One-Parameter Formal Lie Groups Over $\mathfrak{p}$-Adic Integer Rings*

By JONATHAN LUBIN

Introduction

An n-parameter formal Lie group is a set of n-formal power series in $2n$ variables which behave formally like the equations describing the multiplication in an n-dimensional Lie group. In the case $n = 1$, the formal power series $F(x, y)$ must have first degree term $x + y$ and satisfy the associativity relation $F(x, F(y, z)) = F(F(x, y), z)$. Over a field of characteristic zero, a change of coordinates makes any such *group law* take the form $x + y$. It is the purpose here to examine the category of one-parameter formal Lie groups over a $\mathfrak{p}$-adic integer ring.

If E is an elliptic curve defined over a $\mathfrak{p}$-adic integer ring $\mathfrak{o}$, whose reduction modulo $\mathfrak{p}$ (where $\mathfrak{p}$ is the maximal ideal of $\mathfrak{o}$) is also elliptic, then the group G of those points of E rational over $\mathfrak{o}$ which are in the kernel of the reduction homomorphism may be studied by formal Lie group methods. If we localize E at the identity and complete the local ring, the formula for addition on E becomes a formal Lie group defined over $\mathfrak{o}$; if we call this group law $F(x, y)$, then the set $\mathfrak{p}$ is made a group by the addition $\alpha + \beta = F(\alpha, \beta) \in \mathfrak{p}$; and this group is isomorphic in a natural way to G, the kernel of reduction modulo $\mathfrak{p}$.

The theory is interesting also for the parallels with the theory of elliptic curves. An analogue of the fact that two elliptic curves with complex multiplication which have isomorphic endomorphism rings are isogenous, is the main theorem here (Theorem 4.3.2) which says that two *full* formal Lie groups are isomorphic if their endomorphism rings are the same. Also, the construction in § 5 of full formal Lie groups with any desired endomorphism ring can be thought of as analogous to the theorem of Deuring [1, p. 259] that an elliptic curve in characteristic p, together with one complex multiplication on it, can be lifted consistently to characteristic zero.

This paper employs the direct methods of Lazard [11] rather than the infinitesimal methods developed by Dieudonné in his series of papers [2] through [9], and it will be obvious to the reader to what extent I am indebted to Lazard. Equally great, but less obvious, is my dept to Professor John Tate for his insights and suggestions.

* This work was supported in part by a grant from the Research Corporation.

1. General notions

1.1.1. For any commutative ring A with unit, $A[[T_1, \cdots, T_n]]$ will denote the ring of formal power series in the indeterminates $T_1, \cdots, T_n$. The operation of substituting power series in a power series is well-defined as long as the substituents have no constant term.

1.1.2. If F and G are power series in $A[[T_1, \cdots, T_n]]$, we will say that F *is congruent to G modulo degree r*, $F \equiv G \bmod \deg r$, if F and G differ only in terms of total degree greater than or equal to r.

DEFINITION 1.2.1. A *one-parameter formal Lie group over the ring A* (or more simply: *group law over A*) is a formal power series $F(x, y) \in A[[x, y]]$ satisfying:

(i) $F(x, y) \equiv x + y \bmod \deg 2$

(ii) $F(F(x, y), z) = F(x, F(y, z))$.

1.2.2. REMARKS. An easy computation with formal power series shows that there is a power series $i_F(T) \in A[[T]]$ such that $F(T, i_F(T)) = 0$. Only part (i) of the above definition is used. Part (ii) shows, equally easily, that $F(x, 0) = x$.

All rings A over which group laws will be defined will be assumed to be commutative, with unit, and to have no nilpotent elements. According to Lazard [10], a group law defined over such a ring must be abelian, i.e., $F(x, y) = F(y, x)$.

DEFINITION 1.3.1. Let F and G be group laws over A. The power series f is an *A-homomorphism of F into G* if

(i) $f(T) \in A[[T]]$

(ii) f has constant term equal to zero

(iii) $f(F(x, y)) = G(fx, fy)$.

DEFINITION 1.3.2. The set of all A-homomorphisms of F into G is called $\mathrm{Hom}_A(F, G)$.

1.3.3. If $f_1, f_2 \in \mathrm{Hom}_A(F, G)$, then their sum $f_1 + f_2$ can be defined by: $(f_1 + f_2)(T) = G(f_1(T), f_2(T))$. A computation shows that, since G is abelian and associative, $f_1 + f_2$ is in $\mathrm{Hom}_A(F, G)$, and $+$ is commutative and associative. The formal power series $[0](T) = 0$ acts as an additive identity in $\mathrm{Hom}_A(F, G)$, and the additive inverse of $f(T)$ is $i_G(f(T)) = f(i_F(T))$. Thus $\mathrm{Hom}_A(F, G)$ is an abelian group.

Now if $f \in \mathrm{Hom}_A(F, G)$ and $g \in \mathrm{Hom}_A(G, H)$, then the composed power series $g \circ f$, defined by $(g \circ f)(T) = g(f(T))$, is in $\mathrm{Hom}_A(F, H)$. Composition is associative, and as a map

$$\mathrm{Hom}_A(G, H) \times \mathrm{Hom}_A(F, G) \to \mathrm{Hom}_A(F, H) ,$$

it is bi-additive.

Finally the power series $[1](T) = T$ is in every $\mathrm{Hom}_A(F, F)$, and has the property $[1] \circ f = f \circ [1] = f$.

Because of all these facts, the set of all group laws over A forms an additive category.

1.3.4. $\mathrm{End}_A(F)$, which is defined to be $\mathrm{Hom}_A(F, F)$, is now seen to be a ring with unit, but not necessarily commutative. We call $[n]_F$ the image of $n \in \mathbf{Z}$ under the canonical homomorphism of $\mathbf{Z}$ into $\mathrm{End}_A(F)$. With this notation, $[-1]_F$ is equal to the power series i_F mentioned in 1.2.2.

1.4.1. If $f \in \mathrm{Hom}_A(F, G)$, say $f(T) = a_1T + a_2T^2 + \cdots$, then we let $c(f)$ be the first-degree coefficient of f: $c(f) = a_1 \in A$. It follows immediately from the definitions of $+$ and $\circ$ that $c(f_1 + f_2) = c(f_1) + c(f_2)$ if $f_1, f_2 \in \mathrm{Hom}_A(F, G)$; and that $c(g \circ f) = c(g)c(f)$ if $f \in \mathrm{Hom}_A(F, G)$ and $g \in \mathrm{Hom}_A(G, H)$. Thus we have a canonical homomorphism c: $\mathrm{Hom}_A(F, G) \to A$ which is a unitary homomorphism of rings in the case c: $\mathrm{End}_A(F) \to A$.

1.5.1. If both A and B are commutative rings with unit and if $a \to a^*$ is a unitary ring homomorphism of A into B, then a group law $F(x, y)$ defined over A can be transformed to a group law $F^*(x, y)$ defined over B: if $F(x, y) = \sum a_{ij}x^iy^j$, then $F^*(x, y) = \sum a_{ij}^*x^iy^j$. Similarly, if $f \in \mathrm{Hom}_A(F, G)$, we have $f^* \in \mathrm{Hom}_B(F^*, G^*)$. If $f_1, f_2 \in \mathrm{Hom}_A(F, G)$, then $(f_1 + f_2)^* = f_1^* + f_2^*$; and if $f \in \mathrm{Hom}_A(F, G)$, $g \in \mathrm{Hom}_A(G, H)$, then $(g \circ f)^* = g^* \circ f^*$. Thus we have a covariant additive functor from the category of group laws over A to the category of group laws over B. For the endomorphism rings, this means that $f \to f^*$ is a unitary ring homomorphism of $\mathrm{End}_A(F)$ into $\mathrm{End}_B(F^*)$. In all the applications, B will be the residue-class field of A with respect to a maximal ideal, and $*$ will be the residue mapping.

2. Basic properties of $\mathrm{Hom}_{\mathfrak{o}}(F, G)$ and $\mathrm{End}_{\mathfrak{o}}(F)$

2.0. From now on we assume that our ground ring is a complete discrete valuation ring $\mathfrak{o}$ of characteristic zero with maximal ideal $\mathfrak{p} = \pi\mathfrak{o}$, such that the residue-class field $k = \mathfrak{o}/\mathfrak{p}$ is of characteristic $p > 0$. We use the fact that the fraction field L of $\mathfrak{o}$ is of characteristic zero to show that c maps $\mathrm{Hom}_{\mathfrak{o}}(F,G)$ isomorphically onto a subgroup of $\mathfrak{o}$ which is topologically closed, and $\mathrm{End}_{\mathfrak{o}}(F)$ onto a closed subring of $\mathfrak{o}$. Then, under the assumption that F^* is not isomorphic over k to the additive group law $x + y$, we will show that $*$: $\mathrm{Hom}_{\mathfrak{o}}(F, G) \to \mathrm{Hom}_k(F^*, G^*)$ is an injection. From known facts about $\mathrm{Hom}_k(F^*, G^*)$, we will see that this group is a finite module over $\mathbf{Z}_p$, the ring of p-adic integers. Thus $\text{End}_{\mathfrak{o}}(F)$ turns out to be finite over $\mathbf{Z}_p$, and we will show in fact that the degree of the fraction field of $\text{End}_{\mathfrak{o}}(F)$ over $\mathbf{Q}_p$ is bounded by a certain integer (the *height*) which depends only on F^*.

LEMMA 2.1.1. *c: $\text{Hom}_{\mathfrak{o}}(F, G) \to \mathfrak{o}$ is an isomorphism onto a closed subgroup of $\mathfrak{o}$.*

PROOF. We have already seen that c is a homomorphism. Since L, the fraction field of $\mathfrak{o}$, is of characteristic zero, both F and G are isomorphic over L to the additive group law $x + y$, by [11, p. 261]. In other words, there are power series $u, v \in L[[T]]$ with first-degree coefficient non-zero, so that u^{-1} and v^{-1} exist, such that $F(x, y) = u(u^{-1}x + u^{-1}y)$ and $G(x, y) = v(v^{-1}x + v^{-1}y)$. In fact, without loss of generality, we may assume that the first-degree coefficients of u and v are 1.

Substituting into the relation $f(F(x, y)) = G(fx, fy)$ which must hold for any $f \in \text{Hom}_{\mathfrak{o}}(F, G)$, we get

$$(f \circ u)(u^{-1}x + u^{-1}y) = v\big((v^{-1} \circ f)x + (v^{-1} \circ f)y\big)$$

so that

$$(v^{-1} \circ f \circ u)(x + y) = (v^{-1} \circ f \circ u)x + (v^{-1} \circ f \circ u)y ,$$

which means that $v^{-1} \circ f \circ u$ is an additive power series. But the only additive power series in characteristic zero are the linear monomials: $(v^{-1} \circ f \circ u)(T) = aT$ where $a = c(f)$. Now if $c(f) = 0$ then $(v^{-1} \circ f \circ u)(T) = 0$ and thus $f = [0]$, so that c is an injection.

Now we have chosen u and v to be particular power series with coefficients in L such that every $f \in \text{Hom}_{\mathfrak{o}}(F, G)$ is of the form $v \circ (a) \circ u^{-1}$, where $(a)(T) = aT$, and $a = c(f)$. In fact for any $a \in L$, $v \circ (a) \circ u^{-1} \in \text{Hom}_L(F, G)$, with $c(v \circ (a) \circ u^{-1}) = a$. Since $\text{Hom}_{\mathfrak{o}}(F, G) = \text{Hom}_L(F, G) \cap \mathfrak{o}[[T]]$, $v \circ (a) \circ u^{-1}$ is in $\text{Hom}_{\mathfrak{o}}(F, G)$ if and only if it is in $\mathfrak{o}[[T]]$. If we call $b_i(a)$ the i^{th}-degree coefficient of the power series $v \circ (a) \circ u^{-1}$, we see that $b_i(a)$ is a polynomial function of a with coefficients in L, and thus is a continuous function of a. Calling X_i the set of all $a \in \mathfrak{o}$ such that $b_i(a) \in \mathfrak{o}$, X_i is closed in $\mathfrak{o}$ because $\mathfrak{o}$ is closed in L; and the closed set $\bigcap X_i$ is exactly the set of all $a \in \mathfrak{o}$ such that $v \circ (a) \circ u^{-1} \in \mathfrak{o}[[T]]$, so that $c(\text{Hom}_{\mathfrak{o}}(F, G)) = \bigcap X_i$ is closed in $\mathfrak{o}$, q.e.d.

2.1.2. REMARKS. For $n \in \mathbf{Z}$, $c([n]_F) = n$. In fact, we we see as a corollary of Lemma 2.1.1 that it makes sense to speak of $[a]_F$ for any $a \in L$ whatever: $[a]_F$ is *the* L-endomorphism of F whose first-degree coefficient is a. Then we always have $c([a]_F) = a$.

Since $\mathbf{Z}$ is contained in $\text{End}_{\mathfrak{o}}(F)$, its closure $\mathbf{Z}_p$ is contained in $\text{End}\,\mathfrak{o}(F)$: if a is any p-adic integer, $[a]_F \in \text{End}_{\mathfrak{o}}(F)$. Thus we can always regard

$\mathrm{Hom}_{\mathfrak{D}}(F, G)$ as a Z_p-module: if $a \in \mathbf{Z}_p$, and $f \in \mathrm{Hom}_{\mathfrak{D}}(F, G)$, we have $[a]_G \circ f = f \circ [a]_F \in \mathrm{Hom}_{\mathfrak{D}}(F, G)$.

Finally we remark that in the case of an integral domain A of characteristic zero, the first part of the proof of Lemma 2.1.1 shows that c: $\mathrm{Hom}_A(F, G) \rightarrow A$ is an injection.

2.2.0. In this subsection are proved several results on $\mathrm{Hom}_k(F, G)$ for group laws F and G defined over a field k of characteristic $p > 0$. They are all easy consequences or generalizations of facts from [8] and [11].

LEMMA 2.2.1. *If $f \in \mathrm{Hom}_k(F, G)$ and if $f \neq [0]$, there is $q = p^r$ such that $f(T) \equiv aT^q \bmod \deg (q + 1)$, with $a \neq 0$.*

PROOF. Let n be the least degree of a non-zero term of $f(T)$: $f(T) \equiv aT^n \bmod \deg (n + 1)$ with $a \neq 0$. We have

$$f\big(F(x, y)\big) \equiv G(fx, fy) \bmod \deg (n + 1) ,$$

so that $a(x + y)^n \equiv ax^n + ay^n \bmod \deg (n + 1)$, and thus $x^n + y^n = (x + y)^n$ which can happen only if n is a power of p, the characteristic of k, q.e.d.

Lemma 2.2.1 makes possible the following:

DEFINITION 2.2.2. If $[p]_F(T) \equiv aT^q \bmod \deg (q + 1)$ for $a \neq 0$ and $q = p^h$, then h is the *height* of F. If $[p]_F = [0]$, then the height of F is said to be infinite.

2.2.3. If F and G are of unequal heights, then $\mathrm{Hom}_k(F, G) = 0$, because if $f(F(x, y)) = G(fx, fy)$ with $f \neq [0]$, then $f \circ [p]_F = [p]_G \circ f$ which certainly is impossible unless $[p]_F$ and $[p]_G$ are both zero or both have the same leading degree p^h.

On the other hand, if F and G are both of infinite height, they are isomorphic, by [11, Prop. 6]. Lazard's main theorem, [11, Theorem IV], is that over an algebraically closed ground field, any two group laws of the same finite height are isomorphic in the category of group laws over that field: for F and G of the same height $h < \infty$, $\mathrm{Hom}_k(F, G)$ (for K algebraically closed) contains a homomorphism u whose first-degree coefficient is non-zero.

2.2.4. For any field k of characteristic $p > 0$, and any two group laws F and G over k, the topology on $k[[T]]$ induces a topology on $\mathrm{Hom}_k(F, G)$ for which a basis for the open neighborhoods of $[0]$ consists of sets of the form

$$U_{FG}(r) = \{f \in \mathrm{Hom}_k(F, G) \colon f(T) \equiv 0 \bmod \deg r\} .$$

It is clear that $U(r) + U(r) \subset U(r)$ so that $\mathrm{Hom}_k(F, G)$ is a topological group.

Also, it is easily checked that composition of homomorphisms is continuous in both arguments simultaneously. Thus $\mathrm{End}_k(F)$ is a topological ring and $\mathrm{Hom}_k(F, G)$ is a left topological module over $\mathrm{End}_k(G)$. It is clear that

$\mathrm{Hom}_k(F, G)$ is complete.

Now let us suppose that the height of G is $h < \infty$. $\mathrm{End}_k(G)$ certainly has no zero-divisors, so that the homomorphism $n \longrightarrow [n]_G$ of $\mathbf{Z}$ into $\mathrm{End}_k(G)$ must have kernel equal to zero or to $q\mathbf{Z}$ for some prime integer q. But if $q \neq p$, then $[q]_G(T) \equiv qT \bmod \deg 2$, and $q \neq 0$ in k. And the assumption of finiteness of the height of G means that $[p]_G \neq [0]$. Thus $\mathbf{Z}$ is embedded in $\mathrm{End}_k(G)$. Considering $\mathbf{Z}$ as a topological ring with the p-adic topology, this embedding is continuous because $[p^r]_G \circ (\mathrm{End}_k(G)) \subset U_{GG}(p^{rh})$; and since $\mathrm{End}_k(G)$ is complete, the embedding may be extended to the completion of $\mathbf{Z}$, that is, to $\mathbf{Z}_p$. According to Dieudonné [8, Th. 3], for K algebraically closed, $\mathrm{End}_K(G)$ is isomorphic to an order in the central division algebra D_h of rank h^2 over Q_p, of invariant $1/h$. In § 5, we make a computation which shows very simply why this must be the unique maximal order in D_h. $\mathrm{End}_K(G)$ is a free $\mathbf{Z}_p$-module of rank h^2, and so is $\mathrm{Hom}_K(F, G)$ if the height of F is h. But over an arbitrary field k, all we can say about $\mathrm{End}_k(G)$ is that it is isomorphic to an order in a $\mathbf{Q}_p$-division algebra of rank dividing h^2, and that $\mathrm{Hom}_k(F, G)$ is a $\mathbf{Z}_p$-module of rank at most h^2.

2.3.0. We return to the case that F is a group law over the ring $\mathfrak{o}$ (same hypotheses as in 2.0), and under the additional hypothesis that F^* is of finite height h, show that $*$: $\mathrm{Hom}_{\mathfrak{o}}(F, G) \longrightarrow \mathrm{Hom}_k(F^*, G^*)$ is injective. This implies immediately (since the operation of $\mathbf{Z}_p$ on $\mathrm{Hom}_{\mathfrak{o}}(F, G)$ and $\mathrm{Hom}_k(F^*, G^*)$ commutes with reduction modulo $\mathfrak{p}$) that $\mathrm{Hom}_{\mathfrak{o}}(F, G)$ must be of rank $\leqq h^2$ over $\mathbf{Z}_p$. We will see in fact that the rank of $\mathrm{End}_{\mathfrak{o}}(F)$ must be a divisor of h.

It is in this section that we first make essential use of the fact that $\mathfrak{o}$ is discretely valued. The very elementary proof of Lemma 2.3.1 was pointed out to me by Tate; in fact it is possible to show that for F^* of finite height, the reduction map $*$: $\mathrm{End}_{\mathfrak{o}}(F) \longrightarrow \mathrm{End}_k(F^*)$ is an injection even if $\mathfrak{o}$ is not discretely valued, but the proof is much less direct.

LEMMA 2.3.1. $*$: $\mathrm{Hom}_{\mathfrak{o}}(F, G) \longrightarrow \mathrm{Hom}_k(F^*, G^*)$ *is an injection if the height of* F^* *is finite.*

PROOF. Let $f \in \mathrm{Hom}_{\mathfrak{o}}(F, G)$ with $f \neq [0]$. If any coefficient of f is a unit in $\mathfrak{o}$, then $f^* \neq [0]$. Suppose then that no coefficient of f is a unit, so that since $\mathfrak{o}$ is discretely valued, we can write $f(T) = \pi^r g(T)$ where $g(T) \in \mathfrak{o}[[T]]$, $r > 0$, and $g^*(T) \neq 0$. Since f is a homomorphism,

$$\begin{aligned} \pi^r \cdot g(F(x, y)) &= G(\pi^r g(x), \pi^r g(y)) \\ &= \pi^r g(x) + \pi^r g(y) + \pi^{2r} \qquad \text{(power series in } x, y). \end{aligned}$$

Therefore, dividing by π^r and reducing modulo $\mathfrak{p}$, we see that $g^*(F^*(x, y)) = g^*(x) + g^*(y)$, so that g^* is a non-zero homomorphism of F^* into the additive group law $x + y$ which is of infinite height. This is impossible by 2.2.3, so that $f^* \neq [0]$, q.e.d.

It should be noted that if F^* is of infinite height and G^* is of finite height, then $*$ may not be an injection: let $F(x, y) = x + y + bxy$ where $b \in \mathfrak{p}$, and let $G(x, y) = x + y + xy$. The height of G^* is 1. If $f(T) = bT$, then $f \in \operatorname{Hom}_{\mathfrak{o}}(F, G)$ and $f^* = [0]$.

THEOREM 2.3.2. *If the height of F^* is $h < \infty$, then the degree of the fraction field of* $\operatorname{End}_{\mathfrak{o}}(F)$ *over* $\mathbf{Q}_p$ *is a divisor of h.*

PROOF. $\operatorname{End}_{\mathfrak{o}}(F)$ can be considered, because of Lemma 2.3.1, as commutative subring of the central division algebra D_h of rank h^2, invariant $1/h$, over $\mathbf{Q}_p$. Its fraction field is a subfield of D_h which is contained in a maximal subfield of D_h. Any such maximal subfield is of degree h over $\mathbf{Q}_p$, so that the degree of the fraction field of $\operatorname{End}_{\mathfrak{o}}(F)$ over $\mathbf{Q}_p$ must be a divisor of h, q.e.d.

2.3.3. Let $\mathfrak{o}'$ be any complete discrete valuation ring containing all coefficients of F and also the integer rings in all extensions of $\mathbf{Q}_p$ of degree h, and let E be the finite extension of $\mathbf{Z}_p$ which is isomorphic *via* c to $\operatorname{End}_{\mathfrak{o}'}(F)$. Then it follows that for any $\mathfrak{o}$ over which F is defined, $\operatorname{End}_{\mathfrak{o}}(F) \cong E \cap \mathfrak{o}$. This is true because $[a]_F \in \operatorname{End}_{\mathfrak{o}}(F)$ if and only if each coefficient of $[a]_F$ is in $\mathfrak{o}$; and in view of the fact that each coefficient of $[a]_F$ is a polynomial function of a (with coefficients in the fraction field of $\mathfrak{o}$), we see that as long as $a \in \mathfrak{o}$, every coefficient of $[a]_F$ is in $\mathfrak{o}$ if and only if every coefficient of $[a]_F$ is integral. But the set of all a such that each coefficient of $[a]_F$ is integral is exactly E.

There is, therefore, an *absolute* endomorphism ring, isomorphic to E, which is simply $\operatorname{End}_{\mathfrak{o}}(F)$ for sufficiently large $\mathfrak{o}$: in particular, $\mathfrak{o}$ is large enough if its fraction field contains all extensions of $\mathbf{Q}_p$ of degree h. This justifies the notation End (F), by which we mean the *absolute* endomorphism ring of F.

3. A sufficient condition for $\operatorname{End}_{\mathfrak{o}}(F)$ to be integrally closed

3.0. This section contains several technical lemmas on $\operatorname{Hom}_{\mathfrak{o}}(F, G)$ which are proved directly by computation, as well as the theorem that if the coefficients of the terms of F of total degree $\leq p^h$ all lie in an unramified extension of $\mathbf{Z}_p$ (where $h < \infty$ is the height of F^*), then $\operatorname{End}_{\mathfrak{o}}(F)$ is integrally closed in its fraction field.

LEMMA 3.1.1. *Let F and G be group laws defined over $\mathfrak{o}$. Then there exists, for each $i \geqq 2$, a polynomial P_i in $i - 1$ indeterminates, with coefficients in $\mathfrak{o}$, and a polynomial R_i in one indeterminate, with coefficients in L, the fraction field of $\mathfrak{o}$, such that*:

1. $R_i(X) = P_i(X, R_2(X), \cdots, R_{i-1}(X))$ *if i is not a power of p*

2. *$R_i(X) = (1/p)P_i(X, R_2(X), \cdots, R_{i-1}(X))$ if i is a power of p*

3. *If $f \in \mathrm{Hom}_L(F, G)$ and $c(f) = a \in L$, then the coefficient of T^i in $f(T)$ is $R_i(a)$.*

PROOF. Suppose that for each $j < i$, P_j and R_j are defined. In case i is not a p-power, let $i = mq$ where $m > 1$, p is not a factor of m, and q is a power of p. In case i is a p-power, set $m = p$ and again write $i = mq$. Say that $f(T) = a_1T + a_2T^2 + \cdots$, where $f \in \mathrm{Hom}_L(F, G)$. In the equation $f(F(x, y)) = G(fx, fy)$, look at the coefficients of the $x^q y^{(m-1)q}$ terms. In $G(fx, fy)$ this is a polynomial in the a's and the coefficients of G in which a_i does not appear; in $f(F(x, y))$ this coefficient is a polynomial in the a's and the coefficients of F in which a_i appears only to the first power, multiplied by only a binomial coefficient which is a p-unit if m is not divisible by p, and which has p-order exactly one if $m = p$. We equate the coefficients of $x^q y^{(m-1)q}$ in $f(F(x, y))$ and $G(fx, fy)$ and solve for a_i: if i is not a p-power, a_i is a polynomial function of the a_j's ($j < i$), with coefficients from $\mathfrak{o}$; and if i is a p-power, a_i is $1/p$ times a polynomial function of the a_j's ($j < i$). And this gives the construction of P_i, q.e.d.

COROLLARY 3.1.2. *Let $f \in \mathrm{Hom}_L(F, G)$ where F and G are defined over $\mathfrak{o}$. Let $i > 1$ be the least integer such that the i^{th}-degree coefficient a_i of f is not in $\mathfrak{o}$. Then i is a power of p, and $pa_i \in \mathfrak{o}$.*

3.2.1. Following Lazard [11] we make the definitions:

Let n be any integer $\geqq 2$. We define $B_n(x, y)$ to be the form $(x + y)^n - x^n - y^n$, and $C_n(x, y)$ to be the form with integer coefficients defined by:

$C_n = B_n$ if n is not a prime-power,

$C_n = (1/q)B_n$ if n is a power of the prime integer q.

It is easily verified that for each n, the coefficients of C_n are relatively prime, so that for no n is C_n zero when viewed as a form with coefficients in a field. According to [11, Prop. 2], for any commutative ring A with unit, if F and G are abelian group laws over A with $F \equiv G$ mod deg n, then there is $a \in A$ such that $F(x, y) \equiv G(x, y) + aC_n(x, y)$ mod deg $(n + 1)$.

If $f(T_1, \cdots, T_r)$ is a power series with no constant term, and $u(T)$ is a power series whose inverse u^{-1} exists, we define $f^u(T_1, \cdots, T_r)$ to be the power series $u(f(u^{-1}T_1, \cdots, u^{-1}T_r))$. Clearly a necessary and sufficient condition that F and G be isomorphic in the category of group laws over a ring A is that there exist $u(T) \in A[[T]]$ with the first-degree coefficient of u a unit in A, such that $G = F^u$.

Computation shows directly that if $u(T) \equiv T + aT^n$ mod deg $(n + 1)$, then

$F^u(x, y) \equiv F(x, y) + aB_n(x, y) \bmod \deg (n + 1)$.

Finally, if $f(T_1, \cdots, T_r)$ is any power series, the *n-bud of f* is the polynomial consisting of all terms of f of total degree $\leqq n$. Thus the n-bud of f is equal to the n-bud of g if and only if $f \equiv g \bmod \deg (n + 1)$.

LEMMA 3.2.2. *Let F be a group law defined over $\mathfrak{o}$, such that the height of F^* is $h < \infty$, and such that the coefficients of the q-bud of F (where $q = p^h$) all lie in a subring $\mathfrak{u}$ of $\mathfrak{o}$ whose field of fractions is an unramified extension U of $\mathbf{Q}_p$. Then F is isomorphic over $\mathfrak{u}$ (and thus over $\mathfrak{o}$) to a group law G of the form*

$$G(x, y) \equiv x + y + aC_q(x, y) \quad \bmod \deg (q + 1)$$

where a is a unit in $\mathfrak{u}$.

PROOF. We make use of the theorem of Lazard, [11, Lemma 6], that if

$$F^*(x, y) \equiv H^*(x, y) + aC_r(x, y) \quad \bmod \deg (r + 1) \ ,$$

where $a \in k$ and $r = p^s$, then

$$[p]_{F^*}(T) \equiv [p]_{H^*}(T) - aT^r \quad \bmod \deg (r + 1) \ .$$

If it should be impossible to find G isomorphic to F such that $G(x, y) \equiv x + y \bmod \deg q$, then let r be the greatest integer less than $q = p^h$ for which we can find G isomorphic (*via* $u(T) \in \mathfrak{u}[[T]]$) to F, with $G(x, y) \equiv x + y \bmod \deg r$. Then $G(x, y) \equiv x + y + bC_r(x, y) \bmod \deg (r + 1)$, where $b \in \mathfrak{u}$. If r is not a power of p, then $C_r = \beta B_r$ where β is a unit in $\mathbf{Z}_p$ and thus in $\mathfrak{u}$. If we let $u(T) = T - b\beta T^r \in \mathfrak{u}[[T]]$, then $G^u(x, y) \equiv x + y \bmod \deg (r + 1)$, and G^u is isomorphic over $\mathfrak{u}$ to F. If r is a power of p, say $r = p^s$, then b must not be a unit of $\mathfrak{u}$: if it were, we would have $[p]_{G^*}(T) \equiv -b^* T^r \bmod \deg (r + 1)$ so that G^* would be of height $s < h$, which is impossible. Thus b is not a unit, and since U is unramified over $\mathbf{Q}_p$, $b = p\beta$ with $\beta \in \mathfrak{u}$. Again, setting $u(T) = T - \beta T^r \in \mathfrak{u}[[T]]$, we get $G^u(x, y) \equiv x + y \bmod \deg (r + 1)$.

Consequently we can get $G(x, y) \equiv x + y \bmod \deg q$ with $G = F^v$ for some $v(T) \in \mathfrak{u}[[T]]$, and so

$$G(x, y) \equiv x + y + aC_q(x, y) \quad \bmod \deg (q + 1) \ ,$$

with $a \in \mathfrak{u}$. If a were not a unit, we could apply the theorem of Lazard once more to show that $[p]_{G^*}(T) \equiv 0 \bmod \deg (q + 1)$, so that the height of G^* would be greater than h, which is impossible since G^* is isomorphic to F^*, q.e.d.

THEOREM 3.3.1. *If F is a group law defined over $\mathfrak{o}$, such that the height of F^* is $h < \infty$, and if the coefficients of the q-bud of F (where $q = p^h$) all lie in a subring of $\mathfrak{o}$ whose fraction field is an unramified extension of $\mathbf{Q}_p$, then* $\mathrm{End}_{\mathfrak{o}}(F)$ *is integrally closed in its fraction field.*

PROOF. Let us call E the subring of $\mathfrak{o}$ which is isomorphic to $\mathrm{End}_{\mathfrak{o}}(F)$: $E = c(\mathrm{End}_{\mathfrak{o}}(F))$. Let E' be the integral closure of E in its fraction field. Since E and E' are both finite $\mathbf{Z}_p$-modules, of the same rank, E is an open subset of E'. Therefore, $p^r E' \subset E$ for some $r \geqq 1$. Consequently, if E is not integrally closed, there is $a \in \mathfrak{o}$ with $a \notin E$, such that $pa \in E$.

We will show that if $a \in \mathfrak{o}$ and $[a]_F \notin \mathrm{End}_{\mathfrak{o}}(F)$, then $[pa]_F \notin \mathrm{End}_{\mathfrak{o}}(F)$. The idea is as follows: suppose the lowest degree with a non-integral coefficient in $[a]_F(T)$ is $r = p^s$. Then it will turn out that $[pa]_F$ has a non-integral coefficient in degree $qr = p^{h+s}$.

According to Lemma 3.2.2, we may assume that

$$F(x, y) \equiv x + y + \gamma C_q(x, y) \mod \deg (q + 1) ,$$

with γ a unit in $\mathfrak{o}$.

In L, the fraction field of $\mathfrak{o}$, let *ord* be the valuation which is normalized so that $\mathrm{ord}\,(p) = 1$.

Let $a \in \mathfrak{o}$, but $[a]_F \notin \mathrm{End}_{\mathfrak{o}}(F)$. Let $[a]_F(T) = \sum a_i T^i$, where $a_1 = a$. According to Corollary 3.1.2, the first coefficient which is not in $\mathfrak{o}$ must be some a_r where $r = p^s$, and if we set $d = \mathrm{ord}\,(a_r)$, then $-1 \leqq d < 0$.

Let $[p]_F(T) = \sum b_i T^i$, where $b_1 = p$.

It should be observed that since $F(x, y)$ is linear modulo degree q, any F-endomorphism must also be linear modulo degree q, so that in particular,

$$[a]_F(T) = a_1 T + a_q T^q + a_{q+1} T^{q+1} + \cdots ,$$
$$[p]_F(T) = pT + b_q T^q + b_{q+1} T^{q+1} + \cdots .$$

Note also that, since F^* is of height h, b_q is a unit in $\mathfrak{o}$.

We now prove inductively, using the relationship $[p]_F \circ [a]_F = [a]_F \circ [p]_F$ that $\mathrm{ord}\,(a_i) \geqq id/r$ for all $i < qr$.

Suppose this is true for all $j < i$. We look at the T^i-term of $[q]_F \circ [a]_F$ and of $[a]_F \circ [p]_F$:

The T^i-term of $[p]_F \circ [a]_F$ has as coefficient:

$$pa_i + \sum_{j=q}^{i-1} b_j \Phi_j + b_i a_1^i$$

where Φ_j is a sum of monomials in the a's, each of degree j and weight i; by the *weight* of a_m we mean m. Now firstly none of the Φ_j involves a_i. By the inductive hypothesis, since $\mathrm{ord}\,(a_n) \geqq nd/r$, each monomial in Φ_j is of order $\geqq id/r$. But this does not take into account the multinomial coefficients that arise, since these come from $([a]_F(T))^j$. In Φ_q, every monomial is multiplied by a multinomial coefficient which is divisible by p unless the monomial in question is a_j^q, which is integral for $j < r$, and of weight equal to $jq \geqq qr > i$ if $j \geqq r$. Thus the coefficient of b_q is actually of order $\geqq 1 + id/r$.

In Φ_{mq+n}, where $0 \leqq n < q$, any monomial is a product of m monomials of degree q and weight $w_1, w_2, \cdots, w_m$, and a monomial of degree n and weight $i - w_1 - w_2 - \cdots - w_m$. These come, respectively, from the $w_1, \cdots$, and the w_m-degree term of $([a]_F(T))^q$ and the $(i - w_1 - w_2 - \cdots - w_m)$-degree term of $([a]_F(T))^n$. If any w_t-degree term of $([a]_F(T))^q$ has a multinomial coefficient which is divisible by p, the whole monomial must then have order $\geqq 1 + id/r$. If this does not happen, every one of those m monomials is $a_{j_t}^q$ for $j_t < r$ and is thus integral, while since $w_t \geqq q$, $i - w_1 - \cdots - w_m \leqq r - mq = n < q \leqq r$, so that the monomial from $([a]_F(T))^n$ can not contain any a_j for $j \geqq r$, and must be integral too.

Thus in all cases, the order of Φ_j is $\geqq 1 + id/r$, so that the total coefficient of T^i in $[p]_F \circ [a]_F$ is of the form $pa_i + \varphi$, where ord $(\varphi) \geqq 1 + id/r$.

Now we look at the T^i-term of $[a]_F \circ [p]_F$. It is:

$$a_1 b_i + \sum_{j=q}^{i-1} a_j \Theta_j + a_i p^i$$

where each Θ_j is a sum of monomial in the b's, each of degree j and weight i. For $r \leqq j < i$, any such monomial must have at least one factor b_m for $m < q$. (If not, the weight of that monomial would be $>i$.) But the only b_m for $m < q$ is $b_1 = p$. Thus every term here is of order $\geqq 1 + id/r$.

Because of this, $(p - p^i)a_i$ is of order at least $1 + id/r$, since the T^i-coefficients of $([p]_F \circ [a]_F)(T)$ and $([a]_F \circ [p]_F)(T)$ must be equal, and therefore ord $(a_i) \geqq id/r$, as claimed.

A slight modification of the preceding argument, where now we look at the coefficients of T^{qr} in $[p]_F \circ [a]_F$ and $[a]_F \circ [p]_F$, shows that:

$$pa_{qr} + b_q a_r^q + \varphi = \theta + a_{qr} p^{qr}$$

where φ is of order $\geqq qd + 1$ and θ is of order $>qd$, so that ord $(a_{qr}) = qd - 1$, since ord $(a_r) = d$.

The proof will be done when we show that the T^{qr}-term of $([a]_F \circ [p]_F)(T)$ has a non-integral coefficient. This coefficient is

$$a_1 b_{qr} + \sum_{i=q}^{r-1} a_i \Theta_i + a_r(b_q^r + p\Theta_r) + \sum_{i=r+1}^{qr-1} a_i \Theta_i + a_{qr} p^{qr}$$

where each Θ_i is a polynomial in the b's. Now $a_r b_q^r$ is a non-integer: its order is $d < 0$. But everything else is an integer: the only possibilities for non-integers are the terms $a_i \Theta_i$ for which $r < i < qr$. Here, each Θ_i is a sum of monomials in the b's of degree i and weight qr. Now any such monomial has at most $r - 1$ of the b_n's with $n \geqq q$ and thus there will be at least $1 + i - r$ b_n's for which $n < q$; i.e., at least $1 + i - r$ b_1's. Thus the order of any coefficient of a_i is $\geqq 1 + i - r$. Since the order of a_i is $\geqq id/r$, the order of the term involving a_i is at least

$$1 + id/r + i - r = 1 + d + (i - r)(1 + d/r) > 0 .$$

So, $a_r b_q^r$ is indeed the only non-integral quantity in the coefficient of T^{qr} in $([a]_F \circ [p]_F)(T)$, so that $[pa]_F \notin \mathrm{End}_{\mathfrak{o}}(F)$, q.e.d.

COROLLARY 3.3.2. *Under the hypothesis of Theorem* 3.3.1, *the fraction field of* $\mathrm{End}_{\mathfrak{o}}(F)$ *is an unramified extension of* $\mathbf{Q}_p$.

PROOF. We may assume at the outset that F is of the form $F(x, y) \equiv 0 \bmod \deg q$. Then any endomorphism of F must be linear modulo degree q. If the fraction field of $\mathrm{End}_{\mathfrak{o}}(F)$ were ramified over $\mathbf{Q}_p$, there would be endomorphisms f and g of F such that $f \circ g = [p]_F$ and such that $c(f) \in \mathfrak{p}$, $c(g) \in \mathfrak{p}$. But this implies that $f^*(T) \equiv 0 \bmod \deg q$, $g^*(T) \equiv 0 \bmod \deg q$, and consequently $(f^* \circ g^*)(T) \equiv 0 \bmod \deg q^2$, which is impossible since $f^* \circ g^* = [p]_{F^*}$ and $[p]_{F^*}(T) \not\equiv 0 \bmod \deg q^2$, q.e.d.

4. Isomorphisms between group laws

4.0. In this section is proved the main theorem of the paper, which states that, for those group laws whose endomorphism ring is in some sense maximal, the endomorphism ring itself determines the isomorphism class of the group law. This has as an immediate corollary the fact, which has been known to Tate and others for some time, that if F^* is of height one, then F is isomorphic (over a suitably extended ring) to the multiplicative group law $x + y + xy$.

DEFINITION 4.1.1. For any ring A, $A[[T_1, \cdots, T_n]]_r$ is the set of all power series which have non-zero coefficients only in degrees $\equiv 1 \bmod (r - 1)$.

If $f \in A[[T_1, \cdots, T_n]]_r$ and $u \in A[[T]]_r$, where $u^{-1}(T)$ exists, then also $u^{-1} \in A[[T]]_r$, and $f^u \in A[[T_1, \cdots, T_n]]_r$. In fact the rings $A[[T_1, \cdots, T_n]]_r$ are closed under all operations involving composition of power series.

LEMMA 4.1.2. *Let n be an integer which is not divisible by p. Let w be a primitive n^{th} root of unity, with $w \in \mathfrak{o}$. Let $f(T) \in \mathfrak{o}[[T]]$ be such that $f^{(n)}(T) = T$, where by $f^{(n)}$ is meant $f \circ f^{(n-1)}$, $f^{(1)} = f$. Suppose $f(T) \equiv wT$* $\bmod \deg 2$. *Then there is $u(T) \in \mathfrak{o}[[T]]$ such that $u^{-1}(T)$ is in $\mathfrak{o}[[T]]$ and such that $f^u(T) = wT$.*

PROOF. It suffices to show that if $f_m(T) \equiv wT \bmod \deg m$, then there is $u_m(T) \equiv T + aT^m \bmod \deg (m+1)$ such that $u_m(f_m(u_m^{-1}(T))) \equiv wT \bmod \deg (m+1)$, for then, since $\mathfrak{o}[[T]]$ is complete, $\lim (u_m \circ u_{m-1} \circ \cdots \circ u_3 \circ u_2) = u$ exists, and this u is the desired power series.

Suppose $f(T) \equiv wT \bmod \deg m$.

Case 1. $m \not\equiv 1 \bmod n$. If $u(T) = T + bT^m$ and $f(T) \equiv wT + aT^m \bmod \deg (m + 1)$, then

$$f^u(T) \equiv wT + \big(a + b(w^m - w)\big)T^m \mod \deg (m + 1) .$$

$w^m \neq w$, and in fact, since w^* is a primitive n^{th} root of 1 in k, $w^{*m} \neq w^*$, so that $w^m - w$ is a unit in $\mathfrak{o}$. Therefore we can set $b = a(w - w^m)^{-1} \in \mathfrak{o}$ to construct the desired u.

Case 2. $m \equiv 1 \bmod n$. Then $w^m = w$.

Let $f(T) \equiv wT + aT^m \bmod \deg (m + 1)$. It can be checked that:

$$\begin{aligned} f^{(n)}(T) &\equiv w^n T + (w^{n-1} + w^{m+n-2} + \cdots + w^{(n-1)m})aT^m \\ &\equiv T + nw^{-1}aT^m \quad \bmod \deg (m + 1) \ , \end{aligned}$$

so that $a = 0$, and therefore $f(T) \equiv wT \bmod \deg (m + 1)$ already, q.e.d.

As a corollary of Lemma 4.1.2, we have:

PROPOSITION 4.1.3. *Let w be a primitive $(r - 1)^{\text{th}}$ root of* 1 *in $\mathfrak{o}$, where $r = p^s$. Suppose F is a group law defined over $\mathfrak{o}$ such that $[w]_F \in \operatorname{End}_{\mathfrak{o}}(F)$. Then F is isomorphic over $\mathfrak{o}$ to a group law $G(x, y) \in \mathfrak{o}[[x, y]]_r$.*

PROOF. Call $[w]_F = f$. Then f satisfies the hypotheses of Lemma 4.1.2, so that there is an inversible power series $u(T) \in \mathfrak{o}[[T]]$ such that $f^u(T) = wT$. Call $G = F^u$. Then $f^u \in \operatorname{End}_{\mathfrak{o}}(G)$. If $G(x, y)$ were not in $\mathfrak{o}[[x, y]]_r$, there would be a least $m \not\equiv 1 \bmod (r - 1)$ such that $G(x, y)$ had terms of degree m. Say $G \equiv G_1 + H \bmod \deg (m + 1)$ where $G_1(x, y) \in \mathfrak{o}[[x, y]]_r$ and H is a form of degree m. We have:

$$\begin{aligned} wG_1(x, y) + wH(x, y) \equiv wG(x, y) &\equiv f^u\big(G(x, y)\big) \equiv G(f^u x, f^u y) \\ &\equiv G_1(wx, wy) + H(wx, wy) \\ &\equiv wG_1(x, y) + w^m H(x, y) \quad \bmod \deg (m + 1) \ . \end{aligned}$$

Thus $wH = w^m H$, which shows that H must be zero, q.e.d.

The next two lemmas are slight sharpenings of propositions of Lazard. Lemma 4.1.4 corresponds to [11, Lemma 5], and Lemma 4.1.5 corresponds to the final remark on p. 274 of [11].

LEMMA 4.1.4. *Let k be a field of characteristic $p > 0$, and let F be a group law defined over k. Let $f \in \operatorname{End}_k(F)$, such that $f(T) \equiv aT^r$* $\bmod \deg (r + 1)$ *where $r = p^s$ and $a \neq 0$. Then $f(T)$ is actually a power series in T^r.*

PROOF. An examination of Lazard's proof [11, p. 266], which is for $f = [p]_F$, shows that no special properties of the endomorphism f are used other than that its first term is of degree $r = p^s$, q.e.d.

LEMMA 4.1.5. *Let K be an algebraically closed field of characteristic $p > 0$. Suppose that $f(T) \in K[[T]]_r$ where $r = p^s$, that $f(T)$ is actually a power series in T^r, and that $f(T) \equiv aT^r$* $\bmod \deg (r + 1)$ *where $a \neq 0$. Then there is an inversible power series $u(T) \in K[[T]]_r$ such that $f^u(T) = aT^r$.*

PROOF. Again, because of the completeness of $K[[T]]$, we need only show that if f satisfies the hypotheses and if in addition $f(T) \equiv aT^r \bmod \deg m$, then we can find $u(T) \in K[[T]]_r$ with $u(T) \equiv T \bmod \deg j_m$ where $j_m \to \infty$ as $m \to \infty$, such that $f^u(T) \equiv aT^r \bmod \deg (m + 1)$.

Suppose now that $f(T) \equiv aT^r + bT^m \bmod \deg (m + 1)$. The hypotheses imply that if $b \neq 0$, $m \equiv r \bmod (r^2 - r)$; i.e., $m = rn$ with $n \equiv 1 \bmod (r - 1)$. Since $n > 1$, we are looking for $u(T) \equiv T + cT^n \bmod \deg (n + 1)$ such that $f^u(T) \equiv aT^r \bmod \deg (m + 1)$. Thus we take c satisfying $ac^r - a^nc - b = 0$, q.e.d.

4.1.6. REMARK. It is easily seen that once we have $f^u(T) = aT^r$, then by setting $v(T) = \alpha T$ where α is any $(r - 1)^{\text{th}}$ root of a, $f^{v \circ u}(T) = T^r$.

LEMMA 4.2.1. *Let F and G be two group laws defined over the field L of characteristic zero, and let $f(T) \in L[[T]]$ be such that*:

$f(F(x, y)) \equiv F(fx, fy) \bmod \deg n$

$f(G(x, y)) \equiv G(fx, fy) \bmod \deg n$

$c(f) \neq 0$, $c(f) \neq$ *any root of* 1.

Then $F \equiv G \bmod \deg n$.

PROOF. Let $u(T) = T + \cdots$, $v(T) = T + \cdots$ be power series in $L[[T]]$ such that $F^u(x, y) = x + y$, $G^v(x, y) = x + y$. Then f^u and f^v must be linear modulo degree n: $f^u(T) \equiv aT \bmod \deg n$, $f^v(T) \equiv aT \bmod \deg n$ where $a = c(f)$. Thus

$$(v \circ u^{-1})(aT) \equiv v\big(f(u^{-1}T)\big) \equiv a \cdot \big(v \circ u^{-1}(T)\big) \quad \bmod \deg n \ ,$$

so that $v \circ u^{-1}$ is a series which commutes modulo degree n with a linear monomial. But any such series must itself be linear modulo degree n: if $g(T) \equiv bT + dT^r \bmod \deg (r + 1)$ where $r < n$, and $a \cdot g(T) \equiv g(aT) \bmod \deg n$ (and thus $\bmod \deg (r + 1)$), then $abT + adT^r \equiv abT + da^rT^r \bmod \deg (r + 1)$, so that $d(a^r - a) = 0$, which implies that $d = 0$ since $a^r - a$ is non-zero by hypothesis. Therefore $(v \circ u^{-1})(T) \equiv bT \bmod \deg n$ and in fact $b = 1$ because of the way u and v were originally chosen, so that $u \equiv v \bmod \deg n$ and consequently $F \equiv G \bmod \deg n$, q.e.d.

The following definition is made in terms of the *absolute* endomorphism ring End (F) of F defined in 2.3.3.

DEFINITION 4.3.1. Let F be a group law defined over $\mathfrak{o}$ such that F^* is of height $h < \infty$. F is *full* if:

1. End (F) is integrally closed in its fraction field, and
2. End (F) is of rank h over $\mathbf{Z}_p$.

The second condition in the definition implies that the fraction field of End (F) is of degree h over $\mathbf{Q}_p$.

THEOREM 4.3.2. *Let F and G be group laws defined over $\mathfrak{o}$ such that F^* and G^* are of finite height. Suppose that $\mathfrak{o}$ is large enough so that* $\mathrm{End}_{\mathfrak{o}}(F) = \mathrm{End}(F)$ *and* $\mathrm{End}_{\mathfrak{o}}(G) = \mathrm{End}(G)$, *and also that $\mathfrak{o}/\mathfrak{p}$ is algebraically closed. If F and G are full and if* $c(\mathrm{End}(F)) = c(\mathrm{End}(G))$, *then F is isomorphic over $\mathfrak{o}$ to G.*

PROOF. Let the ramification index of $\mathrm{End}(F)$ over $\mathbf{Z}_p$ be e. Let $s = h/e$ where h is the common height of F^* and G^*, and let $r = p^s$. Since s is the residue-class field degree of $\mathrm{End}(F)$ over $\mathbf{Z}_p$, and since $\mathrm{End}(F)$ and $\mathrm{End}(G)$ are integrally closed, there exist $[w]_F \in \mathrm{End}(F)$ and $[w]_G \in \mathrm{End}(G)$ where w is a primitive $(r-1)^{\text{th}}$ root of 1, so that by Proposition 4.1.3, we may assume that $F(x, y)$ and $G(x, y)$ are in $\mathfrak{o}[[x, y]]_r$.

Now let $[a]_F$ be a prime element of $\mathrm{End}(F)$: $a^e = p\alpha$ where α is a unit in $\mathfrak{o}$ such that $[\alpha]_F \in \mathrm{End}(F)$. Certainly $[a]_F(T) \in \mathfrak{o}[[T]]_r$ because $[a]_F(wT) = w \cdot [a]_F(T)$, and so $([a]_F)^*(T) \in k[[T]]_r$. Also, $([a]_F)^*(T) \equiv bT^r \bmod \deg(r+1)$, where $b \neq 0$ in k, since $([p]_F)^*(T)$ has its first non-zero coefficient in degree $p^h = r^e$. Thus, applying Lemma 4.1.5, and 4.1.6, we can find some $u'(T) \in k[[T]]_r$ such that $([a]_F)^{*u'}(T) = T^r$. Then we let $u(T) \in \mathfrak{o}[[T]]_r$ be any power series such that $u^* = u'$, so that $(([a]_F)^u)^*(T) = T^r$. But of course $([a]_F)^u = [a]_{F^u}$. Since we can do the same for G, we have now reduced the problem to the case that F and G are both in $\mathfrak{o}[[T]]_r$, and $([a]_F)^*(T) = ([a]_G)^*(T) = T^r$.

In the remaining part of the proof, we make use of the fact that $p^s - 1$ divides $p^m - 1$ if and only if s divides m, or in other words, that the only powers of p which are $\equiv 1 \bmod (p^s - 1)$ are actually powers of $p^s = r$.

Let us call $[a]_F = f$, $[a]_G = g$, and set

$$f(T) = a_1T + a_rT^r + a_{2r-1}T^{2r-1} + \cdots$$
$$g(T) = b_1T + b_rT^r + b_{2r-1}T^{2r-1} + \cdots$$

where $a_1 = b_1 = a$. We are looking for

$$u(T) = c_1T + c_rT^r + c_{2r-1}T^{2r-1} + \cdots \in \mathfrak{o}[[T]]_r$$

such that $u \circ f = g \circ u$ and such that c_1 is a unit in $\mathfrak{o}$.

For N, a power of r, let $S_N(X_1, X_r, \cdots, X_{Nr})$ be a polynomial in $1 + (Nr - 1)/(r - 1)$ indeterminates, with coefficients from $\mathfrak{o}$, determined in the following way. Let $U(X, T)$ be the power series $X_1T + X_rT^r + \cdots$. The coefficient of T^{Nr} in $(U \circ f)(T)$ is a polynomial $S'_N(X_1, \cdots, X_{Nr})$ with coefficients in $\mathfrak{o}$, as is the coefficient $S''_N(X_1, \cdots, X_{Nr})$ of T^{Nr} in $(g \circ U)(T)$. Then $S_N = S'_N - S''_N$.

At this point we observe that in Lemma 3.1.1, if both F and G are group laws in $\mathfrak{o}[[x, y]]_r$, then since any L-homomorphism $f(T)$ of F into G is necessarily in $L[[T]]_r$, the polynomials R_i which are used to give the i^{th}-degree coefficient of $f(T)$ in terms of its first-degree coefficient have the property that whenever $i \not\equiv 1 \bmod (r - 1)$, $R_i = 0$. Thus we see that for $N \equiv 1 \bmod (r - 1)$, $R_N(X) = P'_N(X, R_r(X), \cdots, R_{N-(r-1)}(X))$ where $P'_N(x_1, x_r, \cdots, x_{N-(r-1)})$ is the polynomial gotten from $P_N(x_1, x_r, \cdots, x_{N-1})$ by substituting zero for all x_i for which $i \not\equiv 1 \bmod (r - 1)$.

Let us call a sequence $(d) = (d_1, d_r, d_{2r-1}, \cdots)$ of elements of $\mathfrak{o}$ an *n-approximant for u* if:

1. For N, not a power of r, $d_N = P'_N(d_1, d_r, \cdots, d_{N-(r-1)})$.
2. For N, a power of r, $S_N(d_1, \cdots, d_{Nr}) \equiv 0 \bmod p^n$.

Let us call an $(n + 1)$-approximant $(d') = (d'_1, d'_r, \cdots)$ a *refinement* of the n-approximant (d) if for each N, $d_N \equiv d'_N \bmod \mathfrak{p}^n$.

To complete the proof, we will now show that there exists a 1-approximant (d) for u with $d_1 = 1$, and that for each n-approximant (d) there is an $(n + 1)$-approximant (d') which is a refinement of (d). Then by completeness of $\mathfrak{o}$, there is a limit sequence (c) such that if N is not a p-power, $c_N = P_N(c_1, \cdots, c_{N-(r-1)})$, and for p-powers N, $S_N(c_1, \cdots, c_{Nr}) = 0$. And, setting $u(T) = c_1T + c_rT^r + \cdots$, we see easily that c_1 is a unit in $\mathfrak{o}$, and $F^u = G$. Indeed, if F^u were not equal to G, we could let N be the greatest integer such that $F^u \equiv G \bmod \deg N$. Then N must be congruent to 1 modulo $r - 1$. If N were not a power of p, then since $c_N = P_N(c_1, \cdots, c_{N-(r-1)})$, we would have, according to Lemma 3.1.1, $u(F(x, y)) \equiv G(ux, uy) \bmod \deg (N + 1)$, and thus $F^u \equiv G \bmod \deg (N + 1)$. On the other hand, if N were a power of p, and thus a power of r, $F^u \equiv G \bmod \deg N$ would imply that $u \circ f \equiv g \circ u \bmod \deg (N + 1)$, and so $f^u \equiv g \bmod \deg (N + 1)$. But by Lemma 4.2.1, since f^u would then be an endomorphism of both F^u and G modulo degree $(N + 1)$ and since $c(f^u) = a$ is not a root of 1, we would have $F^u \equiv G \bmod \deg (N + 1)$, contradicting maximality of N.

We now construct a 1-approximant for u. Let $d_1 = 1$, and for $N = r^m$ let $d_N = 0$, while for $N < i < rN$, let $d_i = P_i(d_1, d_r, \cdots, d_{i-(r-1)})$. We must now show that for $N = r^m$, $S_N(d_1, \cdots, d_{Nr}) \equiv 0 \bmod \mathfrak{p}$. This will be the case if, setting $v(T) = d_1T + d_rT^r + \cdots$, the T^{rN}-terms of $(v \circ f)^*(T)$ and $(g \circ v)^*(T)$ are equal. But $(v \circ f)^*(T) = v^*(T^r)$, and $(g \circ v)^*(T) = (v^*(T))^r$, the T^{rN}-terms of both of which are 1 or 0 according as $N = 1$ or $N > 1$, so that in (d) we do have a 1-approximant for u.

Now suppose that $(d) = (d_1, d_r, d_{2r-1}, \cdots)$ is an n-approximant for u. Since $S_1(d_1, d_r) \equiv 0 \bmod \mathfrak{p}^n$, we have $d_1a_r + d_ra_1^r = b_1d_r + b_rd_1^r + \pi^nz$ for some $z \in \mathfrak{o}$, where π is a prime element of $\mathfrak{p}$; and because a_r is a unit in $\mathfrak{o}$, we can set $d'_1 = d_1 - \pi^nz/a_r$ to get $d'_1a_r + d_ra_1^r \equiv b_1d_r + b_rd_1'^r \bmod \mathfrak{p}^{n+1}$, and this congruence will not be affected if we replace d_r by any d'_r congruent to it modulo $\mathfrak{p}^n$.

Now let $N \equiv 1 \bmod (r-1)$ be a power of p, and let $N > 1$. If $v(T) = d_1T + d_rT^r + d_{2r-1}T^{2r-1} + \cdots$, then the coefficient of T^{rN} in $(v \circ f)(T)$ is $d_N a_r^N + \pi\Gamma(d_1, \cdots, d_{rN})$, where Γ is a polynomial with integral coefficients. Similarly, the coefficient of T^{rN} in $(g \circ v)(T)$ is $b_r d_N^r + \pi\Theta(d_1, \cdots, d_{rN})$, Θ having integral coefficients. Since

$$d_N a_r^N + \pi\Gamma(d_1, \cdots, d_{rN}) = b_r d_N^r + \pi\Theta(d_1, \cdots, d_{rN}) + \pi^n z$$

for some $z \in \mathfrak{o}$, if we let $d'_N = d_N - \pi^n z / a_r^N$, then

$$d'_N a_r^N + \pi\Gamma(d_1, \cdots, d'_N, \cdots, d_{rN}) \equiv b_r d'^r_N + \pi\Theta(d_1, \cdots, d'_N, \cdots, d_{rN}) \mod \mathfrak{p}^n$$

and this congruence is not affected if we substitute d'_i for d_i $(i \neq N)$ if $d'_i \equiv d_i \bmod \mathfrak{p}^n$. Defining $d'_i = P_i(d'_1, \cdots, d'_{i-(r-1)})$ for i not a power of p, we automatically have $d'_i \equiv d_i \bmod \mathfrak{p}^n$. (d') is clearly an $(n+1)$-approximant for u, and it is a refinement of (d), q.e.d.

COROLLARY 4.3.3. *If F is a group law defined over $\mathfrak{o}$, where $k = \mathfrak{o}/\mathfrak{p}$ is algebraically closed, and if F^* is of height one, then F is isomorphic over $\mathfrak{o}$ to the multiplicative group law $x + y + xy$.*

PROOF. Certainly $x + y + xy$ is of height one. The endomorphism rings of $F(x, y)$ and $x + y + xy$ must contain $\mathbf{Z}_p$, but can be no larger, since they are contained in an extension of $\mathbf{Q}_p$ of degree one. Therefore both $F(x, y)$ and $x + y + xy$ are full, and are consequently isomorphic over $\mathfrak{o}$.

5. Examples, counter-examples, conjectures

5.0. In this section we give a construction that shows that there are full formal Lie groups with all possible endomorphism rings: if $\mathfrak{o}$ is the ring of integers of an extension L of $\mathbf{Q}_p$ of finite degree n, then there is a group law $F(x, y) \in \mathfrak{o}[[x, y]]$ such that End $(F) \cong \mathfrak{o}$, and F^* is of height n. Also, in the second part of this section, we show that not every group law is full; and then finally we put forth some conjectures, all prompted by the similarity that this theory bears to the theory of elliptic curves.

LEMMA 5.1.1. *Let $\mathfrak{o}$ be the ring of integers in a finite extension L of $\mathbf{Q}_p$, whose residue-class field degree is s, and whose ramification index is e. Let π be a prime element of $\mathfrak{o}$, so that* ord $(\pi) = 1/e$, *and let $F(x, y) \in \mathfrak{o}[[x, y]]_q$ be a group law, where $q = p^s$. If $[\pi]_F(T) = \sum b_i T^i$ and b_r is the first non-integral coefficient, then* ord $(b_r) \geqq (1 - e)/e$.

PROOF. Calling $\mathfrak{u}$ the ring of integers in the maximal unramified extension of $\mathbf{Q}_p$ contained in L, $\mathfrak{u}$ is isomorphic, via c^{-1}, to a subring of $\text{End}_{\mathfrak{o}}(F)$, because $c(\text{End}_{\mathfrak{o}}(F))$ certainly contains all $(q-1)^{\text{th}}$ roots of 1. Thus if $e = 1$ the

Lemma is certainly true, and we can assume from now on that $e > 1$. Now $\mathfrak{o} = \mathfrak{u} + \pi\mathfrak{u} + \cdots + \pi^{e-1}\mathfrak{u}$ so that $p/\pi = a_0 + \pi a_1 + \cdots + \pi^{e-1}a_{e-1}$ with $a_i \in \mathfrak{u}$. Consequently if $[p/\pi]_F(T) = \sum \gamma_i T^i$, we have $\gamma_i \in \mathfrak{o}$ for $i < r$.

The power series $[\pi]_F$ and $[p/\pi]_F$ have the property that when composed in either order, the resulting power series, $[p]_F$, has all its coefficients in $\mathfrak{o}$.

First let us look at the r-degree term of $[\pi]_F \circ [p/\pi]_F$: since $b_1 = \pi$, its coefficient is $\pi\gamma_r + \lambda + b_r(p/\pi)^r \in \mathfrak{o}$, where $\lambda \in \mathfrak{o}$. Now $r \geqq 2$, and ord $(b_r(p/\pi)^r) \geqq -1 + r(e-1)/e$, so that $b_r(p/\pi)^r \in \mathfrak{o}$. Therefore ord $(\gamma_r) \geqq -1/e$. On the other hand, the r-degree coefficient in $[p/\pi]_F \circ [\pi]_F$ is $(p/\pi)b_r + \mu + \gamma_r\pi^r \in \mathfrak{o}$, where $\mu \in \mathfrak{o}$, and thus $(p/\pi)b_r \in \mathfrak{o}$, q.e.d.

THEOREM 5.1.2. *Let $\mathfrak{o}$ be the ring of integers in a finite extension L of $\mathbf{Q}_p$, whose residue-class field degree is s and whose ramification index is e. Let $\mathfrak{O}$ be the ring of integers in the unramified extension of L of degree t. Then there is a full group law $F(x, y) \in \mathfrak{o}[[x, y]]$ such that* End $(F) \cong \mathfrak{O}$. *Furthermore, the construction can be done in such a way that if π is a prime element of $\mathfrak{o}$, $([\pi]_F)^*(T) = T^q$, where $q = p^{st}$.*

PROOF. We make use of the theorem of Lazard [11, Th. III] that if $F_1(x, y)$ is an *associative n-bud*, i.e., if $F_1(x, y)$ is a polynomial of degree n such that $F_1(x, y) \equiv x + y \bmod \deg (n + 1)$, $F_1(x, y) = F_1(y, x)$, and $F_1(F_1(x, y), z) \equiv F_1(x, F_1(y, z)) \bmod \deg (n + 1)$, then there is a group law F, defined over the same ring as F_1, such that $F \equiv F_1 \bmod \deg (n + 1)$. In case $F_1(x, y) \in \mathfrak{o}[[x, y]]_m$, $F(x, y)$ can also be taken to be in $\mathfrak{o}[[x, y]]_m$, because of the fact that if F_1 is associative modulo degree $(n + 1)$ where $n \equiv 1 \bmod (m - 1)$, and if $F_1(x, y) \in \mathfrak{o}[[x, y]]_m$, then F_1 is automatically associative modulo degree $(n + m - 1)$.

Now consider $F_1(x, y) = x + y + p(\pi^q - \pi)^{-1}C_q(x, y)$ and $f_1(T) = \pi T + T^q$. F_1 is associative modulo degree $(q+1)$, and $F_1(f_1x, f_1y) \equiv f_1(F_1(x, y)) \bmod \deg (q+1)$. Since $\pi \in \mathfrak{o}$, and ord $(\pi^q - \pi) = 1/e \leqq 1 =$ ord (p), $p(\pi^q - \pi)^{-1} \in \mathfrak{o}$ also. Now we show that F_1 and f_1 can be completed to a group law F and an F-endomorphism $f = [\pi]_F$ with coefficients in $\mathfrak{o}$. We now complete F_1 in any way to a group law $F(x, y) \in \mathfrak{o}[[x, y]]_q$, and call $f(T) = \sum b_i T^i = [\pi]_F(T)$. If $f(T) \in \mathfrak{o}[[T]]$, we are done. If not, let b_r be the first non-integral coefficient. $b_r \in L$, and ord $(b_r) \geqq (1 - e)/e$, by Lemma 5.1.1.

Let $\varphi(T) = T + b_r(\pi - \pi^r)^{-1}T^r$. Then $f^\varphi(T) = \varphi(f(\varphi^{-1}T)) \equiv f(T) - b_rT^r \bmod \deg (r + 1)$, while

$$\begin{aligned} F^\varphi(x, y) &\equiv F(x, y) + b_r(\pi - \pi^r)^{-1}B_r(x, y) \\ &\equiv F(x, y) + pb_r(\pi - \pi^r)^{-1}C_r(c, y) \quad \bmod \deg (r + 1) \end{aligned}$$

because r is a power of p. If we call F_2 the r-bud of F^φ and f_2 the r-bud of

f^φ, then F_2 is associative modulo degree $(r + 1)$ and f_2 is an endomorphism of F_2 modulo degree $(r + 1)$. Since F_2 and f_2 now have integral coefficients, we can continue inductively, getting in the limit a group law F for which $[\pi]_F$ has integral coefficients and such that $F(x, y) \in \mathfrak{o}[[x, y]]_q$.

$\operatorname{End}_{\mathfrak{O}}(F)$ certainly has a subring isomorphic to $\mathfrak{O}$ because $[w]_F \in \operatorname{End}_{\mathfrak{O}}(F)$ for any $(q - 1)^{\text{th}}$ root w of 1, and by our construction $[\pi]_F \in \operatorname{End}_{\mathfrak{O}}(F)$. $\mathfrak{O}$ is the ring of integers in an extension of $\mathbf{Q}_p$ of degree *est*, and once we show that the height of F^* is *est*, Theorem 2.3.2 will imply that $c(\operatorname{End}(F))$ can be no larger than $\mathfrak{O}$, and so equals $\mathfrak{O}$, so that F is full.

$\pi^e = pa$ for some unit $a \in \mathfrak{o}$, so that $[p]_F = [a^{-1}]_F \circ ([\pi]_F)^{(e)}$; and since $([\pi]_F)^{*(e)}(T) \equiv T^r \bmod \deg (r + 1)$ where $r = q^e = p^{est}$,

$$\begin{aligned}[p]_{F^*}(T) &\equiv ([a^{-1}]_F)^*(T^r)\\ &\equiv a^{*-1}T^r \mod \deg (r + 1)\end{aligned}$$

and so F^* is of height *est*, as desired.

By taking a little more care we can construct a group law $F'(x, y) \in \mathfrak{o}[[x, y]]_q$ such that $[\pi]_{F'}(T) \in \mathfrak{o}[[T]]$ and such that $([\pi]_{F'})^*(T) = T^q$. Take the group law F constructed above, and let $f(T) = [\pi]_F(T) = \sum b_i T^i$. If for every $\rho > q$ we have $b_\rho \in \mathfrak{p}$, then let $F' = F$. If some b_ρ is a unit, consider $\gamma(T) = -T^q$. γ is an endomorphism of F^* because the coefficients of F^* all lie in the finite field with q elements, and in case $p \neq 2$ the only nonzero coefficients of F are in odd degrees. Call μ the F^*-endomorphism $\gamma + f^*$. $\mu(T) \equiv b_\rho^* T^\rho \bmod \deg (\rho + 1)$ so that ρ is a power of p by Lemma 2.2.1. But just as before we can modify F by $\varphi(T) = T + b_\rho(\pi - \pi^\rho)^{-1}T^\rho$ to get a polynomial F_2 which is the ρ-bud of F^φ and f_2 which is the ρ-bud of f^φ. Then we complete these as in the previous construction to a group law F_2' and an F_2'-endomorphism f_2' which has the property that $f_2'^*(T) \equiv T^q \bmod \deg (\rho + 1)$. So we continue inductively and get in the limit a group law F' of the desired sort, q.e.d.

5.1.3. By taking $\mathfrak{o} = \mathbf{Z}_p$ and $t = h$, $\pi = p$, we get a group law F defined over $\mathbf{Z}_p$ such that the height of F^* is h, and such that $\operatorname{End}(F)$ is isomorphic to the unramified extension $\mathfrak{u}_h$ of $\mathbf{Z}_p$ of degree h. This ring is injected by $*$ into $\operatorname{End}_K(F^*)$ where K is the algebraic closure of $\mathbf{Z}/p\mathbf{Z}$, the field over which F^* is defined. $\varphi(T) = T^p$ is a K-endomorphism of F^*, and $\varphi^{(h)} = [p]_{F^*}$. We know by [8, Th. 3] that $\operatorname{End}_K(F^*)$ is isomorphic to an order in the central division algebra D_h of rank h^2 over $\mathbf{Q}_p$, and invariant $1/h$. But the maximal order in D_h is characterized by the existence of a subring $\mathfrak{U}$ isomorphic to $\mathfrak{u}_h$ and an h^{th} root π of p, such that for $a \in \mathfrak{U}$, $\pi a = a^\sigma \pi$ where σ is the Frobenius automorphism of $\mathfrak{U}$ over $\mathbf{Q}_p$. But it is easily verified that if $b \in \mathfrak{u}$ and $[b]_F(T) =$

$\sum b_i T^i$, then $([b^\sigma]_F)^*(T) = \sum b_i^{*p} T^i$ which shows that $\varphi \circ ([b]_F)^* = ([b^\sigma]_F)^* \circ \varphi$. Thus $\mathrm{End}_K(F^*)$ is isomorphic to the maximal order in D_h.

5.2.1. It is easy enough to construct group laws F for which F^* is of finite height h, but $\mathrm{End}\,(F) \cong \mathbf{Z}_p$. For example, apply Theorem 5.1.2 with $\mathfrak{o} = \mathbf{Z}_p$, $t = h$, to get a full group law $F'(x, y) \in \mathbf{Z}_p[[x, y]]_q$ where $q = p^h$. Let $r = p^{h+1}$, and let F_1 be the polynomial of degree r such that

$$F_1(x, y) \equiv F'(x, y) + C_r(x, y) \mod \deg (r + 1)\ .$$

Since F_1 is associative modulo degree $(r + 1)$, we can complete it to a group law $F(x, y) \in \mathbf{Z}_p[[x, y]]$. Since $[p]_F(T) \equiv pT + Tq \mod \deg (q + 1)$, F^* is of height h. Now $\mathrm{End}\,(F)$ is integrally closed in its fraction field, by Theorem 3.3.1, so to show that $\mathrm{End}\,(F) \cong \mathbf{Z}_p$, it is sufficient to show that there are no $(p^s - 1)^{\text{th}}$ roots of 1 in $c(\mathrm{End}\,(F))$ for $s > 1$, and no $\pi \in c(\mathrm{End}\,(F))$ for which $\pi^e = pa$ where $e > 1$ and a is a unit in $c(\mathrm{End}\,(F))$. There are no roots of 1 in $c(\mathrm{End}\,(F))$ because of the occurrence of the C_r term in F; and since any endomorphism of F must be linear modulo degree q, $([\pi]_F)^*(T) \equiv 0 \mod \deg q$ which is impossible if $\pi^e = pa$.

5.3.1. Let us call F and G *isogenous over* $\mathfrak{o}$ if neither $\mathrm{Hom}_{\mathfrak{o}}(F, G)$ nor $\mathrm{Hom}_{\mathfrak{o}}(G, F)$ is zero. This is clearly an equivalence relation. Let us call F *almost full* if $c(\mathrm{End}\,(F))$ is an order in an extension of $\mathbf{Q}_p$ of degree h, where h is the height of F^*. We make the following conjecture:

If F and G are almost full, and if $c(\mathrm{End}\,(F))$ *and* $c(\mathrm{End}\,(G))$ *are orders in the same extension of* $\mathbf{Q}_p$, *then F is isogenous to G over a sufficiently large ground ring* $\mathfrak{o}$.

This would be the exact analogue of the fact that two elliptic curves, whose endomorphism rings are isomorphic to orders in the same quadratic number field, are isogenous.

5.3.2. We can also ask, if R is an order in a finite extension of $\mathbf{Q}_p$, whether there is always a group law F such that $R = c(\mathrm{End}\,(F))$.

BOWDOIN COLLEGE

BIBLIOGRAPHY

1. M. DEURING, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg, 14 (1941), 197-272.
2. J. DIEUDONNÉ, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique* $p > 0$, Comment. Math. Helv., 28 (1954), 87-118.
3. ———, *Lie groups and Lie hyperalgebras over a field of characteristic* $p > 0$: II, Amer. J. Math., 77 (1955), 218-244.
4. ———, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique* $p > 0$: III, Math. Z., 63 (1955), 53-75.
5. ———, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$: IV, Amer.

J. Math., 77 (1955), 429-452.

6. ————, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$*: V, Bull. Soc. Math. France, 84 (1956), 207-239.
7. ————, *Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$*: VI, Amer. J. Math., 79 (1957), 331-388.
8. ————, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$*: VII, Math. Ann. 134 (1957), 114-133.
9. ————, *Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$*: VIII, Amer. J. Math., 80 (1958), 740-772.
10. M. LAZARD, *La non-existence des groupes de Lie formels non-abéliens à un paramètre*, C. R. Acad. Sci. Paris, 239 (1954), 942-945.
11. ————, *Sur les groupes de Lie formels à un paramètre*, Bull. Soc. Math. France, 83 (1955), 251-274.

(Received November 5, 1963)