New York Journal of Mathematics

New York J. Math. **12** (2006) 219–233.

Endomorphism rings of almost full formal groups

David J. Schmitz

Abstract. Let $\mathfrak{o}_K$ be the integral closure of $\mathbb{Z}_p$ in a finite field extension K of $\mathbb{Q}_p$, and let F be a one-dimensional full formal group defined over $\mathfrak{o}_K$. We study certain finite subgroups C of F and prove a conjecture of Jonathan Lubin concerning the absolute endomorphism ring of the quotient F/C when F has height 2. We also investigate ways in which this result can be generalized to p-adic formal groups of higher height.

Contents

Introduction

In September, 2000, Jonathan Lubin conveyed to me the following two conjectures of his describing the quotients of full and almost full height 2 p-adic formal groups by certain finite subgroups:

Conjecture 1. *Let F be a full p-adic formal group of height 2, and let C be a cyclic subgroup of F having order p^n. Assume that* $\mathrm{End}(F)$*, the absolute endomorphism ring of F, is isomorphic to the ring of integers $\mathfrak{o}_K$ in a quadratic p-adic number field K; assume further that if $K/\mathbb{Q}_p$ is totally ramified, then C does not contain $\ker\,[\pi]_F$, where π is a uniformizer of $\mathfrak{o}_K$. Then* $\mathrm{End}(F/C) \cong \mathbb{Z}_p + p^n\,\mathfrak{o}_K$.

Conjecture 2. *Suppose G is an almost full p-adic formal group of height 2 with* $\mathrm{End}(G) \cong \mathbb{Z}_p + p^n\mathfrak{o}$*, where $\mathfrak{o}$ is some p-adic integer ring. Then there is a cyclic subgroup D of G of order p^n, canonical somehow, such that G/D is full.*

Received February 28, 2006.

Mathematics Subject Classification. 11S31, 14L05.

Key words and phrases. p-adic formal groups, endomorphism rings.

ISSN 1076-9803/06

We prove the first of these conjectures in this paper as Theorem 6.3. Furthermore, as we describe below, we are able to generalize this result in a couple of ways to p-adic formal groups of arbitrary (finite) height. The proofs of Conjecture 2 and some its generalizations are left for a subsequent paper. (See [S].)

If F is a p-adic formal group with $\mathrm{End}(F)$ integrally closed, then $c : g \mapsto g'(0)$ defines an isomorphism from $\mathrm{End}(F)$ onto a p-adic integer ring $\mathfrak{o}$. Via this association, we can view the torsion subgroup $\Lambda(F)$ of F as an $\mathfrak{o}$-module. For a finite subgroup C of $\Lambda(F)$, we denote by $\mathcal{I}(C)$ the annihilator of C in $\mathfrak{o}$. We prove the following as Theorem 4.3:

Theorem 1. *Let F be a p-adic formal group such that $\mathrm{End}(F)$ is integrally closed. If C is a finite cyclic subgroup of $\Lambda(F)$, then $c\big(\mathrm{End}(F/C)\big) = \mathbb{Z}_p + \mathcal{I}(C)$.*

This generalizes Conjecture 1 since $\mathcal{I}(C) = p^n\mathfrak{o}$ for the finite subgroups described there.

We are also able to say something about $c\big(\mathrm{End}(F/C)\big)$ when C is not necessarily cyclic. We will say that a finite subgroup C of the torsion subgroup of a p-adic formal group F is *a deflated subgroup of F* if there is no finite subgroup D of $\Lambda(F)$ having fewer elements than C such that $F/D \cong F/C$. We show in Section 3 that if F is full, then C is a deflated subgroup of F if and only if C does not contain the kernel of any noninvertible F-endomorphism. Lubin proves in [Lu2] that if F is full, then for any finite subgroup C of $\Lambda(F)$, $c(\mathrm{End}(F/C))$ is a subring of $c(\mathrm{End}(F))$. More specifically, we prove as Theorem 4.4:

Theorem 2. *Let F be a full p-adic formal group, and let C be a deflated subgroup of F. The conductor of $c\big(\mathrm{End}(F)\big)$ with respect to $c\big(\mathrm{End}(F/C)\big)$ is $\mathcal{I}(C)$.*

In Section 1, we review the basic theory of p-adic formal groups, paying particular attention to the integer rings over which certain homomorphisms are defined; we point out when some of the theorems from [Lu2] can be extended in this respect. In Section 2, we use the Tate module of F to study the $\mathrm{End}(F)$-module structure of the torsion subgroup of F. After describing the basic properties of deflated subgroups in Section 3, we prove in the final sections several theorems concerning almost full p-adic formal groups, including Theorem 1, Theorem 2, and Conjecture 1. We also see what other conclusions can be drawn in the height 2 case using our general theorems.

1. *p*-adic formal groups and isogenies

Fix a prime p. Let $\mathbb{C}_p$ be the completion of a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ with respect to the unique extension of the p-adic valuation v on $\mathbb{Q}_p$ normalized so that $v(p) = 1$. Then v extends uniquely to a rational valuation on $\mathbb{C}_p$, and we denote this valuation by v as well. Let $\overline{\mathbb{Z}}_p$ (resp., $\mathfrak{O}$) be the set of elements in $\overline{\mathbb{Q}}_p$ (resp., in $\mathbb{C}_p$) with nonnegative valuation, and let $\overline{\mathfrak{m}}$ (resp., $\mathfrak{M}$) be the maximal ideal of $\overline{\mathbb{Z}}_p$ (resp., of $\mathfrak{O}$). For any subfield K of $\mathbb{C}_p$, we denote by $\mathfrak{o}_K$ the integer ring of K, i.e., $\mathfrak{o}_K = K \cap \mathfrak{O}$. Subfields of $\mathbb{C}_p$ which are finite extensions of $\mathbb{Q}_p$ are called *p-adic number fields*, and their integer rings are called *p-adic integer rings*. We define a *p-adic formal group* to be a one-dimensional formal group of finite height defined over a p-adic integer ring.

We will first review some of the basic results from the theory of p-adic formal groups. Proofs and more detailed discussions of these facts can be found in [F],

[Lu2], [Lu3], and [Laz]. Our purpose here is not merely to be expository. In many of the published works on p-adic formal groups, the theorems refer only to homomorphisms defined over a p-adic integer ring. Our methods will sometimes involve homomorphisms which are defined over the completion of a discretely-valued, infinite extension field of $\mathbb{Q}_p$. In this section, we will point out where the standard results can be extended to cover these "nonalgebraic" cases.

If F and G are two p-adic formal groups, then we define $\mathrm{Hom}(F,G)$ to be the abelian group of all homomorphisms from F to G defined over $\mathfrak{O}$. If there is some $g \in \mathrm{Hom}(F,G)$ with invertible linear coefficient, then F *is isomorphic to* G, written $F \cong G$, and g is called an *isomorphism from* F *to* G. It is easily shown that the compositional inverse g^{-1} of an isomorphism $g : F \to G$ belongs to $\mathrm{Hom}(G,F)$. If $F = G$, then we write $\mathrm{End}(F)$ instead of $\mathrm{Hom}(F,F)$, and we refer to it as the *absolute endomorphism ring of* F. The *automorphism group of* F, denoted by $\mathrm{Aut}(F)$, is the group of units of $\mathrm{End}(F)$.

For p-adic formal groups F and G, the map $c : \mathrm{Hom}(F,G) \to \mathfrak{O}$ sending a homomorphism $g : F \to G$ to its linear coefficient is an injective group homomorphism with closed image [Lu3, §2]. When $F = G$, c is a map of commutative $\mathbb{Z}_p$-algebras, for if $[n]_F$ is the multiplication-by-n endomorphism of F, then $c([n]_F) = n$. Following Lubin, we denote by $[a]_F$ *the* element of $\mathrm{End}(F)$ such that $c([a]_F) = a$, provided such an endomorphism exists. Another consequence of the injectivity of c is that if H is another p-adic formal group and if $0 \neq g \in \mathrm{Hom}(F,G)$ and $0 \neq j \in \mathrm{Hom}(G,H)$, then $0 \neq j \circ g \in \mathrm{Hom}(F,H)$. Furthermore, if $g \in \mathrm{Hom}(F,G)$ is an isomorphism, then $j \mapsto g \circ j \circ g^{-1}$ defines a ring isomorphism from $\mathrm{End}(F)$ onto $\mathrm{End}(G)$, and so $c\big(\mathrm{End}(F)\big) = c\big(\mathrm{End}(G)\big)$.

Lubin [Lu3, p 470] showed that if F is a p-adic formal group of height h, and if K is a p-adic number field containing the coefficients of F and all p-adic number fields of degree h over $\mathbb{Q}_p$, then $\mathrm{End}(F) \subset \mathfrak{o}_K[[T]]$. This is equivalent to stating $c\big(\mathrm{End}(F)\big) \subseteq \mathfrak{o}_K$ because each coefficient of $g \in \mathrm{Hom}(F,G)$ is a polynomial function of $c(g)$ with coefficients in any field containing the coefficients of F and G [F, p 98]. We denote by Σ_F the fraction field of $c\big(\mathrm{End}(F)\big)$. Since $\mathbb{Z}_p \subseteq c\big(\mathrm{End}(F)\big) \subseteq \mathfrak{o}_{\Sigma_F}$, we see that $c\big(\mathrm{End}(F)\big)$ is a $\mathbb{Z}_p$-order in Σ_F; moreover, $[\Sigma_F : \mathbb{Q}_p]$ is a divisor of h [Lu3, 2.3.2].

Definition 1.1. A p-adic formal group F of height h is *full* if $[\Sigma_F : \mathbb{Q}_p] = h$ and $c\big(\mathrm{End}(F)\big) = \mathfrak{o}_{\Sigma_F}$. We say F is *almost full* if $[\Sigma_F : \mathbb{Q}_p] = h$ but $c\big(\mathrm{End}(F)\big) \neq \mathfrak{o}_{\Sigma_F}$.

For any p-adic number field K, Lubin and Tate [LT] give a way of constructing full p-adic formal groups F defined over $\mathfrak{o}_K$ such that $c\big(\mathrm{End}(F)\big) = \mathfrak{o}_K$.

Whereas the endomorphisms of a p-adic formal group are all defined over a single p-adic integer ring, the same cannot be said of the homomorphisms between different p-adic formal groups. (See [Lu3, 4.3.2].) We will say that $g : F \to G$ is an *isogeny* if g is defined over some $\mathfrak{o}_L$ (or, equivalently, if $c(g) \in \mathfrak{o}_L$), where L is a complete, discretely-valued subfield of $\mathbb{C}_p$ containing the coefficients of F and G. We write $\mathrm{Isog}(F,G)$ for the set of all isogenies from F to G, and we say that F *is isogenous to* G if $\mathrm{Isog}(F,G) \neq 0$. We show later that $\mathrm{Isog}(F,G)$ is a subgroup of $\mathrm{Hom}(F,G)$. It is clear that every endomorphism of a p-adic formal group is an isogeny. In [Lu2] and [F], for example, an isogeny is assumed to be defined over the integers in a finite extension of the field over which the p-adic formal groups are defined. We will show that those homomorphisms which satisfy our more general definition of isogeny share many of the properties exhibited by "p-adic isogenies".

A p-adic formal group F can be used to define an abelian group law on $\mathfrak{M}$ by setting $\alpha +_{F} \beta = F(\alpha, \beta)$ for $\alpha, \beta \in \mathfrak{M}$. We denote this group by $F(\mathfrak{O})$, and refer to it as *the points of* F. From the definition of a p-adic formal group, we see that for $\alpha, \beta \in F(\mathfrak{O})$, $v\left(\alpha +_{F} \beta\right) \geq \min\{v(\alpha), v(\beta)\}$, with equality if $v(\alpha) \neq v(\beta)$. For any $g \in \mathrm{Hom}(F, G)$, the association $\alpha \mapsto g(\alpha)$ defines a group homomorphism from $F(\mathfrak{O})$ to $G(\mathfrak{O})$, which we also denote by g. In particular, if the integer m is prime to p, then $[m]_F$ maps $F(\mathfrak{O})$ isomorphically onto itself, and so the order of an element of $F(\mathfrak{O})$ of finite order is necessarily a power of p. Therefore the torsion subgroup $\Lambda(F)$ of the points of F can be expressed as

$$\Lambda(F) = \bigcup_{n \in \mathbb{N}} \ker\,[p^n]_F.$$

Proposition 1.2. *If $g \in \mathrm{Hom}(F, G)$ and $\alpha \in F(\mathfrak{O})$, then $v\big(g(\alpha)\big) \geq v(\alpha)$, with equality if and only if either $\alpha = 0$ or $c(g) \in \mathfrak{O}^{\times}$.*

Proof. Writing $g(T) = T \cdot j(T)$, where $j(T) \in \mathfrak{O}[[T]]$, we see that $v\big(g(\alpha)\big) \geq v(\alpha)$ because $j(\alpha) \in \mathfrak{O}$. Furthermore, if $\alpha \neq 0$, then $v\big(g(\alpha)\big) = v(\alpha)$ if and only if $v\big(j(\alpha)\big) = 0$, which holds if and only if $j(0) = c(g)$ is a unit in $\mathfrak{O}$ because $v(\alpha) > 0$. $\square$

If g is a nonzero isogeny defined over the complete discretely-valued subring $\mathfrak{o}_L$ of $\mathfrak{O}$, then the Weierstrass Preparation Theorem [Lang, V.11.2] implies that there is a monic polynomial $P(T) \equiv T^d \pmod{\mathfrak{m}_L}$ of degree $d = \mathrm{wdeg}\,(g)$, the *Weierstrass degree of* g, and a power series $U(T) \in \mathfrak{o}_L[[T]]$ with $U(0) \notin \mathfrak{m}_L$ such that $g = P \cdot U$. The elements of $\ker(g)$ are the roots of $P(T)$; they belong to $\mathfrak{M}$ and have multiplicity one [Lu2, §1.2]. Thus, the kernel of any nonzero isogeny $g : F \to G$ is a finite subgroup of $F(\mathfrak{O})$ of order $\mathrm{wdeg}\,(g)$. In particular, $\ker\,[p]_F$ has order p^h, where h is the height of F. The elements of $\Lambda(F)$ are all integral over $\mathbb{Z}_p$: indeed, for every $n \in \mathbb{N}$, $[p^n]_F$, is defined over any p-adic integer ring $\mathfrak{o}_K$ containing the coefficients of F, and so the polynomial $P(T) \in \mathfrak{o}_K[T]$ arising from the Weierstrass Preparation Theorem has roots in $\overline{\mathfrak{m}}$.

If $g \in \mathrm{Hom}(F, G)$, then for every $m \in \mathbb{Z}$, $[m]_G \circ g = g \circ [m]_F$, and therefore $g\,(\Lambda(F)) \subseteq \Lambda(G)$. A slight modification of the argument in [Lu2, §1.2] will show that $g : \Lambda(F) \to \Lambda(G)$ is surjective whenever g is a nonzero isogeny. Suppose that g is defined over $\mathfrak{o}_L$, where L is a complete, discretely-valued subfield of $\mathbb{C}_p$. For any $\alpha \in \Lambda(G)$, the power series $g(T) - \alpha$ is defined over the ring of integers in $L(\alpha)$ (which is also a complete discretely-valued subfield of $\mathbb{C}_p$ because α is integral over $\mathbb{Z}_p$), and $\mathrm{wdeg}\big(g(T) - \alpha\big) = \mathrm{wdeg}\,(g) \geq 1$. The Weierstrass Preparation Theorem implies that $g(T) - \alpha$ has $\mathrm{wdeg}\,(g)$ zeros in $F(\mathfrak{O})$ all belonging to $\Lambda(F)$ since $\alpha \in \Lambda(G)$ and g is a homomorphism of p-adic formal groups having a finite kernel.

If C is a finite subgroup of $F(\mathfrak{O})$, Lubin [Lu2, 1.4] proved that the power series

$$\varphi_C(T) = \prod_{\gamma \in C} F(T, \gamma)$$

is a p-adic isogeny from F to the p-adic formal group $\varphi_C\left(F\big({\varphi_C}^{-1}(X), {\varphi_C}^{-1}(Y)\big)\right)$, which we denote by F/C and refer to as *the quotient of F by C*. It is clear that $\ker(\varphi_C) = C$. Lubin showed that any p-adic isogeny $j : F \to H$ vanishing on C

factors uniquely through F/C. Using nearly the same proof, one can show that this fact holds for any such isogeny j. One needs only to observe (as above) that if K is a complete discretely-valued subfield of $\mathbb{C}_p$ and if $C = \{\alpha_1, \ldots, \alpha_n\}$ is a finite subgroup of $\Lambda(F)$, then $K(\alpha_1, \ldots, \alpha_n)$ is also a complete discretely-valued subfield of $\mathbb{C}_p$. We record the precise result here.

Theorem 1.3 ([Lu2, 1.5])**.** *Let F, G, H be p-adic formal groups and let L be a complete discretely-valued subfield of $\mathbb{C}_p$ containing the coefficients of F, G, and H. If $g_1 : F \to G$, $g_1 \neq 0$, and $g_2 : F \to H$ are isogenies defined over $\mathfrak{o}_L$ such that $\ker(g_1) \subseteq \ker(g_2)$, then there is a unique isogeny $j : G \to H$ defined over $\mathfrak{o}_L$ such that $j \circ g_1 = g_2$. If $\ker(g_1) = \ker(g_2)$, then j is an isomorphism.*

We can interpret Theorem 1.3 in terms of divisibility in the ring $c\bigl(\mathrm{End}(F)\bigr)$.

Corollary 1.4. *Let F be a p-adic formal group, and let $\zeta_1, \zeta_2 \in c\bigl(\mathrm{End}(F)\bigr)$. Then ζ_1 divides ζ_2 in $c\bigl(\mathrm{End}(F)\bigr)$ if and only if $\ker\,[\zeta_1]_F \subseteq \ker\,[\zeta_2]_F$. In particular, ζ_1 and ζ_2 are associates in $c\bigl(\mathrm{End}(F)\bigr)$ if and only if $\ker\,[\zeta_1]_F = \ker\,[\zeta_2]_F$.*

Proof. If there is an $\eta \in c\bigl(\mathrm{End}(F)\bigr)$ such that $\eta \cdot \zeta_1 = \zeta_2$, then $[\eta]_F \circ [\zeta_1]_F = [\zeta_2]_F$, and so $\ker\,[\zeta_1]_F$ is contained in $\ker\,[\zeta_2]_F$. Conversely, if $\ker\,[\zeta_1]_F \subseteq \ker\,[\zeta_2]_F$, then we may apply Theorem 1.3 to find $j \in \mathrm{End}(F)$ such that $j \circ [\zeta_1]_F = [\zeta_2]_F$. Therefore, $c(j) \cdot \zeta_1 = \zeta_2$. $\square$

The next result shows that, like endomorphisms of a p-adic formal group, all homomorphisms between isogenous p-adic formal groups are defined over a single complete discretely-valued subring of $\mathbb{C}_p$.

Proposition 1.5. *Let F and G be p-adic formal groups, and assume $g : F \to G$ is a nonzero isogeny defined over the integers $\mathfrak{o}_L$ in a complete discretely-valued subfield L of $\mathbb{C}_p$ containing Σ_F and the coefficients of F and G. Then $\mathrm{Isog}(F, G) = \mathrm{Hom}(F, G) \subset \mathfrak{o}_L[[T]]$.*

Proof. By [Lu2, §1.6], there exists a nonzero isogeny $\widetilde{g} : G \to F$ defined over $\mathfrak{o}_L$. Post-composition with $\widetilde{g}$ defines an injective group homomorphism from $\mathrm{Hom}(F, G)$ to $\mathrm{End}(F)$. So, for any $j \in \mathrm{Hom}(F, G)$, $c(\widetilde{g}) \cdot c(j) \in c\bigl(\mathrm{End}(F)\bigr) \subset L$, whence $c(j) \in \mathfrak{O} \cap L = \mathfrak{o}_L$. $\square$

Corollary 1.6. *For p-adic formal groups F and G, either $\mathrm{Isog}(F, G) = 0$ or $\mathrm{Isog}(F, G) = \mathrm{Hom}(F, G)$. In either case, $\mathrm{Isog}(F, G)$ is a group.*

The next corollary is essentially a generalization of a result in [Lu2, §3.2] which states that an almost full p-adic formal group is isogenous to a full p-adic formal group.

Corollary 1.7. *Let $\{G_i\}$ $(i = 1, ..., n)$ be full or almost full p-adic formal groups such that $\Sigma_{G_1} = \cdots = \Sigma_{G_n} = \Sigma$. Then there is a complete discretely-valued subfield L of $\mathbb{C}_p$ such that $0 \neq \mathrm{Isog}(G_i, G_j) = \mathrm{Hom}(G_i, G_j) \subset \mathfrak{o}_L[[T]]$ for every $1 \leq i, j \leq n$.*

Proof. According to [Lu2, §3.2], for each $i = 1, \ldots n$, there is a full p-adic formal group F_i and nonzero p-adic isogenies $g_i : F_i \to G_i$ and $\widetilde{g_i} : G_i \to F_i$. Let K be a p-adic number field containing Σ and the coefficients of all of these p-adic formal groups and isogenies. For each $1 \leq i, j \leq n$, $\Sigma_{F_i} = \Sigma_{G_i} = \Sigma_{G_j} = \Sigma_{F_j}$ [Lu2, §3.0], and so there is an isomorphism $u_{ij} : F_i \to F_j$ defined over $\mathfrak{o}_L$, where L is the completion of the maximal unramified extension K^{nr} of K [Lu3, 4.3.2]. Because K^{nr} is discretely-valued, so is L. Therefore,

$$0 \neq g_j \circ u_{ij} \circ \widetilde{g_i} \in \mathrm{Hom}(G_i, G_j) \cap \mathfrak{o}_L[[T]] \subseteq \mathrm{Isog}(G_i, G_j).$$

The corollary now follows from Proposition 1.5. □

We conclude with our main tool for investigating almost full p-adic formal groups.

Corollary 1.8. *Let G be an almost full p-adic formal group. Then there is a full p-adic formal group F and a finite subgroup C of $\Lambda(F)$ such that G is isomorphic to F/C over a p-adic integer ring.*

Proof. As in the proof of Corollary 1.7, we can find a full p-adic formal group F with $\Sigma_F = \Sigma_G$ and a nonzero isogeny $g : F \to G$ defined over a p-adic integer ring. If $C = \ker(g)$, then $\ker(g) = \ker(\varphi_C)$, and so G and F/C are isomorphic over a p-adic integer ring by Theorem 1.3. □

The main focus of the rest of this article will be to see how the structure of the subgroup C influences that of the ring $\mathrm{End}(F/C)$.

2. Points of finite order of a full formal group

In this section, we investigate certain structures within and on the torsion subgroup a full p-adic formal group F. We are primarily interested in the F-endomorphism kernels and the cyclic subgroups contained in $\Lambda(F)$, two kinds of subgroups mentioned in Conjecture 1. Furthermore, a study of the $c\big(\mathrm{End}(F)\big)$-module structure on $\Lambda(F)$ will provide the key to our proof of Conjecture 1. We first review some facts concerning the Tate module of F.

For any p-adic formal group F of height h, the *Tate module* of F is defined to be

$$T(F) = \varprojlim \ker\, [p^n]_F$$

where the inverse limit is taken with respect to the surjective homomorphisms $[p]_F : \ker\,[p^{n+1}]_F \to \ker\,[p^n]_F$. If G is another p-adic formal group, then any homomorphism $g : F \to G$ defines a group homomorphism $T(g) : T(F) \to T(G)$ by $T(g)\big((a_0, a_1, \dots)\big) = \big(g(a_0), g(a_1), \dots\big)$. If $0 \neq g \in \mathrm{Isog}(F, G)$, then $\ker(g)$ is finite, and hence $T(g)$ is injective. In particular, $T(F)$ is a torsion-free $c\big(\mathrm{End}(F)\big)$-module and a free $\mathbb{Z}_p$-module of rank h [F, IV §4]. If $c\big(\mathrm{End}(F)\big)$ is integrally closed (and thus a PID) of rank d over $\mathbb{Z}_p$, then $T(F)$ is a free $c\big(\mathrm{End}(F)\big)$-module of rank $\frac{h}{d}$. Therefore, when F is full, $T(F)$ is free of rank 1 over $c\big(\mathrm{End}(F)\big)$. In Proposition 5.1, we derive a condition for determining when the Tate module of an almost full p-adic formal group G is free of rank 1 over $c\big(\mathrm{End}(G)\big)$.

We denote by $V(F)$ the set of sequences $(a_0, a_1, \dots)$ such that for all $n \geq 0$, $a_n \in \Lambda(F)$ and $[p]_F(a_{n+1}) = a_n$. It is not difficult to see that $V(F) \cong T(F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, whence $V(F)$ is an h-dimensional $\mathbb{Q}_p$-vector space, called the *Tate vector space of* F. If $g \in \mathrm{Hom}(F, G)$, the $\mathbb{Z}_p$-module homomorphism $T(g) : T(F) \to T(G)$ extends to a linear map $V(g) : V(F) \to V(G)$ of $\mathbb{Q}_p$-vector spaces which is injective if g is a nonzero isogeny. In fact, the existence of such a g implies that F and G have equal heights [Lu3, 2.2.3 and 2.3.1], and therefore $V(g)$ is an isomorphism. Since $\Sigma_F = c\big(\mathrm{End}(F)\big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, the $c\big(\mathrm{End}(F)\big)$-module structure on $T(F)$ induces a Σ_F-vector space structure on $V(F)$. If $[\Sigma_F : \mathbb{Q}_p] = d$, then $V(F)$ is an $\frac{h}{d}$-dimensional

Σ_F-vector space; in particular, when F is full or almost full, $V(F)$ is 1-dimensional over Σ_F. Finally, if $0 \neq g \in \mathrm{Isog}(F, G)$, then $\Sigma_F = \Sigma_G$ and $V(g) : V(F) \to V(G)$ is a Σ_F-isomorphism.

Proposition 2.1. *If $g, j \in \mathrm{Isog}(F, G)$, then $V(g) = V(j)$ if and only if $g = j$.*

Proof. Indeed, if $V(g) = V(j)$, then $g(\alpha) = j(\alpha)$ for all $\alpha \in \Lambda(F)$, which implies that $g - j$ is identically 0 on $\Lambda(F)$. Since $\mathrm{Isog}(F, G)$ is a group, $g - j \in \mathrm{Isog}(F, G)$, and so its kernel is finite unless $g - j = 0$. □

Throughout the remainder of this section, we denote by F a p-adic formal group of height h with $\mathrm{End}(F)$ integrally closed, and we let π be a fixed uniformizer of $c\big(\mathrm{End}(F)\big)$. Moreover, we denote by e (resp., f) the ramification index (resp., the residue field degree) of the extension $\Sigma_F / \mathbb{Q}_p$.

The group $\Lambda(F)$ is the union of the kernels of the endomorphisms $[p^n]_F$ $(n \geq 0)$. If g is any nonzero endomorphism of F, then $\ker(g)$ is also a finite subgroup of $\Lambda(F)$, not necessarily equal to the kernel of one of the multiplication-by-p^n endomorphisms. However, $c(g)$ is an associate of π^m in the ring $c\big(\mathrm{End}(F)\big)$, where $m = e \cdot v\big(c(g)\big)$, and so by Corollary 1.4, $\ker(g) = \ker\,[\pi^m]_F$. Therefore, $\big\{\ker\,[\pi^m]_F\big\}_{m\geq 0}$ is the set of kernels of the nonzero F-endomorphisms, and

$$\Lambda(F) = \bigcup_{n\geq 0} \ker\,[p^n]_F = \bigcup_{m\geq 0} \ker\,[\pi^m]_F.$$

Moreover, because $\ker\,[\pi^{m-1}]_F \subset \ker\,[\pi^m]_F$, the family $\big\{\ker\,[\pi^m]_F\big\}_{m\geq 0}$ is a filtration of subgroups of $\Lambda(F)$, with $\ker\,[\pi]_F$ being the smallest kernel of any noninvertible F-endomorphism.

Proposition 2.2. *The kernel of $[\pi^m]_F$ has $p^{m(h/e)}$ elements. In particular, if F is full, then $\big|\ker\,[\pi^m]_F\big| = p^{mf}$.*

Proof. If $\big|\ker\,[\pi]_F\big| = p^s$, then the surjectivity of $[\pi]_F : \Lambda(F) \to \Lambda(F)$ implies inductively that $\big|\ker\,[\pi^m]_F\big| = p^{sm}$. Therefore $p^h = \big|\ker\,[p]_F\big| = \big|\ker\,[\pi^e]_F\big| = p^{se}$, and so $s = h/e$. Finally, when F is full, we note that $h = [\Sigma_F : \mathbb{Q}_p] = ef$. □

We can interpret the endomorphism kernels in terms of annihilators.

Definition 2.3. The *annihilator* $\mathcal{I}(X)$ of a subset X of $\Lambda(F)$ is the set

$$\big\{\zeta \in c\big(\mathrm{End}(F)\big) \,\big|\, \forall \alpha \in X, [\zeta]_F(\alpha) = 0\big\}.$$

If $\gamma \in \Lambda(F)$, we will write $\mathcal{I}(\gamma)$ instead of $\mathcal{I}(\{\gamma\})$.

Remarks 2.4.

(i) Because $\mathfrak{o} = c\big(\mathrm{End}(F)\big)$ is a commutative ring, $\mathcal{I}(X)$ is an ideal of $\mathfrak{o}$. Therefore $\mathcal{I}(X) = \pi^m\mathfrak{o}$ for some integer $m \geq 0$. In fact, for each $m \in \mathbb{N}$,

$$\big\{\alpha \in \Lambda(F) \,\big|\, \mathcal{I}(\alpha) = \pi^m\mathfrak{o}\big\} = \ker\,[\pi^m]_F - \ker\,[\pi^{m-1}]_F\,.$$

(ii) If C is the cyclic subgroup generated by $\gamma \in \Lambda(F)$, then $\mathcal{I}(C) = \mathcal{I}(\gamma)$. More generally, it follows from Lemma 2.5 below that if C is any finite subgroup of $\Lambda(F)$, where F is a full p-adic formal group, then $\mathcal{I}(C) = \mathcal{I}(\gamma)$, where $\gamma \in C$ is an element of minimal valuation.

We have seen (Corollary 1.8) that any almost full p-adic formal group is isomorphic over a p-adic integer ring to the quotient of a full p-adic formal group F by a finite subgroup C of $\Lambda(F)$. The quotient is much easier to study when the subgroup C can be chosen to be cyclic; this is always possible in height 2 (see §6). In Corollary 6.4, we will use this fact to prove that the isomorphism class of a height 2 almost full p-adic formal group depends only on its absolute endomorphism ring. A key step in our proof is the result given below in Corollary 2.8, which describes when two cyclic subgroups of $\Lambda(F)$ are isomorphic to each other via an automorphism of F. We begin, however, with the following lemma, the proof of which uses the fact that $T(F)$ is free of rank 1 over $c\big(\mathrm{End}(F)\big)$.

Lemma 2.5. *Let F be a full p-adic formal group. For any pair $\gamma, \delta \in \Lambda(F)$, $v(\gamma) \le v(\delta)$ if and only if there exists some $\zeta \in c\big(\mathrm{End}(F)\big)$ such that $[\zeta]_F(\gamma) = \delta$.*

Proof. Without loss of generality, we may assume that both γ and δ are nonzero. The implication ($\Leftarrow$) follows from Proposition 1.2. Conversely, suppose $v(\gamma) \le v(\delta)$, and choose n large enough so that $\gamma, \delta \in \ker [p^n]_F$. Then there exist $c, d \in T(F)$ such that $c_n = \gamma$ and $d_n = \delta$. If $b = (b_0, b_1, \dots)$ is any basis of $T(F)$ over $c\big(\mathrm{End}(F)\big)$, then there are (unique) elements $\eta, \theta \in c\big(\mathrm{End}(F)\big)$ such that $\eta \cdot b = c$ and $\theta \cdot b = d$. Assume $v(\eta) \le v(\theta)$. Then $\zeta = \theta\, \eta^{-1} \in \mathfrak{o}_{\Sigma_F} = c\big(\mathrm{End}(F)\big)$ and $\delta = [\theta]_F(b_n) = [\theta\, \eta^{-1}]_F\big([\eta]_F(b_n)\big) = [\zeta]_F(\gamma)$, which proves the lemma in this case. If, on the other hand, $v(\eta) > v(\theta)$, then a similar calculation would show that $[\eta\, \theta^{-1}]_F(\delta) = \gamma$, which contradicts Proposition 1.2 since $\eta\, \theta^{-1}$ is not a unit in $c\big(\mathrm{End}(F)\big)$. □

If C is any subgroup of $F(\mathfrak{O})$ and if $\lambda \in \mathbb{R}$, then $C_\lambda = \{\gamma \in C \mid v(\gamma) \ge \lambda\}$ is a subgroup of C. Using Lemma 2.5 and Proposition 1.2, we can obtain a description of the cyclic $\mathrm{End}(F)$-submodules of $\Lambda(F)$ when F is full. For any $\alpha \in \Lambda(F)$,

$$\mathrm{End}(F) \cdot \alpha = \big\{\beta \in \Lambda(F) \;\big|\; v(\beta) \ge v(\alpha)\big\} = \Lambda(F)_{v(\alpha)}\,.$$

The subsets $\Lambda(F)_{v(\alpha)}$ are examples of *congruence-torsion subgroups of* F (see [Lu1]). These turn out to be the so-called "canonical subgroups" mentioned in Conjecture 2.

Theorem 2.6. *Let F be a full p-adic formal group. The following are equivalent for elements $\gamma, \delta \in \Lambda(F)$:*

(i) $v(\gamma) = v(\delta)$.
(ii) *There exists some $u \in \mathrm{Aut}(F)$ such that $u(\gamma) = \delta$.*
(iii) $\mathcal{I}(\gamma) = \mathcal{I}(\delta)$.

Proof. (i) $\Rightarrow$ (ii): This follows immediately from Lemma 2.5 and Proposition 1.2.

(ii) $\Rightarrow$ (iii): If $\epsilon = c(u) \in c\big(\mathrm{End}(F)\big)^\times$, then $\zeta \mapsto \zeta \cdot \epsilon$ is a bijection from $\mathcal{I}(\delta)$ onto $\mathcal{I}(\gamma)$. Because these two sets are ideals of $c\big(\mathrm{End}(F)\big)$, they are equal.

(iii) $\Rightarrow$ (i): Without loss of generality, we may assume that $v(\gamma) < v(\delta)$. Choose $\zeta \in c\big(\mathrm{End}(F)\big)$ such that $[\zeta]_F(\gamma) = \delta$ and suppose π^m ($m \ge 1$) generates $\mathcal{I}(\gamma)$. Since ζ is not a unit in $c\big(\mathrm{End}(F)\big)$ (Proposition 1.2), $\zeta = \pi\, \eta$ for some $\eta \in c\big(\mathrm{End}(F)\big)$. Then $\pi^{m-1} \in \mathcal{I}(\delta)$ because $[\pi^{m-1}]_F(\delta) = [\pi^m]_F\big([\eta]_F(\gamma)\big) = [\eta]_F\big([\pi^m]_F(\gamma)\big) = 0$. Therefore, $\mathcal{I}(\gamma) \ne \mathcal{I}(\delta)$. □

Corollary 2.7. *Let F be a full p-adic formal group. For any $m \in \mathbb{N}$, $\mathrm{Aut}(F)$ acts transitively on the set $\ker [\pi^m]_F - \ker [\pi^{m-1}]_F$.*

Proof. Using Remark 2.4(i) and Theorem 2.6 (iii) $\Rightarrow$ (i), we see that all the elements of $\ker[\pi^m]_F - \ker[\pi^{m-1}]_F$ have the same valuation, which, in light of Lemma 2.5, is less than the valuation of any of the elements of $\ker[\pi^{m-1}]_F$. The corollary now follows from Theorem 2.6 (i) $\Rightarrow$ (ii). $\square$

Corollary 2.8. *Let F be a full p-adic formal group and let C_1 and C_2 be finite cyclic subgroups of $\Lambda(F)$. Then there exists some $u \in \mathrm{Aut}(F)$ such that $C_1 = u(C_2)$ if and only if $\mathcal{I}(C_1) = \mathcal{I}(C_2)$.*

Proof. This follows from Remark 2.4(ii) and Theorem 2.6. $\square$

3. Deflated subgroups

When expressing a full or almost full p-adic formal group G as being isomorphic to the quotient of a full p-adic formal group F by a finite subgroup C of $\Lambda(F)$, F is uniquely determined up to isomorphism. Indeed, if $F/C \cong F'/C'$, where F and F' are full, then $\Sigma_F = \Sigma_{F/C} = \Sigma_{F'/C'} = \Sigma_{F'}$ (see the proof of Corollary 1.7), whence $F \cong F'$ via an isogeny [Lu3, 4.3.2]. However, the subgroup C is by no means unique (not even up to isomorphism).

Proposition 3.1. *Let F be any p-adic formal group. If C is a finite subgroup of $\Lambda(F)$ and $0 \neq g \in \mathrm{End}(F)$, then $F/g^{-1}(C) \cong F/C$ over a p-adic integer ring.*

Proof. Since $g^{-1}(C)$ is the kernel of the p-adic isogenies $\varphi_{g^{-1}(C)} : F \to F/g^{-1}(C)$ and $\varphi_C \circ g : F \to F/C$, we can use Theorem 1.3. $\square$

Taking $g = [p^n]_F$ for various $n \in \mathbb{N}$, we see that there are infinitely many nonisomorphic finite subgroups of $\Lambda(F)$ which yield isomorphic quotients. This prompts the following.

Definition 3.2. Let F be a p-adic formal group. For finite subgroups C_1, C_2 of $\Lambda(F)$, we write $C_1 \sim C_2$ if $F/C_1 \cong F/C_2$.

It is clear that $\sim$ is an equivalence relation on the set of finite subgroups of $\Lambda(F)$. If C and D are two subgroups of $\Lambda(F)$ such that $C \sim D$, then we will say that C and D are *equivalent*. We now show that when F is a full p-adic formal group, then the converse of Proposition 3.1 is true.

Proposition 3.3. *Let F be a full p-adic formal group and let C, D be equivalent finite subgroups of $\Lambda(F)$. If $|C| \geq |D|$, then there exists $0 \neq g \in \mathrm{End}(F)$ such that $C = g^{-1}(D)$.*

Proof. By assumption, there is an isomorphism $u : F/C \to F/D$, and according to Proposition 1.5, the homomorphism $u \circ \varphi_C$ is a nonzero isogeny (since φ_D is). Thus, the maps $V(u \circ \varphi_C), V(\varphi_D) : V(F) \to V(F/D)$ are isomorphisms of Σ_F-vector spaces (see §2). Also, since F is full, F/D must be full or almost full [Lu2, 3.0], and so $V(F)$ and $V(F/D)$ are one-dimensional over Σ_F. Consequently, $V(u \circ \varphi_C)$ $\big($resp., $V(\varphi_D)\big)$ is scalar multiplication by some nonzero element α (resp., β) of Σ_F. Assume now that $\beta^{-1}\alpha \in c\big(\mathrm{End}(F)\big)$, and let $g = [\beta^{-1}\alpha]_F$. Then $V(g)$ operates on $V(F)$ via scalar multiplication by $\beta^{-1}\alpha$, and so $V(u \circ \varphi_C) = V(\varphi_D) \circ V(g) = V(\varphi_D \circ g)$. Therefore, $u \circ \varphi_C = \varphi_D \circ g$ by Proposition 2.1. Comparing kernels, we see that $C = g^{-1}(D)$.

We now show that $\beta^{-1}\alpha$ must be in $c\bigl(\mathrm{End}(F)\bigr)$. If $\beta^{-1}\alpha \notin c\bigl(\mathrm{End}(F)\bigr)$, then because $c\bigl(\mathrm{End}(F)\bigr)$ is a valuation ring, it follows that $\alpha^{-1}\beta \in c\bigl(\mathrm{End}(F)\bigr)$, but it is not a unit. The same reasoning as above shows that $\varphi_D = (u \circ \varphi_C) \circ \widetilde{g}$, where $\widetilde{g} = [\alpha^{-1}\beta]_F$. This implies that $\widetilde{g}^{-1}(C) = D$, and since $\ker\bigl(\widetilde{g}\bigr) \neq \{0\}$, we arrive at $|D| > |C|$, a contradiction. □

If F is a full p-adic formal group and C a finite subgroup of $\Lambda(F)$, then many properties of $\Lambda(F/C)$ and $\mathrm{End}(F/C)$ depend on the element(s) of minimal size in the equivalence class of C. We now name these subgroups.

Definition 3.4. Let F be a p-adic formal group. A finite subgroup D of $\Lambda(F)$ is a *deflated subgroup of* F if $D \sim C$ implies $|D| \leq |C|$.

There may be multiple deflated subgroups of F belonging to the same equivalence class. Indeed, if $u \in \mathrm{Aut}(F)$ and if D is a deflated subgroup of F, then $u^{-1}(D) \sim D$ and $u^{-1}(D)$ is deflated since $|u^{-1}(D)| = |D|$. On the other hand, if $\ker(g) \subseteq D$ for some $0 \neq g \in \mathrm{End}(F) - \mathrm{Aut}(F)$, then D is not deflated. To see this, we notice that $g(D) \sim D$ because $g^{-1}\bigl(g(D)\bigr) = D$, and $|g(D)| < |D|$ because $\ker(g) \neq \{0\}$. In the next theorem, we show that when F is full, this property characterizes the nondeflated subgroups of F.

Theorem 3.5. *Let F be a full p-adic formal group. A finite subgroup C of $\Lambda(F)$ is a deflated subgroup of F if and only if* $\ker{[\pi]_F} \nsubseteq C$.

Proof. We have already shown why C is not a deflated subgroup of F if it contains $\ker{[\pi]_F}$. Conversely, if C is not a deflated subgroup of F, then there is a finite subgroup D of $\Lambda(F)$ such that $D \sim C$ and $|D| < |C|$. By Proposition 3.3, there is some $0 \neq g \in \mathrm{End}(F)$ such that $C = g^{-1}(D)$; in particular, $\ker(g) \subseteq C$. Also, $\ker(g) \neq \{0\}$ because $|C| \neq |D|$. The result now follows since the kernels of the endomorphisms of F are totally ordered with respect to inclusion, with $\ker{[\pi]_F}$ the smallest nonzero subgroup among them. □

If F is a p-adic formal group of height 1, then $c\bigl(\mathrm{End}(F)\bigr) = \mathbb{Z}_p$, and F is necessarily full. We can take p to be a uniformizer of $c\bigl(\mathrm{End}(F)\bigr)$, and $\ker{[p]_F}$ has order p. It follows that *every* nonzero finite subgroup C of $\Lambda(F)$ is cyclic and contains $\ker{[p]_F}$; therefore, by Theorem 3.5, C is not a deflated subgroup of F. However, for full p-adic formal groups F of height $h > 1$, nondeflated cyclic subgroups are more the exception than the rule. According to Theorem 3.5, F has nondeflated cyclic subgroups if and only if $\ker{[\pi]_F}$ is cyclic, where π is a uniformizer of $c\bigl(\mathrm{End}(F)\bigr)$. Using Proposition 2.2, plus the fact that $\ker{[\pi]_F} \subseteq \ker{[p]_F}$, we see that $\ker{[\pi]_F}$ is cyclic if and only if $\Sigma_F/\mathbb{Q}_p$ is totally ramified.

We can now restate Conjecture 1 more concisely using the terminology and notation we have developed so far:

Conjecture 1. *Let F be a full p-adic formal group of height 2, and let C be a deflated cyclic subgroup of F of order p^n. Then $c\bigl(\mathrm{End}(F/C)\bigr) = \mathbb{Z}_p + p^n\mathfrak{o}$, where $\mathfrak{o} = c\bigl(\mathrm{End}(F)\bigr)$.*

4. Generalizations of Conjecture 1

We now prove a couple of theorems which generalize Conjecture 1 to p-adic formal groups of arbitrary height. First we look at the situation where the finite subgroup C is cyclic, but not necessarily deflated, and then where C is deflated, but not necessarily cyclic. Our main tool is Lemma 4.1, which is a special case of [Lu2, 3.1].

Lemma 4.1. *Let F be a p-adic formal group such that* $\mathrm{End}(F)$ *is integrally closed. If C is a finite subgroup of $\Lambda(F)$, then*

$$c\big(\mathrm{End}(F/C)\big) = \big\{\zeta \in c\big(\mathrm{End}(F)\big) \;\big|\; [\zeta]_F(C) \subseteq C\big\}.$$

Proof. Let L be the lattice in $V(F)$ consisting of all elements $(a_0, a_1, \dots)$ with $a_0 \in C$. Then L is the lattice corresponding to $\varphi_C : F \to F/C$ as described in [Lu2, §2.2]. Therefore, according to [Lu2, 3.1],

$$c\big(\mathrm{End}(F/C)\big) = \big\{\zeta \in \Sigma_F \,\big|\, \zeta L \subseteq L\big\}.$$

Because $c\big(\mathrm{End}(F/C)\big)$ is a $\mathbb{Z}_p$-order in Σ_F, $c\big(\mathrm{End}(F/C)\big) \subseteq \mathfrak{o}_{\Sigma_F} = c\big(\mathrm{End}(F)\big)$. Thus

$$c\big(\mathrm{End}(F/C)\big) = \big\{\zeta \in c\big(\mathrm{End}(F)\big) \,\big|\, \zeta L \subseteq L\big\}.$$

But for $\zeta \in c\big(\mathrm{End}(F)\big)$ and $a = (a_0, a_1, \dots) \in V(F)$, $\zeta \cdot a = \big([\zeta]_F(a_0), [\zeta]_F(a_1), \dots\big)$. Hence $\zeta L \subseteq L$ if and only if $[\zeta]_F(C) \subseteq C$. □

Remark 4.2. If G is a p-adic formal group where $c\big(\mathrm{End}(G)\big)$ is not integrally closed, then there is some $n \in \mathbb{N}$ such that $p^n\, \mathfrak{o}_{\Sigma_G} \subseteq c\big(\mathrm{End}(G)\big)$. In this case, recall that for $\zeta \in \mathfrak{o}_{\Sigma_G}$ and $a = (a_0, a_1, \dots) \in V(G)$,

$$\zeta \cdot a = \big([p^n\zeta]_G(a_n), [p^n\zeta]_G(a_{n+1}), \dots\big).$$

A modification of the proof of Lemma 4.1 yields

$$c\big(\mathrm{End}(G/C)\big) = \Big\{\zeta \in \mathfrak{o}_{\Sigma_G} \,\Big|\, [p^n\zeta]_G\big([p^n]_G^{-1}(C)\big) \subseteq C\Big\}.$$

When F is a full p-adic formal group and C is a cyclic subgroup of $\Lambda(F)$, then the ring $c\big(\mathrm{End}(F/C)\big)$ has a rather simple description in terms of the annihilator of C in $\mathfrak{o} = c\big(\mathrm{End}(F)\big)$. We note that Theorem 4.3 is a generalization of Conjecture 1 since, as we will show, $\mathcal{I}(C) = p^n\mathfrak{o}$ for the subgroups C considered there.

Theorem 4.3. *Let F be a p-adic formal group such that* $\mathrm{End}(F)$ *is integrally closed. If C is a finite cyclic subgroup of $\Lambda(F)$, then $c\big(\mathrm{End}(F/C)\big) = \mathbb{Z}_p + \mathcal{I}(C)$.*

Proof. Let γ be a generator of C. By Remark 2.4(ii), $\mathcal{I}(C) = \mathcal{I}(\gamma)$. If $\zeta \in \mathcal{I}(C)$, then $[\zeta]_F(C) = \{0\} \subseteq C$, and so by Lemma 4.1, $\zeta \in c\big(\mathrm{End}(F/C)\big)$. It is now clear that $\mathbb{Z}_p + \mathcal{I}(C) \subseteq c\big(\mathrm{End}(F/C)\big)$. Conversely, take any $\zeta \in c\big(\mathrm{End}(F/C)\big)$. Then by Lemma 4.1, $[\zeta]_F(\gamma) \in C$, and so there is an $m \in \mathbb{Z}$ such that $[\zeta]_F(\gamma) = [m]_F(\gamma)$. Hence, $\zeta - m \in \mathcal{I}(\gamma) = \mathcal{I}(C)$, i.e., $\zeta \in \mathbb{Z}_p + \mathcal{I}(C)$. □

When C is a deflated (but not necessarily cyclic) subgroup of a full p-adic formal group F, we can determine the conductor of $c\big(\mathrm{End}(F)\big)$ with respect to $c\big(\mathrm{End}(F/C)\big)$. Recall that if $A \subseteq B$ are commutative unitary rings, then the *conductor of B with respect to A* is the ideal $\mathfrak{c} = \{b \in B \mid bB \subseteq A\}$.

Theorem 4.4. *Let F be a full p-adic formal group, and let C be a deflated subgroup of F. The conductor $\mathfrak{c}$ of $c\big(\mathrm{End}(F)\big)$ with respect to $c\big(\mathrm{End}(F/C)\big)$ is $\mathcal{I}(C)$.*

Proof. Let π be a uniformizer of $\mathfrak{o} = c\big(\mathrm{End}(F)\big)$. As the result is trivial if $C = \{0\}$, we may assume that $\mathcal{I}(C) = \pi^m \mathfrak{o}$ for some $m \geq 1$. Then $\mathfrak{c} = \pi^k \mathfrak{o}$, where k is the smallest nonnegative integer for which $\pi^k \mathfrak{o} \subseteq c\big(\mathrm{End}(F/C)\big)$. Now, if $\zeta \in \mathfrak{o}$, then $[\pi^m \zeta]_F(C) = [\zeta]_F\big([\pi^m]_F(C)\big) = \{0\} \subseteq C$. By Lemma 4.1, $\pi^m \zeta \in c\big(\mathrm{End}(F/C)\big)$, and so $k \leq m$. Suppose that $\pi^{m-1}\mathfrak{o} \subseteq c\big(\mathrm{End}(F/C)\big)$. Then for every $\epsilon \in \mathfrak{o}^\times$, $[\epsilon]_F\big([\pi^{m-1}]_F(C)\big) \subseteq C$. Since $\{0\} \neq [\pi^{m-1}]_F(C) \subseteq \ker [\pi]_F$, Corollary 2.7 implies that

$$\bigcup_{u \in \mathrm{Aut}(F)} u\big([\pi^{m-1}]_F(C)\big) = \ker [\pi]_F,$$

whence $\ker [\pi]_F \subseteq C$. According to Theorem 3.5, this contradicts the assumption that C is a deflated subgroup of F, and so $k = m$. Therefore, $\mathfrak{c} = \mathcal{I}(C)$. $\square$

5. Free Tate modules of rank 1

Lubin [Lu2, §3.2] showed that if R is a $\mathbb{Z}_p$-order in a finite extension K of $\mathbb{Q}_p$ with $R \neq \mathfrak{o}_K$, then there exists an almost full p-adic formal group G with $c\big(\mathrm{End}(G)\big) = R$. However, unlike the situation for full p-adic formal groups, there do exist nonisomorphic almost full p-adic formal groups which have isomorphic absolute endomorphism rings. (We show in §6, however, that such formal groups cannot have height 2.) Waterhouse [W] proves that two almost full p-adic formal groups G_1 and G_2 are isomorphic if and only if $c\big(\mathrm{End}(G_1)\big) = c\big(\mathrm{End}(G_2)\big) = R$ and $T(G_1) \cong T(G_2)$ as R-modules. A key lemma in his proof asserts that there is an almost full p-adic formal group H with $c\big(\mathrm{End}(H)\big) = R$ such that $T(H)$ is free of rank 1 over R. In our next proposition, we use our results to derive a necessary and sufficient condition on a finite subgroup C of the points of a full p-adic formal group F which guarantees that $T(F/C)$ is free of rank 1 over $c\big(\mathrm{End}(F/C)\big)$. In the proof, we use the fact that if G is a p-adic formal group, then an element $(a_0, a_1, a_2, \dots)$ of $V(G)$ belongs to $T(G)$ if and only if $a_0 = 0$.

Proposition 5.1. *Let F be a full p-adic formal group and let C be a finite nonzero subgroup of $\Lambda(F)$. Then $T(F/C)$ is free of rank one over $c\big(\mathrm{End}(F/C)\big)$ if and only if there exists a $\gamma \in C$ satisfying the following two properties:*

(P1) *γ has minimal valuation among the elements of C.*
(P2) *If $g \in \mathrm{End}(F)$ and $g(\gamma) \in C$, then $g(C) \subseteq C$.*

Proof. Assume that $\gamma \in C$ satisfies (P1) and (P2); note that $\gamma \neq 0$ because $C \neq \{0\}$. Choose any $b \in V(F)$ such that $b_0 = \gamma$, and define $b' = V(\varphi_C)(b)$. We will show that $T(F/C) = c\big(\mathrm{End}(F/C)\big) \cdot b'$. If $\zeta \in c\big(\mathrm{End}(F/C)\big)$, then $[\zeta]_F(C) \subseteq C$ by Lemma 4.1, and hence

$$\begin{aligned} \zeta \cdot b' &= \zeta \cdot V(\varphi_C)(b) \\ &= \big([\zeta]_{F/C}(\varphi_C(b_0)), [\zeta]_{F/C}(\varphi_C(b_1)), \dots\big) \\ &= \big(\varphi_C([\zeta]_F(\gamma)), \varphi_C([\zeta]_F(b_1)), \dots\big) \\ &= (0, \dots) \in T(F/C). \end{aligned}$$

Therefore, $c\big(\mathrm{End}(F/C)\big) \cdot b' \subseteq T(F/C)$. Conversely, take any $a \in T(F/C)$, and let ζ be the unique element of Σ_F such that $a = \zeta \cdot b'$. Choose an integer n large enough so that $p^n\zeta \in c\big(\mathrm{End}(F)\big)$. Then

$$\begin{aligned} a &= V(\varphi_C)(\zeta \cdot b) \\ &= V(\varphi_C)(p^{-n} \cdot p^n\zeta \cdot b) \\ &= \big(\varphi_C([p^n\zeta]_F(b_n)), \varphi_C([p^n\zeta]_F(b_{n+1})), \dots\big), \end{aligned}$$

which implies that $[p^n\zeta]_F(b_n) \in C$ since $a_0 = 0$. By (P1), $v(\gamma) \leq v\big([p^n\zeta]_F(b_n)\big)$, and so by Lemma 2.5 there is an $\eta \in c\big(\mathrm{End}(F)\big)$ such that $[\eta]_F(\gamma) = [p^n\zeta]_F(b_n)$. Therefore, because $\gamma = [p^n]_F(b_n)$, we know that $p^n(\zeta - \eta) \in \mathcal{I}(b_n)$. However, $p^n \notin \mathcal{I}(b_n)$ (since $\gamma \neq 0$) and so $v\big(p^n(\zeta - \eta)\big) > v(p^n)$. This in turn implies that $v(\zeta - \eta) > 0$, which proves that $\zeta \in c\big(\mathrm{End}(F)\big)$. We see now that

$$\begin{aligned} a = \zeta \cdot V(\varphi_C)(b) &\implies \varphi_C\big([\zeta]_F(\gamma)\big) = 0 \\ &\implies [\zeta]_F(\gamma) \in C \\ &\implies [\zeta]_F(C) \subseteq C \quad \big(\text{from (P2)}\big) \end{aligned}$$

which shows that $\zeta \in c\big(\mathrm{End}(F/C)\big)$ according to Lemma 4.1.

Now, suppose that $T(F/C)$ is free of rank 1 over $c\big(\mathrm{End}(F/C)\big)$ and choose any $b \in V(F)$ such that $\big\{V(\varphi_C)(b)\big\}$ is a $c\big(\mathrm{End}(F/C)\big)$-basis for $T(F/C)$. Because $V(\varphi_C)(b) \in T(F/C)$, it follows that $\varphi_C(b_0) = 0$, i.e., $b_0 \in C$. We will show that $\gamma = b_0$ satisfies (P1) and (P2). Take any $\delta \in C$ and $d \in V(F)$ with $d_0 = \delta$. As $V(\varphi_C)(d) \in T(F/C)$, there is a unique $\zeta \in c\big(\mathrm{End}(F/C)\big) \subseteq c\big(\mathrm{End}(F)\big)$ such that $V(\varphi_C)(d) = \zeta \cdot V(\varphi_C)(b) = V(\varphi_C)(\zeta \cdot b)$. Because $V(\varphi_C)$ is an isomorphism, $\zeta \cdot b = d$, and so $[\zeta]_F(\gamma) = \delta$. Proposition 1.2 shows that $v(\delta) \geq v(\gamma)$, which establishes (P1). Finally, if $g \in \mathrm{End}(F)$ and $g(\gamma) \in C$, then

$$c(g) \cdot V(\varphi_C)(b) = V(\varphi_C \circ g)(b) = \big(\varphi_C(g(\gamma)), \dots\big) = (0, \dots) \in T(F/C).$$

This implies that $c(g) \in c\big(\mathrm{End}(F/C)\big)$, i.e., $g(C) \subseteq C$, and so (P2) holds as well. $\square$

Corollary 5.2. *If F is a full p-adic formal group and if C is a finite cyclic subgroup of $\Lambda(F)$, then $T(F/C)$ is free of rank 1 over $c\big(\mathrm{End}(F/C)\big)$.*

Proof. The result is clear if $C = \{0\}$. Otherwise, if $C = \langle\gamma\rangle \neq \{0\}$, then the pair (C, γ) satisfies (P1) (use Proposition 1.2) and (P2) of Proposition 5.1. $\square$

The converse of Corollary 5.2 is not true in general, even if we require the subgroup to be deflated. Let F be a full p-adic formal group and let π be a uniformizer of $\mathfrak{o} = c\big(\mathrm{End}(F)\big)$. Fix any $0 \neq \gamma \in \Lambda(F)$ and let C be a finite subgroup of $\Lambda(F)$ containing γ as an element of minimal valuation. By Remark 2.4(ii), $\mathcal{I}(C) = \mathcal{I}(\gamma) = \pi^k\mathfrak{o}$ for some $k \in \mathbb{N}$. The set

$$\mathcal{S}_C = \big\{\zeta \in \mathfrak{o} \,\big|\, [\zeta]_F(C) \subseteq C\big\} = c\big(\mathrm{End}(F/C)\big)$$

is a subring of $\mathfrak{o}$ containing $\mathcal{I}(\gamma)$, and the set

$$\mathcal{T}_{C,\gamma} = \big\{\zeta \in \mathfrak{o} \,\big|\, [\zeta]_F(\gamma) \in C\big\}$$

is a subgroup of $\mathfrak{o}$ containing $\mathcal{S}_C$. Moreover, the evaluation map $\zeta \mapsto [\zeta]_F(\gamma)$ induces a group isomorphism $\mathcal{T}_{C,\gamma}/\mathcal{I}(\gamma) \to C$ (see Lemma 2.5). Therefore the pair (C, γ) satisfies (P1) and (P2) if and only if $\mathcal{S}_C = \mathcal{T}_{C,\gamma}$, i.e., if and only if $\overline{\mathcal{S}_C} = \mathcal{S}_C/\pi^k\mathfrak{o}$ and C have the same order. Conversely, if $\mathcal{S}$ is any subring of $\mathfrak{o}$ which contains $\mathcal{I}(\gamma)$, then we can consider the submodule $C_{\mathcal{S}} = \mathcal{S} \cdot \gamma = \big\{[\zeta]_F(\gamma) \,\big|\, \zeta \in \mathcal{S}\big\}$ of the finite $\mathcal{S}$-module $\ker\,[\pi^k]_F$. According to Proposition 1.2, the pair $(C_{\mathcal{S}}, \gamma)$ satisfies

(P1). Furthermore, $\mathcal{S} \subseteq \mathcal{S}_{C_{\mathcal{S}}} \subseteq \mathcal{T}_{C_{\mathcal{S}},\gamma} \subseteq \mathcal{S}$, which shows that $(C_{\mathcal{S}}, \gamma)$ satisfies (P2) as well. We note also that if (C, γ) satisfies (P1) and (P2), then $C_{\mathcal{S}_C} = C$. Indeed, it is clear that $C_{\mathcal{S}_C} \subseteq C$, and $C \subseteq C_{\mathcal{S}_C}$ according to Lemma 2.5 plus the fact that $\mathcal{S}_C = \mathcal{T}_{C,\gamma}$. This proves the following.

Corollary 5.3. *Let F be a full p-adic formal group. For each $0 \neq \gamma \in \Lambda(F)$, the association $C \mapsto \mathcal{S}_C$ defines a one-to-one correspondence between finite subgroups C of $\Lambda(F)$ for which the pair (C, γ) satisfies properties* (P1) *and* (P2) *of Proposition* 5.1 *and subrings of $\mathfrak{o}_{\Sigma_F}$ containing the ideal $\mathcal{I}(\gamma)$.*

In the special case where $\mathcal{I}(\gamma) = \pi\mathfrak{o}$, for any subgroup C of $\ker[\pi]_F$ containing γ, $\overline{\mathcal{S}_C}$ is a subfield of the residue field $\mathfrak{o}/\pi\mathfrak{o} = \mathbb{F}_{p^f}$. For each divisor r of f, one can use Corollary 5.3 to construct a (unique) subgroup C_r of $\ker[\pi]_F$ of order p^r such that (C_r, γ) satisfies (P1) and (P2); more specifically, $\overline{\mathcal{S}_{C_r}}$ is the subfield of $\mathbb{F}_{p^f}$ of order p^r. If f is composite and $r \neq 1$ or f, then C_r is a noncyclic deflated subgroup of F such that $T(F/C_r)$ is a free $c\big(\mathrm{End}(F/C_r)\big)$-module of rank 1.

6. Special results for height 2 formal groups

Our general results from §4 and §5 yield a wealth of information about p-adic formal groups of height 2 because of the following.

Proposition 6.1. *If F is a p-adic formal group of height* 2*, then every deflated subgroup of F is cyclic.*

Proof. Because $\ker[p]_F$ has p^2 elements, C is a product of at most two cyclic subgroups. But as C is deflated, $\ker[p]_F \nsubseteq C$. Hence $C \cap \ker[p]_F$ has at most p elements which proves that C is cyclic. □

The discussion after Theorem 3.5 shows that the converse of Proposition 6.1 is not true.

Corollary 6.2. *If G is an almost full p-adic formal group of height* 2*, then $T(G)$ is a free* $\mathrm{End}(G)$*-module of rank* 1*.*

We now give a proof of Conjecture 1.

Theorem 6.3. *Let F be a full p-adic formal group of height* 2*, and let C be a deflated* (*and hence cyclic*) *subgroup of F of order p^n. If $\mathfrak{o} = c\big(\mathrm{End}(F)\big)$, then $c\big(\mathrm{End}(F/C)\big) = \mathbb{Z}_p + p^n\mathfrak{o}$.*

Proof. The result is obvious if $C = \{0\}$, so we may assume that $n \geq 1$. By Theorem 4.3 and Remark 2.4(ii), it suffices to show that $\mathcal{I}(\gamma) = p^n\mathfrak{o}$, where γ is a generator of C. Clearly, $[p^n]_F(\gamma) = 0$ and $[p^{n-1}]_F(\gamma) \neq 0$. If $\Sigma_F/\mathbb{Q}_p$ is unramified, then p is a uniformizer of $\mathfrak{o}_{\Sigma_F}$, which shows that $\mathcal{I}(\gamma) = p^n\mathfrak{o}$ in this case. On the other hand, if $\Sigma_F/\mathbb{Q}_p$ is totally ramified and if π is a uniformizer of $\mathfrak{o}$, then either p^n or πp^{n-1} generates $\mathcal{I}(\gamma)$. If $[\pi p^{n-1}]_F(\gamma) = 0$, then $[p^{n-1}]_F(\gamma)$ would be a nonzero element of $\ker[\pi]_F \cap C$, which would imply that $\ker[\pi]_F \subseteq C$ because $\ker[\pi]_F$ is cyclic. This contradicts the assumption that C is a deflated subgroup of F, and so $\mathcal{I}(\gamma) = p^n\mathfrak{o}$ in this case as well. □

Finally, as an application, we use our results to show that the isomorphism class of an almost full p-adic formal group of height 2 depends only on its absolute endomorphism ring. This is a generalization in height 2 of [Lu3, 4.3.2].

Corollary 6.4. *Let G_1 and G_2 be almost full p-adic formal groups of height 2 such that $c(\mathrm{End}(G_1)) = c(\mathrm{End}(G_2))$. Then G_1 and G_2 are isomorphic via an isogeny.*

Proof. Using Corollary 1.8 and the results in §3, we can find full p-adic formal groups F_1 and F_2 and deflated subgroups C_1 and C_2 of F_1 and F_2 respectively such that $F_1/C_1 \cong G_1$ and $F_2/C_2 \cong G_2$. Since $\Sigma_{F_1} = \Sigma_{G_1} = \Sigma_{G_2} = \Sigma_{F_2}$, we may assume without loss of generality that $F_1 = F_2 = F$ [Lu3, 4.3.2]. Then, according to Theorem 4.4, the fact that $c(\mathrm{End}(G_1)) = c(\mathrm{End}(G_2))$ implies that $\mathcal{I}(C_1) = \mathcal{I}(C_2)$. Since C_1 and C_2 are cyclic, it follows from Corollary 2.8 that there exists some $u \in \mathrm{Aut}(F)$ such that $C_1 = u(C_2)$. Therefore, $C_1 \sim C_2$ by Proposition 3.1, whence $G_1 \cong G_2$ by definition. That this isomorphism is an isogeny follows from Corollary 1.7. $\square$

Remark 6.5. We could have instead used the main theorem in [W] to prove Corollary 6.4. Indeed, for $i = 1, 2$, C_i is cyclic, and therefore the Tate module $T(G_i)$ is free of rank 1 over $R = c(\mathrm{End}(G_i))$, according to Corollary 5.2. So, certainly $T(G_1)$ and $T(G_2)$ are isomorphic as R-modules.

References

[F] Fröhlich, A. Formal groups. Lecture Notes in Mathematics, 74. *Springer-Verlag, Berlin-New York*, 1968. MR0242837 (39 #4164), Zbl 0177.04801.

[Lang] Lang, Serge. Algebra, Second edition. *Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA*, 1984. MR0783636 (86j:00003), Zbl 0712.00001.

[Laz] Lazard, Michel. Sur les groupes de Lie formels à un paramétre. *Bull. Soc. Math. France* **83** (1955), 251–274. MR0073925 (17,508e), Zbl 0068.25703.

[Lu1] Lubin, Jonathan. Canonical subgroups of formal groups. *Trans. Amer. Math. Soc.* **251** (1979), 103–127, MR0531971 (80j:14039), Zbl 0431.14014.

[Lu2] Lubin, Jonathan. Finite subgroups and isogenies of one-parameter formal Lie groups. *Ann. of Math.* **85** (1967), 296–302. MR0209287 (35 #189), Zbl 0166.02803.

[Lu3] Lubin, Jonathan. One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings. *Ann. of Math.* **80** (1964), 464–484. MR0168567 (29 #5827), Zbl 0135.07003.

[LT] Lubin, Jonathan; Tate, John. Formal complex multiplication in local fields. *Ann. of Math.* **81** (1965), 380–387, MR0172878 (30 #3094), Zbl 0128.26501.

[S] Schmitz, David. Canonical and filling subgroups of formal groups. *New York J. Math.* **12** (2006), 235–247.

[W] Waterhouse, William C. A classification of almost full formal groups. *Proc. Amer. Math. Soc.* **20** (1969), 426–428. MR0236189 (38 #4487), Zbl 0176.30303.

DEPARTMENT OF MATHEMATICS, NORTH CENTRAL COLLEGE, 30 N BRAINARD ST, NAPERVILLE, IL 60540
djschmitz@noctrl.edu

This paper is available via http://nyjm.albany.edu/j/2006/12-13.html.