(C^+/u_t, R) \otimes N) = (\varinjlim \mathrm{Hom}_R(C^+/u_t, R)) \otimes N = H_G^+ \otimes N,$$

here we use the fact that $\varinjlim$ and $\otimes$ commute.

Definition 1.31. *Define a natural transformation* $\Phi : G = \mathrm{Spf} C \to (\mathbb{G}_m H_G)^\wedge$ *by*

$$\Phi_N : G(N) \to (\mathbb{G}_m H_G)^\wedge(N) = (1 + H_G^+ \otimes_R N)^\times$$

$$\xi \mapsto 1 + \xi.$$

On the right hand side, using the inclusion $G(N) \subset H_G^+ \otimes_R N$, *we identify* $\xi \in G(N)$ *with an element of* $H_G^+ \otimes_R N$.

[1] For any finitely generated projective R-module P, we have $\mathrm{Hom}(P^\vee, M) \cong P \otimes M$, where $P^\vee = \mathrm{Hom}(P, R)$ is the dual module of P. In fact, we have a canonical homomorphism $P \otimes M \to \mathrm{Hom}(P^\vee, M)$ defined by $p \otimes m \mapsto (f \mapsto f(p)m)$. If P is free and finitely generated, this map is obviously an isomorphism. In general, take a resolution $0 \to N \to F \to P \to 0$, with F is finitely generated R-module. Since P is projective, this sequence is split exact, so N is also projective, i.e., $P \oplus N = F$. So $P^\vee \oplus N^\vee = F^\vee$ is also free. By this we see that $P^\vee$ is also projective. The split exactness shows that we have the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & N \otimes M \arrow[r] \arrow[d, "a"'] & F \otimes M \arrow[r] \arrow[d, "b"'] & P \otimes M \arrow[r] \arrow[d, "c"'] & 0 \\
0 \arrow[r] & \mathrm{Hom}(N^\vee, M) \arrow[r] & \mathrm{Hom}(F^\vee, M) \arrow[r] & \mathrm{Hom}(P^\vee, M) \arrow[r] & 0
\end{tikzcd}$$

b is an isomorphism by the above discussion. The 5-Lemma shows that a is injective and c is surjective. Since P and N are symmetric, we can change the roles of N and P to see both a and c are isomorphisms. Now apply this to $\mathrm{Hom}_R(C^+/u_t, N) = (C^+/u_t)^\vee$, which is also finitely generated and projective, as we have seen.

Lemma 1.32. *For any $N \in \mathbf{Nil}_R$, the map Φ_N is a group homomorphism.*

We first show Lemma 1.32.

Proof of Lemma 1.32. Let $A = R \oplus N$ be the deduced augmented algebra. Recall that $G = \mathrm{Spf}C$. By definition, $G(N) = G(A) = \mathrm{Hom}_{caa}(C, A) = \mathrm{Hom}_{cua}(C, A)$. Given $\xi_1, \xi_2 \in G(A)$, then $\xi_i : \mathrm{Spec}A \to G$. We need to show that $\Phi_N(\xi_1 + \xi_2) = \Phi_N(\xi_1)\Phi_N(\xi_2)$.

We first check what the morphism $\xi_1 + \xi_2$ is. Let $\Delta : \mathrm{Spec}A \to \mathrm{Spec}A \times \mathrm{Spec}A$ be the diagonal morphism. We know that Δ corresponds to the multiplication homomorphism $m : A \otimes_R A \to A : m(x_1 \otimes x_2) = x_1x_2$. The right triangle of the following diagram

$$\begin{tikzcd}
 & \mathrm{Spec}A \arrow[d, "\Delta"] \arrow[rd, "\xi_1+\xi_2"] & \\
 & \mathrm{Spec}A \times \mathrm{Spec}A \arrow[ld, dashed] \arrow[d, "\xi_1\times\xi_2"] & \\
\mathrm{Spec}C/\mathfrak{c}_t \times \mathrm{Spec}C/\mathfrak{c}_t \arrow[r] & G \times G \arrow[r, "+"] & G
\end{tikzcd}$$

is commutative, since the composite of the vertical arrows is (ξ_1, ξ_2). This shows that $\xi_1 + \xi_2 = + \circ (\xi_1 \times \xi_2) \circ \Delta$. Since $\xi_i \in \mathrm{Hom}_{caa}(C, A)$ is continuous, there is $t \in \mathbb{N}$ such that ξ_i factor through $C/\mathfrak{c}_t$ for both $i = 1, 2$. So we have the left triangle of the above diagram. The bottom line of the diagram is obtained from

$$C \xrightarrow{\delta_t} C/\mathfrak{c}_t \otimes C/\mathfrak{c}_t \ ,$$

where δ_t is the composite

$$C \xrightarrow{m_C^*} C \otimes C \longrightarrow C/\mathfrak{c}_t \otimes C/\mathfrak{c}_t \ .$$

Here m_C^* is the map obtained from the multiplicative structure on X, see the proof of Lemma 1.28. So $\xi_1 + \xi_2$ corresponds to the following homomorphism

$$C \xrightarrow{\delta_t} C/\mathfrak{c}_t \otimes_R C/\mathfrak{c}_t \xrightarrow{\xi_1\otimes\xi_2} A \otimes A \xrightarrow{m} A$$

Recall (Lemma 1.28) that the multiplication in H_G is defined as follows. Given $h_1, h_2 \in H_G$, then $h_1 \cdot h_2 = (h_1 \otimes h_2) \circ \delta_t$ for t large enough.

As before, there is an isomorphism

$$H_G \otimes_R A \cong \mathrm{Hom}_{cR}(C, A)$$

$$h \otimes a \mapsto (c \mapsto h(c)a).$$

Suppose ξ_i corresponds to $h_i \otimes a_i$ under this isomorphism. The above discussion shows that $\xi_1 + \xi_2$ corresponds to $(h_1 \cdot h_2)a_1a_2$. The map $G(A) \to (H_G \otimes A)^\times$ is obtained from the inclusion $G(A) \subset \mathrm{Hom}_{cR}(C, A)$, therefore preserves the multiplicative structure. By the definition of Φ_N, we have a commutative diagram

$$\begin{tikzcd}
G(N) \arrow[r, "\Phi_N"] \arrow[d, "\cong"] & (1 + H_G^+ \otimes N)^\times \arrow[d, hook] \\
G(A) \arrow[r] & (H_G \otimes A)^\times
\end{tikzcd}$$

So Φ_N is a group homomorphism. □

The homomorphism Φ_N is obtained from an inclusion, so it is an embedding. Next, we will describe the image of Φ_N.

Let $m : C \otimes C \to C$ be the multiplication. It is obtained from the diagonal morphism $\Delta : G \to G \times G$. Since Δ is a homomorphism of group functors, the deduced map

$$m^* : H_G \to H_G \otimes H_G$$

is a homomorphism of algebras.

Proposition 1.33. *We have*

$$G(A) = \left\{ x \in \left(1 + H_G^+ \otimes_R A^+\right)^\times | m_A^* x = x \otimes x \right\}$$

where $m_A^* = m^* \otimes \mathrm{id}_A : H_G \otimes A \to H_G \otimes H_G \otimes A$*, and* $x \otimes x$ *is identified with the image of* $x \otimes x$ *under the map* $\mathrm{id}_{H_G \otimes H_G} \otimes m_A : H_G \otimes H_G \otimes A \otimes A \to H_G \otimes H_G \otimes A$.

Proof. Given $(\rho : C \to A) \in G(A) = \mathrm{Hom}_{caa}(C, A)$, then $\rho(1) = 1$ since ρ respect the augmentation structure. Since ρ is a an algebra homomorphism, we have a commutative diagram

$$\begin{tikzcd}
C \otimes C \arrow[r, "m"] \arrow[d, "\rho \otimes \rho"] & C \arrow[d, "\rho"] \\
A \otimes A \arrow[r, "m_A"] & A
\end{tikzcd}$$

Given $x \in H_G \otimes A = \mathrm{Hom}_{cR}(C, A)$, x corresponds a homomorphism $\hat{x} : C \to A$. Assume $\hat{x}$ respect the augmentation, i.e., $\hat{x}(1) = 1$. Then $\hat{x}$ is a homomorphism of commutative rings with 1 if and only if the above diagram commutes for $\rho = \hat{x}$, i.e., $x \in G(A)$ if and only if $\hat{x} m = m_A \circ (\hat{x} \otimes \hat{x})$. It is easy to see that

$$m_A^*(x) = \hat{x} \circ m, \quad x \otimes x = m_A \circ (\hat{x} \otimes \hat{x}).$$

Hence we get the proposition. □

We begin with some general notions.

Definition 1.34. *Let S be an augmented R-algebra. Let S^+ be its augmentation ideal. We define a group functor*

$$(\mathbb{G}_m S)^\wedge : \mathbf{Nil}_R \longrightarrow \mathbf{Ab}$$

by

$$(\mathbb{G}_m S)^\wedge(N) = (1 + S^+ \otimes_R N)^\times.$$

As we saw in Lemma 1.20, if S^+ is a flat R-module, then $(\mathbb{G}_m S)^\wedge$ is a formal group. The construction $S \mapsto (\mathbb{G}_m S)^\wedge$ is functorial.

Although $S \to S \otimes S$, $x \mapsto x \otimes x$ is not an algebra homomorphism (not additive), we still have a morphism of group functors

$$(\mathbb{G}_m S)^\wedge \to (\mathbb{G}_m (S \otimes_R S))^\wedge \tag{1.6}$$

$$x \mapsto x \otimes x.$$

Explicitly, the map (1.5) is defined by $x = 1 + y \mapsto x \otimes x = 1 + 1 \otimes y + y \otimes 1 + y \otimes y$ for $x \in (1 + S^+ \otimes N)^\times, y \in S^+ \otimes_R N$. Here $1 \otimes y + y \otimes 1 + y \otimes y \in [(R \otimes S^+) \oplus (S^+ \otimes R) \oplus (S^+ \otimes S^+)] \otimes N = (S \otimes S)^+ \otimes N$. It is easy to check this is a morphism of group functors directly.

For any $N \in \mathbf{Nil}_R$, we associate to N a new nilpotent algebra N^{ab} such that as an R-module, N^{ab} is just N, and the new multiplication on N^{ab} is defined by $(N^{ab})^2 = 0$.

Definition 1.35. *For any functor $H : \mathbf{Nil}_R \to \mathbf{Sets}$, we define the* ***Lie algebra functor*** *of H*

$$\mathrm{Lie}H : \mathbf{Nil}_R \longrightarrow \mathbf{Sets}$$

by $\mathrm{Lie}H(N) = H(N^{ab})$.

If H is left exact, there is a canonical abelian group structure on $\mathrm{Lie}H(N)$.

Note that $H(N^{ab}) = t_H(N^{ab})$. The difference between the Lie algebra functor and the tangent functor is that the Lie algebra functor is defined on $\mathbf{Nil}_R$, while the tangent functor is defined on $\mathbf{Mod}_R$.

Definition 1.36. *A sequence of group functors $H_1 \to H_2 \to H_3$ is called* ***exact*** *if for any $N \in \mathbf{Nil}_R$, the sequence*

$$H_1(N) \to H_2(N) \to H_3(N)$$

of abelian groups is exact.

By definition of $\mathrm{Lie}H$, the functor Lie is exact.

Now suppose we are given a pro-representable formal group $G = \mathrm{Spf}C$. We have defined $H_G = \mathrm{Hom}_{cR}(C, R)$.
Remark: H_G has a bi-algebra structure defined by $m^* : H_G \to H_G \otimes H_G$, so $\mathrm{Spec}H_G$ is a group scheme. In literature, $\mathrm{Spec}H_G$ is called the dual of G. In our treatment, this plays no role.

Recall that in the last lecture we showed that there is an embedding of formal groups $G :\to (\mathbb{G}_m H_G)^\wedge$ and for any $N \in \mathbf{Nil}_R$, the image of $G(N)$ is

$$\left\{x \in (1 + H_G^+ \otimes N)^\times | m^* x = x \otimes x\right\}.$$

The above results are summarized in

Theorem 1.37. *We have the following exact sequence of formal groups*

$$\begin{tikzcd} 0 \arrow[r] & G \arrow[r] & (\mathbb{G}_m H_G)^\wedge \arrow[r, "\gamma_1-\gamma_2"] & (\mathbb{G}_m(H_G \otimes H_G))^\wedge \end{tikzcd}$$

where γ_1 is the morphism induced by $m^* : H_G \to H_G \otimes H_G$, and γ_2 is the map (1.5)*, i.e., the morphism induced by $\Delta : H_G \to H_G \otimes H_G$, $\Delta(x) = x \otimes x$.*

In the remainder of this section, we assume that R is a $\mathbb{Q}$-algebra. If $N \in \mathbf{Nil}_R$, $y \in N$, then $\exp(y) = \sum_{n=0}^{\infty} \frac{y^n}{n!}$ is well-defined. Let S be any augmented algebra, $H = (\mathbb{G}_m S)^\wedge$. It is easy to see that we have an isomorphism

$$[S^+ \otimes N]^+ \to H(N) = (1 + S^+ \otimes N)^\times$$
$$y \mapsto \exp(y)$$

with inverse $1 + z \mapsto \log(1 + z)$. The left hand side $[S^+ \otimes N]^+$ means $S^+ \otimes N$ with additive abelian group structure. We also have an isomorphism

$$\mathrm{Lie} H(N) \cong (1 + S^+ \otimes N^{ab})^\times \cong S^+ \otimes N^{ab} = [S^+ \otimes N]^+,$$
$$1 + y \mapsto y.$$

So we have an isomorphism

$$\exp : \mathrm{Lie} H \xrightarrow{\simeq} H \ . \tag{1.7}$$

Proposition 1.38. *Assume R is a $\mathbb{Q}$-algebra. Then for any strictly representable formal group G, there is an exponential map $\exp_G : \mathrm{Lie} G \to G$, which is an isomorphism functorial in G*

Proof. By Theorem 1.37 and the fact that Lie is an exact functor, we have

$$\begin{tikzcd} (*) & 0 \arrow[r] & \mathrm{Lie} G \arrow[r] \arrow[d, dashed, "\exp_G"] & \mathrm{Lie}(\mathbb{G}_m H_G)^\wedge \arrow[r] \arrow[d, "\exp"] & \mathrm{Lie}(\mathbb{G}_m(H_G \otimes H_G))^\wedge \arrow[d, "\exp"] \\ & 0 \arrow[r] & G \arrow[r] & (\mathbb{G}_m H_G)^\wedge \arrow[r, "\gamma_1-\gamma_2"] & (\mathbb{G}_m(H_G \otimes H_G))^\wedge \end{tikzcd}$$

We check that the right hand side square is commutative. Since γ_1 is obtained from an algebra homomorphism, γ_1 commutes with exp by functoriality. We check that γ_2 commutes with exp. Given $N \in \mathbf{Nil}_R$, the homomorphism γ_2 is defined by (1.5). If we identify $\mathrm{Lie}(\mathbb{G}_m H_G)^\wedge(N) = (1 + H_G^+ \otimes N^{ab})^\times$ with $H_G^+ \otimes N$ by $1 + y \mapsto y$, then $\mathrm{Lie}(\gamma_1)$ is defined by $y \mapsto 1 \otimes y + y \otimes 1$ (note $y \otimes y = 0$).

$$\begin{tikzcd} (H_G^+ \otimes N^{ab})^+ \arrow[r] \arrow[d, "\exp"] & (H_G \otimes H_G)^+ \otimes N^{ab} \arrow[d, "\exp"] \\ (1 + H_G^+ \otimes N)^\times \arrow[r] & (1 + (H_G \otimes H_G)^+ \otimes N)^\times \end{tikzcd}$$

So we have to check

$$\exp(1 \otimes y + y \otimes 1) = \exp(y) \otimes \exp(y).$$

Note that $\exp(1 \otimes y) = \sum_{n \geq 1} \frac{(1 \otimes y)^n}{n!} = 1 \otimes \exp(y)$ since $\exp(y) = \sum_{n \geq 0} \frac{y^n}{n!}$. So

$$\exp(1 \otimes y + y \otimes 1) = \exp(1 \otimes y) \exp(y \otimes 1) = (1 \otimes \exp(y))(\exp(y) \otimes 1) = \exp(y) \otimes \exp(y).$$

Consequently, we get the commutativity of the right hand square of diagram $(*)$.

The last two vertical arrows of diagram ($*$) are isomorphisms by (1.6), so this diagram induces an isomorphism $\exp_G : \mathrm{Lie}G \to G$. □

Theorem 1.39. *Assume R is a $\mathbb{Q}$-algebra. Let $G = \mathrm{Spf}(C, \{\mathfrak{c}_t\})$ be a strictly pro-representable functor, such that for t large enough, $\mathfrak{c}_t \subset (C^+)^2$ and $C^+/(C^+)^2$ is a free R-module of rank d. Then $G \cong \hat{\mathbb{G}}_a^d$.*

Proof. By definition, $\mathrm{Lie}G(N) = \mathrm{Hom}_{ca}(C^+, N^{ab})$. Since $(N^{ab})^2 = 0$ and $\mathfrak{c}_t \hookrightarrow (C^+)^2$ for t large enough, we have

$$\mathrm{Lie}G(N) = \mathrm{Hom}_{ca}(C^+/(C^+)^2, N) = N \otimes (C^+/(C^+)^2)^\wedge \cong (N^{(d)}, +).$$

So $\mathrm{Lie}G \cong \hat{\mathbb{G}}_a^d$. Proposition 1.38 shows that $G \cong \mathrm{Lie}G$, hence the theorem. □

Corollary 1.40. *Let R be a $\mathbb{Q}$-algebra. If $G = \mathrm{Spec}A$ is a group scheme, with A a nilpotent R-augmented algebra which is finitely generated as an R-module, then $G = 0$.*

Proof. Assume first that R is a field k. Take $C = A$ with ideals $\mathfrak{c}_t = 0$. Then the condition of Theorem 1.39 is satisfied automatically. Hence, by Theorem 1.39, we have $G \cong \hat{\mathbb{G}}_a^d = \mathrm{Spf}k[[X_1, \ldots, X_d]]$. If $d \neq 0$, A^+ is not nilpotent. Hence $d = 0$, G is trivial.

For the general case, let $\mathfrak{m}$ be any maximal ideal of R. Denote the quotient map $R \to R/\mathfrak{m}$ by κ. Then $\kappa_\bullet G = \mathrm{Spec}A/\mathfrak{m}A$ is a group scheme over the field $R/\mathfrak{m}R$. The above discussion shows $A/\mathfrak{m}A \cong R/\mathfrak{m}R$. So $A^+/\mathfrak{m}A^+ = 0$. Then Nakayama's lemma shows $A^+_{\mathfrak{m}} = 0$. Since this is true for all $\mathfrak{m}$, we have $A^+ = 0$. □

Remark. 1. The corollary is false if R has characteristic $p > 0$. Consider the functor $G : \mathbf{Nil}_R \to \mathbf{Ab}$ defined by $G(N) = \{n \in N | n^p = 0\}$. This is well-defined since $(n_1 + n_2)^p = n_1^p + n_2^p$. It is easy to see that $G = \mathrm{Spec}R[X]/X^p$. Then G is a non-trivial finite group scheme.
2. The corollary is equivalent to the following Theorem of Cartier. Any finite group scheme over a field of characteristic 0 is étale.

Definition 1.41. *Let R be any commutative ring with 1. Let I be an R-algebra (maybe without 1). A **divided power (pd) structure** on I consists of a collection of maps $\gamma_i : I \to I$, $i \geq 1$, such that*
(1) $\gamma_1(x) = x$; $n!\gamma_n(x) = x^n, n \geq 1$; $\gamma_n(ax) = a^n\gamma_n(x)$.
(2) $\gamma_n(x + y) = \sum_{i=1}^{n-1} \gamma_i(x)\gamma_{n-i}(x) + \gamma_n(x) + \gamma_n(y)$.
(3) $\gamma_p(x)\gamma_q(x) = \binom{p+q}{p}\gamma_{p+q}(x)$.
(4) $\gamma_p(\gamma_q(x)) = \frac{(pq)!}{p!(q!)^q}\gamma_{pq}(x)$.

*If there is an $N \in \mathbb{N}^+$ such that $\gamma_{n_1}(x_1) \ldots \gamma_{n_r}(x_r) = 0$ for all $n_1 + \cdots + n_r \geq N$ and all $x_1, \ldots, x_r \in I$, the divided powers are called **nilpotent**.*

If we define $\gamma_0(x) = 1$, then we can simplify formula (2). But note that I need not contain 1.
Example: If R is a $\mathbb{Q}$-algebra, then any R-algebra I has a pd structure defined by $\gamma_n(x) = \frac{x^n}{n!}$. This is the example which motivates the definition.

A non-trivial example in introduced next.

Let R be a commutative ring with 1. Let p be a fixed prime number. Assume that for any prime number $l \neq p$, l is invertible in R. An example satisfying these conditions is $\mathbb{Z}_{(p)}$. Let S be an R-algebra with 1. Consider $I = pS$. Given $x = py \in I$ with $y \in S$, define $\gamma_n(x) = \frac{p^n}{n!} y^n, n \geq 1$.

Claim: γ_n defines a pd structure on I.
First, we check that γ_n is well-defined. It is easy to see the denominator of $\frac{p^n}{n!}$ is prime to p, hence it makes sense in R by our assumption. If $pz = 0$, because $p | \frac{p^n}{n!}$ in R, it is easy to see

$$\frac{p^n}{n!}(y+z)^n = \frac{p^n}{n!} y^n.$$

So $\gamma_n(x)$ is independent of the choice of y.

Next, we check that $\gamma_n(x)$ satisfies the relations (1)-(4) in Definition 1.41.

If R and S have no $\mathbb{Z}$-torsion, then $S \subset S \otimes_{\mathbb{Z}} \mathbb{Q}$. Under this inclusion, $\gamma_n(x) = \frac{x^n}{n!}$. So γ_n satisfies (1)-(4).

For the general case, we only show

$$\gamma_n(x+y) = \sum_{i=1}^{n-1} \gamma_i(x)\gamma_{n-i}(x) + \gamma_n(x) + \gamma_n(y).$$

The other formulas are similarly proven.

Given $x, y \in I$, define a map $\alpha : p\mathbb{Z}[X,Y] \longrightarrow pS = I$ by $\alpha(X) = x, \alpha(Y) = y$. Let $\gamma'_n(t) = \frac{t^n}{n!}$, $t \in p\mathbb{Z}[X,Y]$. Then $\gamma_n(\alpha(t)) = \alpha(\gamma'_n(t))$, for all $t \in p\mathbb{Z}[X,Y]$. $\gamma_n(x+y) = \gamma_n(\alpha(X+Y)) = \alpha(\gamma'_n(X+Y))$. Since we know the corresponding formula holds in $p\mathbb{Z}[X,Y]$, the formula holds also in pS.

In this lecture, we treat divided power structure more seriously.

Definition 1.42. *Let R be a commutative ring with 1 and let $I \subset R$ be an ideal. A collection of maps $\gamma_n : I \to I, n \geq 1$ is called **divided powers**(pd in French) if the following relations are satisfied:*

$$\gamma_n(rx) = r^n \gamma_n(x), \quad r \in R, \quad x \in I;$$

$$n!\gamma_n(x) = x^n;$$

$$\gamma_n(x+y) = \sum_{i=0}^{n} \gamma_i(x)\gamma_{n-i}(x),$$

where we set $\gamma_0(x) = 1$;

$$\gamma_p(x)\gamma_q(x) = \binom{p+q}{p}\gamma_{p+q}(x);$$

$$\gamma_p(\gamma_q(x)) = \frac{(pq)!}{p!(q!)^q}\gamma_{pq}(x).$$

More generally, if I is any R-algebra, $\gamma_n : I \to I$ is called divided powers if this sequence defines divided powers on $0 \oplus I$ in the ring $R \oplus I$. This definition coincides with Definition 1.41. We can define nilpotent divided powers as in Definition 1.41. Note that if γ_n are nilpotent divided powers, then I is nilpotent by the relation

$n!\gamma_n(x) = x^n$.

Example: If R has no $\mathbb{Z}$-torsion, then $R \subset R \otimes \mathbb{Q}$. So $\frac{x^n}{n!} \in R \otimes \mathbb{Q}$ is well-defined. Suppose I is an ideal of R, then I has divided powers if and only if $\frac{x^n}{n!} \in I$.

Proposition 1.43. *Let I, J be two R-algebras. Suppose I has divided powers $\{\gamma_n\}, n \geq 1$. Then there is a unique divided power structure $\{\tilde{\gamma}_n\}$ on $I \otimes_R J$ such that $\tilde{\gamma}_n(x \otimes y) = \gamma_n(x) \otimes y^n$ for all $x \in I, y \in J$.*

The proof is omitted but it is nontrivial.

Let R be a $\mathbb{Z}_{(p)}$-algebra. We consider the polynomial ring $A = R[\{X_i\}, i \in M]$ in possibly infinitely many indeterminates $h_i, i \in M$, where M is a set. Let $\mathfrak{a} = \langle \{X_i^p\}, i \in M\rangle$ be the ideal generated by X_i^p. Let $S = A/\mathfrak{a}$. Then S is an augmented R-algebra. Put $x_i = X_i (\mathrm{mod}\ \mathfrak{a})$. Then the augmentation ideal S^+ of S is generated by the x_i.

Proposition 1.44. *There is a unique divided powers structure $\{\gamma_n\}$ on S^+ which satisfies:*

$$\gamma_n(x_i) = x_i^n/n! \textit{ for } i < p; \quad \gamma_n(x_i) = 0, i \geq p.$$

Proof. First, we assume R has no p torsion. For $y \in S$, we can write $y = \sum_{1 \leq r \leq m} a_r Z_r$, where $a_r \in R$ and Z_r has the form

$$X_{i_1}^{e_1} \cdots X_{i_l}^{e_l}, \quad 0 \leq e_i < p.$$

Now $y \in S^+$ means $Z_r \neq 1$. So

$$y^n = \sum_{j_1 + \cdots + j_m = n} a_1^{j_1} Z_1^{j_1} \cdots a_m^{j_m} Z_m^{j_m}.$$

Note that for $j_i \geq p, Z_i^{j_i} = 0$, hence

$$\frac{y^n}{n!} = \sum_{\substack{j_1 + \cdots + j_m = n \\ j_i < p}} \frac{1}{j_1! \cdots j_m!} a_1^{j_1} Z_1^{j_1} \cdots a_m^{j_m} Z_m^{j_m}$$

makes sense and is an element of S^+. We are done.

For a general R, take a surjection $R_1 \twoheadrightarrow R$ such that R_1 has no $\mathbb{Z}$ torsion. Similarly, we have S_1, S_1^+. The above discussion shows we can define divided powers, say $\tilde{\gamma}_n$, on S_1^+. Let $\mathfrak{b} = \mathrm{Ker}(R_1 \to R)$. Then $S_1^+ \to S^+$ has kernel $\mathfrak{b}S_1 \cap S_1^+ = \mathfrak{b}S_1^+$. We have $S^+ = S_1^+/\mathfrak{b}S_1^+$.

Claim: $\tilde{\gamma}_n$ is well-defined on equivalence classes defined by $\mathfrak{b}S_1^+$, i.e., if $y \in S_1^+, h \in \mathfrak{b}S_1^+$, then $\tilde{\gamma}_n(y) = \tilde{\gamma}_n(y + h)$.

In fact, we have

$$\tilde{\gamma}_n(y + h) = \tilde{\gamma}_n(y) + \sum_{i \geq 1} \tilde{\gamma}_{n-i}(y)\tilde{\gamma}_i(h).$$

But $h \in \mathfrak{b}S_1^+$ has the form $\sum a_r Z^r$ with $a_r \in \mathfrak{b}, Z_r$ are monomials in x_i, so for $i \geq 1$,

$$\tilde{\gamma}_i(h) = \sum_{\substack{j_1 + \cdots + j_m = n \\ j_i < p}} \frac{1}{j_1! \cdots j_m!} a_1^{j_1} Z_1^{j_1} \cdots a_m^{j_m} Z_m^{j_m} \in \mathfrak{b}S_1^+.$$

The claim follows.

The claim shows that we can define $\gamma_n : S_1 \to S_1$ by the reduction of $\tilde{\gamma}_n$. We are done. □

Theorem 1.45. *Let k be a field with characteristic p. There exists a set $\{a_i \in k | i \in M\}$, where M is an index set, such that $a_{i_1}^{e_1} \cdots a_{i_m}^{e_m}, 0 \leq e_i < p$, make a basis of k over k^p. Such a set $\{a_i \in k | i \in M\}$ is called a **p-basis** of k. A p-basis exists.*

We omit the proof.

Let $\{a_i \in k | i \in M\}$ be a p-basis of k. Let $l = k^{1/p}$. We can write

$$l = k[\{T_i\}_{i \in M}]/(T_i^p - a_i).$$

Then

$$l \otimes_k l = k[\{T_i, T_i'\}_{i \in M}]/(T_i^p - a_i, T_i'^p - a_i).$$

If we put $X_i = T_i - T_i'$, we can write

$$l \otimes_k l = k[\{T_i, X_i\}_{i \in M}]/(T_i^p - a_i, X_i^p) = l[\{X_i\}_{i \in M}]/(X_i^p).$$

By Proposition 1.30, we can define a divided power structure on $(l \otimes_k l)^+$. Consider the multiplication $l \otimes_k l \to l$. We use I to denote the kernel of the multiplication map. It is not hard to see that the X_i generate I, hence $I = (l \otimes_k l)^+$.

Corollary 1.46. *The kernel of the multiplication $l \otimes_k l \to l$ has a divided power structure* (*not unique, relies on the choice of a p-basis*).

Remark: If M is infinite, the kernel I is not nilpotent, since $X_{i_1} \cdots X_{i_n} \neq 0$ for different i_j. Corollary 1.46 shows that we can define a pd structure on non-nilpotent ideals.

We can generalize Proposition 1.38 as follows.

Lemma 1.47. *Let $F = (\mathbb{G}_m S)^\wedge$ for an augmented R-algebra S. Let $N \in \mathbf{Nil}_R$ with nilpotent divided powers $\{\gamma_n\}$. Then we have an isomorphism*

$$\exp : \mathrm{Lie}F(N) = (1 + N^{ab} \otimes_R S^+)^\times \to (1 + N \otimes S^+)^\times$$

$$1 + n \otimes s \mapsto \sum_{l \geq 0} \gamma_l(n) \otimes s^l$$

Proof. By Proposition 1.29, for $l \geq 1$, $n \otimes s \mapsto \gamma_l(n) \otimes s^l$ defines a divided power structure on $N \otimes S^+$. It is easy to see that

$$(N \otimes S^+)^+ \to (1 + N \otimes S^+)^\times$$

$$n \otimes s \mapsto \sum_{l \geq 0} \gamma_l(n) \otimes s^l$$

is a group homomorphism. It is an isomorphism since it has an inverse

$$1 - n \otimes s \mapsto - \sum_{l \geq 1} (l-1)! \gamma_l(n) \otimes s^l.$$

Since $\mathrm{Lie}F(N) = (1 + N^{ab} \otimes_R S^+)^\times$ is isomorphic to $(N \otimes_R S^+)^+$ by $1 + y \mapsto y$, we are done. □

Proposition 1.48. *Take $N \in \mathbf{Nil}_R$ with nilpotent divided power structures $\gamma_n : N \to N$. Let G be a strictly pro-representable formal group. Then we have an isomorphism*

$$\exp_N : \operatorname{Lie}G(N) \xrightarrow{\simeq} G(N)$$

*functorial in $(N, \{\gamma_n\})$ and G. This exponential map is called the **Grothendieck-Messing exponential**.*

Proof. The proof is the same with the proof of Proposition 1.24, except that we have to replace the isomorphism (1.6) by Lemma 1.47. □

Let $G : \mathbf{Nil}_R \to \mathbf{Ab}$ be a strictly pro-representable formal group such that $G = \operatorname{Spf}C$. Given $N \in \mathbf{Nil}_R$, and divided powers $\gamma = \{\gamma_n\}$ on N. In Proposition 1.48, we showed that we have the Grothendieck-Messing exponential isomorphism $\operatorname{Lie}G(N) \to G(N)$.

Let us be given a surjective homomorphism $\rho : S \twoheadrightarrow R$ of rings with 1. Let $\mathfrak{a} = \operatorname{Ker}\rho$. Suppose $\mathfrak{a}$ has pd structure $\delta = (\delta_n)$. For any $N \in \mathbf{Nil}_S$, we know that $\mathfrak{a} \otimes_S N$ has pd structure $\tilde{\delta}_m(a \otimes x) = \delta_m(a) \otimes x^m$. Since N is nilpotent, $\tilde{\delta}$ is nilpotent. We have an exact sequence

$$0 \to \mathfrak{a} \to S \to R \to 0,$$

hence

$$\mathfrak{a} \otimes_S N \to N \to N \otimes_S (S/\mathfrak{a}) = N/\mathfrak{a}N \to 0.$$

Let G be a strictly pro-representable formal group. Since G is exact, we have the exact sequence

$$G(\mathfrak{a} \otimes_S N) \longrightarrow G(N) \xrightarrow{\rho_N} G(N/\mathfrak{a}N) \longrightarrow 0 \tag{1.8}$$

Note that we have an isomorphism $\operatorname{Lie}G(\mathfrak{a} \otimes_S N) \cong G(\mathfrak{a} \otimes_S N)$. The sequence (1.7) is also left exact if N is a flat S-module.

Fix a prime number p once and for all.

Lemma 1.49. *Let R be a ring with 1. Let G be a strictly pro-representable formal group over R. Given $N \in \mathbf{Nil}_R$. Assume*
(i) $x^p = 0$ *for each* $x \in N$;
(ii) $p \cdot N = 0$.
Then $p \cdot G(N) = 0$.

Proof. Let $H = (\mathbb{G}_m H_G)^\wedge$. We know that $G \hookrightarrow H$. So it suffice to show that $p \cdot H(N) = 0$. Consider $1 + y \in H(N) = (1 + H_G^+ \otimes N)^\times$ with $y \in H_G^+ \otimes N$. Then $(1+y)^p = 1 + y^p = 1$ by the assumptions. We are done. □

In the sequence of (1.7), if we assume $p \cdot \mathfrak{a} = 0$, then the divided power structure shows $a^p = p!\delta_p(a) = 0$ for any $a \in \mathfrak{a}$. So condition (i) in Lemma 1.35 is automatically satisfied. Hence $p \cdot G(\mathfrak{a} \otimes_S N) = 0$. In particular, $p \cdot \operatorname{Ker}(\rho_N) = 0$.

Definition 1.50. *Let R be a commutative ring with 1 such that p is nilpotent in R. Let G be a formal group over R such that $G \cong \hat{\mathbb{A}}_R^d$. Consider the multiplication by p map $p_G : G \to G$ (i.e., for any $N \in \mathbf{Nil}_R$, $x \in G(N)$, $p_G(x) = p \cdot x$). Then p_G is defined by formal power series $f_1(X_1, \ldots, X_d), \ldots, f_d(X_1, \ldots, X_d) \in$*

*$R[[X_1,\ldots,X_d]]$ with $f_i(\underline{0})=\underline{0}$. The formal group G is called a **p-divisible** (formal) group if each X_i is nilpotent in*

$$R[[X_1,\ldots,X_d]]/(f_1(X_1,\ldots,X_d),\ldots,f_d(X_1,\ldots,X_d)).$$

Example: Let K be a field of a characteristic p. Let A be an abelian variety over K. Then the *completion* of A along the origin

$$\hat{A}(N)=\mathrm{Ker}(A(K\oplus N)\to A(K))$$

is a p-divisible group.

Theorem 1.51 (Weierstrass Preparation Theorem)**.** *Assume that G is a p-divisible group. Notations as in Definition* 1.50*. Then the homomorphism*

$$R[[X_1,\ldots,X_d]]\to R[[X_1,\ldots,X_d]]$$
$$X_i\mapsto f_i$$

is faithfully flat, finite, and

$$R[[X_1,\ldots,X_d]]/(f_1(X_1,\ldots,X_d),\ldots,f_d(X_1,\ldots,X_d))$$

is a finite projective R-module.

Recall that a ring homomorphism $A\to B$ is called *faithfully flat* if any sequence of A-modules

$$0\to M\to N\to P\to 0,$$

is exact if and only if

$$0\to M\otimes_A B\to N\otimes_A B\to P\otimes_A B$$

is exact. The proof of Theorem 1.51 can be found in [Z].

Corollary 1.52. *The kernel $G(p)$ of p_G is* $\mathrm{Spec}R[[X_1,\ldots,X_d]]/(f_1,\ldots,f_d)$*. This $G(p)$ is a finite flat group scheme over R.*

Note if $\rho : A\to B$ is a faithfully flat morphism of rings, then ρ is injective. In fact, by faithful flatness, it suffice to show $\rho\otimes_A B : A\otimes_A B\to B\otimes_A B$ is injective. But $\rho\otimes_A B$ has a section $b_1\otimes b_2\mapsto b_1b_2$, hence it is injective.

Corollary 1.53. *Let G be a p-divisible group. Then p_G is "surjective" in the following sense. Let $F:\mathbf{Nil}\to\mathbf{Ab}$ be any left exact functor. Given*

$$\begin{tikzcd} G \arrow[r, "p_G"] & G \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & F \end{tikzcd}$$

such that $\alpha\cdot p_G=\beta\cdot p_G$, then $\alpha=\beta$.

Proof. For simplicity, we write $\underline{X}$ for $(X_1,\ldots,X_d)$ and $\underline{f}=(f_1,\ldots,f_d)$. Note that

$$\begin{aligned}\mathrm{Hom}(G,F)&=\varprojlim_m \mathrm{Hom}(\mathrm{Spec}R[[\underline{X}]]/(\underline{X})^m,F)\\ &=\varprojlim_m F(R[[\underline{X}]]/(\underline{X})^m),\end{aligned}$$

where the last equality follows from Yoneda's Lemma. So given $\alpha,\beta\in\mathrm{Hom}(G,F)$, there are two projective systems $\{\alpha_m\},\{\beta_m\}$ with $\alpha_m,\beta_m\in F(R[[\underline{X}]]/(\underline{X})^m)$. Since

$$p_G^*:R[[\underline{X}]]\to R[[\underline{X}]]$$

$$X_i \mapsto f_i$$

is faithfully flat,

$$R[[\underline{X}]]/(\underline{X})^m \to R[[\underline{X}]]/(\underline{f})^m$$

is also faithfully flat, hence injective. Since F is left exact, we have an injective map

$$F(R[[\underline{X}]]/(\underline{X})^m) \to F(R[[\underline{X}]]/(\underline{f})^m).$$

This map is induced by p_G^*, so it maps α_m to $\alpha_m \circ p_G$. The assumption means that $\alpha_m \circ p_G = \beta_m \circ p_G$. The injectivity implies $\alpha_m = \beta_m$, for any m. Hence $\alpha = \beta$. □

Lemma 1.54. *If G is a p-divisible group over S, then $f_\bullet G$ is a p-divisible group over R.*

Proof. Suppose that as an S-functor, the multiplication by p map $p_G : G \to G$ is defined by $(f_1, \ldots, f_d)$ with $f_i \in S[[X_1, \ldots, X_d]]$. Let $\bar{f}_i \in R[[X_1, \ldots, X_d]]$ be the image of f_i under the map $f : S \to R$. Then $p_{f_\bullet G} : f_\bullet G \to f_\bullet G$ is defined by $(\bar{f}_1, \ldots, \bar{f}_d)$. Now the assertion is clear. □

Lemma 1.55 (Rigidity Lemma for p-Divisible Groups)**.** *Let $f : S \to R$ be a surjective homomorphism, denote its kernel by $\mathfrak{a}$. Assume that there are natural numbers n, m such that $p^n S = 0$ and $a^{p^m} = 0$ for all $a \in \mathfrak{a}$. Let G be a p-divisible group over S. Let F be a strictly pro-representable formal group. Then the map*

$$\mathrm{Hom}_S(G, F) \to \mathrm{Hom}_R(f_\bullet G, f_\bullet F)$$

$$\alpha \mapsto f_\bullet \alpha$$

is injective, i.e., if $\alpha, \beta : G \to F$ are two morphisms of group functors such that $f_\bullet \alpha = f_\bullet \beta$, then $\alpha = \beta$.

Proof. We first assume $m = n = 1$, i.e., $p \cdot \mathfrak{a} = 0$ and $a^p = 0$ for any $a \in \mathfrak{a}$. Given any $N \in \mathbf{Nil}_S$, we have a commutative diagram (note that F is an exact functor)

$$\begin{tikzcd}
 & & G(N) \arrow[r] \arrow[dl, dashed, "\alpha_N-\beta_N"'] \arrow[d, "\alpha_N-\beta_N"] & G(N/\mathfrak{a}N) \arrow[d, "\alpha_{N/\mathfrak{a}N}-\beta_{N/\mathfrak{a}N}"] \\
0 \arrow[r] & F(\mathfrak{a}N) \arrow[r] & F(N) \arrow[r] & F(N/\mathfrak{a}N)
\end{tikzcd}$$

Since $N/\mathfrak{a}N$ is an $S/\mathfrak{a} = R$-algebra, then by assumption, $\alpha_{N/\mathfrak{a}N} = \beta_{N/\mathfrak{a}N}$. Since the above diagram is commutative, $\alpha_N - \beta_N$ factors through $F(\mathfrak{a}N)$. Because $p \cdot \mathfrak{a}N = 0$ and for any $x \in \mathfrak{a}N$ we have $x^p = 0$, we conclude that $p \cdot F(\mathfrak{a}N) = 0$ by Lemma 1.49. So $p \cdot \alpha_N = p \cdot \beta_N$ for any N. Since α_N is a group homomorphism, we have $p \cdot \alpha_N(x) = \alpha_N(p_G(x))$. Hence $\alpha_N \circ p_G = \beta_N \circ p_G$ for any N. So $\alpha \circ p_G = \beta \circ p_G$. Now by Corollary 1.53, we get $\alpha = \beta$. This completes the proof for $m = n = 1$.

For $m = 1$ and general n, we can reduce the lemma to the case $m = n = 1$ by considering the following sequence

$$S = S/p^n S \to S/p^{n-1} S \to \cdots \to S/p\mathfrak{a} \to R.$$

For a general m, put $\mathfrak{a}_r = \langle x^{p^r} | x \in \mathfrak{a} \rangle$. The lemma reduces to the above case on considering

$$S = S/\mathfrak{a}_m \to \cdots \to S/\mathfrak{a}_1 \to S/\mathfrak{a}_0.$$

□

Lemma 1.56. *Suppose $f : S \to R$ is faithfully flat. Then for any S-module M, we have an exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] & M \otimes_S R \arrow[r, "\pi_1 - \pi_2"] & M \otimes_S R \otimes_S R \end{tikzcd} ,$$

where the map $M \to M \otimes_S R$ is defined by $m \mapsto m \otimes 1$ and $\pi_1(m \otimes r) = m \otimes r \otimes 1, \pi_2(m \otimes r) = m \otimes 1 \otimes r$.

A proof can be found in [Z]. It is omitted here.

Proposition 1.57. *Suppose that $f : S \to R$ is faithfully flat and $p \cdot S = 0$. Assume that $r^p \in S$ for any $r \in R$ (note that this makes sense, since f is injective by faithful flatness). Let G be a p-divisible group over S. Let F be a strictly pro-representable formal group over S. Then the map*

$$\mathrm{Hom}_S(G, F) \to \mathrm{Hom}_R(f_\bullet G, f_\bullet F)$$

$$\alpha \mapsto f_\bullet \alpha$$

is bijective.

Proof. We first show the surjectivity of the given map. To show the surjectivity, given a homomorphism $\tilde{\alpha} : f_\bullet G \to f_\bullet F$, we want to construct a homomorphism $\alpha : G \to F$ such that $f_\bullet \alpha = \tilde{\alpha}$.

Let π_1, π_2 be the homomorphisms $R \to R \otimes_S R$ defined by $\pi_1(r) = r \otimes 1, \pi_2(r) = 1 \otimes r$. Let $G_{R \otimes_S R} = (\pi_1 f)_\bullet G = (\pi_2 f)_\bullet G$ (the last equality holds, because, $f(s) \otimes 1 = 1 \otimes f(s)$ for $s \in S$, i.e., the S-module structures on $R \otimes_S R$ defined by $\pi_1 f$ and $\pi_2 f$ are the same). Define $F_{R \otimes_S R}$ similarly. Let $\tilde{\alpha}_i = (\pi_i)_\bullet \tilde{\alpha} : G_{R \otimes_S R} \to F_{R \otimes_S R}$ for $i = 1, 2$.

Claim: $\tilde{\alpha}_1 = \tilde{\alpha}_2$.
Consider the multiplication map $m : R \otimes_S R \to R$ defined by $m(r_1 \otimes r_2) = r_1 r_2$. By definition, $m\pi_1 = m\pi_2 = \mathrm{id}_R$. So $\tilde{\alpha} = (m\pi_i)_\bullet \tilde{\alpha} = m_\bullet \tilde{\alpha}_i$. In particular, we have $m_\bullet \tilde{\alpha}_1 = m_\bullet \tilde{\alpha}_2$. This means $\tilde{\alpha}_1$ and $\tilde{\alpha}_2$ have the same image under the map

$$\Phi : \mathrm{Hom}_{R \otimes_S R}(G_{R \otimes_S R}, F_{R \otimes_S R}) \to \mathrm{Hom}_R(m_\bullet(G_{R \otimes_S R}), m_\bullet(F_{R \otimes_S R})),$$

Hence to prove the claim, it suffice to show Φ is injective. Let $\mathfrak{a} = \mathrm{Ker}(m)$. Note that m is surjective. Hence by Lemma 1.55, it suffice to show that $p \cdot \mathfrak{a} = 0$ and $a^p = 0$ for any $a \in \mathfrak{a}$. Now $p \cdot \mathfrak{a} = 0$ holds by assumption. It is easy to see that $\mathfrak{a}$ is generated by $r_1 \otimes r_2 - r_2 \otimes r_1, r_1, r_2 \in R$. Since $r^p \in S$ for any $r \in R$, we have

$$(r_1 \otimes_S r_2 - r_2 \otimes_S r_1)^p = r_1^p \otimes_S r_2^p - r_2^p \otimes_S r_1^p = 0.$$

We get the claim.

For any $N \in \mathbf{Nil}_S$, by Lemma 1.56, we have an exact sequences

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & N \otimes_S R \arrow[r, "\pi_1 - \pi_2"] & N \otimes_S R \otimes_S R \end{tikzcd} .$$

Applying the exact functors G and F, we get the following diagram with exact rows,

$$\begin{tikzcd}
0 \arrow[r] & G(N) \arrow[r] \arrow[d, dashed, "\alpha"] & G(N \otimes_S R) \arrow[r, "\pi_1-\pi_2"] \arrow[d, "\tilde{\alpha}"] & G(N \otimes_S R \otimes_S R) \arrow[d, "\tilde{\alpha}_1=\tilde{\alpha}_2"] \\
0 \arrow[r] & F(N) \arrow[r] & F(N \otimes_S R) \arrow[r, "\pi_1-\pi_2"] & F(N \otimes_S R \otimes_S R)
\end{tikzcd}$$

It is easy to see that

$$\pi_i \circ \tilde{\alpha} = \tilde{\alpha}_i \circ \pi_i,$$

so we get the commutativity of the right hand square. Then it is follows that there is an $\alpha : G(N) \to F(N)$ such that the diagram is commutative. So we get the surjectivity.

If we have two $\alpha, \alpha' \in \mathrm{Hom}_S(G, F)$ such that $f_\bullet \alpha = f_\bullet \alpha' = \tilde{\alpha}$, then it is easy to see $\alpha = \alpha'$ by the above commutative diagram. We are done. □

Corollary 1.58. *Let k be a field of characteristic p. Put $l = k^{1/p}$. Let G (resp.F) be a p-divisible formal group (resp. a strictly pro-representable formal group) over k. Then*

$$\mathrm{Hom}_k(G, F) \to \mathrm{Hom}_l(G_l, F_l)$$

is a bijection, where $G_l = i_\bullet G$, $i : k \to l$ is the inclusion.

This is a direct consequence of Corollary 1.57.

Remark: This corollary is false if G is not a p-divisible group. For example, take $G = F = \hat{\mathbb{G}}_a$. Since $p_G = 0$, $\hat{\mathbb{G}}_a$ is not a p-divisible group. It is easy to see the corollary is false by Proposition 1.22.

In the above remark, we saw that $\hat{\mathbb{G}}_a$ is not a p-divisible group. We claim that $G = \hat{\mathbb{G}}_m$ is a p-divisible group over R if $p \cdot R = 0$. For any $N \in \mathbf{Nil}_R$, any $n \in N$, $(1+n)^p = 1 + n^p$. Hence, the multiplication p_G is defined by $f(X) = X^p \in R[[X]]$. Then X is nilpotent in $R[[X]]/(X^p)$. Hence $\hat{\mathbb{G}}_m$ is a p-divisible group. In particular, if k is a field of characteristic p, then $\hat{\mathbb{G}}_m$ is a p-divisible group over k. Generally, we have

Proposition 1.59. *Let k be a field of characteristic p. If G is a formal group such that $G \cong \hat{\mathbb{A}}^1$ and p_G is nontrivial, then G is a p-divisible group.*

Proof. Suppose p_G is defined by a power series $f(X) \in k[[X]]$. Since p_G is nontrivial, $f(X)$ is non-zero. We can write

$$f(X) = X^h(a_0 + a_1 X + \cdots), \quad a_i \in k, \quad a_0 \neq 0.$$

Then $a_0 + a_1 X + \cdots$ is a unit in $k[[X]]$. Hence

$$k[[X]]/(f(X)) \cong k[[X]]/(X^h),$$

and X is nilpotent in $k[[X]]/(f(X))$. □

2. Witt Rings and Display

Fix a prime p once and for all. Consider the following polynomials with coefficients in $\mathbb{Z}$,

$$\begin{aligned}&\mathbb{W}_0 = X_0,\\ &\mathbb{W}_1 = X_0^p + pX_1,\\ &\cdots\cdots\\ &\mathbb{W}_n = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^nX_n.\end{aligned}$$

Lemma 2.1. *Let R be a commutative ring with 1 such that p is invertible in R. Then for any $n \geq 0$, the map*

$$(\mathbb{W}_0, \ldots, \mathbb{W}_n) : R^{n+1} \to R^{n+1},$$

$$(x_0, \ldots, x_n) \mapsto (\mathbb{W}_0(x_0), \mathbb{W}_1(x_0, x_1), \ldots, \mathbb{W}_n(x_0, \ldots, x_n))$$

is bijective. The R^{n+1} on the left inherits a new ring structure from the usual ring structure of R^{n+1} on the right. Write $W_n(R)$ for this new ring structure.

The lemma is easy to see.

In the ring $W_n(R)$, we can write the additive law as

$$(2.1)\quad (X_0, \ldots, X_n) +_W (Y_0, \ldots, Y_n) = (S_0(X_0, Y_0), \ldots, S_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n)).$$

Here the subscript W means that $+_W$ is the additive law in $W_n(R)$ and S_i are polynomials in $\mathbb{Z}[\frac{1}{p}][X_0, \ldots, X_i, Y_0, \ldots, Y_i]$ which are uniquely determined by

$$(2.2)\qquad \mathbb{W}_i(S_0, \ldots, S_i) = \mathbb{W}_i(X_0, \ldots, X_i) + \mathbb{W}_i(Y_0, \ldots, Y_i), \quad 0 \leq i \leq n.$$

Similarly we have polynomials $P_i \in \mathbb{Z}[\frac{1}{p}][X_0, \ldots, X_i, Y_0, \ldots, Y_i]$ such that

$$(2.3)\qquad (X_0, \ldots, X_n) \times_W (Y_0, \ldots, Y_N) = (P_0, \ldots, P_n).$$

Here $\times_F$ means the multiplicative law in $W_n(R)$.

Next, we want to show that the polynomials S_i, P_i defined above have coefficients in $\mathbb{Z}$. Consequently, for any ring R, we can define a new ring structure on R^{n+1} by formulas (2.1) and (2.3) directly.

Proposition 2.2. *Let R be a ring without p torsion. Assume that there is a ring homomorphism $\tau : R \to R$ such that $\tau(x) \equiv x^p (\mathrm{mod}\ p)$. Consider the map*

$$(\mathbb{W}_0, \ldots, \mathbb{W}_n) : R^{n+1} \to R^{n+1}$$

defined as in Lemma 2.1. Consider $(u_0, \ldots, u_n) \in R^{n+1}$. Then $(u_0, \ldots, u_n)$ is in the image of the map $(\mathbb{W}_0, \ldots, \mathbb{W}_n)$ if and only if $\tau(u_i) \equiv u_{i+1} (\mathrm{mod}\ p^{i+1})$ for $0 \leq i \leq n-1$.

Proof. First we claim that $\tau(x^{p^m}) \equiv x^{p^{m+1}} (\mathrm{mod}\ p^{m+1})$ for any $m \geq 0$.

For $m = 0$ the claim follows from the assumption. For $m = 1$, $\tau(x^p) = \tau(x)^p \equiv x^{p^2} (\mathrm{mod}\ p^2)$. The general case can be deduced by induction.

Assume there are $x_i \in R$ such that $u_m = \mathbb{W}_m(x_0, \ldots, x_m)$. Then

$$\tau(u_m) - u_{m+1}$$

$= \tau(x_0^{p^m} + px_1^{p^{m-1}} + \cdots + p^m x_m) - (x_0^{p^{m+1}} + px_1^{p^m} + \cdots + p^m x_m^p + p^{m+1}x_{m+1})$.
By the above claim, it is easy to see if $i \leq m$, we have

$$\tau(p^i x^{p^{m-i}}) \equiv p^i(x^{p^{m-i+1}})(\text{mod } p^{m+1}.)$$

Hence $\tau(u_m) \equiv u_{m+1}(\text{mod } p^{m+1})$.

Conversely, suppose we are given $(u_0, \ldots, u_n) \in R^{n+1}$ such that

$$\tau(u_m) \equiv u_{m+1}(\text{mod } p^{m+1}).$$

We will construct x_i by induction such that $u_m = \mathbb{W}_m(x_0, \ldots, x_m)$. First x_0 must be u_0. Suppose that we defined $x_0, \ldots, x_{m-1}$. We have seen that $\tau(u_{m-1}) \equiv (x_0^{p^m} + px_1^{p^{m-1}} \cdots + p^{m-1}x_{m-1})(\text{mod } p^m)$. So $u_m - (x_0^{p^m} + px_1^{p^{m-1}} \cdots + p^{m-1}x_{m-1}) \equiv u_m - \tau(u_{m-1}) \equiv 0(\text{mod } p^m)$. So there is an $x_m \in R$ such that $u_m = x_0^{p^m} + px_1^{p^{m-1}} + \cdots + p^{m-1}x_{m-1} + p^m x_m$. We are done. □

Corollary 2.3. *The polynomials S_i defined by* (2.1) *or* (2.2) *have coefficients in* $\mathbb{Z}$*.*

Proof. Let $A = \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$. Then A has no p torsion. We first justify that S_i is uniquely determined by (2.2). In fact, $A \subset A \otimes \mathbb{Z}[\frac{1}{p}]$, $W_n(A) \subset W_n(A) \otimes \mathbb{Z}[\frac{1}{p}]$ and $(\mathbb{W}_0, \ldots, \mathbb{W}_n) : W_n(A \otimes \mathbb{Z}[\frac{1}{p}]) \to (A \otimes \mathbb{Z}[\frac{1}{p}])^{n+1}$ is an isomorphism. So $(\mathbb{W}_0, \ldots, \mathbb{W}_n) : W_n(A) \to A^{n+1}$ is injective. So S_i is uniquely determined by the formula (2.2).

Define a ring homomorphism $\tau : A \to A$ by $\tau(X_i) = X_i^p, \tau(Y_i) = Y_i^p$. It is easy to see that $\tau(f) \equiv f^p(\text{mod } p)$.

Now let $u_m = \mathbb{W}_m(X_0, \ldots X_m) + \mathbb{W}_m(Y_0, \ldots, Y_m)$. Since S_i is uniquely determined by the formula (2.2), it suffice to show that $(u_0, \ldots, u_n)$ is in the image of $(\mathbb{W}_0, \ldots, \mathbb{W}_n) : W_n(A) \to A^{n+1}$. By Proposition 2.2, we need to check that $\tau(u_m) \equiv u_{m+1}(\text{mod } p^{m+1})$. This is obvious from

$$\tau(\mathbb{W}_m(\underline{X})) \equiv \mathbb{W}_{m+1}(\underline{X})(\text{mod } p^{m+1}).$$

□

We can similarly prove that P_i has coefficients in $\mathbb{Z}$.

The above results are summarized in

Theorem 2.4. *The polynomials defined by* (2.1) *and* (2.3) *have coefficients in* $\mathbb{Z}$*. For any ring R* (*possibly without* 1), *the set R^{n+1} equipped with addition and multiplication defined by* (2.1) *and* (2.3) *forms a ring $W_n(R)$.*

Proof. We have to show that the addition and multiplication satisfy the associative law and distributive law. But these laws are just identities in S_i, P_i. These identities hold if p is invertible in R. Since S_i, P_i have coefficients in $\mathbb{Z}$, these identities are independent of the choice of R. We are done. □

Definition 2.5. *Let $W(R)$ be the set $\{(x_0, \ldots, x_n, \ldots)|x_i \in R\}$ equipped with the addition and multiplication defined by* (2.1), (2.3)*. Then $W(R)$ is a ring. It is called the* ***Witt ring*** *of R.*

By definition,

$$\mathbb{W} = (\mathbb{W}_n; n \geq 0) : W(R) \to \prod_0^\infty R$$

is a ring isomorphism. For any n, we have a map

$$W(R) \to W_n(R)$$
$$(x_0, x_1, \dots) \mapsto (x_0, \dots, x_n).$$

It is a ring homomorphism, by definition.

Lemma 2.6. *The map*

$$^V : W(R) \to W(R)$$
$$^V(x_0, x_1, \dots) = (0, x_0, x_1, \dots)$$

is a group endomorphism of the additive group $(W(R), +)$. *It is called the* ***Verschiebung morphism*** *of* $W(R)$.

Proof. For any $\xi \in W(R)$, it follows from the definition that $\mathbb{W}_n(^V\xi) = 0$ if $n = 0$ and $\mathbb{W}_n(^V\xi) = p\mathbb{W}_{n-1}(\xi)$ if $n > 0$. Using the fact that $\mathbb{W}_n : W_n(R) \to \prod_0^n R$ is a ring homomorphism, it is easy to see that

$$\mathbb{W}_n(^V\xi + {^V\eta}) = \mathbb{W}_n(^V(\xi + \eta)), \quad \forall n \geq 0. \tag{2.4}$$

If R has no p torsion, we deduce that $^V\xi + {^V\eta} = {^V(\xi + \eta)}$ from (2.4), since $\mathbb{W} : W(R) \to \prod_0^\infty R$ is injective.

For a general R, take a surjective ring homomorphism $\pi : S \twoheadrightarrow R$ with S which has no p torsion. Then $W(\pi) : W(S) \to W(R)$ is a surjective ring homomorphism and π commutes with ^{V}. Given $\xi, \eta \in W(R)$, let $\tilde{\xi}, \tilde{\eta} \in W(S)$ be such that $\pi(\tilde{\xi}) = \xi, \pi(\tilde{\eta}) = \eta$. By the above discussion, we know that $^V\tilde{\xi} + {^V\tilde{\eta}} = {^V(\tilde{\xi} + \tilde{\eta})}$. Applying π to both sides and since π commutes with V we get $^V\xi + {^V\eta} = {^V(\xi + \eta)}$. □

Proposition 2.7. *The construction* $R \mapsto W(R)$ *has the following properties*:
(*a*) *if* $f : R \to S$ *is a ring homomorphism, then the map*

$$W(f) : W(R) \longrightarrow W(S),$$
$$(x_0, x_1, \dots) \mapsto (f(x_0), f(x_1), \dots)$$

is also a ring homomorphism;
(*b*) *for every* n, *the map*

$$\mathbb{W}_n : W(R) \longrightarrow R$$
$$(x_0, x_1, \dots) \mapsto x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^{n-1}x_{n-1}^p + p^n x_n$$

is a ring homomorphism.

Lemma 2.8. *Define a map* $[\cdot] : R \to W(R)$ *by* $[x] = (x, 0, 0, \dots)$. *Then*
(1) $[x][y] = [xy]$ *for any* $x, y \in R$.
(2) $(x_0, x_1, \dots) = \sum_{n=0}^\infty {^{V^n}}[x_n]$.

Proof. (1) If R has no 1, we can embed R into $\mathbb{Z} \oplus R$. Then we can assume R has 1. Consider the ring homomorphism $f : \mathbb{Z}[X, Y] \to R$ defined by $X \mapsto x, Y \mapsto y$. Applying the functor W, we get a ring homomorphism $W(f) : W(\mathbb{Z}[X, Y]) \to W(R)$. If we know that $[X][Y] = [XY]$ in $W(\mathbb{Z}[X, Y])$, then applying the homomorphism $W(f)$ we get $[x][y] = [xy]$.

Consider the injective map $\mathbb{W} : W(\mathbb{Z}[X,Y]) \to \prod_0^\infty \mathbb{Z}[X,Y]$. By definition, $\mathbb{W}_n([X]) = X^{p^n}$. So $\mathbb{W}_n([X][Y]) = \mathbb{W}_n([XY])$. Now by the injectivity of $\mathbb{W}$, we deduce that $[X][Y] = [XY]$. We are done.

(2) Using the same method as in the proof of Lemma 2.6, we can assume R has no p torsion. Then it suffice to show

$$\mathbb{W}_n((x_0, x_1, \dots)) = \mathbb{W}_n\left(\sum_{i=0}^{\infty} {}^{V^i}[x_i]\right), \quad \forall n \geq 0. \tag{2.5}$$

Since $\mathbb{W}_n$ is a ring homomorphism, we have

$$\mathbb{W}_n(\sum_{i=0}^{\infty} {}^{V^i}[x_i]) = \sum_i \mathbb{W}_n({}^{V^i}[x_i]).$$

We saw in the proof of Lemma 2.6 that $\mathbb{W}_n({}^V\xi) = 0$ if $n = 0$; $\mathbb{W}_n({}^V\xi) = p\mathbb{W}_{n-1}(\xi)$ if $n > 0$. So if $n = 0$, both sides of (2.5) are equal to x_0. If $n > 0$, $\mathbb{W}_n({}^{V^i}[x_i]) = p^i\mathbb{W}_{n-i}([x_i]) = p^i x_i^{p^{n-i}}$ if $i \leq n$ and $\mathbb{W}_n({}^{V^i}[x_i]) = 0$ for $i > n$. Then it is easy to check the equality of (2.5). □

Definition 2.9. *For any $\xi = (x_0, x_1, x_2, \dots) \in W(R)$, by* (2) *of Lemma* 2.8 *we have $\xi = [x_0] + {}^V\eta$ with $\eta = (x_1, x_2, \dots)$. Define the* ***Frobenius map*** ${}^F : W(R) \to W(R)$ *by*

$${}^F\xi = [x_0^p] + p\eta.$$

Lemma 2.10. *The Frobenius map is a ring homomorphism.*

Proof. By definition of ^{F}, we have

$$\begin{aligned}\mathbb{W}_n({}^F\xi) &= \mathbb{W}_n([x_0^p]) + p\mathbb{W}_n(\eta)\\ &= x_0^{p^{n+1}} + p(x_1^{p^n} + px_2^{p^{n-1}} + \cdots + p^n x_{n+1}) = \mathbb{W}_{n+1}(\xi).\end{aligned}$$

So $\mathbb{W}_n({}^F\xi + {}^F\xi') = \mathbb{W}_n({}^F\xi) + \mathbb{W}_n({}^F\xi') = \mathbb{W}_{n+1}(\xi) + \mathbb{W}_{n+1}(\xi') = \mathbb{W}_{n+1}(\xi + \xi') = \mathbb{W}_n({}^F(\xi + \xi'))$. Similarly, $\mathbb{W}_n({}^F\xi{}^F\xi') = \mathbb{W}_n({}^F(\xi\xi'))$. As in the proofs of Lemmas 2.6 and 2.8, we can assume that R has no p torsion. Then the injectivity of $\mathbb{W}$ implies that ${}^F\xi + {}^F\xi' = {}^F(\xi + \xi')$ and ${}^F\xi{}^F\xi' = {}^F(\xi\xi')$. □

Lemma 2.11. *We have*
(a) $F \circ V = p$;
(b) $({}^V\xi) \cdot \eta = {}^V(\xi \cdot {}^F\eta)$ *for* $\xi, \eta \in W(R)$.

Proof. (a) Since $\mathbb{W}_n({}^{F\circ V}\xi) = \mathbb{W}_{n+1}({}^V\xi) = p\mathbb{W}_n(\xi)$, we are done since we can assume R has no p torsion.
(b) We have $\mathbb{W}_n(({}^V\xi)\cdot\eta) = \mathbb{W}_n({}^V\xi)\mathbb{W}_n(\eta) = p\mathbb{W}_{n-1}(\xi)\mathbb{W}_n(\eta)$ for $n \geq 1$ and 0 if $n = 0$. On the other hand, if $n \geq 1$, $\mathbb{W}_n({}^V(\xi \cdot {}^F\eta)) = p\mathbb{W}_{n-1}(\xi \cdot {}^F\eta) = p\mathbb{W}_{n-1}(\xi)\mathbb{W}_n(\eta)$. If $n = 0$, $\mathbb{W}_n({}^V(\xi \cdot {}^F\eta)) = 0$. We are done. □

Lemma 2.12. *Given $x \in R$, put $\xi = p[x] - {}^V[x^p]$. Then all components of ξ are in $p \cdot R$, i.e., $\xi \in W(p \cdot R)$.*

Proof. Without loss of generality, we can assume that R has 1 and has no p torsion. It is easy to check that $\mathbb{W}_0(\xi) = px$, and for $n \geq 1$ we have

$$\mathbb{W}_n(\xi) = px^{p^n} - \mathbb{W}_n({}^V[x^p]) = px^{p^n} - p\mathbb{W}_{n-1}([x^p]) = 0.$$

Write $\xi = (\xi_0, \dots, \xi_n, \dots)$. We will show that $p|\xi_i$ by induction. We know $px = \mathbb{W}_0(\xi) = \xi_0$. So $p|\xi_0$. Suppose for $n \geq 1$, we have shown $p|\xi_0, \dots, \xi_{n-1}$. Then $0 = \mathbb{W}_n(\xi) = \xi_0^{p^n} + p\xi_1^{p^{n-1}} + \cdots + p^{n-1}\xi_{n-1}^p + p^n\xi_n$. So by the induction assumption, $p^{n+1}|p^n\xi_n$. We are done. □

Proposition 2.13. *Let R be a ring such that $p \cdot R = 0$. Then*

$$ {}^F(x_0, x_1, \dots) = (x_0^p, x_1^p, \dots). $$

Proof. By Lemma 2.8 (2) we have

$$ (x_0, x_1, \dots) = \sum_{n=0}^{\infty} {}^{V^n}[x_n]. $$

Hence

$$ {}^F(x_0, x_1, \dots) = {}^F[x_0] + \sum_{n=1}^{\infty} {}^{FV^n}[x_n]. $$

Note that for $n \geq 1$ we have $FV^n = pV^{n-1}$ and V is an endomorphism of the additive group of $W(R)$, hence commutes with p. By definition ${}^F[x_0] = [x_0^p]$, consequently

$$ {}^F(x_0, x_1, \dots) = [x_0^p] + \sum_{n=1}^{\infty} {}^{V^{n-1}}p[x_n]. $$

Since $p \cdot R = 0$, we have $p[x_n] = {}^V[x_n^p]$ by Lemma 2.12. So we get

$$ {}^F(x_0, x_1, \dots) = [x_0^p] + \sum_{n=1}^{\infty} {}^{V^n}[x_n^p] = (x_0^p, x_1^p, \dots). $$

The last equality follows from Lemma 2.8 (2). □

Example 2.13.1. In the ring $W(\mathbb{F}_p)$, the Frobenius is the identity map by Proposition 2.13 since for $x \in \mathbb{F}_p$ we have $x^p = x$.

Recall we have fixed a prime number p.

Definition 2.14. *A ring R is called a* ***perfect*** *if $p \cdot R = 0$ and the map $R \to R$, $x \mapsto x^p$, is a bijection.*

Proposition 2.15. *Let R be a perfect ring. Let A be a ring with an ideal $\mathfrak{a}$. Suppose there is a positive integer c such that $a^c = 0$ for every $a \in \mathfrak{a}$ and $p^c = 0$ in A. Then for any ring homomorphism $\alpha : R \to A/\mathfrak{a}$, there is a unique ring homomorphism $\beta : W(R) \to A$ such that the following diagram is commutative*

$$\begin{tikzcd}
W(R) \arrow[r, dashed, "\beta"] \arrow[d, "\mathbb{W}_0"] & A \arrow[d, "\pi"] \\
R \arrow[r, "\alpha"] & A/\mathfrak{a}
\end{tikzcd}$$

where $\pi : A \to A/\mathfrak{a}$ is the canonical projection.

Proof. Consider $\mathbb{W}_n : W(A) \to A$, $\mathbb{W}_n(x_0, \dots, x_n, \dots) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n$. By our assumption on the integer c, it is clear that for n large enough, $\mathbb{W}_n(x_0, \cdots, x_n, \cdots) = 0$ if $x_i \in \mathfrak{a}$. We fix one such n. Then the map

$$ \mathbb{W}_n : W(A) \to A $$

factors though $W(A/\mathfrak{a})$, i.e., we have the following commutative diagram

$$\begin{tikzcd}
W(A) \arrow[r, "\mathbb{W}_n"] \arrow[d, "W(\pi)"] & A \arrow[d, "\pi"] \\
W(A/\mathfrak{a}) \arrow[r, "\mathbb{W}_n"] \arrow[ur, dashed, "\tilde{\mathbb{W}}_n"] & A/\mathfrak{a}
\end{tikzcd}$$

The lower triangular is commutative because $\mathbb{W}_n : W(A/\mathfrak{a}) \to A/\mathfrak{a}$ is defined by the same formula. Since $p \cdot R = 0$, the Frobenius map ${}^{F} : W(R) \to W(R)$ is defined by ${}^{F}(r_0, r_1, \dots) = (r_0^p, r_1^p, \dots)$ by Proposition 2.13. It is an isomorphism because R is perfect. So we can consider ${}^{F^{-n}}$. We have the following commutative diagram

$$\begin{tikzcd}
W(R) \arrow[r, "{}^{F^{-n}}"] & W(R) \arrow[r, "W(\alpha)"] \arrow[d, "\mathbb{W}_n"] & W(A/\mathfrak{a}) \arrow[r, "\tilde{\mathbb{W}}_n"] \arrow[d, "\mathbb{W}_n"] & A \arrow[dl, "\pi"] \\
 & R \arrow[r, "\alpha"] & A/\mathfrak{a} &
\end{tikzcd}$$

Define $\beta = \tilde{\mathbb{W}}_n \circ W(\alpha) \circ {}^{F^{-n}}$. Since $\mathbb{W}_n({}^{F}\xi) = \mathbb{W}_{n+1}(\xi)$, we have $\mathbb{W}_n \circ {}^{F^{-n}} = \mathbb{W}_0$. Hence $\pi \circ \beta = \pi \circ \tilde{\mathbb{W}}_n \circ W(\alpha) \circ {}^{F^{-n}} = \alpha \circ \mathbb{W}_0$ by the above diagram.

Now we prove the uniqueness. For $r \in R$, consider $\beta([r])$. Let $r_n = r^{1/p^n}$. Then ${}^{F^{-n}}([r]) = [r_n]$. We have $W(\alpha)([r_n]) = [\alpha(r_n)]$. Moreover $\tilde{\mathbb{W}}_n([\alpha(r_n)]) = \widetilde{\alpha(r_n)}^{p^n}$, where $\widetilde{\alpha(r_n)} \in A$ is any lift of $\alpha(r_n)$. So

$$\beta([r]) = \widetilde{\alpha(r^{1/p^n})}^{p^n}.$$

Let $\beta' : W(R) \to A$ is another homomorphism such that $\pi \circ \beta = \alpha \circ \mathbb{W}_0$. Then $\beta'([r_n])$ is a lift of $\alpha[r_n]$. So

$$\beta([r]) = \beta'([r_n])^{p^n} = \beta'([r_n^{p^n}]) = \beta'([r]).$$

By Lemma 2.11 (a), we have $F \circ V = p$. In our case, we can show $V \circ F = p$ on $W(R)$ too. In fact, by Proposition 2.13 and Lemma 2.6, for $\eta = (r_0, r_1, \dots) \in W(R)$ we have

$${}^{VF}(r_0, r_1, \dots) = (0, r_0^p, r_1^p, \dots).$$

Then $\mathbb{W}_0({}^{VF}\eta) = 0 = p\mathbb{W}_0(\eta)$, $\mathbb{W}_1({}^{VF}\eta) = pa_0^p = 0 = p\mathbb{W}_1(\eta)$. Inductively, $\mathbb{W}_n({}^{VF}\eta) = 0 = p\mathbb{W}_n(\eta)$. Hence $VF = p$.

By Lemma 2.8, for any element $\xi = (x_0, x_1, \dots) \in W(R)$, $\xi = \sum {}^{V^i}[x_i] = \sum {}^{V^i F^i}[x_i^{1/p^i}]$. By the above discussion, we have $VF = FV = p$. Hence $\xi = \sum p^i [x_i^{1/p^i}]$. Since we know β and β' agree on $[r]$ for any $r \in R$, we have $\beta(\xi) = \beta'(\xi)$. □

Corollary 2.16. *For any positive integer m, we have a homomorphism $W(\mathbb{F}_p) \to \mathbb{Z}/p^m\mathbb{Z}$ such that*

$$\begin{tikzcd}
W(\mathbb{F}_p) \arrow[r, dashed] \arrow[d, "\mathbb{W}_0"] & \mathbb{Z}/p^m\mathbb{Z} \arrow[d] \\
\mathbb{F}_p \arrow[r, "\mathrm{id}"] & \mathbb{Z}/p\mathbb{Z}
\end{tikzcd}$$

is commutative. Hence we have a homomorphism

$$\mathbb{W}(\mathbb{F}_p) \to \varprojlim_m \mathbb{Z}/p^m\mathbb{Z} = \mathbb{Z}_p.$$

Remark 2.16.1. In fact, one can show that the map $\mathbb{W}(\mathbb{F}_p) \to \mathbb{Z}_p$ is an isomorphism.

Next, we consider the formal group associated to a Witt ring. Fix a ring R. We have a functor

$$W : \mathbf{Nil}_R \to \mathbf{Ab}$$
$$N \mapsto W(N).$$

This functor is clearly exact. But it is not a formal group, since $W(N)$ is not always equal to $\cup W(N_i)$, for $N = \cup N_i$. The reason that this equality fails is that $W(N)$ has infinite length in general. Hence, for $(n_0, n_1, \dots)$, it is impossible to find one i such that $n_k \in N_i$ for all k. For any $N \in \mathbf{Nil}_R$, we define

$$\hat{W}(N) = \{\xi = (x_0, x_1, \dots) | x_i = 0 \text{ for } i \text{ large enough}\}.$$

For a general ring S, $\hat{W}(S)$ is not even a group. For example,

$$[x] + [y] = (\dots, S_i(x, 0, \dots, y, 0, \dots), \dots).$$

Although $[x], [y]$ have length 1, $[x] + [y]$ may have infinite length. But we will show that if N is nilpotent, $\hat{W}(N)$ is closed under addition, hence it is an abelian group.

In $\mathbb{W}_n(X_0, \dots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + \dots + p^n X_n$, if we define $\deg X_i = p^i$, then $\deg \mathbb{W}_n = p^n$. A homogeneous polynomial in this new definition is called a *quasi-homogeneous* polynomial.

Lemma 2.17. *The polynomial S_n defined by* (2.2) *is quasi-homogeneous of degree p^n in $X_0, \dots, X_n, Y_0, \dots, Y_n$ for each n.*

Proof. By (2.2)

$$p^n S_n + \dots + S_0^{p^n} = \mathbb{W}_n(X_0, \dots, X_n) + \mathbb{W}_n(Y_0, \dots, Y_n).$$

The lemma follows by induction. □

Corollary 2.18. *If $N \in \mathbf{Nil}_R$, $\hat{W}(N)$ is closed addition. Hence $\hat{W}(N)$ is an abelian group. The functor*

$$\hat{W} : \mathbf{Nil}_R \to \mathbf{Ab}$$

is a formal group.

In the last lecture, we defined $\hat{W} : \mathbf{Nil}_R \to \mathbf{Ab}$ and we showed that $\hat{W}(N)$ is an abelian group for $N \in \mathbf{Nil}_R$. Now we will show that it is a $W(R)$-module. Since we have a homomorphism $W(R) \to W(R \oplus N)$ and $W(N)$ is an ideal of $W(R \oplus N)$, there is a natural $W(R)$-module structure on $W(N)$.

Lemma 2.19. *The group $\hat{W}(N)$ is also a $W(R)$-module.*

Proof. We only consider the case $N^2 = 0$. The general case follows using a filtration. Then we claim that

(*a*) $(n_0, n_1, \dots) + (n'_0, n'_1 \dots) = (n_0 + n'_0, n_1 + n'_1, \dots);$
(*b*) ${}^F(n_0, n_1, \dots) = (pn_0, pn_1, \dots);$
(*c*) $\xi \in W(R)$ acts by $\xi(n_0, n_1, \dots) = (\mathbb{W}_0(\xi)n_0, \mathbb{W}_1(\xi)n_1, \dots).$

From these formulae, we can see that $\hat{W}(N)$ is invariant under the action of $W(R)$. The claims (a)-(c) can be checked in a standard way, i.e., we can assume R is torsion free and then prove these formulas by applying $\mathbb{W}_i$. So in the case $N^2 = 0$, if we write $N_{[\mathbb{W}_i]}$ for N regarded as a $W(R)$-module via $\mathbb{W}_i : W(R) \to R$, we have an isomorphism

$$\hat{W}(N) \cong \bigoplus_i N_{[\mathbb{W}_i]}$$

of $W(R)$-modules. □

Let R be a ring such that p is nilpotent in R.

Lemma 2.20. *Let I_R be the kernel of $\mathbb{W}_0 : W(R) \to R$. We note that $I_R = {}^V W(R)$. Let* $\mathrm{rad}W(R)$ *denote the radical of $W(R)$, i.e., the intersection of all maximal ideals of $W(R)$. Then*

$$I_R \subset \mathrm{rad}W(R).$$

Proof. For every $x \in I_R$, we have to show that $1 - x$ is unit. Since $I_R = {}^V W(R)$, we can assume $x = {}^V\xi$. Then it suffices to show that

$$1 + {}^V\xi + ({}^V\xi)^2 + \dots$$

is convergent in $W(R) = \varprojlim W(R)/{}^{V^n}W(R)$. It suffice to show that for any m, there exists an n such that $({}^V\xi)^n \in {}^{V^m}W(R)$. By Lemma 2.11, we can check that

$$({}^V\xi)^n = p^{n-1V}\xi^n.$$

For example, ${}^V\xi{}^V\xi = {}^V(\xi{}^{FV}\xi) = {}^V(p\xi^2)$. Hence it suffice to show that if n is big enough, then $p^n W(R) \subset {}^{V^m}W(R)$. It is enough to check this for $m = 1$. But this clear, since $W(R)/{}^V W(R) \cong R$ is annihilated by some power of p by our assumption on R. □

We are now ready to define the notion of a display.

Definition 2.21. *Let P, Q be two $W(R)$-modules. A map $f : P \to Q$ is called* ^{F}***-linear*** *if f is additive and $f(\xi x) = {}^F\xi f(x)$ for all $\xi \in W(R)$ and $x \in P$.*

Given an ^{F}-linear map $f : P \to Q$, the map $f^\sharp : W(R) \otimes_{W(R),F} P \to P$ defined by $f^\sharp(\xi \otimes x) = \xi f(x)$ is linear. The map $f^\sharp$ is called the **linearization** of f.

Definition 2.22. *Let R be a commutative ring with 1 such that p is nilpotent in R. A* ***display*** *over R is a quadruple $\mathcal{P} = (P, Q, F, \dot{F})$, where P is a finitely generated projective $W(R)$-module, $Q \subset P$ is a submodule and $F, \dot{F}$ are ^{F}-linear maps $F : P \to P$, $\dot{F} : Q \to P$, satisfying the following conditions.*

(i) *$I_R P \subset Q$.*
(ii) *The quotient P/Q is a finitely generated projective R-module.*
(iii) *If $\xi \in W(R)$ and $x \in P$, we have the relation*

$$\dot{F}({}^V\xi x) = \xi F(x).$$

(iv) *$\dot{F}(Q)$ generates P as a $W(R)$-module.*

The number $\mathrm{rk}_{W(R)}P$ *is well-defined locally and is called the* ***height*** *of $\mathcal{P}$. The R-module P/Q is called the* ***Lie algebra*** *of $\mathcal{P}$ and* $\mathrm{rk}_R(P/Q)$ *is called the* ***dimension*** *of $\mathcal{P}$.*

Remarks:(1) That P/Q has an $R = W(R)/I_R$-module structure follows from (i). Since $\dot{F}$ is not linear, $\dot{F}(Q)$ is not a submodule of P in general.
(2) By (iii), we have

$$F(x) = 1 \cdot F(x) = \dot{F}({}^V 1 \cdot x) = {}^{FV}1\dot{F}(x) = p\dot{F}(x) \tag{2.6}$$

for every $x \in Q$.

A morphism of two displays is defined to be a homomorphism of the corresponding projective modules satisfying certain obvious compatible conditions. The displays over R forms a category.

Proposition 2.23. *Let $S \to R$ be a surjective ring homomorphism such that any element in the kernel is nilpotent. Then any projective R-module P lifts to a projective S-module $\tilde{P}$, i.e., there is a projective S-module $\tilde{P}$ and an isomorphism $\phi : \tilde{P} \otimes_S R \simeq P$. The pair $(\tilde{P}, \phi)$ is uniquely determined up to isomorphism*

Proof. To be added.

□

Lemma 2.24. *For any display $\mathcal{P} = (P, Q, F, \dot{F})$, we have a decomposition*

$$P = T \oplus L, \quad Q = I_R T \oplus L,$$

where T and L are projective $W(R)$-modules. This decomposition is called a ***normal decomposition*** *of $\mathcal{P}$.*

Here we only give a sketch of the proof. For details see [Z1] Lemma 2.

Proof. We first show each projective R-module M can be lifted to a $W(R)$-module. Set $A_n = W(R)/I_R^n$. Then $W(R) = \varprojlim A_n, R = A_1$. The map $A_{n+1} \to A_n$ is surjective and any element in the kernel is nilpotent. So M can be lifted to an A_n-module M_n step by step. Such $\{M_n\}$ forms a projective system. Then take $P = \varprojlim M_n$.

Since P/Q is a projective R-module, we have a split exact sequence

$$0 \to Q/I_R P \to P/I_R P \to P/Q \to 0$$

of R-modules. Let L be a projective $W(R)$-module which lifts $Q/I_R P$. By projectivity of L, $L \to Q/I_R P$ factors through Q. Similarly we can lift P/Q to a projective $W(R)$-module T. The map $T \to P/Q$ factors though P. Then we have a homomorphism $L \oplus T \to P$. By construction, this homomorphism becomes an isomorphism after tensoring with $W(R)/I_R$. Since $I_R \subset \mathrm{rad} W(R)$, we can apply Nakayama's Lemma to conclude that the homomorphism $L \oplus T \to P$ is surjective. Since P is projective, we deduce that the homomorphism $L \oplus T \to P$ is an isomorphism by comparing ranks.
We can show that $Q = I_R T \oplus L$ similarly. □

Let $\mathcal{P} = (P, Q, F, \dot{F})$ be a display. Suppose we are given a normal decomposition $P = T \oplus L$. Define a map

$$\Phi = F \oplus \dot{F} : T \oplus L \to P$$

$$(a, b) \mapsto F(a) + \dot{F}(b).$$

Then Φ is Frobenius linear.

Lemma 2.25. *The map*

$$\Phi^\sharp : W(R) \otimes_{F,W(R)} P \to P$$
$$w \otimes x \mapsto w\Phi(x)$$

is an isomorphism.

Proof. By definition, $\Phi^\sharp$ is linear. Since P is projective, it suffice to show that the map is surjective. We use the axiom that $\dot{F}(Q) = \dot{F}(I_R T \oplus L)$ generates P. So it suffice to show $\dot{F}(Q) \subset \mathrm{Im}\Phi^\sharp$. For ${}^V\xi t \in I_R T$, we have $\dot{F}({}^V\xi t) = \xi F(t) \in \mathrm{Im}(\Phi)$ by (iii) in the definition of a display. For $l \in L$, $\dot{F}(l) \in \mathrm{Im}(\Phi)$ by the definition of Φ. We are done. □

Assume L, T are free R-modules. Suppose $t_1, \dots, t_d$ is a basis of T and $l_1, \dots, l_c$ is a basis of L. Her d indicates "dimension" and c indicates "codimension". Then we have

$$F(t_j) = \sum_i \alpha_{ij} t_i + \sum_i \beta_{ij} l_i, \tag{2.7}$$

$$\dot{F}(l_j) = \sum_i \gamma_{ij} t_i + \sum_i \delta_{ij} l_i, \tag{2.8}$$

with $\alpha_{ij}, \beta_{ij}, \gamma_{ij}, \delta_{ij} \in W(R)$. By Lemma 2.25, we have

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in \mathrm{GL}_{c+d}(W(R)). \tag{2.9}$$

Conversely, if we are given an invertible matrix as in (2.9), we can define a display $\mathcal{P} = (P, Q, F, \dot{F})$ with a given normal decomposition, as follows. Put $T = W(R)^d, L = W(R)^c$, and $P = T \oplus L, Q = I_R T \oplus L$. Define

$$\dot{F} : I_R T \oplus L \to P$$

by

$$\dot{F}\begin{pmatrix} {}^V\xi_1 \\ \cdots \\ {}^V\xi_d \\ \eta_1 \\ \cdots \\ \eta_c \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} \xi_1 \\ \cdots \\ \xi_d \\ {}^F\eta_1 \\ \cdots \\ {}^F\eta_c \end{pmatrix}$$

and $F : T \to P$ by Formula (2.7). We extend F to $P \to P$ by Formula (2.6). So we have a map $F : P \to P$. Then it is easy to check that we have defined a display $\mathcal{P} = (P, Q, F, \dot{F})$.

We first look at an example of a display.

Definition 2.26. *Let k be a perfect field of characteristic p. A* ***Dieudonné module*** *over k is a triple $\mathcal{P} = (P, F, V)$, where P is a finitely generated free $W(k)$-module and $F : P \to P$, $V : P \to P$ are additive maps such that*

$$F(\xi x) = {}^F\xi F(x), \quad V(\xi x) = {}^{F^{-1}}\xi V(x) \qquad \forall \xi \in W(k), x \in P,$$

and

$$FV = p = VF.$$

Proposition 2.27. *Let k be a perfect field with characteristic p. Let (P, F, V) be a Dieudonné module. Define $Q = VP$ and $\dot{F} : Q \to P$ by $Vx \mapsto x$. Then $(P, Q, F, \dot{F})$ is a display. The assignment*

$$(P, F, V) \mapsto (P, Q, F, \dot{F})$$

defines an equivalence between the category of Dieudonné modules over k and the category of displays over k.

Proof. For a given Dieudonné module (P, F, V), the construction obviously gives a display $(P, Q, F, \dot{F})$. Conversely, suppose we are given a display $(P, Q, F, \dot{F})$. We need to construct a map $V : P \to P$. Since k is perfect, one can show that $W(k)$ is a complete discrete valuation ring with maximal ideal $I = I_k = pW(k) = {}^{V}W(k)$. So in our case, each projective module is free. Let $P = L \oplus T$, $Q = IT \oplus L$ be a normal decomposition. We have an isomorphism

$$\dot{F}^{\sharp} : W(k) \otimes_{F,W(k)} Q \to P,$$

by the definition of a display. In our case, the Frobenius ${}^{F} : W(k) \to W(k)$ is also an isomorphism by Proposition 2.13. Define

$$\theta : W(k) \otimes_{F,W(k)} Q \to Q$$

by

$$\xi \otimes x \mapsto {}^{F^{-1}}\xi x.$$

Define a map

$$V : P \to W(k) \otimes_{F,W(k)} Q \to Q \to P,$$

where the first arrow is the inverse of $\dot{F}^{\sharp}$ and the second arrow is θ and the last arrow is the inclusion. Then (P, F, V) is a Dieudonné module.

It is not hard to see that the two constructions establish the required equivalence. □

Next, we will construct a formal group for a display over any ring R such that p is nilpotent in R.

We fix a display $\mathcal{P} = (P, Q, F, \dot{F})$. We set

$$\hat{P}(N) = \hat{W}(N) \otimes_{W(R)} P.$$

Regarded as a functor on $\mathbf{Nil}_R$, $\hat{P}$ is a formal group, since $\hat{W}$ is a formal group and P is projective over $W(R)$. Define a homomorphism

$$\hat{P}(N) = \hat{W}(N) \otimes_{W(R)} P \to N \otimes_R (P/Q) \tag{2.10}$$

by

$$\xi \otimes p \mapsto \mathbb{W}_0(\xi) \otimes \bar{p}.$$

Lemma 2.28. *Let $P = T \oplus L, Q = I_R T \oplus L$ be a normal decomposition. Then the kernel $\hat{Q}(N)$ of the map (2.10) is $\hat{I}_R(N) \otimes_{W(R)} T \oplus \hat{W}(N) \otimes_{W(R)} L$, where $\hat{I}_R(N) = {}^{V}\hat{W}(N)$. The functor $\hat{Q} : \mathbf{Nil}_R \to \mathbf{Ab}$ is a formal group.*

The lemma is trivial. By abuse of notation, we will use id : $\hat{Q}(N) \to \hat{P}(N)$ to denote the inclusion map later on.

We define a map

$$\dot{F} : \hat{Q}(N) \to \hat{P}(N)$$

as follows. Fix a normal decomposition $P = T \oplus L, Q = I_R T \oplus L$. By Lemma 2.28, $\hat{Q}(N)$ is generated by elements of the form ${}^V\eta \otimes t + \xi \otimes l$ with $\eta, \xi \in \hat{W}(N), t \in T, l \in L$. Then we define

$$\dot{F}({}^V\eta \otimes t + \xi \otimes l) = \eta \otimes F(t) + {}^F\xi \otimes \dot{F}(l).$$

Note, by abuse of language, we have two maps called $\dot{F}$. It can be shown that the definition of $\dot{F}$ is independent of the choice of the decomposition.

Theorem 2.29. *Let $\mathcal{P} = (P, Q, F, \dot{F})$ be a display. Define a functor $\mathrm{BT}_{\mathcal{P}} : \mathbf{Nil}_R \to \mathbf{Ab}$ as follows. For any $N \in \mathbf{Nil}_R$, we define*

$$\mathrm{BT}_{\mathcal{P}}(N) = \mathrm{Coker}[\dot{F} - \mathrm{id} : \hat{Q}(N) \longrightarrow \hat{P}(N)].$$

Then $\mathrm{BT}_{\mathcal{P}}$ is a formal group and we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \hat{Q}(N) \arrow[r, "\dot{F}-\mathrm{id}"] & \hat{P}(N) \arrow[r] & BT_{\mathcal{P}}(N) \arrow[r] & 0 \end{tikzcd} \tag{2.11}$$

for any $N \in \mathbf{Nil}_R$. Moreover the tangent space of $\mathrm{BT}_{\mathcal{P}}$ is P/Q. The construction $\mathcal{P} \to BT_{\mathcal{P}}$ is functorial.

Note that BT stands for “Barsotti-Tate”.

Proof. For simplicity, put $X = \mathrm{BT}_{\mathcal{P}}$.

We first consider the case $N^2 = 0$. In this case, by the proof of Lemma 2.19, we see that

$$\hat{W}(N) = \bigoplus_{n=0}^{\infty} N_{[\mathbb{W}_n]}.$$

By the definitions of $\hat{P}, \hat{Q}$, we have

$$\begin{aligned} \hat{P}(N) &= \textstyle\bigoplus_{n=0}^{\infty} N_{[\mathbb{W}_n]} \otimes_{W(R)} P \\ \hat{Q}(N) &= (N_{[\mathbb{W}_0]} \otimes_{W(R)} L) \oplus \textstyle\bigoplus_{n=1}^{\infty} N_{[\mathbb{W}_n]} \otimes_{W(R)} P \end{aligned} \tag{2.12}$$

Note that $N_{[\mathbb{W}_0]} \otimes_{W(R)} L$ is generated by $[a] \otimes l$ for $a \in N, l \in L$. We have

$$\dot{F}([a] \otimes l) = {}^F[a] \otimes \dot{F}(l) = [a^p] \otimes \dot{F}(l) = 0$$

since $N^2 = 0$.

As a $W(R)$-module $N_{[\mathbb{W}_n]} \cong {}^{V^n}[N] = \{(0, \dots, 0, a, 0, \dots) | a \in N\}$, where a is in the n^{th} place. Hence $N_{[\mathbb{W}_n]} \otimes_{W(R)} P$ is generated by the tensors ${}^{V^n}[a] \otimes x$ with $a \in N, x \in P$. We have

$$\dot{F}({}^{V^n}[a] \otimes x) = {}^{V^{n-1}}[a] \otimes F(x) \in N_{[\mathbb{W}_{n-1}]} \otimes_{W(R)} P.$$

Therefore $\dot{F}$ acts on the right hand side of (2.12) by maps

$$\begin{gathered} F(n) : N_{[\mathbb{W}_n]} \otimes_{W(R)} P \to N_{[\mathbb{W}_{n-1}]} \otimes_{W(R)} P \\ a \otimes x \mapsto a \otimes Fx. \end{gathered}$$

Namely, for $(0, u_1, u_2, \dots) \in \bigoplus_{n\geq 1} N_{[\mathbb{W}_n]} \otimes P$, we have

$$\dot{F}((0, u_1, u_2, \dots)) = (F(1)u_1, F(2)u_2, \dots).$$

Now define an endomorphism $\tilde{F} : \hat{P}(N) \to \hat{P}(N)$ by

$$\tilde{F}(u_0, u_1, \dots) = (F(1)u_1, F(2)u_2, \dots).$$

Then $\tilde{F}$ is an extension of $\dot{F} : \hat{Q}(N) \to \hat{P}(N)$. Since only finitely many of the components u_i are nonzero, we see that $\tilde{F}$ is a pointwise nilpotent endomorphism. Therefore

$$\tilde{F} - \mathrm{id} : \hat{P}(N) \to \hat{P}(N)$$

is an isomorphism.

We obtain a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \hat{Q}(N) \arrow[r, "\mathrm{id}"] \arrow[d, "\mathrm{id}"] & \hat{P}(N) \arrow[r] \arrow[d, "\tilde{F}-\mathrm{id}"] & N \otimes_R (P/Q) \arrow[r] & 0 \\
& \hat{Q}(N) \arrow[r, "\dot{F}-\mathrm{id}"] & \hat{P}(N) \arrow[r] & X(N) \arrow[r] & 0
\end{tikzcd}$$

In other words the tangent space of the functor X is P/Q.

Moreover it follows that $\dot{F} - \mathrm{id}$ is injective for $N \in \mathbf{Nil}_R$ with $N^2 = 0$. For an arbitrary $N \in \mathbf{Nil}_R$ we find a finite chain

$$0 = N_t \subset \dots \subset N_2 \subset N_1 \subset N_0 = N$$

such that $N_i^2 \subset N_{i+1}$. Using the exactness of the functors $\hat{P}$ and $\hat{Q}$ an induction with the snake-lemma shows that $\dot{F} - \mathrm{id}$ is injective in general, i.e. we proved that the sequence (2.11) is exact. But this implies that the functor X is exact. The second condition of a formal group is easy to verify, as we did for $\hat{W}(N)$. This proves the Theorem. □

Remark 2.29.1. If P/Q is a free R-module rank d then $X \cong \hat{\mathbb{A}}^d$ by Theorem 1.14, i.e., we may describe X by power series.

Lemma 2.30. *Let $\mathcal{P} = (P, Q, F, \dot{F})$ be a display. Then there is a unique $W(R)$-module homomorphism*

$$V^\sharp : P \to W(R) \otimes_{F,W(R)} P$$

such that

$$V^\sharp(\xi \dot{F}(y)) = \xi \otimes y, \quad \forall \xi \in W(R), y \in Q, \tag{2.13}$$

$$V^\sharp(\xi F(x)) = p\xi \otimes x, \quad \forall \xi \in W(R), x \in P. \tag{2.14}$$

Proof. The uniqueness follows from formula (2.13), since $\dot{F}(Q)$ generates P. To prove the existence, we fix a normal decomposition $P = T \oplus L$. Then we have an isomorphism

$$\Phi = F^\sharp \oplus \dot{F}^\sharp : W(R) \otimes_{F,W(R)} T \oplus W \otimes_{F,W(R)} L \to P,$$

where $F^\sharp$ is the linearization of F. Consider the map

$$p \oplus \mathrm{id} : W(R) \otimes_{F,W(R)} T \oplus W \otimes_{F,W(R)} L \to W \otimes_{F,W(R)} P$$

$$\xi \otimes t + \eta \otimes l \mapsto p\xi \otimes t + \eta \otimes l.$$

Define

$$V^\sharp : P \to W(R) \otimes_{W(R),F} P$$

to be the composition of $p \oplus \mathrm{id}$ with Φ^{-1}. We proceed to check that $V^\sharp$ satisfies the required conditions. Clearly $V^\sharp$ is linear.

Take $y \in Q$ to be of the form $y = l + {}^V ut$ with $l \in L, u \in W(R), t \in T$. Then

$$\begin{aligned} V^\sharp(\xi \dot{F}(y)) &= V^\sharp(\xi \dot{F}(l)) + V^\sharp(\xi u F(t)) \\ &= \xi \otimes l + p\xi u \otimes t = \xi \otimes l + \xi^{FV} u \otimes t \\ &= \xi \otimes (l + {}^V ut) = \xi \otimes y. \end{aligned}$$

This shows the identity (2.13).

To verify (2.14), take $x = l + t$ with $l \in L, t \in T$. We have

$$\begin{aligned} V^\sharp(\xi F(x)) &= V^\sharp(\xi F(l)) + V^\sharp(\xi F(t)) \\ &= V^\sharp(\dot{F}({}^V \xi l)) + V^\sharp(\xi F(t)) \\ &= 1 \otimes {}^V \xi l + p\xi \otimes t = p\xi \otimes (l + t) = p\xi \otimes x. \end{aligned}$$

We are done. □

Let us denote by ${}^F V^\sharp$ the $W(R)$-linear map

$$\mathrm{id}_W(R) \otimes_{F,W(R)} V^\sharp : W(R) \otimes_{F,W(R)} P \to W(R) \otimes_{F,W(R)} W(R) \otimes_{F,W(R)} P.$$

Denote the right hand side space by $W \otimes_{F^2,W(R)} P$. Inductively, we have

$${}^{F^i} V^\sharp = \mathrm{id} \otimes_{F^i,W(R)} V^\sharp : W(R) \otimes_{F^i,W(R)} P \to W(R) \otimes_{F^{i+1},W(R)} P.$$

We denote by $(V^n)^\sharp$ the composite

$${}^{F^{n-1}} V^\sharp \circ \cdots \circ {}^F V^\sharp \circ V^\sharp.$$

Definition 2.31. *A display $\mathcal{P} = (P, Q, F, \dot{F})$ is called* ***nilpotent*** *if there is an $n \in \mathbb{N}$ such that the map*

$$(V^n)^\sharp : P \to W(R) \otimes_{F^n,W(R)} P$$

is zero modulo $I_R + pW(R)$.

Remark 2.31.1 The nilpotence condition for a display $\mathcal{P} = (P, Q, F, \dot{F})$ is equivalent to that the map

$$R/pR \otimes_{\mathbb{W}_0,W(R)} (V^n)^\sharp : (R/pR) \otimes_{\mathbb{W}_0,W(R)} P \to (R/pR) \otimes_{\mathbb{W}_n,W(R)} P \tag{2.15}$$

induced by $(V^n)^\sharp$ is zero.

If P, Q are free module, then the maps are given by invertible matrices. In this case, we can express the nilpotence condition of a display by the matrices. Explicitly, let $\mathcal{P} = (P, Q, F, \dot{F})$ be a display which has a normal decomposition with $T = W(R)^d, L = W(R)^c, h = d + c$. Suppose the map $\Phi = F^\sharp \oplus \dot{F}^\sharp$ is given by a matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

i.e.,

$$\Phi \begin{pmatrix} t \\ l \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} {}^F t \\ {}^F l \end{pmatrix}$$

for $t \in T, l \in L$. The matrix is invertible by Lemma 2.25. Consider the inverse matrix

$$\begin{pmatrix} \breve{A} & \breve{B} \\ \breve{C} & \breve{D} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1}.$$

Hence $V^\sharp$ is defined by

$$V^\sharp \begin{pmatrix} t \\ l \end{pmatrix} = \begin{pmatrix} p\breve{A} & p\breve{B} \\ \breve{C} & \breve{D} \end{pmatrix} \begin{pmatrix} {}^F t \\ {}^F l \end{pmatrix}.$$

Then $V^\sharp(\text{mod } (I_R + pW(R)))$ is defined by the matrix

$$\begin{pmatrix} 0 & 0 \\ \breve{C}_1 & \breve{D}_1 \end{pmatrix}$$

where $\breve{D}_1 = \breve{D}(\text{mod } (I_R + pW(R)))$ is a matrix with entries in R/pR. Denote by $\breve{D}_1^{(p^m)}$ the matrix each of whose entries is the p^m-th power of the corresponding entry of $\breve{D}_1$. Then "$\mathcal{P}$ is nilpotent" is equivalent to the statement that there is an integer $n > 0$ such that

$$\breve{D}_1^{(p^{n-1})} \cdot \breve{D}_1^{(p^{n-2})} \cdot \dots \cdot \breve{D}_1^{(p)} \cdot \breve{D}_1 = 0. \tag{2.16}$$

The following is the main theorem of the theory of displays.

Theorem 2.32 (Zink)**.** *Let R be a commutative ring with 1 such that p is nilpotent in R. Let $\mathcal{P}$ be a nilpotent display. Then $\mathrm{BT}_{\mathcal{P}}$ is a formal p-divisible group. Moreover, the functor*

$$\mathrm{BT} : \{\textit{nilpotent displays}\} \longrightarrow \{\textit{formal p-divisible groups}\}$$

is an equivalence of the categories.

This is Theorem [9] in [Z1]. We will discuss the proof later but will not give a detailed proof.

Definition 2.33. *A **frame** consists of a surjective homomorphism of commutative rings $f : S \to R$ whose kernel is denoted by I, an endomorphism $\sigma : S \to S$ and a σ-linear map $\dot{\sigma} : I \to S$ such that*
(i) $\sigma(s) = s^p(\text{mod } pS)$ *for each $s \in S$.*
(ii) $\dot{\sigma}(I)$ *generates S as an ideal.*
(iii) $I \subset \mathrm{rad}(S)$ *and* $p \in \mathrm{rad}(S)$.
(vi) *Every finitely generated projective R-module lifts to a finitely generated projective S-module.*
We will often denote the frame by $(S, I, R, \sigma, \dot{\sigma})$ and omit the map f from the notations for simplicity.

Example 2.33.1. Let R be a commutative ring such that p is nilpotent in R. Put $S = W(R)$ and $I = I_R = {}^V W(R)$. Define $\sigma : W(R) \to W(R)$ to be the Frobenius, i.e., $\sigma(\xi) = {}^F\xi, \xi \in W(R)$. Define $\dot{\sigma} = {}^{V^{-1}} : I \to W(R)$ by $\dot{\sigma}({}^V\eta) = \eta$. Then $(S, I_R, R, {}^F, {}^{V^{-1}})$ is a frame. The condition (ii) in the definition of a frame has been used in the proof of Lemma 2.24. Note that in this example, we have $\sigma({}^V\eta) = p\dot{\sigma}({}^V\eta)$ for any ${}^V\eta \in I$. For a general frame, we have the following lemma.

Lemma 2.34. *Let $\mathcal{F} = (S, I, R, \sigma, \dot{\sigma})$ be a frame. Then there is a unique $\theta \in S$ such that*

$$\sigma(i) = \theta\dot{\sigma}(i)$$

for all $i \in I$.

Proof. We first show the uniqueness. If θ' is a second element in S satisfying the condition, then $(\theta' - \theta)\dot{\sigma}(i)$ for all $i \in I$. But $\dot{\sigma}(i)$ generates S, so we get $\theta' = \theta$.

For the existence, we write $1 = \sum_k s_k\dot{\sigma}(i_k)$ with $s_k \in S, i_k \in I$. Then for any $i \in I$, we have

$$\sigma(i) = \sum_k \sigma(i)s_k\dot{\sigma}(i_k) = \sum_k s_k\dot{\sigma}(ii_k) = \sum_k s_k\sigma(i_k)\dot{\sigma}(i),$$

by the fact that the map $\dot{\sigma}$ is σ-linear. Then $\theta = \sum_k s_k\sigma(i_k)$ satisfies the required condition. □

Definition 2.35. *Let $\mathcal{F} = (S, I, R, \sigma, \dot{\sigma})$ be a frame. A* ***window*** *over $\mathcal{F}$ is a quadruple $(P, Q, F, \dot{F})$, where F is a finitely generated projective S-module, Q is a submodule of P, $F : P \to P$, $\dot{F} : Q \to P$ are two σ-linear maps, satisfying the following conditions.*

(i) *$IP \subset Q$.*
(ii) *The quotient P/Q is a finitely generated projective R-module.*
(iii) *If $i \in I$ and $x \in P$, we have the relation*

$$\dot{F}(ix) = \dot{\sigma}(i)F(x).$$

(iv) *$\dot{F}(Q)$ generates P as an S-module.*
(v) *If $y \in Q$, then $F(y) = \theta\dot{F}(y)$, where θ is defined in Lemma 2.33.*

Example 2.35.1. If we take $\mathcal{F} = (W(R), I_R, R, {}^F, {}^{V^{-1}})$ as in the Example 2.33.1, then an $\mathcal{F}$-window is equivalent to a display over R.
Remark 2.35.2. We can define nilpotent windows in the same manner as for displays. We omit the explicit definition.

Definition 2.36. *Let $\mathcal{F} = (S, I, R, \sigma, \dot{\sigma})$ and $\mathcal{F}' = (S', I', R', \sigma', \dot{\sigma}')$ be two frames. A* ***morphism*** *$\Theta : \mathcal{F} \to \mathcal{F}'$ of frames consists of two homomorphism of rings $\Theta_1 : S \to S'$ and $\Theta_2 : R \to R'$ such that Θ_1 and Θ_2 are compatible with all datum in $\mathcal{F}$ and $\mathcal{F}'$. Explicitly, we require the diagram*

$$\begin{tikzcd}
S \arrow[r, "\Theta_1"] \arrow[d] & S' \arrow[d] \\
R \arrow[r, "\Theta_2"] & R'
\end{tikzcd}$$

to be commutative. Hence Θ_1, Θ_2 induce a map $I \to I'$, which we denote by Θ_1 again, by abuse of language. Furthermore, we require

$$\Theta_1 \circ \sigma = \sigma' \circ \Theta_1, \quad \Theta_1 \circ \dot{\sigma} = \dot{\sigma}' \circ \Theta_1.$$

Remark 2.36.1 Since a display is a special window, we have the notion of morphism between displays.

We consider base change functor of windows.

Definition 2.37. *Suppose we are given a morphism $\Theta : \mathcal{F} \to \mathcal{F}'$ of frames. Then we define the base change functor*

$$\Theta_\bullet : \{\mathcal{F}\text{-}windows\} \longrightarrow \{\mathcal{F}'\text{-}windows\}$$

by the assignment

$$\mathcal{P} = (P, Q, F, \dot{F}) \mapsto \mathcal{P}' = (P', Q', F', \dot{F}'), \tag{2.17}$$

where $P' = S' \otimes_S P$, $Q' = \mathrm{Ker}(S' \otimes_S P \to R' \otimes_R (P/Q))$, $F' = \sigma' \otimes F : P' \to P'$. Note that Q' is generated by $I' \otimes_S P$ and $S' \otimes_S Q$. We define $\dot{F}' : Q' \to P'$ by

$$\dot{F}'(i' \otimes x) = \dot{\sigma}'(i) \otimes F(x), \quad i' \in I', x \in P,$$

$$\dot{F}'(s' \otimes y) = \sigma'(s') \otimes \dot{F}(y), \quad s' \in S', y \in Q.$$

It is not hard to check that $\mathcal{P}'$ is an $\mathcal{F}'$-window. Moreover, we have $P'/Q' = R' \otimes_R (P/Q)$.

Remark 2.37.1. Since display is a special case of windows, we have the notion of base change of displays.

As in Lemma 2.24, for any $\mathcal{F}$-window $\mathcal{P} = (P, Q, F, \dot{F})$, we can show that there is a normal decomposition $P = T \oplus L$, $Q = IT \oplus L$. Then we have an isomorphism

$$\Phi = F^\sharp \oplus \dot{F}^\sharp : S \otimes_{\sigma,S} T \oplus S \otimes_{\sigma,S} L \to P.$$

Suppose that T and L are free. Then Φ is given by an invertible matrix

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}_h(S), \quad h = \mathrm{rk} P.$$

In fact, it can be shown that $\mathcal{P}$ is uniquely determined by the matrix M. We proved this for displays, and the proof is similar for windows. So we can identify $\mathcal{F}$-windows which have free P, Q with $M \in \mathrm{GL}_h(S)$, where $h = \mathrm{rk} P$.

Suppose $\mathcal{F}'$ is another frame and $\Theta : \mathcal{F} \to \mathcal{F}'$ is a morphism of frames. Then it is easy to see, under the above identification, that the base change functor can be identified with the map

$$\mathrm{GL}_h(S) \to \mathrm{GL}_h(S')$$

$$M \mapsto \Theta(M)$$

where $\Theta(M)$ is the matrix obtained by applying Θ_1 to each entry of M.

Next, we will see how to construct morphisms of frames.

Lemma 2.38. *Let $\mathcal{F} = (S, I, R, \sigma, \dot{\sigma})$ be a frame. Assume S has no p torsion. Then there is a ring homomorphism $\delta : S \to W(S)$ such that $\mathbb{W}_n(\delta(s)) = \sigma^n(s)$, for all $n \geq 0$, $s \in S$. Furthermore, we have $\delta(\sigma(s)) = {}^F\delta(s)$.*

Proof. For any $s \in S$, set $u_n = \sigma^n(s)$. Note that as $\sigma(s) \equiv s^p (\mathrm{mod}\, pS)$, we can apply Proposition 2.2 to conclude there is a $\xi \in W(s)$ such that $\mathbb{W}_n(\xi) = u_n$. Such ξ is unique since S has no p torsion and the map $\mathbb{W} = (\mathbb{W}_i; i \geq 0) : W(S) \to \prod_{i\geq 0} S$ is injective. Then we can define $\delta(s) = \xi$. Since σ is a ring homomorphism, so is δ.

To prove the second assertion, we only need to check, for all $n \geq 0$ and $s \in S$, that

$$\mathbb{W}_n(\delta(\sigma(s))) = \mathbb{W}_n({}^{F}(\delta(s))). \tag{2.18}$$

The left hand side of (2.18) equals $\sigma^n(\sigma(s)) = \sigma^{n+1}(s)$. The right hand side of (2.18) is $\mathbb{W}_{n+1}(\delta(s)) = \sigma^{n+1}(s)$. We are done. □

Proposition 2.39. *Assume that $\mathcal{F} = (S, I, R, \sigma, \dot\sigma)$ is a frame such that $\theta = p$. Define $\mathfrak{X} : S \to W(R)$ to be the composition of $\delta : S \to W(S)$ and the canonical homomorphism $W(S) \to W(R)$, where δ is defined in Lemma* 2.38. *Then the map*

$$\mathfrak{X} : (S, I, R, \sigma, \dot\sigma) \to (W(R), I_R, R, {}^{F}, {}^{V^{-1}}),$$

consisting of $\mathfrak{X} : S \to W(R)$ and id $: R \to R$ *is a morphism of frames* (*see the Definition* 2.36) *if and only if*

$$\mathfrak{X}(\dot\sigma(i)) = {}^{V^{-1}}\mathfrak{X}(i), \quad \forall i \in I. \tag{2.19}$$

Proof. By the definition of δ, we have $\mathbb{W}_0(\delta(s)) = s$. So we have the following commutative diagrams

$$\begin{tikzcd}
S \arrow[r, "\delta"] \arrow[dr, "\mathrm{id}"'] & W(S) \arrow[r] \arrow[d, "\mathbb{W}_0"] & W(R) \arrow[d, "\mathbb{W}_0"] \\
 & S \arrow[r] & R
\end{tikzcd}
\qquad
\begin{tikzcd}
S \arrow[r] \arrow[d, "\mathfrak{x}"] & R \arrow[d, "\mathrm{id}"] \\
W(R) \arrow[r, "\mathbb{W}_0"] & R
\end{tikzcd}$$

In particular, $\mathfrak{X}$ induces a map $I \to I_R$. Hence (2.19) makes sense. If $\mathfrak{X}$ is a morphism of frames, then we have (2.19) by Definition 2.36. Conversely, suppose (2.19) holds. Multiplying on both sides of (2.19) by p, the left hand side becomes

$$p\mathfrak{X}(\dot\sigma(i)) = \mathfrak{X}(p\dot\sigma(i)) = \mathfrak{X}(\sigma(i)).$$

The right hand side becomes

$$p^{V^{-1}}\mathfrak{X}(i) = {}^{FVV^{-1}}\mathfrak{X}(i) = {}^{F}\mathfrak{X}(i).$$

We get $\mathfrak{X}(\sigma(i)) = {}^{F}\mathfrak{X}(i)$. This shows that $\mathfrak{X}$ is a morphism of frames. □

Corollary 2.40. *Suppose that $\theta = p$ in $\mathcal{F}$, and $W(R)$ has no p torsion. Then* (2.19) *holds. Consequently, we have a morphism of frames*

$$\mathfrak{X} : (S, I, R, \sigma, \dot\sigma) \to (W(R), I_R, R, {}^{F}, {}^{V^{-1}}).$$

Proof. Composing the canonical map $W(S) \to W(R)$ with δ of Lemma 2.38 and using that Lemma, we get

$$\mathfrak{X}(\sigma(i)) = {}^{F}\mathfrak{X}(i).$$

This is equivalent to

$$p\mathfrak{X}(\dot\sigma(i)) = p({}^{V^{-1}}\mathfrak{X}(i)),$$

see the proof of Proposition 2.39. Since we assume $W(R)$ has no p torsion, we get (2.19). □

Example 2.40.1 If $p \cdot R = 0$ and R is reduced, then

$$p(r_0, r_1, \dots) = (0, r_0^p, r_1^p, \dots)$$

in $W(R)$. So $W(R)$ has no p torsion.

Suppose $\mathfrak{X} : \mathcal{F} \to (S, I, R, {}^F, {}^{V^{-1}})$ defined in Proposition 2.39 is a morphism of frames. Then we can consider the composite functors

$$\{\mathcal{F}\text{-windows}\} \to \{\text{displays over } R\} \to \{\text{formal groups}\} \tag{2.20}$$

where the first functor is the base change functor defined by $\mathfrak{X}$ and the second functor is BT.

Example 2.40.2 Let k be a perfect field of characteristic p. Put $R = k[T_1, \dots, T_n]$. Then R is reduced. We set $S = W(k)[X_1, \dots, X_n]^\wedge$, the p-adic completion of $W(k)[X_1, \dots, X_n]$. Consider the map $f : S \to R$, $f(X_i) = T_i$. Let I be the ideal pS. Define $\sigma : S \to S$ by $\sigma|_{W(k)} = {}^F$ and $\sigma(X_i) = X_i^p$. Define $\dot{\sigma} : I = pS \to S$ by $\dot{\sigma}(ps) = \sigma(s)$. We get a frame $\mathcal{F} = (S, pS, R, \sigma, \dot{\sigma})$. It is clear that $\theta = p$. Since $W(R)$ has no p torsion, we get a morphism of frames

$$\mathfrak{X} : \mathcal{F} \to (W(R), I_R, R, {}^F, {}^{V^{-1}})$$

by Corollary 2.40. We have

$$\mathfrak{X} : S \to W(R)$$
$$X_i \mapsto [T_i] = (T_i, 0, 0, \dots).$$

Let S, R be two rings with 1. Suppose p is nilpotent in S. Let $S \twoheadrightarrow R$ be a surjective homomorphism of commutative rings with kernel $\mathfrak{a}$. Suppose there are pd structures γ_n on $\mathfrak{a}$. Let $\mathfrak{a}^{\mathbb{N}}$ be the additive group $\prod_{i \in \mathbb{N}} \mathfrak{a}$. We define a $W(S)$-module structure on $\mathfrak{a}^{\mathbb{N}}$ by

$$\xi[a_0, a_1, \dots] = [\mathbb{W}_0(\xi)a_0, \mathbb{W}_1(\xi)a_1, \dots], \quad \xi \in W(S), a = [a_0, a_1, \dots] \in \mathfrak{a}^{\mathbb{N}}.$$

We set $\alpha_{p^n}(a) = (p^n - 1)!\gamma_{p^n}(a)$ and

$$\mathbb{W}'_n(X_0, \dots, X_n) = \alpha_{p^n}(X_0) + \alpha_{p^{n-1}}(X_1) + \dots + X_n. \tag{2.21}$$

Then $\mathbb{W}'_n(a)$ is well-defined for $a \in \mathfrak{a}^{\mathbb{N}}$ and $p^n \mathbb{W}'_n(a) = \mathbb{W}_n(a)$.

Lemma 2.41. *The polynomials* $\mathbb{W}'_n$ *define an isomorphism*

$$\log : W(\mathfrak{a}) \to \mathfrak{a}^{\mathbb{N}}$$
$$\eta \mapsto \mathbb{W}'_n(\eta)$$

of $W(S)$*-algebras.*

We omit the proof.
We denote $\tilde{\mathfrak{a}} = \log^{-1}[\mathfrak{a}, 0, 0, \dots]$. Then $\tilde{\mathfrak{a}}$ is an ideal of $W(S)$.
It is not difficult to compute the corresponding multiplication, Frobenius homomorphism, and Verschiebung homomorphism on $\mathfrak{a}^{\mathbb{N}}$ under the isomorphism log by the universal property of $\mathbb{W}'_i$:

$$\begin{aligned} [a_0, a_1, \dots][b_0, b_1, \dots] &= [a_0 b_0, p a_1 b_1, \dots, p^i a_i b_i, \dots] \\ {}^F[a_0, a_1, \dots, a_i, \dots] &= [p a_1, p a_2, \dots, p a_i, \dots] \\ {}^V[a_0, a_1, \dots, a_i, \dots] &= [0, a_0, a_1, \dots, a_i, \dots] \end{aligned} \tag{2.22}$$

Lemma 2.42. *Let $\rho : W(S) \to R$ be the composition of the natural maps $W(S) \to W(R)$ and $\mathbb{W}_0 : W(R) \to R$. Then ρ is surjective, and* $\mathrm{Ker}(\rho) = \tilde{\mathfrak{a}} \oplus I_S$. *If we define*

$$V^{-1} : \tilde{\mathfrak{a}} \oplus I_S \to W(S)$$

by $V^{-1}|_{\tilde{\mathfrak{a}}} = 0$ and $V^{-1}({}^V\eta) = \eta$ for ${}^V\eta \in I_S$, then

$$(W(S), \tilde{\mathfrak{a}} \oplus I(S), R, {}^F, V^{-1}),$$

where ^{F} is the Frobenius on $W(S)$, is a frame. Denote this frame by $\mathcal{W}_{S/R}$.

Proof. It is easy to see that ρ is surjective and $\mathrm{Ker}\rho = W(\mathfrak{a}) + I_S$. Note that $W(\mathfrak{a}) = \tilde{\mathfrak{a}} + {}^VW(\mathfrak{a})$ by (2.22) and ${}^VW(\mathfrak{a}) \subset I_S = {}^VW(S)$. Then it is clear that $\mathrm{Ker}\rho = \tilde{\mathfrak{a}} \oplus I_S$.

To show that $W_{S/R}$ is a frame, we need to show that $\mathrm{Ker}\rho \subset \mathrm{rad}W(S), p \in \mathrm{rad}W(S)$ and the lifting property (ii) of Definition 2.33.

To show that $p \in \mathrm{rad}W(S)$, we need to show that for any $y \in W(S)$, $1 - py$ is a unit in $W(S)$. Since p is nilpotent in S, $1 + (py) + \cdots + (py)^m + \cdots$ is well-defined in $W(S) = \varprojlim W(S)/{}^{V^n}W(S)$, it is clear that $1 - py$ is a unit.

Next we show that: $\mathrm{Ker}\rho \in \mathrm{rad}W(S)$. For any x in $\mathrm{Ker}\rho$, $y \in W(S)$, we have to show that $1 - xy$ is a unit in $W(S)$. Since $\mathrm{Ker}\rho$ is an ideal, $xy \in \mathrm{Ker}\rho$. So we only have to show that $1 - x$ is a unit for all $x \in \mathrm{Ker}\rho$. So we have to show that $1 + x^2 + \cdots + x^m + \cdots$ is convergent in $W(S) = \varprojlim W(S)/{}^{V^n}W(S)$. It suffice to show that for any n, there is an m such that $x^m \in {}^{V^n}W(S)$. It suffice to show that for m large enough $x^m \in {}^VW(S)$. Suppose $x = (x_0, x_1, \dots, x_i, \dots) \in W(S)$. Since $x = [x_0] + {}^Vx$ and ${}^Vx \in {}^VW(S)$, it suffice to show that $[x_0]^m \in {}^VW(S)$ for m large. But $x \in \mathrm{Ker}\rho$ implies $x_0 \in \mathfrak{a}$. We can view $[x_0]$ as an element of $\mathfrak{a}^{\mathbb{N}}$, i.e., $[x_0] = [x_0, 0, \dots, 0, \dots]$. By (2.22), $[x_0, 0, \dots, 0, \dots]^m = [x_0^m, 0, \dots]$. Since $\mathfrak{a}$ has divided power and p is nilpotent in S, then for n large enough we have that $x_0^{p^n} = (p^n)!\gamma_{p^n}(x_0)$ is zero. It suffice to take $m = p^n$.

The lifting property can be proved in a similar way as in the proof of Lemma 2.24. □

It is obvious that we have a morphism of frames

$$\Theta : \mathcal{W}_{S/R} = (W(S), \tilde{\mathfrak{a}} \oplus I(S), R, {}^F, V^{-1}) \to \mathcal{W}_R = (W(R), I_R, R, {}^F, {}^{V^{-1}}).$$

Theorem 2.43. *The base change functor defined by Θ induce an equivalence of categories*

$$\{\textit{nilpotent } \mathcal{W}_{S/R}\textit{-windows}\} \to \{\textit{nilpotent displays over } R\}.$$

We devote the following section and the next section to the proof of this theorem. Consider the ideal $p^i\mathfrak{a}$. Then $p^i\mathfrak{a}$ has pd structure defined by

$$\gamma_n^{(i)}(p^i a) = (p^i)^n \gamma_n(a), \quad a \in \mathfrak{a}.$$

We have the exact sequence

$$0 \to p^{i-1}\mathfrak{a}/p^i\mathfrak{a} \to S/p^i\mathfrak{a} \to S/p^{i-1}\mathfrak{a} \to 0.$$

We will show that

$$\mathcal{W}_{(S/p^i\mathfrak{a})/R} \to \mathcal{W}_{(S/p^{i-1}\mathfrak{a})/R}$$

induces an equivalence of categories of the corresponding nilpotent windows. Note that, we assume that p is nilpotent in S. Hence for some i, $p^i = 0$ in S, i.e., $S/p^i\mathfrak{a} = S$. Then the theorem will follow.

Observe that the Frobenius on $W(p^{i-1}\mathfrak{a}/p^i\mathfrak{a})$ is zero by (2.22) and the fact that $pa = 0$ for any $a \in p^{i-1}\mathfrak{a}/p^i\mathfrak{a}$. Hence the theorem is a consequence of the following proposition.

Proposition 2.44. *Let*

$$\Theta : \mathcal{F} = (S, I, R, \sigma, \dot{\sigma}) \to \bar{\mathcal{F}} = (\bar{S}, \bar{I}, \bar{R}, \bar{\sigma}, \bar{\dot{\sigma}})$$

be a morphism of frames with $\bar{R} = R$. Assume that p is nilpotent in S, I has pd structure and the map $S \to \bar{S}$ is surjective with kernel $\mathfrak{c}$. By the snake lemma, we can see that $\mathfrak{a} = \mathrm{Ker}(I \to \bar{I})$. So $\dot{\sigma}$ is defined on $\mathfrak{c}$. We assume $\dot{\sigma}(\mathfrak{c}) \subset \mathfrak{c}$ and $\sigma(\mathfrak{c}) = 0$. Then the base change functor defined by $\Theta : \mathcal{F} \to \bar{\mathcal{F}}$ induces an equivalence of categories

$$\{\textit{nilpotent } \mathcal{F}\textit{-windows}\} \to \left\{\textit{nilpotent } \bar{\mathcal{F}}\textit{-windows}\right\}.$$

Proof of Proposition 2.44. For simplicity, we assume that the windows that we considered have free normal decompositions. There is no essential difficulty to generalize the following proof to the general case.

Recall that a functor is an equivalence if and only if it is fully faithful and essentially surjective. We first show that the base change functor in our case is fully faithful.

We begin with some general remarks. Let $\mathcal{P}_1 = (P_1, Q_1, F_1, \dot{F}_1)$ be an $\mathcal{F}$-window. Take a normal decomposition

$$P_1 = T_1 \oplus L_1, \quad Q_1 = IT_1 \oplus L_1.$$

We assume that T_1, L_1 are free S-modules, say $T_1 \simeq S^d, L_1 \simeq S^c$. Consider the map

$$\Phi = F_1 \oplus \dot{F}_1 : T_1 \oplus L_1 \to P_1.$$

Then Φ is defined by an invertible matrix

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix},$$

i.e.,

$$\Phi \begin{pmatrix} t \\ l \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \begin{pmatrix} \sigma(t) \\ \sigma(l) \end{pmatrix}.$$

The map Φ is uniquely determined by $\dot{F}_1$

$$\dot{F}_1 \begin{pmatrix} t \\ l \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \begin{pmatrix} \dot{\sigma}(t) \\ \sigma(l) \end{pmatrix}.$$

Let $\mathcal{P}_2 = (P_2, Q_2, F_2, \dot{F}_2)$ be another window. Take a normal decomposition $P_2 = T_2 \oplus L_2, Q_2 = IT_2 \oplus L_2$ with free T_2, L_2. We consider $\mathrm{Hom}(\mathcal{P}_1, \mathcal{P}_2)$. A map

$\alpha : \mathcal{P}_1 \to \mathcal{P}_2$ is given by a matrix

$$\begin{pmatrix} X & J \\ Z & Y \end{pmatrix} \tag{2.23}$$

with $X \in \operatorname{Hom}(T_1, T_2), Y \in \operatorname{Hom}(L_1, L_2), Z \in \operatorname{Hom}(T_1, L_2), J \in \operatorname{Hom}(L_1, IT_2)$. X, Y, Z have coefficients in S and J has coefficients in I. Then α is a homomorphism if and only if the diagram

$$\begin{tikzcd}
IT_1 \oplus L_1 \arrow[r, "\alpha"] \arrow[d, "\dot{F}_1"] & IT_2 \oplus L_2 \arrow[d, "\dot{F}_2"] \\
IT_1 \oplus L_1 \arrow[r, "\alpha"] & IT_2 \oplus L_2
\end{tikzcd}$$

is commutative (Recall: $\dot{F}$ determines F). The diagram is commutative if and only if

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \begin{pmatrix} \sigma(X) & \dot{\sigma}(J) \\ \theta\sigma(Z) & \sigma(Y) \end{pmatrix} = \begin{pmatrix} X & J \\ Z & Y \end{pmatrix} \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}, \tag{2.24}$$

where θ is defined in Lemma 2.34.

Claim: Let $\mathcal{P}_1, \mathcal{P}_2$ be two nilpotent windows which have the same base change $\bar{\mathcal{P}}$. Then there is a unique isomorphism $\mathcal{P}_1 \to \mathcal{P}_2$ which lifts $\mathrm{id}_{\bar{\mathcal{P}}}$.

Proof of the claim: Suppose $\bar{\mathcal{P}} = (\bar{P}, \bar{Q}, \bar{F}, \dot{\bar{F}})$. Assume $\bar{P} = \bar{T} \oplus \bar{L}$ is a normal decomposition. Assume $\bar{T} = \bar{S}^d, \bar{L} = \bar{S}^c$ and that $\bar{\Phi} = \bar{F} \oplus \dot{\bar{F}} : \bar{T} \oplus \bar{L} \to \bar{P}$ is defined by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Let $P_i = T_i \oplus L_i$, $i = 1, 2$, be normal decompositions of P_i. Without loss of generality, we can assume $T_i \otimes_S \bar{S} = \bar{T}, L_i \otimes_S \bar{S} = \bar{L}$. We have $T_1 \simeq T_2 = T, L_1 \simeq L_2 = L$. Suppose Φ_i is given be a matrix

$$\begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix}.$$

Suppose $\alpha : \mathcal{P}_1 \to \mathcal{P}_2$ is a morphism given by a matrix as in (2.23), which lifts the identity $\mathrm{id}_{\bar{\mathcal{P}}}$. By (2.24), we have

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \begin{pmatrix} \sigma(X) & \dot{\sigma}(J) \\ \theta\sigma(Z) & \sigma(Y) \end{pmatrix} = \begin{pmatrix} X & J \\ Z & Y \end{pmatrix} \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}. \tag{2.25}$$

Since α lifts the identity, we have that

$$\begin{pmatrix} E_d & 0 \\ 0 & E_c \end{pmatrix} - \begin{pmatrix} X & J \\ Z & Y \end{pmatrix} \tag{2.26}$$

has coefficients in $\mathfrak{c}$.

Consider the left side of (2.25).

(2.27)

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \begin{pmatrix} \sigma(X) & \dot{\sigma}(J) \\ \theta\sigma(Z) & \sigma(Y) \end{pmatrix} = \begin{pmatrix} A_2\sigma(X) + \theta B_2\sigma(Z) & A_2\dot{\sigma}(J) + B_2\sigma(Y) \\ C_2\sigma(X) + \theta D_2\sigma(Z) & C_2\dot{\sigma}(J) + D_2\sigma(Y) \end{pmatrix}$$

By (2.26) and the assumption $\sigma(\mathfrak{c}) = 0$, we have $\sigma(X) = 1, \sigma(Y) = 1, \sigma(Z) = 0$, thus (2.27) becomes

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} + \begin{pmatrix} 0 & A_2\dot{\sigma}(J) \\ 0 & C_2\dot{\sigma}(J) \end{pmatrix} \tag{2.28}$$

Then (2.25) becomes

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} + \begin{pmatrix} 0 & A_2\dot{\sigma}(J) \\ 0 & C_2\dot{\sigma}(J) \end{pmatrix} = \begin{pmatrix} X & J \\ Z & Y \end{pmatrix} \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \tag{2.29}$$

Multiplying (2.29) by

$$\begin{pmatrix} \breve{A}_1 & \breve{B}_1 \\ \breve{C}_1 & \breve{D}_1 \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}^{-1}$$

on the right we get

$$\begin{pmatrix} \xi_A & \xi_B \\ \xi_C & \xi_D \end{pmatrix} + \begin{pmatrix} 0 & A_2\dot{\sigma}(J) \\ 0 & C_2\dot{\sigma}(J) \end{pmatrix} \begin{pmatrix} \breve{A}_1 & \breve{B}_1 \\ \breve{C}_1 & \breve{D}_1 \end{pmatrix} = \begin{pmatrix} X & J \\ Z & Y \end{pmatrix}. \tag{2.30}$$

We see that X, Y, Z are uniquely determined by J, and J satisfies

$$\xi_B + A_2\dot{\sigma}(J)\breve{D}_1 = J. \tag{2.31}$$

Hence to prove the uniqueness and existence of α, it suffice to show that there is a unique J satisfying (2.31). We define

$$U(J) = A_2\dot{\sigma}(J)\breve{D}_1.$$

It is enough to show that U is pointwise nilpotent. In fact, once we have that U is pointwise nilpotent, then

$$(\mathrm{id} - U)^{-1} = \mathrm{id} + U + U^2 + \cdots$$

exists and $J = (\mathrm{id} - U)^{-1}\xi_B$ is the unique solution of (2.31).

The nilpotence of U follows from the nilpotence of our windows. In fact,

$$U^2(J) = A_2\dot{\sigma}(A_2\dot{\sigma}(J)\breve{D}_1)\breve{D}_1 = A_2\sigma(A_2)\dot{\sigma}^2(J)\sigma(\breve{D}_1)\breve{D}_1.$$

Inductively, we have

$$U^n(J) = A_2\sigma(A_2)\cdots\sigma^{n-1}(A_2)\dot{\sigma}^n(J)\sigma^{n-1}(\breve{D}_1)\cdots\sigma(\breve{D}_1)\breve{D}_1.$$

Let $N = \dot{\sigma}^{n-1}(J)$, and $M = \sigma^{n-2}(\breve{D}_1)\cdots\breve{D}_1$. By (2.16), there is an integer $c > 0$ such that

$$\sigma^{c-1}(\breve{D}_1)\cdots\sigma(\breve{D}_1)\breve{D}_1 \in I.$$

So if we take $n \geq c + 1$, M has coefficients in I. Since $\dot{\sigma}(\mathfrak{c}) \subset \mathfrak{c}$, we see that N has coefficients in $\mathfrak{c}$. Then

$$\dot{\sigma}(N)\sigma(M) = \dot{\sigma}(NM) = \sigma(N)\dot{\sigma}(M) = 0$$

since $\sigma(\mathfrak{c}) = 0$. Hence U is nilpotent. Now the claim follows.

The above proof is also valid when our windows do not have free normal decompositions.

Next we show the base change functor is fully faithful, i.e., for any nilpotent $\mathcal{F}$-window $\mathcal{P}_1, \mathcal{P}_2$, with base change $\bar{\mathcal{P}}_1, \bar{\mathcal{P}}_2$, then

$$\mathrm{Hom}_{\mathcal{F}}(\mathcal{P}_1, \mathcal{P}_2) \longrightarrow \mathrm{Hom}_{\bar{\mathcal{F}}}(\bar{\mathcal{P}}_1, \bar{\mathcal{P}}_2)$$

is a bijection.

From the above claim, the map is bijective when $\bar{\mathcal{P}}_1 \simeq \bar{\mathcal{P}}_2$. In the general case, let $\bar{\alpha} : \bar{\mathcal{P}}_1 \to \bar{\mathcal{P}}_2$ be a morphism. Consider the isomorphism

$$\begin{pmatrix} \mathrm{id}_{\bar{\mathcal{P}}_1} & 0 \\ \bar{\alpha} & \mathrm{id}_{\bar{\mathcal{P}}_2} \end{pmatrix} : \bar{\mathcal{P}}_1 \oplus \bar{\mathcal{P}}_2 \to \bar{\mathcal{P}}_1 \oplus \bar{\mathcal{P}}_2.$$

It lifts uniquely to an isomorphism

$$\begin{pmatrix} \mathrm{id}_{\mathcal{P}_1} & 0 \\ \alpha & \mathrm{id}_{\mathcal{P}_2} \end{pmatrix} : \mathcal{P}_1 \oplus \mathcal{P}_2 \to \mathcal{P}_1 \oplus \mathcal{P}_2.$$

Then α is the unique lift of $\bar{\alpha}$. This shows that the base change functor is fully faithful.

The base change functor is essentially surjective since any window $\bar{\mathcal{P}}$ lifts by lifting the matrix. If we do not assume our windows have free normal decompositions, we have to apply Proposition 2.23. Now the proof of Proposition 2.44, hence the proof of Theorem 2.43 is complete. □

Definition 2.45. *Let R be a commutative ring with 1 such that p is nilpotent in R. We denote by R^{crys} the category defined as follows. An object of R^{crys} is a pair $(f : S \twoheadrightarrow R, \delta_S)$, where $f : S \twoheadrightarrow R$ is a surjective homomorphism and δ_S is a divided power structure on* Ker$f$*. A morphism between $(f : S \twoheadrightarrow R, \delta_S)$ and $(f' : S' \twoheadrightarrow R, \delta_{S'})$ in R^{crys} is a ring homomorphism $\alpha : S \to S'$ such that $f'\alpha = f$ and α respects the divided power structures.*

Definition 2.46. *Let R be as above. A **crystal** $\mathcal{M}$ over R consists of the following data*:
(i) *for each $(f : S \twoheadrightarrow R, \delta_S) \in R^{\mathrm{crys}}$, there is a finitely generated S-module M_S*;
(ii) *for each morphism $\alpha : (f : S \twoheadrightarrow R, \delta_S) \to (f' : S' \twoheadrightarrow R, \delta_{S'}) \in R^{\mathrm{crys}}$, there is an isomorphism*

$$\phi_{S',S} : S' \otimes_S M_S \simeq M_{S'};$$

such that for any two morphisms $\alpha : (f : S \twoheadrightarrow R, \delta_S) \to (f' : S' \twoheadrightarrow R, \delta_{S'})$, and $\beta : (f'' : S' \twoheadrightarrow R, \delta_{S'}) \to (f' : S'' \twoheadrightarrow R, \delta_{S''})$, the following diagram

$$\begin{tikzcd}
S'' \otimes_{S'} S' \otimes_S M_S \arrow[r, "\mathrm{id}_{S''} \otimes \phi_{S',S}"] \arrow[d, "\simeq"] & S'' \otimes_S M_{S'} \arrow[d, "\phi_{S'',S'}"] \\
S'' \otimes_S M_S \arrow[r, "\phi_{S'',S}"] & M_{S''}
\end{tikzcd}$$

is commutative.

Remark 2.46.1. In fact, the category R^{crys} can be used to define a site Crys$X$, where $X = \mathrm{Spec}R$. See [M] page 106-111. We have the structure sheaf $\mathcal{O}_X^{\mathrm{crys}}$ on this site defined by $\mathcal{O}_X^{\mathrm{crys}}(S) = S$ for any $(f : S \twoheadrightarrow R, \delta_S) \in R^{\mathrm{crys}}$. Then we can define a crystal as a coherent sheaf $\mathcal{M}$ of $\mathcal{O}_{\mathrm{Spec}R}^{\mathrm{crys}}$-modules satisfying an additional condition: for $(\alpha : S \to S') \in R^{\mathrm{crys}}$, the restriction map $\mathcal{M}(S) \to \mathcal{M}(S')$ induces an isomorphism

$$S' \otimes_S \mathcal{M}(S) \simeq \mathcal{M}(S').$$

It is easy to globalize the above notions.

For any $(f : S \twoheadrightarrow R, \delta_S) \in R^{\mathrm{crys}}$, we have proved that the base change functor induced by $\mathcal{W}_{S/R} \to \mathcal{W}_R$ (Theorem 2.43) defines an equivalence

$$f_\bullet : \{\text{nilpotent windows of } \mathcal{W}_{S/R}\} \to \{\text{nilpotent displays over } R\}\,.$$

For each nilpotent display $\mathcal{P}$ over R, let $\mathcal{P}_S = (P_S, Q_S, F, \dot{F})$ be the corresponding nilpotent $\mathcal{W}_{S/R}$-window under the above equivalence. Let $\mathbb{D}_\mathcal{P}(S) = P_S/I_S P_S$. Then $\mathbb{D}_\mathcal{P}(S)$ is a finitely generated projective S-module. Let $\alpha : (f : S \twoheadrightarrow R, \delta_S) \to (f' : S' \twoheadrightarrow R, \delta_{S'})$ be a morphism in R^{crys}. Since $f' = \alpha f$, we have $f'_\bullet = \alpha_\bullet f_\bullet$. Recall, $f_\bullet$ is the base change functor induced by f, see Definition 2.37. Hence if we let $\mathcal{P}_{S'} = \alpha_\bullet(\mathcal{P}_S)$ be the nilpotent display obtained by the base change induced by α, then $f'_\bullet(\mathcal{P}_{S'}) = \mathcal{P}$. So there is a canonical isomorphism $\phi_{S',S} : S' \otimes_S \mathbb{D}_\mathcal{P}(S) \simeq \mathbb{D}_\mathcal{P}(S')$.

Proposition 2.47. *For a given nilpotent display $\mathcal{P}$ over R, the assignment*

$$(f : S \twoheadrightarrow R, \delta_S) \mapsto \mathbb{D}_\mathcal{P}(S)$$

$$[\alpha : (f : S \twoheadrightarrow R, \delta_S) \to (f' : S' \twoheadrightarrow R, \delta_{S'})] \mapsto \phi_{S',S}$$

defines a crystal over R.

The proposition is clear.

Recall the notion of connections.

Definition 2.48. *Let S be a scheme and X a finite type scheme over S. Let $\mathcal{E}$ be a coherent sheaf over X. A **connection** on $\mathcal{E}$ is an $\mathcal{O}_S$-linear map*

$$\nabla : \mathcal{E} \to \mathcal{E} \otimes \Omega^1_{X/S}$$

satisfying

$$\nabla(fs) = s \otimes df + f\nabla m,$$

where $\Omega^1_{X/S}$ is the Kähler differential and $d : \mathcal{O}_X \to \Omega_{X/S}$ is the natural map, f is a section of $\mathcal{O}_X$ and s is a section of $\mathcal{E}$.

Similarly, we can define a connection for a crystalline site. It just replaces X in the above definition by Crys$X$.

To a crystal $\mathcal{M}$ on $X = \mathrm{Spec}R$, we will associate a connection. Let I be the kernel of the multiplication map $R \otimes R \to R$. Then $\Omega^1_R := \Omega^1_{R/\mathbb{Z}} \simeq I/I^2$, see [H], II.8. The map $d : R \to \Omega^1_R$ is $dr = 1 \otimes r - r \otimes 1 (\mathrm{mod}\ I^2)$. Let

$$U = (R \otimes R)/I^2.$$

Then the kernel of the multiplication map $U \to R$ is I/I^2. There is a natural pd structure δ_U on I/I^2 defined by

$$\gamma_1(x) = x, \quad \gamma_i(x) = 0, \quad i > 1.$$

Then $(U \to R, \delta_U) \in R^{\mathrm{crys}}$. We can view $\mathrm{id} : R \to R$ with the trivial pd structures as an element of R^{crys}. There are two morphisms in R^{crys}: $u_1 : R \to U$ defined by $u_1(r) = 1 \otimes r (\mathrm{mod}\ I^2)$, $u_2 : R \to U$ defined by $u_2(r) = r \otimes 1 (\mathrm{mod}\ I^2)$. Note that $dr = u_1(r) - u_2(r)$. There is an isomorphism

$$U \simeq R \oplus \Omega^1_R. \tag{2.32}$$

Under this isomorphism, u_1 is identified with $\kappa : R \to R \oplus \Omega^1_R$, $\kappa(r) = (r, 0)$; u_2 is identified with $\kappa \oplus (-d) : R \to R \oplus \Omega^1_R$, $r \mapsto (r, -dr)$. By the definition of a crystal, we have isomorphisms

$$U \otimes_{u_1,R} M_R \simeq M_U \simeq U \otimes_{u_2,R} M_R.$$

Under the identifications using the isomorphism (2.32), we have the following diagram

$$\begin{tikzcd}
M_R \otimes_{R,\kappa} (R \oplus \Omega^1_R) \arrow[rr, "\phi", "\simeq"'] \arrow[dr, "\rho_1"'] & & M_R \otimes_{R,\kappa\oplus(-d)} (R \oplus \Omega^1_R) \arrow[dl, "\rho_2"] \\
& M_R &
\end{tikzcd}$$

where ρ_1, ρ_2 are induced by $U \to R$.

Proposition 2.49. *For any $m \in M_R$, define*

$$\nabla(m) = \phi(m \otimes (1, 0)) - m \otimes (1, 0).$$

Then $\nabla(m) \in M_R \otimes \Omega^1_R$ and

$$\nabla(fm) = m \otimes df + f\nabla(m)$$

for $f \in R, m \in M_R$.

Proof. Note that $\rho_i(m \otimes (1, 0)) = m$ for $i = 1, 2$ and $\rho_2\phi = \rho_1$. Hence we have $\nabla(m) \in \mathrm{Ker}(\rho_2) = M_R \otimes \Omega^1_R$. Since ϕ is a U-module homomorphism, we have

$$\begin{aligned}\phi(fm \otimes (1, 0)) = \phi(m \otimes (f, 0)) = (m \otimes (1, 0) + \nabla m)(f, 0)\\ = m \otimes (f, 0) + f\nabla m = m \otimes (f, -df) + m \otimes (0, df) + f\nabla m\\ = fm \otimes (1, 0) + m \otimes df + f\nabla m.\end{aligned}$$

We get

$$\nabla(fm) = m \otimes df + f\nabla(m).$$

□

By base change, we can get a homomorphism

$$\nabla : \mathcal{M} \to \mathcal{M} \otimes \Omega^1_{\mathrm{Spec}R},$$

which is a connection by Proposition 2.48.

In [M], Messing associate to any formal p-divisible group X a crystal $\mathbb{D}_X$, called the **Grothendieck-Messing crystal**.

Theorem 2.50. *Let $\mathcal{P}$ be a nilpotent display over R. Let $X = \mathrm{BT}_{\mathcal{P}}$. Then there is a canonical isomorphism*

$$\mathbb{D}_{\mathcal{P}}(S) \simeq \mathbb{D}_X(S)$$

for any $(f : S \twoheadrightarrow R, \delta_S) \in R^{crys}$.

Definition 2.51. *Given are $(S \twoheadrightarrow R, \delta_S) \in R^{crys}$, and a nilpotent display $\mathcal{P}$ over R. Then a **deformation** of $\mathcal{P}$ to S is pair $(\tilde{\mathcal{P}}, \iota)$, where $\tilde{\mathcal{P}}$ is a display over S and ι is an isomorphism $\tilde{\mathcal{P}}_R \to \mathcal{P}$. Here $\tilde{\mathcal{P}}_R$ is the base change of $\tilde{\mathcal{P}}$ to R. A **homomorphism** $f : (\tilde{\mathcal{P}}, \iota) \to (\tilde{\mathcal{P}}', \iota')$ of deformations is a homomorphism $f : \tilde{\mathcal{P}} \to \tilde{\mathcal{P}}'$ of displays such that $\iota' \circ f_R = \iota$. We denote by*

$$\mathrm{Def}_{\mathcal{P}}(S)$$

the set of isomorphism classes of deformations of $\mathcal{P}$ to S.

Definition 2.52. *Let $\mathcal{P} = (P, Q, F, \dot{F})$ be a display over R. Recall we have defined $\mathbb{D}_{\mathcal{P}}(R) = P/I_R P$ in Proposition* 2.47. *We call the quotient map*

$$\mathbb{D}_{\mathcal{P}}(R) = P/I_R P \twoheadrightarrow P/Q$$

*the **Hodge filtration** of $\mathcal{P}$.*

Given are $(f : S \twoheadrightarrow R, \delta_S) \in R^{\text{crys}}$ and a nilpotent display $\mathcal{P}$ over R. We have defined $\mathbb{D}_{\mathcal{P}}(S)$ in Proposition 2.47. By a **lifting** of the Hodge filtration of $\mathcal{P}$, we mean a map $\rho : \mathbb{D}_{\mathcal{P}}(S) \twoheadrightarrow U$, where U is a finitely generated projective S-module, and a commutative diagram

$$\begin{tikzcd}
\mathbb{D}_{\mathcal{P}}(S) \arrow[r] \arrow[d, "\rho"] & \mathbb{D}_{\mathcal{P}}(R) \arrow[d] \\
U \arrow[r] & P/Q
\end{tikzcd}$$

such that $U \otimes_S R \simeq P/Q$.

Theorem 2.53. *Let $\tilde{\mathcal{P}} = (\tilde{P}, \tilde{Q}, F, \dot{F})$ be a deformation of $\mathcal{P}$ to S. Then the Hodge filtration $\tilde{P}/I_S\tilde{P} \twoheadrightarrow \tilde{P}/\tilde{Q}$ of $\tilde{\mathcal{P}}$ is a lifting of the Hodge filtration of $\mathcal{P}$. This assignment gives a bijection between the set* $\text{Def}_{\mathcal{P}}(S)$ *and the set of isomorphism classes of liftings of the Hodge filtration of $\mathcal{P}$.*

Proof. We first show that $\tilde{P}/I_S\tilde{P} \to \tilde{P}/\tilde{Q}$ is a lifting of the Hodge filtration of $\mathcal{P}$. By definition, $\tilde{P}/\tilde{Q}$ is finitely generated, projective, and we have $S \otimes_R (\tilde{P}/\tilde{Q}) \simeq P/Q$. So it suffices to show that $\mathbb{D}_{\mathcal{P}}(S) \simeq \tilde{P}/I_S\tilde{P}$. By the definition of $\mathbb{D}_{\mathcal{P}}(S)$, we only have to show that there is a nilpotent $\mathcal{W}_{S/R}$-window $(P_1, Q_1, F, \dot{F})$ with $P_1 = \tilde{P}$.

Consider the map $\pi : \tilde{P} \to \tilde{P} \otimes_S R \simeq P$ and $\psi : \tilde{Q} \to \tilde{Q} \otimes_S R \simeq Q$. Let $\tilde{P} = \tilde{T} \oplus \tilde{L}, \tilde{Q} = I_S\tilde{T} \oplus \tilde{L}$ be a normal decomposition of $\tilde{\mathcal{P}}$. Let $T = W(R) \otimes_{W(S)} \tilde{T}, L = W(R) \otimes_{W(S)} \tilde{L}$. Then we can identify P with $T \oplus L$ and identify Q with $I_R T \oplus L$. Then π and ψ are surjective. Put $\mathfrak{a} = \text{Ker}(S \to R)$. We know that $W(\mathfrak{a}) = \text{Ker}(W(S) \twoheadrightarrow W(R))$, hence $W(\mathfrak{a})\tilde{P} = \text{Ker}(\tilde{P} \twoheadrightarrow P)$. Then it is clear that

$$\pi^{-1}(Q) = \tilde{Q} + W(\mathfrak{a})\tilde{P} = \tilde{\mathfrak{a}}\tilde{P}.$$

Here $\tilde{\mathfrak{a}}$ is defined after Lemma 2.41. Note that there is a map $\dot{F}$ on $\tilde{Q}$. We extend $\dot{F}$ to $\pi^{-1}(Q)$ by $\dot{F}|_{\tilde{\mathfrak{a}}\tilde{P}} = 0$. Note that $\tilde{Q} \cap \tilde{\mathfrak{a}}\tilde{P} = \tilde{\mathfrak{a}}\tilde{L}$ and $\dot{F}(al) = {}^{F}a\dot{F}(\tilde{l}) = 0$, for $a \in \tilde{\mathfrak{a}}, l \in \tilde{L}$, since ${}^{F}a = 0$ for all $a \in \tilde{\mathfrak{a}}$ by Equation (2.22). Hence the extended $\dot{F}$ is well-defined. It is easy to see that $(\tilde{P}, \pi^{-1}, F, \dot{F})$ is a nilpotent $\mathcal{W}_{S/R}$-window which lifts $\mathcal{P}$ under the base change functor. Hence $\mathbb{D}_{\mathcal{P}}(S) = \tilde{P}/I_S\tilde{P}$.

Conversely, let $\rho : \mathbb{D}_{\mathcal{P}}(S) \twoheadrightarrow U$ be a lifting of the Hodge filtration of $\mathcal{P}$. We will construct a deformation of $\mathcal{P}$ to S. Let $(\tilde{P}, \tilde{Q}, F, \dot{F})$ be a nilpotent $\mathcal{W}_{S/R}$-window which lifts $\mathcal{P}$ (see Theorem 2.42). Then $\mathbb{D}_{\mathcal{P}}(S) = \tilde{P}/I_S\tilde{P}$. Put

$$U' = \text{Ker}(\tilde{P} \to \tilde{P}/I_S\tilde{P} = \mathbb{D}_{\mathcal{P}}(S) \to U).$$

Then it can be checked that $(\tilde{P}, U', F, \dot{F})$ is a display over S. It is easy to see that the above two constructions are inverse to each other, hence give the desired bijection. □

Theorem 2.54 (Grothendieck-Messing)**.** *Let X be a formal p-divisible group over R and $\mathbb{D}_X$ the Grothendieck-Messing crystal of X. Then we have a surjection*

$$\mathbb{D}_X(R) \twoheadrightarrow \mathrm{Lie}(X),$$

which is called the ***Hodge filtration*** *of $\mathbb{D}_X$. The isomorphism classes of deformations of X to S are bijective to the isomorphism classes of liftings of the Hodge filtration of $\mathbb{D}_X$.*

For the proof, see [M].

Remark 2.54.1 By theorems 2.49, 2.52, 2.53, to prove the Main Theorem 2.32 for S with $S \to R \in R^{\mathrm{crys}}$, it suffice to prove the main theorem for R. We will not do this. See [Z1].

3. Classification of Formal p-Divisible Groups up to Isogeny

As before, we fix a prime number p. Let R be a commutative ring with 1.

Definition 3.1. *Let X, Y be two formal groups over R of the same dimension. Assume*

$$X = \mathrm{Spf} R[[T_1, \dots, T_d]], \quad Y = \mathrm{Spf} R[[S_1, \dots, S_d]].$$

A homomorphism $f : X \to Y$ is called an ***isogeny*** *if for*

$$f^* : R[[S_1, \dots, S_d]] \to R[[T_1, \dots, T_d]]$$

there is an integer $n \in \mathbb{N}$ such that

$$T_i^n \subset \mathrm{Im} f^*.$$

Remark 3.1.1. By Weierstrass Preparation Theorem (Theorem 1.51), an isogeny is faithfully flat and finite.

Example 3.1.2. Assume that $p \cdot R = 0$ and that X is a formal group over R given by

$$X = \mathrm{Spf} R[[T_1, \dots, T_d]].$$

We define a new formal group $X^{(p)}$ by

$$X^{(p)} : \mathbf{Nil}_R \longrightarrow \mathbf{Ab}$$

$$X^{(p)}(N) = X(N_{[\mathrm{Frob}]}),$$

where Frob : $R \to R$ is the Frobenius $x \mapsto x^p$, and $N_{[\mathrm{Frob}]}$ is the R-algebra on N defined by $r \circ n = r^p \cdot n$, for $r \in R, n \in N$. The map $\phi : N \to N_{[\mathrm{Frob}]}$, $\phi(n) = n^p$ is an algebra homomorphism. Hence we can apply the functor X to obtain a homomorphism

$$X(\phi) : X(N) \to X(N_{[\mathrm{Frob}]}) = X^{(p)}(N)$$

of formal groups.

Claim 3.1.3. $X(\phi)$ is an isogeny. It is called the **Frobenius** homomorphism of X and will be denoted by F_X.

In fact, as a set $X(N) = X(N_{[\mathrm{Frob}]}) = N^d$, and F_X is given by $(n_1, \dots, n_d) \mapsto (n_1^p, \dots, n_d^p)$. Hence

$$F_X^* : R[[T_1, \dots, T_d]] \longrightarrow R[[T_1, \dots, T_d]]$$

is given by

$$T_i \mapsto T_i^p.$$

So it suffices to show that F_X preserves the group structures. Suppose the group structure of X is given by the group law $F_1(\underline{T}, \underline{T}'), \dots, F_d(\underline{T}, \underline{T}')$. Then the group law of $X^{(p)}$ is given by $F_1^{(p)}(\underline{T}, \underline{T}'), \dots, F_d^{(p)}(\underline{T}, \underline{T}')$, where $F_i^{(p)}(\underline{T}, \underline{T}')$ is obtained by applying the Frobenius to the coefficients of $F_i(\underline{T}, \underline{T}')$. Then

$$\underline{n} +_X \underline{n}' = (F_i(\underline{n}, \underline{n}')),$$

Hence

$$F_X(\underline{n} +_X \underline{n}') = (F_i(\underline{n}, \underline{n}')^p),$$

while

$$F_X(\underline{n}) +_{X^{(p)}} F_X(\underline{n}') = (F_i^{(p)}(F_X(\underline{n}), F_X(\underline{n}'))).$$

It is easy to see that

$$F_X(\underline{n} +_X \underline{n}') = F_X(\underline{n}) +_{X^{(p)}} F_X(\underline{n}').$$

We are done.

Lemma 3.2. *Assume $p \cdot R = 0$. Let $\mathcal{P} = (P, Q, F, \dot{F})$ be a display over R. Put $X = \mathrm{BT}_{\mathcal{P}}$. Let $\mathcal{P}^{(p)}$ be the base change of $\mathcal{P}$ under* Frob : $R \to R$.
(i) *If we write $\mathcal{P}^{(p)} = (P^{(p)}, Q^{(p)}, F^{(p)}, \dot{F}^{(p)})$, then*

$$\begin{aligned} P^{(p)} &= W(R) \otimes_{F,W(R)} P \\ Q^{(p)} &= I_R \otimes_{F,W(R)} P + \quad \mathrm{Image(W(R) \otimes_{F,W(R)} Q)} \end{aligned}$$

The operators $F^{(p)}$ and $\dot{F}^{(p)}$ are uniquely determined by the relations:

$$\begin{aligned} F^{(p)}(w \otimes x) &= {}^F w \otimes F(x), \quad w \in W(R), x \in P \\ \dot{F}^{(p)}({}^V w \otimes x) &= w \otimes F(x), \\ \dot{F}^{(p)}(w \otimes y) &= {}^F w \otimes \dot{F}(y), \quad y \in Q. \end{aligned}$$

(ii) *The map*

$$V^\sharp : P \longrightarrow W(R) \otimes_{F,W(R)} P$$

defined in Lemma 2.30 *induces a morphism* $\mathrm{Fr}_{\mathcal{P}} : \mathcal{P} \to \mathcal{P}^{(\mathrm{p})}$, *which is called the Frobenius homomorphism of $\mathcal{P}$.*
(iii) *We have an isomorphism $X^{(p)} \simeq \mathrm{BT}_{\mathcal{P}^{(p)}}$ and F_X can be identified with* $\mathrm{BT}(\mathrm{Fr}_{\mathcal{P}})$ *under this isomorphism.*

The first two parts of the lemma is Example 23 in [Z1]. The third part of the lemma is Proposition 87 of [Z1]. The following proof is a copy of them.

Proof. (i) By Proposition 2.13, we have $W(\mathrm{Frob}) = F$. So $P^{(p)} = W(R) \otimes_{F,W(R)} P$. Now Part (i) follows from the definition (2.37) directly.
(ii) By definition of $V^\sharp$, it is easy to see that $V^\sharp(Q) \subset Q^{(p)}$. Using the fact that P is generated as a $W(R)$-module by the elements $\dot{F}(y)$ for $y \in Q$, a routine calculation shows that $V^\sharp$ commutes with F and $\dot{F}$, hence $V^\sharp$ induces a homomorphism of displays

$$\mathrm{Fr}_{\mathcal{P}} : \mathcal{P} \to \mathcal{P}^{(\mathrm{p})}.$$

(iii) By definition, for $N \in \mathbf{Nil}_R$,

$$\mathrm{BT}_{\mathcal{P}^{(p)}}(N) = \mathrm{Coker}[\dot{F}^{(p)} - \mathrm{id} : \widehat{Q^{(p)}}(N) \to \widehat{P^{(p)}}(N)],$$

see Theorem 2.29. Here

$$\widehat{P^{(p)}(N)} = \hat{W}(N) \otimes_{W(R)} P^{(p)} = \hat{W}(N) \otimes_{W(R)} W(R) \otimes_{F,W(R)} P.$$

While by definition,

$$X^{(p)}(N) = X(N_{[\mathrm{Frob}]}) = \mathrm{Coker}\left\{\hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} Q \to \hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} P\right\}.$$

The identification

$$\theta : \hat{W}(N) \otimes_{W(R)} W(R) \otimes_{F,W(R)} P \simeq \hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} P$$

$$\xi \otimes 1 \otimes y \mapsto {}^F\xi \otimes \dot{F}(y), \quad \xi \in \hat{W}(N), y \in Q$$

and a similar isomorphism for Q establish the isomorphism $\mathrm{BT}_{\mathcal{P}^{(p)}} \simeq X^{(p)}$.

$$\begin{tikzcd}
0 \arrow[r] & \widehat{Q^{(p)}}(N) \arrow[r] \arrow[d, "\theta"] & \widehat{P^{(p)}}(N) \arrow[r] \arrow[d, "\theta"] & \mathrm{BT}_{\mathcal{P}^{(p)}}(N) \arrow[r] & 0 \\
0 \arrow[r] & \hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} Q \arrow[r] & \hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} P \arrow[r] & X^{(p)}(N) \arrow[r] & 0
\end{tikzcd}$$

Consider the following two diagram

$$\begin{tikzcd}
\hat{W}(N) \otimes_{W(R)} P \arrow[r] \arrow[d, "{}^F\otimes \mathrm{id}_P"'] & X(N) \arrow[d, "F_X"] \\
\hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} P \arrow[r] & X(N_{[\mathrm{Frob}]})
\end{tikzcd}
\qquad
\begin{tikzcd}
\hat{W}(N) \otimes_{W(R)} P \arrow[r] \arrow[d, "\mathrm{id}\otimes V^\sharp"] & X(N) \arrow[d, "F_X"] \\
\hat{W}(N) \otimes_{W(R)} P^{(p)} \arrow[r] & X(N_{[\mathrm{Frob}]})
\end{tikzcd}$$

where the bottom arrow of the second diagram is obtained via the identification $\theta : \hat{W}(N) \otimes_{W(R)} P^{(p)} \simeq \hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} P$. To show $F_X \simeq \mathrm{BT}(\mathrm{Fr}_{\mathcal{P}})$, we only have to check that the second diagram is commutative. Since the Frobenius on $\hat{W}(N)$ is just the operator ^{F}, the left diagram is commutative. Hence, to prove (iii), it suffices to verify that for $\xi \in \hat{W}(N)$ and $x \in P$, the elements ${}^F \otimes x \in \hat{W}(N_{[\mathrm{Frob}]}) \otimes_{W(R)} P = \hat{W}(N) \otimes_{F,W(R)} P$ and $\xi \otimes V^\sharp x \in \hat{W}(N) \otimes_{W(R)} P^{(p)}$ have the same image by the lower horizontal map of the left diagram. Since P is generated as an abelian group by elements of the form $u\dot{F}(y)$ for $y \in Q$ and $u \in W(R)$, it is enough to verify the equality for $x = u\dot{F}y$. In $\hat{W}(N) \otimes_{F,W(R)} P$, we have the equalities:

$$ {}^F\xi \otimes u\dot{F}y = {}^F(\xi u) \otimes \dot{F}y = \dot{F}(\xi u \otimes y). $$

The last element has the same image in $X(N_{[\mathrm{Frob}]})$ as $\xi u \otimes y$, by the exact sequence (2.11). Hence the lemma follows from the equality:

$$ \xi \otimes V^\sharp(u\dot{F}y) = \xi u \otimes y. $$

We note that here the left hand side is considered as an element of $\hat{W}(N) \otimes_{W(R)} P^{(p)}$, while the right hand side is considered as an element of $\hat{W}(N) \otimes_{F,W(R)} P$. □

Remark 3.2.1. Let $f : X \to Y$ be a homomorphism of formal groups. Then f is an isogeny if and only if there is an integer m and a homomorphism $g : Y \to X^{(p^m)}$ such that $g \circ f = F_X^m$.

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "F_X^m"'] & & Y \arrow[dl, "g"] \\
& X^{(p^m)} &
\end{tikzcd}$$

This is clear by the definition of an isogeny.

Next, we consider formal groups over a field.

Let K be a field such that $p \cdot K = 0$. Let $K_n = K^{1/p^n}$. We take K_n in a fixed algebraic closure of K and such that $K_n \subset K_{n+1}$. Note that if K is perfect, then $K_n = K$. Define

$$ A_K = \cup W(K_n). \tag{3.1} $$

Note that if K is perfect, we have $A_K = W(K)$.

Lemma 3.3. *The ring A_K is a discrete valuation ring and p is a prime element. Furthermore, we have*

$$A_K/pA_K \simeq \cup K_n,$$

which is the perfect closure K^{perf} of K.

Proof. As in the proof of Lemma 2.42, we can see that $p \in \text{rad}A_K$. Since $p = V \circ F$ (see the proof of Proposition 2.15) in each $W(K_n)$, by Proposition 2.13, we see that

$$p(x_0, x_1, \dots) = (0, x_0^p, x_1^p, \dots).$$

Then it is clear that $A_K/pA_K = \cup K_n$, which is a field. It follows that A_K is a local ring and pA_K is the maximal ideal. It also follows that p is not nilpotent in A_K. In fact, if p is nilpotent, then $p^k = 0$ in A_K. Hence

$$p^k(x_0, x_1, \dots) = 0,$$

for every $(x_0, x_1, \dots) \in W(K_n)$ and every n. But on the other hand, we have

$$p^k(x_0, x_1, \dots) = (0, \dots, 0, x_0^{p^k}, x_1^{p^k}, \dots) \neq 0,$$

where $x_0^{p^k}$ is in the $k+1$-th places. This is a contradiction.

Claim: For any $\xi \in A_K$, there is a natural number t such that $\xi = p^t\zeta$ for a unit $\zeta \in A_K$.

Suppose $\xi \in W(K_n)$. Let t be the smallest integer such that we can write $\xi = {}^{V^t}\eta$ with $\eta \in W(K_n)$ and $\mathbb{W}_0(\eta) \neq 0$. It is clear such t exist. Write $\eta = (x_0, x_1, \dots)$, $x_0 \neq 0$. Define $\zeta = (x_0^{1/p^t}, x_1^{1/p^t}, \dots) \in W(K_{n+t})$. Then $\eta = {}^{F^t}\zeta$. Then $\xi = p^t\zeta$. We show ζ is a unit. Actually, for any $y = (y_0, y_1, \dots) \in W(K_i)$ for some i with $y_0 \neq 0$, we will show that y is a unit in A_K. In fact, we can write $y = [y_0] + z$ with $z \in {}^{V}W(K_i)$, see Lemma 2.8 (2). By Lemma 2.8 (1), we see $[y_0]$ is a unit in $W(K_i)$. By Lemma 2.20, we know $z \in \text{rad}W(K_i)$, hence y is a unit. We get the claim.

By the claim and the fact p is not nilpotent in A_K, we see that A_K is an integral domain. Now it is clear A_K is a discrete valuation ring by the above claim. □

Remark 3.3.1. We claim that $A_K \otimes_{\mathbb{Z}} \mathbb{Q} = W(K) \otimes_{\mathbb{Z}} \mathbb{Q}$, i.e., A_K and $W(K)$ have the same fraction field. It is clear that $W(K) \otimes_{\mathbb{Z}} \mathbb{Q} \subset A_K \otimes_{\mathbb{Z}} \mathbb{Q}$. For $\eta \in W(K_n) \subset A_K$, we know $\xi = {}^{F^n}\eta \in W(K)$. Then

$$\eta = \frac{1}{p^n} {}^{V^n F^n}\eta = \frac{1}{p^n} {}^{V^n}\xi \in W(K) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Hence $A_K \subset W(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. So we have $A_K \otimes_{\mathbb{Z}} \mathbb{Q} = W(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. We denote the quotient field by

$$W_{\mathbb{Q}}(K).$$

Note that the Frobenius ${}^{F} : A_K \to A_K$ is given by $(x_0, x_1, \dots) \mapsto (x_0^p, x_1^p, \dots)$. This is an isomorphism. We will denote it by σ later on, because there are so many maps denoted by F.

Definition 3.4. *A* ***Dieudonné module*** *over A_K is a pair (M, Φ), where M is a free A_K-module of finite type and Φ is an endomorphism of M, such that*

$$\begin{aligned}&\Phi(\xi m) = \sigma(\xi)\Phi(m), \quad \xi \in A_K, m \in M\\ &pM \subset \Phi(M) \subset M.\end{aligned}$$

Note that $\Phi(M)$ is a submodule of M: $\xi\Phi(m) = \Phi(\eta m)$ if $\sigma(\eta) = \xi$.

Remark 3.4.1. Since A_K is a principal ideal domain, any submodule of a free A_K-module should be free. From this fact, we can see that Φ in Definition 3.4 is injective. In fact, if it is not injective, then $\mathrm{Ker}\Phi$ should be a free module with positive rank. Then $\mathrm{rk}\Phi(M) < \mathrm{rk}M = \mathrm{rk}pM$, which contradicts to $pM \subset M$. Hence for a Dieudonné module (M, Φ), there is a well-defined map

$$\Psi : M \to M$$

$$m \mapsto m', \quad pm = \Phi(m').$$

This map is σ^{-1}-linear and satisfies $\Psi \circ \Phi = \Phi \circ \Psi = p$. Sometimes we will denote Ψ by $p\Phi^{-1}$.

Conversely, suppose we are given a triple (M, Φ, Ψ), where M is a free A_K-module and Φ, Ψ are endomorphisms such that Φ is σ-linear and Ψ is σ^{-1}-linear and $\Psi \circ \Phi = \Phi \circ \Psi = p$. Then it is clear that (M, Φ) is a Dieudonné module. Hence if K is perfect, Definition 3.4 is equivalent to Definition 2.26.

Definition 3.5. *A Dieudonné module (M, Φ) is called* ***nilpotent*** *if Ψ defined in Remark* 3.4.1. *is nilpotent on M/pM.*

Later, we will see this definition is consistent with the nilpotence condition for a display.

Let K be a field of characteristic p. We defined the ring A_K in (3.1). Recall it is a discrete valuation ring by Lemma 3.1.

Lemma 3.6. *Let $\mathcal{P} = (P, Q, F, \dot{F})$ be a display over K. Then*

$$(M, \Phi) = (A_K \otimes_{W(K)} P, \sigma \otimes F)$$

is a Dieudonné module over A_K. The display $\mathcal{P}$ is a nilpotent if and only if (M, Φ) is a nilpotent Dieudonné module.

Proof. Let $P = T \oplus L, Q = I_K T \oplus L$ be a normal decomposition. Suppose $T \simeq W(K)^d$ and $L \simeq W(K)^c$. Suppose the map

$$F \oplus \dot{F} : T \oplus L \to P$$

is given by

$$\begin{pmatrix} \underline{t} \\ \underline{l} \end{pmatrix} \mapsto \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} {}^F\underline{t} \\ {}^F\underline{l} \end{pmatrix}.$$

Then the map $F : P \to P$ is given by

$$\begin{aligned} F\begin{pmatrix} \underline{t} \\ \underline{l} \end{pmatrix} &= \begin{pmatrix} A & pB \\ C & pD \end{pmatrix} \begin{pmatrix} {}^F\underline{t} \\ {}^F\underline{l} \end{pmatrix} \\ &= \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E_d & 0 \\ 0 & pE_c \end{pmatrix} \sigma \begin{pmatrix} \underline{t} \\ \underline{l} \end{pmatrix}. \end{aligned}$$

If we define a map $\Psi : M \to M$, where $M = A_K \otimes_{W(K)} P$, by

$$\Psi = \begin{pmatrix} pE_d & 0 \\ 0 & E_c \end{pmatrix} \left[\sigma^{-1} \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} \right] \sigma^{-1},$$

then it is clear that Ψ is σ^{-1}-linear and $\Phi \circ \Psi = \Psi \circ \Phi = p$, where $\Phi = \sigma \otimes F$. Hence $(A_K \otimes_{W(K)} P, \sigma \otimes F)$ is a Dieudonné module over A_K.

The last assertion can be deduced by (2.16) and the definition of Ψ. □

Remark 3.6.1 If $\mathcal{P}_n$ is a display over K_n, the construction defined by Lemma 3.6 also gives an A_K-module. In the next lemma, we can see that every Dieudonné module over A_K can be obtained in this way.

Lemma 3.7. *Let (M, Φ) be a Dieudonné module over A_K. Then there is an integer n and a display $\mathcal{P} = (P, Q, F, \dot{F})$ over K_n, such that $M \simeq A(K) \otimes_{W(K_n)} P$ and $\Phi = \sigma \otimes F$, i.e., (M, Φ) is obtained from $\mathcal{P}$ by the construction in Lemma* 3.6.

Proof. Let $\Psi = p\Phi^{-1}$ be the map defined in Remark 3.4.1. It is clear that $pM \subset \Psi(M) \subset M$. We know M/pM is a finite dimensional vector space over A_K/pA_K and we have the following exact sequence of A_K/pA_K-vector spaces:

$$0 \to \Psi(M)/pM \to M/pM \to M/\Psi(M) \to 0.$$

Let $(\bar{e}_1, \dots, \bar{e}_d)$ be a basis of $M/\Psi(M)$ and $(\bar{e}_{d+1}, \dots, \bar{e}_h)$ be a basis of $\Psi(M)/pM$. Lift $\bar{e}_i$ to $e_i \in M$, such that$e_i \in \Psi(M)$ for $i = d+1, \dots, h$. Then by construction, $e_i (\text{mod } pM), 1 \le i \le h$ is a basis of M/pM. Hence by Nakayama's Lemma, we see that $(e_i, 1 \le i \le h)$ is basis of M. Write

$$\Phi(e_i) = \sum_{j=1}^{h} a_{ji} e_j, \quad i = 1, \dots, d. \tag{3.2}$$

Similar to that Φ is injective as we showed in Remark 3.4.1., we can see Ψ is also injective by the same proof. Since we require $e_i \in \Psi(M), i = d+1, \dots, h$, it makes sense to talk $\Psi^{-1}(e_i)$ for $i = d+1, \dots, h$. We write

$$\Psi^{-1}(e_i) = \sum_{j} a_{ji} e_j, \quad i = d+1, \dots, h. \tag{3.3}$$

In Equation (3.2) and (3.3), $a_{ij} \in A(K)$. Since there are only finitely many a_{ij}, we can find an integer n such that $a_{ij} \in W(K_n)$ for all i, j. Since Φ is injective, $\Phi(e_i)(\text{mod } pM), 1 \le i \le d$, forms a basis of $\Phi(M)/\Phi(\Psi(M)) = \Phi(M)/pM$. Similarly, $\Psi^{-1}(e_i)(\text{mod } \Phi(M)), d+1 \le i \le h$, is a basis of $M/\Phi(M)$. Then by Nakayama's Lemma again, $\{\Phi(e_1), \dots, \Phi(e_d), \Psi^{-1}(e_{d+1}), \Psi^{-1}(e_h)\}$ is a basis of M. Consequently, the matrix $(a_{ij})_{1 \le i,j \le h}$ lies in $\mathrm{GL}_h(W(K_n))$. We set $T = \oplus_{1 \le i \le d} W(K_n) e_i$, $L = \oplus_{d+1 \le i \le h} W(K_n) e_i$, $P = T \oplus L$, $Q = I_{K_n} T \oplus L$. Define

$$Fe_i = \sum_j a_{ji} e_j, \quad i = 1, \dots, d,$$

$$\dot{F} e_i = \sum a_{ji} e_j, \quad i = d+1, \dots, h.$$

It is clear that $\mathcal{P} = (P, Q, F, \dot{F})$ is a display over $W(K_n)$ and $P \otimes_{W(K_n)} A_K = M$, $\sigma \otimes F = \Phi$. □

Lemma 3.8. *Let X, Y be two formal p-divisible groups over K, then*

$$\mathrm{Hom}(X, Y) \simeq \mathrm{Hom}_{K^{1/p}}(X_{K^{1/p}}, Y_{K^{1/p}}),$$

where $X_{K^{1/p}}$ is the base change of X under the inclusion $K \hookrightarrow K^{1/p}$. In general, if X, Y are two formal p-divisible groups defined over K_n, then for any $u \geq m$, we have

$$\mathrm{Hom}_{K_n}(X, Y) \simeq \mathrm{Hom}_{K_u}(X_u, Y_u),$$

where X_u means the base change of X under the inclusion $K_n \hookrightarrow K_u$.

Proof. The first assertion follows from Corollary 1.58, and the second assertion is a corollary of the first one. □

Definition 3.9. *We define the category of* ***potential formal p-divisible groups over*** *K, denoted by $\mathcal{C}$, as follows. The objects of $\mathcal{C}$ are pairs (X, n), where $n \in \mathbb{N}$, and X is a formal p-divisible group over K_n. The homomorphisms are defined by*

$$\mathrm{Hom}((X, n), (Y, m)) = \mathrm{Hom}(X_{K_u}, Y_{K_u}),$$

where $u \geq \max(m, n)$. This definition is independent of the choice of u by Lemma 3.8.

Theorem 3.10. *There is an equivalence of categories*

$$\{\textit{nilpotent Dieudonné-modules over } A_K\} \simeq \mathcal{C}.$$

Proof. Let (M, Φ) be a nilpotent Dieudonné module over A_K. By Lemma 3.7, there is an integer n and a display $\mathcal{P} = (P, Q, F, \dot{F})$ such that $M \simeq A_K \otimes_{W(K_n)} P$. By Lemma 3.6, $\mathcal{P}$ is nilpotent. Then by the Main Theorem 2.32, $X = \mathrm{BT}_{\mathcal{P}}$ is a formal p-divisible group over K_n. Hence

$$(M, \Phi) \mapsto (\mathcal{P}, n) \mapsto (\mathrm{BT}_{\mathcal{P}}, n)$$

defines a functor

$$\{\text{nilpotent Dieudonné-modules over } A_K\} \to \mathcal{C}.$$

By Lemma 3.6, Remark 3.6.1. and Lemma 3.7, it is easy to see that

$$(M, \Phi) \mapsto (\mathcal{P}, n)$$

is an equivalence of categories. The functor

$$(\mathcal{P}, n) \mapsto (X, n)$$

is an equivalence by the Main Theorem 2.32. We are done. □

Recall we use $W_{\mathbb{Q}}(K)$ to denote the quotient field of A_K, which is also the quotient field of $W(K)$. In this section, we fix the following notation. Let N be a $W_{\mathbb{Q}}(K)$ vector space. Let $\Phi : N \to N$ be a bijective σ^a-linear map. Here $a \geq 1$ is a fixed integer. We will denote these data by a pair (N, Φ) in this section.

Definition 3.11. *Let (N, Φ) be a pair as defined above. A* ***lattice*** *M of N is a finite generated A_K-module such that*

$$W_{\mathbb{Q}}(K) \otimes_{A_K} M \simeq N.$$

We fix the a lattice M. For $x \in N$, we define

$$\mathrm{ord}_M x = \max\left\{t \in \mathbb{Z} | x \in p^t M\right\}.$$

We define

$$\mathrm{ord}_M\Phi = \max\left\{t \in \mathbb{Z} | \Phi(M) \subset p^t M\right\}.$$

We define the ***Newton slope*** *of* Φ *by*

$$\mathrm{Newt}(N, \Phi) = \sup_{n \geq 1} \frac{1}{n} \mathrm{ord}_M \Phi^n.$$

Remark 3.11.1. Since A_K is a PID and any torsion free module over a PID is free, we see a lattice is a free A_K-module.

Remark 3.11.2 By definition, $\mathrm{ord}_M x = t$ if and only if $x \in p^t M$ but $x \notin p^{t+1}M$. Similarly, $\mathrm{ord}_M \Phi = t$ if and only if $\Phi(M) \subset p^t M$ but $\Phi(M) \not\subseteq p^{t+1} M$.

Lemma 3.12. *Notations as in the above definition.*
(1) *For* $m, n \geq 1$*, we have*

$$\frac{1}{n}\mathrm{ord}_M \Phi^n \leq \frac{1}{mn} \mathrm{ord}_M \Phi^{mn}.$$

(2) *We have*

$$\mathrm{Newt}(N, \Phi) = \lim_{n \to \infty} \frac{1}{n} \mathrm{ord}_M \Phi^n.$$

(3) *The Newton slope defined above is independent of the choice of the lattice* M*. This justifies the notation* $\mathrm{Newt}(N, \Phi)$*.*
(4) *The Newton slope* $\mathrm{Newt}(N, \Phi)$ *is finite.*

Proof. (1) If $\Phi M \subset p^t M$, then $\Phi^n M \subset p^{tn} M$. It follows that $\mathrm{ord}_M \Phi^n \geq n \mathrm{ord}_M \Phi$. Hence, we have

$$\frac{1}{n}\mathrm{ord}_M \Phi^n \leq \frac{1}{mn} \mathrm{ord}_M \Phi^{mn}.$$

(2) To be added. □

Proposition 3.13. *Let* (N, Φ) *be a pair as defined in the beginning of this section. Let* M *be a lattice in* N *such that* $\Phi^u M \subset p^{-1}M$ *for some* $u \geq \dim_{W_{\mathbb{Q}}(K)} N + 1$*. Then there is a lattice* M_1 *in* N *such that* $\Phi M_1 \subset M_1$*.*

Proof. Put $M' = M + \Phi M + \cdots + \Phi^{u-1} M$. Then

$$M' + \Phi M' + \cdots + \Phi^u M' = \sum_{i=0}^{2u-1} \Phi^i M$$

$$= M' + \sum_{j=0}^{u-1} \Phi^j (\Phi^u M) \subset M' + \sum_{j=0}^{u-1} \Phi^j p^{-1} M \subset p^{-1} M'.$$

Then we have a filtration

$$M' \subset M' + \Phi M' \subset \cdots \subset M' + \cdots + \Phi^u M' \subset p^{-1} M'$$

of length $u + 1$. Since

$$\dim_{K^{\mathrm{perf}}} p^{-1}M'/M' = \dim_{K^{\mathrm{perf}}} M' \otimes_{A_K} (A_K/pA_K) = \mathrm{rk} M' = \dim_{W_{\mathbb{Q}}(K)} N < u,$$

there is an integer e, with $1 \leq e \leq u$ such that

$$M' + \Phi M' + \cdots + \Phi^{e-1} M' = M' + \cdots + \Phi^e M'.$$

Put

$$M_1 = M' + \Phi M' + \cdots + \Phi^{e-1} M'.$$

Then it is clear that

$$\Phi(M_1) \subset M_1.$$

□

Proposition 3.14. *Let (N, Φ) be a pair as defined in the beginning of this section. Suppose $h = \dim_{W_{\mathbb{Q}}(K)} N$. Let $M \subset N$ be an arbitrary lattice, put*

$$M_1 = M + \Phi M + \cdots + \Phi^{h-1} M.$$

Then $\Phi(M_1) \subset M_1$.

Corollary 3.15. *Let (N, Φ) be a pair defined in the beginning of this section. Assume $\mathrm{Newt}(N, \Phi) \geq 0$. Then N contains a Φ-invariant lattice.*

Proof. Let $M \subset N$ be an arbitrary lattice. Put $h = \dim N$. By assumption that the Newton slope is non-negative and (2) of Lemma 3.12, there is an integer $n \in \mathbb{N}$ such that

$$\frac{1}{n(h+1)} \mathrm{ord}_M \Phi^{n(h+1)} \geq -\frac{1}{h+1},$$

i.e., $\mathrm{ord}_M \Phi^{n(h+1)} \geq -n$. Hence $\Phi^{n(h+1)} M \subset p^{-n} M$, namely,

$$\left(p \Phi^{h+1}\right)^n M \subset M.$$

If we take $M' = M + p\Phi^{h+1} M + \cdots + (p\Phi^{h+1})^{n-1} M$, then $(p\Phi^{h+1}) M' \subset M'$, i.e., $\Phi^{h+1} M' \subset p^{-1} M'$. Then by Proposition 3.13 there is a Φ-invariant lattice $M \subset N$. □

Corollary 3.16. *Let (N, Φ) be a pair as before, assume $\mathrm{Newt}(N, \Phi) \geq \frac{s}{r}$, with $r, s \in \mathbb{Z}, r > 0$. Then there is a lattice $M \subset N$ such that*

$$\Phi^r M \subset p^s M.$$

Proof. We have $\mathrm{Newt}(N, p^{-s}\Phi^r) = r\mathrm{Newt}(N, \Phi) - s \geq 0$. Then by Corollary 3.16, we have there is a lattice $M \subset N$ such that $p^{-s}\Phi^r M \subset M$. Then $\Phi^r M \subset p^s M$. □

Lemma 3.17. *Given a pair (N, Φ) as before. Suppose $\dim N = h$. Let M be a lattice in N. Assume there is an integer n such that $\mathrm{ord}_M \Phi \neq \frac{1}{n} \mathrm{ord}_M \Phi^n$. Then*

$$\mathrm{ord}_M \Phi + \frac{1}{h} \leq \frac{1}{h} \mathrm{ord}_M \Phi^h.$$

Proof. Put $t = \mathrm{ord}_M \Phi$. By assumption and (1) of Lemma 3.12, we have $t = \mathrm{ord}_M \Phi < \frac{1}{n} \mathrm{ord}_M \Phi^n$. Hence $\mathrm{ord}_M \Phi^n \geq tn + 1$. Set

$$M_i = \left\{ m \in M | \Phi^i(m) \in p^{it+1} M \right\}.$$

Then above discussion shows that $M_n = M$. It is clear that M_i is an A_K-submodule of M. Given $m \in M_i$, then $\Phi^i(m) \in p^{it+1} M$. Hence $\Phi^{i+1}(m) \in p^{it+1} \Phi(M)$. By definition of t, we have $\Phi(M) \subset p^t M$. So $\Phi^{i+1}(m) \in p^{t(i+1)+1} M$. It follows that $M_i \subset M_{i+1}$. Hence we get a filtration

$$pM = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_i \subset M_{i+1} \subset \cdots \subset M.$$

Claim: If $M_i = M_{i+1}$, then $M_{i+1} = M_{i+2}$.
Let $m \in M_{i+2}$. Since $\Phi(M) \subset p^t(M)$ by the definition of t, we can suppose $\Phi(m) = p^t m_1$ for some $m_1 \in M$. Now $m \in M_{i+2}$ implies that

$$\Phi^{i+2}(m) = \Phi^{i+1}(\Phi(m)) = p^t \Phi^{i+1}(m_1) \in p^{(i+2)t+1}M.$$

Hence $\Phi^{i+1}(m_1) \in p^{(i+1)t+1}M$. So $m_1 \in M_{i+1}$ by definition. Now by assumption, $m_1 \in M_i$. So $\Phi^i(m_1) \in p^{it+1}M$. This implies

$$\Phi^{i+1}(m) = \Phi^i(\Phi(m)) = \Phi^i(p^t m_1) = p^t \Phi^i(m_1) \in p^{(i+1)t+1}M,$$

i.e., $m \in M_{i+1}$. The claim follows.

Since $\dim_{K^{\mathrm{perf}}} M/pM = h$, by the above claim there is an integer $i \leq h$ with $M_i = M_{i+1}$. Since $M_n = M$ for the given n, we must have $M_h = M_n = M$, i.e., $\Phi^h(M) \subset p^{ht+1}M$. So by the definition of the order, we have

$$\mathrm{ord}_M \Phi^h \geq ht + 1.$$

This is exactly what we want to show. □

Proposition 3.18 (Dirichlet)**.** *Given are $x \in \mathbb{R}$, $R \in \mathbb{Z}$ with $R \geq 2$. Then there exist $r, s \in \mathbb{Z}$, with $1 \leq r \leq R$ such that*

$$\left| x - \frac{s}{r} \right| \leq \frac{1}{rR}.$$

This is an elementary result in Diophantine approximation.

Proof. If x is rational, nothing to prove. Suppose x is irrational, consider the set

$$\{qx - [qx]; q = 0, 1, \ldots, R\}.$$

Here $[qx]$ is the greatest integer less than or equal to qx. There are $R+1$ distinct points in this set, and each point of this set lies in the interval $[0,1]$, so there exists $0 \leq q_1 < q_2 \leq R$ such that

$$|(q_2x - [q_2x]) - (q_1x - [q_1x])| \leq 1/R.$$

Hence

$$\left| x - \frac{[q_2x] - [q_1x]}{q_2 - q_1} \right| \leq \frac{1}{(q_2 - q_1)R}.$$

It suffices to take $r = q_2 - q_1, s = [q_2x] - [q_1x]$. □

Theorem 3.19. *For any pair (N, Φ) as above, we have*

$$\mathrm{Newt}(N, \Phi) \in \mathbb{Q}.$$

Proof. Assume $\dim N = h$. Let $\lambda = \mathrm{Newt}(N, \Phi)$. By Lemma 3.12 (4), $\lambda \in \mathbb{R}$. Then by Proposition 3.18, there exists $r, s \in \mathbb{Z}$, $1 \leq r \leq h+1$ such that

$$\left| \lambda - \frac{s}{r} \right| \leq \frac{1}{r(h+1)}.$$

Set $\lambda' = r\lambda - s$, $\Phi' = p^{-s}\Phi^r$. Then $\lambda' = \mathrm{Newt}(N, \Phi')$. We have

$$-\frac{1}{h+1} \leq \lambda' \leq \frac{1}{h+1}.$$

By Corollary 3.16, there is a lattice $M' \subset N$ such that

$$(\Phi')^{h+1} \subset p^{-1}M'.$$

By Proposition 3.13, there exists a lattice $M \subset N$ such that $\Phi' M \subset M$. Hence $\mathrm{ord}_M(\Phi') \geq 0$ by the definition of the order. It follows that $\lambda' \geq 0$ by the definition of the Newton slope.

Claim: $\lambda' = 0$.
If $\lambda' > 0$, by the definition of the Newton slope again, there is an integer $n > 0$, such that

$$\frac{1}{n}\mathrm{ord}_M(\Phi')^n > 0.$$

If $\mathrm{ord}_M \Phi' = 0$, then by Lemma 3.17, we have

$$\frac{1}{h} = \mathrm{ord}_M \Phi' + \frac{1}{h} \leq \frac{1}{h}\mathrm{ord}_M(\Phi')^h \leq \lambda',$$

this contradicts $\lambda' \leq \frac{1}{h+1}$. So $\mathrm{ord}_M \Phi' \geq 1$. But then

$$\lambda' = \sup_n \frac{1}{n}\mathrm{ord}_M(\Phi')^n \geq 1.$$

This contradicts $\lambda' \leq \frac{1}{h+1}$. The claim, hence the theorem, follows. □

3.1. **27.** Let K be a field of characteristic p. Recall we have defined A_K, which is a discrete valuation ring. Our aim of this section is to prove the following

Theorem 3.20. *Let M be a finitely generated free A_K-module, $\Phi : M \to M$ be a σ^a-linear homomorphism.*
(i) *Then there is a unique direct summand $M^{\mathrm{bij}} \subset M$ such that M^{bij} is Φ-invariant, $\Phi : M^{\mathrm{bij}} \to M^{\mathrm{bij}}$ is bijective and $\Phi : M/M^{\mathrm{bij}} \to M/M^{\mathrm{bij}}$ is nilpotent modulo p.*
(ii) *Moreover, if K is separably closed, then M^{bij} has a basis $m_1, \ldots, m_r$ such that $\Phi(m_i) = m_i$.*

As a warm-up, let us first consider the case where K is perfect. In this case $A_K = W(K)$. We begin with a lemma.

Lemma 3.21 (Fitting Decomposition Lemma.)**.** *Let R be a ring, σ an automorphism of R. Let M be an R-module of finite length and $\Phi : M \to M$ a σ^a-linear homomorphism.*
(i) *Then there is a unique decomposition $M = M^{\mathrm{bij}} \oplus M^{\mathrm{nil}}$ such that both M^{bij} and M^{nil} are Φ-invariant, $\Phi|_{M^{\mathrm{bij}}}$ is bijective and $\Phi|_{M^{\mathrm{nil}}}$ is nilpotent.*
(ii) *Furthermore, the decomposition in* (i) *is functorial. More precisely, Let S be another ring with an automorphism σ', and $f : R \to S$ a ring homomorphism respecting the automorphisms. Put $M_S = M \otimes_R S$. Let $M_S = M_S^{\mathrm{bij}} \oplus M_S^{\mathrm{nil}}$ be the corresponding decomposition. Then $M_S^{\mathrm{bij}} \simeq M^{\mathrm{bij}} \otimes_R S$ and $M_S^{\mathrm{nil}} \simeq M^{\mathrm{nil}} \otimes_R S$.*

Proof. Recall that M has finite length if and only if M satisfies both ascending chain condition and descending chain condition. Consider the following chains:

$$\mathrm{Ker}\Phi \subset \mathrm{Ker}\Phi^2 \subset \cdots \subset \mathrm{Ker}\Phi^t \subset \cdots$$

$$\mathrm{Im}\Phi \supset \mathrm{Im}\Phi^2 \supset \cdots \supset \mathrm{Im}\Phi^t \supset \cdots .$$

Since σ is an automorphism, it is easy to check both $\mathrm{Ker}\Phi^t$ and $\mathrm{Im}\Phi^i$ are submodules of M. That M has finite length implies that there is an integer t such that for any $s > t$, we have $\mathrm{Ker}\Phi^s = \mathrm{Ker}\Phi^{t-1}, \mathrm{Im}\Phi^s = \mathrm{Im}\Phi^{t-1}$. Take $M^{\mathrm{bij}} = \mathrm{Im}\Phi^t$, $M^{\mathrm{nil}} = \mathrm{Ker}\Phi^t$. It is clear that $\Phi|_{M^{\mathrm{nil}}}$ is nilpotent. Given $m \in M^{\mathrm{bij}}$, then $\Phi(m) \in \Phi^{t+1}(M) = M^{\mathrm{bij}}$ by the choice of t. Hence M^{bij} is Φ-invariant. Similarly M^{nil}

is also Φ-invariant. Suppose $m \in M^{\mathrm{bij}}$ and $\Phi(m) = 0$. Since $m \in M^{\mathrm{bij}} = \mathrm{Im}\Phi^t$, we can suppose $m = \Phi^t(m_1)$ for $m_1 \in M$. Then $0 = \Phi(m) = \Phi^{t+1}(m_1)$. Hence $m_1 \in \mathrm{Ker}\Phi^{t+1} = \mathrm{Ker}\Phi^t$. We get $m = \Phi^t(m_1) = 0$, i.e., $\Phi|_{M^{\mathrm{bij}}}$ is injective. If $m \in M^{\mathrm{bij}} = \mathrm{Im}\Phi^t$, we can take $m_1 \in M$ such that $m = \Phi^t(m_1) = \Phi(\Phi^{t-1}m_1)$. Now $\Phi^{t-1}m \in \mathrm{Im}\Phi^{t-1} = \mathrm{Im}\Phi^t$. We get that $\Phi|_{M^{\mathrm{bij}}}$ is bijective.

Now we have to show that $M = M^{\mathrm{bij}} \oplus M^{\mathrm{nil}}$. Since $\Phi|_{M^{\mathrm{bij}}}$ is bijective and $\Phi|_{M^{\mathrm{nil}}}$ is nilpotent, we must have $M^{\mathrm{bij}} \cap M^{\mathrm{nil}} = 0$. So it suffices to show that $M = M^{\mathrm{bij}} + M^{\mathrm{nil}}$. Given $m \in M$, we have $\Phi^t(m) \in \mathrm{Im}\Phi^t = \mathrm{Im}\Phi^{2t}$. So there exist $m_1 \in M$ such that $\Phi^t(m) = \Phi^{2t}(m_1)$. Then $m - \Phi^t m_1 \in \mathrm{Ker}\Phi^t = M^{\mathrm{nil}}$. Hence $M = M^{\mathrm{bij}} + M^{\mathrm{nil}}$.

Now we show the uniqueness. If $M = M_1^{\mathrm{bij}} \oplus M_1^{\mathrm{nil}}$ is another decomposition, consider $M_1^{\mathrm{bij}} \cap M^{\mathrm{nil}}$. Since $\Phi|_{M_1^{\mathrm{bij}}}$ is bijective and $\Phi|_{M^{\mathrm{nil}}}$ is nilpotent, we get $M_1^{\mathrm{bij}} \cap M^{\mathrm{nil}} = 0$. Hence $M_1^{\mathrm{bij}} \subset M^{\mathrm{bij}}$. Symmetrically, $M^{\mathrm{bij}} \subset M_1^{\mathrm{bij}}$. Hence $M_1^{\mathrm{bij}} = M_1^{\mathrm{bij}}$. Similarly, $M_1^{\mathrm{nil}} = M^{\mathrm{nil}}$. The functorial property follows from the uniqueness. □

Proposition 3.22. *Let K be a perfect field, and M a finitely generated free $W(K)$-module. Suppose $\Phi : M \to M$ is a σ^a-linear homomorphism. Recall $\sigma = {}^{F}$ here. Then there is a decomposition $M = M^{\mathrm{bij}} \oplus M^{\mathrm{nil}}$ such that both M^{nil} and M^{bij} are Φ-invariant, $\Phi|_{M^{\mathrm{bij}}}$ is bijective and $\Phi|_{M^{\mathrm{nil}}}$ is nilpotent.*

This assertion is stronger than that of Theorem 3.20.

Proof. Set $M(n) = W_n(K) \otimes_{W(K)} M$. Note that $W_n(K)$ is an Artin ring since $W_n(K)$ is a finite dimensional vector space over the field K. Then $M(n)$ has finite length. Take $\sigma_n = {}^{F}$ to be the Frobenius on $W_n(K)$. Then σ_n is an automorphism of $W_n(K)$. Take $\Phi_n = {}^{F^n} \otimes \Phi$, which is σ_n^a-linear. Hence we can apply Lemma 3.21 to get a decomposition

$$M(n) = M(n)^{\mathrm{bij}} \oplus M(n)^{\mathrm{nil}}$$

for Φ_n. By the functorial property, we see $\left\{M(n)^{\mathrm{bij}}\right\}_n$ forms a projective system. Put $M^{\mathrm{bij}} = \varprojlim M(n)^{\mathrm{bij}}$. Similarly, we can define $M^{\mathrm{nil}} = \varprojlim M(n)^{\mathrm{nil}}$. It is easy to see that $M = M^{\mathrm{bij}} \oplus M^{\mathrm{nil}}$ gives the desired decomposition. □

Remark 3.22.1 The proof of Proposition 3.22. suggests that we can reduce the problem to a problem over Artin rings, and then take projective limit. In our general case, we have Artin rings A_K/p^nA_K. Then we have a decomposition $M_n = M/p^nM = M_n^{\mathrm{bij}} \oplus M_n^{\mathrm{nil}}$. But the module $\varprojlim M_n^{\mathrm{bij}}$ is a module over $\hat{A}_K = W(K^{\mathrm{perf}})$, which is not A_K in general. This is not what we want to get.

Let us go back to our general case, i.e., the situation of Theorem 3.20. Since M is finitely generated, we can find an integer m such that Φ is defined over $K_m = K^{1/p^m}$, i.e., there is free module M_0 over $W(K_m)$ and a ${}^{F^a}$-linear homomorphism $\Phi_0 : M_0 \to M_0$ such that $M = A_K \otimes_{W(K_m)} M_0$ and $\Phi = \sigma^a \otimes \Phi_0$. Set

$$M(n) = W_n(K_m) \otimes_{W(K_m)} M_0,$$

$$\Phi_n = {}^{F^a} \otimes \Phi_0 : M(n) \to M(n).$$

Proposition 3.23. *There exists a unique Φ_n-invariant direct summand $M(n)^{\text{bij}}$ of $M(n)$ such that $\Phi_n^\sharp : M(n)^{\text{bij}} \to M(n)^{\text{bij}}$ is an isomorphism and Φ_n is nilpotent on $M(n)/M(n)^{\text{bij}}$. Here $\Phi_n^\sharp$ is the linearization of Φ_n, see Definition* 2.21.

Example 3.23.1. If K is not perfect, a stronger assertion as in Proposition 3.22. is false. But we can expect Proposition 3.23. to be true. For example, let K be a non-perfect field. Let n be 1. Then $W_1(K) = K$. Consider the K-module $M = K^{1/p}$ with the ^{F}-linear map $\Phi : M \to M$ defined by $\Phi(m) = m^p$. Then $K \subset M$ and $\Phi|_K : K \to K$, $k \mapsto k^p$. It is easy to see that

$$\Phi^\sharp : K \otimes_{\text{Frob},K} K \to K$$
$$\xi \otimes k \mapsto \xi^p k$$

is an isomorphism. But $\Phi|_K$ is not surjective. It is clear that Φ is zero on M/K. Hence we can take $M^{\text{bij}} = K$. But there is no $M^{\text{nil}} \subset M$ such that $M = K \oplus M^{\text{nil}}$ and $M^{\text{nil}} \simeq M/K$. Note that in this example ^{F} is not an isomorphism on K, so we cannot use Lemma 3.21.

Remark 3.23.2. Assume Proposition 3.23., then $M_0^{\text{bij}} = \varprojlim M(n)^{\text{bij}}$ is a $W(K_m)$-module and $M^{\text{bij}} = A_K \otimes_{W(K_m)} M_0^{\text{bij}}$ satisfying the condition Theorem 3.20. (why is $\Phi : M^{\text{bij}} \to M^{\text{bij}}$ bijective?) Hence, Proposition 3.23. implies Theorem 3.20. (i).

We now proceed to prove Proposition 3.23. We start with a lemma.

Lemma 3.24 (Dieudonné)**.** *Assume K is a separably closed field and V is a finite dimensional vector space over K. Let $\Phi : V \to V$ be a Frob^a-linear isomorphism, i.e., $\Phi(\xi v) = \xi^{p^a}\Phi(v)$, where a is a positive integer. Then V has a basis of Φ-invariant vectors, i.e., we can write $V = \oplus K e_i$ with $\Phi(e_i) = e_i$.*

The proof of this lemma is omitted.

Remark 3.24.1. Notations as in Lemma 3.24. For $v \in V$, we can write $v = \sum \xi e_i$ with $\xi_i \in K$. Then $\Phi(v) = v$ implies that $\xi_i^{p^a} = \xi_i$, i.e., $\xi_i \in \mathbb{F}_{p^a}$ for all i. Hence $V_0 = V^\Phi$ is an $\mathbb{F}_{p^a}$-vector space and we have

$$V = K \otimes_{\mathbb{F}_{p^a}} V_0.$$

Note that under this isomorphism, we have $\Phi(\xi \otimes v_0) = \xi^{p^a} \otimes v_0$.

Corollary 3.25. *Assume K is separably closed. Let M_n be a free $W_n(K)$-module and $\Phi : M_n \to M_n$ an ${}^{F^a}$-linear isomorphism. Then there is a free $W_n(\mathbb{F}_{p^a})$-module such that*

$$M_n = W_n(K) \otimes_{W_n(\mathbb{F}_{p^a})} L.$$

Under this isomorphism, we have $\Phi(\xi \otimes l) = {}^{F^a}\xi \otimes l$.

Proof. The corollary is a direct consequence of Remark 3.24.1. and Nakayama's Lemma, by noting that $W_n(K)/pW_n(K) = K$ is separably closed. □

Proposition 3.26. *Let R be a ring such that $p \cdot R = 0$, and M a free $W_n(R)$-module. Let $\Phi : M \to M$ be an ${}^{F^a}$-linear homomorphism. Then the functor*

$$C_R : \{R\text{-algebra}\} \longrightarrow \textbf{Sets}$$

$$C_R(S)=\left\{m\in W_n(S)\otimes_{W_n(R)} M \mid \ {}^{F^a}\otimes\Phi(m)=m\right\}$$

for $S\in\{R\text{-algebra}\}$ *is representable by an affine étale scheme over* R.

Proof. For simplicity, we write C for C_R. Let $\{e_1,\dots,e_d\}$ be a basis of M. Suppose $\Phi(e_j)=\sum a_{ij}e_i$ with $a_{ij}\in W_n(R)$. Let $A=(a_{ij})$. Then $\Phi(\underline{m})=A^{F^a}\underline{m}$. So

$$C(S)=\left\{\underline{m}\in W_n(S)^d \mid \ \underline{m}=A^{F^a}\underline{m}\right\}.$$

Since $W_n(S)\simeq\mathbb{A}_S^n$, we see that $C(S)$ is a closed subscheme of $(\mathbb{A}_S^n)^d$. Hence C is representable.

To show that C is representable by an étale scheme, we have to show: for any exact

$$0\longrightarrow\mathfrak{a}\longrightarrow S\xrightarrow{f}T\longrightarrow 0\ ,$$

where S,R are two R-algebras and $f:S\twoheadrightarrow T$ is a surjective ring homomorphism with kernel $\mathfrak{a}$ such that $\mathfrak{a}^2=0$, then f induce a bijection $C(f):C(S)\simeq C(T)$.

We have the following commutative diagram

$$\begin{tikzcd}
 & & C(S) \arrow[r] \arrow[d] & C(T) \arrow[d] & \\
0 \arrow[r] & W_n(\mathfrak{a})\otimes_{W_n(R)} M \arrow[r] & W_n(S)\otimes_{W_n(R)} M \arrow[r] & W_n(T)\otimes_{W_n(R)} M \arrow[r] & 0
\end{tikzcd}$$

We first show that $C(f)$ is injective. If $m\in C(S)$ such that $f(m)=0$, we have to show that $m=0$. By the above diagram, we see that $m\in W_n(\mathfrak{a})\otimes_{W_n(R)}M$, hence we can write $m=\sum\xi_i\otimes n_i$ with $\xi_i\in W_n(\mathfrak{a})$ and $n_i\in M$. Now $m\in C(S)$ implies that $m={}^{F^a}\otimes\Phi(m)=\sum{}^{F^a}\xi_i\otimes\Phi(n_i)$. If $\xi_i=(x_0,x_1,\dots),x_i\in\mathfrak{a}$, then $p\cdot R=0$ implies ${}^{F}\xi_i=(x_0^p,x_1^p,\dots)$, see Proposition 2.13. Now $\mathfrak{a}^2=0$ implies ${}^{F^a}\xi_i=0$. So $m=0$.

Next, we check that $C(f)$ is surjective. For $m\in C(T)$, we first lift m to $\tilde{m}\in W_n(S)\otimes_{W_n(R)}M$. Denote $\eta={}^{F^a}\otimes\Phi(\tilde{m})-\tilde{m}$. Then ${}^{F^a}\otimes\Phi(\tilde{m})$ is a lift of ${}^{F^a}\otimes\Phi(m)=m$, since $m\in C(T)$. Hence $\eta\in W_n(\mathfrak{a})\otimes_{W_n(R)}M$. As above, we have ${}^{F^a}\otimes\Phi(\eta)=0$. Then

$${}^{F^a}\otimes\Phi(\tilde{m}+\eta)=\tilde{m}+\eta,$$

i.e., $\tilde{m}+\eta\in C(S)$. It is clear that $\tilde{m}+\eta$ is a lift of m. We are done. □

Now we turn to the proof of Proposition 3.23.

References

[B] P. Berthelot, *Notes on Crystalline Cohomology.*

[H] R. Hartshorne, *Algebraic Geometry.*

[M] W. Messing, *The crystals associated to Barsotti-Tate Groups: with Applications to Abelian Schemes.*

[Z] T. Zink, *Cartiertheorie Kommutativer Former Gruppen.* Teubner 1984.

[Z1] T. Zink, *The Display of a Formal p-Divisible Group.*