APPENDIX A2

Formal Group Laws

In this appendix we will give a self-contained account of the relevant aspects of the theory of commutative one-dimensional formal group laws. This theory was developed by various algebraists for reasons having nothing to do with algebraic topology. The bridge between the two subjects is the famous result of Quillen [**2**] (4.1.6) which asserts that the Lazard ring L (A2.1.8) over which the universal formal group law is defined is naturally isomorphic to the complex cobordism ring. A most thorough and helpful treatment of this subject is given in Hazewinkel [**1**]. An account of the Lazard ring is also given in Adams [**5**], while the classification in characteristic p can also be found in Fröhlich [**1**].

We now outline the main results of Section 1. We define formal group laws (A2.1.1) and homomorphisms between them (A2.1.5) and show that over a field of characteristic 0 every formal group law is isomorphic to the additive one (A2.1.6). The universal formal group law is constructed (A2.1.8) and the structure of the ring L over which it is defined is determined (A2.1.10). This result is originally due to Lazard [**1**]. Its proof depends on a difficult lemma (A2.1.12) whose proof is postponed to the end of the section.

Then we define p-typical formal group laws (A2.1.17 and A2.1.22) and determine the structure of the p-typical analog of the Lazard ring, V (A2.1.24). This result is due to Carrier [**1**]; Quillen [**2**] showed that V is naturally isomorphic to $\pi^*(BP)$ (4.1.12). Using a point of view due to Landweber [**1**], we determine the structure of algebraic objects LB (A2.1.16) and VT (A2.1.26), which turn out to be isomorphic to $MU_*(MU)$ (4.1.11) and $BP_*(BP)$ (4.1.19), respectively.

All of the results of this section can be found in Adams [**5**], although our treatment of it differs from his.

In Section 2 we give the explicit generators of V [i.e., of $\pi_*(BP)$] given by Hazewinkel [**2**] (A2.2.1) and Araki [**1**] (A2.2.2) and determine the behavior of the right unit η_R on Araki's generators (A2.2.5).

For the Morava theory of Chapter 6 we will need the classification of formal group laws over separably closed fields of characteristic $p > 0$ (A2.2.11) originally due to Lazard [**2**], and a description of the relevant endomorphism rings (A2.2.17 and A2.2.18) originally due to Dieudonné [**1**] and Lubin [**1**].

For a scheme theoretic approach to this subject, see Strickland [**1**].

1. Universal Formal Group Laws and Strict Isomorphisms

A2.1.1. DEFINITION. *Let R be a commutative ring with unit. A* formal group law *over R is a power series $F(x, y) \in R[[x, y]]$ satisfying*

(i) $F(x, 0) = F(0, x) = x$,

(ii) $F(x, y) = F(y, x)$, *and*

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

Strictly speaking, such an object should be called a commutative one-dimensional formal group law; we omit the first two adjectives as this is the only type of formal group law we will consider. It is known (Lazard [**3**]) that (ii) is redundant if R has no nilpotent elements.

The reason for this terminology is as follows. Suppose G is a one-dimensional commutative Lie group and $g\colon \mathbf{R} \to U \subset G$ is a homomorphism to a neighborhood U of the identity which sends 0 to the identity. Then the group operation $G \times G \to G$ can be described locally by a real-valued function of two real variables. If the group is analytic then this function has a power series expansion about the origin that satisfies (i)–(iii). These three conditions correspond, respectively, to the identity, commutativity, and associativity axioms of the group. In terms of the power series, the existence of an inverse is automatic, i.e.,

A2.1.2. PROPOSITION. *If F is a formal group law over R then there is a power series $i(x) \in R[[x]]$ (called the* formal inverse*) such that $F(x, i(x)) = 0$.*

In the Lie group case this power series must of course converge, but in the formal theory convergence does not concern us. Formal group laws arise in more algebraic situations; e.g., one can extract a formal group law from an elliptic curve defined over R; see Chapter 7 of Silverman [**1**]. One can also reverse the procedure and get a group out of a formal group law; if R is a complete local ring then $F(x,y)$ will converge whenever x and y are in the maximal ideal, so a group structure is defined on the latter which may differ from the usual additive one.

Before proceeding further note that A2.1.1(i) implies

A2.1.3. PROPOSITION. *If F is a formal group law then*

$$F(x,y) \equiv x + y \mod (x,y)^2. \qquad \square$$

A2.1.4. EXAMPLES OF FORMAL GROUP LOWS. (a) $F_a(x,y) = x + y$, the additive formal group law.

(b) $F(x,y) = x + y + uxy$ (where u is a unit in R), the multiplicative formal group law, so named because $1 + uF = (1+ux)(1+uy)$.

(c) $F(x,y) = (x+y)/(1+xy)$.

(d) $F(x,y) = (x\sqrt{1-y^4} + y\sqrt{1-x^4})/(1+x^2y^2)$, a formal group law over $\mathbf{Z}[1/2]$.

The last example is due to Euler and is the addition formula for the elliptic integral

$$\int_0^x \frac{dt}{\sqrt{1-t^4}}$$

(see Siegel [**1**, pp. 1-9]). These examples will be studied further below (A2.2.9).

The astute reader will recognize (c) as the addition formula for the hyperbolic tangent function; i.e., if $x = \tanh(u)$ and $y = \tanh(v)$ then $F(x,y) = \tanh(u+v)$. Hence we have

$$\tanh^{-1}(F(x,y)) = \tanh^{-1}(x) + \tanh^{-1}(y)$$

or

$$F(x,y) = \tanh(\tanh^{-1}(x) + \tanh^{-1}(y)),$$

where $\tanh^{-1}(x) = \sum_{i\ge 0} x^{2i+1}/(2i+1) \in R \otimes \mathbf{Q}[[x]]$.

We have a similar situation in (b), i.e.,

$$\log(1+uF) = \log(1+ux) + \log(1+uy),$$

where $\log(l + ux) = \sum_{i>0}(-1)^{i+1}(ux)^i/i \in R \otimes \mathbf{Q}[[x]]$.

This means that the formal group laws of (b) and (c) are isomorphic over $\mathbf{Q}$ to the additive formal group law (a) in the following sense.

A2.1.5. DEFINITION. *Let F and G be formal group laws. A* homomorphism *from F to G is a power series $f(x) \in R[[x]]$ with constant term 0 such that $f(F(x,y)) = G(f(x), f(y))$. It is an* isomorphism *if it is invertible, i.e., if $f'(0)$ (the coefficient of x) is a unit in R, and a* strict isomorphism *if $f'(0) = 1$. A strict isomorphism from F to the addition formal group law $x + y$ is a logarithm for F, denoted by $\log_F(x)$.*

Hence the logarithms for A2.1.4(b) and (c) are

$$\sum_{i>0} \frac{(-u)^{i-1}x^i}{i} \qquad \text{and} \qquad \tanh^{-1}(x)$$

respectively.

On the other hand, these formal group laws are not isomorphic to the additive one over $\mathbf{Z}$. To see this for (b), set $u = 1$. Then $F(x,x) = 2x + x^2 \equiv x^2 \mod 2$, while $F_a(x,x) = 2x \equiv 0 \mod 2$, so the two formal group laws are not isomorphic over $\mathbf{Z}/(2)$. The formal group law of (c) is isomorphic to F_a over $\mathbf{Z}_{(2)}$, since its logarithm $\tanh^{-1} x$ has coefficients in $\mathbf{Z}_{(2)}$, but we have $F(F(x,x),x) = (3x+x^3)/(1+3x^2) \equiv x^3 \mod (3)$ while $F_a(F_a(x,x),x) = 3x \equiv 0 \mod 3$. Similarly, it can be shown that F and F_a are distinct at every odd prime (see A2.2.9).

A2.1.6. THEOREM. *Let F be a formal group law and let $f(x) \in R \otimes \mathbf{Q}[[x]]$ be given by*

$$f(x) = \int_0^x \frac{dt}{F_2(t,0)}$$

where $F_2(x,y) = \partial F/\partial y$. Then f is a logarithm for F, i.e., $F(x,y) = f^{-1}(f(x) + f(y))$, and F is isomorphic over $R \otimes \mathbf{Q}$ to the additive formal group law.

PROOF. Let $w = f(F(x,y)) - f(x) - f(y)$. We wish to show $w = 0$. We have $F(F(x,y),z) = F(x, F(y,z))$. Differentiating with respect to z and setting $z = 0$ we get

$$F_2(F(x,y),0) = F_2(x,y)F_2(y,0). \tag{A2.1.7}$$

On the other hand, we have $\partial w/\partial y = f'(F(x,y))F_2(y,0) - f'(y)$, which by the definition of f becomes

$$\frac{\partial w}{\partial y} = \frac{F_2(x,y)}{F_2(F(x,y),0)} - \frac{1}{F_2(y,0)} = 0 \quad \text{by A2.1.7.}$$

By symmetry we also have $\partial w/\partial x = 0$, so w is a constant. But f and F both have trivial constant terms, so $w = 0$. □

Now we wish to consider the universal formal group law. Its construction is easy.

A2.1.8. THEOREM. *There is a ring L (called the Lazard ring) and a formal group law*

$$F(x,y) = \sum a_{i,j}x^iy^j$$

defined over it such that for any formal group law G over any commutative ring with unit R there is a unique ring homomorphism $\theta\colon L \to R$ such that $G(x,y) = \sum \theta(a_{i,j})x^i y^j$.

PROOF. Simply set $L = \mathbf{Z}[a_{i,j}]/I$, where I is the ideal generated by the relations among the $a_{i,j}$ required by the definition A2.1.1, i.e., by $a_{1,0}-1$, $a_{0,1}-1$, $a_{i,0}$, and $a_{0,i}$ for (i), $a_{i,j}-a_{ji}$ for (ii), and b_{ijk} for (iii), where

$$F(F(x,y),z) - F(x,F(y,z)) = \sum b_{ijk}x^i y^j z^k.$$

Then θ can be defined by the equation it is supposed to satisfy. $\square$

Determining the structure of L explicitly is more difficult. At this point it is convenient to introduce a grading on L by setting $|a_{i,j}| = 2(i+j-1)$. Note that if we have $|x| = |y| = -2$ then $F(x,y)$ is a homogeneous expression of degree -2.

A2.1.9. LEMMA. (a) *$L \otimes \mathbf{Q} = \mathbf{Q}[m_1, m_2, \dots]$ with $|m_i| = 2i$ and $F(x,y) = f^{-1}(f(x)+f(y))$ where $f(x) = x + \sum_{i>0} m_i x^{i+1}$.*

(b) *Let $M \subset L \otimes \mathbf{Q}$ be $\mathbf{Z}[m_1, m_2, \dots]$. Then $\operatorname{im} L \subset M$.*

PROOF. (a) By A2.1.6 every formal group law G over a $\mathbf{Q}$-algebra R has a logarithm $g(x)$ so there is a unique $\phi\colon \mathbf{Q}[m_1 m_2, \dots] \to R$ such that $\phi(f(x)) = g(x)$. In particular we have $\phi\colon \mathbf{Q}[m_1, m_2, \dots] \to L \otimes \mathbf{Q}$ as well as $\theta\colon L \otimes \mathbf{Q} \to \mathbf{Q}[m_1, m_2, \dots]$ with $\theta\phi$ and $\phi\theta$ being identity maps, so θ and ϕ are isomorphisms.

(b) $F(x,y)$ is a power series with coefficients in M, so the map from L to $L \otimes \mathbf{Q}$ factors through M. $\square$

Now recall that if R is a graded connected ring (e.g., $L \otimes \mathbf{Q}$) the group of indecomposables QR is I/I^2 where $I \subset R$ is the ideal of elements of positive degree.

A2.1.10. THEOREM (Lazard [**1**]). (a) *$L = \mathbf{Z}[x_1, x_2, \dots]$ with $|x_i| = 2i$ for $i > 0$.*

(b) *x_i can be chosen so that its image in $QL \otimes \mathbf{Q}$ is*

$$\begin{cases} pm_i & \text{if } i = p^k - 1 \text{ for some prime } p \\ m_i & \text{otherwise.} \end{cases} \qquad \square$$

(c) *L is a subring of M* [A2.1.9(b)].

The proof of this is not easy and we will postpone the hardest part of it (A2.1.12) to the end of this section. The difficulty is in effect showing that L is torsion-free. Without proving A2.1.12 we can determine L/torsion with relative ease. We will not give F in terms of the x_i, nor will the latter be given explicitly. Such formulas can be found, however, in Hazewinkel [**3**] and in Section 5 of Hazewinkel [**1**].

Before stating the hard lemma we need the following exercise in binomial coefficients.

A2.1.11. PROPOSITION. *Let u_n be the greatest common divisor of the numbers $\binom{n}{i}$ for $0 < i < n$. Then*

$$u_n = \begin{cases} p & \text{if } n = p^k \text{ for some prime } p \\ 1 & \text{otherwise.} \end{cases} \qquad \square$$

Now we are ready for the hard lemma. Define homogeneous symmetric polynomials $B_n(x,y)$ and $C_n(x,y)$ of degree n for all $n > 0$ by

$$B_n(x,y) = (x+y)^n - x^n - y^n$$
$$C_n(x,y) = \begin{cases} B_n/p & \text{if } n = p^k \text{ for some prime } p \\ B_n & \text{otherwise.} \end{cases}$$

It follows from A2.1.11 that $C_n(x,y)$ is integral and that it is not divisible by any integer greater than one.

A2.1.12. Comparison Lemma (Lazard [**1**]). *Let F and G be two formal group laws over R such that $F \equiv G \mod (x,y)^n$. Then $F \equiv G + aC_n \mod (x,y)^{n+1}$ for some $a \in R$.* □

The proof for general R will be given at the end of this section. For now we give a proof for torsion-free R.

In this case we lose no information by passing to $R\otimes\mathbf{Q}$, where we know (A2.1.6) that both formal group laws have logarithms, say $f(x)$ and $g(x)$, respectively. Computing mod $(x,y)^{n+1}$ we have

$$f(x) \equiv g(x) + bx^n \quad \text{for some } b \in R\otimes\mathbf{Q} \quad \text{so} \quad f^{-1}(x) = g^{-1}(x) - bx^n$$

and

$$\begin{aligned} F - G &= f^{-1}(f(x)+f(y)) - g^{-1}(g(x)+g(y)) \\ &\equiv g^{-1}(g(x)+g(y)+b(x^n+y^n)) - b(x+y)^n - g^{-1}(g(x)+g(y)) \\ &\equiv g^{-1}(g(x)+g(y)) + b(x^n+y^n) - b(x+y)^n - g^{-1}(g(x)+g(y)) \\ &\equiv -bB_n(x,y). \end{aligned}$$

Since this must lie in R it must have the form $aC_n(x,y)$, completing the proof for torsion-free R.

A2.1.13. Lemma. (a) *In $QL\otimes\mathbf{Q}$, $a_{i,j} = -\binom{i+j}{j} m_{i+j-1}$.*
(b) *QL is torsion-free.*

Proof. (a) Over $L\otimes\mathbf{Q}$ we have $\sum m_{n-1}(\sum a_{i,j}x^iy^j)^n = \sum m_{n-1}(x^n+y^n)$. Using A2.1.3 to pass to $QL\otimes\mathbf{Q}$ we get

$$\sum a_{i,j}x^iy^j + \sum_{n>1} m_{n-1}(x+y)^n = \sum_{n>0} m_{n-1}(x^n+y^n),$$

which gives the desired formula.

(b) Let $Q_{2n}L$ denote the component of QL in degree $2n$, and let R be the graded ring $\mathbf{Z}\oplus Q_{2n}L$. Let F be the formal group law over R induced by the obvious map $\theta\colon L\to R$, and let G be the additive formal group law over R. Then by A2.1.12, $F(x,y) \equiv x + y + aC_{n+1}(x,y)$ for $a \in Q_{2n}L$. It follows that $Q_{2n}L$ is a cyclic group generated by a. By (a) $Q_{2n}L\otimes\mathbf{Q} = \mathbf{Q}$, so $\mathbf{Q}_{2n}L = \mathbf{Z}$ and QL is torsion-free. □

It follows from the above that L is generated by elements x_i whose images in $QL\otimes\mathbf{Q}$ are u_im_i, where u_i is as in A2.1.11, i.e., that L is a quotient of $\mathbf{Z}[x_i]$. By A2.1.9 it is the quotient by the trivial ideal, so A2.1.10 is proved.

Note that having A2.1.12 for torsion-free R implies that L/torsion is as claimed.

The reader familiar with Quillen's theorem (4.1.6) will recognize L as $\pi_*(MU) = MU_*$. We will now define an object which is canonically isomorphic to $\pi_*(MU \wedge MU) = MU_*(MU)$. This description of the latter is due to Landweber [**1**].

A2.1.14. DEFINITION. *Let R be a commutative ring with unit. Then $FGL(R)$ is the set of formal group laws over R* (A2.1.1) *and $SI(R)$ is the set of triples (F, f, G) where $F, G \in FGL(R)$ and $f\colon F \to G$ is a strict isomorphism* (A2.1.5)*, i.e., $f(x) \in R[[x]]$ with $f(0) = 0$, $f'(0) = 1$, and $f(F(x, y)) = G(f(x), f(y))$. We call such a triple a* matched pair

A2.1.15. PROPOSITION. *$FGL(-)$ and $SI(-)$ are covariant functors on the category of commutative rings with unit. $FGL(-)$ is represented by the Lazard ring L and $SI(-)$ is represented by the ring $LB = L \otimes \mathbf{Z}[b_1, b_2, \dots]$. In the grading introduced above, $|b_i| = 2i$.*

PROOF. All but the last statement are obvious. Note that a matched pair (F, f, G) is determined by F and f and that f can be any power series of the form $f(x) = x + \sum_{i>0} f_i x^{i+1}$. Hence such objects are in 1-1 correspondence with ring homomorphisms $\theta\colon LB \to R$ with $\theta(b_i) = f_i$. □

Now LB has some additional structure which we wish to describe. Note that $FGL(R)$ and $SI(R)$ are the sets of objects and morphisms, respectively, of a groupoid, i.e., a small category in which every morphism is an equivalence. Hence these functors come equipped with certain natural transformations reflecting this structure. The most complicated is the one corresponding to composition of morphisms, which gives a natural (in R) map from a certain subset of $SI(R) \times SI(R)$ to $SI(R)$. This structure also endows (L, LB) with the structure of a Hopf algebroid (A1.1.1). Indeed that term was invented by Haynes Miller with this example in mind. We now describe this structure.

A2.1.16. THEOREM. *In the Hopf algebroid (L, LB) defined above $\varepsilon\colon LB \to L$ is defined by $\varepsilon(b_i) = 0$; $\eta_L\colon L \to LB$ is the standard inclusion while $\eta_R\colon L \otimes \mathbf{Q} \to LB \otimes \mathbf{Q}$ is given by*

$$\sum_{i \geq 0} \eta_R(m_i) = \sum_{i \geq 0} m_i \left(\sum_{j \geq 0} c(b_j) \right)^{i+1},$$

where $m_0 = b_0 = 1$; $\sum_{i \geq 0} \Delta(b_i) = \sum_{j \geq 0} (\sum_{i \geq 0} b_i)^{j+1} \otimes b_j$; and $c\colon LB \to LB$ is determined by $c(m_i) = \eta_R(m_i)$ and $\sum_{i \geq 0} c(b_i) \left(\sum_{j \geq 0} b_j \right)^{i+1} = 1$.

These are the structure formulas for $MU_*(MU)$ (4.1.11).

PROOF. ε and η_L are obvious. For c, if $f(x) = \sum b_i x^{i+1}$ then $f^{-1}(x) = \sum c(b_i) x^{i+1}$. Expanding $f^{-1}(f(1)) = 1$ gives the formula for $c(b_i)$. For η_R, let $\log x = \sum m_i x^{i+1}$ and $\operatorname{mog} x = \sum \eta_R(m_i) x^{i+1}$ be the logarithms for F and G, respectively. Then we have

$$f^{-1}(G(x, y)) = F(f^{-1}(x), f^{-1}(y))$$

so

$$\log(f^{-1}(G(x, y))) = \log(f^{-1}(x)) + \log(f^{-1}(y)).$$

We also have

$$\operatorname{mog}(G(x, y)) = \operatorname{mog}(x) + \operatorname{mog}(y)$$

for which we deduce

$$\operatorname{mog}(x) = \log f^{-1}(x).$$

Setting $x = 1$ gives the formula for η_R. For Δ let $f_1(x) = b_i' x^{i+1}$, $f_2(x) = \sum b_i'' x^{i+1}$, and $f(x) = f_2(f_1(x))$. Then expanding and setting $x = 1$ gives $\sum b_i = \sum b_i''(\sum b_j')^{i+1}$. Since f_2 follows f_1 this gives the formula for Δ. □

Note that (L, LB) is split (Al.1.22) since Δ defines a Hopf algebra structure on $B = \mathbf{Z}[b_i]$.

Next we will show how the theory simplifies when we localize at a prime p, and this will lead us to BP_* and $BP_*(BP)$.

A2.1.17. DEFINITION. *A formal group law over a torsion-free $\mathbf{Z}_{(p)}$-algebra is* p-typical *if its logarithm has the form $\sum_{i\geq 0} \ell_i x^{p^i}$ with $\ell_0 = 1$.*

Later (A2.1.22) we will give a form of this definition which works even when the $\mathbf{Z}_{(p)}$-algebra R has torsion. Assuming this can be done, we have

A2.1.18. THEOREM (Cartier [**1**]). *Every formal group law over a $\mathbf{Z}_{(p)}$-algebra is canonically strictly isomorphic to a p-typical one.*

Actually A2.1.17 is adequate for proving the theorem because it suffices to show that the universal formal group law is isomorphic over $L \otimes \mathbf{Z}_{(p)}$ to a p-typical one.

The following notation will be used repeatedly.

A2.1.19. DEFINITION. *Let F be a formal group law over R. If x and y are elements in an R-algebra A which also contains the power series $F(x, y)$, let*

$$x +_F y = F(x, y).$$

This notation may be iterated, e.g., $x +_F y +_F z = F(F(x, y), z)$. Similarly, $x -_F y = F(x, i(y))$ (A2.1.2). For nonnegative integers n, $[n]_F(x) = F(x, [n-1]_F(x))$ with $[0]_F(x) = 0$. (The subscript F will be omitted whenever possible.) $\sum^F(\ )$ will denote the formal sum of the indicated elements.

A2.1.20. PROPOSITION. *If the formal group law F above is defined over a K-algebra R where K is asubring of $\mathbf{Q}$, then for each $r \in K$ there is a unique power series $[r]_F(x)$ such that*

(a) *if r is a nonnegative integer, $[r]_F(x)$ is the power series defined above,*
(b) *$[r_1 + r_2]_F(x) = F([r_1]_F(x), [r_2]_F(x))$,*
(c) *$[r_1 r_2]_F(x) = [r_1]_F([r_2]_F(x))$.*

PROOF. Let $[-1]_F(x) = i(x)$ (A2.1.2), so $[r]_F(x)$ is defined by (b) for all $r \in \mathbf{Z}$. We have $[r]_F(x) \equiv rx \mod (x^2)$, so if $d \in \mathbf{Z}$ is invertible in K, the power series $[d]_F(x)$ is invertible and we can define $[d^{-1}]_F(x) = [d]_F^{-1}(x)$. □

Now we suppose q is a natural number which is invertible in R. Let

$$f_q(x) = [1/q]\left(\sum_{i=1}^{q}{}^F \zeta^i x\right) \tag{A2.1.21}$$

where ζ is a primitive qth root of unity. A priori this is a power series over $R[\zeta]$, but since it is symmetric in the ζ^i it is actually defined over R.

If R is torsion-free and $\log(x) = \sum_{i\geq 0} m_i x^{i+1}$, we have

$$\begin{aligned}\log(f_q(x)) &= \frac{1}{q}\sum_{i=1}^{q}\log(\zeta^i x)\\ &= \frac{1}{q}\sum_{i=1}^{q}\sum_{j\geq 0} m_j x^{j+1}\zeta^{i(j+1)}\\ &= \frac{1}{q}\sum_{j\geq 0} m_j x^{j+1}\sum_{i=1}^{q}\zeta^{i(j+1)}.\end{aligned}$$

The expression $\sum_{i=1}^{q}\zeta^{i(j+1)}$ vanishes unless $(j+1)$ is divisible by q, in which case its value is q. Hence, we have

$$\log(f_q(x)) = \sum_{j>0} m_{qj-1}x^{qj}.$$

If F is p-typical for $p \neq q$, this expression vanishes, so we make

A2.1.22. Definition. *A formal group law F over a $\mathbf{Z}_{(p)}$-algebra is* p-typical *if $f_q(x) = 0$ for all primes $q \neq p$.*

Clearly this is equivalent to our earlier definition A2.1.17 for torsion-free R.

To prove Cartier's theorem (A2.1.18) we claim that it suffices to construct a strict isomorphism $f(x) = \sum f_i x^i \in L\otimes\mathbf{Z}_{(p)}[[x]]$ from the image of F over $L\otimes\mathbf{Z}_{(p)}$ to a p-typical formal group law F'. Then if G is a formal group law over a $\mathbf{Z}_{(p)}$-algebra R induced by a homomorphism $\theta\colon L\otimes\mathbf{Z}_{(p)} \to R$, $g(x) = \sum\theta(f_i)x^i \in R[[x]]$ is a strict isomorphism from G to a p-typical formal group law G'.

Recall that if $\operatorname{mog}(x)$ is the logarithm for F' then

$$\operatorname{mog}(x) = \log(f^{-1}(x)).$$

We want to use the $f_q(x)$ for various primes $q \neq p$ to concoct an $f^{-1}(x)$ such that

$$\log(f^{-1}(x)) = \sum_{i\geq 0} m_{p^i-1}x^{p^i}.$$

It would not do to set

$$f^{-1}(x) = x -_F \sum_{q\neq p}^{F} f_q(x)$$

because if n is a product of two or more primes $\neq p$ then a negative multiple of $M_{n-1}x^n$ would appear in $\log f^{-1}(x)$. What we need is the Möbius function $\mu(n)$ defined on natural numbers n by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by a square}\\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes.}\end{cases}$$

Note that $\mu(1) = 1$ and $\mu(q) = -1$ if q is prime. Then we define $f(x)$ by

$$f^{-1}(x) = \sum_{p\nmid q}^{F}[\mu(q)]_F(f_q(x)). \tag{A2.1.23}$$

[Note also that $f_1(x) = x$.] The sum is over all natural numbers q not divisible by p. This infinite formal sum is well defined because $f_q(x) \equiv 0 \mod (x^q)$.

Now

$$\log(f^{-1}(x)) = \sum_{p\nmid q} \mu(q) \sum_{j>0} m_{qj-1} x^{qj} = \sum_{n>0} \left(\sum_{\substack{p\nmid q\\ q|n}} \mu(q) \right) m_{n-1} x^n.$$

It is elementary to verify that

$$\sum_{\substack{p\nmid q\\ q|n}} \mu(q) = \begin{cases} 1 & \text{if } n = p^k \\ 0 & \text{otherwise.} \end{cases}$$

It follows that F' has logarithm

$$\operatorname{mog}(x) = \sum_{i\ge 0} m_{p^i-1} x^{p^i}, \tag{A2.1.24}$$

so F' is p-typical. This completes the proof of A2.1.18.

Now we will construct the universal p-typical formal group law.

A2.1.25. THEOREM. *Let $V = \mathbf{Z}_{(p)}[v_1, v_2, \dots]$ with $|v_n| = 2(p^n - 1)$. Then there is a universal p-typical formal group law F defined over V; i.e., for any p-typical formal group law G over a commutative $\mathbf{Z}_{(p)}$-algebra R, there is a unique ring homomorphism $\theta\colon V \to R$ such that $G(x, y) = \theta(F(x, y))$. Moreover the homomorphism from $L \otimes \mathbf{Z}_{(p)}$ to V corresponding* (A2.1.8) *to this formal group law is surjective, i.e., V is isomorphic to a direct summand $L \otimes \mathbf{Z}_{(p)}$.* □

We will give an explicit formula for the v_n's in terms of the log coefficients m_{p^n-1} below (A2.2.2). In 4.1.12 it is shown that V is canonically isomorphic to $\pi_*(BP)$.

PROOF. Recall that the canonical isomorphism f above corresponds to an endomorphism ϕ of $L \otimes \mathbf{Z}_{(p)}$ given by

$$\phi(m_i) = \begin{cases} m_i & \text{if } i = p^k - 1 \\ 0 & \text{otherwise.} \end{cases}$$

This ϕ is idempotent, i.e., $\phi^2 = \phi$ and its image is a subring $V \subset L \otimes \mathbf{Z}_{(p)}$ over which the universal p-typical formal group law is defined. An argument similar to the proof of Lazard's theorem A2.1.9 shows that V has the indicated structure. □

Now we will construct a ring VT canonically isomorphic to $BP_*(BP)$ and representing the set of p-typical matched pairs (F, f, G) (A2.1.14), i.e., matched pairs with F and G p-typical. The power series f must be chosen carefully to ensure that G is p-typical, and this choice depends on F. There is no such thing as a "p-typical power series," i.e., one that sends any p-typical F to a p-typical G. To characterize the appropriate f we have

A2.1.26. LEMMA. *Let F be a p-typical formal group law over a $\mathbf{Z}_{(p)}$-algebra R. Let $f(x)$ be an isomorphism* (A2.1.5) *from F to a formal group law G. Then G is p-typical if*

$$f^{-1}(x) = \sum_{i\ge 0}{}^{F} t_i x^{p^i}$$

for $t_i \in R$ with t_0 a unit in R.

PROOF. For a prime number $\neq p$ let

$$h_q(x) = [q^{-1}]_G\left(\sum_{i=1}^{q}{}^{G} \zeta^i x\right)$$

where ζ is a primitive pth root of unity. By A2.1.22 we need to show that $h_q(x) = 0$ for all $q \neq p$ iff f is as specified. From the relation

$$G(x,y) = f(F(f^{-1}(x), f^{-1}(y)))$$

we deduce

$$f^{-1}(h_q(x)) = [q^{-1}]_F\left(\sum_{j=1}^{q}{}^{F} f^{-1}(\zeta^j x)\right).$$

Now for isomorphism $f(x)$ there are unique $c_i \in R$ such that

$$f^{-1}(x) = \sum F_{i>0} c_i x^i$$

with c_1 a unit in R. Hence we have

$$\begin{aligned} f^{-1}(h_q(x)) &= [q^{-1}]_F\left(\sum_{i,j}{}^{F} c_i\zeta^{ij}x^i\right) \\ &= [q^{-1}]_F\left(\sum_{q\nmid i}{}^{F}\sum_{j}{}^{F} \zeta^j c_i x^i\right) +_F [q^{-1}] +_F \left(\sum_{i}{}^{F}[q]_F(c_{qi}x^{qi})\right) \\ &= \sum_{q\nmid i}{}^{F} f_q(c_i x^i) +_F \sum_{i}{}^{F} c_{qi}x^{qi} = \sum_{i>0} c_{qi}x^{qi}. \end{aligned}$$

This expression vanishes for all $q \neq p$ iff $c_{qi} = 0$ for all $i > 0$ and $q \neq p$, i.e., iff f is as specified. □

It follows immediately that $VT = V \otimes \mathbf{Z}_{(p)}[t_1, t_2, \dots]$ as a ring since for a strict isomorphism $t_0 = 1$. The rings V and VT represent the sets of objects and morphisms in the groupoid of strict isomorphisms of p-typical formal group laws over a $\mathbf{Z}_{(p)}$-algebra. Hence (V, VT), like (L, LB), is a Hopf algebroid (Al.1.1) and it is isomorphic to $(BP_*, BP_*(BP))$. Its structure is as follows.

A2.1.27. THEOREM. *In the Hopf algebroid* (V, VT) (*see* A1.1.1)
(a) $V = \mathbf{Z}_{(p)}[v_1, v_2, \dots]$ *with* $|v_n| = 2(p^n - 1)$,
(b) $VT = V \otimes \mathbf{Z}_{(p)}[t_1, t_2, \dots]$ *with* $|t_n| = 2(p^n - 1)$, *and*
(c) $\eta_L\colon V \to VT$ *is the standard inclusion and* $\varepsilon\colon VT \to V$ *is defined by* $\varepsilon(t_i) = 0$, $\varepsilon(v_i) = v_i$.
Let $\ell_i \in V \otimes \mathbf{Q}$ *denote the image of* $m_{p^i-1} \in L \otimes \mathbf{Q}$ (*see* A2.1.9). *Then*
(d) $\eta_R\colon V \to VT$ *is determined by* $\eta_R(\ell_n) = \sum_{0\le i\le n} \ell_i t_{n-i}^{p^i}$ *where* $\ell_0 = t_0 = 1$,
(e) Δ *is determined by* $\sum_{i,j\ge 0} \ell_i \Delta(t_j)^{p^i} = \sum_{i,k,j\ge 0} \ell_i t_j^{p^i} \otimes t_k^{p^{i+j}}$, *and*
(f) c *is determined by* $\sum_{i,j,k\ge 0} \ell_i t_j^{p^i} c(t_k)^{p^{i+j}} = \sum_{i\ge 0} \ell_i$.
(g) *The forgetful functor from p-typical formal group laws to formal group laws induces a surjection of Hopf algebroids* (Al.1.19) $(L\otimes\mathbf{Z}_{(p)}, LB\otimes\mathbf{Z}_{(p)}) \to (V, VT)$.

Note that (e) and (f) are equivalent to

$$\sum_{i\ge 0}{}^{F} \Delta(t_i) = \sum_{i,j\ge 0}{}^{F} t_i \otimes t_j^{p^i} \quad\text{and}\quad \sum_{i,j\ge 0}{}^{F} t_i c(t_j)^{p^i} = 1,$$

respectively.

It can be shown that unlike (L, LB) (A2.1.16), (V, VT) is not split (A1.1.22).

PROOF. Part (a) was proved in A2.1.23, (b) follows from A2.1.23, and (c) is obvious, as is (g).

For (d) let f be a strict isomorphism between p-typical formal group law F and G with logarithms $\log(x)$ and $\mathrm{mog}(x)$, respectively. If $f(x)$ satisfies

$$f^{-1}(x) = \sum_{i\geq 0}^{F} t_i x^{p^i}$$

and

$$\log(x) = \sum_{i\geq 0} \ell_i x^{p^i}$$

then by definition of η_R

$$\mathrm{mog}(x) = \sum_{i\geq 0} \eta_R(\ell_i) x^{p^i}.$$

We have (see the proof of A2.1.16)

$$\begin{aligned}\mathrm{mog}(x) = \log(f^{-1}(x)) &= \log\left(\sum_{i\geq 0}^{F} t_i x^{p^i}\right)\\ &= \sum_{i\geq 0} \log(t_i x^{p^i}) = \sum_{i,j\geq 0} \ell_i t_j^{p^i} x^{p^{i+j}}\end{aligned}$$

and (d) follows.

For (e) let $F \xrightarrow{f_1} G \xrightarrow{f_2} H$ be strict isomorphisms of p-typical formal group laws with

$$f_1^{-1}(x) = \sum_{i\geq 0}^{F} t_i' x^{p^i} \quad \text{and} \quad f_2^{-1}(x) = \sum_{j\geq 0}^{G} t_j'' x^{p^j}.$$

If we set $f = f_2 \circ f_1$, with

$$f^{-1}(x) = \sum_{i\geq 0}^{F} t_i x^{p^i}$$

then a formula for t_i in terms of t_i' and t_i'' will translate to a formula for $\Delta(t_i)$.

We have

$$\begin{aligned}f^{-1}(x) = f_1^{-1}(f_2^{-1}(x)) &= f_1^{-1}\left(\sum_{j\geq 0}^{G} t_j'' x^{p^j}\right)\\ &= \sum_{j}^{F} f_1^{-1}(t_j'' x^{p^j}) = \sum_{i,j}^{F} t_i'(t_j'' x^{p^j})^{p^i}.\end{aligned}$$

This gives

$$\sum_{i}^{F} \Delta(t_i) = \sum_{i,j}^{F} t_i \otimes t_j^{p^i}$$

as claimed.

For (f) let $f\colon F \to G$ be as above. Then

$$f(x) = \sum^{G} c(t_j) x^{p^j}$$

so

$$
\begin{aligned}
x = f^-1(f(x)) &= f^{-1}\left(\sum_j^G c(t_j)x^{p^j} \right) \\
&= \sum_j^F f^{-1}(c(t_j)x^{p^j}) = \sum_{i,j}^F t_i(c(t_j)x^{p^j})^{p^i}
\end{aligned}
$$

setting $x = 1$ gives (f). □

Our only remaining task is to prove Lazard's comparison lemma A2.1.12. The proof below is due to Fröhlich [**1**]. The lemma states that if F and G are formal group laws with $F \equiv G \mod (x, y)^n$ then

$$F \equiv G + aC_n(x, y) \mod (x, y)^{n+1},$$

where

$$C_n(x, y) = \begin{cases} \dfrac{(x + y)^n - x^n - y^n}{p} & \text{if } n = p^k \text{ for some prime } p \\ (x + y)^n - x^n - y^n & \text{otherwise.} \end{cases}$$

Let $\Gamma(x, y)$ be the degree n component of $F - G$.

A2.1.28. LEMMA. *$\Gamma(x, y)$ above is a homogeneous polynomial satisfying*
(i) $\Gamma(x, y) = \Gamma(y, x)$,
(ii) $\Gamma(x, 0) = \Gamma(0, x) = 0$,
(iii) $\Gamma(x, y) + \Gamma(x + y, z) = \Gamma(x, y + z) + \Gamma(y, z)$.

PROOF. Parts (i) and (ii) follow immediately A2.1.1(ii) and (i), respectively. For (iii) let $G(x, y) = x + y + G'(x, y)$. Then mod $(x, y, z)^{n+1}$ we have

$$
\begin{aligned}
F(F(x, y), z) &\equiv G(F(x, y), z) + \Gamma(F(x, y), z) \\
&\equiv F(x, y) + z + G'(F(x, y), z) + \Gamma(x + y, z) \\
&\equiv G(x, y) + \Gamma(x, y) + z + G'(G(x, y), z) + \Gamma(x + y, z) \\
&\equiv G(G(x, y), z) + \Gamma(x, y) + \Gamma(x + y, z).
\end{aligned}
$$

Similarly,

$$F(x, F(y, z)) = G(x, G(y, z)) + \Gamma(x, y + z) + \Gamma(y, z)$$

from which (iii) follows. □

It suffices to show that any such Γ must be a multiple of C_n.

A2.1.29. LEMMA. *Let R be a field of characteristic $p > 0$. Then any $\Gamma(x, y)$ over R as above is a multiple of $C_n(x, y)$.*

PROOF. It is easy to verify that C_n satisfies the conditions of A2.1.28, so it suffices to show that the set of all such Γ is one-dimensional vector space. Let $\Gamma(x, y) = \sum a_i x^i y^{n-i}$. Then from A2.1.28 we have

$$a_0 = a_n = 0, \quad a_i = a_{n-i},$$

and

$$a_i \binom{n-i}{j} = a_{i+j} \binom{i+j}{j} \quad \text{for } 0 < i, i + j < n. \tag{A2.1.30}$$

The case $n = 1$ is trivial so we write $n = sp^k$ with either $s = p$ or $s > 1$ and $s \not\equiv 0 \mod p$. We will prove the lemma by showing $a_i = 0$ if $i \not\equiv 0 \mod (p^k)$ and that a_{cp^k} is a fixed multiple of a_{p^k}.

If $i \not\equiv 0 \mod (p^k)$ we can assume by symmetry that $i < (s-1)p^k$ and write $i = cp^k - j$ with $0 < c < s$ and $0 < j < p^k$. Then A2.1.30 gives

$$a_i \binom{(s-c)p^k + j}{j} = a_{cp^k} \binom{cp^k}{j},$$

i.e., $a_i = 0$.

To show a_{cp^k} is determined by a_{p^k} for $c < s$ let $i = p^k$ and $j = (c-1)p^k$. Then A2.1.30 gives

$$a_{p^k} \binom{(s-1)p^k}{(c-1)p^k} = a_{cp^k} \binom{cp^k}{(c-1)p^k},$$

i.e.,

$$a_{p^k} \binom{s-1}{c-1} = a_{cp^k} c.$$

This determines a_{cp^k} provided $c \not\equiv 0 \mod (p)$. Since $c < s$ we are done for the case $s = p$. Otherwise $a_{cp^k} = a_{(s-c)p^k}$ by symmetry and since $s \not\equiv 0 \mod (p)$ either c or $s - c$ is $\not\equiv 0 \mod (p)$. $\square$

Note that A2.1.29 is also true for fields of characteristic 0; this can be deduced immediately from A2.1.30. Alternatively, we have already proved A2.1.12, which is equivalent to A2.1.29, for torsion-free rings.

The proof of A2.1.29 is the last hard computation we have to do. Now we will prove the analogous statement for $R = \mathbf{Z}/(p^m)$ by induction on m. We have

$$\Gamma(x, y) = aC_n(x, y) + p^{m-1}\Gamma'(x, y),$$

where Γ' satisfies A2.1.28 mod p. Hence by A2.1.29 $\Gamma'(x, y) = bC_n(x, y)$ so

$$\Gamma(x, y) = (a + bp^{m-1})C_n(x, y)$$

as claimed.

To prove A2.1.29 (and hence A2.1.12) for general R note that the key ingredient A2.1.30 involves only the additive structure of R; i.e., we only have to compute in a finitely generated abelian group A containing the coefficient of Γ. We have to show that symmetry and A2.1.30 imply that the coefficients a_i are fixed in relation to each other as are the coefficients of C_n. We have shown that this is true for $A = Z$ (from the case $R = \mathbf{Q}$) and $A = \mathbf{Z}/(p^m)$. It is clear that if it is true for groups A_1 and A_2 then it is true for $A_1 \oplus A_2$, so it is true for all finitely generated abelian groups A. This completes the proof of A2.1.12.

2. Classification and Endomorphism Rings

In order to proceed further we need an explicit choice of the generators v_n. The first such choice was given by Hazewinkel [**2**], which was circulating in preprint form six years before it was published. The same generators for $p = 2$ were defined earlier still by Liulevicius [**3**]. A second choice, which we will use, was given by Araki [**1**].

Hazewinkel's generators are defined by

(A2.2.1) $$p\ell_n = \sum_{0 \le i < n} \ell_i v_{n-i}^{p^i}$$

which gives, for example,

$$\ell_1 = \frac{v_1}{p}, \qquad \ell_2 = \frac{v_2}{p} + \frac{v_1^{1+p}}{p^2},$$
$$\ell_3 = \frac{v_3}{p} + \frac{v_1 v_2^p + v_2 v_1^{p^2}}{p^2} + \frac{v_1^{1+p+p^2}}{p^3}.$$

Of course, it is nontrivial to prove that these v_n are contained in and generate V.

Araki's formula is nearly identical,

$$p\ell_n = \sum_{0\le i\le n} \ell_i v_{n-i}^{p^i} \tag{A2.2.2}$$

where $v_0 = p$. These v_n can be shown to agree with Hazewinkel's mod (p). They give messier formulas for ℓ_n, e.g.,

$$\ell_1 = \frac{v_1}{p-p^p}, \quad (p-p^{p^2})\ell_2 = v_2 + \frac{v_1^{1+p}}{p-p^p},$$
$$(p-p^{p^3})\ell_3 = v_3 + \frac{v_1 v_2^p}{p-p^p} + \frac{v_2 v_1^{p^2}}{p-p^{p^2}} + \frac{v_1^{1+p+p^2}}{(p-p^p)(p-p^{p^2})},$$

but a nicer formula (A2.2.5) for η_R.

A2.2.3. THEOREM (Hazewinkel [**2**], Araki [**1**]). *The sets of elements defined by* A2.2.1 *and* A2.2.2 *are contained in and generate V as a ring, and they are congruent* mod (p).

PROOF. We first show that Araki's elements generate V. Equation A2.2.2 yields

$$\sum_{i\ge 0} p\ell_i x^{p^i} = \sum_{i,j\ge 0} \ell_i v_j^{p^i} x^{p^{i+j}}.$$

Applying exp (the inverse of log) to both sides gives

$$[p]_F(x) = \sum_{i\ge 0}{}^F v_i x^{p^i}, \tag{A2.2.4}$$

which proves the integrality of the v_n, i.e., that $v_n \in V$. To show that they generate V it suffices by A2.1.10 to show $v_n = pu_n\ell_n$ in $QV \otimes \mathbf{Q}$, where u_n is a unit in $\mathbf{Z}_{(p)}$. Reducing A2.2.2 modulo decomposables gives

$$p\ell_n = v_n + \ell_n p^{p^n}$$

so the result follows.

We now denote Hazewinkel's generators of A2.2.1 by w_i. Then A2.2.1 gives

$$p \log x - px = \sum_{i>0} \log w_i x^{p^i}$$

or

$$px = p\log x - \sum_{i>0} \log w_i x^{p^i}.$$

Exponentiating both sides gives

$$\begin{aligned}\exp px &= [p](x) -_F \sum_{i>0}^F w_i x^{p^i}\\ &= px +_F \sum_{i>0}^F v_i x^{p^i} -_F \sum_{i>0}^F w_i x^{p^i} \text{ by A2.2.4.}\end{aligned}$$

If we can show that $(\exp px)/p$ is integral then the above equation will give

$$\sum_{i>0}^F v_i x^{p^i} \equiv \sum_{i>0}^F w_i x^{p^i} \mod (p)$$

and hence $v_i \equiv w_i \mod (p)$ as desired.

To show that $(\exp px)/p$ is integral simply note that its formal inverse is $(\log px)/p = \sum \ell_i p^{p^i-1} x^{p^i}$, which is integral since $p^i \ell_i$ is. □

From now on v_n will denote the Araki generator defined by A2.2.2 or equivalently by A2.2.4. The following formula for $\eta_R(v_n)$ first appeared in Ravenel [**1**], where it was stated mod (p) in terms of the Hazewinkel generators; see also Moreira [**2**].

A2.2.5. THEOREM. *The behavior of η_R on v_n is defined by*

$$\sum_{i,j\geq 0}^F t_i \eta_R(v_j)^{p^i} = \sum_{i,j\geq 0}^F v_i t_j^{p^i}.$$

PROOF. Applying η_R to A2.2.2 and reindexing we get by A2.1.27(d)

$$\sum p\ell_i t_j^{p^i} = \sum \ell_i t_j^{p^i} \eta_R(v_k)^{p^{i+j}}.$$

Substituting A2.2.2 on the left-hand side and reindexing gives

$$\sum \ell_i v_j^{p^i} t_k^{p^{i+j}} = \sum \ell_i t_j^{p^i} \eta_R(v_k)^{p^{i+j}}.$$

Applying the inverse of log to this gives the desired formula. □

This formula will be used to prove the classification theorem A2.2.11 below. Computational corollaries of it are given in Section 4.3.

We now turn to the classification in characteristic p. We will see that formal group laws over a field are characterized up to isomorphism over the separable algebraic closure by an invariant called the height (A2.2.7). In order to define it we need

A2.2.6. LEMMA. *Let F be a formal group law over a commutative $\mathbf{F}_p$-algebra R and let $f(x)$ be a nontrivial endomorphism of F* (A2.1.5). *Then for some n, $f(x) = g(x^{p^n})$ with $g'(0) \neq 0$. In particular f has leading term ax^{p^n}.*

For our immediate purpose we only need the statement about the leading term, which is easier to prove. The additional strength of the lemma will be needed below (A2.2.19). The argument we use can be adapted to prove a similar statement about a homomorphism to another formal group law G.

PROOF. Suppose inductively we have shown that $f(x) = f_i(x^{p^i})$, this being trivial for $i = 0$, and suppose $f_i'(0) = 0$, as otherwise we are done. Define $F^{(i)}(x, y)$

$$F(x,y)^{p^i} = F^{(i)}(x^{p^i}, y^{p^i}).$$

It is straightforward to show that $F^{(i)}$ is also a formal group law. Then we have

$$\begin{aligned} f_i(F^{(i)}(x^{p^i}, y^{p^i})) &= f_i(F(x,y)^{p^i}) = f(F(x,y)) \\ &= F(f(x), f(y)) = F(f_i(x^{p^i}), f_i(y^{p^i})) \end{aligned}$$

so

$$f_i(F^{(i)}(x,y)) = F(f_i(x), f_i(y)).$$

Differentiating with respect to y and setting $y = 0$ we get

$$f_i'(F^{(i)}(x,0))F_2^{(i)}(x,0) = F_2(f_i(x), f_i(0))f_i'(0).$$

Since $f_i'(0) = 0$, $F_2^{(i)}(x,0) \neq 0$, and $F^{(i)}(x,0) = x$, this gives us

$$f_i'(x) = 0 \quad \text{so} \quad f_i(x) = f_{i+1}(x^p).$$

We repeat this process until we get an $f_n(x)$ with $f_n'(0) \neq 0$ and set $g = f_n$. $\square$

A2.2.7. DEFINITION. *A formal group law F over a commutative $\mathbf{F}_p$-algebra R has* height n *if $[p]_F(x)$ has leading term ax^{p^n}. If $[p]_F(x) = 0$ then F has* height ∞.

A2.2.8. LEMMA. *The height of a formal group law is an isomorphism invariant.*

PROOF. Let f be an isomorphism from F to G. Then

$$f([p]_F(x)) = [p]_G(f(x));$$

since $f(x)$ has leading term ux for u a unit in R and the result follows. $\square$

A2.2.9. EXAMPLES. Just for fun we will compute the heights of the mod (p) reductions of the formal group laws in A2.1.4.

(a) $[p]_F(x) = 0$ for all p so F has height ∞.

(b) $[p]_F(x) = u_{p-1}x^p$ so F has height 1.

(c) As remarked earlier, F is isomorphic over $\mathbf{Z}_{(2)}$ to the additive formal group law, so its height at $p = 2$ is ∞. Its logarithm is

$$\sum_{i \geq 0} \frac{x^{2i+1}}{2i+1}$$

so for each odd prime p we have $\ell_1 = m_{p-1} = 1/p$, so $v_1 \neq 0 \mod p$ by A2.2.2, so the height is 1 by A2.2.4 and A2.2.7.

(d) Since F is not defined over $\mathbf{Z}_{(2)}$ (as can be seen by expanding it through degree 5) it does not have a mod 2 reduction. To compute its logarithm we have

$$F_2(x,0) = \sqrt{1 - x^4}$$

so by A2.1.6

$$\begin{aligned}
\log(x) &= \int_0 \frac{dt}{\sqrt{1-t^4}} \\
&= \sum_{i\geq 0} \binom{-1/2}{i} \frac{(-1)^i x^{4i+1}}{4i+1} \\
&= \sum_{i\geq 0} \binom{(2i-1)/2}{i} \frac{x^{4i+1}}{4i+1} \\
&= \sum_{i\geq 0} \frac{1\cdot 3\cdot 5\cdot \cdots \cdot (2i-1)x^{4i+1}}{2^i i!(4i+1)} \\
&= \sum_{i\geq 0} \frac{(2i)!\, x^{4i+1}}{2^{2i}(i!)^2(4i+1)}.
\end{aligned}$$

Now if $p \equiv 1 \mod (4)$, we find that $\ell_1 = m_{p-1}$ is a unit (in $\mathbf{Z}_{(p)}$) multiple of $1/p$, so as in (c) the height is 1. However, if $p \equiv -1 \mod (4)$, $v_1 = \ell_1 = 0$ so so the height is at least 2. We have

$$\ell_2 = m_{p^2-1} = \frac{(2i)!}{4(i!)^2 p^2} \quad \text{where} \quad i = \frac{p^2-1}{4}.$$

Since

$$\frac{p^2-1}{2} = \frac{p(p-1)}{2} + \frac{p-1}{2},$$

$(2i)!$ is a unit multiple of $p^{(p-1)/2}$; since

$$\frac{p^2-1}{4} = p\left(\frac{p-3}{4}\right) + \frac{3p-1}{4}$$

$(i!)$ is a unit multiple of $p^{(p-3)/4}$. It follows that ℓ_2 is a unit multiple of $1/p$, so $v_2 \not\equiv 0 \mod p$ and the height is 2.

It is known that the formal group law attached to a nonsingular elliptic curve always has height 1 or 2. (See Corollary 7.5 of Silverman [**1**]).

Now we will specify a formal group law of height n for each n.

A2.2.10. Definition. $F_\infty(x, y) = x + y$. *For a natural number h let F_n be the p-typical formal group law* (*of height n*) *induced by the homomorphism $\theta\colon V \to R$* (A2.1.25) *defined by $\theta(v_n) = 1$ and $\theta(v_i) = 0$ for $i \neq n$.*

A2.2.11. Theorem (Lazard [**2**]). *Let K be a separably closed field of characteristic $p > 0$. A formal group law G over K of height n is isomorphic to F_n.*

Proof. By Cartier's theorem (A2.1.18) we can assume G is p-typical (A2.1.22) and hence induced by a homomorphism $\theta\colon V \to K$ (A2.1.24). If $n = \infty$ then by A2.2.4 $\theta(v_n) = 0$ for all n and $G = F_\infty$. For n finite we have $\theta(v_i) = 0$ for $i < n$ and $\theta(v_n) \neq 0$. Let $F = F_n$. We want to construct an isomorphism $f\colon F \to G$ with $f^{-1}(x) = \sum_{i\geq 0}^F t_i x^{p^i}$. It follows from A2.2.5 that these t_i must satisfy

$$\sum_{i,j}^F t_i \theta(v_j)^{p^i} x^{p^{i+j}} = \sum_j^F t_j^{p^n} x^{p^{n+j}} \tag{A2.2.12}$$

since the homomorphism from V inducing F is given in A2.2.10, and the $\eta_R(v_j)$ in A2.2.5 correspond to $\theta(v_j)$. Here we are not assuming $t_0 = 1$; the proof of A2.2.5 is still valid if $t_0 \neq 1$.

Equating the coefficient of x^{p^n} in A2.2.12, we get $t_0\theta(v_n) = t_0^{p^n}$, which we can solve for t_0 since K is separably closed. Now assume inductively that we have solved A2.2.12 for $t_0, t_1, \ldots, t_{i-1}$. Then equating coefficients of $x^{p^{i+n}}$ gives

$$t_i\theta(v_n)^{p^i} + c = t_i^{p^n}$$

for some $c \in K$. This can also be solved for t_i, completing the proof. $\square$

Our last objective in this section is to describe the endomorphism rings of the formal group laws F_n of A2.2.10.

A2.2.13. LEMMA. *Let F be a formal group law over a field K of characteristic $p > 0$ and let E be the set of endomorphisms of F.*

(a) *E is a ring under composition and formal sum, i.e., the sum of two endomorphisms $f(x)$ and $g(x)$ is $f(x) +_F g(x)$.*

(b) *E is a domain.*

(c) *E is a $\mathbf{Z}_p$-algebra (where $\mathbf{Z}_p$ denotes the p-adic integers) which is a free $\mathbf{Z}_p$-module if F has finite height, and an $\mathbf{F}_p$-vector space if F has infinite height.*

PROOF.

(a) We need to verify the distributive law for these two operations. Let $f(x)$, $g(x)$, and $h(x)$ be endomorphisms. Then

$$f(g(x) +_F f(x)) = f(g(x)) +_F f(h(x))$$

so

$$f(g + h) = (fg) + (fh) \quad \text{in } E.$$

Similarly,

$$(g +_F h)(f(x)) = g(f(x)) +_F h(f(x))$$

so

$$(g + h)f = (gf) + (hf) \quad \text{in } E.$$

(b) Suppose $f(x)$ and $g(x)$ having leading terms ax^{p^n} and bx^{p^n}, respectively, with $a, b \neq 0$ (A2.2.6). Then $f(g(x))$ has leading term $ab^{p^m}x^{p^{m+n}}$, so $fg \neq 0$ in E.

(c) We need to show that $[a]_F(x)$ is defined for $a \in \mathbf{Z}_p$. We can write $a = \sum a_i p^i$ with $a_i \in \mathbf{Z}$. Then we can define

$$[a]_F(x) = \sum\nolimits^F [a_i]_F([p^i]_F(x))$$

because the infinite formal sum on the right is in $K[[x]]$ since $[p^i]_F(x) \equiv 0$ modulo x^{p^i}. If $h < \infty$ then $[a]_F(x) \neq 0$ for all $0 \neq a \in \mathbf{Z}_p$, so E is torsion-free by (b). If $h = \infty$ then $[p]_F(x) = 0$ so E is an $\mathbf{F}_p$-vector space. $\square$

Before describing our endomorphism rings we need to recall some algebra.

A2.2.14. LEMMA. *Let p be a prime and $q = p^i$ for some $i > 0$.*

(a) *There is a unique field $\mathbf{F}_p$ with q elements.*

(b) *Each $x \in \mathbf{F}_q$ satisfies $x^q - x = 0$.*

(c) *$\mathbf{F}_{p^m}$ is a subfield of $\mathbf{F}_{p^n}$ iff $m \mid n$. The extension is Galois with Galois group $Z/(m/n)$ generated by the Frobenius automorphism $x \mapsto x^{p^m}$.*

(d) *$\overline{\mathbf{F}}_p$ the algebraic closure of $\mathbf{F}_p$ and of each $\mathbf{F}_q$, is the union of all the $\mathbf{F}_q$. Its Galois group is $\widehat{\mathbf{Z}} = \varprojlim \mathbf{Z}/(m)$, the profinite integers, generated topologically by the Frobenius automorphism $x \mapsto x^p$. The subgroup $m\mathbf{Z}$ of index m is generated topologically by $x \mapsto x^{p^m}$ and fixes the field $\mathbf{F}_{p^m}$.* □

A proof can be found, for example, in Lang [**1**, Section VII.5]

Now we need to consider the Witt rings $W(\mathbf{F}_q)$, which can be obtained as follows. Over $\mathbf{F}_p$ the polynomial $x^q - x$ is the product of irreducible factors of degrees at most n (where $q = p^n$) since it splits over $\mathbf{F}_q$, which is a degree n extension of $\mathbf{F}_p$. Let $h(x) \in \mathbf{Z}_p[x]$ be a lifting of an irreducible factor of degree n of $x^q - x$. Then let $W(\mathbf{F}_q) = \mathbf{Z}_p[x]/(h(x))$. It is known to be independent of the choices made and to have the following properties.

A2.2.15. LEMMA. (a) *$W(\mathbf{F}_q)$ is a $\mathbf{Z}_p$-algebra and a free $\mathbf{Z}_p$-module of rank n, where $q = p^n$ [e.g., $W(\mathbf{F}_p) = \mathbf{Z}_p$].*

(b) *$W(\mathbf{F}_q)$ is a complete local ring with maximal ideal (p) and residue field $\mathbf{F}_q$.*

(c) *Each $w \in W(\mathbf{F}_q)$ can be written uniquely as $w = \sum_{i \geq 0} w_i p^i$ with $w_i^q - w_i = 0$ for each i.*

(d) *The Frobenius automorphism of $\mathbf{F}_q$ lifts to an automorphism σ of $W(\mathbf{F}_q)$ defined by*

$$w^\sigma = \sum_{i \geq 0} w_i^p p^i.$$

σ generates the Galois group $\mathbf{Z}/(n)$ of $W(\mathbf{F}_q)$ over $\mathbf{Z}_p$.

(e) *$W(\mathbf{F}_q) = \varprojlim W(\mathbf{F}_q)/(p^i)$, so it is a compact topological ring.*

(f) *The group of units $W(\mathbf{F}_q)^\times$ is isomorphic to $W(\mathbf{F}_q) \oplus \mathbf{F}_q^\times$, where $\mathbf{F}_q^\times \cong \mathbf{Z}/(q-1)$, for $p > 2$, and to $W(\mathbf{F}_q) \oplus \mathbf{F}_q^\times \oplus \mathbf{Z}/(2)$ for $p = 2$, the extra summand being generated by -1.*

(g) *$W(\mathbf{F}_q) \otimes \mathbf{Q} = \mathbf{Q}_p[x]/(h(x))$, the unramified degree n extension of $\mathbf{Q}_p$, the field of p-adic numbers.*

A proof can be found in Mumford [**1**, Lecture 26] and in Serre [**1**, Section 11.5.6]. We will sketch the proof of (f). For $p > 2$ there is a short exact sequence

$$1 \to W(\mathbf{F}_q) \xrightarrow{i} W(\mathbf{F}_q)^\times \xrightarrow{j} \mathbf{F}_q^\times \to 1$$

where j is mod (p) reduction and $i(w) = \exp pw = \sum_{i \geq 0} (pw)^i/i!$ [this power series converges in $W(\mathbf{F}_q)$]. To get a splitting $\mathbf{F}_q^\times \to W(\mathbf{F}_q)^\times$ we need to produce $(q-1)$th roots of unity in $W(\mathbf{F}_q)$, i.e., roots of the equation $x^q - x = 0$. [This construction is also relevant to (c).]

These roots can be produced by a device known as the Teichmüller construction. Choose a lifting u of a given element in $\mathbf{F}_q$, and consider the sequence $\{u, u^q, u^{q^2}, \dots\}$. It can be shown that it converges to a root of $x^q - x = 0$ which is independent of the choice of u.

For $p = 2$ the power series $\exp 2w$ need not converge, so we consider instead the short exact sequence

$$1 \to W(\mathbf{F}_q) \xrightarrow{i} W(\mathbf{F}_q)^\times \xrightarrow{j} W(\mathbf{F}_q)/(4)^\times \to 1,$$

where j is reduction mod (4) and $i(w) = \exp 4w$, which always converges. This sequence does not split. We have $W(\mathbf{F}_q)/(4)^\times \cong \mathbf{F}_q \oplus \mathbf{F}_q^\times$. Since $W(\mathbf{F}_q) \otimes \mathbf{Q}$ is a field, $W(\mathbf{F}_q)^\times$ can have no elements of order 2 other than ± 1, so the other elements of order 2 in $W(\mathbf{F}_q)/(4)^\times$ lift to elements in $W(\mathbf{F}_q)^\times$ with nontrivial squares.

Next we describe the noncommutative $\mathbf{Z}_p$-algebra E_n, which we will show to be isomorphic to the endomorphism ring of F_n, for finite n.

A2.2.16. LEMMA. *Let E_n be the algebra obtained from $W(\mathbf{F}_q)$ by adjoining an indeterminate S and setting $S^n = p$ and $Sw = w^\sigma S$ for $w \in W(\mathbf{F}_q)$. Then*

(a) *E_n is a free $\mathbf{Z}_p$ module of rank n^2.*

(b) *Each element $e \in E_n$ can be expressed uniquely as $\sum_{i \geq 0} e_i S^i$ with $e_i^q - e_i = 0$.*

(c) *E_n is generated as a $\mathbf{Z}_p$-algebra by S and a primitive $(q-1)$th root of unity ω with relations $S^n - p = 0$, $S\omega = \omega^p S = 0$, and $h(w) = 0$, where $h(x)$ is an irreducible degree n factor of $x^q - x$ over $\mathbf{Z}_p$.*

(d) *E_n is the maximal order in $D_n = E_n \otimes \mathbf{Q}$ which is a division algebra with center $\mathbf{Q}_p$ and invariant $1/n$.*

The proofs of (a), (b), and (c) are elementary. To see that D_n is a division algebra, note that any element in D_n can be multiplied by some power of S to give an element in E_n which is nonzero mod (S). It is elementary to show that such an element is invertible.

The invariant referred to in (d) is an element in $\mathbf{Q}/\mathbf{Z}$ which classifies division algebras over $\mathbf{Q}_p$. Accounts of this theory are given in Serre [**1**, Chapters XII and XIII] Cassels and Fröhlich [**1**, pp. 137–139], Hazewinkel [**1**, Sections 20.2.16 and 23.1.4]. We remark that for $0 < i < n$ and i prime to n a division algebra with invariant i/n has a description similar to that of D_n except that S^n is p^i instead of p.

Our main results on endomorphism rings are as follows.

A2.2.17. THEOREM (Dieudonné [**1**] and Lubin [**1**]). *Let K be a field of characteristic p containing $\mathbf{F}_q$, with $q = p^n$. Then the endomorphism ring of the formal group law F_n* (A2.2.10) *over K is isomorphic to E_n. The generators ω and S* [A2.2.16(c)] *correspond to endomorphisms $\overline{\omega}x$ and x^p, respectively.*

A2.2.18. THEOREM. *Let R be a commutative $\mathbf{F}_p$-algebra. Then the endomorphism ring of the additive formal group law F_∞ over R is the noncommutative power series ring $R\langle\langle S\rangle\rangle$ in which $Sa = a^p S$ for $a \in R$. The elements a and S correspond to the endomorphisms ax and x^p, respectively.*

PROOF OF A2.2.18. An endomorphism $f(x)$ of F_∞ must satisfy $f(x+y) = f(x) + f(y)$. This is equivalent to $f(x) = \sum_{i \geq 0} a_i x^{p^i}$ for $a_i \in R$. The relation $Sa = a^p S$ corresponds to $(ax)^p = a^p x^p$. □

There is an amusing connection between this endomorphism ring and the Steenrod algebra. Theorem A2.2.18 implies that the functor which assigns to each commutative $\mathbf{F}_p$-algebra R the strict automorphism group of the additive formal group law is represented by the ring

$$P = \mathbf{F}_p[a_1, a_1, \dots]$$

since $a_0 = 1$ in this case. The group operation is represented by a coproduct $\Delta\colon P \to P \otimes P$. To compute Δa_n let $f_1(x) = \sum a'_j x^{p^k}$, $f_2(x) = \sum a''_k x^{p^k}$, and $f(x) = f_2(f_1(x)) = \sum a_i x^{p^i}$ with $a'_0 = a''_0 = a_0 = 1$. Then we have

$$f(x) = \sum a''_k \left(\sum a'_j x^{p^j}\right)^{p^k} = \sum a''_k (a'_j)^{p^j} x^{p^{j+k}}.$$

It follows that

$$\Delta a_n = \sum_{0 \le i \le n} a_{n-i}^{p^i} \otimes a_i \quad \text{with } a_0 = 1,$$

i.e., P is isomorphic to the dual of the algebra of Steenrod reduced powers.

Before proving A2.2.17 we need an improvement of A2.2.6.

A2.2.19. Lemma. *Let F be a formal group law over a field K of characteristic $p > 0$, and let $f(x)$ be an endomorphism of F. Then*

$$f(x) = \sum_{i \ge 0}^{F} a_i x^{p^i}$$

for some $a_i \in K$.

Proof. Suppose inductively we have $f(x) = \sum_{i=0}^{m-1} a_i x^{p^i} +_F f_m(x^{pm})$, this being trivial for $m = 0$. Then set $a_m = f'_m(0)$ and consider the power series

$$g(x^{p^m}) = f_m(x^{p^m}) -_F a_m x^{p^m}.$$

By A2.2.13 this is an endomorphism and we have $g'_m(0) = 0$, so by A2.2.6 $g(x^{p^m}) = f_{m+1}(x^{p^{m+1}})$, completing the inductive step and the proof. ☐

A2.2.17 will follow easily from the following.

A2.2.20. Lemma. *Let $E(F_n)$ be the endomorphism ring of F_n* (A2.2.10) *over a field K containing $\mathbf{F}_q$ where $q = p^n$. Then*

(a) *if $f(x) = \sum^{F_n} a_i x^{p^i}$ is in $E(F_n)$, then each $a_i \in \mathbf{F}_q$;*
(b) *for $a \in \mathbf{F}_q$, $ax \in E(F_n)$;*
(c) *$x^p \in E(F_n)$; and*
(d) *$E(F_n)/(p) = E_n/(p) = \mathbf{F}_q\langle S\rangle/(S^n)$ with $Sa = a^p S$.*

Proof. (a) By the definition of F_n (A2.2.10) and A2.2.14 we have

(A2.2.21) $$[p](x) = x^{p^n}.$$

Any endomorphism f commutes with $[p]$ so by A2.2.19 we have

$$[p](f(x)) = [p]\Big(\sum^F a_i x^{p^i}\Big) = \sum^F [p](a_i x^{p^i}) = \sum^F a_i^{p^n} x^{p^{i+n}}.$$

This must equal

$$f([p](x)) = \sum^F a_i([p](x))^{p^i} = \sum^F a_i x^{p^{i+n}}.$$

Hence $a_i^{p^n} = a_i$ for all i and $a_i \in \mathbf{F}_q$.

(b) It suffices to prove this for $K = \mathbf{F}_q$. $\mathbf{F}_n$ can be lifted to a formal group law $\widetilde{F}_n$ over $w(\mathbf{F}_q)$ (A2.2.15) by the obvious lifting of $\theta\colon V \to \mathbf{F}_q$, to $W(\mathbf{F}_q)$. It suffices to show that ωx is an endomorphism of $\widetilde{F}_n$ if $\omega^q - \omega = 0$. By A2.2.2 $\widetilde{F}_n$ has a logarithm of the form

$$\log(x) = \sum a_i x^{q^i}$$

so $\log(\omega x) = \omega \log(x)$ and ωx is an endomorphism.

(c) This follows from the fact that F_n is defined over $\mathbf{F}_p$, so $F_n(x^p, y^p) = F_n(x, y)^p$.

(d) By A2.2.21, (b) and (c), $f(x) \in pE(F_n)$ iff $a_i = 0$ for $i < n$. It follows that for $f(x), g(x) \in E(F_n)$, $f \equiv g \mod (p)E(F_n)$ iff $f(x) \equiv g(x) \mod (x^q)$. Now our lifting $\widetilde{F}_n$ of F_n above has $\log x \equiv x \mod (x^q)$, so $F_n(x, y) \equiv x + y \mod (x, y)^q$. It follows that $E(F_n)/(p)$ is isomorphic to the corresponding quotient of $E(F_\infty)$ over $\mathbf{F}_q$, which is as claimed by A2.2.17. □

Proof of A2.2.17. . By A2.2.16(c) E_n is generated by ω and S. The corresponding elements are in $E(F_n)$ by A2.2.20(b) and (c). The relation $S\omega = \omega^p S$ corresponds as before to the fact that $(\overline{\omega} x)^p = \overline{\omega}^p x^p$, where $\overline{\omega}$ is mod (p) reduction of ω. Hence we have a homomorphism $\lambda\colon E_n \to E(F_n)$ which is onto by A2.2.19. We know [A2.2.13(c)] that $E(F_n)$ is a free $\mathbf{Z}_p$-module. It has rank n^2 by A2.2.20(d), so λ is 1-1 by A2.2.16(a). □