New York Journal of Mathematics

New York J. Math. **15** (2009) 435–450.

Formal group law homomorphisms over $\mathcal{O}_{\mathbb{C}_p}$

Kevin Keating

Abstract. Let K be a finite extension of the p-adic field $\mathbb{Q}_p$ and let $F(X,Y)$ and $G(X,Y)$ be one-dimensional formal group laws over the ring of integers $\mathcal{O}_K$ of K. Let $\phi(X)$ be a homomorphism from F to G which is defined over the ring of integers $\mathcal{O}_{\mathbb{C}_p}$ of the completion $\mathbb{C}_p$ of $\mathbb{Q}_p^{alg}$. In this paper we prove that if $\ker(\phi)$ is finite then there is a discretely valued subfield $L \subset \mathbb{C}_p$ such that $\phi(X)$ is defined over $\mathcal{O}_L$.

Contents

Let $\mathbb{Q}_p$ be the field of p-adic numbers, let $\mathbb{Q}_p^{alg}$ be an algebraic closure of $\mathbb{Q}_p$, and let $\mathbb{C}_p$ be the completion of $\mathbb{Q}_p^{alg}$ with respect to the p-adic valuation. Let K be a closed discretely valued subfield of $\mathbb{C}_p$ and let $F(X,Y)$, $G(X,Y)$ be one-dimensional formal group laws over the ring of integers $\mathcal{O}_K$ of K. Let L/K be a subextension of $\mathbb{C}_p/K$. A *homomorphism* from F to G over $\mathcal{O}_L$ is defined to be a power series $\phi(X) \in \mathcal{O}_L[[X]]$ such that $\phi(0) = 0$ and $\phi(F(X,Y)) = G(\phi(X), \phi(Y))$. Let K^{alg} be the algebraic closure of K in $\mathbb{C}_p$. It is well-known (see [3, p. 106]) that every homomorphism from F to G with coefficients in $\mathcal{O}_{K^{alg}}$ is defined over $\mathcal{O}_M$ for some finite subextension M/K of K^{alg}/K. In [10] Schmitz raised the question of whether every homomorphism from F to G with coefficients in $\mathcal{O}_{\mathbb{C}_p}$ is defined over the ring of integers $\mathcal{O}_L$ of some discretely valued subfield L of $\mathbb{C}_p$. In this paper we show that this is true as long as F and G both have height $h < \infty$. If we allow

Received March 14, 2009.
Mathematics Subject Classification. 11S31.
Key words and phrases. p-adic formal group laws, homomorphisms, Newton polygons.

ISSN 1076-9803/09

F and G to have different (finite) heights, there can exist homomorphisms from F to G with coefficients in $\mathcal{O}_{\mathbb{C}_p}$ which are not defined over $\mathcal{O}_M$ for any finite extension M of K (see Example 3.8). Any such homomorphism must have infinite kernel.

We now describe the contents of the various sections. In §1 we recall some basic facts about power series in one variable over $\mathcal{O}_{\mathbb{C}_p}$. In §2 we extend some results of Lubin [6] on formal group laws over $\mathcal{O}_K$ to formal group laws over $\mathcal{O}_{\mathbb{C}_p}$. In §3 we prove our main result, as described in the preceding paragraph.

I would like to thank the referee for suggestions which led to several major improvements in the exposition. I also thank David Schmitz for his careful reading of an earlier version of the paper, and especially for pointing out a fatal flaw in my first attempt to prove Theorem 3.2.

1. Power series over $\mathcal{O}_{\mathbb{C}_p}$

In this section we review the theory of power series over $\mathcal{O}_{\mathbb{C}_p}$, in particular the Weierstrass preparation theorem and the theory of Newton polygons. The material in this section is certainly well-known (see for instance [5]), but we include it in order to make the paper more self-contained.

Let p be a prime, let $\mathbb{Q}_p$ be the field of p-adic numbers, and let $\mathbb{Q}_p^{alg}$ be an algebraic closure of $\mathbb{Q}_p$. The p-adic valuation v_p on $\mathbb{Q}_p$ extends uniquely to a valuation on $\mathbb{Q}_p^{alg}$, which we also denote by v_p. Let $\mathbb{C}_p$ denote the completion of $\mathbb{Q}_p^{alg}$ with respect to v_p. Then $\mathbb{C}_p$ is an algebraically closed field [5, Th. 13, p. 72]. For any subfield K of $\mathbb{C}_p$ we define the ring of integers of K to be $\mathcal{O}_K = \{x \in K : v_p(x) \geq 0\}$. Then $\mathcal{O}_K$ is a local ring with maximal ideal $\mathcal{M}_K = \{x \in \mathcal{O}_K : v_p(x) > 0\}$. We say that K is discretely valued if $v_p(K^\times) = \frac{1}{e} \cdot \mathbb{Z}$ for some natural number e. The algebraic closure K^{alg} of K in $\mathbb{C}_p$ is dense in $\mathbb{C}_p$, and if K is closed in $\mathbb{C}_p$ then the action of $\mathrm{Gal}(K^{alg}/K)$ on K^{alg} extends uniquely to a continuous action of $\mathrm{Gal}(K^{alg}/K)$ on $\mathbb{C}_p$.

Let R be a commutative ring with 1 and let $R[[X]]$ denote the ring of formal power series in one variable over R. For $\phi(X), \psi(X) \in R[[X]]$ such that $\psi(0) = 0$ we define the composition of ϕ with ψ to be $(\phi \circ \psi)(X) = \phi(\psi(X))$. We say $\phi(X) \in R[[X]]$ is an invertible power series if $\phi(X) = a_1X + a_2X^2 + \cdots$ with $a_1 \in R^\times$. In this case there exists a unique $\phi^{-1}(X) \in R[[X]]$ such that $(\phi \circ \phi^{-1})(X) = (\phi^{-1} \circ \phi)(X) = X$, and the series $\phi^{-1}(X)$ is itself invertible.

Since $\mathcal{O}_{\mathbb{C}_p}$ is a valuation ring, power series over $\mathcal{O}_{\mathbb{C}_p}$ can be studied using Newton polygons and Newton copolygons. Let $\phi(X) = a_0 + a_1X + a_2X^2 + \cdots$ be a nonzero element of $\mathcal{O}_{\mathbb{C}_p}[[X]]$. For each $i \geq 0$ with $a_i \neq 0$ let

$$Q_i = \{(x, y) \in \mathbb{R}^2 : x \geq i,\ y \geq v_p(a_i)\}, \tag{1.1}$$

and define C to be the convex hull of the union of the collection $\{Q_i : a_i \neq 0\}$. Let B denote the boundary of C and let $m = \min\{i : a_i \neq 0\}$. By removing the half-line $\{(m, y) : y > v_p(a_m)\}$ from B we get the Newton polygon $\mathcal{N}_\phi$ of $\phi(X)$. If there exists $k \geq 0$ such that $v_p(a_k) \leq v_p(a_i)$ for all $i \geq 0$ then $\mathcal{N}_\phi$ is the union of finitely many line segments with negative slope and the half-line $\{(x, v_p(a_d)) : x \geq d\}$, where $d = \min\{j : v_p(a_j) = v_p(a_k)\}$. Otherwise, $\mathcal{N}_\phi$ is the union of countably many line segments with negative slope. The endpoints of the line segments which make up $\mathcal{N}_\phi$ are called the vertices of $\mathcal{N}_\phi$.

The valuation function $\Psi_\phi : (0, \infty) \to (0, \infty)$ of $\phi(X)$ is defined by

$$\Psi_\phi(x) = \min\{v_p(a_i) + ix : i \geq 0\}. \tag{1.2}$$

Let $\psi(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ be another nonzero power series. One easily verifies that $\Psi_{\phi\cdot\psi} = \Psi_\phi + \Psi_\psi$, and that $\Psi_{\phi\circ\psi} = \Psi_\phi \circ \Psi_\psi$ if $\psi(0) = 0$. The graph of $\Psi_\phi(x)$ is known as the Newton copolygon of ϕ, and is denoted $\mathcal{N}^*_\phi$. The Newton copolygon, like the Newton polygon, may be described as a union of line segments and a half line. In fact there is a one-to-one correspondence between the vertices of $\mathcal{N}_\phi$ and the segments of $\mathcal{N}^*_\phi$, and a one-to-one correspondence between the finite-length segments of $\mathcal{N}_\phi$ and the vertices of $\mathcal{N}^*_\phi$: The vertex (a, b) on $\mathcal{N}_\phi$ corresponds to a segment (or half line) on $\mathcal{N}^*_\phi$ with slope a and y-intercept b, and a segment on $\mathcal{N}_\phi$ with slope $-a$ and y-intercept b corresponds to the vertex (a, b) on $\mathcal{N}^*_\phi$.

Say that the power series

$$\phi(X) = a_0 + a_1X + a_2X^2 + \cdots \in \mathcal{O}_{\mathbb{C}_p}[[X]] \tag{1.3}$$

has Weierstrass degree d if $a_i \in \mathcal{M}_{\mathbb{C}_p}$ for $0 \leq i < d$ and $a_d \notin \mathcal{M}_{\mathbb{C}_p}$. We define a distinguished polynomial in $\mathcal{O}_{\mathbb{C}_p}[X]$ to be a monic polynomial

$$b_0 + b_1X + \cdots + b_{d-1}X^{d-1} + X^d \tag{1.4}$$

such that $b_i \in \mathcal{M}_{\mathbb{C}_p}$ for $0 \leq i < d$.

Let K be a closed subfield of $\mathbb{C}_p$. In order to study formal group law homomorphisms defined over $\mathcal{O}_K$ we need to formulate versions of the Weierstrass preparation theorem for power series defined over $\mathcal{O}_K$. Since the field K may not be discretely valued, the ring $\mathcal{O}_K$ need not be Noetherian. The following proposition is an analog of [1, 10.2.1] for power series over $\mathcal{O}_K$, and is proved by essentially the same method.

Proposition 1.1. *Let K be a closed subfield of $\mathbb{C}_p$ and let $\phi(X)$, $\psi(X)$ be elements of $\mathcal{O}_K[[X]]$ such that $\psi(X)$ has Weierstrass degree d. Then there exist unique $q(X) \in \mathcal{O}_K[[X]]$ and $r(X) \in \mathcal{O}_K[X]$ such that $\deg(r) < d$ and $\phi(X) = \psi(X)q(X) + r(X)$.*

Proof. Write $\psi(X) = a_0 + a_1X + a_2X^2 + \cdots$ and choose $c \in \mathcal{M}_K$ such that $a_i \in c\mathcal{O}_K$ for $0 \leq i < d$. We will inductively construct a sequence $(q_n(X))$ of power series and a sequence $(r_n(X))$ of polynomials of degree $< d$ such that

$$\phi(X) \equiv \psi(X)q_n(X) + r_n(X) \pmod{c^n} \tag{1.5}$$

$$q_{n+1}(X) \equiv q_n(X) \pmod{c^n} \tag{1.6}$$

$$r_{n+1}(X) \equiv r_n(X) \pmod{c^n} \tag{1.7}$$

for all $n \geq 0$. Clearly (1.5) holds for $n = 0$ with $q_0(X) = r_0(X) = 0$. Let $n \geq 0$ and assume (1.5) holds for n. Then

$$\phi(X) = \psi(X)q_n(X) + r_n(X) + c^n g(X) \tag{1.8}$$

for some $g(X) \in \mathcal{O}_K[[X]]$. Write $g(X) = b_0+b_1X+b_2X^2+\cdots$ and recall that $\psi(X) = a_0+a_1X+a_2X^2+\cdots$ with $a_d \in \mathcal{O}_K^\times$. Let $\omega(X)$ be the multiplicative inverse of $a_d + a_{d+1}X + a_{d+2}X^2 + \cdots$. Then it is straightforward to verify that

$$q_{n+1}(X) = q_n(X) + c^n\omega(X) \cdot (b_d + b_{d+1}X + b_{d+2}X^2 + \cdots) \tag{1.9}$$

$$r_{n+1}(X) = r_n(X) + c^n(b_0 + b_1X + \cdots + b_{d-1}X^{d-1}) \tag{1.10}$$

satisfy

$$\phi(X) \equiv \psi(X)q_{n+1}(X) + r_{n+1}(X) \pmod{c^{n+1}}. \tag{1.11}$$

We now define $q(X)$, $r(X)$ to be the limits of the sequences $(q_n(X))$, $(r_n(X))$ with respect to the c-adic topology on $\mathcal{O}_K[[X]]$. Then $q(X)$, $r(X)$ satisfy the conditions of the proposition.

To prove uniqueness suppose we also have $\phi(X) = \psi(X)\widetilde{q}(X)+\widetilde{r}(X)$ with $\deg(\widetilde{r}) < d$. Then

$$\psi(X)(q(X) - \widetilde{q}(X)) = \widetilde{r}(X) - r(X). \tag{1.12}$$

If $q(X) \neq \widetilde{q}(X)$ let c^n be the largest power of c which divides $q(X) - \widetilde{q}(X)$. Then $q(X)-\widetilde{q}(X) = c^n h(X)$ for some $h(X) \in \mathcal{O}_K[[X]]$ which is not divisible by c. Since

$$\psi(X) \equiv a_dX^d + a_{d+1}X^{d+1} + \cdots \pmod{c} \tag{1.13}$$

with $v_p(a_d) = 0$ this implies that the left side of (1.12) has at least one term of degree $\geq d$ whose coefficient is not divisible by c^{n+1}. Since the right side of (1.12) is a polynomial of degree $< d$, this is a contradiction. It follows that $q(X) = \widetilde{q}(X)$, and hence that $r(X) = \widetilde{r}(X)$. □

The following corollary extends the Weierstrass preparation theorem to power series with coefficients in the (possibly non-Noetherian) local ring $\mathcal{O}_K$ (cf. [1, 10.2.4]).

Corollary 1.2. *Let K be a closed subfield of $\mathbb{C}_p$ and let $\phi(X) \in \mathcal{O}_K[[X]]$ be a power series with Weierstrass degree d. Then there exist a unit power series $u(X) \in \mathcal{O}_K[[X]]^\times$ and a distinguished polynomial $f(X) \in \mathcal{O}_K[X]$ of degree d such that $\phi(X) = u(X)f(X)$ and $f(X)$ has the same Newton polygon as $\phi(X)$.*

Proof. This is basically the same as the proof of 10.2.4 in [1]: By Proposition 1.1 there are $q(X) \in \mathcal{O}_K[[X]]$ and $r(X) \in \mathcal{O}_K[X]$ such that $X^d = \phi(X)q(X) + r(X)$ and $\deg(r) < d$. By reducing modulo $\mathcal{M}_K[[X]]$ we see that $r(X) \in \mathcal{M}_K[X]$. Hence $f(X) := X^d - r(X)$ is a distinguished polynomial. Since $f(X) = \phi(X)q(X)$, the Weierstrass degree of $q(X)$ is 0, so $q(X)$ is a unit in $\mathcal{O}_K[[X]]$. Setting $u(X)$ equal to the multiplicative inverse of $q(X)$ we get $\phi(X) = u(X)f(X)$, as required. Since $u(X)$ is a unit power series we have $\Psi_u(x) = 0$, and hence

$$\Psi_\phi(x) = \Psi_u(x) + \Psi_f(x) = \Psi_f(x) \tag{1.14}$$

for all $x > 0$. It follows that $\mathcal{N}_\phi^* = \mathcal{N}_f^*$, and hence that $\mathcal{N}_\phi = \mathcal{N}_f$. □

The following is another version of the Weierstrass preparation theorem for power series over $\mathcal{O}_{\mathbb{C}_p}$. A similar result for power series over $\mathbb{C}_p$ with constant term 1 is given in [5, Th. 14, p. 97].

Proposition 1.3. *Let $\phi(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ and let (d, e) be a vertex on the Newton polygon $\mathcal{N}_\phi$ of ϕ. Then there exist a power series $\psi(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ and a distinguished polynomial $f(X) \in \mathcal{O}_{\mathbb{C}_p}[X]$ of degree d with the following properties:*

(1) *$\phi(X) = \psi(X)f(X)$.*
(2) *$\mathcal{N}_f^l = \{(x, y) \in \mathcal{N}_f : x \le d\}$ is the translation of $\mathcal{N}_\phi^l = \{(x, y) \in \mathcal{N}_\phi : x \le d\}$ by $(0, -e)$.*
(3) *$\mathcal{N}_\psi$ is the translation of $\mathcal{N}_\phi^r = \{(x, y) \in \mathcal{N}_\phi : x \ge d\}$ by $(-d, 0)$.*

Proof. Let $-w_l$, $-w_r$ denote the slopes of the segments of $\mathcal{N}_\phi$ immediately to the left and right of (d, e); if (d, e) is the left endpoint of $\mathcal{N}_\phi$ let $w_l = \infty$. Then $w_l > w_r$, so there exists $b \in \mathcal{O}_{\mathbb{C}_p}$ such that $w_r < v_p(b) < w_l$. Write $\phi(X) = a_0 + a_1X + a_2X^2 + \cdots$ and set $\rho(X) = \phi(bX)$. Then the coefficient of X^n in $\rho(X)$ is $b^n a_n$, and by the choice of b we have $v_p(b^d a_d) < v_p(b^n a_n)$ for all $n \ne d$. Hence $a_d^{-1} b^{-d} \rho(X)$ is an element of $\mathcal{O}_{\mathbb{C}_p}[[X]]$ with Weierstrass degree d. By Corollary 1.2 there is a unit power series $u(X)$ and a distinguished polynomial $g(X)$ of degree d such that $a_d^{-1} b^{-d} \rho(X) = u(X)g(X)$. Let $\psi(X) = a_d u(b^{-1}X)$ and $f(X) = b^d g(b^{-1}X)$. Then $\psi(X)f(X) = \phi(X)$ with $f(X) \in \mathcal{O}_{\mathbb{C}_p}[X]$ a distinguished polynomial of degree d. We claim that $\psi(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$. By Proposition 1.1 there exist $q(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ and $r(X) \in \mathcal{O}_{\mathbb{C}_p}[X]$ such that $\phi(X) = f(X)q(X) + r(X)$ and $\deg(r) < d$. By replacing X with bX we get $\rho(X) = g(X) \cdot b^d q(bX) + r(bX)$. Since we also have $\rho(X) = g(X) \cdot a_d b^d u(X)$, by the uniqueness statement in Proposition 1.1 we get $b^d q(bX) = a_d b^d u(X)$. Hence $\psi(X) = a_d u(b^{-1}X) = q(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$.

It follows from Corollary 1.2 that $g(X)$ has the same Newton polygon as $a_d^{-1} b^{-d} \rho(X)$. Hence $b^d g(X)$ has the same Newton polygon as $a_d^{-1} \rho(X)$. Therefore $\Psi_{b^d g}(x) = \Psi_{a_d^{-1}\rho}(x)$ for all $x > 0$. Since $f(X) = b^d g(b^{-1}X)$ and $a_d^{-1}\phi(X) = a_d^{-1}\rho(b^{-1}X)$ we get $\Psi_f(x) = \Psi_{a_d^{-1}\phi}(x)$ for all $x > v_p(b)$. Since

$v_p(b) < w_l$ it follows from the correspondence between Newton polygons and copolygons that $\mathcal{N}_f^l = \mathcal{N}_{a_d^{-1}\phi}^l$. Hence $\mathcal{N}_f^l$ is the translation of $\mathcal{N}_\phi^l$ by $v_p(a_d) = e$ units downwards, so property (2) holds.

It follows from the preceding paragraph that the rightmost finite segment of $\mathcal{N}_f$ has slope $-w_l$ and right endpoint $(d, 0)$. Therefore $\Psi_f(x) = dx$ for $0 \le x \le w_l$. Since $\phi(X) = \psi(X)f(X)$ we have $\Psi_\psi(x) = \Psi_\phi(x) - \Psi_f(x)$, and hence $\Psi_\psi(x) = \Psi_\phi(x) - dx$ for $0 \le x \le w_l$. Since $\psi(X) = a_d u(b^{-1}X)$ with $u(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]^\times$, for $x \ge v_p(b)$ we have $\Psi_\psi(x) = v_p(a_d) = e$. Since $v_p(b) < w_l$, these two facts determine $\Psi_\psi(x)$ and $\mathcal{N}_\psi^*$ completely. We find that the segments of $\mathcal{N}_\psi^*$ have the same y-intercepts as the segments of $\mathcal{N}_\phi^*$ which lie to the left of $x = w_l$, but the slopes of the segments on $\mathcal{N}_\psi^*$ are d less than the slopes of the corresponding segments on $\mathcal{N}_\phi^*$. It follows from the correspondence between Newton polygons and Newton copolygons that the vertices of $\mathcal{N}_\psi$ are the translates of the vertices of $\mathcal{N}_\phi^r$ by d units to the left. This gives property (3). □

Remark 1.4. In fact the series $\psi(X)$ and the polynomial $f(X)$ in the conclusion of Proposition 1.3 are uniquely determined by $\phi(X)$ and (d, e). Furthermore, if $\phi(X) \in \mathcal{O}_K[[X]]$ for some closed subfield K of $\mathbb{C}_p$ then $\psi(X)$ and $f(X)$ have coefficients in K. We omit the proofs of these facts because they are not needed for our applications.

Corollary 1.5. *Let $\phi(X) \in X\mathcal{O}_{\mathbb{C}_p}[[X]]$ and let α be an element of $\mathcal{M}_{\mathbb{C}_p}$ which does not divide $\phi(X)$ in $\mathcal{O}_{\mathbb{C}_p}[[X]]$. Then there is $\beta \in \mathcal{M}_{\mathbb{C}_p}$ such that $\phi(\beta) = \alpha$.*

Proof. The assumption on α implies that the Newton polygon of $\phi(X) - \alpha$ has at least one segment with negative slope. It follows from Proposition 1.3 that we can write $\phi(X) - \alpha = \psi(X)f(X)$, with $\psi(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ and $f(X) \in \mathcal{O}_{\mathbb{C}_p}[X]$ a distinguished polynomial of degree $d \ge 1$. Let $\beta \in \mathcal{M}_{\mathbb{C}_p}$ be any root of $f(X)$. Then $\phi(\beta) = \alpha$. □

2. Formal group laws

In this section we extend some well-known results in the theory of one-parameter formal group laws over a p-adic integer ring to include group laws and homomorphisms which are defined over $\mathcal{O}_{\mathbb{C}_p}$.

Let R be a commutative ring with 1. A (one-parameter) formal group law over R is a power series $F(X, Y) \in R[[X, Y]]$ such that $F(X, 0) = X$, $F(X, Y) = F(Y, X)$, and $F(F(X, Y), Z) = F(X, F(Y, Z))$. Let $F(X, Y)$ and $G(X, Y)$ be formal group laws over R and let S be a commutative ring which contains R. A homomorphism from F to G over S is a power series $\phi(X) \in S[[X]]$ such that $\phi(0) = 0$ and $\phi(F(X, Y)) = G(\phi(X), \phi(Y))$. Given homomorphisms $\phi(X)$ and $\psi(X)$ from F to G, we define the sum of ϕ and ψ to be $(\phi +_G \psi)(X) = G(\phi(X), \psi(X))$. The series $(\phi +_G \psi)(X)$

is itself a homomorphism from F to G. This operation makes the set of S-homomorphisms from F to G into an abelian group, which we denote by $\mathrm{Hom}_S(F,G)$. If $\phi(X) \in \mathrm{Hom}_S(F,G)$ is invertible (with respect to composition of power series) we say that ϕ is an isomorphism from F to G. In this case $\phi^{-1}(X)$ is an isomorphism from G to F. A homomorphism from F to itself is called an endomorphism of F. The group $\mathrm{End}_S(F) = \mathrm{Hom}_S(F,F)$ of S-endomorphisms of F is a ring, with multiplication given by composition of power series. For $n \in \mathbb{Z}$ we define $[n]_F(X)$ to be the image of n under the canonical map from $\mathbb{Z}$ to $\mathrm{End}_S(F)$. Thus for n positive $[n]_F(X)$ is the sum in $\mathrm{End}_S(F)$ of n copies of the identity map $[1]_F(X) = X$.

Let $F(X,Y)$ be a formal group law over a field k of characteristic $p > 0$. Then either $[p]_F(X) = 0$ or $[p]_F(X) = \psi(X^{p^h})$ for some $h \geq 1$ and $\psi(X) \in k[[X]]$ such that $\psi(0) \neq 0$ (see for instance [4, 18.3.1]). In the first case we say that F has infinite height; in the second case we say that F has height h. Suppose that R is a local ring with maximal ideal $\mathcal{M}$ whose residue field $R/\mathcal{M}$ has characteristic p. Then the image $\overline{F}(X,Y)$ of $F(X,Y)$ in $(R/\mathcal{M})[[X,Y]]$ is a formal group law over $R/\mathcal{M}$. We define the height of $F(X,Y)$ to be equal to the height of $\overline{F}(X,Y)$.

Let E be a finite extension of $\mathbb{Q}_p$ and let R be an $\mathcal{O}_E$-algebra, with structure map $i : \mathcal{O}_E \to R$. A formal $\mathcal{O}_E$-module over R is defined to be a pair (F,j), where $F(X,Y)$ is a formal group law over R and

$$j : \mathcal{O}_E \longrightarrow \mathrm{End}_R(F) \tag{2.1}$$

is a ring homomorphism with $j(c) = i(c)X + a_2X^2 + \cdots$ for every $c \in \mathcal{O}_E$. We write $j(c) = [c]_F(X)$. The height of the formal $\mathcal{O}_E$-module (F,j) is defined to be $h/[E : \mathbb{Q}_p]$, where h is the height of the the formal group law F. If $h < \infty$ then the height of (F,j) is a positive integer [4, 21.8.2]. Suppose R is a complete local ring with maximal ideal $\mathcal{M}$ whose residue field $R/\mathcal{M}$ has characteristic p. Then R is a $\mathbb{Z}_p$-algebra and the map $n \mapsto [n]_F(X)$ can be uniquely extended to a ring homomorphism $j : \mathbb{Z}_p \to \mathrm{End}_R(F)$. The pair (F,j) is then a formal $\mathbb{Z}_p$-module.

Let $F(X,Y)$ be a formal group law over $\mathcal{O}_{\mathbb{C}_p}$. We define the point group $F(\mathcal{M}_{\mathbb{C}_p})$ of F to be the set $\mathcal{M}_{\mathbb{C}_p}$ with the operation $\alpha * \beta = F(\alpha,\beta)$. Any formal group law homomorphism $\phi : F \to G$ over $\mathcal{O}_{\mathbb{C}_p}$ induces a group homomorphism $\alpha \mapsto \phi(\alpha)$ from $F(\mathcal{M}_{\mathbb{C}_p})$ to $G(\mathcal{M}_{\mathbb{C}_p})$. The kernel of $\phi(X)$ is defined to be the kernel of the associated homomorphism of point groups. Suppose $F(X,Y)$ has height $h < \infty$. Then $\ker([p^n]_F(X))$ is a free $(\mathbb{Z}/p^n\mathbb{Z})$-module of rank h and $\alpha \mapsto [p]_F(\alpha)$ gives a surjective homomorphism from $\ker([p^{n+1}]_F(X))$ to $\ker([p^n]_F(X))$. By taking the projective limit of $\ker([p^n]_F(X))$ for $n \geq 1$ we get the Tate module $T_p(F)$, which is a free $\mathbb{Z}_p$-module of rank h. If $F(X,Y)$ is defined over $\mathcal{O}_K$ for some closed subfield K of $\mathbb{C}_p$ then $\mathrm{Gal}(K^{alg}/K)$ acts on $\ker([p^n]_F(X))$ and on $T_p(F)$.

Let $1 \leq h < \infty$. Since $\mathbb{Q}_p$ is a locally compact field it follows from Krasner's Lemma that there are only finitely many subextensions $L/\mathbb{Q}_p$ of

$\mathbb{Q}_p^{alg}/\mathbb{Q}_p$ such that $[L:\mathbb{Q}_p] \le h$. Let J_h denote the compositum of all such fields L. Then J_h is a finite extension of $\mathbb{Q}_p$.

Lemma 2.1. *Let $F(X,Y)$ be a formal group law of height $h < \infty$ over $\mathcal{O}_{\mathbb{C}_p}$ and let $\phi(X) = a_1X + a_2X^2 + \cdots \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ be an endomorphism of F. Then $a_1 \in \mathcal{O}_{J_h}$.*

Proof. Let $T_p(\phi)$ denote the endomorphism of $T_p(F)$ induced by $\phi(X)$ and let $g(X)$ be the minimum polynomial of $T_p(\phi)$ over $\mathbb{Q}_p$. Then $g(X) \in \mathbb{Z}_p[X]$, $\deg(g) \le h$, and $g(\phi) \in \mathrm{End}_{\mathcal{O}_{\mathbb{C}_p}}(F)$ annihilates $T_p(F)$. Hence for $n \ge 1$ the p^n-torsion points of F lie in the kernel of $g(\phi)$. Let $f(X) = \prod_\alpha(\alpha - X)$, where the product is taken over $\alpha \in \ker([p^n]_F(X))$. Then $f(X)$ divides $g(\phi)$ in $\mathcal{O}_{\mathbb{C}_p}[[X]]$. It follows that the product of the nonzero p^n-torsion points of F divides $g(a_1)$, the coefficient of X in $g(\phi)$. Since the sum of the p-valuations of the nonzero p^n-torsion points of F is n, we get $p^n \mid g(a_1)$ for every $n \ge 1$. Thus $g(a_1) = 0$. Since $\deg(g) \le h$, this implies $a_1 \in J_h \cap \mathcal{O}_{\mathbb{C}_p} = \mathcal{O}_{J_h}$. □

Proposition 2.2. *Let K be a subfield of $\mathbb{C}_p$, let $F(X,Y)$ be a formal group law of height $h < \infty$ over $\mathcal{O}_K$, and let $\phi(X) \in \mathrm{End}_{\mathcal{O}_{\mathbb{C}_p}}(F)$. Then $\phi(X)$ has coefficients in $\mathcal{O}_M$, where $M = KJ_h$.*

Proof. Let $l(X) = X + c_2X^2 + c_3X^3 + \cdots \in K[[X]]$ be the logarithm of F. Thus $l(X)$ is an isomorphism over K from $F(X,Y)$ to the additive formal group law $\mathbb{G}_a(X,Y) = X+Y$ (see [4, 5.4.4]). Since $\phi(X) = a_1X + a_2X^2 + \cdots$ is an endomorphism of F with coefficients in $\mathcal{O}_K$, the series $l(\phi(l^{-1}(X))) \in K[[X]]$ is an endomorphism of $\mathbb{G}_a$. Since K is a field of characteristic 0, every endomorphism of $\mathbb{G}_a$ over K is of the form $i(X) = bX$ for some $b \in K$ (see for instance Corollary 2 on p. 97 of [3]). Since the coefficient of X in $l(\phi(l^{-1}(X)))$ is a_1 we get $l(\phi(l^{-1}(X))) = a_1X$. By Lemma 2.1 we have $a_1 \in J_h$. It follows that $\phi(X) = l^{-1}(a_1 l(X))$ has coefficients in $\mathcal{O}_{\mathbb{C}_p} \cap M = \mathcal{O}_M$. □

Remark 2.3. It is proved in [3, IV §1, Prop. 4] that if K is a closed discretely valued subfield of $\mathbb{C}_p$ and $F(X,Y)$ is formal group law defined over $\mathcal{O}_K$ then the conclusion to Proposition 2.2 is valid with J_h replaced by the compositum of the extensions $L/\mathbb{Q}_p$ such that $[L:\mathbb{Q}_p]$ *divides* h. One could obtain this improved version of Proposition 2.2 for general $K \subset \mathbb{C}_p$ using the fact (stated without proof in [7, 2.3.0]) that the reduction map from $\mathrm{End}_{\mathcal{O}_{\mathbb{C}_p}}(F)$ to $\mathrm{End}_{\mathbb{F}_p^{alg}}(\overline{F})$ is injective.

Proposition 2.4. *Let F, G be formal group laws over $\mathcal{O}_{\mathbb{C}_p}$ such that F has height $h < \infty$, and let $\phi : F \to G$ be a nonzero homomorphism over $\mathcal{O}_{\mathbb{C}_p}$. Then there is no $c \in \mathcal{M}_{\mathbb{C}_p}$ such that c divides every coefficient of $\phi(X)$.*

Proof. Write $[p]_F(X) = a_1X + a_2X^2 + \cdots$ and choose $1 \le j < p^h$ such that $v_p(a_j) \le v_p(a_i)$ for $1 \le i < p^h$. Since $a_1 = p$ and $F(X,Y)$ has height h we have $0 < v_p(a_j) \le 1$. Let S be the set of elements of $\mathcal{O}_{\mathbb{C}_p}$ which divide $\phi(X)$

in $\mathcal{O}_{\mathbb{C}_p}[[X]]$, and set $m = \sup\{v_p(a) : a \in S\}$. If $m > 0$ then there exists $c \in \mathcal{O}_{\mathbb{C}_p}$ such that $\frac{1}{2}m < v_p(c) < m$ and $v_p(c) > m - v_p(a_j)$. Since $v_p(c) < m$ we have $\phi(X) = c\psi(X)$ for some $\psi(X) = b_1X + b_2X^2 + \cdots \in \mathcal{O}_{\mathbb{C}_p}[[X]]$. Since $m - v_p(c) < v_p(a_j)$ and $m - v_p(c) < v_p(c)$, the b_i do not all lie in the ideal $I = (c, a_j)$ of $\mathcal{O}_{\mathbb{C}_p}$. Let n be the smallest positive integer such that $b_n \notin I$. Since $\phi([p]_F(X)) = [p]_G(\phi(X))$ we have

$$c\psi([p]_F(X)) = [p]_G(c\psi(X)). \tag{2.2}$$

The coefficients on the right side of (2.2) all lie in cI. Since

$$\psi(X) \equiv b_nX^n + \cdots \pmod{I} \tag{2.3}$$

$$[p]_F(X) \equiv a_{p^h}X^{p^h} + \cdots \pmod{I} \tag{2.4}$$

with $a_{p^h} \in \mathcal{O}_{\mathbb{C}_p}^\times$, the coefficient of X^{np^h} on the left side of (2.2) does not lie in cI. This is a contradiction, so we must have $m = 0$. Hence $\phi(X)$ is not divisible by any element of $\mathcal{M}_{\mathbb{C}_p}$. □

Corollary 2.5. *Let F, G be formal group laws over $\mathcal{O}_{\mathbb{C}_p}$ such that F has finite height, and let $\phi : F \to G$ be a homomorphism defined over $\mathcal{O}_{\mathbb{C}_p}$ which has trivial kernel. Then $\phi(X)$ is an isomorphism.*

Proof. Since $\phi(X) = a_1X + a_2X^2 + \cdots$ is nonzero and $\mathcal{O}_{\mathbb{C}_p}$ has characteristic 0 we have $a_1 \neq 0$. If $\phi(X)$ is not an isomorphism then $v_p(a_1) > 0$. Using Proposition 2.4 we see that $\phi(X)$ is not divisible by any element of $\mathcal{M}_{\mathbb{C}_p}$. Therefore the Newton polygon of $\phi(X)$ has at least one segment with negative slope. Hence by Proposition 1.3 we have $\phi(X) = \psi(X)f(X)$ with $\psi(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ and $f(X) \in \mathcal{O}_{\mathbb{C}_p}[X]$ a distinguished polynomial of degree $d > 1$. It follows that $\phi(X)$ has a nontrivial zero in $\mathcal{M}_{\mathbb{C}_p}$, contrary to assumption. Therefore $\phi : F \to G$ is an isomorphism. □

The following proposition is an apparent generalization of Theorem 1.4 in [6]. The result presented here applies to homomorphisms $\phi(X)$ defined over $\mathcal{O}_{\mathbb{C}_p}$, rather than over the ring of integers of a finite extension of K as in [6]. However, it will follow from Theorem 3.2 that every $\phi(X)$ which satisfies the hypotheses of Proposition 2.6 also satisfies the hypotheses of [6, Th. 1.4]. The more general statement given below is needed for the proof of Theorem 3.2.

Proposition 2.6. *Let K be a discretely valued subfield of $\mathbb{C}_p$ and let F, G be formal group laws defined over $\mathcal{O}_K$ such that F has height $h < \infty$. Let $\phi : F \to G$ be a homomorphism defined over $\mathcal{O}_{\mathbb{C}_p}$ such that $W = \ker(\phi)$ is finite, and let L be the closure of $K(W)$ in $\mathbb{C}_p$. Then L is discretely valued and there is a formal group law G' defined over $\mathcal{O}_L$, a homomorphism $\phi' : F \to G'$ defined over $\mathcal{O}_L$, and an isomorphism $i : G' \to G$ defined over $\mathcal{O}_{\mathbb{C}_p}$ such that $i \circ \phi' = \phi$. Furthermore, G and G' both have height h.*

Proof. Since W is a finite subgroup of $F(\mathcal{M}_{\mathbb{C}_p})$ we have $W \le \ker([p^n]_F(X))$ for some $n \ge 0$. By the Weierstrass preparation theorem the elements of $\ker([p^n]_F(X))$ are the roots of a distinguished polynomial with coefficients in $\mathcal{O}_K$. Hence $[K(W) : K] < \infty$, so $K(W)$ is discretely valued. It follows that L is discretely valued as well.

By [6, Th. 1.4] there is a formal group law G' defined over $\mathcal{O}_L$ such that the power series

$$\phi'(X) = \prod_{\gamma \in W} F(X, \gamma) \in \mathcal{O}_L[[X]] \tag{2.5}$$

is a homomorphism from F to G' with kernel W. By considering the reduction modulo $\mathcal{M}_{\mathbb{C}_p}$ of the formula $\phi' \circ [p]_F = [p]_{G'} \circ \phi'$ we see that G' has the same height h as F. Set $\xi = \phi'(X)$ and $A_0 = \mathcal{O}_K[[\xi]] \subset \mathcal{O}_L[[\mathrm{X}]]$. Then by [6, Lemma 1.3] the power series

$$Q(T) = -\xi + \prod_{\gamma \in W} F(T, \gamma) \tag{2.6}$$

lies in $A_0[[T]]$. Since A_0 is a complete Noetherian local ring, by the general form of the Weierstrass preparation theorem [1, 10.2.4] we have $Q(T) = U(T)H(T)$, where $U(T) \in A_0[[T]]^\times$ and $H(T) \in A_0[T]$ has degree $|W|$.

We now construct $i(X)$ by imitating the proof of [6, Lemma 1.3]. Set $A = \mathcal{O}_{\mathbb{C}_p}[[\xi]]$, $B = \mathcal{O}_{\mathbb{C}_p}[[X]]$, $\mathcal{K} = \mathrm{Frac}(A)$, and $\mathcal{L} = \mathrm{Frac}(B)$. Then $\mathcal{L} = \mathcal{K}(X)$ and X is a root of $H(T)$, so we have $[\mathcal{L} : \mathcal{K}] \le \deg(H) = |W|$. On the other hand, for $\gamma \in W$ and $\Delta(X) \in \mathcal{L}$ define $(\gamma \cdot \Delta)(X) = \Delta(F(X, \gamma))$; the right side of this equation makes sense because $v_p(\gamma) > 0$. This gives a faithful $\mathbb{C}_p$-linear action of W on $\mathcal{L}$. By (2.5) we have $\gamma \cdot \xi = \xi$ for every $\gamma \in W$. Thus $\mathcal{K}$ is contained in the fixed field $\mathcal{L}^W$ of W, so we have $[\mathcal{L} : \mathcal{K}] \ge |W|$. Hence $[\mathcal{L} : \mathcal{K}] = |W|$ and $\mathcal{K} = \mathcal{L}^W$. Since B is free of rank $|W|$ over A, with basis $\{1, X, X^2, \dots, X^{|W|-1}\}$, we have $A = \mathcal{K} \cap B = \mathcal{L}^W \cap B = B^W$. Since $\phi(X) \in B^W = A$ there is $i(X) \in \mathcal{O}_{\mathbb{C}_p}[[X]]$ such that $\phi(X) = i(\xi)$. Thus $\phi = i \circ \phi'$.

Since $\phi' : F \to G'$ and $\phi : F \to G$ are formal group law homomorphisms, $i(X)$ is a homomorphism from G' to G. If $\alpha \in \ker(i)$ then by Corollary 1.5 there is $\beta \in \mathcal{M}_{\mathbb{C}_p}$ such that $\phi'(\beta) = \alpha$. Hence $\phi(\beta) = i(\phi'(\beta)) = i(\alpha) = 0$, so $\beta \in W$. Since $\ker \phi' = W$ we get $\alpha = \phi'(\beta) = 0$, and hence $\ker(i) = \{0\}$. It follows from Corollary 2.5 that $i(X)$ is an isomorphism. Since G' has the same height h as F and G is isomorphic to G' over $\mathcal{O}_{\mathbb{C}_p}$ we deduce that G also has height h. □

3. Homomorphisms of formal group laws

Let K be a discretely valued subfield of $\mathbb{C}_p$ and let F, G be formal group laws over $\mathcal{O}_K$ with the same finite height. In this section we prove that there is a closed discretely valued subfield M of $\mathbb{C}_p$ such that every homomorphism from F to G is defined over $\mathcal{O}_M$.

To begin we assume that K is closed in $\mathbb{C}_p$ as well as discretely valued. Since $\mathcal{O}_K$ is an integral domain of characteristic 0 we may identify $\mathrm{End}_{\mathcal{O}_K}(F)$ with a subring of $\mathcal{O}_K$ using the map $D_F : \mathrm{End}_{\mathcal{O}_K}(F) \to \mathcal{O}_K$ which maps $\phi(X) = a_1X + a_2X^2 + \cdots$ onto $D_F(\phi) = a_1$. If $D_F(\psi) = b$ we write $\psi(X) = [b]_F(X)$. Let A be a $\mathbb{Z}_p$-subalgebra of $\mathrm{End}_{\mathcal{O}_K}(F)$; then D_F identifies A with a subring of $\mathcal{O}_K$. Hence $E = \mathrm{Frac}(A)$ is a subfield of K which is a finite extension of $\mathbb{Q}_p$. The Tate module $T_p(F)$ is a module over A, and $V_p(F) = T_p(F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a vector space over E. Let K^{alg} be the algebraic closure of K in $\mathbb{C}_p$, and let K^{ab}/K, K^{nr}/K be the maximum abelian subextension and the maximum unramified subextension of K^{alg}/K. The action of Galois on $V_p(F)$ gives a representation

$$\rho_F : \mathrm{Gal}(K^{alg}/K) \longrightarrow \mathrm{Aut}_E(V_p(F)). \tag{3.1}$$

For $\sigma \in \mathrm{Gal}(K^{alg}/K^{nr})$ let $\widetilde{\sigma}$ denote the restriction of σ to $\mathrm{Gal}(E^{ab}/E^{nr})$, and let $u_{\widetilde{\sigma}}$ be the element of $\mathcal{O}_E^\times$ which corresponds to $\widetilde{\sigma}$ under the reciprocity isomorphism $\mathrm{Gal}(E^{ab}/E^{nr}) \cong \mathcal{O}_E^\times$ of local class field theory. Then the map

$$\psi_E^K : \mathrm{Gal}(K^{alg}/K^{nr}) \longrightarrow \mathcal{O}_E^\times \tag{3.2}$$

defined by $\psi_E^K(\sigma) = u_{\widetilde{\sigma}}$ is a homomorphism.

The following is a slight generalization of a theorem proved by Strauch [11, Th. 3.3] in the case $A = \mathcal{O}_E$. The case $A = \mathbb{Z}_p$ was proved by Raynaud [9, Prop. 4.2].

Proposition 3.1. *Let K be a closed discretely valued subfield of $\mathbb{C}_p$ and let $F(X,Y)$ be a formal group law over $\mathcal{O}_K$ with finite height. Let A be a $\mathbb{Z}_p$-subalgebra of* $\mathrm{End}_{\mathcal{O}_K}(F)$*, set* $E = \mathrm{Frac}(A)$*, and let*

$$\rho_F : \mathrm{Gal}(K^{alg}/K) \longrightarrow \mathrm{Aut}_E(V_p(F))$$

be the Galois representation associated to F. Then $\det(\rho_F(\sigma)) = \psi_E^K(\sigma)^{-1}$ *for every* $\sigma \in \mathrm{Gal}(K^{alg}/K^{nr})$*, where ψ_E^K is induced by the class field theory isomorphism* $\mathrm{Gal}(E^{ab}/E^{nr}) \cong \mathcal{O}_E^\times$.

Proof. By [6, p. 301] there exist a formal $\mathcal{O}_E$-module (F', j') and a nonzero homomorphism $\pi : F \to F'$, both defined over $\mathcal{O}_K$. The map π induces a $\mathrm{Gal}(K^{alg}/K)$-equivariant $\mathbb{Z}_p$-module homomorphism

$$T_p(\pi) : T_p(F) \longrightarrow T_p(F') \tag{3.3}$$

which is one-to-one with finite cokernel. Thus the induced map

$$V_p(\pi) : V_p(F) \longrightarrow V_p(F') \tag{3.4}$$

is a $\mathrm{Gal}(K^{alg}/K)$-equivariant isomorphism which is E-linear since

$$\pi \circ [a]_F = [a]_{F'} \circ \pi \tag{3.5}$$

for $a \in A$. It follows that $\det(\rho_F(\sigma)) = \det(\rho_{F'}(\sigma))$ for $\sigma \in \mathrm{Gal}(K^{alg}/K)$. Since (F', j') is a formal $\mathcal{O}_E$-module, by Strauch's result [11, Th. 3.3] we have

$\det(\rho_{F'}(\sigma)) = \psi_E^K(\sigma)^{-1}$ for every $\sigma \in \mathrm{Gal}(K^{alg}/K^{nr})$. Hence $\det(\rho_F(\sigma)) = \psi_E^K(\sigma)^{-1}$ for $\sigma \in \mathrm{Gal}(K^{alg}/K^{nr})$. □

We now use Propositions 2.6 and 3.1 to prove our main result.

Theorem 3.2. *Let K be a discretely valued subfield of $\mathbb{C}_p$, let F, G be formal group laws over $\mathcal{O}_K$ such that F has height $h < \infty$, and let $\phi : F \to G$ be a homomorphism over $\mathcal{O}_{\mathbb{C}_p}$ with finite kernel. Then there is a closed discretely valued subfield M of $\mathbb{C}_p$ such that $\phi(X)$ has coefficients in $\mathcal{O}_M$.*

Proof. Let $W = \ker(\phi)$ and let L be the closure of $K(W)$ in $\mathbb{C}_p$. Then by Proposition 2.6 there is a formal group law $G'(X,Y)$ over $\mathcal{O}_L$, a homomorphism $\phi' : F \to G'$ over $\mathcal{O}_L$, and an isomorphism $i : G' \to G$ over $\mathcal{O}_{\mathbb{C}_p}$ such that $i \circ \phi' = \phi$. Furthermore, L is discretely valued and G, G' both have height h. Recall that J_h is the compositum of all the extensions of $\mathbb{Q}_p$ of degree $\le h$, and let N be the closure in $\mathbb{C}_p$ of the maximum unramified extension of LJ_h. Since $J_h/\mathbb{Q}_p$ is finite, N is discretely valued. To prove the theorem it suffices to show that there is a finite extension M/N such that i is defined over $\mathcal{O}_M$.

Let $A = \{a_1 : a_1X + a_2X^2 + \cdots \in \mathrm{End}_{\mathcal{O}_{\mathbb{C}_p}}(G)\}$ be the image of D_G, and let E be the field of fractions of A. By Lemma 2.1 we have $A \subset \mathcal{O}_{J_h}$, which implies that E is contained in N. Therefore for $\sigma \in \mathrm{Gal}(K^{alg}/N)$ we have $i^\sigma \circ i^{-1} \in \mathrm{Aut}_{\mathcal{O}_{\mathbb{C}_p}}(G) \cong A^\times$, and hence $i^\sigma \circ i^{-1} = [a_\sigma]_G$ for some $a_\sigma \in A^\times$. Let $T_p(i) : T_p(G') \to T_p(G)$ be the isomorphism induced by i. Then for $v \in T_p(G')$ we have

$$\sigma(T_p(i)(v)) = T_p(i^\sigma)(\sigma \cdot v) = T_p([a_\sigma]_G \circ i)(\sigma \cdot v) = a_\sigma T_p(i)(\sigma \cdot v). \tag{3.6}$$

Let

$$\rho_G : \mathrm{Gal}(K^{alg}/N) \longrightarrow \mathrm{Aut}_E(V_p(G)) \tag{3.7}$$

$$\rho_{G'} : \mathrm{Gal}(K^{alg}/N) \longrightarrow \mathrm{Aut}_E(V_p(G')) \tag{3.8}$$

be the representations associated to G and G'. It follows from (3.6) that

$$\rho_G(\sigma) \circ T_p(i) = a_\sigma T_p(i) \circ \rho_{G'}(\sigma). \tag{3.9}$$

Since $T_p(i)$ induces an isomorphism $V_p(i) : V_p(G') \to V_p(G)$ we get

$$\det(\rho_G(\sigma)) = \det(a_\sigma \rho_{G'}(\sigma)) = a_\sigma^d \det(\rho_{G'}(\sigma)), \tag{3.10}$$

where $d = \dim_E(V_p(G')) = h/[E : \mathbb{Q}_p]$. Hence by Proposition 3.1 we have $a_\sigma^d = 1$ for every $\sigma \in \mathrm{Gal}(K^{alg}/N)$. One easily verifies that the map

$$\lambda : \mathrm{Gal}(K^{alg}/N) \longrightarrow A^\times \tag{3.11}$$

defined by $\lambda(\sigma) = a_\sigma$ is a continuous homomorphism. Hence the fixed field M of the kernel of λ is an extension of N of degree $\le d$. Since $i^\sigma(X) = i(X)$ for all $\sigma \in \mathrm{Gal}(K^{alg}/M)$, the coefficients of $i(X)$ lie in the subfield of $\mathbb{C}_p$ fixed by $\mathrm{Gal}(K^{alg}/M)$. Since the completion of K^{alg} is $\mathbb{C}_p$, it follows from

Ax's theorem [2] that the fixed field of $\mathrm{Gal}(K^{alg}/M)$ acting on $\mathbb{C}_p$ is M. Hence $i(X)$ has coefficients in $M \cap \mathcal{O}_{\mathbb{C}_p} = \mathcal{O}_M$. □

Remark 3.3. It is well-known that there need not exist a *finite* extension M/K such that the coefficients of $\phi(X)$ lie in $\mathcal{O}_M$. Indeed, let K be a finite extension of $\mathbb{Q}_p$, let $K^{nr} \subset \mathbb{C}_p$ be the maximum unramified extension of K, and let N be the closure in $\mathbb{C}_p$ of K^{nr}. Let F be a formal group law over $\mathcal{O}_K$ and let $\alpha(X)$ be an automorphism of F which is defined over $\mathcal{O}_K$ and has infinite order. Then by imitating the proof of [3, III §3, Prop. 3] we see that there is an invertible power series $\phi(X) \in \mathcal{O}_N[[X]]$ such that $\phi^\sigma(X) = \phi(\alpha(X))$, where σ is the continuous automorphism of N induced by the Frobenius element of $\mathrm{Gal}(K^{nr}/K)$. Define $G(X,Y) = \phi(F(\phi^{-1}(X), \phi^{-1}(Y)))$. Then $G(X,Y)$ is a formal group law over $\mathcal{O}_K$ and $\phi(X) \in \mathcal{O}_N[[X]]$ is an isomorphism from F to G. But $\phi(X)$ is not defined over $\mathcal{O}_M$ for any finite extension M of K.

We now consider the properties of homomorphisms $\phi : F \to G$ over $\mathcal{O}_{\mathbb{C}_p}$ with infinite kernel. In Example 3.8 we will construct an example of such a homomorphism.

Lemma 3.4. *Let F, G be formal group laws of finite height over $\mathcal{O}_{\mathbb{C}_p}$ and let $\phi : F \to G$ be a nonzero homomorphism defined over $\mathcal{O}_{\mathbb{C}_p}$. Then for every $\alpha \in \ker(\phi)$ there is $n \geq 0$ such that $[p^n]_F(\alpha) = 0$.*

Proof. Let $\alpha \in \ker(\phi)$. For any $\beta \in \mathcal{M}_{\mathbb{C}_p}$ we have

$$v_p([p]_F(\beta)) \geq \min\{v_p(\beta) + 1, 2v_p(\beta)\}. \tag{3.12}$$

Hence if α is not p^n-torsion for any $n \geq 0$ then $(v_p([p^n]_F(\alpha)))_{n\geq 0}$ is a sequence of rational numbers which increases without bound. By considering the Newton polygon of $\phi(X)$ we see that the valuations of the nonzero elements of $\ker(\phi)$ are bounded above. Therefore for n sufficiently large we have $[p^n]_F(\alpha) \notin \ker(\phi)$, and hence $\alpha \notin \ker(\phi)$. This is a contradiction, so $[p^n]_F(\alpha) = 0$ for some $n \geq 0$. □

Proposition 3.5. *Let F, G be formal group laws over $\mathcal{O}_{\mathbb{C}_p}$ whose heights h_F, h_G are finite. Suppose there exists a nonzero homomorphism $\phi : F \to G$ over $\mathcal{O}_{\mathbb{C}_p}$. Then $h_F \geq h_G$. Furthermore, if $\ker(\phi)$ is infinite then $h_F > h_G$.*

Proof. Let $F(\mathcal{M}_{\mathbb{C}_p})^{tor}$, $G(\mathcal{M}_{\mathbb{C}_p})^{tor}$ denote the torsion subgroups of the point groups $F(\mathcal{M}_{\mathbb{C}_p})$, $G(\mathcal{M}_{\mathbb{C}_p})$. We claim that ϕ maps $F(\mathcal{M}_{\mathbb{C}_p})^{tor}$ onto $G(\mathcal{M}_{\mathbb{C}_p})^{tor}$. Let $\alpha \in G(\mathcal{M}_{\mathbb{C}_p})^{tor}$; then $[p^n]_G(\alpha) = 0$ for some $n \geq 0$. It follows from Proposition 2.4 that α does not divide $\phi(X)$ in $\mathcal{O}_{\mathbb{C}_p}[[X]]$. Therefore by Corollary 1.5 there is $\beta \in \mathcal{M}_{\mathbb{C}_p}$ such that $\phi(\beta) = \alpha$. Hence

$$\phi([p^n]_F(\beta)) = [p^n]_G(\phi(\beta)) = [p^n]_G(\alpha) = 0, \tag{3.13}$$

so we have $[p^n]_F(\beta) \in \ker(\phi)$. It follows from Lemma 3.4 that $[p^n]_F(\beta)$ is p^m-torsion for some $m \geq 0$. Therefore β is p^{m+n}-torsion, and hence

$\beta \in F(\mathcal{M}_{\mathbb{C}_p})^{tor}$. By Lemma 3.4 we have $\ker(\phi) \subset F(\mathcal{M}_{\mathbb{C}_p})^{tor}$, and hence $G(\mathcal{M}_{\mathbb{C}_p})^{tor} \cong F(\mathcal{M}_{\mathbb{C}_p})^{tor}/\ker(\phi)$. Since

$$F(\mathcal{M}_{\mathbb{C}_p})^{tor} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{h_F}, \quad G(\mathcal{M}_{\mathbb{C}_p})^{tor} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{h_G}, \tag{3.14}$$

we get $h_F \geq h_G$, and $h_F > h_G$ if $\ker(\phi)$ is infinite. □

Remark 3.6. Assume $\ker(\phi)$ is infinite and write $\phi(X) = a_1X + a_2X^2 + \cdots$. It follows from Proposition 2.4 that there is no $c \in \mathcal{M}_{\mathbb{C}_p}$ such that $a_i \in c\mathcal{O}_{\mathbb{C}_p}$ for every $i \geq 1$. On the other hand, if $a_i \in \mathcal{O}_{\mathbb{C}_p}^{\times}$ for some i then $\phi(X)$ has finite Weierstrass degree, and hence finite kernel, contrary to assumption. Therefore the coefficients $a_1, a_2, \ldots$ of $\phi(X)$ generate the ideal $\mathcal{M}_{\mathbb{C}_p}$ in $\mathcal{O}_{\mathbb{C}_p}$, and the Newton polygon of $\phi(X)$ is asymptotic to the x-axis.

Using Proposition 3.5 we get a stronger version of Theorem 3.2.

Corollary 3.7. *Let K be a discretely valued subfield of $\mathbb{C}_p$ and let F, G be formal group laws over $\mathcal{O}_K$ with the same finite height h. Then there is a closed discretely valued subfield M of $\mathbb{C}_p$ such that every element of $\mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(F, G)$ has coefficients in $\mathcal{O}_M$.*

Proof. Let N be the closure in $\mathbb{C}_p$ of the maximum unramified extension of K. It follows from Proposition 3.5 and Theorem 3.2 that for every $\phi(X) \in \mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(F, G)$ there is a finite extension M_ϕ/N such that $\phi(X) \in \mathcal{O}_{M_\phi}[[X]]$. Hence by [3, IV §1, Prop. 3] the reduction map from $\mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(F, G)$ to $\mathrm{Hom}_{\mathbb{F}_p^{alg}}(\overline{F}, \overline{G})$ is injective. Since $\mathrm{Hom}_{\mathbb{F}_p^{alg}}(\overline{F}, \overline{G})$ is a free $\mathbb{Z}_p$-module of rank h^2 [3, IV §1, Lemma 1] it follows that $\mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(F, G)$ is a free $\mathbb{Z}_p$-module of finite rank. For a $\mathbb{Z}_p$-basis $\{\phi_1, \ldots, \phi_r\}$ of $\mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(F, G)$, let M be the compositum of the fields $M_{\phi_1}, \ldots, M_{\phi_r}$. Then M is a closed discretely valued subfield of $\mathbb{C}_p$ and every element of $\mathrm{Hom}_{\mathcal{O}_{\mathbb{C}_p}}(F, G)$ has coefficients in $\mathcal{O}_M$. □

We conclude by giving an example of a nonzero homomorphism whose kernel is infinite. We first recall some definitions. Let K be a subfield of $\mathbb{C}_p$ and let $F(X, Y)$ be a formal group law of height $h < \infty$ over $\mathcal{O}_K$. The p^n-torsion group scheme $F(p^n)$ of F is defined to be the affine scheme $\mathrm{Spec}(\mathcal{O}_K[[X]]/([p^n]_F(X)))$ with the group operation induced by $F(X, Y)$. Thus $F(p^n)$ is a connected group scheme of order p^{nh} over $\mathcal{O}_K$. The p-divisible group $F(p^\infty)$ of F is defined to be the injective system of the p^n-torsion group schemes $F(p^n)$ for $n \geq 1$.

I thank Jonathan Lubin for pointing out the following example to me.

Example 3.8. Let K be a discretely valued subfield of $\mathbb{C}_p$ and let E be an elliptic curve over $\mathcal{O}_K$ whose special fiber $E \otimes (\mathcal{O}_K/\mathcal{M}_K)$ is supersingular. By choosing a parameter we get a formal group law $\hat{E}$ for E. Since E has supersingular reduction, the p^n-torsion subgroup scheme $\hat{E}(p^n)$ of $\hat{E}$ can be identified with the p^n-torsion subgroup scheme $E(p^n)$ of E. Hence the Weil pairing on $E(p^n)$ induces a nondegenerate bilinear map of group schemes over $\mathcal{O}_K$

$$(\, , \,)_{p^n} : \hat{E}(p^n) \times \hat{E}(p^n) \longrightarrow \mathbb{G}_m(p^n), \tag{3.15}$$

where $\mathbb{G}_m(p^n)$ is the p^n-torsion subgroup scheme of the multiplicative formal group law $\mathbb{G}_m$. Let $Q_n \in \hat{E}(\mathcal{M}_{\mathbb{C}_p})$ be a point of order p^n. Then

$$(Q_n, *)_{p^n} : \hat{E}(p^n) \longrightarrow \mathbb{G}_m(p^n) \tag{3.16}$$

is a surjective group scheme homomorphism defined over $\mathcal{O}_{\mathbb{C}_p}$. By choosing a sequence $(Q_n)_{n\geq 1}$ of points of order p^n such that $Q_n = [p]_E(Q_{n+1})$ for all $n \geq 1$ we get a surjective homomorphism $\phi_p : \hat{E}(p^\infty) \to \mathbb{G}_m(p^\infty)$ of p-divisible groups over $\mathcal{O}_{\mathbb{C}_p}$.

Let R be a complete Noetherian ring whose residue field has characteristic p. In [12, Prop. 1] Tate showed that the functor $F \mapsto F(p^\infty)$ gives an equivalence from the category of formal group laws of finite height over R to the category of connected p-divisible groups over R. The proof that the induced map from $\mathrm{Hom}_R(F, G)$ to $\mathrm{Hom}_R(F(p^\infty), G(p^\infty))$ is a bijection is valid for non-Noetherian rings R as long as there is a Noetherian subring R_0 of R such that the formal group laws $F(X, Y)$ and $G(X, Y)$ are both defined over R_0. Hence we can apply Tate's result to show that ϕ_p is induced by a nonzero homomorphism $\phi : \hat{E} \to \mathbb{G}_m$ which is defined over $\mathcal{O}_{\mathbb{C}_p}$. The kernel of ϕ is the infinite subgroup of $\hat{E}(\mathcal{M}_{\mathbb{C}_p})$ generated by the set $\{Q_n : n \geq 1\}$. It follows from Remark 3.6 that $\phi(X)$ is not defined over any discretely valued subfield of $\mathbb{C}_p$. Therefore the conclusion to Theorem 3.2 does not hold if we allow $\ker(\phi)$ to be infinite.

References

[1] ABHYANKAR, SHREERAM SHANKAR. Local analytic geometry. Pure and Applied Mathematics, Vol. XIV. *Academic Press, New York-London*, 1964. xv+484 pp. MR0175897 (31 #173), Zbl 0205.50401.

[2] AX, JAMES. Zeros of polynomials over local fields—The Galois action. *J. Algebra* **15** (1970) 417–428. MR0263786 (41 #8386), Zbl 0216.04703.

[3] FRÖHLICH, ALBRECHT. Formal groups. Lecture Notes in Mathematics, 74. *Springer-Verlag, Berlin-New York*, 1968. iii+140 pp. MR0242837 (39 #4164), Zbl 0177.04801.

[4] HAZEWINKEL, MICHIEL. Formal groups and applications. Pure and Applied Mathematics, 78. *Academic Press, New York*, 1978. xxii+573pp. ISBN: 0-12-335150-2. MR0506881 (82a:14020), Zbl 0454.14020.

[5] KOBLITZ, NEAL. p-adic numbers, p-adic analysis, and zeta-functions. Graduate Texts in Mathematics, 58. *Springer-Verlag, New York-Heidelberg*, 1977. xii+150 pp. ISBN: 0-387-96017-1. MR0754003 (86c:11086), Zbl 0364.12015.

[6] LUBIN, JONATHAN. Finite subgroups and isogenies of one-parameter formal Lie groups. *Ann. of Math.* (2) **85** (1967) 296–302. MR0209287 (35 #189), Zbl 0166.02803.

[7] LUBIN, JONATHAN. One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings. *Ann. of Math.* (2) **80** (1964) 464–484. MR0168567 (29 #5827), Zbl 0135.07003. Correction. *Ann. of Math.* (2) **84** (1966) 372. MR0200280 (34 #179), Zbl 0146.25702.

[8] LUBIN, JONATHAN; TATE, JOHN. Formal complex multiplication in local fields. *Ann. of Math.* (2) **81** (1965) 380–387. MR0172878 (30 #3094), Zbl 0128.26501.

[9] RAYNAUD, MICHEL. Schémas en groupes de type $(p,\ldots,p)$. *Bull. Soc. Math. France* **102** (1974) 241–280. MR0419467 (54 #7488), Zbl 0325.14020.

[10] SCHMITZ, DAVID J. Endomorphism rings of almost full formal groups. *New York Journal of Mathematics* **12** (2006) 219–233. MR2242534 (2007f:11131), Zbl 1118.14053.

[11] STRAUCH, MATTHIAS. Geometrically connected components of Lubin-Tate deformation spaces with level structures. *Pure and Applied Mathematics Quarterly* **4** (2008) 1215–1232. MR2441699 (2009e:11116).

[12] TATE, JOHN. p-divisible groups. *Proceedings of a Conference on Local Fields* (Driebergen, 1966) pp. 158–183. *Springer-Verlag, Berlin-New York*, 1967. MR0231827 (38 #155), Zbl 0157.27601.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, GAINESVILLE, FL 32611, USA
keating@ufl.edu

This paper is available via http://nyjm.albany.edu/j/2009/15-25.html.