Formal Modules

Elliptic Modules Learning Seminar

Andrew O'Desky

October 6, 2017

In short, a formal module is to a commutative formal group as a module is to its underlying abelian group. For the purpose of developing the moduli theory of elliptic modules, which are instances of formal modules, they will provide a more flexible context for the deformation arguments required to show that the modular schemes M_I^d constructed in §5B are in fact smooth, hence "manifolds", which fact is required for the proof of their uniformisation in §6 and subsequent compactification in §9, which is then required for the connection with automorphic forms in §10, which was our original motivation (Goal 1.1) in the first talk by (the other) Andrew.

1 Formal Group Laws

Let $\mathcal{O}$ be any commutative ring with unity and B a $\mathcal{O}$-algebra.

Definition A *formal group law over B* is a power series $F(x, y) \in B[\![x, y]\!]$ satisfying the properties

1. $F(X, 0) = X,\ F(0, Y) = Y$
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$

Often F is just called a formal group. If $F(X, Y) = F(Y, X)$ then F is said to be commutative. Note that the composition in (2) makes sense only by virtue of (1), which implies that $F(0, 0) = 0$. Also note that condition (1) implies that

$$F(X, Y) = X + Y \bmod (X, Y)^2$$

and that non-linear terms are always mixed with powers of X and Y. One may also define formal group laws of higher dimension (ours is one dimensional) in a straightforward fashion.

Example The simplest group law is given by $F(X, Y) = X + Y$, which is known as the *additive formal group law.* It is also one of the most important formal group laws. One also has the *multiplicative formal group law* given by $F(X, Y) = X + Y + XY$. More on these to come.

Proposition 1.1. *For any formal group law F there exists a unique power series $i(X) = -X + \cdots \in B[\![X]\!]$ such that $F(X, i(X)) = F(i(X), X) = 0$.*

Proof. Exercise. □

Corollary 1.2. *Suppose B is a complete local ring and let $\mathfrak{m} = \{x \in B : |x| < 1\}$ be its maximal ideal (i.e., the open unit disk about 0). Then for any formal group law F, $(\mathfrak{m}, F)$ is a group with composition defined by $x \cdot y = F(x, y) \in \mathfrak{m}$.*

Proof. Immediate. □

The corollary shows that $F(X, Y)$ may be interpreted as an analytic function giving a law of group composition which may be realized on any ring where it is defined so long as the context allows one to make sense of convergence. In particular, when $F(X, Y)$ and $i(X)$ are both polynomials we may make sense of the group law for any ring whatsoever.

For the additive group, $i(X) = -X$ and we recover the original additive structure even without the assumption of completeness. For the multiplicative group, $i(X)$ is no longer finite so that completeness becomes necessary in general:

$$\begin{tikzcd}
(\mathfrak{m}, F) \times (\mathfrak{m}, F) \arrow[r, "X+1 \times Y+1"] \arrow[d, "F(X,Y)"'] & 1+\mathfrak{m} \times 1+\mathfrak{m} \arrow[d, "XY"] \\
(\mathfrak{m}, F) & 1+\mathfrak{m} \arrow[l, "X-1"']
\end{tikzcd}$$

This diagram both explains why $F(X, Y) = X + Y + XY$ is called the multiplicative group law as well as giving an explicit isomorphism of groups (not formal groups!) between $(\mathfrak{m}, F)$ and $1+\mathfrak{m}$, the 1-units of B under multiplication. It also explains why $i(X)$ must be an infinite series: Clearly $i(X)$ must correspond to $1/X$ on the right (recall uniqueness of $i(X)$ for F). We "change bases" to find $i(X) = \frac{1}{1+X} - 1 = -X + X^2 - X^3 + \cdots$. One may now plug $i(X)$ into the multiplicative group law to check its validity, whence by uniqueness one has the expression for $i(X)$.

It turns out that when B has no nilpotent elements which are also (additive) torsion that one-dimensional formal group laws over B are always commutative. For example, any (one-dimensional) formal group law over a reduced ring in characteristic zero is commutative. From here on out *we will always assume our formal group laws are one-dimensional and commutative.*

A homomorphism of formal group laws F, G over B is a power series $f \in B[\![X]\!]$ with zero constant term such that $f(F(X, Y)) = G(f(X), f(Y))$. $\mathrm{Hom}_B(F, G)$ is naturally an abelian group where we define

$$(f +_G g)(X) = G(f(X), g(X)) = f(X) +_G g(X)$$

We check:

$$\begin{aligned}
(f +_G g)(F(X, Y)) &= G(f(F(X, Y)), g(F(X, Y))) \\
&= G(G(f(X), f(Y)), G(g(X), g(Y))) \\
&= (f(X) +_G f(Y)) +_G (g(X) +_G g(Y)) \\
&= (f(X) +_G g(X)) +_G (f(Y) +_G g(Y)) \\
&= G((f +_G g)(X), (f +_G g)(Y))
\end{aligned}$$

from which it follows that $\mathrm{End}\, F$ is a ring under composition. We thus have a natural map

$$\mathbb{Z} \to \mathrm{End}\, F : n \mapsto [n]_F$$

where $[1]_F(X) = X$, $[-1]_F(X) = i(X)$, and $[n+1]_F(X) = F([n]_F(X), X)$. Let us define the map $D : \operatorname{End} F \to B$ that sends the endomorphism f to $f'(0)$. D is a ring homomorphism.

Proposition 1.3. *If B is an integral domain, then End$F$ is a (non-commutative) integral domain, and Hom$_B(F, G)$ is a torsion-free left End$F$ and right End$G$ module.*

Proof. See Fröhlich [1, III.1, Prop. 2, p58]. □

Historically formal group laws were introduced in 1946 by Bochner as an abstraction of the analytic group laws of Lie groups. Bochner there showed that one may prove direct analogues of Lie's theorems using only the group laws. Meanwhile the necessity of restricting to the maximal ideal in order to assure convergence in complete generality shows that these formal group laws should be thought of as being of a local nature, as suggested by their historical origin. In fact in characteristic zero the study of a Lie algebra and the formal group law associated with its Lie group are essentially equivalent, the commutator being recovered from the formal group law via its quadratic terms $[X, Y] = F_2(X, Y) - F_2(Y, X)$.

2 Formal $\mathcal{O}$-Modules and the Ring $\Lambda_{\mathcal{O}}$

Let B be an $\mathcal{O}$-algebra and write $\mathcal{O} \xrightarrow{i} B$ for its structure map. We now consider formal groups whose ring of endomorphisms is (potentially) larger than expected:

Definition A *formal $\mathcal{O}$-module* over B is a pair (F, ρ), where F is a commutative formal group over B, and ρ is a ring homomorphism from $\mathcal{O}$ to End$F$ such that $D \circ \rho = i$. In other words, $\rho(a)(X) = i(a)X + \cdots$.

Remark. It will be important for us later to consider $\mathcal{O}$-algebras for which the structure map is not injective.

Examples

- Any (commutative) formal group over B is a formal $\mathbb{Z}$-module over B.
- The additive group law $F = X + Y$ together with $\rho(a)(X) = aX$ defines a formal $\mathcal{O}$-module over B for any ring $\mathcal{O}$ and any $\mathcal{O}$-algebra B. This formal module is uncreatively called the *additive module.*
- An *elliptic $\mathcal{O}$-module* over K is defined as any formal $\mathcal{O}$-module whose underlying group law is the additive group law over K which is not the additive module over K, whose endomorphisms are all defined with polynomials (as opposed to power series).
- Lubin-Tate Theory in local class field theory
- $\mathbb{Z}[\tau] = \operatorname{End}(F_\tau)$, for F_τ the formal group law over associated to the elliptic curve $E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$, $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$, $\tau \notin \mathbb{R}$.

We now think of $\mathcal{O}$ as fixed and consider the problem of finding the most general formal $\mathcal{O}$-module. More specifically, we will look for a $\mathcal{O}$-algebra $\Lambda_{\mathcal{O}}$ and a formal $\mathcal{O}$-module (F_u, ρ_u) over $\Lambda_{\mathcal{O}}$ such that for any formal $\mathcal{O}$-module (G, ρ_G) over a $\mathcal{O}$-algebra B, there exists a unique $\mathcal{O}$-algebra map $\Lambda_{\mathcal{O}} \xrightarrow{\theta} B$ such that applying θ to the coefficients yields $F_u^\theta = G$ and $\rho_u^\theta = \rho_G$. In other words, we want to represent the functor from the category of $\mathcal{O}$-algebras to the category of sets given by $B \mapsto$ set of formal $\mathcal{O}$-modules over B.

Let a_{ij} and b_{ka}, $i, j \geq 0$, $k \geq 2$, $a \in \mathcal{O}$ be indeterminates and consider the power series in $\mathcal{O}[a_{ij}, b_{ka}][\![X, Y]\!]$ given by

$$F(X,Y) = \sum_{i,j\geq 0} a_{ij} X^i Y^j \qquad \rho(a)(X) = aX + \sum_{k\geq 2} b_{ka} X^k$$

where there is an individual power series $\rho(a)$ for every $a \in \mathcal{O}$. We now subject these symbols to the relations that F_u should be a commutative formal group law and that ρ should be a ring homomorphism:

$$F(F(X,Y),Z) = F(X, F(Y,Z)), \qquad F(X,Y) = F(Y,X)$$
$$F(\rho(a)(X), \rho(a)(Y)) = \rho(a)(F(X,Y))$$
$$\rho(a)(\rho(b)(X)) = \rho(ab)(X), \qquad \rho(a+b)(X) = F(\rho(a)(X), \rho(b)(X))$$
$$F(\rho(-a)(X), \rho(a)(X)) = 0, \quad \rho(1)(X) = X, \quad \rho(0)(X) = 0$$

Note that any relation on the coefficients in any of the above equations can be written using only ring operations in $\mathcal{O}[a_{ij}, b_{ka}]$. If I is the ideal of these relations then we set $\Lambda_A = \mathcal{O}[a_{ij}, b_{ka}]/I$ and write F_u and ρ_u for the images of F and ρ. We may also put a grading on this ring if we set $\deg a_{ij} = i + j - 1$, $\deg b_{ka} = k - 1$ and $\deg X = \deg Y = -1$. Note that $\deg a_{ij}, \deg b_{ka} \geq 0$ since $a_{00} = 0$. Now all the equations above are homogeneous in degree -1 so that I is homogeneous and Λ_A will be graded.

It is immediate that $\mathrm{Hom}_{\mathcal{O}}(\Lambda_A, -)$ represents the functor above. In particular, when $\mathcal{O} = \mathbb{Z}$ we recover *Lazard's ring* $\Lambda_{\mathbb{Z}}$. For the remainder of the talk we will study structural results on $\Lambda_{\mathcal{O}}$ for various $\mathcal{O}$.

Elements of the form xy, where $x, y \in \Lambda_{\mathcal{O}}$ are homogeneous of degree > 1, generate a homogeneous ideal. Everything in this submodule is a sum of "decomposable" elements. Write $\widetilde{\Lambda_{\mathcal{O}}}$ for the quotient of $\Lambda_{\mathcal{O}}$ by this ideal.

Proposition 2.1. *Let $n > 1$. Then $\widetilde{\Lambda_{\mathcal{O}}}^{n-1}$ as an $\mathcal{O}$-module can be defined by the symbols d and h_a for all $a \in \mathcal{O}$ subject to the relations*

$$\begin{aligned} d(a^n - a) &= v(n) h_a, && \text{for all } a \in \mathcal{O} \\ h_{a+b} - h_a - h_b &= dC_n(a,b), && \text{for all } a, b \in \mathcal{O} \\ a h_b + b^n h_a &= h_{ab}, && \text{for all } a, b \in \mathcal{O} \end{aligned} \tag{1}$$

where

$$v(n) = \begin{cases} 1, & \text{if } n \text{ is not a power of a prime number} \\ p, & \text{if } n = p^k \end{cases}$$

and for all $n > 1$ we define $C_n(X,Y) = v(n)^{-1}((X+Y)^n - X^n - Y^n) \in \mathbb{Z}[X,Y]$. So $C_2 = XY$, $C_3 = X^2Y + XY^2$, $C_4 = 2XY^3 + 3X^2Y^2 + 2X^3Y$.

We postpone the proof. The importance of the polynomial $C_n(X,Y)$ is demonstrated by the following three lemmas:

Lemma 2.2. *For all $n > 1$ the polynomial $C_n(X,Y) \in \mathbb{Z}[X,Y]$ is* primitive *(i.e., the greatest common divisor of its coefficients is* 1*).*

Proof. Simple argument: see Fröhlich [1, III.1, Lemma 1, p60]. □

Lemma 2.3. *Let $F(X,Y)$ and $G(X,Y)$ be two formal group laws over an $\mathcal{O}$-algebra B which agree up to degree n terms (i.e., $F-G \in (X,Y)^n$), $n>1$. Then there is a unique element $a \in B$ such that $F(X,Y) \equiv G(X,Y) + aC_n(X,Y) \mod (X,Y)^{n+1}$.*

Proof. One has that $F \equiv G+\Gamma$ for some homogeneous polynomial $\Gamma(X,Y)$ of degree n. I claim that Γ satisfies

$$\begin{aligned}&\Gamma(X,Y)=\Gamma(Y,X)\\&\Gamma(X,0)=\Gamma(0,Y)=0\\&\Gamma(X,Y)+\Gamma(X+Y,Z)=\Gamma(Y,Z)+\Gamma(X,Y+Z)\end{aligned} \tag{2}$$

The first two equations are easy. Let us write $G(X,Y)=X+Y+G_2(X,Y)$. Modulo degree $n+1$ terms we have

$$\begin{aligned}F(F(X,Y),Z)) &\equiv G(F(X,Y),Z)+\Gamma(F(X,Y),Z)\\&\equiv F(X,Y)+Z+G_2(F(X,Y),Z)+\Gamma(X+Y,Z)\\&\equiv G(X,Y)+\Gamma(X,Y)+Z+G_2(G(X,Y),Z)+\Gamma(X+Y,Z)\\&\equiv G(G(X,Y),Z)+\Gamma(X,Y)+\Gamma(X+Y,Z)\end{aligned}$$

Similarly one shows that $F(X,F(Y,Z)) \equiv G(X,G(Y,Z))+\Gamma(X,Y+Z)+\Gamma(Y,Z)$. This proves the third formula for Γ. It is now sufficient to prove the next lemma. □

Lemma 2.4. *Let $\Gamma(X,Y) \in \mathcal{O}[X,Y]$ be a homogeneous polynomial of degree n satisfying equations* (2)*. Then there is an $a \in B$ such that $\Gamma(X,Y)=aC_n(X,Y)$.*

Proof. Fröhlich [1, III.1, Theorem 1a, p62] proves it by making a series of reductions until it is sufficient to show it in the case that B is a field. In that situation one shows that the subspace of homogeneous polynomials of degree n satisfying equations (2) is at most one-dimensional. Since $C_n(X,Y)$ satisfies them, it is sufficient to know that $C_n \neq 0$ in B for which one uses the first lemma. Hazewinkel [2, I.4.3, Lemma 4.3.1, p23] proves it using facts about binomial coefficients. □

We will now prove a version of Lemma 2.3 for formal modules.

Lemma 2.5. *Let $(F(X,Y),\rho_F)$ and $(G(X,Y),\rho_G)$ be two formal $\mathcal{O}$-modules over an $\mathcal{O}$-algebra B and suppose they are congruent modulo $(X,Y)^n$ for some $n>1$. Then there exist a unique element $d \in B$ and unique elements $c_a \in B$, one for each $a \in \mathcal{O}$, such that*

$$\begin{aligned}F(X,Y) &\equiv G(X,Y)+dC_n(X,Y) \mod (X,Y)^{n+1}\\ \rho_F(a)(X) &\equiv \rho_G(a)(X)+c_aX^n \mod (X,Y)^{n+1}\end{aligned}$$

where the elements d and c_a satisfy the relations

$$\begin{gathered}d(a^n-a)=v(n)c_a \qquad \textit{for all } a \in \mathcal{O}\\ c_{a+b}-c_a-c_b=dC_n(a,b) \qquad \textit{for all } a,b \in \mathcal{O}\\ ac_b+b^nc_a=c_{ab} \qquad \textit{for all } a,b \in \mathcal{O}\end{gathered} \tag{3}$$

Proof. By Lemma 2.3 we have a $d \in \mathcal{O}$ such that $F(X,Y) \equiv G(X,Y)+dC_n(X,Y) \mod$ degree $n+1$. As for the second equation there are clearly such c_a. To show the relations (3), we have the congruences modulo degree $n+1$, for arbitrary $a \in \mathcal{O}$:

$$\begin{aligned}\rho_F(a)(F(X,Y)) &\equiv \rho_F(a)(G(X,Y))+adC_n(X,Y)\\&\equiv \rho_G(a)(G(X,Y))+c_a(X+Y)^n+adC_n(X,Y)\end{aligned}$$

on the other hand

$$\begin{aligned}\rho_F(a)(F(X,Y)) &= F(\rho_F(a)(X), \rho_F(a)(Y))\\ &\equiv G(\rho_F(a)(X), \rho_F(a)(Y)) + dC_n(aX, aY)\\ &\equiv G(\rho_G(a)(X), \rho_G(a)(Y)) + c_aX^n + c_aY^n + dC_n(aX, aY)\\ &= \rho_G(a)(G(X,Y)) + c_aX^n + c_aY^n + a^n dC_n(X,Y)\end{aligned}$$

These two expressions show that $c_a v(n) C_n(X,Y) = d(a^n - a)C_n(X,Y)$. By primitivity of C_n we must have $c_a v(n) = d(a^n - a)$.

To calculate the second and third identities of (3), calculate congruences relating $\rho_F(a+b)(X)$ and $\rho_G(a+b)(X)$, then $\rho_F(a)(\rho_F(b)(X))$ and $\rho_G(a)(\rho_G(b)(X))$, respectively. See Hazewinkel [2, 21.2.4, p204] for the details. □

We now return to the proof of Proposition 2.1.

Proof of Proposition 2.1. For $n > 1$ define $J^{n-1} \subset \Lambda_{\mathcal{O}}$ to be the ideal generated by all elements of degree $< n-1$. Now we apply Lemma 2.5 using $B = \Lambda_{\mathcal{O}}/J^{n-1}$ to compare the additive module over B, $X+Y$, with the formal $\mathcal{O}$-module corresponding to the homomorphism $F_u \mapsto F_u + J^{n-1} \in B[\![X,Y]\!]$. These modules are equivalent modulo $(X,Y)^n$:

$$F_u + J^{n-1} \equiv X + Y \mod (X,Y)^n$$

$$\rho_u(a)(X) + J^{n-1} \equiv aX \mod (X)^n$$

so that the Lemma guarantees the existence of a unique $d \in B$ and unique $c_a \in B$, one for each $a \in \mathcal{O}$, such that

$$\begin{aligned}F_u + J^{n-1} &\equiv X + Y + dC_n(X,Y) \mod (X,Y)^{n+1}\\ \rho_u(a)(X) + J^{n-1} &\equiv aX + c_aX^n \mod (X)^{n+1}\end{aligned}$$

The key point is that the parts of these equations homogeneous in X and Y of (X,Y)-degree n is independent of $(X,Y)^{n+1}$ and J^{n-1}.

$$\sum_{i=0}^{n} a_{i,n-i}X^iY^{n-i} = dC_n(X,Y)$$

$$b_{na}X^n = c_aX^n$$

So we find that modulo J^{n-1}, the element $d \in B$ generates all the $a_{i,n-i}$ of degree $n-1$ and $c_a \in B$ equals b_{na} for all $a \in \mathcal{O}$. On the other hand, J^{n-1} is trivial in degree $n-1$. They do not generate Λ_A^{n-1} because we might have products of lower-degree terms which cannot be expressed in terms of these generators, but they do generate $\widetilde{\Lambda_{\mathcal{O}}}^{n-1}$ as was to be shown.

□

We will now specialize the general theorems stated above to a few cases of interest which will be relevant for developing elliptic modules.

Proposition 2.6. *If $\mathcal{O}$ is a field, then every formal $\mathcal{O}$-module is isomorphic to an additive module. If $\mathcal{O}$ is an infinite field, then there exists a unique isomorphism with an additive module, whose derivative at zero equals* 1. *In this case $\Lambda_{\mathcal{O}} \simeq \mathcal{O}[g_1, g_2, \ldots]$, where $\deg g_i = i$.*

Proof. Omitted. See Drinfeld's paper. □

Lemma 2.7. *If $\mathcal{O}$ is the ring of integers of a local nonarchimedean field, then $\widetilde{\Lambda_{\mathcal{O}}}^{n-1} \simeq \mathcal{O}$.*

Proof. Let $\pi \in \mathcal{O}$ be a prime element, $p = \operatorname{char} \mathcal{O}/(\pi)$ and $q = |\mathcal{O}/(\pi)|$. We will show that $\widetilde{\Lambda_{\mathcal{O}}}^{n-1}$ is free as an $\mathcal{O}$-module on a generator u. There will be two cases to consider:

1. If n is not a power of q, then $c_a = (a^n - a)u$ and $d = v(n)u$, where u is a generator of $\widetilde{\Lambda_{\mathcal{O}}}^{n-1}$.

2. If $n = q^k$, then $c_a = (a^n - a)u/\pi$ and $d = pu/\pi$, where u is a generator of $\widetilde{\Lambda_{\mathcal{O}}}^{n-1}$.

1) If n is not a power of p, then c_a may be expressed in terms of d by means of the relation $(a^n - a)d = c_a$; here we may take $u = d$. If n is a power of p, but not of q, then there exists $a \in \mathcal{O}$ such that $a^n - a \notin (\pi)$ (n-th powering on the residue field does not fix everything). Now from the relation $ac_b + b^n c_a = c_{ab}$ we get that $(a^n - a)c_b = (b^n - b)c_a$; here we take $u = (a^n - a)^{-1}c_a$, so we need to show that we may express d in terms of c_a, which follows immediately from the relation $d(a^n - a) = pc_a$.

2) Let n be a power of q. In this case we have that $a^n - a \in (\pi)$ for all $a \in \mathcal{O}$ (either a is a unit or it's not; in either case this is true). Hence there exists an epimorphism of $\mathcal{O}$-modules $\widetilde{\Lambda_{\mathcal{O}}}^{n-1} \to \mathcal{O}$ sending $c_a \mapsto (a^n - a)/\pi$ and $d \mapsto p/\pi$, as one easily verifies that the three relations between the c_a and d hold under the map. It is surjective because there is at least one $a \in \mathcal{O}$ such that $\nu_\pi(a^n - a) = 1$ (namely any a with valuation 1). Under this $\mathcal{O}$-module map, $c_\pi \mapsto \pi^{n-1} - 1$ which is a generator for $\mathcal{O}$. We take $u = c_\pi$, and claim that c_π generates $\widetilde{\Lambda_{\mathcal{O}}}^{n-1}$ as an $\mathcal{O}$-module. This will show that the map above is an isomorphism. Note that in the case $\operatorname{char} \mathcal{O} = p$ $d \mapsto 0$, but in that case d is zero in $\Lambda_{\mathcal{O}}$ as well.

We consider $M = \widetilde{\Lambda_{\mathcal{O}}}^{n-1}/(c_\pi)$. If $x \in \widetilde{\Lambda_{\mathcal{O}}}^{n-1}$ write $\bar{x}$ for the image of x in M. From the relation $ac_b + b^n c_a = c_{ab}$ we get $(\pi^n - \pi)c_a = (a^n - a)c_\pi$, so that $(\pi^n - \pi)\overline{c_a} = 0$, whence $\pi\overline{c_a} = 0$ for any $a \in \mathcal{O}$ since $1 - \pi^{n-1}$ is a unit. The same relation also shows $c_{\pi b} = \pi c_b + \pi^n c_\pi$ so that $\overline{c_{\pi b}} = \pi\overline{c_b} = 0$ in M for any $b \in \mathcal{O}$. In particular, $\overline{c_p} = 0$. But $c_p = (p^{n-1} - 1)d$ and so $\overline{d} = 0$ as well.

It follows that M is an $\mathcal{O}/(\pi)$-module so that $\overline{x}^n = \overline{x}$ for all $x \in \mathcal{O}$. Hence we have $\overline{c_{ab}} = a\overline{c_b} + b\overline{c_a}$ so that $\bar{c} : \mathcal{O}/(\pi) \to M$ is a derivation. But then for any $a \in \mathcal{O}$ we have $\overline{c_a} = \overline{c_{a^n}} = n\overline{a}^{n-1}\overline{c_a} = 0$. Since $\widetilde{\Lambda_{\mathcal{O}}}^{n-1}$ was generated by the c_a and d, we've shown $M = 0$.

In the first case we took $u = d$ or $u = (a^n - a)^{-1}c_a$ for a certain $a \in \mathcal{O}$, and in the second case $u = c_\pi$. From the relations (3) defining d and the c_a it is clear that neither d nor any c_a are non-zero torsion elements. The result follows.

□

Remark. *It turns out to be true more generally that $\widetilde{\Lambda_{\mathcal{O}}}^{n-1} \simeq \mathcal{O}$ whenever $\mathcal{O}$ is a PID, a result due to Hazewinkel [2, Prop. 21.3.1, p207].*

Proposition 2.8. *If $\mathcal{O}$ is the ring of integers of a local nonarchimedean field, then we also have that $\Lambda_{\mathcal{O}} \simeq \mathcal{O}[g_1, g_2, \ldots]$, $\deg g_i = i$.*

Proof. There exists an epimorphism of $\mathcal{O}$-algebras $\mathcal{O}[g_1, g_2, \ldots] \to \Lambda_{\mathcal{O}}$ consistent with the gradation simply by mapping c_n to the generator u of $\widetilde{\Lambda_{\mathcal{O}}}^{n}$ which is guaranteed by Lemma 2.7. Meanwhile Proposition 2.6 implies that $\Lambda_{\mathcal{O}} \otimes K \simeq K[g_1, g_2, \ldots]$ (where $K = \operatorname{Frac} \mathcal{O}$) and $\deg g_i = i$. Therefore the epimorphism above is an isomorphism. □

Corollary 2.9. *1) Every formal $\mathcal{O}$-module defined modulo $(X, Y)^n$ arises from a formal $\mathcal{O}$-module. 2) If $B \to C$ is an epimorphism of $\mathcal{O}$-algebras, then every formal $\mathcal{O}$-module over C arises from an $\mathcal{O}$-module over B.*

Proof. Both assertions follow from the fact that $\Lambda_{\mathcal{O}}$ is a polynomial algebra on the g_i. As they are algebraically independent one may extend a formal $\mathcal{O}$-module defined in low degree in any way which is consistent with the relations (3). □

We also have a more specific version of the lemma comparing formal modules agreeing modulo some degree:

Proposition 2.10. *Let $\mathcal{O}$ be the ring of integers of a local nonarchimedean field. For statements* (1) *and* (2) *suppose (F, ρ_F) and (G, ρ_G) are formal $\mathcal{O}$-modules over B such that $(F, \rho_F) \cong (G, \rho_G)$ $\mod \deg n$.*

1. *If n is not a power of q, then for a unique $v \in B$*

$$F(X,Y) \equiv G(X,Y) + v[(X+Y)^n - X^n - Y^n] \mod (X,Y)^{n+1}$$
$$\rho_F(a)(X) \equiv \rho_G(a)(X) + v(a^n - a)X^n \mod (X,Y)^{n+1}$$

2. *If n is a power of q, then for a unique $v \in B$*

$$F(X,Y) \equiv G(X,Y) + v\frac{p}{\pi}C_n(X,Y) \mod (X,Y)^{n+1}$$
$$\rho_F(a)(X) \equiv \rho_G(a)(X) + v\frac{a^n - a}{\pi}X^n \mod (X,Y)^{n+1}$$

3. *Let $\psi \in B[\![X]\!]$, $\psi(X) \equiv X - vX^n \mod (X)^{n+1}$, and suppose that for all $a \in B$*

$$G(\psi(X), \psi(Y)) = \psi(F(X,Y)), \quad \psi(\rho_F(a)(X)) = \rho_G(a)(\psi(X))$$

In other words, that $\psi : (F, \rho_F) \to (G, \rho_G)$ is a map of formal $\mathcal{O}$-modules. Then

$$F(X,Y) \equiv G(X,Y) + v[(X+Y)^n - X^n - Y^n] \mod (X,Y)^{n+1}$$
$$\rho_F(a)(X) \equiv \rho_G(a)(X) + v(a^n - a)X^n \mod (X,Y)^{n+1}$$

Proof. For (1) and (2) take v to be the image of $u \in \Lambda_{\mathcal{O}}$ from Lemma 2.7. (3) may be checked directly. The idea is that the assumed form of ψ implies that $F \equiv G$ in degree $< n+1$ so that one may use (1). □

Corollary 2.11. *The formal $\mathcal{O}$-module (F, ρ) is isomorphic to an additive module if and only if the coefficients of $\rho(\pi)$ are divisible by π.*

For the remainder of the talk we will assume that $\mathcal{O}$ is the ring of integers of a local nonarchimedean field with a field E given over $\mathcal{O}$ (i.e., there is a given map $i : \mathcal{O} \to E$) such that $(\pi) \subset \ker(i)$ (E is of "finite characteristic"); for instance, $\mathcal{O} = A_\nu \subset k_\nu$, $k = \mathbb{F}_q(T)$. Our applications later will take $E = \widehat{A}_\nu^{nr}/\nu$, where ν is some finite place of A. We now introduce the height of such a formal module, which is the most important invariant it has:

Theorem 2.12 (Theorem-Definition)**.** *Let ϕ be a homomorphism of formal group laws over E. If $\phi \neq 0$ then $\phi(X) = a_1X^{p^h} + a_2X^{2p^h} + \cdots$ where $a_1 \neq 0$, $h > 0$, and $p = char(E)$. The number h is uniquely determined by ϕ and is defined to be its* height*: $ht\phi = h$. By definition, $ht0 = \infty$. The height of a formal $\mathcal{O}$-module over E is the height of the endomorphism of multiplication by π.*

Proof. We prove that $D(\phi) = 0$ if and only if $\phi = 0$ or $\phi \neq 0$ and $\phi = \psi(X^{p^h})$, where $D(\psi) \neq 0$. Consider the defining relation

$$\phi(F(X,Y)) = G(\phi(X), \phi(Y))$$

and partial differentiate with respect to Y to get

$$\phi'(F(X,Y))F_Y(X,Y) = G_Y(\phi(X), \phi(Y))\phi'(Y)$$

then set $Y = 0$

$$\phi'(X))F_Y(X,0) = G_Y(\phi(X), 0)\phi'(0)$$

Now $F_Y(X,0) = 1 + X + \cdots$ so is invertible in $E[\![X]\!]$ and $\phi'(0) = D(\phi)$. Assuming $D(\phi) = 0$ means $\phi'(X) = 0$. (Note that if E were characteristic 0 then this shows $\phi = 0$, so that the notion of height is only interesting in positive characteristic.) As E is characteristic p this shows $\phi = \psi(X^{p^h})$ for some $h > 0$. Take h to be maximal.

I now claim that $\psi(X)$ is non-zero in X-degree 1 so that $D(\psi) \neq 0$. Let $q = p^h$ and set $H(X,Y)$ to be the power series obtained by raising all of F's coefficients to the qth power. Then $\psi(H(X,Y)) = \psi(F(X,Y)^q) = \phi(F(X,Y)) = G(\phi(X), \phi(Y)) = G(\psi(X^q), \psi(Y^q))$ so that ψ is a homomorphism of formal group laws from H to G. Now if $D(\psi) = 0$ we could repeat the argument above which contradicts maximality of h. □

Remark. *In the case of the height of a homomorphism ϕ of formal $\mathcal{O}$-modules with $p^k = q = |\mathcal{O}/(\pi)|$, the $\mathcal{O}$-linearity of ϕ makes it so that $k | ht\,\phi$. For convenience, Drinfeld takes $ht\,\phi/k$ as his definition of the height. For consistency we will use Drinfeld's convention from here on out.*

Proposition 2.13. *1) There exist modules of arbitrary (finite) height.*
2) There exist homomorphisms only between modules of the same height.
3) A formal $\mathcal{O}$-module of height h is isomorphic to the additive module mod $\deg q^h$.

Proof. 1) Consider any $\mathcal{O}$-algebra map $\lambda : \Lambda_{\mathcal{O}} \to E$ such that $\lambda(g_{q^h-1}) \neq 0$ and $\lambda(g_i) = 0$ when $i < q^h - 1$ (the higher-degree generators can be mapped in an arbitrary way). From the universal property of $\Lambda_{\mathcal{O}}$, we get a formal $\mathcal{O}$-module over E given by applying λ to F_u and ρ_u. In this degree we map $\lambda(g_{q^h-1})$ to the corresponding d and we have the relation $(a^n - a)d = c_a$ for all $a \in \mathcal{O}$. In particular $c_\pi \neq 0$ so that $\rho_u^\lambda(\pi)(X) = c_\pi X^{q^h} + \cdots$ shows this module is of height h.

2) A basic property of the height is that the height of a composition of homomorphisms equals the sum of their heights. Hence isomorphisms have height 0, so that the heights of the isomorphic modules must be the same.

3) Follows from Proposition 2.10.

□

Proposition 2.14. *1) All formal $\mathcal{O}$-modules of a finite height $h < \infty$ become isomorphic over the separable closure of E.*
2) The ring of endomorphisms of such a module over the separable closure of E is isomorphic to the ring of integers of a central division algebra over K with invariant $1/h$.

Proof. The proof of this is rather long. It is a formal $\mathcal{O}$-module version of an analogous statement for formal groups. Fröhlich attributes the formal group version to Dieudonne and Lubin; see [1, III.2, Theorem 3, p72]. For the proof, see Drinfeld's paper. □

References

[1] A. Fröhlich, *Formal Groups.* Lecture Notes in Mathematics Vol. 74

[2] M. Hazewinkel, *Formal Groups and Applications.* Pure and Applied Mathematics