ENTIRENESS OF THE ENDOМОРPHISM RINGS OF
ONE-DIMENSIONAL FORMAL GROUPS

JONATHAN LUBIN

ABSTRACT. If, for a one-dimensional formal group of height \( h \) which is defined over the integers in a local field of characteristic zero, all the coefficients in degree less than \( p^h \) lie in an unramified extension of the \( p \)-adic numbers, then the endomorphism ring of the formal group is integrally closed.

In this note, \( \mathbb{Q}_p \) and \( \mathbb{Z}_p \) denote the field of \( p \)-adic numbers and the ring of \( p \)-adic integers, respectively; \( K \) and \( B \) denote a finite field extension of \( \mathbb{Q}_p \) and the integral closure of \( \mathbb{Z}_p \) in \( K \), respectively; \( \overline{K} \) will be a fixed algebraic closure of \( K \), and \( v \) the unique extension to \( \overline{K} \) of the (additive) \( p \)-adic valuation on \( \mathbb{Q}_p \), normalized so that \( v(p) = 1 \); and finally, \( M \) will be the maximal ideal in the integral closure of \( B \) in \( \overline{K} \), or, equivalently, the set of all elements \( z \) of \( \overline{K} \) for which \( v(z) > 0 \). All formal groups considered will be commutative and one dimensional.

In [3] the following proposition appeared:

**Theorem 3.3.1.** If \( F \) is a one-dimensional formal group defined over \( B \), of height \( h < \infty \), and if the coefficients of \( F \) in terms of total degree less than \( p^h \) all lie in an unramified extension of \( \mathbb{Q}_p \), then \( \text{End}_B(F) \) is integrally closed in its fraction-field.

It was soon pointed out to me by A. Fröhlich and A. Trojan that the proof in [3] was incorrect. Later [4] I proved the weaker result that if \( F \) itself is defined over an unramified extension of \( \mathbb{Q}_p \), then \( \text{End}_B(F) \) is integrally closed. That proof made essential use of the fact [4, Theorem 1.5] that if \( F, G, \) and \( H \) are formal groups defined over \( B \), with \( f \in \text{Hom}_B(F, G) \) and \( g \in \text{Hom}_B(F, H) \) such that \( \ker(f) \subseteq \ker(g) \), then there is some \( h \in \text{Hom}_B(G, H) \) for which \( h \circ f = g \). In this note I will use that fact together with the theory of the Newton polygon of a power series, as described for instance in [2], to show that Theorem 3.3.1 of [3] is correct as stated there.

The proofs below are for the category of formal groups, i.e., formal \( \mathbb{Z}_p \)-modules; the generalization, in the spirit of [5] or [1], to the category of
formal $A$-modules, for $A$ the ring of integers in a finite field extension of $\mathbb{Q}_p$, is a comparatively easy exercise.

Now let $F$ be a fixed one-dimensional formal group defined over $B$, and of finite height $h$, with the property that all its coefficients in terms of total degree less than $p^h$ lie in an unramified extension of $\mathbb{Q}_p$. Then according to Lemma 3.2.2 of [3], $F$ is $B$-isomorphic to a formal group which is linear modulo degree $p^h$. We may assume from now on that $F$ itself has this shape. It is a consequence of this, since $B$ is of characteristic zero, that any endomorphism of $F$ is also linear modulo degree $p^h$.

The points of finite order of $F$, in $M$, form a group $W$ which is the disjoint union of $\{0\}$ with all the sets $X_m = \ker([p^m]_F) - \ker([p^{m-1}]_F)$, $m \geq 1$. We can now use the theory of the Newton polygon to show that if $w \in X_m$, then $v(w) = (p^h - 1)^{-1}p^h(1-m)$. Indeed, since $[p]_F(x) = px + wx^{p^h \mod(p^{h+1})}$, for some unit $u$ of $B$, the Newton polygon of $[p]_F(x)$ has its first vertex at $(1,1)$ and its next vertex at $(p^h, 0)$, so that the nonzero roots $w$ of $[p]_F$ in $M$ have $v(w) = 1/(p^h - 1)$. Inductively, if all elements $y$ of $X_{m-1}$ have $v(y) = (p^h - 1)^{-1}p^h(2-m)$, we use the fact that any $w$ in $X_m$ is a root of $-y + [p]_F(x)$ for some such $y$; the Newton polygon of this power series has no vertices between $(0, v(y))$ and $(p^h, 0)$. The slope of this segment of the polygon is $-v(y)/p^h$, and this is the only segment of the polygon with negative slope. Thus $v(w) = v(y)/p^h$, completing the induction.

Now let $f$ be a $B$-endomorphism of $F$. It will turn out that if $f$ is not an automorphism, there is some $g \in \text{End}_B(F)$ such that $f = [p]_F \circ g$; in other words, $\text{End}_B(F)$ is a discrete valuation ring with prime element $[p]_F$, and hence certainly integrally closed in its fraction field.

Suppose now that the $B$-endomorphism $f$ of $F$ is not an automorphism, and not zero. Then $\ker(f) \neq \{0\}$, and in fact $\ker(f) \cap \ker([p]_F) \neq \{0\}$, since all elements of $\ker(f)$ are annihilated by some power of $p$. The fact that $f$ has some nonzero roots in $M$ implies that the first segment of the Newton polygon is not horizontal; the fact that $f$ is linear modulo $(x^{p^h})$ implies that the right-hand endpoint of this segment has abscissa at least $p^h$. Nonzero elements of $W$ with greatest $v$-value are just the elements of $X_1$. So since $f$ has some roots in $X_1$, and at least $p^h - 1$ nonzero roots of greatest $v$-value, it follows that $f$ has $p^h - 1$ roots in $X_1$: we have $\ker([p]_F) \subset \ker(f)$. This completes the proof.

REFERENCES

3. Jonathan Lubin, One-parameter formal Lie groups over $p$-adic integer rings,
Ann. of Math. (2) 80 (1964), 464–484; Correction, ibid. (2) 84 (1966), 372. MR 29 #5827; 34 #179.


DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912