On one-dimensional perfect formal group laws

Jan Kohlhaase

Abstract. Let p be a prime number and let R denote a commutative unital ring which is perfect of characteristic p. We show that every one-dimensional commutative perfect formal group law over R is an ordinary formal group law.

Contents

Acknowledgments. This work was written while the author was a member of the RTG 2553 *"Symmetries and classifying spaces: analytic, arithmetic and derived"*. He gratefully acknowledges the financial support of the DFG.

Notation and conventions. Let p be a prime number. By $\mathbb{N}$ we denote the set of non-negative integers and by $\mathbb{N}[\frac{1}{p}]$ the set of rational numbers of the form ip^n for some $i \in \mathbb{N}$ and $n \in \mathbb{Z}$. Let $\mathbb{Q}_p$ denote the field of p-adic numbers and $\mathbb{Z}_p$ its ring of integers. The p-adic valuation v_p on $\mathbb{Q}_p$ will be normalized through $v_p(p) = 1$. Unless stated otherwise, all rings will be assumed commutative and unital. If S is an integral domain we denote by $\mathrm{Frac}(S)$ its field of fractions. We say that a ring S has characteristic p if $pS = 0$. In this case, the endomorphism $\varphi = (s \mapsto s^p)$ of S is called its Frobenius. A ring S of characteristic p is called perfect if its Frobenius endomorphism is bijective. Throughout this article we fix a non-zero perfect ring R of characteristic p and denote by Alg_R the category of R-algebras. By an adic ring we mean a separated and complete topological ring S whose topology coincides with the I-adic topology for some ideal $I \subseteq S$. Any such ideal is called an ideal of definition. If R is an adic ring we denote by Alg_R^{ad} the category of adic R-algebras.

1 Perfect formal power series

Endow the perfect ring R with the discrete topology. Given indeterminates $X = (X_1, \ldots, X_d)$ we denote by $R[\![X]\!] = R[\![X_1, \ldots, X_d]\!]$ the corresponding formal power series ring with coefficients in R endowed with the (X)-adic

2010 Mathematics Subject Classification.

topology. Denote by $\varinjlim_{\varphi} R[\![X]\!]$ the coperfection of $R[\![X]\!]$, i.e. the colimit of the countable system of ring homomorphisms

$$R[\![X]\!] \stackrel{\varphi}{\to} R[\![X]\!] \stackrel{\varphi}{\to} R[\![X]\!] \stackrel{\varphi}{\to} \dots .$$

The initial term allows us to view $R[\![X]\!]$ as a subring of $\varinjlim_{\varphi} R[\![X]\!]$. We denote by

$$R[\![X^{1/p^\infty}]\!] = R[\![X_1^{1/p^\infty}, \dots, X_d^{1/p^\infty}]\!]$$

the (X)-adic completion of $\varinjlim_{\varphi} R[\![X]\!]$ endowed with the (X)-adic topology. It is called the ring of *perfect formal power series* with coefficients in R. In more concrete terms, given $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{N}[\frac{1}{p}]^d$ set $|\alpha| = \alpha_1 + \dots + \alpha_d$. Consider the R-module S of formal expressions of the form

$$f(X) = \sum_{\alpha \in \mathbb{N}[\frac{1}{p}]^d} c_\alpha X^\alpha \tag{1}$$

with $c_\alpha \in R$ such that for any $n \in \mathbb{N}$ the set $\{\alpha \in \mathbb{N}[\frac{1}{p}]^d \mid c_\alpha \neq 0 \text{ and } |\alpha| \leq n\}$ is finite. Addition and scalar multiplication are defined coefficientwise. By the above finiteness condition the multiplication

$$(\sum_{\alpha \in \mathbb{N}[\frac{1}{p}]^d} c_\alpha X^\alpha) \cdot (\sum_{\beta \in \mathbb{N}[\frac{1}{p}]^d} d_\beta X^\beta) = \sum_{\gamma \in \mathbb{N}[\frac{1}{p}]^d} (\sum_{\alpha+\beta=\gamma} c_\alpha d_\beta) X^\gamma$$

of two elements of S is well-defined and makes S into a ring of characteristic p with unit element $1 = X^0$. It contains $R[\![X]\!]$ as a subring by identifying X_i with X^{e_i}. Here $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ with 1 in position i. We then have $X^\alpha = X_1^{\alpha_1} \cdot \ldots \cdot X_d^{\alpha_d}$ in S for all $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{N}[\frac{1}{p}]^d$. The Frobenius of S is given by

$$\varphi(\sum_{\alpha \in \mathbb{N}[\frac{1}{p}]^d} c_\alpha X^\alpha) = \sum_{\alpha \in \mathbb{N}[\frac{1}{p}]^d} \varphi(c_\alpha) X^{p\alpha}$$

whence S is perfect. One checks directly that S is (X)-adically separated and complete and that the induced ring homomorphism $R[\![X^{1/p^\infty}]\!] \to S$ is an isomorphism. In fact, $\varinjlim_{\varphi} R[\![X]\!]$ maps isomorphically onto the dense subring

$$\bigcup_{n \in \mathbb{N}} R[\![X_1^{1/p^n}, \dots, X_d^{1/p^n}]\!] = \bigcup_{n \in \mathbb{N}} \varphi^{-n}(R[\![X]\!])$$

consisting of all elements of the form $\sum_{\alpha \in \frac{1}{p^n}\mathbb{N}^d} c_\alpha X^\alpha$ for some $n \in \mathbb{N}$.

If $f(X)$ is a perfect formal power series as in (1) and if $n \in \mathbb{Z}$ then we let $f^{(p^n)}$ denote the perfect formal power series obtained by applying φ^n to the coefficients of f, i.e.

$$f^{(p^n)}(X) = \sum_{\alpha \in \mathbb{N}[\frac{1}{p}]^d} c_\alpha^{p^n} X^\alpha.$$

If $f = (f_1, \dots, f_e) \in R[\![X]\!]^e$ is a family of perfect formal power series then we set $f^{(p^n)} = (f_1^{(p^n)}, \dots, f_e^{(p^n)})$.

Remark 1.1. If R is a more general adic ring with ideal of definition $I \subseteq R$ then $R[\![X^{1/p^\infty}]\!]$ is defined as the (I, X)-adic completion of $\varinjlim_\varphi R[\![X]\!]$. This can be identified with the set of all series as in (1) such that for any $n \in \mathbb{N}$ the set of $\alpha \in \mathbb{N}[\frac{1}{p}]^d$ with $|\alpha| \leq n$ and $c_\alpha \notin I^n$ is finite. With this convention we have canonical isomorphisms $R[\![X^{1/p^\infty}]\!][\![Y^{1/p^\infty}]\!] \cong R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$ of adic R-algebras for any second family of indeterminates Y.

Let Perf_R^{ad} denote the full subcategory of Alg_R^{ad} consisting of all adic R-algebras S on which the Frobenius $\varphi : S \to S$ is an automorphism of adic rings, i.e. it is bijective with a continuous inverse. Note that $\varphi^{-1} : S \to S$ is continuous if and only if the ideal $\varphi^{-1}(I)/I \subseteq S/I$ is nilpotent for some (equivalently, for every) ideal of definition I of S. This is true, for example, if S admits a finitely generated ideal of definition. By abuse of terminology we call Perf_R^{ad} the category of perfect adic R-algebras. By $(\cdot)^\flat : \mathrm{Alg}_R^{ad} \to \mathrm{Perf}_R^{ad}$ we denote the perfection given by

$$S \mapsto S^\flat = \varprojlim_\varphi S = \{(s_n)_{n\geq 0} \in S^{\mathbb{N}} \mid s_{n+1}^p = s_n \text{ for all } n \geq 0\}$$

where $S^\flat$ is endowed with the projective limit topology. Note that $S^\flat$ is an R-algebra via $r \cdot (s_n)_{n\geq 0} = (r^{1/p^n} \cdot s_n)_{n\geq 0}$. Moreover, $\varphi^{-1} : S^\flat \to S^\flat$ is given by $(s_n)_{n\geq 0} \mapsto (s_{n+1})_{n\geq 0}$ which is clearly continuous.

Given an adic ring S let $S^{\circ\circ} = \{s \in S \mid \lim_{n\to\infty} s^n = 0\}$ denote its ideal of topologically nilpotent elements. The universal properties of rings of perfect formal power series can be summarized as follows.

Proposition 1.2. *(i) For any $S \in \mathrm{Perf}_R^{ad}$ the projection $S^\flat \to S$ defined by $(s_n)_{n\geq 0} \mapsto s_0$ is an isomorphism of adic R-algebras.*

(ii) For any $S \in \mathrm{Perf}_R^{ad}$ the inclusion $R[\![X]\!] \hookrightarrow R[\![X^{1/p^\infty}]\!]$ induces a functorial bijection $\mathrm{Hom}_{R\text{-alg}}^{cont}(R[\![X^{1/p^\infty}]\!], S) \cong \mathrm{Hom}_{R\text{-alg}}^{cont}(R[\![X]\!], S)$.

(iii) For any $S \in \mathrm{Alg}_R^{ad}$ the projection $S^\flat \to S$ induces a functorial bijection $\mathrm{Hom}_{R\text{-alg}}^{cont}(R[\![X^{1/p^\infty}]\!], S^\flat) \cong \mathrm{Hom}_{R\text{-alg}}^{cont}(R[\![X^{1/p^\infty}]\!], S)$.

(iv) For any $S \in \mathrm{Perf}_R^{ad}$ the map $\mathrm{Hom}_{R\text{-alg}}^{cont}(R[\![X^{1/p^\infty}]\!], S) \to (S^{\circ\circ})^d$ sending ψ to $(\psi(X_1), \dots, \psi(X_d))$ is bijective.

Proof. If S is perfect adic then the inverse in (i) is given by $s \mapsto (s^{1/p^n})_{n\geq 0}$. Parts (ii) and (iii) are the usual adjunctions between the adic (co)perfection and the inclusion $\mathrm{Perf}_R^{ad} \hookrightarrow \mathrm{Alg}_R^{ad}$. Part (iv) follows from (ii) and the universal property of $R[\![X]\!]$. □

Given a family $s = (s_1, \ldots, s_d)$ of topologically nilpotent elements of $S \in \mathrm{Perf}_R^{ad}$ the corresponding homomorphism $\psi_s : R[\![X^{1/p^\infty}]\!] \to S$ in Proposition 1.2 (iv) is the substitution homomorphism given by

$$\psi_s\Big(\sum_{\alpha\in\mathbb{N}[\frac{1}{p}]^d} c_\alpha X^\alpha\Big) = \sum_{\alpha\in\mathbb{N}[\frac{1}{p}]^d} c_\alpha s^\alpha = \sum_{\alpha\in\mathbb{N}[\frac{1}{p}]^d} c_\alpha s_1^{\alpha_1}\cdots s_d^{\alpha_d}.$$

Here we use the convention $s^\beta = s^{i/p^n} = \varphi^{-n}(s^i)$ for all $s \in S$ and for all $\beta = i/p^n \in \mathbb{N}[\frac{1}{p}]$ with $i \in \mathbb{N}$ and $n \in \mathbb{Z}$. Given $f \in R[\![X^{1/p^\infty}]\!]$ we write $\psi_s(f) = f(s)$ as usual.

A non-zero perfect formal power series of the form $c_\alpha X^\alpha$ with $\alpha \in \mathbb{N}[\frac{1}{p}]^d$ and $c_\alpha \in R$ is called a monomial of degree $|\alpha|$. A non-zero element $f \in R[\![X^{1/p^\infty}]\!]$ is called homogenous of degree $\nu \in \mathbb{N}[\frac{1}{p}]$ if it is a finite sum of monomials of degree ν. With this terminology, any perfect formal power series $f(X)$ as in (1) admits the convergent decomposition $f(X) = \sum_{\nu\in\mathbb{N}[\frac{1}{p}]} f_\nu(X)$ where $f_\nu(X) = \sum_{|\alpha|=\nu} c_\alpha X^\alpha$ is either zero or homogenous of degree ν. If f is non-zero we call

$$\begin{aligned}\mathrm{ord}(f) &= \min\{\nu \in \mathbb{N}[\tfrac{1}{p}] \mid f_\nu \neq 0\}\\ &= \min\{\nu \in \mathbb{N}[\tfrac{1}{p}] \mid \text{there is } \alpha \in \mathbb{N}[\tfrac{1}{p}]^d \text{ with } |\alpha| = \nu \text{ and } c_\alpha \neq 0\}\end{aligned}$$

the order of f and formally set $\mathrm{ord}(0) = \infty$. We then have the usual rules

$$(2)\quad \mathrm{ord}(f-g) \geq \min\{\mathrm{ord}(f), \mathrm{ord}(g)\} \quad \text{and} \quad \mathrm{ord}(fg) \geq \mathrm{ord}(f) + \mathrm{ord}(g).$$

In the first case we have equality if the orders of f and g are distinct. In the second case we have equality if R is an integral domain. This follows from the corresponding fact for ordinary formal power series. For any real number $\nu \geq 0$ consider the ideals

$$\begin{aligned}\mathfrak{m}_{\geq\nu} &= \{f \in R[\![X^{1/p^\infty}]\!] \mid \mathrm{ord}(f) \geq \nu\} \text{ and}\\ \mathfrak{m}_{>\nu} &= \{f \in R[\![X^{1/p^\infty}]\!] \mid \mathrm{ord}(f) > \nu\}\end{aligned}$$

of $R[\![X^{1/p^\infty}]\!]$ and set $\mathfrak{m} = \mathfrak{m}_{>0}$. Note that we have $\mathfrak{m}_{\geq 1} = (X)$ and that $\mathfrak{m}^n = \mathfrak{m}$ for any positive integer n.

Let $\psi_0 : R[\![X^{1/p^\infty}]\!] \to R$ denote the augmentation homomorphism sending a perfect formal power series to its constant term $f(0) = c_0 \in R$. Note that $R^{\circ\circ} = 0$ because R carries the discrete topology and is reduced. As a consequence, an element $f \in R[\![X^{1/p^\infty}]\!]$ is topologically nilpotent if and only if $f(0) = 0$, i.e. $R[\![X^{1/p^\infty}]\!]^{\circ\circ} = \ker(\psi_0) = \mathfrak{m}$. In particular, given a second family of variables $Y = (Y_1, \ldots, Y_e)$ and $g = (g_1, \ldots, g_d) \in R[\![Y^{1/p^\infty}]\!]^d$ such that $g(0) = (g_1(0) = \ldots = g_d(0)) = 0$ we have the substitution homomorphism $\psi_g : R[\![X^{1/p^\infty}]\!] \to R[\![Y^{1/p^\infty}]\!]$ and set

$$\mathrm{ord}(g) = \min\{\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_d)\}.$$

Lemma 1.3. *Let $f \in R[\![X^{1/p^\infty}]\!]$ and $g \in R[\![Y^{1/p^\infty}]\!]^d$ with $g(0) = 0$.*

(i) We have $\operatorname{ord}(f(g)) \geq \operatorname{ord}(f) \cdot \operatorname{ord}(g)$.

(ii) If $d = e = 1$ and if the lowest coefficient $c_{\operatorname{ord}(f)}$ of f is not a zero divisor then $\operatorname{ord}(f(g)) = \operatorname{ord}(f) \cdot \operatorname{ord}(g)$.

Proof. Part (i) follows directly from (2). As for (ii), let $\alpha = \operatorname{ord}(f)$, $\beta = \operatorname{ord}(g)$ and let c_α and d_β be the corresponding coefficients of f and g, respectively. Plugging $d_\beta Y^\beta$ into $c_\alpha X^\alpha$ gives $c_\alpha d_\beta^\alpha Y^{\alpha\beta}$. If $d_\beta \neq 0$ then also $d_\beta^\alpha \neq 0$ because R is reduced. If c_α is not a zero divisor we get $c_\alpha d_\beta^\alpha \neq 0$. Since $f(g) \equiv c_\alpha d_\beta^\alpha Y^{\alpha\beta} \mod \mathfrak{m}_{>\alpha\beta}$ by (i) the claim follows. □

For the substitution into ordinary formal power series, the following lemma is a variant of [6], Lemme 1.

Lemma 1.4. *Let $f \in R[\![X]\!]$ and $g_i, h_i \in R[\![Y^{1/p^\infty}]\!]$ with $f(0) = g_i(0) = h_i(0) = 0$ for $1 \leq i \leq d$. Setting $g = (g_1, \ldots, g_d)$ and $h = (h_1, \ldots, h_d)$ we have*

$$\operatorname{ord}(f(g) - f(h)) \geq (\operatorname{ord}(f) - 1) \cdot \min\{\operatorname{ord}(g), \operatorname{ord}(h)\} + \operatorname{ord}(h - g). \tag{3}$$

Proof. If $1 \leq i \leq d$ and $m_i \in \mathbb{N}$ then $g_i^{m_i} = h_i^{m_i} + \sum_{j=1}^{m_i} \binom{m_i}{j} h_i^{m_i - j}(g_i - h_i)^j$. Setting $\mu = \min\{\operatorname{ord}(g), \operatorname{ord}(h)\}$ we have $\operatorname{ord}(g_i - h_i) \geq \operatorname{ord}(g - h) \geq \mu$ and the above expansion shows that $\operatorname{ord}(g_i^{m_i} - h_i^{m_i}) \geq (m_i - 1) \cdot \mu + \operatorname{ord}(g - h)$. If $m = (m_1, \ldots, m_d)$ is non-zero then the expansion of a monomial

$$g^m = \prod_{i=1}^d g_i^{m_i} = \prod_{i=1}^d (h_i^{m_i} + (g_i^{m_i} - h_i^{m_i}))$$

gives h^m plus a sum of terms of the form $\prod_{i \in J} h_i^{m_i} \cdot \prod_{i \in J'} (g_i^{m_i} - h_i^{m_i})$ where $\{1, \ldots, d\}$ is the disjoint union of J and J' with $J' \neq \varnothing$. Using the above estimates and $\operatorname{ord}(g - h) \geq \mu$ the order of any such product is bounded by $(|m| - 1) \cdot \mu + \operatorname{ord}(g - h)$ from below. Since f is the convergent series of monomials $c_m X^m$ with $|m| \geq \operatorname{ord}(f) > 0$ the claim follows. □

In particular, congruences between perfect formal power series are always preserved by plugging them into ordinary formal power series. For the substitution into perfect formal power series we only get the following estimate.

Lemma 1.5. *Let $f \in R[\![X^{1/p^\infty}]\!]$ and $g_i, h_i \in R[\![Y^{1/p^\infty}]\!]$ with $f(0) = g_i(0) = h_i(0) = 0$ for $1 \leq i \leq d$. Assume that $\operatorname{ord}(g_i - h_i) > \min\{\operatorname{ord}(g_i), \operatorname{ord}(h_i)\}$ for $1 \leq i \leq d$. Setting $g = (g_1, \ldots, g_d)$ and $h = (h_1, \ldots, h_d)$ we have*

$$\operatorname{ord}(f(g) - f(h)) > \operatorname{ord}(f)\operatorname{ord}(g) = \operatorname{ord}(f)\operatorname{ord}(h). \tag{4}$$

Proof. Note first that our assumptions imply $\mathrm{ord}(g_i) = \mathrm{ord}(h_i)$ and $\mathrm{ord}(g) = \mathrm{ord}(h)$. Given $\alpha_i = m_i/p^{n_i} \in \mathbb{N}[\frac{1}{p}]$ with $m_i \in \mathbb{N}$ and $n_i \in \mathbb{Z}$ we have

$$g_i^{\alpha_i} = h_i^{\alpha_i} + \sum_{j=1}^{m_i} \binom{m_i}{j} h_i^{(m_i-j)/p^{n_i}} (g_i - h_i)^{j/p^{n_i}}, \tag{5}$$

whence $\mathrm{ord}(g_i^{\alpha_i} - h_i^{\alpha_i}) > \alpha_i \cdot \mathrm{ord}(h_i) \geq \alpha_i \cdot \mathrm{ord}(g)$ by our assumptions. If $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{N}[\frac{1}{p}]^d$ is non-zero then the expansion of a monomial

$$g^\alpha = \prod_{i=1}^{d} g_i^{\alpha_i} = \prod_{i=1}^{d} (h_i^{\alpha_i} + (g_i^{\alpha_i} - h_i^{\alpha_i}))$$

shows $\mathrm{ord}(g^\alpha - h^\alpha) > |\alpha| \cdot \mathrm{ord}(g)$ by arguing as in the proof of Lemma 1.4. Now f is the convergent series of monomials $c_\alpha X^\alpha$ with $|\alpha| \geq \mathrm{ord}(f) > 0$. Moreover, $\inf\{|\alpha| \mid c_\alpha \neq 0 \text{ and } |\alpha| > \mathrm{ord}(f)\} > \mathrm{ord}(f)$. This implies the claim. □

We shall also need the following result.

Lemma 1.6. *Fix $f \in R[\![X^{1/p^\infty}]\!]$ and consider the ideal $\mathfrak{m} \subset R[\![Y^{1/p^\infty}]\!]$. Then the map $\mathfrak{m}^d \to R[\![Y^{1/p^\infty}]\!]$ defined by $h \mapsto f(h)$ is continuous for the (Y)-adic topology on both sides.*

Proof. Since $R[\![Y^{1/p^\infty}]\!]$ is a topological ring on which Frobenius is a homeomorphism, the statement is clear if f is a monomial. If $f(X) = \sum_\alpha c_\alpha X^\alpha$ it suffices to see that the pointwise convergence of $h \mapsto f(h)$ is uniform on $\mathfrak{m}^d_{\geq \nu}$ for any $\nu > 0$. This follows from Lemma 1.3 (i) because we have $(\sum_{|\alpha| \geq n/\nu} c_\alpha X^\alpha)(\mathfrak{m}^d_{\geq \nu}) \subseteq \mathfrak{m}_{\geq n}$ for any $n \in \mathbb{N}$. □

The condition for being a unit in $R[\![X^{1/p^\infty}]\!]$ is the same as for ordinary formal power series. Namely, an element $f \in R[\![X^{1/p^\infty}]\!]$ is a unit in $R[\![X^{1/p^\infty}]\!]$ if and only if $f(0)$ is a unit in R. In fact, if $f(0) \in R$ is a unit we may assume $f(0) = 1$ and use the geometric series to construct a multiplicative inverse of f in $R[\![X^{1/p^\infty}]\!]$.

In the case of ordinary formal power series, the formal inverse function theorem tells us that a substitution homomorphism $\psi_g : R[\![X]\!] \to R[\![X]\!]$ with $g = (g_1, \ldots, g_d) \in R[\![X]\!]^d$ and $g(0) = 0$ is an isomorphism if and only if $\det((\frac{\partial g_i}{\partial X_j}(0))_{i,j})$ is a unit in R. If $d = 1$ then we will also write g' for the formal derivative of an ordinary formal power series g. Note that formal derivation is not available for perfect formal power series. In fact, the only known bijectivity criterion for perfect formal power series concerns the case $d = 1$. This was first studied by Kedlaya (cf. [4], Theorem 1). We give an

alternative proof and slightly correct the criterion for general perfect rings (cf. Example 1.13). In order to prepare for this note that the infinite product

$$c = \prod_{h=1}^{\infty} \frac{p^h}{p^h - 1} = \prod_{h=1}^{\infty} (1 + \frac{1}{p^h - 1})$$

converges in the real numbers with

$$1 < c \leq \exp(\sum_{h=1}^{\infty} \frac{1}{p^h - 1}) \leq \exp(\sum_{h=0}^{\infty} \frac{1}{p^{h-1}}) = \exp(1 + \frac{1}{p-1}) \leq \exp(2).$$

Theorem 1.7. *Assume that $d = 1$ and that R is an integral domain. Let $g \in R[\![X^{1/p^\infty}]\!]$ and $\nu \in \mathbb{N}[\frac{1}{p}]$ with $\nu > \mathrm{ord}(g) = 1$. If there is $f \in \mathfrak{m}$ with $g(f) \equiv X \mod \mathfrak{m}_{\geq c\nu}$ then $\mathrm{ord}(f) = 1$ and $f, g \in R[\![X]\!] + \mathfrak{m}_{>\nu}$.*

Proof. By working over the fraction field of R we may assume that $R = k$ is a perfect field of characteristic p. By Lemma 1.3 (ii) we have $\mathrm{ord}(g(f)) = \mathrm{ord}(g) \cdot \mathrm{ord}(f) = \mathrm{ord}(f)$. Since $\mathrm{ord}(g(f) - X) \geq c\nu > \nu > 1 = \mathrm{ord}(X)$ this implies $\mathrm{ord}(f) = 1$.

Assume that we can show $g \in k[\![X]\!] + \mathfrak{m}_{>\nu}$. Let $h \in k[\![X]\!]$ with $g - h \in \mathfrak{m}_{>\nu}$. Since $\nu > \mathrm{ord}(g)$ this implies $\mathrm{ord}(h) = \mathrm{ord}(g) = 1$ whence ψ_h is bijective by the inverse formal function theorem. Set $H = \psi_h^{-1}(X) \in Xk[\![X]\!]$ so that $H(h) = X$. By Lemma 1.4 we have $H(g) \equiv H(h) = X \mod \mathfrak{m}_{>\nu}$. This implies $\mathrm{ord}(H(g)(f) - f) = \mathrm{ord}(H(g) - X) \cdot \mathrm{ord}(f) > \nu$ by Lemma 1.3 (ii). On the other hand, $H(g)(f) = H(g(f)) \equiv H \mod \mathfrak{m}_{>\nu}$ by Lemma 1.4 because $\mathrm{ord}(g(f) - X) \geq c\nu > \nu$. Altogether, $f \equiv H(g)(f) \equiv H \mod \mathfrak{m}_{>\nu}$ which proves $f \in k[\![X]\!] + \mathfrak{m}_{>\nu}$.

It remains to show $g \in k[\![X]\!] + \mathfrak{m}_{>\nu}$. Assume the contrary and write $g(X) = \sum_{\alpha \in \mathbb{N}[\frac{1}{p}]} c_\alpha X^\alpha$. Set $g_0 = \sum_{\alpha \in \mathbb{N}} c_\alpha X^\alpha \in k[\![X]\!]$. For $i \geq 1$ we define g_i inductively. If $g_{i-1} \neq g$ set $\nu_i = \mathrm{ord}(g - g_{i-1})$, $h_i = -v_p(\nu_i)$ and $g_i = \sum_{v_p(\alpha) \geq -h_i} c_\alpha X^\alpha \in k[\![X^{1/p^{h_i}}]\!]$. If $g_{i-1} = g$ we set $g_i = g_{i-1}$, $\nu_i = \nu_{i-1}$ and $h_i = h_{i-1}$. Both sequences $(\nu_i)_{i \geq 1}$ and $(h_i)_{i \geq 1}$ are strictly increasing until they possibly become constant. This happens if and only if $g \in k[\![X^{1/p^h}]\!]$ with $h = \lim_{i \to \infty} h_i$. Otherwise, the sequences $(\nu_i)_{i \geq 1}$ and $(h_i)_{i \geq 1}$ are both unbounded. Assume for the moment that we have the inequality

$$\mathrm{ord}(g_i(f) - X) < \frac{p^{h_i}}{p^{h_i} - 1} \nu_i \tag{6}$$

for all $i \geq 1$. We will show by induction on $i \geq 1$ that

$$\mathrm{ord}(g_i(f) - X) < (\prod_{j=1}^{i} \frac{p^{h_j}}{p^{h_j} - 1}) \cdot \nu_1, \tag{7}$$

as long as the sequence $(h_1, \ldots, h_i)$ is strictly increasing. For $i = 1$ this follows directly from (6). Now assume that (7) holds for i and note that our assumption $g \notin k[\![X]\!] + \mathfrak{m}_{>\nu}$ implies $\nu_1 \leq \nu$. Since the values $h_1, \ldots, h_i$ are pairwise distinct we get $\operatorname{ord}(g_i(f) - X) < c\nu_1 \leq c\nu \leq \operatorname{ord}(g(f) - X)$. This implies

$$\begin{aligned} \operatorname{ord}(g_i(f) - X) &= \operatorname{ord}(g_i(f) - g(f) + g(f) - X) = \operatorname{ord}(g_i(f) - g(f)) \\ &= \operatorname{ord}(g_i - g) = \nu_{i+1} \end{aligned}$$

by Lemma 1.3 (ii) because $\operatorname{ord}(f) = 1$. Consequently,

$$\operatorname{ord}(g_{i+1}(f) - X)) < \frac{p^{h_{i+1}}}{p^{h_{i+1}} - 1}\nu_{i+1} = \frac{p^{h_{i+1}}}{p^{h_{i+1}} - 1}\operatorname{ord}(g_i(f) - X)$$

which implies (7) for $i + 1$ by the induction hypothesis. If $g_{i-1} \neq g = g_i$ for some $i \geq 1$ this yields the contradiction $\operatorname{ord}(g(f) - X) = \operatorname{ord}(g_i(f) - X) < \operatorname{ord}(g(f) - X)$. If $g_i \neq g$ for all $i \geq 1$ we get that the sequence $(\nu_i)_{i\geq 1}$ is bounded above by $c\nu_1$. This is a contradiction, too.

In order to complete the proof it remains to show (6). We will ease the notation and assume $g = \sum_\alpha c_\alpha X^\alpha \in k[\![X^{1/p^h}]\!]$ with $\operatorname{ord}(g) = 1$ and $h \geq 1$ such that there is $\alpha \in p^{-h}\mathbb{N}$ with $v_p(\alpha) = -h$ and $c_\alpha \neq 0$. Set

$$\nu = \min\{\alpha \in \frac{1}{p^h}\mathbb{N} \mid c_\alpha \neq 0 \text{ and } v_p(\alpha) = -h\}$$

and write $\nu = i/p^h$ with $i \in \mathbb{N} \setminus p\mathbb{N}$. We will show that

$$\operatorname{ord}(g(f) - X) \leq \frac{i-1}{p^h - 1} \tag{8}$$

for all $f \in k[\![X^{1/p^\infty}]\!]$ with $\operatorname{ord}(f) = 1$. Since $(i-1)/(p^h-1) < \frac{p^h}{p^h-1}\nu$ this will complete the proof of the theorem.

Let $E = \operatorname{Frac}(k[\![X]\!])$ and $F = \operatorname{Frac}(k[\![X^{1/p^\infty}]\!])$. The valuation ord extends uniquely to a valuation on a fixed algebraic closure of E and to its completion C. We still denote it by ord and view F as a subfield of C. The absolute Galois group of E acts on C by isometries. The action on F is trivial because this is the completion of a purely inseparable extension of E.

Set $h = \sum_{\alpha \leq (i-1)/(p^h-1)} c_\alpha X^\alpha$ and consider the polynomial

$$H(T) = h(T^{p^h}) - X \in k[\![X]\!][T] \subset E[T].$$

Note that $\operatorname{ord}(g) = 1 < \nu$ whence $i > p^h$ and $(i-1)/(p^h-1) > \nu$. This gives $i \leq \deg(H) = m$. If n denotes the largest integer less than ν the minimality

of ν implies

$$H(T) = \sum_{j=1}^{n} c_j T^{jp^h} + c_\nu T^i + \sum_{j=i+1}^{m} c_{j/p^h} T^j - X.$$

Since $H'(T) \in k[T]$ the roots of H' in C are 0 or of order 1. No such element is a root of H so that H is separable over E. Since $H'(T) = ic_\nu T^{i-1}G(T)$ with $G \in k[T]$ and $G(0) \neq 0$ we have $\mathrm{ord}(H'(\beta)) = (i-1)\mathrm{ord}(\beta)$ for all $\beta \in C$ with $\mathrm{ord}(\beta) > 0$.

Since $\mathrm{ord}(g) = 1$ we have $c_1 \in k^\times$. Therefore, the reduction $\overline{H} = H \mod (X)$ satisfies $\overline{H}(T) = T^{p^h} \cdot \overline{H}_2(T)$ for some polynomial $\overline{H}_2 \in k[T]$ of degree $m - p^h$ with $\overline{H}_2(0) = c_1 \neq 0$. In particular, T^{p^h} and $\overline{H}_2$ are relatively prime. By Hensel's lemma the decomposition lifts to a decomposition $H = H_1 \cdot H_2$ in $k[\![X]\!][T]$ with H_1 monic of degree p^h. In particular, $H_2(0) \in k[\![X]\!]^\times$ and $\mathrm{ord}(H_1(0)) = \mathrm{ord}(H(0)) = 1$. Moreover, the coefficients of H_1 lie in $Xk[\![X]\!]$ except for the leading one. Therefore, H_1 is an Eisenstein polynomial, hence is irreducible. Since it divides H it is also separable over E.

Let $\alpha_1, \ldots, \alpha_{p^h} \in C$ be the roots of $H_1(T) = \prod_{j=1}^{p^h}(T - \alpha_j)$. Note that these are Galois conjugate because H_1 is irreducible. Thus, they all have the same order. Since $1 = \mathrm{ord}(H_1(0)) = \sum_{j=1}^{p^h} \mathrm{ord}(\alpha_j)$ we get $\mathrm{ord}(\alpha_j) = 1/p^h$ for all j. Note also that $\mathrm{ord}(H_2(f^{1/p^h})) = 0$ because the constant term of H_2 is a unit and $\mathrm{ord}(f^{1/p^h}) > 0$. This implies $\mathrm{ord}(H_1(f^{1/p^h})) = \mathrm{ord}(H(f^{1/p^h}))$.

Moreover, $H'(\alpha_1) = H_1'(\alpha_1)H_2(\alpha_1)$ with $\mathrm{ord}(H_2(\alpha_1)) = 0$ as above which implies $\mathrm{ord}(H_1'(\alpha_1)) = \mathrm{ord}(H'(\alpha_1)) = (i-1)/p^h$. Since the Galois action fixes f^{1/p^h} and permutes the roots of H_1 transivitely we also get $\mathrm{ord}(f^{1/p^h} - \alpha_j) = \mathrm{ord}(f^{1/p^h} - \alpha_1)$ for all $1 \leq j \leq p^h$. This implies

$$\begin{aligned} \mathrm{ord}(\alpha_1 - \alpha_j) &\geq \min\{\mathrm{ord}(f^{1/p^h} - \alpha_j), \mathrm{ord}(f^{1/p^h} - \alpha_1)\} \\ &= \mathrm{ord}(f^{1/p^h} - \alpha_j). \end{aligned}$$

Altogether, the decompositions $H_1(f^{1/p^h}) = \prod_{j=1}^{p^h}(f^{1/p^h} - \alpha_j)$ and $H_1'(\alpha_1) = \prod_{j=2}^{p^h}(\alpha_1 - \alpha_j)$ give

$$\begin{aligned} \mathrm{ord}(h(f) - X) &= \mathrm{ord}(H(f^{1/p^h})) = \mathrm{ord}(H_1(f^{1/p^h})) = \sum_{j=1}^{p^h} \mathrm{ord}(f^{1/p^h} - \alpha_j) \\ &= \frac{p^h}{p^h - 1} \sum_{j=2}^{p^h} \mathrm{ord}(f^{1/p^h} - \alpha_j) \leq \frac{p^h}{p^h - 1} \sum_{j=2}^{p^h} \mathrm{ord}(\alpha_1 - \alpha_j) \\ &= \frac{p^h}{p^h - 1} \mathrm{ord}(H_1'(\alpha_1)) = \frac{i-1}{p^h - 1}. \end{aligned}$$

By the definition of h and by Lemma 1.3 (ii) we obtain $\mathrm{ord}(g(f)-h(f)) = \mathrm{ord}(g-h) > (i-1)/p^h \geq \mathrm{ord}(h(f)-X)$. This implies $\mathrm{ord}(g(f)-X) = \mathrm{ord}(g(f)-h(f)+h(f)-X) = \mathrm{ord}(h(f)-X) \leq (i-1)/(p^h-1)$ as claimed. □

As an immediate application we obtain the following bijectivity criterion.

Corollary 1.8. *Assume that $d = 1$ and let $g \in R[\![X^{1/p^\infty}]\!]$ with $g(0) = 0$. If R is an integral domain then $\psi_g : R[\![X^{1/p^\infty}]\!] \to R[\![X^{1/p^\infty}]\!]$ is bijective if and only if $g(X) = \tilde{g}(X^{p^h})$ for some $h \in \mathbb{Z}$ and $\tilde{g} \in R[\![X]\!]$ with $\tilde{g}'(0) \in R^\times$. In this case the integer h and the power series $\tilde{g}$ are uniquely determined by g.*

Proof. The uniqueness is clear from $h = \log_p(\mathrm{ord}(g))$ and $\tilde{g}(X) = g(X^{p^h})$. By the inverse formal function theorem, the condition is clearly sufficient for the bijectivity of ψ_g. Conversely, if ψ_g is bijective then there is $f \in R[\![X^{1/p^\infty}]\!]$ with $f(g) = X$. Thus, $f(0) = 0$ and $\psi_f = \psi_g^{-1}$. Let $\alpha = \mathrm{ord}(g)$, $\beta = \mathrm{ord}(f)$ and let c_α and d_β be the corresponding coefficients of g and f, respectively. As in the proof of Lemma 1.3 (ii) we have $X = g(f) \equiv c_\alpha d_\beta^\alpha X^{\alpha\beta} \mod \mathfrak{m}_{>\alpha\beta}$. Now $c_\alpha d_\beta^\alpha \neq 0$ because R is an integral domain. This implies $X = c_\alpha d_\beta^\alpha X^{\alpha\beta}$ which gives $c_\alpha, d_\beta \in R^\times$ and $\alpha\beta = 1$ in $\mathbb{N}[\frac{1}{p}]$. In particular, we must have $\alpha = p^h$ for some $h \in \mathbb{Z}$.

Replacing g by $g(X^{1/p^h})$ we may thus assume $\mathrm{ord}(g) = \mathrm{ord}(f) = 1$. The statement is then a consequence of Theorem 1.7. □

Remark 1.9. If $g(X) = X + X^{1+\frac{1}{p}} \in \mathbb{F}_p[\![X^{1/p^\infty}]\!]$ then ψ_g is not bijective by Corollary 1.8. Still, one can run the usual algorithm and try to find $f \in \mathbb{F}_p[\![X^{1/p^\infty}]\!]$ with $g(f(X)) = X$. In fact, define $f_n(X) = \sum_{j=0}^n c_j X^{\alpha_j}$ inductively by $f_0 = X$ and $X - g(f_n(X)) \equiv c_{n+1} X^{\alpha_{n+1}} \mod \mathfrak{m}_{>\alpha_{n+1}}$ with $c_{n+1} \neq 0$. The algorithm cannot converge, i.e. the strictly increasing sequence $(\alpha_n)_{n\geq 0}$ has to be bounded. However, it seems hard to prove this directly even in this explicit example.

Under the assumptions of Corollary 1.8 the integer

$$h = \mathrm{ht}(\psi_g) = \log_p(\mathrm{ord}(g))$$

is called the height of the automorphism ψ_g. More generally, assume that $g \in R[\![X^{1/p^\infty}]\!]$ with $d = 1$ and $g(0) = 0$ where R is an arbitrary perfect ring of characteristic p. Note that if $\mathfrak{p} \in \mathrm{Spec}(R)$ is a prime ideal then also the integral domain $R/\mathfrak{p}$ is a perfect ring of characteristic p. Moreover, ψ_g induces an endomorphism of $(R/\mathfrak{p})[\![X^{1/p^\infty}]\!]$ by reducing all coefficients modulo $\mathfrak{p}$. It coincides with $\psi_{g_\mathfrak{p}}$ where $g_\mathfrak{p}$ is the image of g under the canonical ring homomorphism $R[\![X^{1/p^\infty}]\!] \to (R/\mathfrak{p})[\![X^{1/p^\infty}]\!]$. If ψ_g is bijective then so is $\psi_{g_\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Indeed, we have $\psi_g^{-1} = \psi_f$ for some $f \in R[\![X^{1/p^\infty}]\!]$ with

$f(0) = 0$ and $\psi_{f_\mathfrak{p}}$ is inverse to $\psi_{g_\mathfrak{p}}$. We then define the height of ψ_g as the map

$$\mathrm{ht}(\psi_g) : \mathrm{Spec}(R) \longrightarrow \mathbb{Z}, \quad \mathfrak{p} \mapsto \mathrm{ht}(\psi_{g_\mathfrak{p}}). \tag{9}$$

Lemma 1.10. *The height function (9) is Zariski locally constant.*

Proof. Let $\mathfrak{p}$ and $\mathfrak{q}$ be prime ideals of R with $\mathfrak{p} \subseteq \mathfrak{q}$. Then $\mathrm{ord}(g_\mathfrak{p}) = \mathrm{ord}(g_\mathfrak{q})$ because the lowest coefficient of $g_\mathfrak{p}$ is a unit in $R/\mathfrak{p}$ (cf. Lemma 1.8) and stays a unit when reducing further modulo $\mathfrak{q}$. This shows that the subset of $\mathrm{Spec}(R)$ where $\mathrm{ht}(\psi_g)$ takes a fixed constant value is closed under specialization.

Now write $g(X) = \sum_{j=0}^{\infty} c_j X^{\alpha_j}$ with $c_j \in R$ and $\alpha_j < \alpha_{j+1}$ for all $j \geq 0$. Note that any value of $\mathrm{ht}(\psi_g)$ is of the form $\log_p(\alpha_j)$ for some $j \geq 0$. Define $X_j = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathrm{ord}(g_\mathfrak{p}) = \alpha_j\}$ and note that either $X_j = \varnothing$ or $\alpha_j = p^{h_j}$ for some $h_j \in \mathbb{Z}$ (cf. Lemma 1.8). In the latter case the height function takes the constant value $\log_p(\alpha_j) = h_j$ on X_j. Therefore, it suffices to show that the sets X_j are open in $\mathrm{Spec}(R)$. We have $X_0 = D(c_0)$ and

$$X_j = V(c_0) \cap \ldots \cap V(c_{j-1}) \cap D(c_j) \tag{10}$$

for all $j > 0$ with the usual notation for principal open and closed subsets of $\mathrm{Spec}(R)$. We will show by induction on $j \geq 0$ that $\bigcap_{i=0}^{j} V(c_i)$ and X_j are both open and closed. Of course, $D(c_0) = X_0$ is open and quasi-compact, hence is constructible (cf. [3], Proposition 10.44). By the above arguments X_0 is stable under specialization, hence is closed by [3], Remark 10.46. Therefore, also $V(c_0)$ is open and closed, settling the case $j = 0$.

Now assume that the statement is true for $j-1$. Then X_j is open and quasi-compact by (10). The same arguments as above show that X_j is also closed. By the induction hypothesis, also $\bigcup_{i=0}^{j} D(c_i) = X_j \cup \bigcup_{i=0}^{j-1} D(c_i)$ is both open and closed and so is its complement $\bigcap_{i=0}^{j} V(c_i)$. □

Proposition 1.11. *Let $d = 1$ and $g \in R[\![X^{1/p^\infty}]\!]$ with $g(0) = 0$ and assume that ψ_g is bijective. If $h \in \mathbb{Z}$ denotes the minimal value of the height function $\mathrm{ht}(\psi_g)$ then $\tilde{g}(X) = g(X^{1/p^h}) \in R[\![X]\!]$. We have $\tilde{g}'(0) \in R^\times$ if and only if $\mathrm{ht}(\psi_g)$ is constant.*

Proof. Note first that the minimal value $h \in \mathbb{Z}$ exists because $\mathrm{Spec}(R)$ is quasi-compact and $\mathrm{ht}(\psi_g)$ is locally constant (cf. Lemma 1.10). To show that $\tilde{g}(X) = g(X^{p^{-h}})$ is an ordinary formal power series write $\tilde{g}(X) = \sum_{\alpha \in \mathbb{N}[\frac{1}{p}]} c_\alpha X^\alpha$ and let $\mathfrak{p} \in \mathrm{Spec}(R)$. Together with ψ_g also $\psi_{\tilde{g}}$ and $\psi_{\tilde{g}_\mathfrak{p}}$ are bijective. By Lemma 1.3 (ii) and Lemma 1.8 we have

$$p^{\mathrm{ht}(\psi_{\tilde{g}_\mathfrak{p}})} = \mathrm{ord}(\tilde{g}_\mathfrak{p}) = \mathrm{ord}(g_\mathfrak{p}(X^{p^{-h}})) = p^{-h} \cdot \mathrm{ord}(g_\mathfrak{p}) = p^{\mathrm{ht}(\psi_{g_\mathfrak{p}})-h} \geq 1$$

by the minimality of h. This implies $\mathrm{ht}(\tilde{g}_\mathfrak{p}) \geq 0$ and therefore $\tilde{g}_\mathfrak{p} \in (R/\mathfrak{p})[\![X]\!]$ by Lemma 1.8 again. This gives $c_\alpha \in \mathfrak{p}$ for all $\alpha \notin \mathbb{N}$ and all $\mathfrak{p} \in \mathrm{Spec}(R)$. Since R is reduced, the intersection of all $\mathfrak{p}$ is zero. Thus, $c_\alpha = 0$ for all $\alpha \notin \mathbb{N}$.

If $\mathrm{ht}(\psi_g)$ is constant it remains to see that the first coefficient c_1 of $\tilde{g}$ is a unit in R. Since $\mathrm{ord}(\tilde{g}_\mathfrak{p}) = p^{-h} \cdot \mathrm{ord}(g_\mathfrak{p}) = 1$ we have $c_1 \notin \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of R. This implies $c_1 \in R^\times$. Conversely, if $\tilde{g}'(0) \in R^\times$ then the lowest coefficient of $g(X) = \tilde{g}(X^{p^h})$ is a unit in R. This implies $\mathrm{ord}(g_\mathfrak{p}) = \mathrm{ord}(g) = p^h$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$, whence $\mathrm{ht}(\psi_g)$ is constant with value h. □

As a consequence we obtain the following generalization of Corollary 1.8.

Corollary 1.12. *Assume that $d = 1$ and let $g \in R[\![X^{1/p^\infty}]\!]$ with $g(0) = 0$. If R is connected then $\psi_g : R[\![X^{1/p^\infty}]\!] \to R[\![X^{1/p^\infty}]\!]$ is bijective if and only if $g(X) = \tilde{g}(X^{p^h})$ for some $h \in \mathbb{Z}$ and $\tilde{g} \in R[\![X]\!]$ with $\tilde{g}'(0) \in R^\times$. In this case the integer h is the unique value of* $\mathrm{ht}(\psi_g)$.

Proof. By the inverse formal function theorem, the condition is clearly sufficient for the bijectivity of ψ_g. Conversely, if ψ_g is bijective then $\mathrm{ht}(\psi_g)$ is constant by Lemma 1.10 because $\mathrm{Spec}(R)$ is connected. The statement then follows from Proposition 1.11. □

More generally, if ψ_g is bijective then Lemma 1.10 allows us to decompose $R = \prod_{i=1}^n R_i$ into a finite direct product of perfect rings R_i such that $\mathrm{ht}(\psi_g)$ has some constant value h_i on $\mathrm{Spec}(R_i)$. There is an induced decomposition $R[\![X^{1/p^\infty}]\!] = \prod_{i=1}^n R_i[\![X^{1/p^\infty}]\!]$ such that $\psi_g = (\psi_{g_1}, \ldots, \psi_{g_n})$ where $g = (g_1, \ldots, g_n)$ is the corresponding decomposition of g. Then $\psi_{(g_i)_\mathfrak{p}} = \psi_{g_\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R_i)$ and $\mathrm{ht}(\psi_{g_i})$ is constant. Therefore, $\tilde{g}_i(X) = g_i(X^{1/p^{h_i}}) \in R_i[\![X]\!]$ with $\tilde{g}_i'(0) \in R_i^\times$ by Proposition 1.11. Such a representation of g need not exist globally, as soon as R is disconnected.

Example 1.13. Consider the perfect ring $R = \mathbb{F}_p \times \mathbb{F}_p$ with principal idempotents $e_1 = (1,0)$ and $e_2 = (0,1)$. Then $g(X) = e_1 X + e_2 X^p$ and $f(X) = e_2 X^{1/p} + e_1 X$ satisfy $g(f) = f(g) = X$ whence $\psi_g : R[\![X^{1/p^\infty}]\!] \to R[\![X^{1/p^\infty}]\!]$ is bijective with inverse ψ_f. The height function $\mathrm{ht}(\psi_g)$ has the constant value 0 on $D(e_1)$ and the constant value 1 on $D(e_2)$. The corresponding decomposition of g over the two copies of $\mathbb{F}_p$ is $g = (X, X^p)$. Globally, g cannot be written in the form $g(X) = \tilde{g}(X^{p^h})$ with $h \in \mathbb{Z}$, $\tilde{g} \in R[\![X]\!]$ and $\tilde{g}'(0) \in R^\times$ (cf. Proposition 1.11 or a direct check). Although ψ_g is bijective on $R[\![X^{1/p^\infty}]\!]$ and although g is an ordinary formal power series of order 1 the induced endomorphism of $R[\![X]\!]$ is not bijective. Note that in this example we have $1 = \mathrm{ord}(X) = \mathrm{ord}(g(f)) > 1/p = \mathrm{ord}(g)\mathrm{ord}(f)$ in contrast to what is claimed at the beginning of the proof of [4], Theorem 1. This also shows that the extra condition on R in Lemma 1.3 (ii) and Theorem 1.7 is really necessary.

We also include the following result which probably admits a more direct proof.

Corollary 1.14. *Assume that $d = 1$ and let $g \in R[\![X^{1/p^\infty}]\!]$ with $g(0) = 0$. Then ψ_g is bijective if and only if $\psi_{g_\mathfrak{p}}$ is bijective for all $\mathfrak{p} \in \mathrm{Spec}(R)$.*

Proof. If ψ_g is bijective then $\psi_g^{-1} = \psi_f$ for some $f \in R[\![X^{1/p^\infty}]\!]$ and $\psi_{f_\mathfrak{p}}$ is inverse to $\psi_{g_\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Conversely, if all $\psi_{g_\mathfrak{p}}$ are bijective one can define the height function $\mathrm{ht}(\psi_g) : \mathrm{Spec}(R) \to \mathbb{Z}$ as in (9). The proof of Lemma 1.10 then goes through because the bijectivity of ψ_g is never used. Decomposing R as above we may assume that $\mathrm{ht}(\psi_g)$ is constant with value h. Setting $\tilde{g}(X) = g(X^{1/p^h})$ we have $\tilde{g}_\mathfrak{p} \in (R/\mathfrak{p})[\![X]\!]$ and $\tilde{g}'_\mathfrak{p}(0) \in (R/\mathfrak{p})^\times$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$ by Lemma 1.8. Since R is reduced this implies $\tilde{g} \in R[\![X]\!]$ and $\tilde{g}'(0) \in R^\times$. But then $\psi_{\tilde{g}}$ is bijective by the formal inverse function theorem and so is ψ_g. □

A posteriori, being an automorphism of $R[\![X^{1/p^\infty}]\!]$ is Zariski local on $\mathrm{Spec}(R)$ in the following more classical sense. Note that if $\mathfrak{p} \in \mathrm{Spec}(R)$ then the localization $R_\mathfrak{p}$ is again a perfect ring. Given $g \in R[\![X^{1/p^\infty}]\!]$ we denote by $g_{(\mathfrak{p})}$ its image under the canonical ring homomorphism $R[\![X^{1/p^\infty}]\!] \to R_\mathfrak{p}[\![X^{1/p^\infty}]\!]$.

Corollary 1.15. *Assume that $d = 1$ and let $g \in R[\![X^{1/p^\infty}]\!]$ with $g(0) = 0$. Then ψ_g is bijective if and only if $\psi_{g_{(\mathfrak{p})}}$ is bijective for all $\mathfrak{p} \in \mathrm{Spec}(R)$.*

Proof. As before it suffices to show that the condition is sufficient. Thus, let us assume that all $\psi_{g_{(\mathfrak{p})}}$ are bijective. Write $g = \sum_{j=0}^\infty c_j X^{\alpha_j}$ with $\alpha_j < \alpha_{j+1}$ and $c_j \in R$ for all $j \geq 0$. Then $\mathrm{ord}(g_{(\mathfrak{p})}) = \alpha_0$ for all $\mathfrak{p} \in D(c_0)$. Since any local ring is connected we have $\alpha_0 = p^h$ and $g_{(\mathfrak{p})}(X^{1/p^h}) \in R_\mathfrak{p}[\![X]\!]$ for some $h \in \mathbb{Z}$ by Corollary 1.12. Note that α_0 and hence h are independent of $\mathfrak{p} \in D(c_0)$ and that the canonical map $R_0 = R_{c_0} \to \prod_{\mathfrak{p} \in D(c_0)} R_\mathfrak{p}$ is injective. If g_0 denotes the image of g under the induced map $R[\![X^{1/p^\infty}]\!] \to R_0[\![X^{1/p^\infty}]\!]$ we obtain $g_0(X^{1/p^h}) \in R[\![X]\!]$ with lowest coefficient $c_0 \in R_0^\times$. It follows from the formal inverse function theorem that ψ_{g_0} is bijective.

For any prime ideal $\mathfrak{p} \in V(c_0)$ we have $c_0 \notin R_\mathfrak{p}^\times$. Since the local ring $R_\mathfrak{p}$ is connected the lowest coefficient of $g_{(\mathfrak{p})}$ is a unit in $R_\mathfrak{p}$ by Corollary 1.12. Thus, $c_0 = 0$ in $R_\mathfrak{p}$ and there is $s \in R \setminus \mathfrak{p}$ with $sr = 0$ in R. This implies $c_0 = 0$ in $R_\mathfrak{q}$ and hence $c_0 \in \mathfrak{q}$ for any $\mathfrak{q} \in D(s)$. We get that $D(s) \subseteq V(c_0)$ is an open neighborhood of $\mathfrak{p}$. Since $\mathfrak{p}$ was arbitrary $V(c_0)$ is an open subset of $\mathrm{Spec}(R)$. Setting $R'_0 = R/c_0R$ it follows that the canonical ring homomorphism $R \to R_0 \times R'_0$ is bijective and that both factors are again perfect. We obtain corresponding decompositions $g = (g_0, g'_0)$ and $\psi_g = (\psi_{g_0}, \psi_{g'_0})$ for which ψ_{g_0} is bijective by the first part of the proof.

Proceeding inductively we construct decompositions $R \cong R_0 \times \ldots \times R_n \times R'_n$ for any $n \geq 0$ such that $R'_n = R/(c_0, \ldots, c_n)$ and such that if $g = (g_0, \ldots, g_n, g'_n)$ denotes the corresponding decomposition of g then ψ_{g_j} is bijective for all $0 \leq j \leq n$. Let $I \subseteq R$ be the ideal generated by the coefficients of g. If I were a proper ideal we could choose a prime ideal $\mathfrak{m} \in \mathrm{Spec}(R)$ with $I \subseteq \mathfrak{m}$. But then none of the coefficients of $g_{(\mathfrak{m})}$ would be a unit in $R_{\mathfrak{m}}$ and $\psi_{g_{(\mathfrak{m})}}$ could not be bijective by Corollary 1.12. Thus, $I = R$ which implies $(c_0, \ldots, c_n) = R$ for some $n \geq 0$ and $R'_n = 0$. Thus, $R \cong R_0 \times \ldots \times R_n$ and the bijectivity of $\psi_{g_0}, \ldots, \psi_{g_n}$ implies that of ψ_g. □

2 Perfect formal group laws

Let Set^* denote the category of pointed sets. For any integer $d \geq 1$ we have the functor

$$\mathrm{Nil}^d : \mathrm{Perf}_R^{ad} \longrightarrow \mathrm{Set}^*, \quad S \mapsto (S^{\circ\circ})^d, \tag{11}$$

with $0 = (0, \ldots, 0) \in (S^{\circ\circ})^d$ as the distinguished element. As seen in Proposition 1.2 it is represented by $R[\![X^{1/p^\infty}]\!]$ with $X = (X_1, \ldots, X_d)$.

Definition 2.1. *A d-dimensional perfect formal group law over R is a family $G = (G_1, \ldots, G_d) \in R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]^d$ of d perfect formal power series $G_i(X, Y)$ in $2d$ variables $(X, Y) = (X_1, \ldots, X_d, Y_1, \ldots, Y_d)$ such that*

(i) $G(X, 0) = X$ *in* $R[\![X^{1/p^\infty}]\!]^d$ *and*

(ii) $G(G(X, Y), Z) = G(X, G(Y, Z))$ *in* $R[\![X^{1/p^\infty}, Y^{1/p^\infty}, Z^{1/p^\infty}]\!]^d$.

A perfect formal group law G is called commutative if

(iii) $G(X, Y) = G(Y, X)$ *in* $R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]^d$.

Here we use the usual convention $G(f, f') = (G_1(f, f'), \ldots, G_d(f, f'))$ for the substitution of $f = (f_1, \ldots, f_d)$ and $f' = (f'_1, \ldots, f'_d)$ and set $Z = (Z_1, \ldots, Z_d)$. Of course, any ordinary d-dimensional (commutative) formal group law over R is a (commutative) perfect formal group law in the sense of Definition 2.1. Since we will only be interested in the commutative case, we will simply speak of perfect formal group laws in the following.

Let G be a d-dimensional perfect formal group law over R. Given $S \in \mathrm{Perf}_R^{ad}$ it functorially turns the set $\mathrm{Nil}^d(S) = (S^{\circ\circ})^d$ into a monoid $G(S)$ with zero element $0 = (0, \ldots, 0)$ via $s +_G t = G(s, t)$. If G is commutative then so is the monoid $G(S)$.

Proposition 2.2. *Let $\mathcal{G}$ be a functor from Perf_R^{ad} to the category of monoids whose composition with the forgetful functor into Set^* isomorphic to Nil^d.*

(i) *There is a unique perfect formal group law G of dimension d over R such that the addition in the monoid $\mathcal{G}(S) = (S^{\circ\circ})^d$ is given by $s + t = s +_G t = G(s,t)$ functorially in S for all $S \in \mathrm{Perf}_R^{ad}$.*

(ii) *The functor $\mathcal{G}$ takes values in the category of commutative monoids if and only if G is commutative.*

(iii) *If $\mathcal{G}$ takes values in the category* Ab *of abelian groups then there is a unique family $\iota = (\iota_1, \ldots, \iota_d) \in R[\![X^{1/p^\infty}]\!]^d$ with $\iota(0) = 0$ such that the inversion in $\mathcal{G}(S) = (S^{\circ\circ})^d$ is given by $-s = \iota(s)$ functorially in S for all $S \in \mathrm{Perf}_R^{ad}$.*

Proof. Set $S = R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$ and define $G = X + Y$ in $\mathcal{G}(S)$ noting that $X, Y \in (R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]^{\circ\circ})^d$. It then follows from the axioms of the monoid $\mathcal{G}(S)$ that G is a perfect formal group law. Under the assumptions in (iii) set $S = R[\![X^{1/p^\infty}]\!]$ and define $\iota = -X$ in $\mathcal{G}(S)$. All of the remaining statements then follow from the fact that the underlying functor of $\mathcal{G}$ into pointed sets is represented by $R[\![X^{1/p^\infty}]\!]$. □

In the situation of Proposition 2.2 we have $G(X, \iota(X)) = 0$. If $G \in R[\![X,Y]\!]^d$ is an ordinary formal group law over R then the existence of $\iota \in R[\![X]\!]^d$ with $\iota(0) = 0$ and $G(X, \iota(X)) = 0$ is already implied by the axioms in Definition 2.1. Thus, in the ordinary case $G(S)$ is automatically an abelian group and not only a commutative monoid. In the one-dimensional perfect case, we shall see that the existence of ι is automatic, as well (cf. Corollary 2.6 (ii)).

Definition 2.3. *Let G and H be perfect formal group laws over R of dimensions d and e, respectively. A homomorphism $f : G \to H$ is a family $f = (f_1, \ldots, f_e)$ of elements $f_i \in R[\![X^{1/p^\infty}]\!]$ in d-variables $X = (X_1, \ldots, X_d)$ such that $f(0) = 0$ and $f(G(X,Y)) = H(f(X), f(Y))$ in $R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]^e$ where $Y = (Y_1, \ldots, Y_d)$.*

In the situation of Definition 2.3 we shall write $\mathrm{Hom}_R(G,H)$ for the set of homomorphisms from G to H. If we define the composition of homomorphisms via substitution then perfect formal group laws over R form a category $\mathrm{FGL}_R^{\mathrm{perf}}$ with $id_G = X$. Via $+_H$ the set $\mathrm{Hom}_R(G,H)$ is in fact a commutative monoid and $\mathrm{End}_R(G) = \mathrm{Hom}_R(G,G)$ is a semiring. Note that there is a unique homomorphism

$$\mathbb{N} \longrightarrow \mathrm{End}_R(G), \quad m \mapsto [m]_G,$$

of semirings which can be constructed inductively via $[0](X) = 0$, $[1](X) = X$ and $[m+1](X) = G([m]_G(X), X)$ for all $m \in \mathbb{N}$.

Lemma 2.4. *If G and H are perfect formal group laws over R of dimensions d and e, respectively, then $\mathrm{Hom}_R(G,H)$ is complete for the topology induced by the X-adic topology on $R[\![X^{1/p^\infty}]\!]^e$.*

Proof. Let $(f^{(n)})_{n\in\mathbb{N}} = ((f_1^{(n)},\dots,f_e^{(n)}))_{n\in\mathbb{N}}$ be sequence of homomorphisms $f^{(n)}: G \to H$ which is an X-adic Cauchy sequence and let $f = (f_1,\dots,f_d) = \lim_{n\to\infty} f^{(n)} = (\lim_{n\to\infty} f_1^{(n)},\dots,\lim_{n\to\infty} f_e^{(n)}) \in R[\![X^{1/p^\infty}]\!]^e$. By the continuity of the substitution homomorphism ψ_G and by the continuity of $h \mapsto H_i(h(X),h(Y))$ (cf. Lemma 1.6) we have $f_i(G(X,Y)) - H_i(f(X),f(Y)) = \lim_{n\to\infty}(f_i^{(n)}(G(X,Y)) - H_i(f^{(n)}(X),f^{(n)}(Y))) = 0$ for $1 \le i \le e$. □

For the following discussion we fix a one-dimensional perfect formal group law $G = G(X,Y)$ over R. Write

$$G(X,Y) = \sum_{\alpha,\beta\in\mathbb{N}[\frac{1}{p}]} c_{\alpha\beta} X^\alpha Y^\beta$$

with $c_{\alpha\beta} \in R$ and let $G = \sum_{\nu\in\mathbb{N}[\frac{1}{p}]} G_\nu$ be the decomposition of G into its homogeneous components. For any $\alpha \in \mathbb{N}[\frac{1}{p}]$ write $G(X,Y)^\alpha = \sum_\beta f_{\alpha\beta}(X)Y^\beta$ with $f_{\alpha\beta} \in R[\![X^{1/p^\infty}]\!]$. The law of associativity gives

$$\begin{aligned}\sum_\beta f_{\alpha\beta}(G(X,Y))Z^\beta &= G(G(X,Y),Z)^\alpha = G(X,G(Y,Z))^\alpha \\ &= \sum_\delta f_{\alpha\delta}(X)G(Y,Z)^\delta = \sum_{\gamma,\delta} f_{\alpha\delta}(X)f_{\delta\gamma}(Y)Z^\gamma\end{aligned}$$

whence

$$f_{\alpha\beta}(G(X,Y)) = \sum_\delta f_{\alpha\delta}(X)f_{\delta\beta}(Y) \tag{12}$$

in $R[\![X^{1/p^\infty},Y^{1/p^\infty}]\!]$ for all $\alpha,\beta \in \mathbb{N}[\frac{1}{p}]$.

It follows from Definition 2.1 (i) and (iii) that the perfect formal power series G satisfies $G(X,Y) = X+Y+\sum_{\alpha,\beta>0} c_{\alpha\beta}X^\alpha Y^\beta$, i.e. except for $X+Y$ it has only mixed terms. We will use the relations (12) to prove the following strengthening. An even stronger result is claimed in [1], Lemma 4.12. The first part of our proof is taken from [1], Proposition 4.20. It says that the ideal $(X) \subset R[\![X^{1/p^\infty}]\!]$ is a topological coideal for the topological Hopf algebra structure on $R[\![X^{1/p^\infty}]\!]$ induced by G.

Lemma 2.5. *If G is a one-dimensional perfect formal group law over R then $G(X,Y) \in (X,Y)$, i.e. if $\alpha,\beta \in \mathbb{N}[\frac{1}{p}]$ with $c_{\alpha\beta} \neq 0$ then $\alpha \ge 1$ or $\beta \ge 1$. In particular,* $\operatorname{ord}(G) = 1$ *and $G_1(X,Y) = X+Y$.*

Proof. We need to see $c_{\alpha\beta} = 0$ whenever $\alpha < 1$ and $\beta < 1$. Since R is reduced this can be checked after reduction modulo the various prime ideals of R. We may therefore assume that R is an integral domain. Passing to its field of fractions we may even assume that $R = k$ is field. In this case $k[\![X^{1/p^\infty}]\!]$ is a valuation ring.

Consider the ideal $I = (f_{1\beta})_{\beta<1} \subset k[\![X^{1/p^\infty}]\!]$ and note that $(X) \subseteq I$ because $f_{10} = X$. Moreover, $f_{1\beta} = \sum_\alpha c_{\alpha\beta} X^\alpha$ and there are only finitely many α, β with $\alpha < 1$, $\beta < 1$ and $c_{\alpha\beta} \neq 0$. Thus, $f_{1\beta} \in (X)$ for almost all $\beta < 1$ and I is finitely generated. Finally, if $\beta \neq 1$ then $f_{1\beta} \in \mathfrak{m}$ whence I is not the unit ideal. Altogether, we obtain $I = (X^\nu)$ for some $0 < \nu \leq 1$.

We claim that $G(X,Y)^\nu \in (X^\nu, Y^\nu)$ and need to show $f_{1\beta}(G(X,Y)) \in (X^\nu, Y^\nu)$ for all $\beta < 1$. By (12) it suffices to show $f_{\delta\beta} \in I$ whenever $\beta < 1 \leq \delta$. But if $\delta \geq 1$ the equality

$$\begin{aligned}\sum_\beta f_{\delta\beta}(X)Y^\beta &= G(X,Y)^\delta = G(X,Y)\cdot G(X,Y)^{\delta-1} \\ &= (\sum_\mu f_{1\mu}(X)Y^\mu)\cdot(\sum_\gamma f_{\delta-1,\gamma}(X)Y^\gamma) \\ &= \sum_\beta(\sum_{\mu+\gamma=\beta} f_{1\mu}(X) f_{\delta-1,\gamma}(X))Y^\beta\end{aligned}$$

gives $f_{\delta\beta} = \sum_{\mu+\gamma=\beta} f_{1\mu} f_{\delta-1,\gamma}$. If $\mu + \gamma = \beta < 1$ then also $\mu < 1$ and we get $f_{\delta\beta} \in I$ as desired. Writing $\nu = i/p^h$ with $h \in \mathbb{Z}$ and $i \in \mathbb{N} \setminus p\mathbb{N}$ we get $G(X,Y)^i \in (X^i, Y^i)$ and need to show $i = 1$.

If $\nu_0 = \operatorname{ord}(G)$ then $G(X,Y)^i \equiv G_{\nu_0}(X,Y)^i \mod \mathfrak{m}_{>i\nu_0}$ by Lemma 1.5. Further, $\operatorname{ord}(G_{\nu_0}(X,Y)^i) = i\nu_0$ and $G_{\nu_0}(X,Y)^i$ is the homogeneous component of $G(X,Y)^i$ of lowest degree. Together with $G(X,Y)^i$ all of its homogeneous components lie in (X^i, Y^i). In particular, we get $G_{\nu_0}(X,Y)^i \in (X^i, Y^i)$.

Let us first assume $\nu_0 < 1$. Then G_{ν_0} consists only of mixed terms. If $X^\alpha Y^{\nu_0-\alpha}$ is the unique monomial of G_{ν_0} with the smallest power of X then $X^{i\alpha}Y^{i(\nu_0-\alpha)}$ is one of the monomials of $G^i_{\nu_0}$. Since $\alpha < \nu_0 < 1$ and $\nu_0 - \alpha < \nu_0 < 1$ this does not lie in (X^i, Y^i). This contradiction implies $\nu_0 = 1$. If the monomial of G_1 with the smallest positive power of X is of the form $X^\alpha Y^{1-\alpha}$ with $0 < \alpha < 1$ then $Y^{i-1}X^\alpha Y^{1-\alpha} = X^\alpha Y^{i-\alpha}$ is one of the monomials of G^i_1. Since $\alpha < 1 \leq i$ and $i - \alpha < i$ this does not lie in (X^i, Y^i). This contradiction implies $G_1(X,Y) = X + Y$. But since $i \neq 0$ in k we have $(X+Y)^i \in (X^i, Y^i)$ if and only if $i = 1$. □

Corollary 2.6. *If G is a one-dimensional perfect formal group law over R then the following statements hold.*

(i) For any $m \in \mathbb{N}$ we have $[m]_G(X) \equiv mX \mod \mathfrak{m}_{>1}$.

(ii) The limit $\iota(X) = \lim_{n\to\infty}[p^n - 1]_G(X)$ exists in $\operatorname{End}_R(G)$ and satisfies $G(X, \iota(X)) = 0$. In particular, $G(S)$ is an abelian group with inversion $-s = \iota(s)$ for all $s \in S$ functorially in $S \in \operatorname{Perf}_R^{ad}$.

(iii) The homomorphism $\mathbb{N} \to \mathrm{End}_R(G)$ extends to a continuous ring homomorphism $\mathbb{Z}_p \to \mathrm{End}_R(G)$ still denoted by $m \mapsto [m]_G(X)$. Its kernel is zero or the ideal generated by p.

(iv) If $m \in \mathbb{Z}_p^\times$ then $[m]_G(X) \in R[\![X]\!]$ is an ordinary formal power series with $[m]'_G(0) \in R^\times$.

Proof. Part (i) is proved by induction on $m \geq 0$, the cases $m = 0$ and $m = 1$ being clear. Let the statement be true for m. By Lemma 2.5 we may write $G(X,Y) = X + Y + \rho(X,Y)$ with $\mathrm{ord}(\rho) > 1$. Then $\mathrm{ord}(\rho(X,[m]_G(X))) \geq \mathrm{ord}(\rho) > 1$ by Lemma 1.3 (i) and the induction hypothesis. This gives $[m+1]_G(X) = G(X,[m]_G(X)) = X + [m]_G(X) + \rho(X,[m]_G(X)) \equiv (m+1)X \mod \mathfrak{m}_{>1}$.

Since $pR = 0$ we obtain $\mathrm{ord}([p]_G(X)) > 1$ and $\lim_{n\to\infty}[(p-1)p^n]_G(X) = 0$ in the X-adic topology by Lemma 1.3. For any $n \in \mathbb{N}$ let us set $\iota_n(X) = [p^n - 1]_G(X)$ and note that $\mathrm{ord}(\iota_n) \geq 1$ by (i). Since ρ consists of mixed terms we have $\lim_{n\to\infty} \rho(\iota_n(X), [(p-1)p^n]_G(X)) = 0$. As

$$\begin{aligned} \iota_{n+1}(X) &= G(\iota_n(X), [(p-1)p^n]_G(X)) \\ &= \iota_n(X) + [(p-1)p^n]_G(X) + \rho(\iota_n(X), [(p-1)p^n]_G(X)) \end{aligned}$$

we see that $(\iota_n)_{n\in\mathbb{N}}$ is an X-adic Cauchy sequence. Therefore, the limit $\iota(X)$ exists in $R[\![X^{1/p^\infty}]\!]$ and is an endomorphism of G by Lemma 2.4. By Lemma 1.6 we have

$$\begin{aligned} G(X, \iota(X)) &= G(X, \lim_{n\to\infty} \iota_n(X)) = \lim_{n\to\infty} G(X, \iota_n(X)) \\ &= \lim_{n\to\infty} [p^n]_G(X) = 0. \end{aligned}$$

This proves (ii). In particular, $\mathrm{End}_R(G)$ is not only a semiring but a (not necessarily commutative) ring. Therefore, the map $\mathbb{N} \to \mathrm{End}_R(G)$ extends to a ring homomorphism $\mathbb{Z} \to \mathrm{End}_R(G)$. By the arguments already given, it is continuous for the p-adic topology on $\mathbb{Z}$ and extends to $\mathbb{Z}_p$ as required. If the kernel of $\mathbb{Z}_p \to \mathrm{End}_R(G)$ is non-zero there is a positive integer n with $[p^n]_G(X) = 0$. Assume that $\nu = \mathrm{ord}([p](X)) < \infty$ and let c denote the lowest coefficient of $[p]_G(X)$. Then $0 = [p^n]_G(X) \equiv c^\mu X^{n\nu} \mod \mathfrak{m}_{>n\nu}$ for some $\mu \in \mathbb{N}[\frac{1}{p}]$. This implies $c = 0$ because R is reduced, leading to a contradiction.

If $m \in \mathbb{Z}_p^\times$ then the substitution homomorphism $\psi_{[m]_G}$ is bijective with inverse $\psi_{[m^{-1}]_G}$. Note that $\mathrm{ord}([m]_G) = 1$ and that the lowest coefficient of $[m]_G(X)$ is a unit in R by (i). In fact, this is the image of m under the canonical ring homomorphism $\mathbb{Z}_p \to \mathbb{F}_p \to R$. Therefore, the height function of $\psi_{[m]_G}$ is zero and it follows from Proposition 1.11 that $[m]_G(X) \in R[\![X]\!]$. $\square$

We continue to denote by G a one-dimensional perfect formal group law over R. Consider the discrete R-algebra $A = R[\![X^{1/p^\infty}]\!]/(X)$ and note that the canonical map

$$A \otimes_R A = R[\![X^{1/p^\infty}]\!]/(X) \otimes_R R[\![Y^{1/p^\infty}]\!]/(Y) \longrightarrow R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]/(X,Y)$$

is an isomorphism. We will use it to identify these two rings. Since the power series $\iota(X) = [-1]_G(X) \in R[\![X]\!]$ has order 1 by Corollary 2.6 the automorphism ψ_ι of $R[\![X^{1/p^\infty}]\!]$ induces an automorphism

$$\iota : A \to A, \quad f + (X) \mapsto f(\iota(X)) + (X),$$

of A by Lemma 1.3 (i) satisfying $\iota \circ \iota = \mathrm{id}_A$. By Lemma 2.5 the substitution homomorphism $\psi_G : R[\![X^{1/p^\infty}]\!] \to R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$ induces a homomorphism of R-algebras

$$\Delta : A \longrightarrow A \otimes_R A, \quad f + (X) \mapsto f(G(X,Y)) + (X,Y).$$

Finally, consider the structure map $R \to A$ and the augmentation $A \to R$ sending $f + (X)$ to $f(0)$. It then follows from the properties of $G(X,Y)$ and $\iota(X)$ that the above data make A a cocommutative Hopf algebra over R.

Theorem 2.7. *If $G \in R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$ is a one-dimensional perfect formal group law over R then $G \in R[\![X,Y]\!]$, i.e. any one-dimensional perfect formal group law over R is an ordinary formal group law.*

Proof. Writing $G(X,Y) = \sum_{\alpha,\beta \in \mathbb{N}[\frac{1}{p}]} c_{\alpha\beta} X^\alpha Y^\beta$ we need to see $c_{\alpha\beta} = 0$ unless $\alpha, \beta \in \mathbb{N}$. Since R is reduced this can be checked after reduction modulo the various prime ideals $\mathfrak{p}$ of R. Passing to the fraction field of $R/\mathfrak{p}$ we may thus assume that $R = k$ is a perfect field of characteristic p.

Note that $A = \bigcup_{n \geq 0} A_n$ is the increasing union of the local subrings $A_n = k[\![X^{1/p^n}]\!]/(X)$ of k-dimension p^n. Let m be an integer with $m \geq 3$. By [8], Theorem 3.3, there is a Hopf subalgebra B of A which is finitely generated as a k-algebra and which contains the class of X^{1/p^m}. Then B is finite dimensional over k and a local ring. By [8], Theorem 14.4, there is an isomorphism

$$B \cong k[T_1, \ldots, T_d]/(T_1^{p^{n_1}}, \ldots, T_d^{p^{n_d}})$$

of k-algebras. Renumbering the variables we may assume $1 \leq n_1 \leq \ldots \leq n_d$. Choosing representatives $T_j = G_j + (X)$ with $G_j \in \mathfrak{m} \subset k[\![X^{1/p^\infty}]\!]$ we have $1/p^{n_j} \leq \mathrm{ord}(G_j) < 1/(p^{n_j} - 1)$ because the index of the nilpotent element T_j is p^{n_j}. The elements $\prod_{j=1}^d T_j^{\alpha_j}$ with $0 \leq \alpha_j < p^{n_j}$ for $1 \leq j \leq d$ form a k-basis of B. If $d \geq 2$ we get that the nilpotent element $T_1 T_2$ has index p^{n_1}. However,

$$\mathrm{ord}(G_1 G_2) \geq \frac{1}{p^{n_1}} + \frac{1}{p^{n_2}} \geq 2\frac{1}{p^{n_1}} \geq \frac{1}{p^{n_1} - 1}$$

shows $(T_1T_2)^{p^{n_1-1}} = 0$. This contradiction implies $d = 1$, i.e. we have $B = k[T]/(T^{p^n})$ for some $n \geq 1$ and write $T = G+(X)$. Since $X^{1/p^m}+(X) \in B$ there is a polynomial $F \in k[X]$ with $F(G) \equiv X^{1/p^m} \mod \mathfrak{m}_{\geq 1} = Xk[\![X^{1/p^\infty}]\!]$. This implies $p^m \cdot \mathrm{ord}(F) \cdot \mathrm{ord}(G) = 1$ with $\mathrm{ord}(F) \in \mathbb{N}$ and $\mathrm{ord}(G) \in \mathbb{N}[\frac{1}{p}]$. The unique prime factorization in $\mathbb{N}$ gives $\mathrm{ord}(G) = 1/p^\ell$ and $\mathrm{ord}(F) = p^{\ell-m}$ for some integer $\ell \geq m$. But then $\ell = n$ by the above bounds on $\mathrm{ord}(G)$.

Setting $g = G^{p^n}$ and $f(X) = F(X^{1/p^n})^{p^m}$ the elements $f, g \in k[\![X^{1/p^\infty}]\!]$ are both of order 1 and satisfy $f(g) = F(G)^{p^m} \equiv X \mod \mathfrak{m}_{\geq p^m}$. Theorem 1.7 then yields $g \in k[\![X]\!] + \mathfrak{m}_{>p^m/c}$ for some real constant $1 < c < 8$. In particular, $g \in k[\![X]\!] + \mathfrak{m}_{\geq p^{m-3}}$ and equivalently $T^{p^{n-m+3}} \in A_{m-3}$. However, the k-subalgebra of $B = k[T]/(T^{p^n})$ generated by $T^{p^{n-m+3}}$ has k-dimension $m-3$. Since this is the k-dimension of A_{m-3} we obtain $A_{m-3} = k[T^{p^{n-m+3}}]/(T^{p^n}) = B^{p^{n-m+3}}$ which is a Hopf subalgebra of A.

Since $m \geq 3$ was arbitrary we get that A_m is a Hopf subalgebra of A for any $m \geq 0$. In particular, we have $\Delta(X^{1/p^m}) = G(X,Y)^{1/p^m} + (X,Y) \in k[\![X^{1/p^m}, Y^{1/p^m}]\!]/(X,Y)$ and hence $G(X,Y) \in k[\![X,Y]\!] + (X^{p^m}, Y^{p^m})$ for any $m \geq 0$. This implies $G(X,Y) \in k[\![X,Y]\!]$ as claimed. □

Remark 2.8. A posteriori, it follows that any one-dimensional perfect formal group law G over R is automatically commutative, i.e. if $d = 1$ then the condition in Definition 2.1 (iii) is automatic (cf. [6], Théorème 1, noting that R is reduced).

We pass back to a more general situation and denote by $G_0 \in R[\![X,Y]\!]^d$ a d-dimensional ordinary formal group law over R. By the same symbol we denote the functor $G_0 : \mathrm{Alg}_R^{ad} \to \mathrm{Ab}$ represented by $R[\![X]\!]$. We write G instead of G_0 if this is viewed as a perfect formal group law, i.e. as an element of $R[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]^d$. It follows from Proposition 1.2 (ii) that the restriction of G_0 to Perf_R^{ad} is isomorphic to G.

By abuse of notation we write $\varphi^n = \varphi^n(X) = X^{p^n} = (X_1^{p^n}, \ldots, X_d^{p^n})$ so that $\varphi \in \mathrm{Hom}_R(G_0^{(p^{n-1})}, G_0^{(p^n)})$ for any $n \in \mathbb{Z}$. Similarly, if $S \in \mathrm{Alg}_R^{ad}$ and $s = (\sigma_1, \ldots, \sigma_d) \in G(S)$ then we write $s^p = (\sigma_1^p, \ldots, \sigma_d^p) = G(\varphi)(s)$. We define the functor $G_0^\flat = \varprojlim_\varphi G_0^{(p^{-n})} : \mathrm{Alg}_R^{ad} \to \mathrm{Ab}$ via

$$G_0^\flat(S) = \{(s_n)_{n\geq 0} \in \prod_{n\geq 0} G_0^{(p^{-n})}(S) \mid s_{n+1}^p = s_n \text{ for all } n \geq 0\}$$

and call $G_0^\flat$ the perfection of G_0. It comes with a natural transformation $G_0^\flat \to G_0$ given by $(s_n)_{n\geq 0} \mapsto s_0$ on S-valued points.

Proposition 2.9. *There is an isomorphism of functors $G \circ (\cdot)^\flat \cong G_0^\flat$. In particular, $G_0^\flat$ is represented by $R[\![X^{1/p^\infty}]\!]$. On Perf_R^{ad} the natural transformation $G_0^\flat \to G_0$ is an isomorphism, i.e. the restriction of $G_0^\flat$ to Perf_R^{ad} is given by the perfect formal group law G.*

Proof. The first statement is simply the universal property of the projective limit. That $G_0^\flat$ is represented by $R[\![X^{1/p^\infty}]\!]$ then follows from Proposition 1.2 (iii). If $S \in \mathrm{Perf}_R^{ad}$ then the map $G_0(S^\flat) = G(S^\flat) \cong G_0^\flat(S) \to G_0(S)$ is obtained by applying G_0 to the projection $S^\flat \to S$ which is an isomorphism by Proposition 1.2 (i). We noted above that the restriction of G_0 to Perf_R^{ad} is isomorphic to G, giving the final statement. Alternatively, it follows directly from $G \circ (\cdot)^\flat \cong G_0^\flat$ because the restriction of $(\cdot)^\flat$ to Perf_R^{ad} is isomorphic to the identity functor (cf. Proposition 1.2 (i)). □

The role of the affine group scheme $\mathrm{Spec}(A)$ introduced before Theorem 2.7 can now be explained as follows. We continue to denote by G_0 a d-dimensional ordinary formal group law over R. For any integer $n \geq 0$ consider the n-th Frobenius kernel $G_0[\varphi^n] = \ker(\varphi^n : G_0 \to G_0^{(p^n)})$. Then $G_0[\varphi^n]$ is a finite flat group scheme represented by $R[\![X]\!]/(X^{p^n}) = R[\![X]\!]/(X_1^{p^n}, \ldots, X_d^{p^n})$. The relative Frobenius $R[\![X]\!]/(X^{p^{n+1}}) \to R[\![X]\!]/(X^{p^n})$ can be identified with the inclusion $R[\![X^{1/p^{n+1}}]\!]/(X) \subset R[\![X^{1/p^{n+1}}]\!]/(X)$ and makes $(G_0[\varphi^n])_{n\geq 0}$ into a projective system. The limit

$$\begin{aligned} T_\varphi G_0 &= \varprojlim_n G_0[\varphi^n] = \mathrm{Spec}(\varinjlim_n R[\![X]\!]/(X^{p^n})) \\ &= \mathrm{Spec}(R[\![X^{1/p^\infty}]\!]/(X)) = \mathrm{Spec}(A) \end{aligned}$$

is a commutative affine group scheme over R that we call the Frobenius-Tate module of G_0. The following result is then immediate.

Lemma 2.10. *If G_0 is a d-dimensional ordinary formal group law over R then the following statements hold.*

(i) We have $T_\varphi G_0 \cong \ker(G_0^\flat \longrightarrow G_0)$ as functors on adic R-algebras, viewed as abstract R-algebras on the left.

(ii) We have $G_0^\flat \cong \varinjlim_\varphi T_\varphi G_0^{(p^n)}$ as functors on discrete perfect R-algebras, viewed as abstract R-algebras on the right. □

Now let G_0 and H_0 be ordinary formal group laws of dimensions d and e over R, respectively, and write G and H if these are viewed as perfect formal group laws. We wish to relate the group $\mathrm{Hom}_R(G, H)$ of homomorphisms of perfect formal group laws to the subgroup $\mathrm{Hom}_R(G_0, H_0) = \mathrm{Hom}_R(G, H) \cap R[\![X]\!]^e$ of homomorphisms of ordinary formal group laws.

The groups $\mathrm{Hom}_R(G_0, H_0^{(p^h)})$ with $h \geq 0$ form an inductive system with injective transition maps

$$\mathrm{Hom}_R(G_0, H_0^{(p^h)}) \to \mathrm{Hom}_R(G_0, H_0^{(p^{h+1})}), \qquad f \mapsto \varphi \circ f.$$

The injective group homomorphisms $\mathrm{Hom}_R(G_0, H_0^{(p^h)}) \to \mathrm{Hom}_R(G, H)$ defined by $f \mapsto \varphi^{-h} \circ f$ induce an injective group homomorphism

$$\varinjlim_{h \geq 0} \mathrm{Hom}_R(G_0, H_0^{(p^h)}) \longrightarrow \mathrm{Hom}_R(G, H). \tag{13}$$

Proposition 2.11. *The group homomorphism (13) is bijective. More precisely, if $f = (f_1, \ldots, f_e) : G \to H$ is a non-zero homomorphism of perfect formal group laws then $\mathrm{ord}(f) = p^{-h}$ for some integer h and $\varphi^h \circ f \in R[\![X]\!]^e$. In particular, $\varphi^h \circ f : G_0 \to H_0^{(p^h)}$ is a homomorphism of ordinary formal group laws.*

Proof. The injectivity of (13) was remarked above so that it suffices to prove the statements about $f : G \to H$. Indeed, if $h \leq 0$ then the statements imply $f \in \mathrm{Hom}_R(G_0, H_0)$ and if $h \geq 0$ then f lies in the image of (13), as well.

We emphasize that the asserted integrality property of f does not rely on Theorem 1.7 and holds in any dimension. As we shall see, it is simply due to the fact that the composition of f with a sufficiently high power of φ induces a homomorphism between the Frobenius-Tate modules that commutes with passage to the cokernels of Frobenius.

To make this precise choose $n \in \mathbb{N}$ sufficiently large so that $\mathrm{ord}(\varphi^n \circ f) = p^n \cdot \mathrm{ord}(f) \geq 1$. Then $g = \varphi^n \circ f \in \mathrm{Hom}_R(G, H^{(p^n)})$ and the corresponding homomorphism of R-algebras $\psi_g : R[\![Z^{1/p^\infty}]\!] \to R[\![X^{1/p^\infty}]\!]$ with $Z = (Z_1, \ldots, Z_e)$ factors through a homomorphism

$$A' = R[\![Z^{1/p^\infty}]\!]/(Z) \to A = R[\![X^{1/p^\infty}]\!]/(X).$$

By the construction of Frobenius-Tate modules this corresponds to a homomorphism of affine group schemes $T_\varphi G_0 \to T_\varphi H_0^{(p^n)}$.

Given $m \in \mathbb{N}$ we first compute the subalgebra B_m of A consisting of all classes $h + (X)$ satisfying

$$h(G_0(X^{p^m}, Y)) \equiv h(Y) \mod (X, Y). \tag{14}$$

It represents the cokernel of φ^m on $T_\varphi G_0$ but we will not need this. If $1 \leq i \leq d$ and $h = X_i^{1/p^m}$ then $h(G_0(X^{p^m}, Y)) \equiv Y_i^{1/p^m} = h(Y) \mod (X)$ because $G_0(X^{p^m}, Y) \equiv Y \mod (X^{p^m})$. This implies $A_m \subseteq B_m$ where $A_m =$

$R[X^{1/p^m}]/(X)$. We claim that $A_m = B_m$.

Let $h+(X) \in B_m$ and set $\nu = \mathrm{ord}(h)$. In order to show $h+(X) \in A_m$ we may assume $0 < \nu \leq 1$. The congruence (14) is equivalent to $h(G_0(X,Y)) \equiv h(Y) \mod (X^{1/p^m}, Y)$. Note that any homogeneous monomial in the expansion of $\tilde{h}(X,Y) = h(G_0(X,Y)) - h(Y)$ then lies in $(X^{1/p^m}, Y)$, as well. If we write $h(X) = \sum_\alpha c_\alpha X^\alpha$ then $\mathrm{ord}(\tilde{h}) \geq \nu$ and

$$\tilde{h}_\nu(X,Y) = \sum_{|\alpha|=\nu} c_\alpha \Big(\prod_{j=1}^{d} (X_j + Y_j)^{\alpha_j} - Y^\alpha\Big).$$

For $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{N}[\frac{1}{p}]^d$ we set $v_p(\alpha) = \min\{v_p(\alpha_1), \ldots, v_p(\alpha_d)\}$ and $s = \min\{v_p(\alpha) \mid c_\alpha \neq 0 \text{ and } |\alpha| = \nu\}$. Choose $\beta \in \mathbb{N}[\frac{1}{p}]^d$ and $1 \leq j_0 \leq d$ with $|\beta| = \nu$, $c_\beta \neq 0$ and $v_p(\beta_{j_0}) = s$. Writing $\beta_{j_0} = ip^s$ we have $i \in \mathbb{N} \setminus p\mathbb{N}$ and claim that $ic_\beta X_{j_0}^{p^s} Y^{\beta - p^s e_{j_0}}$ is one of the monomials in the expansion of $\tilde{h}_\nu$.

It clearly appears in the expansion of $c_\beta(\prod_{j=1}^d (X_j + Y_j)^{\beta_j} - Y^\beta)$. Let us assume that it also appears in the expansion of $c_\alpha(\prod_{j=1}^d (X_j + Y_j)^{\alpha_j} - Y^\alpha)$ where $|\alpha| = \nu$ and $c_\alpha \neq 0$. Then the monomial also appears in the expansion of $c_\alpha (X_{j_0} + Y_{j_0})^{\alpha_{j_0}} \prod_{j \neq j_0} Y_j^{\alpha_j}$ because among the variables $X_1, \ldots, X_d$ only X_{j_0} shows up. Writing $\alpha_{j_0} = tp^\ell$ with $\ell \in \mathbb{Z}$ and $t \in \mathbb{N} \setminus p\mathbb{N}$ the unique smallest positive exponent of X_{j_0} in the expansion of $(X_{j_0} + Y_{j_0})^{\alpha_{j_0}}$ is p^ℓ. By the minimality of s we must have $\ell = s$ and $tc_\alpha X_{j_0}^{p^s} Y_{j_0}^{\alpha_{j_0} - p^s} \prod_{j \neq j_0} Y_j^{\alpha_j} = ic_\beta X_{j_0}^{p^s} Y^{\beta - p^s e_{j_0}}$. Since tc_α and ic_β are both non-zero in R the families of exponents coincide. This gives $\alpha = \beta$ and implies our claim.

Since $ic_\beta \neq 0$ in R and since $|\beta - p^s e_{j(\beta)}| = \nu - p^s < \nu \leq 1$ the above monomial lies in $(X^{1/p^m}, Y)$ if and only if $p^s \geq 1/p^m$. By the minimality of s we get $h_\nu + (X) \in A_m \subseteq B_m$ and therefore $h - h_\nu + (X) \in B_m$. We now proceed inductively to get $h + (X) \in A_m$ after finitely many steps. Thus, $A_m = B_m$ as claimed.

Similarly, $A'_m = R[Z^{1/p^m}]/(Z)$ is the subalgebra of A' consisting of all classes $h + (Z)$ satisfying $\tilde{h}(Z, Z') = h(H_0^{(p^n)}(Z, Z')) - h(Z) \in (Z^{p^m}, Z')$. This condition implies $\tilde{h}(g(X), g(Y)) \in (g(X)^{p^m}, g(Y)) \subseteq (X^{p^m}, Y)$ because $\mathrm{ord}(g) \geq 1$. Since $g(G_0(X,Y)) = H_0^{(p^n)}(g(X), g(Y))$ we obtain

$$h(g(Y)) \equiv h(H_0^{(p^n)}(g(X), g(Y))) \equiv h(g(G_0(X,Y)) \mod (X^{p^m}, Y).$$

Thus, the homomorphism $\psi_g : A' \to A$ maps A'_m into A_m. In particular, $g_i^{1/p^m} = \psi_g(X_i^{1/p^m}) \in A_m = R[X^{1/p^m}]/(X)$ which implies $g_i \in R[\![X]\!] + (X^{p^m})$ for any $1 \leq i \leq e$. Since $m \in \mathbb{N}$ was arbitrary we get $g \in R[\![X]\!]^e$, i.e. $g \in \mathrm{Hom}_R(G_0, H_0^{(p^n)})$. It is now a standard result that $\mathrm{ord}(g) = p^s$ for some

$s \in \mathbb{N}$ and that $g(X^{1/p^s}) \in R[\![X]\!]^e$ (cf. [2], Theorem I.3.2 (ii)). Setting $h = n-s$ we obtain $\mathrm{ord}(f) = p^h$ and $\varphi^h \circ f = \varphi^{-s} \circ g \in \mathrm{Hom}_R(G_0, H_0^{(p^h)})$. □

Recall that a homomorphism $f : G_0 \to H_0$ of formal groups over R is called an isogeny if the corresponding comorphism $\psi_f : R[\![Z]\!] \to R[\![X]\!]$ is faithfully flat and if its kernel is represented by a finite flat group scheme over R. In this case G_0 and H_0 have the same dimension. If the augmentation ideal of the Hopf algebra representing $\ker(f)$ is nilpotent then we call f a *formal isogeny*. Let FGL_R denote the category of ordinary formal group laws over R, let $\mathcal{F}$ denote its class of formal isogenies and recall that we denote by $\mathrm{FGL}_R^{\mathrm{perf}}$ the category of perfect formal group laws over R. By definition, FGL_R is a subcategory of $\mathrm{FGL}_R^{\mathrm{perf}}$.

Corollary 2.12. *(i) The inclusion* $\mathrm{FGL}_R \hookrightarrow \mathrm{FGL}_R^{\mathrm{perf}}$ *extends to a fully faithful embedding* $\mathrm{FGL}_R[\mathcal{F}^{-1}] \subseteq \mathrm{FGL}_R^{\mathrm{perf}}$.

(ii) Two ordinary formal group laws G_0 *and* H_0 *over* R *are isomorphic as perfect formal group laws if and only if there is a formal isogeny* $g : G_0 \to H_0^{(p^h)}$ *for some* $h \in \mathbb{N}$.

Proof. If $f : G_0 \to H_0$ is a formal isogeny then there is a natural number h and a formal isogeny $g : H_0 \to G_0^{(p^h)}$ such that $g \circ f = \varphi^h : G_0 \to G_0^{(p^h)}$ (cf. [9], Satz 5.25). In $\mathrm{FGL}_R^{\mathrm{perf}}$ the morphism φ^h is an isomorphism with inverse φ^{-h}. It follows that any element of $\mathcal{F}$ admits a left inverse in $\mathrm{FGL}_R^{\mathrm{perf}}$, hence is an isomorphism. The results in [9], Satz 5.25 and Satz 5.26, also imply that $\mathcal{F}$ is a saturated, left multiplicative system.

By the universal property of the left localization there is a canonical functor $\iota : \mathrm{FGL}_R[\mathcal{F}^{-1}] \to \mathrm{FGL}_R^{\mathrm{perf}}$ which we claim is fully faithful. The set of homomorphisms $G_0 \to H_0$ in $\mathrm{FGL}_R[\mathcal{F}^{-1}]$ is given as the colimit

$$\varinjlim_{g : H_0 \to H_0'} \mathrm{Hom}_R(G_0, H_0')$$

running over all formal isogenies $g : H_0 \to H_0'$ in FGL_R. By construction, the functor ι maps the class of the homomorphism $f : G_0 \to H_0'$ indexed by $g : H_0 \to H_0'$ to $g^{-1} \circ f \in \mathrm{Hom}_R(G, H)$. The result in [9], Satz 5.25, implies that the subsystem of all $\mathrm{Hom}_R(G_0, H_0^{(p^h)})$ indexed by $\varphi^h : H_0 \to H_0^{(p^h)}$ with $h \in \mathbb{N}$ is cofinal. Thus, the set of homomorphisms $G_0 \to H_0$ in $\mathrm{FGL}_R[\mathcal{F}^{-1}]$ is given by $\varinjlim_{h \geq 0} \mathrm{Hom}_R(G_0, H_0^{(p^h)})$. By Proposition 2.11 the functor ι maps it bijectively onto $\mathrm{Hom}_R(G, H)$. This proves (i) and the if part of (ii).

Conversely, given an isomorphim $f : G \to H$ between the corresponding perfect formal group laws we can write $f = \varphi^{-h} \circ g$ with $h \in \mathbb{N}$ and a homomorphism $g : G_0 \to H_0^{(p^h)}$ of ordinary formal group laws. Then g is an

isomorphism in $\mathrm{FGL}_R^{\mathrm{perf}}$ and it follows from (i) that g is an isomorphism in $\mathrm{FGL}_R[\mathcal{F}^{-1}]$. This implies $g \in \mathcal{F}$ by [5], Proposition 7.1.20 (ii).

One can also give a slightly more direct proof. Namely, write $f^{-1} = \varphi^{-i} \circ \gamma$ with $i \in \mathbb{N}$ and $\gamma : H_0 \to G_0^{(p^i)}$. Setting $g' = \gamma^{(p^h)}$ we get $g' \circ g = \varphi^{h+i}$. It will follow from [9], Satz 5.25, that g is a formal isogeny once we can show that G_0 and H_0 have the same dimension. To see this choose a maximal ideal $\mathfrak{m} \subset R$ and consider the factorization

$$(R/\mathfrak{m})[\![X]\!] \xrightarrow{\psi_{g'_{\mathfrak{m}}}} (R/\mathfrak{m})[\![Z]\!] \xrightarrow{\psi_{g_{\mathfrak{m}}}} (R/\mathfrak{m})[\![X]\!]$$

of the homomorphism of $R/\mathfrak{m}$-algebras sending X to $X^{p^{h+i}}$. Note that $\psi_{g_{\mathfrak{m}}}$ and $\psi_{g'_{\mathfrak{m}}}$ are both injective because they are restrictions of isomorphisms between perfect formal power series rings. It follows that $\psi_{g'_{\mathfrak{m}}}$ is finite injective, hence preserves Krull dimensions. This gives $\dim(G_0) = \dim(H_0)$ as desired. □

By construction, a category has the same objects as any of its localizations. Combining Theorem 2.7 and Corollary 2.12 we therefore obtain the following result.

Theorem 2.13. *The category of one-dimensional perfect formal group laws over R is the category of one-dimensional ordinary formal group laws over R localized at the class of formal isogenies.* □

Remark 2.14. The inclusion $\mathrm{FGL}_R[\mathcal{F}^{-1}] \subseteq \mathrm{FGL}_R^{\mathrm{perf}}$ in Corollary 2.12 (i) is not surjective on objects of dimension at least two, i.e. there do exist perfect formal group laws of dimension at least two which are not given by ordinary formal power series (cf. [1], Corollary 4.19). It might still be an equivalence of categories as this requires only *essential* surjectivity. However, it is presently unknown whether every perfect formal group law of dimension at least two is isomorphic to an ordinary formal group law.

References

[1] G. Doğan: Formal vector spaces in mixed characteristic, *PhD Thesis*, Universität Duisburg-Essen, (2022).

[2] A. Fröhlich: Formal Groups, *Lecture Notes in Mathematics* **74**, Springer, (1968).

[3] U. Görtz, T. Wedhorn: *Algebraic Geometry I: Schemes*, 2nd Edition, Springer Spektrum, (2020), vii+625.

[4] K. Kedlaya: Automorphisms of perfect power series rings, *Journal of Algebra* **511** (2018), 358–363.

[5] M. Kashiwara, P. Schapira: Categories and Sheaves, *Grundlehren der Mathematischen Wissenschaften* **332**, Springer, (2006).

[6] M. Lazard: Sur les groupes de Lie formels à un paramètre, *Bulletin de la S.M.F.* **83** (1955), 251–274.

[7] P. Scholze, J. Weinstein: Moduli of p-divisible groups, *Camb. J. Math.* **1** (2013), no. 2, 145–237.

[8] W. Waterhouse: Introduction to Affine Group Schemes, *Graduate Texts in Mathematics* **66**, Springer, (1979).

[9] Th. Zink: Cartiertheorie kommutativer formaler Gruppen, *Teubner-Texte zur Mathematik* **68**, Teubner, (1984).

Universität Duisburg-Essen
Fakultät für Mathematik
Thea-Leymann-Straße 9
D–45127 Essen, Germany
E-mail address: jan.kohlhaase@uni-due.de