

## Canonical and filling subgroups of formal groups

David J. Schmitz

ABSTRACT. Let  $F$  be a one-dimensional full or almost full  $p$ -adic formal group. We look for finite subgroups  $C$  of  $F$  for which the quotient formal group  $F/C$  is full. In particular, we investigate the connection between such groups and the congruence-torsion subgroups of  $F$  described in Lubin, 1979. In doing so, we prove a conjecture of Jonathan Lubin concerning this relationship when  $F$  has height 2.

### CONTENTS

1. Introduction and notation	235
2. Filling subgroups	238
3. Canonical subgroups	239
4. Further results concerning canonical subgroups	245
References	246

### 1. Introduction and notation

Let  $p$  be a prime number, and let  $\overline{\mathbb{Q}}_p$  be a fixed algebraic closure of the field  $\mathbb{Q}_p$  of  $p$ -adic numbers. Let  $v$  denote the unique extension of the  $p$ -adic valuation on  $\mathbb{Q}_p$  to a rational valuation on  $\overline{\mathbb{Q}}_p$ , normalized so that  $v(p) = 1$ . If  $\mathbb{C}_p$  is the completion of  $\overline{\mathbb{Q}}_p$  with respect to  $v$ , then  $v$  extends uniquely, by continuity, to a rational valuation on  $\mathbb{C}_p$ , and we denote this valuation by  $v$  as well. Furthermore, we write  $\mathfrak{D}$  for the set  $\{x \in \mathbb{C}_p \mid v(x) \geq 0\}$  of  $v$ -integers, and  $\mathfrak{M}$  for the maximal ideal  $\{x \in \mathfrak{D} \mid v(x) > 0\}$  of  $\mathfrak{D}$ . For any subfield  $K$  of  $\mathbb{C}_p$ , we denote by  $\mathfrak{o}_K$  the integer ring of  $K$ , i.e.,  $\mathfrak{o}_K = K \cap \mathfrak{D}$ .

If  $F(X, Y)$  is a  $p$ -adic formal group, i.e., a one-dimensional formal group of finite height defined over some  $\mathfrak{o}_K$  with  $[K : \mathbb{Q}_p] < \infty$ , then  $F$  endows  $\mathfrak{M}$  with a group structure, where, for  $\alpha, \beta \in \mathfrak{M}$ ,  $\alpha +_F \beta = F(\alpha, \beta)$ . This abelian group, called the *points of  $F$* , will be denoted  $F(\mathfrak{D})$ . The torsion subgroup of  $F(\mathfrak{D})$  is

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

Received February 28, 2006.

*Mathematics Subject Classification.* 11S31, 14L05.

*Key words and phrases.*  $p$ -adic formal groups, congruence-torsion subgroups.

This work was partially funded by a North Central College Junior Faculty Enhancement Grant.

where  $[p^n]_F$  denotes multiplication-by- $p^n$  on the group  $F(\mathfrak{D})$  [Lu2, §1.0]. If  $G$  is another  $p$ -adic formal group, then a homomorphism  $g : F \rightarrow G$  (assumed to be defined over  $\mathfrak{D}$ ) induces a group homomorphism (via evaluation)  $g : F(\mathfrak{D}) \rightarrow G(\mathfrak{D})$ , and the set  $\text{Hom}(F, G)$  of all homomorphisms from  $F$  to  $G$  forms a group. The map  $c : \text{Hom}(F, G) \rightarrow \mathfrak{D}$ , which assigns to each homomorphism its linear coefficient, is injective [Lu3, 2.1.1]. An easily-proved, yet very useful result is the following:

**Proposition 1.1** ([S, 1.2]). *If  $g : F \rightarrow G$  is a homomorphism and  $\alpha \in F(\mathfrak{D})$ , then  $v(g(\alpha)) \geq v(\alpha)$ , with equality if and only if either  $\alpha = 0$  or  $c(g) \in \mathfrak{D}^\times$ .*

A homomorphism  $g : F \rightarrow G$  for which  $c(g) \in \mathfrak{D}^\times$  is compositionally invertible (over  $\mathfrak{D}$ ) and is called an *isomorphism* from  $F$  to  $G$ . We say that  $g : F \rightarrow G$  is an *isogeny* if  $g$  is defined over a complete, discretely-valued subfield of  $\mathbb{C}_p$ ; it is enough to check only that  $c(g)$  belongs to such a subfield of  $\mathbb{C}_p$  [S, §1]. The set  $\text{Isog}(F, G)$  of all isogenies from  $F$  to  $G$  is a group [S, 1.6], and we say that  $F$  and  $G$  are *isogenous* if and only if  $\text{Isog}(F, G) \neq 0$ . If  $0 \neq g \in \text{Isog}(F, G)$ , then  $\ker(g) = \{\alpha \in F(\mathfrak{D}) \mid g(\alpha) = 0\}$  is a finite subgroup of  $F(\mathfrak{D})$  and  $g$  maps  $\Lambda(F)$  onto  $\Lambda(G)$  [S, §1].

The *absolute endomorphism ring* of  $F$ , denoted  $\text{End}(F)$ , is the set  $\text{Hom}(F, F)$ . If  $g \in \text{End}(F)$  and  $c(g) = a$ , then instead of  $g$  we will sometimes write  $[a]_F$ . The notation  $[m]_F$  for the multiplication-by- $m$  endomorphism is consistent with this convention since its linear coefficient is  $m$ . If  $F$  has height  $h$ , then  $[\Sigma_F : \mathbb{Q}_p]$  divides  $h$ , where  $\Sigma_F$  (the *endomorphism field* of  $F$ ) is the fraction field of  $c(\text{End}(F))$  in  $\mathbb{C}_p$  [Lu3, 2.3.2]. In particular,  $\Sigma_F$  is algebraic over  $\mathbb{Q}_p$ , and so every endomorphism of a  $p$ -adic formal group is an isogeny, and  $c(\text{End}(F))$  is a  $\mathbb{Z}_p$ -order of  $\Sigma_F$ . When  $[\Sigma_F : \mathbb{Q}_p] = h$  and  $c(\text{End}(F)) = \mathfrak{o}_{\Sigma_F}$  (the maximal order of  $\Sigma_F$ ), then  $F$  is said to be *full*. When  $[\Sigma_F : \mathbb{Q}_p] = h$  but  $c(\text{End}(F)) \neq \mathfrak{o}_{\Sigma_F}$ , then  $F$  is said to be *almost full*. Finally, we will call *quasi-full* any  $p$ -adic formal group  $F$  of height  $h$  where  $\text{End}(F)$  is integrally closed but  $[\Sigma_F : \mathbb{Q}_p] < h$ . Lubin and Tate show in [LT] how to construct a full  $p$ -adic formal group  $F$  over a given  $p$ -adic integer ring  $\mathfrak{o}_K$  such that  $c(\text{End}(F)) = \mathfrak{o}_K$ . According to [Lu3, 4.3.2], two full  $p$ -adic formal groups are isomorphic (via an isogeny) if and only if they have the same endomorphism field. An analogous result holds for almost full  $p$ -adic formal groups of height 2.

**Theorem 1.2** ([S, 6.4]). *Two almost full  $p$ -adic formal groups  $F$  and  $G$  of height 2 are isomorphic via an isogeny if and only if  $c(\text{End}(F)) = c(\text{End}(G))$ .*

Whereas there is essentially only one full  $p$ -adic formal group having a particular endomorphism field, Lubin showed [Lu2] how to construct an almost full  $p$ -adic formal group  $G$  for which  $c(\text{End}(G))$  is isomorphic to a given nonmaximal  $\mathbb{Z}_p$ -order  $R$  in a  $p$ -adic number field  $K$ . Starting with a full  $p$ -adic formal group  $F$  such that  $c(\text{End}(F)) = \mathfrak{o}_K$ , one can associate to  $R$  a finite subgroup  $C$  of  $\Lambda(F)$  [Lu2, 2.2 and 3.2]. If  $\varphi_C(T)$  is the power series

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

then  $\varphi_C$  is an isogeny from  $F$  to the  $p$ -adic formal group  $F/C$  given by

$$(F/C)(X, Y) = \varphi_C\left(F(\varphi_C^{-1}(X), \varphi_C^{-1}(Y))\right),$$

both of which are defined over any  $p$ -adic integer ring containing  $C$  and all the coefficients of  $F$  [Lu2, 1.4]. We refer to  $F/C$  as the *quotient of  $F$  by  $C$*  and to  $\varphi_C$  as the *projection homomorphism from  $F$  to  $F/C$* . If we set  $G = F/C$ , then  $c(\text{End}(G)) = R$  [Lu2, 3.2] and  $G$  is almost full because isogenous  $p$ -adic formal groups have the same height [Lu3, 2.2.3 and 2.3.1].

Another approach is to ask about the structure of the quotient of a given full or almost full  $p$ -adic formal group  $F$  by a finite subgroup  $C$  of  $\Lambda(F)$ . Since  $F$  and  $F/C$  have the same height and the same endomorphism field [Lu2, 3.0],  $F/C$  is either full or almost full as well. A more detailed description of  $F/C$  when  $F$  has height two is the subject of a couple of recent conjectures of Lubin, one of which is proved in [S]. We first recall that a finite subgroup  $D$  of  $\Lambda(F)$  is said to be a *deflated subgroup of  $F$*  if there is no subgroup  $C$  of  $\Lambda(F)$  with fewer elements such that  $F/C$  is isomorphic to  $F/D$ . We note that when  $F$  is full, then this is equivalent to  $D$  not containing the kernel of any noninvertible  $F$ -endomorphism [S, 3.5].

**Theorem 1.3** ([S, 6.3]: Lubin's First Conjecture). *Let  $F$  be a full  $p$ -adic formal group of height 2 and  $C$  a deflated (cyclic) subgroup of  $F$  of order  $p^n$ . Then  $c(\text{End}(F/C)) = \mathbb{Z}_p + p^n \mathfrak{o}_{\Sigma_F}$ .*

In light of Theorem 1.2 and the fact that each  $\mathbb{Z}_p$ -order in a quadratic extension  $K$  of  $\mathbb{Q}_p$  has the form  $\mathbb{Z}_p + p^n \mathfrak{o}_K$  for some integer  $n \geq 0$ , Theorem 1.3 shows how an arbitrary almost full  $p$ -adic formal group of height 2 can be realized as the quotient of a full  $p$ -adic formal group by a cyclic subgroup of a particular order. This is a special case of the fact that any  $p$ -adic formal group  $G$  is isomorphic to the quotient of a full or quasi-full  $p$ -adic formal group by some finite subgroup. Indeed, Lubin [Lu2, 3.2 and 1.6] proved that there exists a  $p$ -adic formal group  $F$  with  $\text{End}(F)$  integrally closed and isogenies  $g : F \rightarrow G$  and  $\tilde{g} : G \rightarrow F$  each defined over a  $p$ -adic integer ring. If  $C = \ker(g)$ , then the following formal analogue of a standard result from the theory of elliptic curves can be used to show that  $F/C$  and  $G$  are isomorphic.

**Theorem 1.4** ([Lu2, 1.5], [S, 1.3]). *Let  $\mathfrak{o}_K$  be the ring of integers of a complete, discretely-valued subfield of  $\mathbb{C}_p$ . If  $F$ ,  $G$ , and  $H$  are  $p$ -adic formal groups defined over  $\mathfrak{o}_K$ , and if  $g_1 : F \rightarrow G$ ,  $g_1 \neq 0$ , and  $g_2 : F \rightarrow H$  are isogenies defined over  $\mathfrak{o}_K$  with  $\ker(g_1) \subseteq \ker(g_2)$ , then there is a unique isogeny  $j : G \rightarrow H$  defined over  $\mathfrak{o}_K$  such that  $j \circ g_1 = g_2$ . If  $\ker(g_1) = \ker(g_2)$ , then  $j$  is an isomorphism.*

Since  $C$  is the kernel of both  $g : F \rightarrow G$  and  $\varphi_C : F \rightarrow F/C$ , Theorem 1.4 implies that  $G$  and  $F/C$  are isomorphic. The same reasoning shows that  $G/D$  is isomorphic to  $F$ , where  $D = \ker(\tilde{g})$ . In other words, every  $p$ -adic formal group possesses at least one subgroup which yields a full or quasi-full quotient. Lubin's second conjecture deals with these special subgroups, which we call *filling subgroups*. He guessed that the quotient of a given height 2 almost full  $p$ -adic formal group  $G$  by a cyclic subgroup of  $\Lambda(G)$  of a certain order should be full, and that this subgroup should be distinguishable in some (other) way from among all cyclic subgroups of  $\Lambda(G)$  of that order. His precise statement is given below.

**Conjecture 1.5** (Lubin's Second Conjecture). *Let  $G$  be a height 2 almost full  $p$ -adic formal group with  $c(\text{End}(G)) = \mathbb{Z}_p + p^n \mathfrak{o}$ , where  $\mathfrak{o}$  is the integer ring in a quadratic extension of  $\mathbb{Q}_p$ . Then  $\Lambda(G)$  has a cyclic subgroup  $D$  of order  $p^n$ , "canonical" somehow, where  $G/D$  is full.*

Proving this conjecture and some of its generalizations provides the focus for this paper. We will prove that the subgroup  $D$  in the second conjecture is “canonical” in the following sense: it consists of the  $p^n$  elements in the kernel of  $[p^n]_G$  which have the largest valuations. Furthermore, we will show that this subgroup is the smallest filling subgroup of  $G$ . Finally, we will investigate the set of all filling subgroups of an arbitrary almost full  $p$ -adic formal group  $G$  and explore how these subgroups relate to the canonical subgroups of  $G$ .

## 2. Filling subgroups

We begin by investigating those finite subgroups  $D$  of the points of a full or almost full  $p$ -adic formal group  $G$  which yield full quotients. We will calculate the orders of all such subgroups of  $\Lambda(G)$  and prove that no two of them have the same order.

**Definition 2.1.** Let  $G$  be a  $p$ -adic formal group. A finite subgroup  $D$  of  $\Lambda(G)$  is a *filling subgroup* of  $G$  if  $\text{End}(G/D)$  is integrally closed, i.e., if  $c(\text{End}(G/D)) = \mathfrak{o}_{\Sigma_G}$ .

As explained in the introduction, every  $p$ -adic formal group has at least one filling subgroup. In fact, if  $c(\text{End}(G)) = \mathbb{Z}_p$ , (such formal groups of all heights exist according to [Lu3, 5.2.1]), then *every* finite subgroup  $D$  of  $\Lambda(G)$  is filling; indeed,  $\mathbb{Z}_p \subseteq c(\text{End}(G/D)) \subseteq \mathfrak{o}_{\Sigma_G} = \mathbb{Z}_p$ . On the other hand, only full or almost full  $p$ -adic formal groups have filling subgroups that yield full quotients because isogenous  $p$ -adic formal groups have the same endomorphism fields and equal heights. Lubin’s second conjecture is concerned with a specific filling subgroup of an almost full  $p$ -adic formal group of height 2, but we aim to classify all filling subgroups of any full or almost full  $p$ -adic formal group. The next proposition is a first step in this direction.

**Proposition 2.2.** *Let  $D$  be any finite subgroup of the points of a  $p$ -adic formal group  $G$ . Then  $G/D \cong G$  if and only if  $D$  is the kernel of some nonzero  $G$ -endomorphism. In particular, the filling subgroups of a full  $p$ -adic formal group are the kernels of its nonzero endomorphisms.*

**Proof.** Assume first that  $D = \ker(g)$ , where  $0 \neq g \in \text{End}(G)$ . As  $g : G \rightarrow G$  and  $\varphi_D : G \rightarrow G/D$  have the same kernel, it follows from Theorem 1.4 that  $G$  is isomorphic to  $G/D$ . Conversely, if  $u : G/D \rightarrow G$  is an isomorphism, then  $u \circ \varphi_D$  is a nonzero endomorphism of  $G$  with kernel  $D$ . The last statement in the proposition follows from the fact that full  $p$ -adic formal groups with the same endomorphism field are isomorphic [Lu3, 4.3.2].  $\square$

The endomorphism kernels of a full or quasi-full formal group  $F$  are easy to describe because  $\text{End}(F)$  is a discrete valuation ring.

**Proposition 2.3** ([S, §2]). *Let  $F$  be a full or quasi-full  $p$ -adic formal group and let  $\pi$  be a uniformizer of  $c(\text{End}(F))$ . If  $g$  is any nonzero  $F$ -endomorphism, then  $\ker(g) = \ker[\pi^{e \cdot v(c(g))}]_F$  where  $e$  is the ramification index of  $\Sigma_F/\mathbb{Q}_p$ . In particular, for each integer  $m \geq 0$ ,  $\ker[p^m]_F = \ker[\pi^{me}]_F$ .*

Suppose  $F$  is a full or quasi-full  $p$ -adic formal group and that  $\pi$  is a uniformizer of  $c(\text{End}(F))$ . If  $X$  is a finite subset of  $\Lambda(F)$ , we will write  $\ell(X) = k$  where  $k$  is the smallest nonnegative integer such that  $X \subseteq \ker[\pi^k]_F$ . Thus,  $\ell$  measures the depth

of a subset of  $\Lambda(F)$  in the filtration of subgroups  $\{\ker [\pi^m]_F\}_{m \geq 0}$ . According to [S, 2.2],  $\ker [\pi^m]_F$  has  $p^{m(h/e)}$  elements, where  $h$  is the height of  $F$  and  $e$  is the ramification index of  $\Sigma_F/\mathbb{Q}_p$ . Therefore, in light of Proposition 2.2, if  $F$  is full, there is for each nonnegative integer  $m$  exactly one filling subgroup of  $F$  of order  $p^{mf}$  (where  $f$  is the residue field degree of  $\Sigma_F/\mathbb{Q}_p$ ), and  $F$  has no other filling subgroups. We next prove similar results for an arbitrary  $p$ -adic formal group, namely, that the orders of some of its filling subgroups form an arithmetic sequence with common difference equal to  $h/e$ , and that no two of these filling subgroups have the same order.

**Theorem 2.4.** *Let  $D$  be a finite subgroup of the points of a full or quasi-full  $p$ -adic formal group  $F$  with  $\ell(D) = n$ . For each  $m \geq 0$ , let  $C_m = \varphi_D(\ker [\pi^m]_F)$ , where  $\pi$  is a uniformizer of  $c(\text{End}(F))$ . Then  $\{C_m\}_{m \geq n}$  is the set of distinct filling subgroups of  $F/D$  yielding a quotient isomorphic to  $F$ . Moreover, if  $|D| = p^k$ , then for each  $m \geq n$ ,  $|C_m| = p^{m(h/e)-k}$ , where  $h$  is the height of  $F$  and  $e$  is the ramification index of  $\Sigma_F/\mathbb{Q}_p$ .*

**Proof.** Let  $G = F/D$ . If  $u : G/C \rightarrow F$  is an isomorphism, then  $u \circ \varphi_C \circ \varphi_D$  is an endomorphism  $g$  of  $F$  with  $D \subseteq \ker(g) = \varphi_D^{-1}(C)$ . According to Proposition 2.3,  $\ker(g) = \ker [\pi^m]_F$  for some integer  $m \geq \ell(D)$ . Using the surjectivity of  $\varphi_D$ , it follows that  $C = \varphi_D(\ker [\pi^m]_F) = C_m$ . Conversely, if  $m \geq \ell(D)$ , then using Theorem 1.4 and Proposition 2.2, we have

$$G/C_m \cong F/(D +_F \ker [\pi^m]_F) = F/\ker [\pi^m]_F \cong F.$$

To compute the order of  $C_m$  ( $m \geq n$ ), we note that  $D = \ker(\varphi_D) \subseteq \ker [\pi^m]_F$  and then refer to the discussion preceding the statement of the theorem. These orders show that the  $C_m$  are distinct. □

**Corollary 2.5.** *Let  $D$  be a finite subgroup of the points of a full  $p$ -adic formal group  $F$  and let  $\pi$  be a uniformizer of  $c(\text{End}(F))$ . Then  $\{\varphi_D(\ker [\pi^m]_F)\}_{m \geq \ell(D)}$  is the set of all filling subgroups of  $F/D$ .*

Our second corollary follows from Theorem 2.4, plus the fact that  $\{0\}$  is a filling subgroup of a full  $p$ -adic formal group.

**Corollary 2.6.** *A full or almost full  $p$ -adic formal group has a unique deflated filling subgroup.*

By contrast, a full or almost full  $p$ -adic formal group can have several nonfilling deflated subgroups which yield isomorphic quotients. For example, let  $F$  be a full  $p$ -adic formal group of height 2, and assume that  $\Sigma_F/\mathbb{Q}_p$  is unramified. Since  $|\ker [p]_F| = p^2$ ,  $\Lambda(F)$  has more than one (cyclic) subgroup of order  $p$ . If  $C$  and  $D$  are two such subgroups, then  $c(\text{End}(F/C)) = c(\text{End}(F/D)) = \mathbb{Z}_p + p\mathfrak{o}_K$  by Theorem 1.3, whence  $F/C \cong F/D$  by Theorem 1.2. Furthermore,  $C$  and  $D$  are both deflated subgroups of  $F$  since they are not filling and since  $\{0\}$  is the only subgroup of  $\Lambda(F)$  with fewer elements.

### 3. Canonical subgroups

Lubin’s second conjecture suggests that filling subgroups of an almost full  $p$ -adic formal group can be distinguished somehow from other subgroups of the same

order. Unlike with full  $p$ -adic formal groups, however, a filling subgroup of an almost full  $p$ -adic formal group  $G$  cannot be the kernel of an endomorphism since for any  $0 \neq g \in \text{End}(G)$ ,  $G/\ker(g)$  is isomorphic to  $G$ . We will show eventually that filling subgroups of all full and almost full  $p$ -adic formal groups are “canonical” in a sense first described in [Lu1]. We begin here with the basic definitions and some preliminary results.

**Definition 3.1.** Let  $G$  be a  $p$ -adic formal group. A subgroup  $S$  of  $\Lambda(G)$  is called a *congruence-torsion subgroup* of  $G$  if there exists a positive real number  $\lambda$  such that  $S = \Lambda(G)_\lambda = \{\alpha \in \Lambda(G) \mid v(\alpha) \geq \lambda\}$ . We say  $S$  is a *canonical subgroup* of  $G$  if  $S = (\ker [p^n]_G)_\lambda$  for some  $\lambda \in \mathbb{R}^+$ , where  $|S| = p^n$ .

**Remarks 3.2.**

- (i) If  $\lambda \in \mathbb{R}^+$  and  $C$  is a subgroup of  $G(\mathfrak{D})$ , then  $C_\lambda = \{\alpha \in C \mid v(\alpha) \geq \lambda\}$  is a subgroup of  $C$ . This follows from the fact that for any  $\alpha, \beta \in G(\mathfrak{D})$ ,  $v(\alpha +_G \beta) \geq \min\{v(\alpha), v(\beta)\}$ , with equality if  $v(\alpha) \neq v(\beta)$  [Lu1, §2].
- (ii) Every congruence-torsion subgroup of  $G$  is finite [Si, IV.6.1].
- (iii) If  $C = \langle \gamma \rangle$  is a cyclic congruence-torsion subgroup of  $G$  of order  $p^n$  and if  $m$  is any integer, then  $[m]_G(\gamma)$  generates  $C$  if and only if  $m$  is prime to  $p$ , i.e., if and only if  $v(m) = 0$ . Then, according to Proposition 1.1, the generators of  $C$  are those elements having the smallest valuation. It follows inductively that every subgroup of  $C$  is also a congruence-torsion subgroup of  $G$ .

In the next proposition, we show that the congruence-torsion subgroups of  $G$  and the canonical subgroups of  $G$  are actually the same. This generalizes a result in [Lu1, §4], where  $C$  is assumed to be cyclic.

**Proposition 3.3.** *Let  $G$  be a  $p$ -adic formal group, and let  $C$  be a subgroup of  $\Lambda(G)$  of order  $p^n$ . Then  $C$  is a congruence-torsion subgroup of  $G$  if and only if  $C$  is a canonical subgroup of  $G$ .*

**Proof.** Assume first that  $C$  is a congruence-torsion subgroup of  $G$ , say  $C = \Lambda(G)_\lambda$ . Because  $|C| = p^n$ , we know that  $C \subseteq \ker [p^n]_G$ . Clearly,  $C = (\ker [p^n]_G)_\lambda$ .

Conversely, assume  $C$  is a canonical subgroup of  $G$ . Set  $\lambda = \min\{v(\alpha) \mid \alpha \in C\}$ , so that  $C = (\ker [p^n]_G)_\lambda$ . If  $C$  is not a congruence-torsion subgroup of  $G$ , then there exists some  $\beta \in \Lambda(G) - C$  such that  $v(\beta) \geq \lambda$ . Since  $\beta \notin \ker [p^n]_G$ ,  $\beta$  has order  $p^m$  for some  $m > n$ . Then  $\gamma = [p^{m-n}]_G(\beta)$  has order  $p^n$  and therefore belongs to  $\ker [p^n]_G$ . From Proposition 1.1 it follows that  $v(\gamma) > v(\beta) \geq \lambda$ , and hence  $\gamma \in C$ . But then  $\gamma$  is a generator of  $C$  since  $|C| = p^n$ . Because the generators are the elements of smallest valuation in a cyclic subgroup of  $\Lambda(G)$  (Remark 3.2(iii)), we see that  $v(\gamma) = \lambda$ , a contradiction.  $\square$

In [Lu1] and [K1], the term “canonical subgroup” is more restrictive than our definition allows. There, a canonical subgroup of a  $p$ -adic formal group  $G$  is a congruence-torsion subgroup of  $G$  which is the kernel of a homomorphism defined on  $G$  that reduces to the Frobenius homomorphism  $T \mapsto T^p$  in characteristic  $p$ . For a one-dimensional  $p$ -adic formal group  $G$ , the kernel of any lifting of  $T \mapsto T^p$  has  $p$  elements; thus, only canonical subgroups of order  $p$  are considered in [Lu1]. Here, there is no assumed connection between canonical subgroups and lifts of Frobenius or any other homomorphism in characteristic  $p$ .

The canonical subgroups of a full  $p$ -adic formal group  $F$  are easily determined using an observation made in the proof of [S, 2.7]. There it is shown that if  $\pi$  is a uniformizer of  $c(\text{End}(F))$ , then the elements of  $\ker [\pi^m]_F - \ker [\pi^{m-1}]_F$  have the same valuation, which is smaller than the valuation of any of the elements of  $\ker [\pi^{m-1}]_F$ . We thus obtain the following.

**Proposition 3.4.** *Let  $F$  be a full  $p$ -adic formal group and let  $\pi$  be a uniformizer of  $c(\text{End}(F))$ . Then for each  $m \geq 0$ ,  $\ker [\pi^m]_F$  is the canonical subgroup of  $F$  of order  $p^{mf}$ , where  $f$  is the residue field degree of  $\Sigma_F/\mathbb{Q}_p$ . These account for all of the canonical subgroups of  $F$ .*

In light of Proposition 2.3, we see that the canonical subgroups of a full  $p$ -adic formal group are precisely the kernels of its nonzero endomorphisms. This fact, together with Proposition 2.2, provides the first clue of a connection between canonical subgroups and filling subgroups.

**Corollary 3.5.** *A subgroup of a full  $p$ -adic formal group is filling if and only if it is canonical.*

We can use this characterization of the canonical subgroups of a full  $p$ -adic formal group in order to explore the connection between canonical and filling subgroups of almost full  $p$ -adic formal groups. In particular, we will determine the extent to which Corollary 3.5 is true for such formal groups and also prove Lubin’s second conjecture concerning almost full  $p$ -adic formal groups of height 2.

If  $G$  is an arbitrary almost full  $p$ -adic formal group, then  $G$  is isomorphic to the quotient of a full  $p$ -adic formal group  $F$  by a finite subgroup  $D$  of  $\Lambda(F)$ . Since isomorphisms map canonical subgroups to canonical subgroups (Proposition 1.1) and filling subgroups to filling subgroups (Theorem 1.4), we may assume without loss of generality that  $G = F/D$ . We will use the homomorphism  $\varphi_D : F \rightarrow G$  to study the valuations of the elements of  $\Lambda(G)$ . (We note here that the following discussion applies to *any*  $p$ -adic formal group  $F$ .) According to the explicit definition of  $\varphi_D$ , we see that for any  $\alpha \in \Lambda(F)$ ,

$$(1) \quad v(\varphi_D(\alpha)) = \sum_{\gamma \in D} v(\alpha +_F \gamma) = \sum_{\beta \in \alpha +_F D} v(\beta).$$

In order to more easily compare the valuations of the images under  $\varphi_D$  of different elements of  $\Lambda(F)$ , we introduce the following notation: if  $\alpha \in \Lambda(F)$ , then  $\tilde{\alpha}$  will denote an element in the coset  $\alpha +_F D$  having maximum valuation. If  $\gamma \in D$  and  $v(\gamma) < v(\tilde{\alpha})$ , then  $v(\tilde{\alpha} +_F \gamma) = v(\gamma)$ ; on the other hand, if  $v(\gamma) \geq v(\tilde{\alpha})$ , then  $v(\tilde{\alpha} +_F \gamma) = v(\tilde{\alpha})$  according to how  $\tilde{\alpha}$  is defined. These observations follow immediately from Remark 3.2(i). As  $\varphi_D(\alpha) = \varphi_D(\tilde{\alpha})$ , we infer from Equation (1) that

$$(2) \quad v(\varphi_D(\alpha)) = \sum_{\gamma \in D} v(\tilde{\alpha} +_F \gamma) = \sum_{\substack{\gamma \in D \\ v(\gamma) < v(\tilde{\alpha})}} v(\gamma) + \sum_{\substack{\gamma \in D \\ v(\gamma) \geq v(\tilde{\alpha})}} v(\tilde{\alpha}).$$

If  $\tilde{\alpha} = 0$ , then both sides of (2) are infinite; otherwise, both sides are finite since  $\varphi_D(\alpha) = 0$  if and only if  $\tilde{\alpha} = 0$ .

**Lemma 3.6.** *Let  $D$  be a finite subgroup of the points of a  $p$ -adic formal group  $F$ . If  $\alpha, \beta \in \Lambda(F)$ , then  $v(\varphi_D(\beta)) \geq v(\varphi_D(\alpha))$  if and only if  $v(\tilde{\beta}) \geq v(\tilde{\alpha})$ . In particular,  $v(\varphi_D(\alpha)) = v(\varphi_D(\beta))$  if and only if  $v(\tilde{\alpha}) = v(\tilde{\beta})$ .*

**Proof.** We may assume without loss of generality that  $\tilde{\beta} \neq 0$ . If  $v(\tilde{\alpha}) = v(\tilde{\beta})$ , then it is clear from Equation (2) that  $v(\varphi_D(\tilde{\alpha})) = v(\varphi_D(\tilde{\beta}))$ . If  $v(\tilde{\beta}) > v(\tilde{\alpha})$ , then

$$\begin{aligned} v(\varphi_D(\tilde{\beta})) &= \sum_{\substack{\gamma \in D \\ v(\gamma) < v(\tilde{\beta})}} v(\gamma) + \sum_{\substack{\gamma \in D \\ v(\gamma) \geq v(\tilde{\beta})}} v(\tilde{\beta}) \\ &= \sum_{\substack{\gamma \in D \\ v(\gamma) < v(\tilde{\alpha})}} v(\gamma) + \sum_{\substack{\gamma \in D \\ v(\tilde{\alpha}) \leq v(\gamma) < v(\tilde{\beta})}} v(\gamma) + \sum_{\substack{\gamma \in D \\ v(\gamma) \geq v(\tilde{\beta})}} v(\tilde{\beta}) \\ &\geq \sum_{\substack{\gamma \in D \\ v(\gamma) < v(\tilde{\alpha})}} v(\gamma) + \sum_{\substack{\gamma \in D \\ v(\tilde{\alpha}) \leq v(\gamma) < v(\tilde{\beta})}} v(\tilde{\alpha}) + \sum_{\substack{\gamma \in D \\ v(\gamma) \geq v(\tilde{\beta})}} v(\tilde{\beta}) \\ &> \sum_{\substack{\gamma \in D \\ v(\gamma) < v(\tilde{\alpha})}} v(\gamma) + \sum_{\substack{\gamma \in D \\ v(\gamma) \geq v(\tilde{\alpha})}} v(\tilde{\alpha}) \\ &= v(\varphi_D(\tilde{\alpha})). \end{aligned}$$

We note that the second inequality is strict because  $D$  always contains an element (e.g., 0) of valuation larger than  $v(\tilde{\beta})$ . The lemma now follows easily.  $\square$

We are now in a position to identify the canonical subgroups of any almost full  $p$ -adic formal group  $G$ . We do so in the next theorem, which is stated in more generality than we need now so as also to be of use in the next section.

**Theorem 3.7.** *Let  $F$  be a full or quasi-full  $p$ -adic formal group, and let  $\pi$  be a uniformizer of  $c(\text{End}(F))$ . Assume that  $\{\ker[\pi^m]_F\}_{m \geq 0}$  is the set of canonical subgroups of  $F$ . If  $D$  is any finite subgroup of  $\Lambda(F)$ , then  $\{\varphi_D(\ker[\pi^m]_F)\}_{m \geq 0}$  is the set of canonical subgroups of  $F/D$ .*

**Proof.** Let  $G = F/D$  and  $C_m = \varphi_D(\ker[\pi^m]_F) = \varphi_D(D +_F \ker[\pi^m]_F)$ . We first show that for every  $m \geq 1$ ,  $C_m$  is a canonical subgroup of  $G$  (the case  $m = 0$  is trivial). For any  $\gamma \in C_m$  and any  $\delta \in \Lambda(F/D) - C_m$ , there exists  $\alpha \in \ker[\pi^m]_F$  and  $\beta \in \Lambda(F) - (D +_F \ker[\pi^m]_F)$  such that  $\gamma = \varphi_D(\alpha)$  and  $\delta = \varphi_D(\beta)$ . Since  $\tilde{\alpha} \in \ker[\pi^m]_F$  (because  $\ker[\pi^m]_F$  is a congruence-torsion subgroup of  $F$ ) and since  $\tilde{\beta} \notin \ker[\pi^m]_F$ , it follows that  $v(\tilde{\alpha}) > v(\tilde{\beta})$ . Therefore by Lemma 3.6,  $v(\gamma) > v(\delta)$ , and so  $C_m$  is a congruence-torsion (i.e., canonical) subgroup of  $G$ .

We now show  $G$  has no other canonical subgroups. Suppose  $C_m \neq C_{m+1}$ . For any  $\gamma \in C_{m+1} - C_m$ , take  $\alpha \in \ker[\pi^{m+1}]_F - (D +_F \ker[\pi^m]_F)$  such that  $\gamma = \varphi_D(\alpha)$ . Using reasoning similar to that above, we see that  $\tilde{\alpha} \in \ker[\pi^{m+1}]_F - \ker[\pi^m]_F$ . This, in light of Lemma 3.6 plus the fact that  $\{\ker[\pi^m]_F\}_{m \geq 0}$  is the set of canonical subgroups of  $F$ , implies that all elements of  $C_{m+1} - C_m$  have the same valuation, and so there can be no canonical subgroups between  $C_m$  and  $C_{m+1}$ .  $\square$

The following corollary is immediate.



**Corollary 3.8.** *If  $G$  is an almost full  $p$ -adic formal group, then every filling subgroup of  $G$  is canonical. Furthermore, every canonical subgroup of  $G$  containing the deflated filling subgroup of  $G$  is itself filling.*

**Remark 3.9.** In the proof of Theorem 3.7, it is possible for  $C_m$  and  $C_{m+1}$  to be equal, even if  $D$  is deflated. (However, according to Corollaries 2.5 and 3.8, this cannot happen if  $C_{m+1}$  is filling.) For example, when  $F$  is full,  $\Sigma_F/\mathbb{Q}_p$  is totally ramified of degree at least 2, and  $D$  is the (deflated) cyclic subgroup of  $\Lambda(F)$  of order  $p$  generated by an element  $\delta_0 \in \ker[\pi^2]_F - \ker[\pi]_F$ , then, by considering orders, we see that  $D +_F \ker[\pi]_F = \ker[\pi^2]_F$  since  $D \cap \ker[\pi]_F = \{0\}$ . Thus  $\varphi_D(\ker[\pi]_F) = \varphi_D(\ker[\pi^2]_F)$ . On the other hand, when  $F$  is full,  $\Sigma_F/\mathbb{Q}_p$  is unramified of any degree greater than 1, and  $D$  is any deflated subgroup of  $F$ , then  $C_m$  is always a proper subset of  $C_{m+1}$ . Indeed,  $C_m = C_{m+1}$  if and only if  $\ker[p^{m+1}]_F \subseteq D +_F \ker[p^m]_F$ , in which case we would have  $\ker[p]_F = [p^m]_F(\ker[p^{m+1}]_F) \subseteq [p^m]_F(D) \subseteq D$ , contradicting the assumption that  $D$  is deflated.

We now prove Lubin’s Second Conjecture, which we restate as:

**Theorem 3.10.** *Let  $G$  be an almost full  $p$ -adic formal group with height 2 and  $c(\text{End}(G)) = \mathbb{Z}_p + p^n \mathfrak{o}$ , where  $\mathfrak{o}$  is the integer ring in a quadratic extension of  $\mathbb{Q}_p$ . Then the deflated filling subgroup of  $G$  is cyclic of order  $p^n$  and canonical.*

**Proof.** Using Theorems 1.2 and 1.3, we may assume that  $G = F/D$  where  $F$  is a full  $p$ -adic formal group with  $\mathfrak{o}_{\Sigma_F} = \mathfrak{o}$  and where  $D$  is a deflated cyclic subgroup of  $F$  of order  $p^n$ . The deflated filling subgroup  $C$  of  $F/D$  is cyclic [S, 6.1] and canonical (Corollary 3.8), and so we have only to determine its order. If  $\Sigma_F/\mathbb{Q}_p$  is unramified, then  $\ell(D) = n$ . If  $\Sigma_F/\mathbb{Q}_p$  is totally ramified and  $\pi$  is a uniformizer of  $c(\text{End}(F))$ , then  $\ell(D) = 2n$ , for if  $\ell(D) = 2n - 1$  then  $\ker[\pi]_F = [p^{n-1}]_F(D) \subset D$ , which contradicts our assumption that  $D$  is deflated. In either case, Corollary 2.5 says that  $C = \varphi_D(\ker[p^n]_F)$ . Therefore,  $|C| = |\ker[p^n]_F|/|D| = p^{2n}/p^n = p^n$ .  $\square$

Corollary 2.5 and Theorem 3.7 together show that, unlike full  $p$ -adic formal groups, almost full  $p$ -adic formal groups may have nonfilling canonical subgroups, namely (using the notation of Corollary 2.5) the subgroups  $\varphi_D(\ker[\pi^m]_F)$  where  $m < \ell(D)$ . However, as long as  $D$  is deflated, all of these subgroups (except for  $\{0\}$ ) are at least “almost filling” as described in the next proposition.

**Proposition 3.11.** *Let  $F$  be a full  $p$ -adic formal group and  $D$  a deflated subgroup of  $F$  with  $\ell(D) = n > 1$ . If  $G = F/D$  and  $C_m = \varphi_D(\ker[\pi^m]_F)$  where  $\pi$  is a uniformizer of  $c(\text{End}(F))$ , then for every  $1 \leq m < n$ ,*

$$c(\text{End}(G)) \subsetneq c(\text{End}(G/C_m)) \subsetneq c(\text{End}(F)).$$

**Proof.** The second strict containment follows from the fact that  $F$  is full and  $C_m$  is a nonfilling subgroup of  $G$ . To derive the first containment, we first note that the kernel of  $\varphi_{C_m} \circ \varphi_D$  is  $D +_F \ker[\pi^m]_F$ , and so  $G/C_m \cong F/(D +_F \ker[\pi^m]_F)$  by Theorem 1.4. Then, according to [S, 4.1],

$$c(\text{End}(G)) = \{ \zeta \in \mathfrak{o}_{\Sigma_F} \mid [\zeta]_F(D) \subseteq D \}$$

and

$$c(\text{End}(G/C_m)) = \{ \zeta \in \mathfrak{o}_{\Sigma_F} \mid [\zeta]_F(D +_F \ker[\pi^m]_F) \subseteq D +_F \ker[\pi^m]_F \}.$$

It is now clear that  $c(\text{End}(G)) \subseteq c(\text{End}(G/C_m))$ . To show the containment is strict, we use the fact that  $D$  is deflated to find an  $\alpha \in \ker[\pi]_F - D$ . If  $\beta \in D$  is an element of minimum valuation, then  $v(\beta) < v(\alpha)$  since  $\ell(D) > 1$ , and so by [S, 2.5] there is some  $\zeta \in c(\text{End}(F))$  such that  $[\zeta]_F(\beta) = \alpha \notin D$ . Thus  $\zeta \notin c(\text{End}(G))$ . On the other hand, the fact that  $\ell(D) = n > 1$  implies that  $\beta \in \ker[\pi^n]_F - \ker[\pi^{n-1}]_F$ , whence  $\zeta = \epsilon\pi^{n-1}$  where  $\epsilon$  is a unit in  $\mathfrak{o}_{\Sigma_F}$  (since  $\alpha$  is a nonzero element of  $\ker[\pi]_F$ ). Therefore, for any  $1 \leq m < n$ ,

$$[\zeta]_F(D +_F \ker[\pi^m]_F) \subseteq [\zeta]_F(\ker[\pi^n]_F) \subseteq [\epsilon]_F(\ker[\pi]_F) \subseteq D +_F \ker[\pi^m]_F.$$

We conclude that  $\zeta \in c(\text{End}(G/C_m)) - c(\text{End}(G))$ .  $\square$

To illustrate this result, let  $G = F/D$  where  $F$  is a full height 2  $p$ -adic formal group and  $D$  is a deflated (cyclic) subgroup of  $F$  of order  $p^n$ . Then  $c(\text{End}(F/D)) = \mathbb{Z}_p + p^n\mathfrak{o}$ , where  $\mathfrak{o} = \mathfrak{o}_{\Sigma_F}$ . The deflated filling subgroup of  $G$ ,  $C = \varphi_D(\ker[p^n]_F)$ , is cyclic of order  $p^n$  (see the proof of Theorem 3.10), and therefore, in light of Remark 3.2(iii),  $G$  has a nonfilling canonical (cyclic) subgroup  $C_m$  of order  $p^m$  for every  $0 \leq m < n$ . In particular,  $C_m = [p^{n-m}]_G(C) = \varphi_D(\ker[p^m]_F)$ . To determine the absolute endomorphism ring of  $G/C_m \cong F/(D +_F \ker[p^m]_F)$ , we first note that  $D +_F \ker[p^m]_F = [p^m]_F^{-1}([p^m]_F(D))$ , and so  $G/C_m \cong F/[p^m]_F(D)$  [S, 3.1]. But  $[p^m]_F(D)$  is a deflated (cyclic) subgroup of  $F$  of order  $p^{n-m}$ , whence  $c(\text{End}(G/C_m)) = \mathbb{Z}_p + p^{n-m}\mathfrak{o}$  by Theorem 1.3.

Our results provide an easy algebraic method for counting the number of elements in the congruence-torsion subgroups of any almost full  $p$ -adic formal group. Furthermore, the fundamental relationship in Corollary 3.8 is useful in establishing results such as the following.

**Proposition 3.12.** *Let  $C$  be a canonical subgroup of a full or almost full  $p$ -adic formal group  $G$ , and let  $0 \neq g \in \text{End}(G)$ . Then*

- (i)  $g(C)$  is a canonical subgroup of  $G$ ;
- (ii)  $g^{-1}(C)$  is canonical subgroup of  $G$  if  $C$  is filling.

**Proof.** (i): As before, we may assume that  $G = F/D$  where  $F$  is a full  $p$ -adic formal group and  $D$  is a finite subgroup of  $\Lambda(F)$ . Then  $C = \varphi_D(\ker[\pi^m]_F)$  for some  $m \geq 0$ , where  $\pi$  is a uniformizer of  $c(\text{End}(F))$  (Theorem 3.7). If  $j = [c(g)]_F \in \text{End}(F)$ , then  $g \circ \varphi_D = \varphi_D \circ j$  by the injectivity of  $c$ . Thus,  $g(C) = \varphi_D(j(\ker[\pi^m]_F))$ . Write  $j = [\epsilon\pi^k]_F$  where  $\epsilon$  is a unit in  $\mathfrak{o}_{\Sigma_F}$  and  $k \geq 0$ . If  $k \geq m$ , then  $g(C) = \{0\}$ , while if  $k < m$ , then  $g(C) = \varphi_D(\ker[\pi^{m-k}]_F)$ . In either case,  $g(C)$  is a canonical subgroup of  $G$  by Theorem 3.7.

(ii): This follows from Corollary 3.8 since  $G/g^{-1}(C) \cong G/C$  by [S, 3.1].  $\square$

**Remark 3.13.** We note that the preimage of a canonical subgroup under an endomorphism may be noncanonical. For example, if  $G$  is a height 2 almost full  $p$ -adic formal group with  $\Sigma_G/\mathbb{Q}_p$  unramified and  $\text{End}(G) \cong \mathbb{Z}_p + p^2\mathfrak{o}_{\Sigma_G}$ , then  $G$  has a nonfilling canonical subgroup  $C$  of order  $p$ , but no canonical subgroup of order  $p^3$ . Therefore  $[p]_G^{-1}(C)$ , which has  $p^3$  elements, cannot be canonical.

### 4. Further results concerning canonical subgroups

If  $G$  is a  $p$ -adic formal group which is neither full nor almost full, it is natural to ask whether there is some relationship between the filling subgroups and the canonical subgroups of  $G$ . Unfortunately, the situation is not as simple as that described in the previous section. We can show without much difficulty that it is *not* true in general that all filling subgroups are canonical. For example, if  $G$  has height  $h > 1$  and  $c(\text{End}(G)) = \mathbb{Z}_p$ , then we've already seen that every finite subgroup of  $\Lambda(G)$  is filling. However, not every finite subgroup of  $\Lambda(G)$  is canonical since  $|\ker [p]_G| > p$  and there can be at most one canonical subgroup of  $G$  of any order.

On the other hand, the canonical subgroups of some  $p$ -adic formal groups which are neither full nor almost full do behave in part like the canonical subgroups of full or almost full  $p$ -adic formal groups. For example, suppose  $F$  is a quasi-full  $p$ -adic formal group of height  $h > 1$  defined over  $\mathfrak{o}_K$ , where  $K$  is a finite unramified extension of  $\Sigma_F$ ; this happens, in particular, when  $F$  is a nonfull  $p$ -adic formal group defined over an unramified extension of  $\mathbb{Q}_p$  [Lu2, 3.3]. If  $\pi$  is a uniformizer of  $c(\text{End}(F))$ , then  $\{\ker [\pi^m]_F\}_{m \geq 0}$  is the set of kernels of all nonzero  $F$ -endomorphisms, and  $[\pi]_F$  is defined over  $\mathfrak{o}_K$ , a complete discrete valuation ring in which  $\pi$  is a uniformizer. Therefore,  $P(T)$ , the distinguished polynomial factor of  $[\pi]_F(T)/T$  coming from the Weierstrass Preparation Theorem, is irreducible over  $\mathfrak{o}_K$  by Eisenstein's criterion. This implies that the nonzero elements of  $\ker [\pi]_F$ , i.e., the roots of  $P(T)$ , are conjugate over  $K$ , whence they have the same valuation  $\lambda$ . For any  $\alpha \in \ker [\pi^{m+1}]_F - \ker [\pi^m]_F$  ( $m \geq 1$ ),  $v(\alpha) < \lambda$  by Proposition 1.1, and so

$$v([\pi]_F(\alpha)) = v(\alpha \cdot P(\alpha)) = \sum_{\xi \in \ker [\pi]_F} v(\alpha - \xi) = p^s v(\alpha),$$

where  $p^s = |\ker [\pi]_F|$ . By induction, we now see that  $v(\alpha) = p^{-ms}\lambda$ . Therefore, the kernels of the nonzero  $F$ -endomorphisms are the canonical subgroups of  $F$ . Since the kernels of the nonzero endomorphisms of a quasi-full  $p$ -adic formal group are filling by Proposition 2.2, we see that *every canonical subgroup of  $F$  is filling*. Furthermore, if  $D$  is any deflated subgroup of  $F$ , then according to Theorem 3.7, the set of canonical subgroups of  $F/D$  is  $\{\varphi_D(\ker [\pi^m]_F)\}_{m \geq 0}$ . When  $m \geq \ell(D)$ , Theorem 2.4 shows that  $\varphi_D(\ker [\pi^m]_F)$  is also filling. Thus, *every canonical subgroup of  $F/D$  of large enough order is filling*.

We can establish other results, weaker than their analogues in the previous section, describing properties of canonical subgroups of arbitrary  $p$ -adic formal groups.

**Proposition 4.1.** *If  $G$  is any  $p$ -adic formal group and  $C$  is any canonical subgroup of  $G$ , then  $c(\text{End}(G)) \subseteq c(\text{End}(G/C))$ .*

**Proof.** According to [S, 4.2],

$$c(\text{End}(G/C)) = \left\{ \zeta \in \mathfrak{o}_{\Sigma_G} \mid [p^n \zeta]_G([p^n]_G^{-1}(C)) \subseteq C \right\},$$

where  $n$  is an integer large enough so that  $p^n \mathfrak{o}_{\Sigma_G} \subseteq c(\text{End}(G))$ . Therefore, for any  $\zeta \in c(\text{End}(G))$ , we see that  $[p^n \zeta]_G([p^n]_G^{-1}(C)) = [\zeta]_G([p^n]_G([p^n]_G^{-1}(C))) = [\zeta]_G(C)$ . But as  $C$  is a canonical subgroup of  $G$ ,  $[\zeta]_G(C) \subseteq C$  by Proposition 1.1. Thus  $\zeta \in c(\text{End}(G/C))$ . □

**Proposition 4.2.** *Let  $C$  be a canonical subgroup of a  $p$ -adic formal group  $G$ . If  $C$  contains the kernel of some  $0 \neq g \in \text{End}(G)$ , then  $D = g^{-1}(C)$  is also a canonical subgroup of  $G$ .*

**Proof.** Let  $\gamma_0$  be an element having the smallest valuation among the elements of  $C$ . Because  $C$  is a canonical subgroup of  $G$ , we know that  $C = \Lambda(G)_{v(\gamma_0)}$ . Since  $v(g(x)) \geq v(x)$  for all  $x \in \Lambda(G)$ , it follows that  $C \subseteq D$ , with equality if and only if  $g \in \text{Aut}(G)$ . Therefore, we may assume that  $g \notin \text{Aut}(G)$ , i.e., that  $\ker(g) \neq \{0\}$ . If  $\kappa = \min\{v(\xi) \mid \xi \in \ker(g)\}$ , then  $v(\gamma_0) \leq \kappa$  because  $\ker(g) \subseteq C$ . If we use the Weierstrass Preparation Theorem to factor

$$g(T) = U(T) \prod_{\xi \in \ker(g)} (T - \xi)$$

where the constant term of  $U(T) \in \mathfrak{D}[[T]]$  is a unit, then we see that for any  $x \in \Lambda(G)$  with  $v(x) < \kappa$ ,

$$v(g(x)) = v(U(x)) + \sum_{\xi \in \ker(g)} v(x - \xi) = p^m v(x)$$

where  $p^m = |\ker(g)|$ .

Now choose any  $\alpha_0 \in \Lambda(G)$  with  $g(\alpha_0) = \gamma_0$ . Since  $g$  is not an automorphism of  $G$ ,  $v(\alpha_0) < v(g(\alpha_0)) = v(\gamma_0) \leq \kappa$ , whence  $v(\alpha_0) = p^{-m}v(\gamma_0)$ . Furthermore,  $\alpha_0$  has the minimum valuation among the elements of  $D$ . Indeed, if there were some  $\delta \in D$  such that  $v(\delta) < v(\alpha_0) < \kappa$ , then  $v(g(\delta)) = p^m v(\delta) < p^m v(\alpha_0) = v(\gamma_0)$ , which would contradict our choice of  $\gamma_0$ . Therefore, we need to show that  $D = \Lambda(G)_{v(\alpha_0)}$ . If not, then there would exist some  $\beta \in \Lambda(G) - D$  such that  $v(\beta) \geq v(\alpha_0)$ . We note that  $\beta \notin C$  (because  $C \subset D$ ), and so  $v(\beta) < v(\gamma_0) \leq \kappa$ . Hence,  $v(g(\beta)) = p^m v(\beta) \geq p^m v(\alpha_0) = v(\gamma_0)$ , which implies that  $g(\beta) \in C$ . This, contradicts the fact that  $\beta \notin D$ . Therefore,  $D$  is a canonical subgroup of  $G$ .  $\square$

We are less likely to find a simple characterization of the filling subgroups of  $p$ -adic formal groups which are neither full nor almost full because they are more “plentiful” than are the filling subgroups of full and almost full  $p$ -adic formal groups. This stems primarily from the fact that [Lu3, 4.3.2] does not hold for quasi-full  $p$ -adic formal groups. In other words, if  $F$  is a quasi-full  $p$ -adic formal group, then there may be nonisomorphic quasi-full  $p$ -adic formal groups  $G$  such that  $\Sigma_F = \Sigma_G$ . As the evidence presented earlier in this section could suggest, perhaps those filling subgroups which are canonical yield quasi-full quotients which possess some special property, such as having their coefficients (or those of an isomorphic formal group) belonging to “nice” (e.g., unramified) extension fields of their endomorphism fields.

## References

- [Kl] Klapper, A. Selmer group estimates arising from the existence of canonical subgroups. *Compositio Math.* **71** (1989), no. 2, 121–137. [MR1012637](#) (90i:14046).
- [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  $p$ -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. [Endomorphism rings of almost full formal groups](#). *New York J. Math.* **12** (2006), 219–233.
- [Si] Silverman, Joseph H. The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. *Springer-Verlag, New York*, 1986. [MR0817210](#) (87g:11070), [Zbl 0585.14026](#).

DEPARTMENT OF MATHEMATICS, NORTH CENTRAL COLLEGE, 30 N BRAINARD ST, NAPERVILLE, IL 60540

[djschmitz@noctrl.edu](mailto:djschmitz@noctrl.edu)

This paper is available via <http://nyjm.albany.edu/j/2006/12-14.html>.