AFFINE AND FORMAL ABELIAN GROUP SCHEMES ON p-POLAR RINGS

TILMAN BAUER

Abstract. We show that the functor of p-typical co-Witt vectors on commutative algebras over a perfect field k of characteristic p is defined on, and in fact only depends on, a weaker structure than that of a k-algebra. We call this structure a p-polar k-algebra. By extension, the functors of points for any p-adic affine commutative group scheme and for any formal group are defined on, and only depend on, p-polar structures. In terms of abelian Hopf algebras, we show that a cofree cocommutative Hopf algebra can be defined on any p-polar k-algebra P, and it agrees with the cofree commutative Hopf algebra on a commutative k-algebra A if P is the p-polar algebra underlying A; a dual result holds for free commutative Hopf algebras on finite k-coalgebras.

1. Introduction

Let p be a prime. We consider the following generalizations of the notion of a k-algebra A:

Definition. Let k be a (commutative) ring and A a k-module. A *p-polar k-algebra structure* on A is a symmetric k-multilinear map $\mu\colon A^{\otimes_k p} \to A$ such that

(ASSOC) $$\mu(\mu(x_1, \dots, x_p), x_{p+1}, \dots, x_{2p-1}) \text{ is } \Sigma_{2p-1}\text{-invariant}$$

for the permutation action of the symmetric group Σ_{2p-1} on $x_1, \dots, x_{2p-1} \in A$. We will call a p-polar $\mathbf{Z}$-algebra a p-polar ring.

A morphism of p-polar algebras is the evident structure-preserving map, making p-polar algebras into a category $\mathrm{Pol}_p(k)$.

Clearly, any k-algebra R gives rise to a p-polar structure for each p by restriction, called its *polarization* $\mathrm{pol}(R)$.

Our main results concern the categories AbSch_k of affine, commutative group schemes, its subcategory AbSch_k^p of p-adic groups (i.e. taking values in abelian pro-p-groups), the category Fgps_k of commutative formal group schemes, and its subcategory Fgps_k^p of formal p-group schemes, all over a perfect field k of characteristic p.

Date: June 24, 2021.

2010 *Mathematics Subject Classification.* 14L05,14L15,14L17,13A99,13A35,16T05.

Key words and phrases. p-polar ring, formal group, affine group scheme, Witt vectors, Dieudonné theory.

Theorem 1.1. *Let k be a perfect field of characteristic p and $M \in \mathrm{AbSch}_k^p$ or $M \in \mathrm{Fgps}_k$. Then the functor of points of M factors uniquely through* pol*:*

$$\begin{array}{ccc} \mathrm{Alg}_k & \xrightarrow{M} & \mathrm{Ab} \\ & \searrow^{\mathrm{pol}} & \uparrow{\scriptstyle \tilde{M}} \\ & & \mathrm{Pol}_p(k) \end{array}$$

Note that the restriction to p-adic group schemes is necessary in the affine case: the multiplicative group $\mathbb{G}_m$ with $\mathbb{G}_m(R) = R^\times$ very much depends on the algebra structure of R. Interestingly, a similar restriction is not necessary for formal groups. In particular, the formal completion $\hat{\mathbb{G}}_m$ of the multiplicative group, with $\hat{\mathbb{G}}_m(R) = (1 + \mathrm{Nil}(R))^\times$, depends only on the p-polar structure.

Theorem 1.1 follows immediately from the following result:

Theorem 1.2. *Let k be a perfect field of characteristic p and denote by $\mathrm{Fr}(R)$ the free affine, abelian, p-adic group scheme on $\operatorname{Spec} R$ for a k-algebra R, or the free abelian formal group on $\operatorname{Spec} R$ for a finite k-algebra R. Then* Fr *factors through* pol*:*

$$\begin{array}{ccc} \mathrm{Alg}_k & \xrightarrow{\mathrm{Fr}} & \mathrm{AbSch}_k^p \ \ (\textit{or } \mathrm{Fgps}_k) \\ & \searrow^{\mathrm{pol}} & \uparrow{\scriptstyle \tilde{\mathrm{Fr}}} \\ & & \mathrm{Pol}_p(k) \end{array}$$

Indeed, given any $M \in \mathrm{AbSch}_k^p$ or $M \in \mathrm{Fgps}_k$, we have that

$$M(R) = \mathrm{Hom}(\operatorname{Spec} R, M) = \mathrm{Hom}(\mathrm{Fr}(R), M),$$

where the last Hom group is of objects of AbSch_k^p or Fgps_k, respectively. This shows that Thm. 1.1 follows from Thm. 1.2.

In terms of Hopf algebras, this can be reformulated in the following way. An abelian (i.e. commutative and cocommutative) Hopf algebra H over k is *p-adic* if $\operatorname{Spec} H$ is a p-adic affine group. This means that $H \cong \operatorname{colim}_n H[p^n]$, where $H[p^n]$ denotes the kernel of the endomorphism $[p^n]$ of H representing multiplication by p^n. In other word, every element $x \in H$ is $[p]$-nilpotent. For instance, all conilpotent Hopf algebras are p-adic.

The affine part of Theorem 1.2 thus says that the cofree cocommutative p-adic Hopf algebra functor on k-algebras factors through p-polar algebras.

The categories of formal groups and of affine abelian groups are anti-equivalent by Cartier duality, represented by taking (continuous) k-linear duals at the level of (formal) Hopf algebras, and this anti-equivalence restricts to an anti-equivalence between Fgps_k and AbSch_k and hence an equivalence between Fgps_k and the category of abelian Hopf algebras. The formal part of Theorem 1.2 says that the *free commutative* Hopf algebra functor on finite-dimensional k-coalgebras factors through the opposite category of finite-dimensional p-polar k-algebras.

Instead of trying to prove Thm. 1.2 directly, we take a detour along the Dieudonné functor to the land of Witt vectors. The Dieudonné functors

$$D\colon \mathrm{AbSch}_k \to \mathrm{Dmod}_k^p$$

and

$$\mathbb{D}^{\mathrm{f}}\colon \mathrm{Fgps}_k \to \mathbb{D}\,\mathrm{mod}_k^F$$

define equivalence between AbSch_k^p and Fgps_k^p and certain categories of $W(k)$-modules with two operations F and V, called Frobenius and Verschiebung. Here $W(k)$ denotes the ring of p-typical Witt vectors of the field k. More generally, let $W_n(R)$ be the group of p-typical Witt vectors of length n of a ring R. By inspection of its definition, it is defined for any p-polar ring R.

The Verschiebung $V\colon W_n(R) \to W_{n+1}(R)$ gives rise to the group of unipotent co-Witt vectors

$$CW^u(R) = \mathrm{colim}(W_1(R) \xrightarrow{V} W_2(R) \xrightarrow{V} \cdots),$$

an object of Dmod_k^p. It has a completion, $CW(R)$, the group of co-Witt vectors, consisting of possibly infinite negatively graded sequences $(\ldots, a_{-1}, a_0)$ of elements of R almost all of which are nilpotent.

We prove:

Theorem 1.3. *Let k be a perfect field of characteristic p. Then there are natural isomorphisms*

$$\mathbb{D}^{\mathrm{f}}(\mathrm{Fr}(R)) \cong CW(R) \quad \textit{for finite } k\textit{-algebras } R$$

and, for arbitrary k-algebras R,

$$D(\mathrm{Fr}(R)) \cong CW^u(R) \oplus \big({}_p((R \otimes_k \bar{k})^\times) \otimes W(\bar{k})\big)^{\mathrm{Gal}(k)}$$

where in the last factor, invariants of the absolute Galois group $\mathrm{Gal}(k)$ *acting diagonally on $\bar{k}$ and $W(\bar{k})$ are taken.*

Because the right-hand side is defined on p-polar algebras, so is the left hand side. Since D is an equivalence between AbSch_k^p and Dmod_k^p, the affine case of Thm. 1.2 follows with the additional observation that the group ${}_p((R \otimes_k \bar{k})^\times)$ is well-defined for any p-polar algebra R. The formal case requires an additional argument.

2. p-POLAR RINGS

Recall the definition of a p-polar algebra A from the introduction. We make the following observations:

- The definition is non-unital in nature. If one were to require the existence of an element $1 \in A$ such that $\mu(1, \ldots, 1, x) = x$, this would make A into a commutative unital ring.
- If $p = 2$ then A is a nonunital algebra.
- The expression in (ASSOC) is $(\Sigma_p \times \Sigma_{p-1})$-equivariant by definition. Given commutativity, the condition is akin to an associative law.

Example 2.1. The multiplication on an ordinary (not necessarily unital) ring A restricts to polar ring structure $\mathrm{pol}(A)$.

Example 2.2. We have that $k[x]_{(j)} =_{\mathrm{def}} k\langle x^{j(1+(p-1)i)} \mid i \geq 0\rangle$ is a polar subalgebra of $k[x]$ for each $j \geq 0$, and it is not an algebra (unless $j = 0$, in which case it is just k, or $j > 0$ and $p = 2$, in which case it is an algebra without unity).

Example 2.3. Let $A = xk[x]/(x^p)$. Then $\mu = 0$, and hence $\mathrm{pol}(A) \cong k^{p-1}$ as p-polar algebras.

Remark 2.4. For a unital algebra A, one can recover A from $\mathrm{pol}(A)$ up to non-canonical isomorphism. Indeed, if B is a p-polar algebra of the form $\mathrm{pol}(A)$, there is an element e such that $\mu(e, \dots, e, x) = x$ for all $x \in B$. For instance, the unity of A is such an element, but B does not preserve that information. One easily checks that an algebra structure on B can be defined by $x \cdot y = \mu(e, \dots, e, x, y)$. With this algebra structure, multiplication by e gives an algebra isomorphism $A \to B$.

For nonunital algebras, this is not possible, as the previous example illustrates.

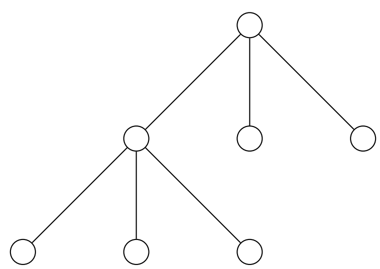
We have:

Proposition 2.5. *Let A be a p-polar k-algebra and $x_1, \dots, x_n \in A$. Then there is at most one way to multiply $x_1, \dots, x_n$ together using μ, and the product exists if and only if $n \equiv 1 \pmod{p-1}$.*

Proof. Let us first make the statement more rigorous. Define a *multiplication scheme* to be a rooted, planar, p-ary tree whose leaves are labelled with $x_1, \dots, x_n$. If a multiplication scheme exists, then it gives a prescription of how to multiply the elements x_i by traversing the tree, applying μ at every internal vertex. If no multiplication scheme exists, then the elements cannot be multiplied together. Since grafting a basic p-ary tree of depth 1 onto an existing tree increases the number of leaves by $p-1$, a multiplication scheme exists iff $n \equiv 1 \pmod{p-1}$.

An equivalence relation on the set of all multiplication schemes is generated by:

(1) $M' \sim M$ if M' results from M by permuting the outgoing edges of any internal vertex;
(2) $M' \sim M$ if M' results from M by permuting the $2p-1$ outgoing edges of a subtree of the form, along with their subtrees (illustrated for $p = 3$).



These relations correspond, of course, to the symmetry and axiom (ASSOC). It is easy to see that under this equivalence relation, every multiplication scheme is equivalent to a "left-associative" one, i.e. a scheme where a vertex has a non-leaf subtree only if it is the leftmost among its siblings, such as in the diagram above. In such a left-associative multiplication scheme, it is then equally easy to see that all leaves can be permuted without changing the equivalence class. Thus all multiplication schemes are equivalent. □

In light of this proposition, we will unambiguously use monomial notations such as x^p for $\mu(x, \dots, x)$ or xy^{p-1} for $\mu(x, y, \dots, y)$ in polar rings.

Example 2.6. Let S be a set. The free p-polar ring $P(S)$ on S is given by the sub-p-polar algebra of the polynomial ring $\mathbf{Z}[S]$ with generators in S spanned by monomials of length congruent to 1 modulo $p-1$ (or spanned by all nonconstant monomials if $p = 2$).

Definition. An *ideal* in a p-polar ring A is a subgroup I such that $\mu(a_1, \ldots, a_{p-1}, i) \in I$ whenever $i \in I$. These are exactly the kernels of homomorphisms of p-polar rings. For a subset $S \subseteq A$, the ideal (S) generated by it is defined to be the smallest ideal containing S. If I is an ideal, then $I^p = \langle \mu(I, \ldots, I) \rangle$ is a subideal.

2.1. **p-typical formal groups and units in p-polar rings.** For a k-algebra R, k of characteristic p, the functor $\mu_{p^\infty}(R) = \{x \in R^\times \mid x^{p^n} = 1 \text{ for some } n \geq 0\}$ is the colimit of the functors $\mu_{p^n}(R)$ represented by $k[y]/(y^{p^n} - 1) \cong k[x]/(x^{p^n})$, where $x = y - 1$. Thus $\mu_{p^\infty(R)} \cong \operatorname{nil}(R)$ as sets, and the group structure on $\operatorname{nil}(R)$ is the multiplicative one: $x * y = x + y + xy$. As is evident, while $\operatorname{nil}(A)$ is well-defined for p-polar k-algebras A, the group law is not.

Recall (e.g. from [Rav86]) that a formal group law G over a torsion free $\mathbf{Z}_p$-algebra R is *p-typical* iff its logarithm $\log_G(x) \in (R \otimes \mathbf{Q})[\![x]\!]$ is of the form $\log_G(x) = \sum_{i \geq 0} l_i x^{p^i}$ (with $l_0 = 1$). It is straightforward to see that the (compositionally) inverse power series $\exp_G(x)$ of a p-typical formal group G has the form

$$\exp_G(x) = \sum_{i \geq 0} a_i x^{1+i(p-1)} \quad \text{for some } a_i \in R \otimes \mathbf{Q},\ a_0 = 1.$$

Thus both $\log_G$ and $\exp_G$ are in fact elements of the p-polar power series algebra

$$\prod_{i \geq 0} (R \otimes \mathbf{Q})\langle x^{1+i(p-1)} \rangle \subset (R \otimes \mathbf{Q})[\![x]\!].$$

Hence if A is a p-polar R-algebra then $\operatorname{nil}(A)$ obtains a group structure by

$$x * y = \exp_G(\log_G(x) + \log_G(y)),$$

agreeing with $G(R)$ is $A = \operatorname{pol}_p(R)$.

Now consider the multiplicative formal group $\hat{\mathbb{G}}_m$ defined over $\mathbf{Z}_p$, represented by $\mathbf{Z}_p[\![x]\!]$ with $\Delta(x) = x \otimes 1 + 1 \otimes x + x \otimes x$. Cartier's theorem [Car67], cf. [Rav86] says that $\hat{\mathbb{G}}_m$ is canonically isomorphic to a p-typical formal group G. By base change to the $\mathbf{Z}_p$-algebra k, this shows that μ_{p^∞} is isomorphic to a functor (indeed, a formal group) defined on all p-polar k-algebras. Thus the functor denotes by $_p((R \otimes_k \bar{k})^\times)$ in Theorem 1.3 is indeed naturally isomorphic to one that extends to p-polar k-algebras.

3. Witt vectors of p-polar rings

The (p-typical) Witt vector functor [Wit37] W and its truncated variants W_n take values in rings and are defined on the category of rings. Since $W_1(A) \cong A$, no information of the input ring is lost. However, if one is only interested in $W(A)$ as an abelian group with Frobenius and Verschiebung operations, one can ask what the minimal required structure on A is. A ring structure is enough; an abelian group structure alone is not. It turns out that the structure is exactly that of a p-polar ring. Background on Witt vectors and related constructions can be found in [Hes08, Haz09, Ser68].

Throughout this section, let k be a perfect field of characteristic p.

Let $W(k)$ denote the ring of p-typical Witt vectors on k. The pth power map on k lifts to a $\mathbf{Z}_p$-linear map $\operatorname{frob}\colon W(k) \to W(k)$ which is an isomorphism since k is perfect.

For a $W(k)$-module M and an integer n, we denote by $M(n)$ the $W(k)$-module with underlying abelian group M and $W(k)$-action

$$a.m = \mathrm{frob}^n(a)m \quad \text{for } a \in W(k),\, m \in M.$$

Define the polynomials $c_i(x,y) \in \mathbf{Z}[x,y]$ inductively by

$$x^{p^n} + y^{p^n} = c_0(x,y)^{p^n} + pc_1(x,y)^{p^{n-1}} + \cdots + p^n c_n(x,y).$$

In particular, $c_0(x,y) = x+y$ and $c_1(x,y) = \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x^i y^{p-i}$.

These polynomials are closely related to the Witt vector addition law for rings. More specifically, if A is a commutative ring and $\underline{a} = (a,0,0,\dots) \in W(A)$ denotes the Teichmüller representative of an element $a \in A$ then

$$\underline{a} + \underline{b} = (c_0(a,b), c_1(a,b), \dots). \tag{3.1}$$

In fact, the addition of any two Witt vectors can be expressed using these polynomials since

$$(a_0, a_1, \dots) = \underline{a_0} + V(\underline{a_1}) + \dots,$$

V is linear, and addition of Witt vectors with disjoint support is defined componentwise.

By Example 2.6 and since the degree of c_i is p^i and $p^i \equiv 1 \pmod{p-1}$ for all i, the polynomials c_i are actually elements of the free p-polar algebra $P(x,y) < \mathbf{Z}[x,y]$. Hence it makes sense to define a Witt vector functor for p-polar rings as follows:

Definition. For a p-polar ring A, define its group of Witt vectors by

$$W(A) = \prod_{i \geq 0} A$$

with the addition defined as in (3.1) and extended to all of $W(A)$ as in the comment following that equation.

The truncated Witt vectors $W_n(A)$ are defined in an analogous manner.

Just as in the classical case, there is a ghost map

$$w\colon W_n(A) \to \prod_{i=0}^{n} A \qquad (0 \leq n \leq \infty)$$

given by

$$w(a_0, a_1, \dots) = (a_0, a_0^p + pa_1, a_0^{p^2} + pa_1^p + p^2 a_2, \dots).$$

If the target of w is given the structure of a product group, then w is a homomorphism of abelian groups.

We will make use of the following version of Dwork's lemma for polar rings:

Lemma 3.2 (Dwork)**.** *Let A be a p-polar $W(k)$-algebra. Assume that there is a polar $W(k)$-algebra map $\phi\colon A \to A(1)$ such that $\phi(a) \equiv a^p \pmod{p}$. Then a sequence $(x_0, x_1, \dots) \in \prod_{i=0}^{\infty} A$ is in the image of w iff $x_n \equiv \phi(x_{n-1}) \pmod{p^n}$ for all $n \geq 1$.*

The classical proof, e.g. as in [Hes08, Lemma 1], works almost without changes. For the reader's convenience, we include it here.

Proof. As a first step, we show that $a^p \equiv b^p \pmod{p^{n+1}}$ if $a \equiv b \pmod{p^n}$. Indeed, if $b = a + p^n d$ then

$$b^p = (a + p^n d)^p = a^p + \sum_{i=1}^{p} \binom{p}{i} p^{ni} a^{p-i} d^i$$

by multilinearity and symmetry of μ. Since $\binom{p}{1} = p$, then $p^{n+1} \mid b^p - a^p$.

In particular, $\phi(a)^{p^n} \equiv a^{p^n} \pmod{p^{n+1}}$ by induction. Now, since ϕ is a homomorphism of polar rings, we have that

$$\phi(w_{n-1}(a)) = \sum_{i=0}^{n-1} p^i \phi(a_i)^{p^{n-1-i}} \equiv \sum_{i=0}^{n} p^i a_i^{p^{n-i}} = w_n(a) \pmod{p^n}.$$

This shows that if $(x_0, x_1, \dots)$ is in the image of w then it satisfies the stated congruence. Conversely, suppose the congruence holds. Construct a_i inductively by first choosing $a_0 = x_0$. Having constructed $a_0, \dots, a_{n-1}$, observe that

$$D_n = x_n - \sum_{i=0}^{n-1} p^i a_i^{p^{n-i}} \equiv 0 \pmod{p^n}.$$

Thus choose a_n such that $p^n a_n = D_n$. □

Corollary 3.3. *In the situation of Dwork's lemma, the natural transformations*

$$F\colon \prod_{i=0}^{n} A \to \prod_{i=1}^{n} A \quad \textit{and} \quad V\colon \prod_{i=1}^{n} A \to \prod_{i=0}^{n} A$$

given by

$$F(x_0, x_1, \dots, x_n) = (x_1, \dots, x_n) \quad \textit{and} \quad V(x_1, \dots, x_n) = (0, px_1, \dots, px_n)$$

descend to natural transformations

$$F\colon W_n(A) \to W_{n-1}(A) \quad \textit{and} \quad V\colon W_{n-1}(A) \to W_n(A).$$

On $W_{n-1}(A)$, V is given by $V(a_0, \dots, a_{n-1}) = (0, a_0, \dots, a_{n-1})$. On $W_n(A)$, F is determined by $F(\underline{a}) = \underline{a^p}$ and $FV = p$.

Denote by $\mathcal{R} = W(k)\langle F, V\rangle/(FV - p)$ the ring obtained from $W(k)$ by adjoining two variables F, V such that $FV = VF = p$ and such that commutation with scalars is governed by

$$Fa = \mathrm{frob}(a)F \quad \text{and} \quad Va = \mathrm{frob}^{-1}(a)V.$$

Then $W_n(A)$ becomes an $\mathcal{R}$-module and w a homomorphism of $\mathcal{R}$-modules with the above structure.

As in [Fon77] or [BC19], we define the group of unipotent co-Witt vectors as the colimit

$$CW^u(A) = \mathrm{colim}(W_0(A) \xrightarrow{V} W_1(A) \xrightarrow{V} \cdots)$$

This works when A is merely a p-polar ring because W_n and V are well-defined there, as shown above.

Define the set of co-Witt vectors as

$$CW(A) = \{(a_i) \in A^{\mathbf{Z}_{\leq 0}} \mid (a_{-r}, a_{-r-1}, \dots)^{p^s} = 0 \text{ for some } r, s \geq 0\}.$$

This functor (as a functor on finite-dimensional k-algebras) is in fact a formal group [Fon77, §II.4], i.e. ind-representable.

To see that $CW(A)$ has the structure of an $\mathcal{R}$-module even when A is just a p-polar ring, containing $CW^u(A)$ as a submodule, we use and adapt the arguments of [Fon77, §II.1.5].

Define the polynomial $S_n(x_0,\dots,x_n,y_0,\dots,y_n)$ as the nth component of the Witt vector addition $(x_0,x_1,\dots,x_n)+(y_0,y_1,\dots,y_n) \in W(\mathbf{Z}[x_0,\dots,x_n,y_0,\dots,y_n])$. Note that this polynomial is in fact an element of the free p-polar ring (cf. Ex. 2.6) $P(x_1,\dots,x_n,y_1,\dots,y_n)$, and hence can be evaluated on elements of p-polar rings.

Proposition 3.4. *Let A be a p-polar ring and $a=(a_i)$, $b=(b_i) \in CW(A)$. Then*

(1) *For each $n \geq 0$, the sequence*
$$S_m(a_{-n-m},\dots,a_{-n},b_{-n-m},\dots,b_{-n})$$
is eventually constant as $m \to \infty$. Let us call the limit value $S_{-n}(a,b)$.

(2) *$S_{-n}(a,b) \in CW(A)$.*

Proof. This is proved for commutative rings in [Fon77, Prop. II.1.1].

Since a, $b \in CW(A)$, there exist natural numbers r,s such that
$$(a_{-r},a_{-r-1},\dots,b_{-r},b_{-r-1},\dots)^{p^s}=0.$$
Let
$$R=\mathbf{Z}[x_i,y_i \mid i \leq 0]/(x_{-r},x_{-r-1},\dots,y_{-r},y_{-r-1},\dots)^{p^s}.$$
Then by [Fon77, Prop. II.1.1], the sequence $S_m(x_{-n-m},\dots,x_{-n},b_{-n-m},\dots,b_{-n})$ is eventually constant as $m \to \infty$, and its limit lies in $CW(R)$. In fact, as observed before, it lies in $CW(P)$, where
$$P=P(x_i,y_i \mid i \leq 0]/(x_{-r},x_{-r-1},\dots,y_{-r},y_{-r-1},\dots)^{p^s} < R.$$
Since this is the universal case for elements a,b with the chosen vanishing properties, the claim follows from naturality. ☐

The $\mathcal{R}$-module structure on $CW(A)$ is thus given by the addition
$$\begin{aligned} a+b &= (\dots,S_{-2}(a,b),S_{-1}(a,b),S_0(a,b)),\\ Va &= (\dots,a_2,a_1), \quad \text{and}\\ Fa &= (\dots,a_2^p,a_1^p,a_0^p). \end{aligned}$$

Remark 3.5. The structure of a p-polar algebra is the minimal structure needed to define the Witt vector functor; indeed, A can be reconstructed from the abelian groups $W_1(A)$ and $W_2(A)$ as follows. As an abelian group, $A=W_1(A)$. For elements $x_1,\dots,x_p \in A$, we have:
$$\underline{x}_1+\dots+\underline{x}_p=(x_1+\dots+x_p,x_1\cdots x_p) \in W_2(A),$$
and the p-polar structure can be extracted from the second coordinate.

Example 3.6 (Witt vectors of free p-polar algebras)**.** The ring $W(\mathbf{F}_p[x])$ is described in [Bor16, Exercise 1(10)]. It is a subring of the p-completed monoid ring $\mathbf{Z}_p[\mathbf{N}[\frac{1}{p}]]^\wedge_p = W(\mathbf{F}_p[\mathbf{N}[\frac{1}{p}]])$ consisting of those series $\sum a_{\frac{n}{p^i}}[\frac{n}{p^i}]$ such that $p^i \mid a_{\frac{n}{p^i}}$. The group $W(P(x))$ of the free p-polar algebra on one generator is the subgroup of power series where $a_{\frac{n}{p^i}}=0$ unless $n \equiv 1 \pmod{p-1}$.

4. The Dieudonné correspondence and proof of the main theorems

Continue to let k be a perfect field of characteristic p.

Definition 4.1. Denote by Dmod_k the category of Dieudonné modules over k. These are $\mathcal{R}$-modules, i.e. $W(k)$-modules with homomorphisms

$$V\colon M \to M \quad \text{and} \quad F\colon M \to M$$

such that $FV = VF = p$, $Fa = \mathrm{frob}(a)F$ and $aV = V\,\mathrm{frob}(a)$ for $a \in W(k)$.

Denote by Dmod_k^p the full subcategory of *p-adic* Dieudonné modules. These are modules M such that for all $x \in M$, the $W(k)$-submodule spanned by $V^i(x)$, for all i, is of finite length.

Dually, let $\mathbb{D}\,\mathrm{mod}_k^F$ be the full subcategory of *F-profinite* Dieudonné modules, i. e. modules M that are profinite as $W(k)$-modules and have a fundamental system of neighborhoods consisting of $W(k)$-modules closed under F.

The following theorem follows from classical Dieudonné theory (cf. [BC19, Section 6], [DG70]):

Theorem 4.2. *There are equivalences of abelian categories*

$$D\colon (\mathrm{AbSch}_k^p)^{\mathrm{op}} \to \mathrm{Dmod}_k^p$$

and

$$\mathbb{D}^{\mathrm{f}}\colon\ \mathrm{Fgps}_k^p \to \mathbb{D}\,\mathrm{mod}_k^F$$

These functors are given by

$$D(G) = \operatorname*{colim}_n \mathrm{Hom}_{\mathrm{AbSch}_k}(G, W_n) \oplus \Big(\mathrm{Gr}(\mathcal{O}_G \otimes_k \bar{k}) \otimes W(\bar{k})\Big)^{\Gamma}$$

and

$$\mathbb{D}^{\mathrm{f}}(G) = \mathrm{Hom}_{\mathrm{Fgps}_k}(G, CW)$$

The statement in [BC19] actually contains an error for the formula for the second summand of $D(G)$, and we take the opportunity to rectify it here.

Proof. The proof given in [BC19] is correct with the exception of the multiplicative part (the second summand) of $D(G)$, i.e. $D(G)$ for G of multiplicative type. Here, an abelian affine group scheme G is said to be of multiplicative type if the formal scheme underlying its dual formal group is pro-étale.

Let

$$D'(G) = I(\mathbb{D}^{\mathrm{f}}(G^*)),$$

where G^* denotes the formal group Cartier dual to G, and $I = \mathrm{Hom}_{W(k)}(-, CW(k))$ denotes Matlis (or Pontryagin) duality between $W(k)$-modules and pro-(finite length) $W(k)$-modules. Since both dualities are anti-equivalences of categories and $\mathbb{D}^{\mathrm{f}}$ is an equivalence, so is D'. It remains to show that $D'(G) = D(G)$.

For this, recall (e.g. from [Fon77, §I.7]) that the category of affine groups of multiplicative type over k is equivalent with the category Mod_Γ of abelian groups with a discrete action of the absolute Galois group Γ via the functor $G \mapsto \mathrm{Gr}(\mathcal{O}_G \otimes_k \bar{k})$, where Gr denotes the grouplike elements of a Hopf algebra.

Write $\overline{CW} = \mathrm{colim}_{k<k'<\bar{k}}\, CW(k')$ and $\overline{W} = \mathrm{colim}_{k<k'<\bar{k}}\, W(k')$, where k' runs through all finite field extensions of k contained in some algebraic closure $\bar{k}$. Then in terms of these Γ-modules, the functors D and D' are given, respectively, by

$$D(M) = (M \otimes \overline{W})^{\Gamma}$$

and

$$D'(M) = I(\mathrm{Hom}^\Gamma(M, \overline{CW})) = I(\mathrm{Hom}^\Gamma_{\overline{W}}(M \otimes \overline{W}, \overline{CW}))$$

By Galois descent (cf. [Fon77, §III.2]), the category of $\overline{W}$-modules with semilinear Γ-actions is equivalent to the category of $W(k)$-modules by taking Γ-fixed points, and hence the last expression equals

$$I(\mathrm{Hom}_{W(k)}((M \otimes \overline{W})^\Gamma, CW(k)) = (M \otimes \overline{W})^\Gamma.$$

□

Proof of Thm. 1.3. We first consider the formal case. For a formal scheme S represented by a profinite algebra A (in particular, for algebras of finite dimension over k), we have that

$$\mathbb{D}^{\mathrm{f}}(\mathrm{Fr}(A)) = \mathrm{Hom}_{\mathrm{Fgps}_k}(\mathrm{Fr}(A), CW) = \mathrm{Hom}_{\mathrm{FSch}_k}(\mathrm{Spf}\,(A)\,, CW) = CW(A).$$

Here FSch_k, the category of formal schemes over k, is dual to the category of profinite k-algebras.

For the affine case of Thm. 1.3, we first describe the free p-adic affine group functor. Recall that an affine group G is p-adic iff $G \cong G^\wedge_p = \lim_n G/p^n$ as affine group schemes. Evidently, the inclusion of p-adic groups into all groups has the p-completion $G \mapsto G^\wedge_p$ as a left adjoint, and the free p-adic group functor is just the free abelian group functor followed by p-completion.

In more explicit terms, any $G \in \mathrm{AbSch}_k$ splits naturally as $G \cong G^m \times G^u$, where G^m is a group of multiplicative type, and G^u is unipotent. Unipotent groups are automatically p-adic (their Dieudonné modules are those where V acts nilpotently on every element), and the free unipotent group on an affine scheme $\mathrm{Spec}\,A$ is represented by the cofree cocommutative unipotent Hopf algebra on A, which is the Hopf algebra of symmetric tensors $\bigoplus_{n\geq 0}(A^{\otimes_k n})^{\Sigma_n}$ (cf. [BC19, Proof of Thm. 1.3]). A group of multiplicative type is p-adic if it is isomorphic to $\mathrm{Spec}\,\bar{k}[M]$ for a p-torsion group M after base change to an algebraic closure $\bar{k}$ of k. In the case where $k \cong \bar{k}$, the free multiplicative p-adic group on $\mathrm{Spec}\,A$ is represented by $k[{}_p(A^\times)]$, where ${}_pA^\times$ denotes the p-torsion part of the group of units of A, and in the general case, it is represented by the Galois invariants (cf. [BC19, Proof of Thm. 1.3])

$$\bar{k}[{}_p(A \otimes \bar{k})^\times]^{\mathrm{Gal}(k)}.$$

Now for a affine scheme S represented by an algebra A, we have that

$$\begin{aligned} D(\mathrm{Fr}(A)) &= \mathrm{colim}\,\mathrm{Hom}_{\mathrm{AbSch}_k}(\mathrm{Fr}(A), W_n) \oplus \Big({}_p(A \otimes_k \bar{k})^\times \otimes W(\bar{k})\Big)^\Gamma \\ &= \mathrm{colim}\,W_n(A) \oplus \Big({}_p(A \otimes_k \bar{k})^\times \otimes W(\bar{k})\Big)^\Gamma, \end{aligned}$$

completing the proof of the affine case. □

Since the Dieudonné functor does not give an equivalence between all formal groups and Dieudonné modules, the proof of Thm. 1.2 is not yet complete in the formal case. Formal groups $G \in \mathrm{Fgps}_k$ split naturally, in a dual fashion to affine groups, as $G \cong G^e \times G^c$ into an étale and a connected part. In fact, Cartier duality $G \mapsto G^*$ between formal groups and affine groups carries this splitting to the splitting of affine groups discussed above:

$$(G^e)^* \cong (G^*)^m \quad \text{and} \quad (G^c)^* \cong (G^*)^u.$$

We denote the étale part of $\mathrm{Fr}(R)$ by $\mathrm{Fr}^e(R)$ and the connected part by $\mathrm{Fr}^c(R)$.

Let us describe the $\mathrm{Fr}^e(R)$ more concretely, for a finite-dimensional k-algebra R. The category of étale formal groups is equivalent to the category Mod_Γ of abelian groups with a discrete action of the absolute Galois group $\Gamma = \mathrm{Gal}(k)$ (cf. [Fon77, §I.7], [BC19, Thm. 1.6]); this equivalence is simply given by the functor $G \mapsto \mathrm{colim}_{k<k'<\bar{k}} G(k')$, where k' runs through the finite extensions of k, and the inverse functor is given by $M \mapsto \mathrm{Spf}\left(\mathrm{map}^\Gamma(M, \bar{k})\right)$.

Lemma 4.3. *Let R be a finite-dimensional k-algebra. Then the Γ-module associated with $\mathrm{Fr}^e(R)$ is*

$$\mathbf{Z}\langle \mathrm{Hom}_{\mathrm{Alg}_k}(R, \bar{k})\rangle$$

Proof. Let G be an étale formal group with corresponding Γ-module M. We have:

$$\begin{aligned}\mathrm{Hom}_{\mathrm{Fgps}_k}(\mathrm{Fr}^e(R), G) &= \mathrm{Hom}_{\mathrm{FSch}_k}(\mathrm{Spec}\, R, G)\\ &= \mathrm{Hom}_{\mathrm{FSch}_k}(\mathrm{Spec}\, R^e, G) = \mathrm{Hom}_{\mathrm{Pro-Alg}_k}(\mathrm{map}^\Gamma(M, \bar{k}), R^e),\end{aligned}$$

where R^e denotes the maximal étale subalgebra of R, isomorphic to $R/\mathrm{Nil}(R)$.

By Galois descent (or rather, ascent), this is isomorphic to the group

$$\underset{j}{\mathrm{colim}}\, \mathrm{Hom}_{\mathrm{Alg}_{\bar{k},\Gamma}}(\mathrm{map}(M^j, \bar{k}), R^e \otimes_k \bar{k}),$$

of Γ-semilinear homomorphisms, where M^j runs through the finite Γ-invariant subsets of M; they exhaust M because the Γ-action on M is discrete. Now $R^e \otimes_k \bar{k}$ is isomorphic to a finite product of copies of $\bar{k}$, indeed $R^e \otimes_k \bar{k} \cong \mathrm{map}(\mathrm{Hom}_{\mathrm{Alg}_k}(R, \bar{k}), \bar{k})$. Since $\mathrm{Hom}_{\mathrm{Alg}_{\bar{k}}}(\mathrm{map}(X, \bar{k}), \bar{k}) = X$ for finite sets X, this is isomorphic to

$$\mathrm{map}^\Gamma(\mathrm{Hom}_{\mathrm{Alg}_k}(R, \bar{k}), M) = \mathrm{Hom}^\Gamma(\mathbf{Z}\langle \mathrm{Hom}_{\mathrm{Alg}_k}(R, \bar{k})\rangle, M),$$

where Γ acts on $\bar{k}$ on the source. ☐

Lemma 4.4. *Let k be algebraically closed and let A be a finite,* reduced *p-polar k-algebra, i.e. one such that for $x \neq 0$, we have that $x^{p^N} \neq 0$ for all $N \geq 0$. Then A is isomorphic to a finite product of polarizations of k.*

Proof. Suppose A has a unity in the sense of Remark 2.4, i.e. an element $u \in A$ such that $u^{p-1}a = a$ for all $a \in A$. Then, by the quoted remark, $A = \mathrm{pol}(\tilde{A})$, where $\tilde{A}$ is the algebra structure on A given by $x \cdot y = \mu(u, \ldots, u, x, y)$. Since $\tilde{A}$ is reduced and finite, it is a product of finitely many copies of k.

For the general case, I claim that A has an element x such that $x^p = x$. Indeed, given any nonzero element $y \in A$, the powers $y, y^p, y^{p^2}, \ldots$ cannot all be linearly independent by the finiteness of A, and they are all nonzero by reducedness, so $y^{p^j} = \sum_{i=0}^{p^j} \alpha_i y^{p^i}$ for some $\alpha_i \in k$, not all zero. Let β be a nonzero root of the polynomial

$$p(x) = \sum_{i=0}^{j-1} \alpha_i^{p^{j-i-1}} x^{p^{j-i}} - x$$

and

$$x = \sum_{k=0}^{j-1} \Big(\sum_{i=0}^{k} \alpha_k^{p^{k-i}} \beta^{p^{k+1-i}} \Big) y^{p^k}.$$

Then it is straightforward to verify that $x^p = x$.

Now consider the map $f\colon A \to A$ given by $y \mapsto x^{p-1}y$. Since $x^p = x$, this map is idempotent and a p-polar k-algebra endomorphism. Thus

$$A \cong \ker(f) \times \operatorname{im}(f)$$

as p-polar algebras. Note that $\operatorname{im}(f)$ is a nontrivial p-polar algebra with unity x, so by the previous case, it is a product of copies of k. The p-polar algebra $\ker(f)$ has smaller dimension over k, so we are done by induction. □

Lemma 4.5. *The functor* $\mathrm{alg}_k \to \mathrm{Mod}_\Gamma$ *given by* $A \mapsto \mathbf{Z}\langle \mathrm{Hom}_{\mathrm{alg}_k}(A, \bar{k})$ *factors through* $\mathrm{pol}_p(k)$.

Proof. Let $\mathcal{E}$ be the full subcategory of $\mathrm{pol}_p(\bar{k})$ of reduced p-polar algebras. There is a functor $\mathrm{pol}_p(\bar{k}) \to \mathcal{E}$ given by $A \mapsto A/\operatorname{Nil}(A)$. By Lemma 4.4, all objects of $\mathcal{E}$ are isomorphic to $\bar{k}^n$ for some $n \geq 0$. Consider the set

$$\mathrm{Hom}_{\mathrm{pol}_p(\bar{k})}(\bar{k}^n, \bar{k}).$$

One easily verifies that a linear map $\bar{k}^n \to \bar{k}$ represented by a row vector $(a_1, \dots, a_p)$ is a homomorphism of p-polar algebras iff it is zero or exactly one a_i is nonzero, and furthermore $a_i \in \mathbf{F}_p$. We now construct a functor to abelian groups,

$$\Phi\colon \mathcal{E} \to \mathrm{Ab}$$

by defining $\Phi(\bar{k}^n) = \mathbf{Z}^n$ and for a morphism $\bar{k}^n \to \bar{k}^m$ represented by a matrix M, $\Phi(M)$ is the matrix M with every nonzero entry replaced by 1. Because of the special form of M, this is indeed a well-defined functor. Moreover, it carries the Γ-action on $A \otimes_k \bar{k}$ to an action by permutation matrices on $\Phi(A \otimes_k \bar{k})$. We have that $\Phi(\mathrm{pol}_p(R)) \cong \mathbf{Z}\langle \mathrm{Hom}_{\mathrm{Alg}_k}(R, k)\rangle$ for reduced R over algebraically closed k.

Now define

$$\mathcal{F}\colon\ \mathrm{pol}_p(k) \to \mathrm{Ab}$$

by $\mathcal{F}(A) = \Phi\Big((A \otimes_k \bar{k})/\operatorname{Nil}(A \otimes_k \bar{k})\Big)$. By the above, this is the desired extension. □

Proof of the formal case of Thm. 1.2. The Hopf algebra H representing G^* for a formal p-group G satisfies $H \cong \operatorname{colim}_n H[p^n]$, the Hopf colimit of the Hopf kernels of the multiplication-by-p^n map $[p^n]$. Unipotent Hopf algebras (and hence connected formal groups) are automatically p-adic, and the Dieudonné functor restricts to an equivalence between unipotent Hopf algebras and V-nilpotent Dieudonné modules. This shows that the required factorization exists for the connected part:

$$\begin{array}{ccc} \mathrm{Alg}_k & \xrightarrow{\mathrm{Fr}^c} & \mathrm{Fgps}_k \\ & \searrow^{\mathrm{pol}} & \uparrow{\scriptstyle \tilde{\mathrm{Fr}}^c} \\ & & \mathrm{Pol}_p(k) \end{array}$$

The factorization of the étale part is Lemma 4.5. □

References

[BC19] Tilman Bauer and Magnus Carlson. Tensor products of abelian affine group schemes, formal groups, and p-divisible groups over perfect fields. *Documenta Mathematica*, 24:2525–2582, 2019.

[Bor16] James Borger. Witt vectors, lambda-rings, and arithmetic jet spaces. Lecture notes and exercises, available at https://maths-people.anu.edu.au/~borger/classes/copenhagen-2016/, 2016.

[Car67] Pierre Cartier. Modules associés à un groupe formel commutatif. Courbes typiques. *C. R. Acad. Sci. Paris Sér. A-B*, 265:A129–A132, 1967.

[DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. Avec un appendice ıt Corps de classes local par Michiel Hazewinkel.

[Fon77] Jean-Marc Fontaine. *Groupes p-divisibles sur les corps locaux*. Société Mathématique de France, Paris, 1977. Astérisque, No. 47-48.

[Haz09] Michiel Hazewinkel. Witt vectors. I. In *Handbook of algebra. Vol. 6*, volume 6 of *Handb. Algebr.*, pages 319–472. Elsevier/North-Holland, Amsterdam, 2009.

[Hes08] Lars Hesselholt. Lecture notes on Witt vectors. preprint at http://web.math.ku.dk/~larsh/papers/s03/wittsurvey.pdf, 2008.

[Rav86] Douglas C. Ravenel. *Complex cobordism and stable homotopy groups of spheres*, volume 121 of *Pure and Applied Mathematics*. Academic Press Inc., Orlando, FL, 1986.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Wit37] Ernst Witt. Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p. *J. Reine Angew. Math.*, 176:126–140, 1937.

KTH Royal Institute of Technology, Institutionen för matematik, Lindstedtsvägen 25, 10044 Stockholm, Sweden

Email address: tilmanb@kth.se