p-Jets of Finite Algebras, I: p-Divisible Groups

Alexandru Buium

Received: January 12, 2012

Communicated by Lars Hesselholt

Abstract. p-jets of finite flat maps of schemes are generally neither finite nor flat. However, for p-isogenies, and in particular for p-divisible groups, this pathology tends to disappear "in the limit". We illustrate this in the case of $\mathbb{G}_m$, elliptic curves, and formal groups of finite height.

2010 Mathematics Subject Classification: 14 L 05, 13 K 05
Keywords and Phrases: Formal groups, p-divisible groups, Witt vectors

1. Introduction

This paper is the first in a series of papers where we investigate p-jet spaces (in the sense of [3]) of finite flat schemes/algebras. The understanding of such p-jet spaces seems to hold the key to a number of central questions about *arithmetic differential equations* [4]. The present paper deals with p-isogenies, and in particular with p-divisible groups; a sequel to this paper [8] will deal with algebras of Witt vectors of finite length.

Let p be an odd prime and let $R = \widehat{\mathbb{Z}_p^{ur}}$ be the p-adic completion of the maximum unramified extension of the ring $\mathbb{Z}_p$ of p-adic numbers. (Throughout the paper the symbol $\widehat{\ }$ means p-adic completion.) Let $k = R/pR$ be the residue field of R. Then for each integer $n \geq 0$ a functor J^n was introduced in [3] that attaches to any scheme of finite type X/R a (Noetherian) p-adic formal scheme $J^n(X)$ over R called the *p-jet space* of X of order n. For each X there are morphisms $J^n(X) \to J^{n-1}(X)$, $n \geq 1$, functorial in X, and $J^0(X) = \widehat{X}$. We refer to [3, 4] for an exposition of the theory and for some of the applications of these spaces; see also [6, 2] for a several prime version of the theory.

The functors J^n behave nicely on smooth schemes and étale morphisms: in particular if X is smooth over R then $J^n(X)$ are p-adic completions of smooth schemes over R; and if $X \to Y$ is an étale morphism then $J^n(X) \simeq J^n(Y) \times_Y X$. So, in particular, if $X \to Y$ is finite and étale then the map $J^n(X) \to J^n(Y)$ is again finite and étale. However if $X \to Y$ is, say, finite and flat then $J^n(X) \to J^n(Y)$ is generally neither finite nor flat. This basic pathology can be seen, in its simplest form, for X a finite flat group scheme of degree a p-power over $Y = Spec\ R$; or for p-isogenies $X \to Y$ (i.e. isogenies of degree a p-power) between smooth group schemes over R. The present paper offers an analysis of p-jets of p-isogenies $[p^\nu] : X \to X$ and of p-divisible groups $(X_\nu; \nu \geq 1)$, $X_\nu := \text{Ker}\ [p^\nu]$, where X is either the multiplicative group, or an elliptic curve, or a (one dimensional) formal group of finite height. (For the latter case one still has at one's disposal a p-jet space theory.) The main moral of the story will be that although the p-jets of order n of the individual X_ν's are generally highly pathological order tends to be restored "in the limit", when either $n \to \infty$ or $\nu \to \infty$. One of our main motivations for trying to understand the p-jets of p-isogenies is their apparent link with the problem of understanding the U-operator (and the Hecke operator $T(p)$) on *differential modular forms*. Discussing this link here would lead us too far afield; the interested reader can see a hint of this in [5, 7].

In order to state some of our main results let us recall/introduce some basic notation. For any scheme of finite type X/R the rings of global functions $\mathcal{O}^n(X) := \mathcal{O}(J^n(X))$ form an inductive system; its direct limit is denoted by $\mathcal{O}^\infty(X)$. There are canonical (non-linear) operators $\delta : \mathcal{O}^n(X) \to \mathcal{O}^{n+1}(X)$ that can be viewed as arithmetic analogues of the total derivative operator in differential geometry/mechanics.

Here is a basic example that we are going to be interested in. Let $x, x', x'', ...$ be variables and consider the rings

$$A^n := R[x, x', ..., x^{(n)}] \subset A := R\{x\} := R[x, x', x'', ...]$$

whose elements are referred to as δ-polynomials. Let $\phi : R \to R$ be the unique ring automorphism that lifts the p-power Frobenius on k and let $\phi : A \to A$ be the unique ring homomorphism which is the ϕ above on R and sends $x, x', x'', ...$ into $x^p + px', (x')^p + px'', (x'')^p + px''', ...$ respectively. Then one defines the following map of sets (the Fermat quotient operator):

$$\delta : A \to A, \quad \delta F = \frac{\phi(F) - F^p}{p}.$$

This map induces maps $\delta : A^n \to A^{n+1}$, and by continuity, maps $\delta : (A^n)\hat{} \to (A^{n+1})\hat{}$ (where $\hat{}$ always denotes in this paper the p-adic completion). Note that if $\mathbb{A}^1 = Spec\ R[x] = Spec\ A^0$ is the affine line over R then $J^n(\mathbb{A}^1) = Spf\ (A^n)\hat{}$ and the arithmetic analogues of the total derivatives $\delta : \mathcal{O}^n(\mathbb{A}^1) \to \mathcal{O}^{n+1}(\mathbb{A}^1)$ identify with the Fermat quotient operators $\delta : (A^n)\hat{} \to (A^{n+1})\hat{}$ we just introduced.

A related example is $\mathbb{G}_m = Spec\ R[x, x^{-1}]$ in which case $J^n(\mathbb{G}_m) = Spf\ A^n[x^{-1}]\hat{}$ and $\delta : \mathcal{O}^n(\mathbb{G}_m) \to \mathcal{O}^{n+1}(\mathbb{G}_m)$ is induced by the δ above. If $[p^\nu] : \mathbb{G}_m \to \mathbb{G}_m$ is the p-isogeny defined by $x \mapsto x^{p^\nu}$ then the induced morphism $[p^\nu] : J^n(\mathbb{G}_m) \to J^n(\mathbb{G}_m)$ is given by the map

$$[p^\nu]^* : A^n[x^{-1}]\hat{} \to A^n[x^{-1}]\hat{}, \quad x^{(i)} \mapsto \delta^i(x^{p^\nu}).$$

Moreover if $\mu_{p^\nu} = \mathbb{G}_m[p^\nu]$ is the kernel of $[p^\nu] : \mathbb{G}_m \to \mathbb{G}_m$ then

$$\mathcal{O}^n(\mu_{p^\nu}) = \frac{A^n[x^{-1}]\hat{}}{(x^{p^\nu} - 1, \delta(x^{p^\nu}), ..., \delta^n(x^{p^\nu}))}$$

So it becomes crucial to compute the δ-polynomials $\delta^n(x^{p^\nu})$.
Consider the filtration of A by the subrings:

$$A^{\{n\}} = A^n + pA^{n+1} + p^2A^{n+2} + ... \subset A$$

and consider the ideal $I = (x', x'', ...) \subset A$. Also consider the ideals $I^{[p^\nu]}$ of A generated by all δ-polynomials of the form $p^i(x^{(s)})^{p^j}$, with $s \geq 1$, $i, j \geq 0$, $i + j = \nu$. By abuse of notation, we will often denote by $[S]$ an element of a set S. The starting point of this paper will be the following "leading term computation". Let $n, \nu \geq 1$.

Theorem 1.1.

$$\delta^n(x^{p^\nu}) = \begin{cases} p^{\nu-n+1}x^{p^n(p^\nu-1)}\phi^{n-1}(x') + [(p^{\nu-n+2}A^{\{1\}}) \cap I^{[p^\nu]}] & \textit{if } n \leq \nu + 1 \\ x^{p^n(p^\nu-1)}\phi^\nu(x^{(n-\nu)}) + [A^{\{n-\nu-1\}} \cap I^{[p^\nu]}] & \textit{if } n \geq \nu + 2. \end{cases}$$

This computation will have a number of consequences (both in characteristic zero and in characteristic p). Here is a consequence in characteristic zero. Let $J^n(\mu_{p^\nu})_1$ be the kernel of the projection $J^n(\mu_{p^\nu}) \to J^0(\mu_{p^\nu})$ and write $\mathcal{O}^n(\mu_{p^\nu})_1 := \mathcal{O}(J^n(\mu_{p^\nu})_1)$. Then for $n \geq 1$ we have:

Corollary 1.2.

$$\lim_{\overleftarrow{\nu}} \mathcal{O}^n(\mu_{p^\nu})_1 = R[x', ..., x^{(n)}]\hat{}.$$

Let us mention some consequences in characteristic p. Before doing so we introduce some notation. For any ring B we denote $\overline{B} = B/(p)$; and for any $b \in B$ we let $\overline{b} \in \overline{B}$ be the image of B. In particular for any scheme of finite type X/R we set

$$\overline{\mathcal{O}^n(X)} := \mathcal{O}^n(X)/(p), \quad \overline{\mathcal{O}^\infty(X)} := \mathcal{O}^\infty(X)/(p). \tag{1.1}$$

Note that the morphisms $\overline{\mathcal{O}^n(X)} \to \overline{\mathcal{O}^\infty(X)}$ are generally not injective ! (They are injective, however, if X/R is smooth [3].) It turns out that for non-smooth X/R a special role is then played by the rings:

$$\widetilde{\mathcal{O}^n(X)} := Im(\overline{\mathcal{O}^n(X)} \to \overline{\mathcal{O}^\infty(X)}). \tag{1.2}$$

According to our notation above we may consider the ring $\overline{A} = k[x, x', x'', ...]$ and its filtration with subrings $\overline{A}^n := \overline{A^n} = k[x, x', ..., x^{(n)}]$. Also we may consider the reduction mod p, $\overline{I} = (x', x'', ...) \subset \overline{A}$, of the ideal $I = (x', x'', ...) \subset A$. Then $\overline{I^{[p^\nu]}}$ coincides with the ideal $\overline{I}^{[p^\nu]}$ in $\overline{A}$ generated by $(x')^{p^\nu}, (x'')^{p^\nu}, ...$ Moreover clearly $\overline{A}^n \cap \overline{I}^{[p^\nu]}$ is generated in $\overline{A}^n$ by $(x')^{p^\nu}, ..., (x^{(n)})^{p^\nu}$. So the reduction mod p of the morphism $J^n([p^\nu]) : J^n(\mathbb{G}_m) \to J^n(\mathbb{G}_m)$ is given by the homomorphism

$$\overline{[p^\nu]^*} : \overline{\mathcal{O}^n(\mathbb{G}_m)} = k[x, x^{-1}, x', ..., x^{(n)}] \to k[x, x^{-1}, x', ..., x^{(n)}], \quad x^{(i)} \mapsto \overline{\delta^i(x^{p^\nu})}$$

where, by Theorem 1.1:

COROLLARY 1.3. *The element* $\overline{\delta^n(x^{p^\nu})} \in \overline{A}^n$ *satisfies*

$$\overline{\delta^n(x^{p^\nu})} = \begin{cases} 0 & \text{if } 1 \leq n \leq \nu \\ x^{p^{\nu+1}(p^\nu-1)}(x')^{p^\nu} & \text{if } n = \nu+1 \\ x^{p^n(p^\nu-1)}(x^{(n-\nu)})^{p^\nu} + [\overline{A}^{n-\nu-1} \cap \overline{I}^{[p^\nu]}] & \text{if } n \geq \nu+2 \end{cases}$$

The "smallest" interesting case is $\nu = 1$, $n = 3$,

$$\overline{\delta^3(x^p)} = x^{p^3(p-1)}(x'')^p - \frac{1}{2}x^{p^3(p-2)}(x')^{2p}.$$

Remark 1.4. By Corollary 1.3, for $n \geq \nu+1$, the map $\overline{[p^\nu]^*} : \overline{\mathcal{O}^n(\mathbb{G}_m)} \to \overline{\mathcal{O}^n(\mathbb{G}_m)}$ induces injective finite flat maps

$$\overline{[p^\nu]^*} : \overline{\mathcal{O}^n(\mathbb{G}_m)}/(x', ..., x^{(\nu)}) \to \overline{\mathcal{O}^{n-\nu}(\mathbb{G}_m)}.$$

Indeed finiteness is clear; injectivity follows by looking at dimensions; and flatness follows from the general fact that finite surjective maps of non-singular (irreducible) varieties are automatically flat (cf., say, [9], Theorem 18.16.).

Corollary 1.3 trivially implies the following determination of $\widetilde{\mathcal{O}^n(\mu_{p^\nu})}$. Let $n, \nu \geq 1$.

COROLLARY 1.5.

$$\widetilde{\mathcal{O}^n(\mu_{p^\nu})} \simeq \frac{k[x, x', x'', ..., x^{(n)}]}{((x-1)^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n)})^{p^\nu})}.$$

The statement of the corollary above should be contrasted with the fact that, as we shall see, for all $n, \nu \geq 1$ the the rings $\overline{\mathcal{O}^n(\mu_{p^\nu})}$ have positive Krull dimension (actually they are polynomial rings in $\min\{n, \nu\}$ variables over some explicit local Artin rings).

Remark 1.6. As we saw the mod p Corollary 1.5 follows trivially from our characteristic zero Theorem 1.1. We will also present an alternative proof of this mod p result using a Witt vector computation; we are indebted to the referee for this alternative proof. We included both approaches because each has its own advantage: the Witt vector computation yields a shorter argument (but apparently working only mod p) whereas the computation in Theorem 1.1 is valid in characteristic zero and has other consequences as well.

The above theory has an analogue for formal groups of height ≥ 2 which we now explain. We consider the rings

$$\mathcal{A}^n = R[[x]][x', ..., x^{(n)}]\hat{}, \quad \mathcal{A} := \bigcup_{n \geq 0} \mathcal{A}^n.$$

Consider the filtration of $\mathcal{A}$ by the subrings:

$$\mathcal{A}^{\{n\}} = \mathcal{A}^n + p\mathcal{A}^{n+1} + p^2\mathcal{A}^{n+2} + ... \subset \mathcal{A}$$

and consider the ideals $\mathcal{I}^{[p^\nu]}$ of $\mathcal{A}$ generated by all δ-polynomials of the form $p^i(x^{(s)})^{p^j}$, with $s \geq 0$, $i,j \geq 0$, $i+j=\nu$. (Note that, unlike in the case of the ideals $I^{[p^\nu]}$, the superscript s here is allowed to be 0! So, for instance $x^{p^\nu} \in \mathcal{I}^{[p^\nu]}$ but $x^{p^\nu} \notin I^{[p^\nu]}$.) The lift of Frobenius $\phi : A \to A$ on $A = R\{x\}$ and the Fermat quotient operator $\delta : A \to A$ induce obvious maps $\phi : \mathcal{A} \to \mathcal{A}$ and $\delta : \mathcal{A} \to \mathcal{A}$.
Now let $\mathcal{F} \in R[[x]]$ be a formal group law (in one variable) of finite height and let $\mathcal{F}[p^\nu]$ be the kernel of the multiplication by p^ν viewed as a finite flat group scheme over R. As we shall see it turns out that

$$\mathcal{O}^n(\mathcal{F}[p^\nu]) = \frac{\mathcal{A}^n}{(F^{\circ\nu}, \delta(F^{\circ\nu}), ..., \delta^n(F^{\circ\nu}))},$$

where $F(x) = [p]_{\mathcal{F}}(x) \in R[[x^p]] + pR[[x]]$ is the series giving the multiplication by p in $\mathcal{F}$ and $F^{\circ\nu}$ is its ν-th iterate. So we shall be interested in computing $\delta^n(F^{\circ\nu})$.
More generally start with any series $F \in R[[x^p]] + pR[[x]]$, $F(0) = 0$; any F of the form $[p]_{\mathcal{F}}(x)$ ($\mathcal{F}$ a formal group) has this shape. Then one easily sees that

$$F^{\circ\nu}(x) = \sum_{j=0}^{\nu} p^{\nu-j} G_j(x^{p^j}), \tag{1.3}$$

where $G_j \in xR[[x]]$, $j \geq 0$. So the computation of $\delta^n(F^{\circ\nu})$ boils down to computing the quantities $\delta^m(p^i G_j(x^{p^j}))$ for $i+j=\nu$ and $m \leq n$. Here is our main characteristic zero "leading term computation" of such quantities.
Assume $G(x) \in xR[[x]]$, $m \geq 1$, $i+j=\nu \geq 1$, $i \geq 0, j \geq 0$. Then:

Theorem 1.7.

$$\delta^m(p^i G(x^{p^j})) =$$
$$= \begin{cases} p^{i-m}\phi^m(G(x^{p^j})) + [(p^{i-m+1}\mathcal{A}^{\{0\}}) \cap \mathcal{I}^{[p^{\nu+1}]}] & \textit{if } m \leq i \\ \phi^i\{\left(\frac{dG}{dx}(x^{p^j})\right)^{p^{m-i}} \delta^{m-i}(x^{p^j})\} + [\mathcal{A}^{\{(m-\nu-1)^+\}} \cap \mathcal{I}^{[p^{\nu+1}]}] & \textit{if } m > i \end{cases}$$

Here for a an integer we set $a^+ = \max\{a, 0\}$.
The above (and indeed a much weaker statement) implies in particular that the natural homomorphism

$$\mathcal{A}^n \to \lim_{\overleftarrow{\nu}} \mathcal{O}^n(\mathcal{F}[p^\nu]) \tag{1.4}$$

is injective; this is in the spirit of Corollary 1.2. A more precise consequence of the above can be obtained by combining Theorems 1.1 and 1.7 to give a "leading term computation" for $\delta^m(F^{\circ\nu})$ in characterististic zero: all one has to do is to replace the expression $\delta^{m-i}(x^{p^j})$ in the formula of Theorem 1.7 by its value given in Theorem 1.1. Rather than stating this consequence in characteristic zero we look at some of its effects in characteristic p.
According to our conventions we may consider the ring $\overline{\mathcal{A}} = k[[x]][x', x'', ...]$ and its filtration with subrings $\overline{\mathcal{A}}^n := \overline{\mathcal{A}^n} = k[[x]][x', ..., x^{(n)}]$. Also we may consider the reduction mod p of the ideal $\mathcal{I}$, $\overline{\mathcal{I}} = (x, x', x'', ...) \subset \overline{\mathcal{A}}$. Then $\overline{\mathcal{I}^{[p^\nu]}}$ coincides

with the ideal $\overline{\mathcal{I}}^{[p^\nu]}$ generated by $x^{p^\nu}, (x')^{p^\nu}, \ldots$. Moreover clearly $\overline{\mathcal{A}}^n \cap \overline{\mathcal{I}}^{[p^\nu]}$ is generated by $x^{p^\nu}, \ldots, (x^{(n)})^{p^\nu}$ in $\overline{\mathcal{A}}^n$.

For the next Corollaries we continue to denote by F any series in $R[[x^p]]+pR[[x]]$ with $F(0)=0$ and to write its ν-th iterate as in Equation 1.3. Note that $\frac{dF^{\circ\nu}}{dx} \in p^\nu R[[x]]$ so we may consider the series

$$\overline{p^{-\nu}\frac{dF^{\circ\nu}}{dx}} \in \overline{\mathcal{A}}^0 = k[[x]].$$

Then our Theorem 1.7 will imply the following. Let $\nu \geq 1$ and $n \geq 0$.

Corollary 1.8. *The element $\overline{\delta^n(F^{\circ\nu})} \in \overline{\mathcal{A}}^n$ is given by*

$$\overline{\delta^n(F^{\circ\nu})} = \begin{cases} (\overline{G_{\nu-n}}(x^{p^{\nu-n}}))^{p^n} + [x^{2p^\nu}\overline{\mathcal{A}}^0] & \text{if } 0 \leq n \leq \nu \\ \left(\overline{p^{-\nu}\frac{dF^{\circ\nu}}{dx}}\right)^{p^n}(x^{(n-\nu)})^{p^\nu} + [\overline{\mathcal{A}}^{n-\nu-1} \cap \overline{\mathcal{I}}^{[p^\nu]}] & \text{if } n \geq \nu+1. \end{cases}$$

Remark 1.9. The case $\nu = 1$ of Corollary 1.8 above can be interpreted as follows. Let us consider $\mathbb{A}^1 = Spec\, R[x]$, the affine line over R, and its reduction mod p, $\overline{\mathbb{A}^1} = Spec\ k[x]$. Then the R-morphism $\Phi : \widehat{\mathbb{A}^1} \to \widehat{\mathbb{A}^1}$ defined by $x \mapsto \Phi^*(x) = F(x) := x^p + pf(x)$, $f(x) \in xR[x]\hat{}$, is the most general R-morphism lifting the relative (k-linear) Frobenius $\overline{\mathbb{A}^1} \to \overline{\mathbb{A}^1}$ and sending 0 into 0; Corollary 1.8 provides then, in particular, a description of the reduction mod p of the induced map

$$J^n(\Phi) : J^n(\mathbb{A}^1) \to J^n(\mathbb{A}^1) = Spf\ R[x, x', \ldots, x^{(n)}]\hat{},$$

(which sends $x, x', \ldots, x^{(n)}$ into $F, \delta F, \ldots, \delta^n F$). Note that the map $J^n(\Phi)$ is generally neither finite nor flat and its behavior depends in an essential way on the series $f(x)$.

Another immediate consequence of Corollary 1.8 is the following structure theorem for $\widetilde{\mathcal{O}^n(\mathcal{F}[p^\nu])}$. We actually prove a slightly more general result covering cases that do not come from formal groups. Let $n, \nu \geq 1$.

Corollary 1.10. *Assume $F(x) \equiv px$ mod x^2. For all $\nu \geq 1$ consider the scheme $X_\nu := Spec\ \frac{R[[x]]}{(F^{\circ\nu})}$. Then for $n \geq 1$ we have:*

$$\widetilde{\mathcal{O}^n(X_\nu)} = \frac{k[x, x', \ldots, x^{(n)}]}{(x^{p^\nu}, (x')^{p^\nu}, \ldots, (x^{(n)})^{p^\nu})}.$$

Recall that if $F = [p]_{\mathcal{F}}(x)$ for some formal group $\mathcal{F}$ then the condition $F(x) \equiv px$ mod x^2 is automatic and $X_\nu = \mathcal{F}[p^\nu]$.

Again Corollary 1.10 should be contrasted to the fact that $\overline{\mathcal{O}^n(X_\nu)}$ have positive Krull dimension (they are, again, polynomial rings in $\min\{n, \nu\}$ variables over some explicit local Artin rings).

Remark 1.11. We already mentioned that Corollary 1.5 can be proved independently of Theorem 1.1 via a Witt vector computation argument. It would be very interesting to find a similar Witt vector argument for Corollary 1.10 which is independent of Theorem 1.7, at least in the case when $F(x)$ is of the form $[p]_{\mathcal{F}}(x)$ for some formal group $\mathcal{F}$.

Remark 1.12. Results similar to Corollaries 1.5 and 1.10 above are obtained in the body of the paper for the p-divisible groups of elliptic curves. The case of ordinary elliptic curves is deduced from (a twisted version of) the results for $\mathbb{G}_m$ while the case of supersingular elliptic curves is deduced from the results on formal groups. In the ordinary case the shape of the results depends on the value of the Serre-Tate parameter.

Remark 1.13. It would be interesting to have a generalization of our computations (in characteristic zero or at least in characteristic p) to the case of arbitrary p-divisible groups.

Remark 1.14. It is interesting to note the following phenomenon. Let $X_0, ..., X_\nu$ be closed subschemes of the affine line $\mathbb{A}^1$ over R which are, say, finite and flat over R, and let

$$X = \bigcup_{i=0}^{\nu} X_i$$

(scheme theoretic union inside $\mathbb{A}^1$, defined by the intersection of the defining ideals). Then, in general,

$$J^n(X) \neq \bigcup_{i=0}^{\nu} J^n(X_i)$$

as closed subschemes of $J^n(\mathbb{A}^1)$. An example is provided by the case when $X_i = Spec\ R[\zeta_{p^i}]$ where ζ_{p^i} is a p^i-th root of unity. In this case $J^n(X_0) = Spec\ R$ and, as we shall see later in the paper, $J^n(X_i) = \emptyset$ for $i \geq 1$ and $n \geq 1$; on the other hand $X = \mu_{p^\nu}$ (kernel of multiplication by p^ν on $\mathbb{G}_m$ over R) and hence $J^n(\mu_{p^\nu})$ has a non-reduced reduction mod p by Theorem 1.10. It would be interesting to understand this phenomenon more generally when, for instance, $X_i = Spec\ R[\alpha_i]$ with α_i integers in a finite ramified extension of the fraction field of R.

Remark 1.15. In a sequel to this paper [8] we shall investigate the p-jet spaces of another remarkable example of finite flat schemes over R namely schemes of the form $Spec\ W_m(R)$ where $W_m(R)$ are the rings of Witt vectors of finite length on R.

A few words about the structure of the paper. We begin by recalling from [3, 4] some of the basic concepts we shall be dealing with. Then we will study the filtrations $A^{\{n\}}$ and $I^{[p^\nu]}$ in a general setting and we will prove Theorem 1.1. Then, in subsequent sections, we will investigate the p-jets of the divisible groups of $\mathbb{G}_m$, ordinary elliptic curves, formal groups of finite height, and supersingular elliptic curves respectively. The $\mathbb{G}_m$ case will be used as a step in the analysis of all the other cases.

Acknowledgment. The author would like to thank the referee for communicating to him the Witt vector computation argument yielding an alternative proof of Corollary 1.5. The material in this paper is based upon work supported by the National Science Foundation under Grant No. 0852591 and by the IHES, France and MPI, Bonn. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation, IHES, or MPI.

2. Review of some basic concepts [3, 4]

Rings in this paper will always be assumed commutative with unity. A p-derivation $\delta : A \to A$ on a ring A is a set theoretic map satisfying

$$\begin{array}{rcl}\delta(x+y) & = & \delta x + \delta y + C_p(x,y)\\ \delta(xy) & = & x^p\delta y + y^p \delta x + p\delta x \delta y,\end{array}$$

where C_p is the polynomial:

$$C_p(X,Y) = p^{-1}(X^p + Y^p - (X+Y)^p) \in \mathbb{Z}[X,Y].$$

If δ is as above then $\phi : A \to A$, $\phi(x) = x^p + p\delta x$, is a ring homomorphism. Note that $\delta(xy) = x^p\delta y + \phi(y)\delta x = y^p \delta x + \phi(x)\delta y$. Also δ and ϕ commute. If A is p-torsion free then δ is, of course, uniquely determined by ϕ; also

$$\delta(x_1 + \dots + x_m) = \delta x_1 + \dots + \delta x_m + C_p(x_1, \dots, x_m), \tag{2.1}$$

where

$$C_p(X_1,\dots,X_m) := p^{-1}(\sum_{i=1}^m X_i^p - (\sum_{i=1}^m X_i)^p) \in \mathbb{Z}[X_1,\dots,X_m].$$

Now the ring $R = \widehat{\mathbb{Z}_p^{ur}}$ has a unique p-derivation defined by $\delta x = (\phi(x) - x^p)/p$ where $\phi : R \to R$ is the unique ring automorphism lifting the p-power Frobenius on R/pR. Let x be a variable (or more generally an N-tuple of variables $x_1, \dots, x_N$.) We consider the *δ-polynomial ring* $R\{x\} = R[x, x', x'', \dots]$; this is the polynomial ring in variables $x, x', x'', \dots, x^{(n)}, \dots$, where $x', x'', \dots$ are variables (or N-tuples of variables), equipped with the unique p-derivation $\delta : R\{x\} \to R\{x\}$ such that $\delta x = x'$, $\delta x' = x''$, etc. For X a scheme of finite type over R one defines the p-jet spaces $J^n(X)$, $n \geq 0$ [3]. The latter are p-adic formal schemes over R fitting into a projective system

$$\dots \to J^n(X) \to J^{n-1}(X) \to \dots \to J^0(X) = \widehat{X}.$$

Note that $X \mapsto J^n(X)$ are functors commuting with open immersions and more generally with étale maps in the sense that if $X \to Y$ is étale then $J^n(X) \simeq J^n(Y) \times_Y X$ in the category of p-adic formal schemes. If $X = Spec\ R[x]/(f)$ for a tuple of variables x and a tuple of polynomials f and then

$$J^n(X) = Spf\ R[x, x', \dots, x^{(n)}]\widehat{\ }/(f, \delta f, \dots, \delta^n f).$$

In particular if $Y \to X$ is a closed immersion so is $J^n(Y) \to J^n(X)$ for all n. Moreover J^n commutes with fiber products: $J^n(Y \times_X Z) \simeq J^n(Y) \times_{J^n(X)}$

$J^n(Z)$. The rings $\mathcal{O}^n(X) := \mathcal{O}(J^n(X))$ form an inductive system, the p-derivation δ on $R\{x\}$ induces operators $\delta : \mathcal{O}^n(X) \to \mathcal{O}^{n+1}(X)$, and the direct limit of these δ's induces a p-derivation δ on the direct limit $\mathcal{O}^\infty(X)$ of the rings $\mathcal{O}^n(X)$. The following universality property holds. Assume for simplicity X is affine. Then any R-algebra homomorphism of $\mathcal{O}(X)$ into a p-adically complete ring B equipped with a p-derivation δ is induced by a unique R-algebra homomorphism $\mathcal{O}^\infty(X) \to B$ that commutes with δ.

3. Filtrations

In this section we will introduce and study some basic filtrations, especially on rings equipped with p-derivations. In the next section we will specialize to the case when the ring in question is the ring $R\{x\}$ of δ-polynomials.

Let A be a ring which for simplicity we assume p-torsion free and let I be an ideal in A. For any integer $\nu \geq 0$ we denote by $I^{[p^\nu]}$ the ideal generated by all the elements of the form $p^i f^{p^j}$ with $f \in I$, $i, j \geq 0$, $i + j = \nu$. (N.B. Sometimes the superscript [ ] is used to denote divided powers of ideals; our use of this superscript here has nothing to do with divided powers but rather it generalizes the notation used for Frobenius powers of ideals in characteristic p.) In particular $I^{[1]} = I$. Also note that $I^{[p^\nu]} \subset I(pA + I)^\nu$, where J^ν is, as usual, the ν-th power of an ideal J.

Lemma 3.1.
1) $I^{[p^{\nu+1}]} \subset I^{[p^\nu]}$.
2) If $f \in I^{[p^\nu]}$ then $pf \in I^{[p^{\nu+1}]}$.
3) If $f \in I^{[p^\nu]}$ then $f^p \in I^{[p^{\nu+1}]}$.
4) If I is generated by a family $\{f_s; s \in S\}$ then $I^{[p^\nu]}$ is generated by the family $\{p^i f_s^{p^j}; s \in S, i, j \geq 0, i + j = \nu\}$.

Proof. Assertions 1 and 2 are clear. For assertion 3 if $f = \sum_{s=1}^N p^{i_s} f_s^{p^{j_s}} g_s$ with $f_s \in I$, $g_s \in A$, and $i_s + j_s = \nu$ for all s then

$$f^p \in \sum_{s=1}^N (p^{i_s} f_s^{p^{j_s}} g_s)^p + pC_p(p^{i_1} f_1^{p^{j_1}} g_1, ..., p^{i_N} f_N^{p^{j_N}} g_N) \subset I^{[p^{\nu+1}]}. \tag{3.1}$$

To check assertion 4 it is sufficient to prove that if $g \in I$ then g^{p^t} is in the ideal generated by the family $\{p^i f_s^{p^j}; s \in S, i, j \geq 0, i + j = t\}$. One proves this by induction on $t \geq 0$. The case $t = 0$ is clear. Now if the statement is true for $t = \nu$ and we set $f = g^{p^\nu}$ then we are done by equation (3.1). $\square$

In what follows we assume we are given a p-derivation $\delta : A \to A$.

Lemma 3.2. *Assume $\delta(I) \subset I$. Then:*
1) $\delta(I^{[p^\nu]}) \subset I^{[p^\nu]}$;
2) $\phi(I^{[p^\nu]}) \subset I^{[p^{\nu+1}]}$.

Proof. First, for any $f \in A$, we have the following computation:

$$\begin{array}{rcl} \delta(f^{p^\nu}) & = & \frac{1}{p}(\phi(f^{p^\nu}) - f^{p^{\nu+1}}) \\ & = & \frac{1}{p}((f^p + p\delta f)^{p^\nu} - f^{p^{\nu+1}}) \\ & = & p^\nu f^{p(p^\nu - 1)}\delta f + p^{\nu+1}(\delta f)^2 P(f, \delta f) \end{array} \tag{3.2}$$

where P is a polynomial with $\mathbb{Z}$-coefficients; indeed this is because for $2 \leq m \leq p^\nu$ (and since p is odd) we have

$$p^{\nu+1} \mid \left(\begin{array}{c} p^\nu \\ m \end{array} \right) p^{m-1}.$$

In particular if $f \in I$ then $\delta(f^{p^\nu}) \in p^\nu I \subset I^{[p^\nu]}$.
Let's prove assertion 1. In view of the equation (2.1) it is enough to note that for $i + j = \nu$, $f \in I$, $g \in A$ we have $\delta(p^i f^{p^j} g) \in I^{[p^\nu]}$. Now

$$\begin{array}{rcl} \delta(p^i f^{p^j} g) & = & \delta(p^i) f^{p^{j+1}} g^p + p^i \delta(f^{p^j} g) \\ & = & \delta(p^i) f^{p^{j+1}} g^p + p^i(\delta(f^{p^j}) g^p + f^{p^{j+1}} \delta g + p(\delta(f^{p^j}))(\delta g)) \\ & \in & I^{[p^\nu]}, \end{array}$$

by Lemma 3.1 and because $\delta(p^i)$ is either 0 or in $p^{i-1}A$ according as $i = 0$ or $i \geq 1$.
To prove assertion 2 note that if $f \in I^{[p^\nu]}$ then $\phi(f) = f^p + p\delta f \in I^{[p^{\nu+1}]}$ by Lemma 3.1. □
In what follows we assume we are given, in addition, a filtration on A

$$A^0 \subset A^1 \subset A^2 \subset ... \subset A^n \subset ... \subset A,$$

by subrings A^n such that $\delta A^n \subset A^{n+1}$ for all $n \geq 0$. Then we define a new filtration by subrings

$$A^{\{0\}} \subset A^{\{1\}} \subset A^{\{2\}} \subset ... \subset A^{\{n\}} \subset ... \subset A, \tag{3.3}$$

$$A^{\{n\}} := \sum_{s=0}^{\infty} p^s A^{n+s} = A^n + pA^{n+1} + p^2 A^{n+2} + ...$$

Lemma 3.3.
1) $pA^{\{n+1\}} \subset A^{\{n\}}$*;*
2) $\delta(A^{\{n\}}) \subset A^{\{n+1\}}$*;*
3) $\phi(A^{\{n\}}) \subset A^{\{n\}}$.

Proof. A trivial exercise. □

We will also need the following general:

Lemma 3.4. *For any* $f, g \in A^0$ *we have the following equality of ideals in* A^n*:*

$$(f - g, \delta(f - g), ..., \delta^n(f - g)) = (f - g, \delta f - \delta g, ..., \delta^n f - \delta^n g).$$

Proof. Induction on n. The induction step follows from the congruence

$$\begin{array}{rcl} \delta(\delta^{n-1}f-\delta^{n-1}g) & - & (\delta^n f-\delta^n g)= \\ & = & C_p(\delta^{n-1}f,-\delta^{n-1}g) \\ & \equiv & C_p(\delta^{n-1}g,-\delta^{n-1}g) \quad \bmod \quad \delta^{n-1}f-\delta^{n-1}g \\ & = & 0. \end{array}$$

□

4. p-jets of p-isogenies of $\mathbb{G}_m$

In this section we specialize the discussion of the previous section to the case when

$$A=R\{x\},\ A^n=R[x,x',...,x^{(n)}],\ I=(x',x'',...). \tag{4.1}$$

So in this case, explicitly,

$$A^{\{n\}}=R[x,x',...,x^{(n)}]+pR[x,x',...,x^{(n+1)}]+p^2R[x,x',...,x^{(n+2)}]+...,$$

while $I^{[p^\nu]}$ is the ideal of $R\{x\}$ generated by all δ-polynomials of the form $p^i(x^{(s)})^{p^j}$, with $s\geq 1$, $i,j\geq 0$, $i+j=\nu$; cf. assertion 4 in Lemma 3.1.

We start by proving Theorem 1.1 in the Introduction.

Proof of Theorem 1.1. First note that for $n\leq \nu+1$ we have $\phi^{n-1}(x')\in I^{[p^{n-1}]}$ by Lemma 3.2 and hence

$$p^{\nu-n+1}x^{p^n(p^\nu-1)}\phi^{n-1}(x')\in I^{[p^\nu]}, \tag{4.2}$$

by Lemma 3.1. Similarly, for $n\geq \nu+2$, we have

$$x^{p^n(p^\nu-1)}\phi^\nu(x^{(n-\nu)})\in I^{[p^\nu]}, \tag{4.3}$$

by Lemma 3.2. We also claim that

$$\delta^n(x^{p^\nu})\in I^{[p^\nu]}. \tag{4.4}$$

To check (4.4) it is enough, by Lemma 3.2, to check that $\delta(x^{p^\nu})\in I^{[p^\nu]}$; this however follows from equation (3.2). In view of (4.2), (4.3), (4.4), in order to prove our theorem it is enough to prove that

$$\delta^n(x^{p^\nu})\in \begin{cases} p^{\nu-n+1}x^{p^n(p^\nu-1)}\phi^{n-1}(x')+p^{\nu-n+2}A^{\{1\}}, & \text{if } n\leq \nu+1 \\ x^{p^n(p^\nu-1)}\phi^\nu(x^{(n-\nu)})+A^{\{n-\nu-1\}}, & \text{if } n\geq \nu+2. \end{cases}$$

We fix ν and proceed by induction on $n\geq 1$. For $n=1$ we are done by (3.2). Next assume the theorem is true for n and we prove it for $n+1$.
Assume first $n\leq \nu+1$. By Lemma 3.3, $\phi^{n-1}(x')\in A^{\{1\}}$. So we have

$$\begin{array}{rcl} \delta^{n+1}(x^{p^\nu}) & \in & \delta(p^{\nu-n+1}x^{p^n(p^\nu-1)}\phi^{n-1}(x'))+\delta(p^{\nu-n+2}A^{\{1\}}) \\ & & +C_p(p^{\nu-n+1}A^{\{1\}},p^{\nu-n+2}A^{\{1\}}). \end{array}$$

Clearly the last term in the last equation is in $p^{\nu-n+1}A^{\{1\}}$. Also, by Lemma 3.3:

$$\begin{array}{rcl} \delta(p^{\nu-n+2}A^{\{1\}}) & \subset & \delta(p^{\nu-n+2})A^{\{1\}}+p^{\nu-n+2}\delta(A^{\{1\}}) \\ & \subset & p^{\nu-n+1}A^{\{1\}}+p^{\nu-n+2}A^{\{2\}} \\ & \subset & p^{\nu-n+1}A^{\{1\}}. \end{array}$$

Now for $n \leq \nu$ we have

$$\delta(p^{\nu-n+1})=p^{\nu-n}-p^{p(\nu-n+1)-1}\in p^{\nu-n}+p^{\nu-n+1}\mathbb{Z}$$

hence:

$$\begin{array}{rcl} \delta(p^{\nu-n+1}x^{p^n(p^\nu-1)}\phi^{n-1}(x')) & = & \delta(p^{\nu-n+1})x^{p^{n+1}(p^\nu-1)}(\phi^{n-1}(x'))^p \\ & & +p^{\nu-n+1}\delta(x^{p^n(p^\nu-1)}\phi^{n-1}(x')) \\ & \in & p^{\nu-n}x^{p^{n+1}(p^\nu-1)}\phi^{n-1}((x')^p)+p^{\nu-n+1}A^{\{1\}} \\ & & +p^{\nu-n+1}\delta(x^{p^n(p^\nu-1)})(\phi^{n-1}(x'))^p \\ & & +p^{\nu-n+1}\phi(x^{p^n(p^\nu-1)})\delta(\phi^{n-1}(x')) \\ & \subset & p^{\nu-n}x^{p^{n+1}(p^\nu-1)}\phi^{n-1}((x')^p) \\ & & +p^{\nu-n+1}A^{\{1\}} \\ & & +p^{\nu-n}(x^{p^{n+1}(p^\nu-1)}+pA^1)(\phi^{n-1}(px'')) \\ & \subset & p^{\nu-n}x^{p^{n+1}(p^\nu-1)}\phi^n(x')+p^{\nu-n+1}A^{\{1\}} \end{array}$$

because $\delta\circ\phi^{n-1}=\phi^{n-1}\circ\delta$, $(x')^p+px''=\phi(x')$, and

$$p^{\nu-n}\cdot pA^1\cdot(\phi^{n-1}(px''))\subset p^{\nu-n+1}\cdot A^1\cdot pA^{\{2\}}\subset p^{\nu-n+1}A^{\{1\}}.$$

So for $n\leq\nu$ we get

$$\delta^{n+1}(x^{p^\nu})=p^{\nu-n}x^{p^{n+1}(p^\nu-1)}\phi^n(x')+p^{\nu-n+1}A^{\{1\}},$$

which ends the induction step in case $n\leq\nu$.
For $n=\nu+1$ we get

$$\begin{array}{rcl} \delta(p^{\nu-n+1}x^{p^n(p^\nu-1)}\phi^{n-1}(x')) & = & \delta(x^{p^n(p^\nu-1)}\phi^{n-1}(x')) \\ & = & \delta(x^{p^n(p^\nu-1)})(\phi^{n-1}(x'))^p \\ & & +\phi(x^{p^n(p^\nu-1)})\delta(\phi^{n-1}(x')) \\ & \in & A^{\{1\}}+(x^{p^{n+1}(p^\nu-1)}+pA^1)(\phi^{n-1}(x'')) \\ & = & x^{p^{n+1}(p^\nu-1)}\phi^{n-1}(x'')+A^{\{1\}}, \end{array}$$

by Lemma 3.3. Hence

$$\delta^{n+1}(x^{p^\nu})=x^{p^{n+1}(p^\nu-1)}\phi^\nu(x^{(n+1-\nu)})+A^{\{n-\nu\}},$$

which ends the induction step in case $n=\nu+1$.
Assume now $n\geq\nu+2$; then, by Lemma 3.3,

$$\begin{array}{rcl} \delta^{n+1}(x^{p^\nu}) & = & \delta(x^{p^n(p^\nu-1)}\phi^\nu(x^{(n-\nu)}))+\delta(A^{\{n-\nu-1\}}) \\ & & +C_p(A^{\{n-\nu\}},A^{\{n-\nu-1\}}) \\ & \in & \delta(x^{p^n(p^\nu-1)}\phi^\nu(x^{(n-\nu)}))+A^{\{n-\nu\}} \\ & = & x^{p^{n+1}(p^\nu-1)}\delta(\phi^\nu(x^{(n-\nu)})) \\ & & +\phi^{\nu+1}(x^{(n-\nu)})\delta(x^{p^n(p^\nu-1)})+A^{\{n-\nu\}} \\ & = & x^{p^{n+1}(p^\nu-1)}\phi^\nu(x^{(n+1-\nu)})+A^{\{n-\nu\}}. \end{array}$$

This ends the induction step in case $n\geq\nu+2$. ∎

Corollary 4.1.

$$\delta^n(x^{p^\nu}) \in \begin{cases} A^{\{0\}} \cap I^{[p^\nu]} & \text{if } n \leq \nu, \\ A^{\{n-\nu\}} \cap I^{[p^\nu]} & \text{if } n \geq \nu+1. \end{cases}$$

The following will also be useful later.

Lemma 4.2.
1) $\delta^n(x^p) \in R[x^p, x', ..., x^{(n)}]$ *for* $n \geq 0$.
2) $\delta^n(x_1 x_2) \in R[x_1^p, x_2^p, x_1', x_2', ..., x_1^{(n)}, x_2^{(n)}]$.

Proof. Trivial induction on n. □

5. p-jets of μ_{p^ν}

Start again with the multiplicative group $\mathbb{G}_m$ and the isogeny $[p^\nu]_{\mathbb{G}_m} : \mathbb{G}_m \to \mathbb{G}_m$. Let

$\mu_{p^\nu} = \mathbb{G}_m[p^\nu] := Ker([p^\nu]_{\mathbb{G}_m}) = Spec\, R[x, x^{-1}]/(x^{p^\nu} - 1) = Spec\, R[x]/(x^{p^\nu} - 1)$

be the kernel of $[p^\nu]_{\mathbb{G}_m}$. More generally, (for the purpose of looking later at p-divisible groups of elliptic curves) we consider, for any $a \in R^\times$, the finite flat scheme

$$\mu_{p^\nu}^a := Spec\ R[x]/(x^{p^\nu} - a).$$

Its functor of points is given by $\mu_{p^\nu}^a(S) = \{s \in S; s^{p^\nu} = a\}$ for any R-algebra S. Then $\mu_{p^\nu}^a$ has a natural structure of μ_{p^ν}-torsor. More generally, for any $a, b \in R^\times$ we have a natural morphism

$$\mu_{p^\nu}^a \times \mu_{p^\nu}^b \xrightarrow{can} \mu_{p^\nu}^{ab}$$

given on S-points by $(s,t) \mapsto st$. We also have a natural isomorphism

$$\mu_{p^\nu}^{a^{p^\nu} b} \xrightarrow{can} \mu_{p^\nu}^b$$

given on points by $s \mapsto s/a$.
Consider the group $U_m = 1 + p^m R = U_1^{p^{m-1}}$.
So if $a \in U_{\nu+1}$ then $a = b^{p^\nu}$, $b \in U_1$, so division by b gives an isomorphism

$$\mu_{p^\nu}^a \simeq \mu_{p^\nu}.$$

Finally the system $(\mu_{p^\nu}; \nu \geq 1)$ is a p-divisible group with embeddings $\mu_{p^\nu} \subset \mu_{p^{\nu+1}}$ given by the inclusions on points. More generally for any $a \in R^\times$ and any $\nu_0 \geq 1$, the schemes $(\mu_{p^\nu}^{a^{p^{\nu-\nu_0}}}; \nu \geq \nu_0)$ form an inductive system with embeddings

$$\mu_{p^{\nu_0}}^a \subset \mu_{p^{\nu_0+1}}^{a^p} \subset ... \subset \mu_{p^\nu}^{a^{p^{\nu-\nu_0}}} \subset \mu_{p^{\nu+1}}^{a^{p^{\nu+1-\nu_0}}} \subset ... \tag{5.1}$$

given by the inclusions on points. Note that if $a \in U_{\nu_0+1}$ then we can write $a = b^{p^{\nu_0}}$ and hence division by b gives an isomorphism between the inductive system (5.1) and the inductive system

$$\mu_{p^{\nu_0}} \subset \mu_{p^{\nu_0+1}} \subset ... \subset \mu_{p^\nu} \subset \mu_{p^{\nu+1}} \subset ... \tag{5.2}$$

Recall that $J^n(\mathbb{G}_m) = Spf\ R[x,x^{-1},x',...,x^{(n)}]\hat{}$ and that $[p^\nu]_{J^n(\mathbb{G}_m)}$: $J^n(\mathbb{G}_m) \to J^n(\mathbb{G}_m)$ is given at the level of rings by $x \mapsto x^{p^\nu}$, $x' \mapsto \delta(x^{p^\nu})$, etc. By the commutation of J^n with fiber products it follows that

$$J^n(\mu_{p^\nu}) = Ker(J^n([p^\nu]_{\mathbb{G}_m}) = Ker([p^\nu]_{J^n(\mathbb{G}_m)}) =: J^n(\mathbb{G}_m)[p^\nu].$$

More generally, if $a \in R^\times$, and if we still denote by $a : Spec\ R \to \mathbb{G}_m$ the point defined by $x \mapsto a$ then

$$J^n(\mu^a_{p^\nu}) = J^n([p^\nu]^{-1}_{\mathbb{G}_m}(a)) = (J^n([p^\nu]_{\mathbb{G}_m})^{-1}(J^n(a)) = ([p^\nu]_{J^n(\mathbb{G}_m)})^{-1}(J^n(a))$$

where $J^n(a) : Spec\ R \to J^n(\mathbb{G}_m)$ is given, at the level of rings, by

$$x \mapsto a,\ x' \mapsto \delta a,\ ..., x^{(n)} \mapsto \delta^n a.$$

It follows that:

Proposition 5.1.

$$\mathcal{O}^n(\mu^a_{p^\nu}) = \frac{R[x,x',...,x^{(n)}]\hat{}}{(x^{p^\nu} - a, \delta(x^{p^\nu}) - \delta a, ..., \delta^n(x^{p^\nu}) - \delta^n a)}.$$

In particular

$$\mathcal{O}^n(\mu_{p^\nu}) = \frac{R[x,x',...,x^{(n)}]\hat{}}{(x^{p^\nu} - 1, \delta(x^{p^\nu}), ..., \delta^n(x^{p^\nu}))}.$$

Alternatively Proposition 5.1 follows from Lemma 3.4.

Remark 5.2. Let $J^n(\mu_{p^\nu})_1$ be the kernel of the projection $J^n(\mu_{p^\nu}) \to J^0(\mu_{p^\nu}) = \widehat{\mu_{p^\nu}}$ and write $\mathcal{O}^n(\mu_{p^\nu})_1 := \mathcal{O}(J^n(\mu_{p^\nu})_1)$. Since μ_{p^ν} has a lift of Frobenius $x \mapsto x^p$ in the category of group schemes we get an isomorphism

$$\mathcal{O}^n(\mu_{p^\nu}) \simeq \mathcal{O}(\mu_{p^\nu})\widehat{\otimes}\mathcal{O}^n(\mu_{p^\nu})_1$$

compatible with the group laws. Equivalently we have

$$J^n(\mu_{p^\nu}) = \widehat{\mu_{p^\nu}} \times J^n(\mu_{p^\nu})_1$$

as groups in the category of formal p-adic schemes over R.

Proposition 5.3. *For all $n \geq 1$ we have*

$$\lim_{\substack{\leftarrow \\ \nu}} \mathcal{O}^n(\mu_{p^\nu})_1 = R[x', ..., x^{(n)}]\hat{}.$$

Proof. By Proposition 5.1

$$\mathcal{O}^n(\mu_{p^\nu})_1 = \frac{R[x',...,x^{(n)}]\hat{}}{(\delta(x^{p^\nu})_{|x=1}, ..., \delta^n(x^{p^\nu})_{|x=1})}.$$

Since, by Theorem 1.1 the denominator in the last equation is in $(p^{\nu-n+1})$ we are done by the following well known fact (whose proof we recall). $\square$

Lemma 5.4. *If A is a Noetherian ring, I is an ideal, A is I-adically complete, and (L_n) is a descending sequence of ideals such that $L_n \subset I^n$ then*

$$A = \lim_{\leftarrow} A/L_n.$$

Proof. The map from A to the projective limit is clearly injective. It is surjective because if $f_n \in A$, $f_{n+1} - f_n \in L_n$ then $f_{n+1} - f_n \in I^n$ hence there exists $f \in A$ such that $f - f_n \in I^n$. Now fix m; since for $n \geq m$, $f - f_m = (f - f_n) + (f_n - f_m) \in I^n + L_m$ and (by [13], Theorems 8.2 and 8.14) $\cap_{n\geq 1}(I^n + L_m) = L_m$ we get $f - f_m \in L_m$ $\square$.

According to our general notation (Equations 1.1 and 1.2) we next recall the rings

$$\overline{\mathcal{O}^n(\mu^a_{p^\nu})}, \quad \widetilde{\mathcal{O}^n(\mu^a_{p^\nu})}.$$

Also recall we set $U_m = 1 + p^m R = U_1^{p^{m-1}}$, $m \geq 1$.

Proposition 5.5. *Let $n, \nu \geq 1$ and $a \in U_1$.*
1) If $a \notin U_{\nu+1}$ then $\widetilde{\mathcal{O}^n(\mu^a_{p^\nu})} = 0$.
2) If $a \in U_{\nu+1}$ then

$$\widetilde{\mathcal{O}^n(\mu^a_{p^\nu})} \simeq \widetilde{\mathcal{O}^n(\mu_{p^\nu})} \simeq \frac{k[x, x', x'', ..., x^{(n)}]}{((x-1)^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n)})^{p^\nu})}. \tag{5.3}$$

$$\overline{\mathcal{O}^n(\mu^a_{p^\nu})} \simeq \overline{\mathcal{O}^n(\mu_{p^\nu})} \simeq \frac{k[x, x', x'', ..., x^{(n)}]}{(x^{p^\nu} - 1)} \quad \textit{if } n \leq \nu, \tag{5.4}$$

$$\overline{\mathcal{O}^n(\mu^a_{p^\nu})} \simeq \overline{\mathcal{O}^n(\mu_{p^\nu})} \simeq \frac{k[x, x', x'', ..., x^{(n)}]}{(x^{p^\nu} - 1, (x')^{p^\nu}, ..., (x^{(n-\nu)})^{p^\nu})} \quad \textit{if } n \geq \nu + 1. \tag{5.5}$$

Proof. To prove assertion 1 let $a \in U_m \backslash U_{m+1}$, $1 \leq m \leq \nu$. Then a simple induction shows that $\delta^m a \in R^\times$ hence, by Corollary 1.3, the reduction mod p of $\delta^m(x^{p^\nu}) - \delta^m a$ is in $k^\times$. By Proposition 5.1 $\overline{\mathcal{O}^N(\mu^a_{p^\nu})} = 0$ for all $N \geq m$ and hence $\widetilde{\mathcal{O}^n(\mu^a_{p^\nu})} = 0$ for all $n \geq 1$.
To prove assertion 2 note that the equalities (5.4) and (5.5) follow from Corollary 1.3 and Proposition 5.1; in particular we have

$$\lim_{\substack{\longrightarrow \\ m}} \overline{\mathcal{O}^m(\mu_{p^\nu})} = \frac{k[x, x', x'', ...]}{(x^{p^\nu} - 1, (x')^{p^\nu}, (x'')^{p^\nu}, ...)}.$$

Now (5.3) follows from the fact that the intersection

$$k[x, x', ..., x^{(n)}] \cap (x^{p^\nu} - 1, (x')^{p^\nu}, (x'')^{p^\nu}, ...)$$

in the ring $k[x, x', x'', ...]$ equals the ideal

$$(x^{p^\nu} - 1, (x')^{p^\nu}, ..., (x^{(n)})^{p^\nu}).$$

$\square$

By the above Proposition we get:

Corollary 5.6. *Let $n, \nu_0 \geq 1$, $a \in U_1$. Then*

$$\lim_{\substack{\longleftarrow \\ \nu}} \widetilde{\mathcal{O}^n(\mu^{a^{p^{\nu-\nu_0}}}_{p^\nu})} = \begin{cases} 0 & \textit{if } a \notin U_{\nu_0+1} \\ k[[x-1, x', ..., x^{(n)}]] & \textit{if } a \in U_{\nu_0+1} \end{cases} \tag{5.6}$$

We also remark the following:

Proposition 5.7. *Assume $n, \nu \geq 1$. Then*
1) $\mathcal{O}^n(\mu_{p^\nu})$ is not a finite R-algebra.
2) $\mathcal{O}^n(\mu_{p^\nu})$ is not a flat R-algebra.

Proof. If $\mathcal{O}^n(\mu_{p^\nu})$ is a finite R-algebra then $\overline{\mathcal{O}^n(\mu_{p^\nu})}$ is a finite k-algebra which is not the case, cf. equations (5.4) and (5.5). If $\mathcal{O}^n(\mu_{p^\nu})$ is a flat R-algebra then it is torsion free. Since, by equation (3.2), $\delta(x^{p^\nu}) \in p^\nu x^{p(p^\nu-1)}x' + p^{\nu+1}A^1$ it follows that an element in $x'+pA^1$ is zero in $\mathcal{O}^n(\mu_{p^\nu})$ hence x' is zero in $\overline{\mathcal{O}^n(\mu_{p^\nu})}$ hence in $\widetilde{\mathcal{O}^n(\mu_{p^\nu})}$. Hence x' is in the denominator of the ring in equation (5.3), a contradiction. □

Remark 5.8. The author is indebted to A. Saha for pointing out assertion 2 in Proposition 5.7 above.

Remark 5.9. We end this section by providing an alternative argument for Corollary 1.5, hence of Proposition 5.5 in case $a = 1$; the author is indebted to the referee for this argument.
We start by recalling that for finitely generated R-algebras B and k-algebras C there are isomorphisms

$$Hom_{k-\text{alg}}(J^n(B), C) \simeq Hom_{R-\text{alg}}(B, W_n(C))$$

functorial in both B and C and compatible with varying n. (Here $W_n(C) = (R^{n+1}, +, \times)$ is the ring of p-typical Witt vectors of length $n+1$.) This follows from the theory in [1]; cf. Section 3.4 of that paper. (The indexing of rings of Witt vectors is also taken from [1] and is not the classical one: the above W_n are usually denoted by W_{n+1}.) Using the isomorphism above Corollary 1.5 is easily seen to be equivalent to the following statement.

Proposition 5.10. *For any k-algebra C and any Witt vector $x = (x_0, ..., x_n) \in W_n(C)$ we have*

$$x^{p^\nu} = 1 \Longleftrightarrow (x_0 - 1)^{p^\nu} = x_1^{p^\nu} = ... = x_{n-\nu}^{p^\nu} = 0$$

Here ... has the obvious meaning if $\nu \geq n$.

Proof. By multiplying x with the inverse of the Teichmüller lift $(x_0, 0, ..., 0)$ of x_0 one may reduce to the case when $x_0 = 1$. Assume this from now on. Then by induction it is enough to show that for all $0 \leq i \leq n - \nu - 1$ and under the assumption $x_1^{p^\nu} = ... = x_i^{p^\nu} = 0$ we have

$$x^{p^\nu} = 1 \Longleftrightarrow x_{i+1}^{p^\nu} = 0$$

To show the latter we may further assume that $i = n - \nu - 1$. Now write $x = 1 + V(z)$ where V is the Verschiebung and $z = (x_1, ..., x_n)$. Then we have

$$x^{p^\nu} = (1 + V(z))^{p^\nu} = 1 + p^\nu V(z) + \sum_{j=2}^{p^\nu} \binom{p}{j} (V(z))^j. \tag{5.7}$$

Since C has characteristic p, if F is the Frobenius, we have $FV = VF = p$ hence

$$\begin{array}{lrcl}
(5.8) & p^\nu V(z) & = & V^{\nu+1}F^\nu(z) \\
& & = & V^{\nu+1}(x_1^{p^\nu},...,x_{n-\nu}^{p^\nu}) \\
& & = & (0,...,0,x_1^{p^\nu},...,x_{n-\nu}^{p^\nu}) \\
& & = & (0,...,0,x_{n-\nu}^{p^\nu}).
\end{array}$$

By Equations 5.7 and 5.8 we are left to prove that for all $j \geq 2$,

$$(5.9) \qquad \left(\begin{array}{c} p \\ j \end{array} \right) (V(z))^j = 0 \in W_n(C).$$

Let $r = \text{ord}_p \left(\begin{array}{c} p \\ j \end{array} \right)$. Then Equation 5.9 is equivalent (due to the general identity $V(a)V(b) = pV(ab)$) to

(5.10)

$$0 = p^r(V(z))^j = p^{r+j-1}V(z^j) = V^{r+j}F^{r+j-1}(z^j) = V^{r+j}(F^{r+j-1}(z)^j).$$

It is therefore enough to show that

$$0 = F^{r+j-1}(z) = (x_1^{p^{r+j-1}},...,x_{n-r-j+1}^{p^{r+j-1}}).$$

Since we know that $x_1^{p^\nu} = ... = x_{n-\nu-1}^{p^\nu} = 0$, it is enough to show that $\nu + 2 \leq r + j$ or, equivalently,

$$\text{ord}_p \left(\begin{array}{c} p^\nu \\ j \end{array} \right) \geq \nu - j + 2$$

for $j \geq 2$, which is true (for $p \geq 3$) for elementary reasons. $\square$

6. p-jets of the irreducible components of μ_{p^ν}

Next note that μ_{p^ν} is connected and has $\nu + 1$ irreducible components:

$$\mu_{p^\nu} = \bigcup_{i=0}^{\nu} \mu_{p^\nu,i}, \quad \mu_{p^\nu,i} := Spec\ R[\zeta_{p^i}],$$

where ζ_{p^i} is a primitive p-root of unity. So $\zeta_1 = 1$, $R[\zeta_1] = R = R[x]/(x-1)$, and

$$R[\zeta_{p^i}] = R[x]/(\Phi_{p^i}(x)), \quad \Phi_{p^i}(x) := \frac{x^{p^i} - 1}{x^{p^{i-1}} - 1}, \quad i \geq 1.$$

The scheme theoretic intersection of these components is

$$Spec\ R[x]/(x-1,p) = Spec\ k.$$

In deep contrast with Proposition 5.5 the p-jets of these components are completely uninteresting:

Proposition 6.1.
1) $\mathcal{O}^n(\mu_{p^\nu,0}) = R$ *for* $n \geq 1$*;*
2) $\mathcal{O}^n(\mu_{p^\nu,i}) = 0$ *for* $i \geq 1$ *and* $n \geq 1$.

Proof. The first equality is clear. The second follows from the fact that $\Phi_{p^i}(x+1)$ is an Eisenstein polynomial plus the following general fact: $\square$

Proposition 6.2. *Let $f(x) = x^e + a_1 x^{e-1} + ... + a_{e-1}x + a_e \in R[x]$ be an Eisentein polynomial (i.e. $e \geq 2$, $a_1, ..., a_e \in pR$, $a_e \notin p^2R$) and let $X = Spec\ R[x]/(f(x))$. Then $\mathcal{O}^n(X) = 0$ for $n \geq 1$.*

Proof. It is enough to show that $\delta f(x)$ is invertible in $\mathcal{O}^1(X) \otimes k$. Now we have:

$$\begin{array}{rcl} \delta f(x) & = & \delta(x^e) + \delta(a_1 x^{e-1}) + ... + \delta(a_{e-1}x) + \delta a_e + C_p(x^e, a_1 x^{e-1}, ..., a_e) \\ & \equiv & e x^{p(e-1)} x' + x^{p(e-1)}(\delta a_1) + ... + x^p(\delta a_{e-1}) + \delta a_e \quad mod \quad p. \end{array}$$

Since the image of x in $\mathcal{O}^1(X) \otimes k$ is nilpotent and the image of δa_e in the same ring is invertible it follows that the image of $\delta f(x)$ in this ring is invertible which ends the proof. $\square$

7. p-jets of $E[p^\nu]$ for ordinary elliptic curves

We start with a review of extensions of $p^{-\nu}\mathbb{Z}/\mathbb{Z}$ by μ_{p^ν}. For any group (respectively group scheme) G we denote by $G[N]$ the kernel of the multiplication by N map. For a finite group Γ we continue to denote by Γ the étale group scheme over R attached to Γ; so for any connected R-algebra S, $\Gamma(S) = \Gamma$. In particular we have the connected R-group scheme $\mu_{p^\nu} = \mathbb{G}_m[p^\nu]$. Also one can consider the étale R-group scheme $p^{-\nu}\mathbb{Z}/\mathbb{Z}$. Let $R_m = R/p^m R$, $m \geq 1$. We also view, when appropriate, μ_{p^ν} and $p^{-\nu}\mathbb{Z}/\mathbb{Z}$ as R_m-group schemes via base change. Then, by Kummer theory,

$$(7.1) \qquad \begin{array}{rcl} Ext^1_{R_m}(p^{-\nu}\mathbb{Z}/\mathbb{Z}, \mu_{p^\nu}) & \simeq & R_m^\times/(R_m^\times)^{p^\nu} \\ & \simeq & (1 + pR_m)/(1 + pR_m)^{p^\nu} \\ & \simeq & (1 + pR_m)/(1 + p^{\nu+1}R_m). \end{array}$$

We will need to recall the following explicit description of the above isomorphism. Let $q \in 1 + pR$. Consider the finite flat R-scheme

$$\Gamma^q_{p^\nu} = \coprod_{i=0}^{p^\nu - 1} \mu_{p^\nu}^{q^i}.$$

This is a group scheme with multiplication given by

$$\mu_{p^\nu}^{q^i} \times \mu_{p^\nu}^{q^j} \xrightarrow{can} \mu_{p^\nu}^{q^{i+j}} \xrightarrow{can} \mu_{p^\nu}^{q^l},$$

where $0 \leq l < p^\nu$, $i + j \equiv l$ mod p^ν. The functor of points of $\Gamma^q_{p^\nu}$ is given by

$$\Gamma^q_{p^\nu}(S) = \{(s, i); s \in S^\times, 0 \leq i < p^\nu, s^{p^\nu} = q^i\}$$

for any R-algebra S with connected spectrum; the multiplication on points is given by $(s, i) \cdot (t, j) = (st, i + j)$ if $i + j < p^\nu$ and $(s, i) \cdot (t, j) = (st/q, i + j - p^\nu)$ if $i + j \geq p^\nu$. We have an extension

$$(7.2) \qquad 0 \to \mu_{p^\nu} \to \Gamma^q_{p^\nu} \to p^{-\nu}\mathbb{Z}/\mathbb{Z} \to 0$$

(the second map being given on points by $(s, i) \mapsto \frac{i}{p^\nu} + \mathbb{Z}$). Then Kummer theory gives:

Lemma 7.1. *The isomorphism (7.1) is given by attaching to the class of $q \in 1 + pR$ in $(1 + pR_m)/(1 + p^{\nu+1}R_m)$ the class of the extension (7.2) in $Ext^1_{R_m}(p^{-\nu}\mathbb{Z}/\mathbb{Z}, \mu_{p^\nu})$.*

Note that the system $(\Gamma^q_{p^\nu}; \nu \geq 1)$ is a p-divisible group via the morphisms $\Gamma^q_{p^\nu} \to \Gamma^q_{p^{\nu+1}}$ given on points by $(s, i) \mapsto (s, pi)$ and given on schemes by the inclusions $\mu^{q^i}_{p^\nu} \subset \mu^{q^{pi}}_{p^{\nu+1}}$. The p-divisible group $(\Gamma^q_{p^\nu}; \nu \geq 1)$ is an extension of the p-divisible group $(p^{-\nu}\mathbb{Z}/\mathbb{Z}; \nu \geq 1)$ by the p-divisible group $(\mu_{p^\nu}; \nu \geq 1)$, where the latter are viewed as p-divisible groups with respect to the natural inclusions.

Next we consider an elliptic curve E/R. References for this are [14, 10]. Let $\overline{E}/k$ be its reduction mod p and let E^{for} be the formal group attached to E. (We use the superscript *for* rather than $\widehat{}$ because the latter is used in the present paper to denote p-adic completion). Let $E^{for}[p^\nu]$ be the kernel of the multiplication by p^ν on E^{for}, viewed as a finite flat group scheme over R. Assume in what follows that $\overline{E}$ is ordinary. Then

$$E^{for} \simeq \mathbb{G}^{for}_m; \tag{7.3}$$

we fix such an isomorphism. So we have induced isomorphisms $E^{for}[p^\nu] \simeq \mu_{p^\nu}$. Moreover we fix isomorphisms

$$\overline{E}(k)[p^\nu] \simeq \mathbb{Z}/p^\nu\mathbb{Z} \simeq p^{-\nu}\mathbb{Z}/\mathbb{Z}. \tag{7.4}$$

With the isomorphisms (7.3) and (7.4) fixed one defines the Serre-Tate parameter $q = q(E) \in 1 + pR$ of E as follows. The isomorphisms (7.4) define a basis (α_ν) of the Tate module $T_p\overline{E} = \lim_{\leftarrow} \overline{E}(k)[p^\nu]$, $\alpha_\nu \in \overline{E}(k)[p^\nu]$ a generator, $p\alpha_\nu = \alpha_{\nu-1}$. If $A_\nu \in E(R)$ lifts α_ν then one defines the Serre-Tate parameter $q(E) \in 1 + pR$ as the image of $\lim p^\nu A_\nu \in E^{for}(R)$ via the isomorphism $E^{for}(R) \simeq 1 + pR$ induced by (7.3); cf. [10], section 2. On the other hand with the isomorphisms (7.3) and (7.4) fixed there are induced exact sequences of finite flat group schemes over R:

$$0 \to \mu_{p^\nu} \to E[p^\nu] \to p^{-\nu}\mathbb{Z}/\mathbb{Z} \to 0. \tag{7.5}$$

Cf., say, [10]. Also by loc.cit. we have

Lemma 7.2. *The class of the extension (7.5) is the image of the Serre-Tate parameter $q(E) \in 1 + pR$ under the isomorphism (7.1).*

We conclude by Lemmas 7.1 and 7.2 that if $q = q(E)$ then $E[p^\nu]$ and $\Gamma^q_{p^\nu}$ are isomorphic as extensions over R_m for any m; the isomorphisms are compatible as m varies so we get the following:

Corollary 7.3. *$E[p^\nu]$ and $\Gamma^q_{p^\nu}$ are isomorphic as extensions over R for $q = q(E)$. In particular if $0 \leq i < p^\nu$ and $\theta = \frac{i}{p^\nu} + \mathbb{Z} \in p^{-\nu}\mathbb{Z}/\mathbb{Z}$ then the connected component $E[p^\nu]_\theta$ of $E[p^\nu]$ lying above θ is isomorphic to $\mu^{q^i}_{p^\nu}$. Consequently if* *we fix* ν_0 *and an index* $0 \leq i_0 < p^{\nu_0}$ *and if* $\theta = \frac{i_0}{p^{\nu_0}} + \mathbb{Z} \in p^{-\nu_0}\mathbb{Z}/\mathbb{Z}$ *then the inductive system*

$$E[p^{\nu_0}]_\theta \subset E[p^{\nu_0+1}]_\theta \subset E[p^{\nu_0+2}]_\theta \subset ... \subset E[p^\nu]_\theta \subset ...$$

identifies with the inductive system

$$\mu_{p^{\nu_0}}^{q^{i_0}} \subset \mu_{p^{\nu_0+1}}^{(q^{i_0})^p} \subset \mu_{p^{\nu_0+2}}^{(q^{i_0})^{p^2}} \subset ... \subset \mu_{p^\nu}^{(q^{i_0})^{p^{\nu-\nu_0}}} \subset ...$$

Putting together Proposition 5.5 and Corollary 7.3 (and making the change of variables $x \mapsto x+1$) we get:

PROPOSITION 7.4. *Let* E/R *be an elliptic curve with ordinary reduction and Serre-Tate parameter* $q = q(E) \in U_1$. *Let* $n \geq 1$, *let* $\theta \in \bigcup_{m \geq 1} p^{-m}\mathbb{Z}/\mathbb{Z}$, *and let* $\nu_0 \geq 1$ *be minimal with the property that* $\theta \in p^{-\nu_0}\mathbb{Z}/\mathbb{Z}$. *Let* $\nu \geq \nu_0$ *and let* $E[p^\nu]_\theta$ *be the connected component of* $E[p^\nu]$ *lying over* θ. *Then:*
1) If $q \notin U_{\nu_0+1}$ *and* $\theta \neq 0$ *then* $\mathcal{O}^n(\widetilde{E[p^\nu]_\theta}) = 0$.
2) If $q \in U_{\nu_0+1}$ *or* $\theta = 0$ *then*

$$\mathcal{O}^n(\widetilde{E[p^\nu]_\theta}) \simeq \frac{k[x, x', x'', ..., x^{(n)}]}{(x^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n)})^{p^\nu})}. \tag{7.6}$$

$$\overline{\mathcal{O}^n(E[p^\nu]_\theta)} \simeq \frac{k[x, x', x'', ..., x^{(n)}]}{(x^{p^\nu})} \quad \textit{if } n \leq \nu, \tag{7.7}$$

$$\overline{\mathcal{O}^n(E[p^\nu]_\theta)} \simeq \frac{k[x, x', x'', ..., x^{(n)}]}{(x^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n-\nu)})^{p^\nu})} \quad \textit{if } n \geq \nu + 1. \tag{7.8}$$

COROLLARY 7.5. *Let* $n, \nu_0 \geq 1$, $q \in U_1$. *Then*

$$\lim_{\overleftarrow{\nu}} \mathcal{O}^n(\widetilde{E[p^\nu]_\theta}) = \begin{cases} 0 & \textit{if } q \notin U_{\nu_0+1} \textit{ and } \theta \neq 0 \\ k[[x, x', ..., x^{(n-1)}]] & \textit{if } q \in U_{\nu_0+1} \textit{ or } \theta = 0. \end{cases} \tag{7.9}$$

Also Proposition 5.7 and Corollary 7.3 imply

COROLLARY 7.6. *Let* $n, \nu \geq 1$. *Then the map*

$$J^n([p^\nu]_E) = [p^\nu]_{J^n(E)} : J^n(E) \to J^n(E)$$

is neither finite not flat.

An analogue of Remark 1.4 should hold nevertheless in the elliptic case as well.

8. p-JETS OF $\mathcal{F}[p^\nu]$

Recall that a series $F(x) \in xR[[x]]$ without constant term is said to have finite height if $F \not\equiv 0 \bmod p$; if this is the case the height of F is defined as the largest integer $h \geq 0$ such that $F \in R[[x^{p^h}]] + pR[[x]]$.

Remark 8.1. The main example we have in mind here arises as follows. Consider a formal group law $\mathcal{F} \in R[[x_1, x_2]]$. By [14] the multiplication by p in $\mathcal{F}$ is given by a series $F(x) := [p]_{\mathcal{F}}(x)$ satisfying $F(x) \equiv px \bmod x^2$. The height of $\mathcal{F}$ is defined to be the height of $F(x)$; if the height is finite then it is ≥ 1. Not every series of height ≥ 1 which is $\equiv px \bmod x^2$ is the multiplication by p of a formal group law $\mathcal{F}$; indeed if $F(x) = [p]_{\mathcal{F}}$ has height h then one knows that the x-adic valuation of the reduction mod p of F in $k[[x]]$ is exactly p^h; cf. [14], p.127.

Let $F(x) \in xR[[x]]$ be a series of finite height $h \geq 1$ and let $F^{\circ\nu} = F \circ ... \circ F$ be the ν fold composition of F with itself for $\nu \geq 1$. Let ep^h be the x-adic valuation of the reduction mod p of F. (So if $F(x) = [p]_{\mathcal{F}}(x)$ for some formal group law $\mathcal{F}$ then $e = 1$.) By "Weierstrass preparation" (cf. [11], p. 130) $F^{\circ\nu} = U_\nu \cdot P_\nu$ where $U_\nu \in R[[x]]^\times$ and $P_\nu \in R[x]$ is monic of degree $e^\nu p^{h\nu}$, $P_\nu \equiv x^{e^\nu p^{h\nu}} \bmod p$. Consider the scheme:

$$X_\nu := Spec\ \frac{R[[x]]}{(F^{\circ\nu})} = Spec\ \frac{R[[x]]}{(P_\nu)} \simeq Spec\ \frac{R[x]}{(P_\nu)};$$

the latter isomorphism follows from "Euclid division" by P_ν in $R[[x]]$; cf. [11], p. 129. So X_ν is a finite flat scheme over R of degree $e^\nu p^{h\nu}$ and we have a natural sequence of closed immersions

$$X_1 \subset X_2 \subset ... \subset X_\nu \subset ... \tag{8.1}$$

Our aim in this section is to understand the rings $\mathcal{O}^n(X_\nu)$. Note that if $F(x) = [p]_{\mathcal{F}}(x)$ is the multiplication by p on some formal group law $\mathcal{F}$ then $X_\nu = \mathcal{F}[p^\nu]$, where the latter is the kernel of $[p^\nu]_{\mathcal{F}}$ on $\mathcal{F}$ and indeed the inductive system (8.1) coincides with the p-divisible group

$$\mathcal{F}[p] \subset \mathcal{F}[p^2] \subset ... \subset \mathcal{F}[p^\nu] \subset ...$$

of $\mathcal{F}$; cf. [15].

Remark 8.2. Recall (cf. [12], p. 480) that any formal group law $\mathcal{F}$ over R of height $h = 1$ is isomorphic to the multiplicative formal group law hence in particular $\mathcal{F}[p^\nu] \simeq \mu_{p^\nu}$. Hence our analysis in Section 5 applies to $\mathcal{O}^n(\mathcal{F}[p^\nu])$ in the height one case. We will consider in what follows the case of formal groups of arbitrary height ≥ 1. More generally we will treat the case of iterates of series of height ≥ 1 which are not necessarily coming from formal groups; so even for height 1 our analysis below will not be covered by Section 5.

To understand the rings $\mathcal{O}^n(X_\nu)$ we will first perform some computations in characteristic zero culminating with a proof of Theorem 1.7. Then we will reduce mod p the outcome of these computations.

We begin by noting that:

$$\begin{array}{lrcl} & \mathcal{O}^n(X_\nu) & = & R[x,x',...,x^{(n)}]\hat{}/(P_\nu,\delta P_\nu,...,\delta^n P_\nu) \\ (8.2) & & = & R[[x]][x',...,x^{(n)}]\hat{}/(P_\nu,\delta P_\nu,...,\delta^n P_\nu) \\ & & = & R[[x]][x',...,x^{(n)}]\hat{}/(F^{\circ\nu},\delta(F^{\circ\nu}),...,\delta^n(F^{\circ\nu})). \end{array}$$

So we will be concerned from now on with understanding the structure of the expressions $\delta^i(F^{\circ\nu})$. To do this we need to develop some filtration machinery on power series.

We start by considering the decreasing filtration of $\mathcal{A}^0 := R[[x]]$ by the subrings $\mathcal{A}^0_\nu$, $\nu \geq 1$, defined by

$$\mathcal{A}^0_\nu = R[[x^{p^\nu}]] + pR[[x^{p^{\nu-1}}]] + p^2R[[x^{p^{\nu-2}}]] + ... + p^\nu R[[x]] \subset R[[x]].$$

Let v_p be the p-adic valuation on R.

Lemma 8.3.

1) $\mathcal{A}^0_\nu = \{\sum_{n\geq 0} a_n x^n \in R[[x]]\ ;\ v_p(a_n) \geq \nu - v_p(n)\}$.

2) If $G_1, G_2, G_3, ... \in \mathcal{A}^0_\nu$, $G_m \in x^m R[[x]]$. Then $\sum_{m\geq 1} G_m \in \mathcal{A}^0_\nu$.

3) If $H \in \mathcal{A}^0_\nu$, $H(0) = 0$, and $G \in R[[x]]$ then $G(H(x)) \in \mathcal{A}^0_\nu$.

4) $p\mathcal{A}^0_\nu \subset \mathcal{A}^0_{\nu+1}$.

5) If $G \in \mathcal{A}^0_\nu$ then $G^p \in \mathcal{A}^0_{\nu+1}$.

6) If $F \in \mathcal{A}^0_1$ and $F(0) = 0$ then $F^{\circ\nu} \in \mathcal{A}^0_\nu$.

Proof. Assertion 1 is easy. Assertion 2 clearly follows from assertion 1. Assertion 3 clearly follows from assertion 2. Assertions 4 and 5 are clear. Assertion 6 follows from assertions 3, 4, 5. □

We continue by considering the filtration

$$\mathcal{A}^n = R[[x]][x',...,x^{(n)}]\hat{},\quad n \geq 0$$

on

$$\mathcal{A} := \bigcup_{n\geq 0} \mathcal{A}^n.$$

(Here $\mathcal{A}^0 = R[[x]]$.) There is a natural p-derivation δ on $\mathcal{A}$ sending $\delta x = x'$, $\delta x' = x''$, etc. Note that $\delta\mathcal{A}^n \subset \mathcal{A}^{n+1}$ for all n. So according to equation (3.3) we may then consider the filtration

$$\mathcal{A}^{\{n\}} = \mathcal{A}^n + p\mathcal{A}^{n+1} + p^2\mathcal{A}^{n+2} + ...$$

on $\mathcal{A}$. Finally let

$$\mathcal{I} = (x, x', x'', ...) \subset \mathcal{A}.$$

So we may consider the descending filtration of $\mathcal{I}$ by ideals $\mathcal{I}^{[p^\nu]}$, $\nu \geq 0$. Note that with A^n, A, I as in 4.1 we have $A^n \subset \mathcal{A}^n$, $A \subset \mathcal{A}$, $I \subset \mathcal{I}$, and hence $I^{[p^\nu]} \subset \mathcal{I}^{[p^\nu]}$. Let $n, i \geq 1$. Note also that Lemma 3.2 immediately implies the injectivity of the map in Equation 1.4 because $\mathcal{I}^{[p^\nu]} \subset (p\mathcal{A}^n + \mathcal{I})^\nu$ and because $\mathcal{A}^n$ is separated in the topology given by the maximal ideal $p\mathcal{A}^n + \mathcal{I}$.

In what follows we prove a series of lemmas that will lead to Theorem 1.7.

Lemma 8.4.

$$\delta^n(p^i x) = \begin{cases} p^{i-n}\phi^n(x) + [(p^{i-n+1}\mathcal{A}^{\{0\}}) \cap \mathcal{I}^{[p^{i+1}]}] & \text{if } n \leq i \\ \phi^i(x^{(n-i)}) + [\mathcal{A}^{\{n-i-1\}} \cap \mathcal{I}^{[p^{i+1}]}] & \text{if } n \geq i+1 \end{cases}$$

Proof. Induction on n. The case $n = 1$ is clear. Now assume the above is true for some $n \geq 1$. If $n \leq i - 1$ we have

$$\begin{array}{rcl} \delta^{n+1}(p^i x) & \in & \delta(p^{i-n}\phi^n(x)) + \delta((p^{i-n+1}\mathcal{A}^{\{0\}}) \cap \mathcal{I}^{[p^{i+1}]}) \\ & & +C_p(p^{i-n}\mathcal{A}^{\{0\}}, (p^{i-n+1}\mathcal{A}^{\{0\}}) \cap \mathcal{I}^{[p^{i+1}]}) \\ & \subset & p^{i-n-1}\phi^{n+1}(x) - p^{(i-n)p-1}\phi^n(x)^p + (p^{i-n}\mathcal{A}^{\{0\}}) \cap \mathcal{I}^{[p^{i+1}]} \\ & & +(p^{i-n+1}\mathcal{A}^{\{0\}}) \cap \mathcal{I}^{[p^{i+1}]} \\ & \subset & p^{i-n-1}\phi^{n+1}(x) + (p^{i-n}\mathcal{A}^{\{0\}}) \cap \mathcal{I}^{[p^{i+1}]}. \end{array}$$

If $n \geq i + 1$ we have

$$\begin{array}{rcl} \delta^{n+1}(p^i x) & \in & \delta(\phi^i(x^{(n-i)})) + \delta(\mathcal{A}^{\{n-i-1\}} \cap \mathcal{I}^{[p^{i+1}]}) \\ & & +C_p(\mathcal{A}^{\{n-i\}}, \mathcal{A}^{\{n-i-1\}} \cap \mathcal{I}^{[p^{i+1}]}) \\ & \in & \phi^i(x^{(n+1-i)}) + \mathcal{A}^{\{n-i\}} \cap \mathcal{I}^{[p^{i+1}]}. \end{array}$$

The case $n = i$ is similar. □

Lemma 8.5. *Let $G \in xR[[x]]$. Then for all $n \geq 1$:*

$$\delta^n(G(x)) = \left(\frac{dG}{dx}\right)^{p^n} x^{(n)} + [\mathcal{A}^{\{n-1\}} \cap \mathcal{I}^{[p]}].$$

Proof. We proceed by induction on n. To check the statement for $n = 1$ write $G(x) = \sum_{m\geq 1} a_m x^m$; then

$$\begin{array}{rcl} \delta(G(x)) & = & \frac{1}{p}[\sum_{m\geq 1}\phi(a_m)(x^p + px')^m - (\sum_{m\geq 1} a_m x^m)^p] \\ & = & \frac{1}{p}[\sum_{m\geq 1}(a_m^p + p\delta a_m)(x^{pm} + pmx^{p(m-1)}x' + \ldots) - (\sum_{m\geq 1} a_m x^m)^p] \\ & \in & x^p\mathcal{A}^0 + (\sum_{m\geq 1} m a_m x^{m-1})^p x' + px'\mathcal{A}^1 \\ & \subset & \left(\frac{dG}{dx}\right)^p x' + \mathcal{A}^{\{0\}} \cap \mathcal{I}^{[p]}, \end{array}$$

which settles the case $n = 1$. For the induction step, assuming the statement true for some $n \geq 1$, we have

$$\begin{array}{rcl} \delta^{n+1}(G(x)) & \in & \delta\left(\left(\frac{dG}{dx}\right)^{p^n} x^{(n)}\right) + \delta(\mathcal{A}^{\{n-1\}} \cap \mathcal{I}^{[p]}) + C_p(\mathcal{A}^{\{n\}}, \mathcal{A}^{\{n-1\}} \cap \mathcal{I}^{[p]}) \\ & \in & \left(\frac{dG}{dx}\right)^{p^{n+1}} x^{(n+1)} + \phi(x^{(n)}) \cdot \delta\left(\left(\frac{dG}{dx}\right)^{p^n}\right) + \mathcal{A}^{\{n\}} \cap \mathcal{I}^{[p]}. \end{array}$$

Now, using Theorem 1.1, we have

$$\begin{array}{rcl} \phi(x^{(n)}) \cdot \delta\left(\left(\frac{dG}{dx}\right)^{p^n}\right) & \in & (\mathcal{A}^n \cap \mathcal{I}) \cdot p^n\mathcal{A}^1 \\ & \subset & \mathcal{A}^n \cap p^n\mathcal{I} \\ & \subset & \mathcal{A}^{\{n\}} \cap \mathcal{I}^{[p]} \end{array}$$

and we are done. □

Next consider any series $\Sigma = \Sigma(x) \in xR[[x]]$ and consider the unique ring endomorphism $\Sigma^* : \mathcal{A} \to \mathcal{A}$ such that $\Sigma^* x = \Sigma(x)$, $\Sigma^* x' = \delta(\Sigma(x))$, $\Sigma^* x'' = \delta^2(\Sigma(x))$, etc. Clearly $\Sigma^*(\mathcal{A}^n) \subset \mathcal{A}^n$ for $n \geq 0$ and hence $\Sigma^*(\mathcal{A}^{\{n\}}) \subset \mathcal{A}^{\{n\}}$ for $n \geq 0$. It is trivial to see that Σ^* and δ commute on $\mathcal{A}$; similarly Σ^* and ϕ commute on $\mathcal{A}$. Moreover for any two series Σ_1, Σ_2 we have the following compatibility of upper $*$ with composition: $(\Sigma_1 \circ \Sigma_2)^* = \Sigma_2^* \circ \Sigma_1^*$.
Recall that for any integer $a \in \mathbb{Z}$ we write $a^+ = \max\{a, 0\}$.

Lemma 8.6. *Assume* $\Sigma(x) = x^{p^m}$, $m \geq 1$, $\nu \geq 0$, $n \geq 0$*; then:*
1) $\Sigma^* \mathcal{J}^{[p^\nu]} \subset \mathcal{J}^{[p^{\nu+m}]}$*;*
2) $\Sigma^* \mathcal{A}^{\{n\}} \subset \mathcal{A}^{\{(n-m)^+\}}$.

Proof. To check assertion 1 it is enough to check it for $m = 1$. Now assertion 1 follows from the following computations in which $i + j = \nu$:

$$\Sigma^*(p^i (x^{(s)})^{p^j}) = p^i (\delta^s(x^p))^{p^j} \in p^i \mathcal{J}^{[p^{j+1}]} \subset \mathcal{J}^{[p^{i+j+1}]} = \mathcal{J}^{[p^{\nu+1}]};$$

in the above we used the fact that since $x^p \in \mathcal{J}^{[p]}$ we have $\delta^s(x^p) \in \mathcal{J}^{[p]}$ hence $(\delta^s(x^p))^{p^j} \in \mathcal{J}^{[p^{j+1}]}$; cf. Lemma 3.1. To prove assertion 2 it is enough, by the compatibility with composition, to prove these two statements for $m = 1$ and $n \geq 1$ which we now assume. Now by Theorem 1.1 we have $\delta^n(x^p) \in \mathcal{A}^{\{n-1\}}$ for $n \geq 1$. Consequently, for $n \geq 1$ and $F \in \mathcal{A}^{n+i}$ we have

$$\Sigma^*(p^i F(x, ..., x^{(n+i)})) = p^i F(x^p, ..., \delta^{n+i}(x^p)) \in p^i \mathcal{A}^{\{n+i-1\}} \subset \mathcal{A}^{\{n-1\}}$$

which proves assertion 2. □

We are ready to prove Theorem 1.7:

Proof of Theorem 1.7. Set $\Sigma(x) = x^{p^j}$. Using Lemmas 8.4, 8.5, 8.6 we have the following computation for $1 \leq m \leq i$:

$$\begin{array}{rcl} \delta^m(p^i G(x^{p^j})) & = & \delta^m(\Sigma^* G^*(p^i x)) \\ & = & \Sigma^* G^*(\delta^m(p^i x)) \\ & \in & \Sigma^* G^* \{p^{i-m} \phi^m(x) + (p^{i-m+1} \mathcal{A}^{\{0\}}) \cap \mathcal{J}^{[p^{i+1}]}\} \\ & \subset & \Sigma^* G^*(p^{i-m} \phi^m(x)) + (p^{i-m+1} \mathcal{A}^{\{0\}}) \cap \mathcal{J}^{[p^{i+1+j}]} \\ & \subset & p^{i-m} \phi^m(G(x^{p^j})) + (p^{i-m+1} \mathcal{A}^{\{0\}}) \cap \mathcal{J}^{[p^{\nu+1}]}. \end{array}$$

For $m \geq i + 1$ we have:

$$\begin{array}{rcl} \delta^m(p^i G(x^{p^j})) & = & \Sigma^* G^*(\delta^m(p^i x)) \\ & \in & \Sigma^* G^* \{\phi^i(x^{(m-i)}) + \mathcal{A}^{\{m-i-1\}} \cap \mathcal{J}^{[p^{i+1}]}\} \\ & \subset & \Sigma^* G^* \{\phi^i(x^{(m-i)})\} + \mathcal{A}^{\{(m-i-1-j)^+\}} \cap \mathcal{J}^{[p^{i+1+j}]} \\ & \subset & \phi^i \Sigma^*(\delta^{m-i} G) + \mathcal{A}^{\{(m-\nu-1)^+\}} \cap \mathcal{J}^{[p^{\nu+1}]} \\ & \subset & \phi^i \Sigma^* \{\left(\frac{dG}{dx}\right)^{p^{m-i}} x^{(m-i)} + \mathcal{A}^{\{m-i-1\}} \cap \mathcal{J}^{[p]}\} \\ & & + \mathcal{A}^{\{(m-\nu-1)^+\}} \cap \mathcal{J}^{[p^{\nu+1}]} \\ & \subset & \phi^i \{\left(\frac{dG}{dx}(x^{p^j})\right)^{p^{m-i}} \cdot \delta^{m-i}(x^{p^j})\} + \mathcal{A}^{\{(m-\nu-1)^+\}} \cap \mathcal{J}^{[p^{\nu+1}]}. \end{array}$$

□

Now Theorem 1.7 and Corollary 1.3 trivially imply:

Corollary 8.7. *Let $m \geq 0$, $\nu \geq 1$, $i+j=\nu$, $i,j \geq 0$, $G \in xR[[x]]$. Then the element $\overline{\delta^m(p^i G(x^{p^j}))} \in \overline{\mathcal{A}}^m$ is given by*

$$\overline{\delta^m(p^i G(x^{p^j}))} = \begin{cases} 0 & \text{if } m < i \\ G(x^{p^j})^{p^i} & \text{if } m = i \\ [\overline{\mathcal{A}}^0 \cap \overline{\mathcal{J}}^{[p^{\nu+1}]}] & \text{if } i < m \leq \nu \\ \left(x^{p^j-1}\frac{dG}{dx}(x^{p^j})\right)^{p^m}(x^{(m-\nu)})^{p^\nu} + [\overline{\mathcal{A}}^{m-\nu-1} \cap \overline{\mathcal{J}}^{[p^\nu]}] & \text{if } m > \nu \end{cases}$$

In particular $\overline{\delta^m(p^i G(x^{p^j}))} \in \overline{\mathcal{A}}^{(m-\nu)^+} \cap \overline{\mathcal{J}}^{[p^\nu]}$.

Lemma 8.8. *Let y be an N-tuple $y_1, ..., y_N$ of variables. Then, for $n \geq 1$,*

$$\delta^n\left(\sum_{i=1}^N y_i\right) = \sum_{i=1}^N y_i^{(n)} + P_{N,n}(y, y', ..., y^{(n-1)})$$

in $R\{y\}$ where $P_{N,n}$ is a polynomial with $\mathbb{Z}$-coefficients without constant term or linear terms.

Proof. Induction on n. □

Note that Corollary 8.7 and Lemma 8.8 immediately imply Corollary 1.8. Also Corollary 1.8 immediately implies Corollary 1.10; one can prove a slightly more precise result:

Proposition 8.9. *Let $F(x) \in xR[[x]]$ be a series of finite height $h \geq 1$ satisfying $F(x) \equiv px \bmod x^2$. For all $\nu \geq 1$ consider the scheme $X_\nu := Spec\ \frac{R[[x]]}{(F^{\circ\nu})}$. Then we have:*

$$\widetilde{\mathcal{O}^n(X_\nu)} = \frac{k[x, x', ..., x^{(n)}]}{(x^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n)})^{p^\nu})} \quad \text{if } n \geq 1, \tag{8.3}$$

$$\overline{\mathcal{O}^n(X_\nu)} = \frac{k[x, x', ..., x^{(n)}]}{(x^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n-\nu)})^{p^\nu})} \quad \text{if } n \geq \nu, \tag{8.4}$$

$$\overline{\mathcal{O}^n(X_\nu)} = \frac{k[x, x', ..., x^{(n)}]}{(x^\mu)} \quad \text{if } 1 \leq n \leq \nu - 1, \tag{8.5}$$

where $\mu \geq p^\nu$.

Proof. By assertion 6 in Lemma 8.3 we may write $F^{\circ\nu} = \sum_{j=0}^\nu p^{\nu-j} G_j(x^{p^j})$, $G_j \in R[[x]]$, $j \geq 0$. We may choose the G_js in $xR[[x]]$ and then $G_0(x) \equiv x$ mod x^2. Also $\overline{p^{-\nu}\frac{dF^{\circ\nu}}{dx}} \equiv 1$ mod x. We conclude by Corollary 1.8 and equation (8.2). □

9. p-jets of $E[p^\nu]$ for supersingular elliptic curves

Proposition 9.1. *Let E/R be an elliptic curve with supersingular reduction and $E[p^\nu]$ the kernel of the multiplication by p. Then for any $n \geq 1$ we have:*

$$\mathcal{O}^n(\widetilde{E[p^\nu]}) = \frac{k[x, x', ..., x^{(n)}]}{(x^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n)})^{p^\nu})} \quad \text{if } n \geq 1, \tag{9.1}$$

$$\overline{\mathcal{O}^n(E[p^\nu])} = \frac{k[x, x', ..., x^{(n)}]}{(x^{p^\nu}, (x')^{p^\nu}, ..., (x^{(n-\nu)})^{p^\nu})} \quad \text{if } n \geq \nu, \tag{9.2}$$

$$\overline{\mathcal{O}^n(E[p^\nu])} = \frac{k[x, x', ..., x^{(n)}]}{(x^\mu)} \quad \text{if } 1 \leq n \leq \nu - 1, \tag{9.3}$$

where $\mu \geq p^\nu$.

Proof. Since E has supersingular reduction $E[p^\nu]$ is connected so it is equal to $\mathcal{F}[p^\nu]$ where $\mathcal{F}$ is the formal group law of E and we conclude by Proposition 8.9. □

References

1. Borger, J., The basic geometry of Witt vectors, I: the affine case, Algebra and Number Theory 5 (2011), no. 2, pp 231-285.
2. Borger, J., The basic geometry of Witt vectors, II: Spaces, Mathematische Annalen 351 (2011), no. 4, pp 877-933.
3. Buium, A.: Differential characters of Abelian varieties over p-adic fields, Invent. Math. 122 (1995), 2, pp. 309-340.
4. Buium, A.: Arithmetic Differential Equations. Math. Surveys and Monographs 118, AMS, 2005.
5. Buium, A.: Differential eigenforms, J. Number Theory 128 (2008), 979-1010.
6. Buium, A., Simanca, S.R.: Arithmetic Laplacians, Advances in Math. 220 (2009), pp. 246-277.
7. Buium, A., Saha, A.: Hecke operators on differential modular forms mod p, J. Number Theory 132 (2012), 966-997.
8. Buium, A.: p-jets of finite algebras, II: p-typical Witt rings, Documenta Math. 18 (2013), 971-996.
9. Eisenbud, D.: Commutative Algebra, GTM 150, Springer 1995.
10. Katz, N.: Serre-Tate local moduli, Springer LNM 868 (1981), 138-202.
11. Lang, S.: Cyclotomic fields I and II, GTM 121, Springer 1990.
12. Lubin, J.: One-parameter formal Lie groups over p-adic integer rings, Annals of Math. 80 (1964), 464-484.
13. Matsumura, H.: Commutative Ring Theory, Cambridge Univ. Press, 1986.
14. Silverman, J.H.: The Arithmetic of Elliptic Curves, GTM 106, Springer, 1986.
15. Tate, J.: p-divisible groups, Proceedings of a Conference on Local Fields, Driebergen, 1966, Springer, 1967, 158-183.

Alexandru Buium
Department of Mathematics
and Statistics
University of New Mexico
Albuquerque NM 87131
USA
buium@math.unm.edu