The Algebraic Properties of Formal Group Laws

Shay Ben Moshe

20/06/2017

1 Introduction

(All rings are commutative with unit.)

Definition. Let R be a ring. A (commutative one-dimensional) *formal group law* over R is an element $F(x,y) \in R[[x,y]]$, such that:

1. $F(x,0) = x = F(0,x)$
2. $F(x,y) = F(y,x)$ (commutativity) **TODO Do we need commutative?**
3. $F(F(x,y),z) = F(x,F(y,x))$ (associativity)

Example. The additive formal group law, $F_a(x,y) = x + y$.

Example. The multiplicative formal group law, $F_m(x,y) = x + y + uxy$ for some unit $u \in R$, and specifically $F_m(x,y) = x + y + xy$.

Lemma. *$p(x) \in R[[x]]$ is (multiplicatively) invertible if and only if $p(0) \in R$ is invertible.*

Proof. Let $p(x) = \sum a_n x^n$, and assume $q(x) = \sum b_n x^n \in R[[x]]$ is an inverse to p, i.e. $pq = 1$. By comparing coefficients it follows that $a_0 b_0 = 1$ (so the first part follows), and $\sum_{k=0}^{n} a_k b_{n-k} = 0$. If a_0 is invertible then we can find a suitable q, by defining $b_0 = a_0^{-1}$, and $b_n = -a_0^{-1}\left(\sum_{k=1}^{n} a_k b_{n-k}\right)$ (so the second part follows). ☐

Definition. An *homomorphism* from F to G, two formal group laws over R, is a $f \in R[[x]]$, such that:

1. $f(0) = 0$
2. $f(F(x,y)) = G(f(x), f(y))$

Definition. The definition of a homomorphism between formal group laws, turns the collection of formal group laws over a ring into a category, denoted $\mathrm{FGL}(R)$.

TODO Should I mention the fact that there is a fully faithful functor $\mathrm{FGL}(R) \to \mathrm{Grp}$? (actually this is the way we define the homomorphisms)

Claim. *$f : F \to G$ is (compositionally) invertible (i.e. an isomorphism) if and only if $f'(0)$.*

Proof. It is easy to see the first implication. If $f'(0) = 0$, we can show explicitly that there exists a unique g such that $g(f(x)) = x$, and $g'(0) = (f'(0))^{-1}$. From the very same claim, it follows that there exists an h such that $h(g(x)) = x$, it follows that $h(x) = h(g(f(x))) = f(x)$. ☐

Definition. $f : F \to G$ is a *strict isomorphism* if $f'(0) = 1$.

Example. The multiplicative formal group law is strictly isomorphic to the additive formal group law, by $f(x) = u^{-1}\log(1+ux) = \sum_{n=1}^{\infty} \frac{(-u)^{n-1}x^n}{n}$:

$$\begin{aligned} f(F_m(x,y)) &= u^{-1}\log(1+uF_m(x,y)) \\ &= u^{-1}\log\left(1+ux+uy+u^2xy\right) \\ &= u^{-1}\log(1+ux)(1+uy) \\ &= u^{-1}\log(1+ux)+\log(1+uy) \\ &= F_a(f(x),f(y)) \end{aligned}$$

(Note that we don't need the u^{-1} to get an isomorphism, but we do need it to get a strict isomorphism.)

Definition. A strict isomorphism from F to F_a is called a *logarithm*.

2 Characteristic 0

Theorem. *A formal group law over a $\mathbb{Q}$-algebra has a logarithm.*

Proof. Let F be such a formal group law, and denote $F_2 = \frac{\partial F}{\partial y}$. Since $F(x,y) = x+y+\cdots$, we know that $F_2(0,0) = 1$, thus $F_2(t,0)$ is (multiplicatively) invertible. Since each $0 \neq n \in \mathbb{Z}$ is invertible, we can define the following:

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

We claim that it is a logarithm. We already know that $f'(0) = \frac{1}{F_2(0,0)} = 1$. We need to prove that $f(F(x,y)) = F_a(f(x),f(y))$, or equivalently, that $w(x,y) = f(F(x,y)) - f(x) - f(y)$ vanishes. Denote the coefficients by $w(x,y) = \sum c_{ij}x^iy^j$. First, note that $w(x,0) = f(F(x,0)) - f(x) - f(0) = f(x) - f(x) - 0 = 0$ and it follows that $c_{i0} = 0$. If we prove that

$$\begin{aligned} 0 &= \frac{\partial w}{\partial y} \\ &= f'(F(x,y))F_2(x,y) - f'(y) \\ &= \frac{1}{F_2(F(x,y),0)}F_2(x,y) - \frac{1}{F_2(y,0)} \end{aligned}$$

it follows that $jc_{ij} = 0$, and since each $0 \neq j \in \mathbb{Z}$ is invertible, $c_{ij} = 0, j > 0$, which finishes the proof. Indeed, by associativity, $F(F(x,y),z) = F(x,F(y,z))$, differentiating w.r.t. z at $z = 0$ we get, $F_2(F(x,y),0) = F_2(x,y)F_2(y,0)$ and the result follows. □

3 Characteristic p

Remark. The above theorem is not true over arbitrary rings.

To see this, we define a notion, that will lead us to the concept of height. Let F be a formal group law over a ring R. We define $[n]_F(x) \in R[[x]]$ by recursion:

$$[0]_F(x) = 0 \qquad [n+1]_F(x) = F(x,[n]_F(x))$$

Clearly, for $f : F \to G$ we get $f([n]_F(x)) = [n]_G(f(x))$. If no confusion will arise, we will denote $[n] = [n]_F(0)$.

For F_a we have $[n]_{F_a}(x) = nx$, and by induction for F_m we have $[n]_{F_a}(x) = (1+x)^n - 1$. Consider them over a field of characteristic p, and assume that $f : F_m \to F_a$ is an homomorphism then

$$0 = [p]_{F_a}(f(x)) = f\left([p]_{F_m}(x)\right) = f((1+x)^p - 1) = f(x^p)$$

which means that f is not invertible, thus F_m and F_a are not isomorphic.

Claim. *For all n, $[n]_F$ is an endomorphism of F.* ***TODO Comm. is used here***

Proof. It is trivial by definition that $[n](0) = 0$. The addition by induction. For $n = 0$ trivial. Now:

$$\begin{aligned}
[n](F(x,y)) &= F(F(x,y), [n-1](F(x,y))) \\
&= F(F(y,x), F([n-1](x), [n-1](y))) \\
&= F(y, F(x, F([n-1](x), [n-1](y)))) \\
&= F(y, F([n](x), [n-1](y))) \\
&= F(y, F([n-1](y), [n](x))) \\
&= F([n](y), [n](x)) \\
&= F([n](x), [n](y))
\end{aligned}$$

□

In what follows in this section, R is an $\mathbb{F}_p$-algebra.

Lemma. *Let F, G be formal group laws over F, and $f : F \to G$ non-trivial. Then $f(x) = g\left(x^{p^n}\right)$ for some n and $g \in R[[x]]$ with $g'(0) \neq 0$, and in particular the leading term of f is ax^{p^n}.*

Proof. If $f'(0) \neq 0$, we are done. Otherwise, we will find a formal group law $\tilde{F}$, and $\tilde{f} : \tilde{F} \to G$, such that $f(x) = \tilde{f}(x^p)$. Since f is non-trivial, and the least non-zero degree is lowered by this process, this process must terminate after a finite amount of stages. So suppose $f'(0) = 0$.

First we claim that $f'(x) = 0$. Deriving $f(F(x,y)) = F(f(x), f(y))$ by y and setting $y = 0$, we get $f'(F(x,0)) F_2(x,0) = F_2(f(x), f(0)) f'(0)$ remembering that $F(x,0) = x, F_2(x,0) = 1, f'(0) = 0$, we conclude that $f'(x) = 0$. Write $f(x) = \sum a_n x^n$, by $f'(x) = 0$, $a_n = 0$ for all $p \nmid n$, therefore $f(x) = \tilde{f}(x^p)$.

Denote by $\varphi : R \to R$ the Frobenius endomorphism $\varphi_i(x) = x^p$. Define $\tilde{F} = \varphi^*(F)$. It follows that $\tilde{f}\left(\tilde{F}(x^p, y^p)\right) = \tilde{f}(F(x,y)^p) = f(F(x,y)) = G(f(x), f(y)) = G\left(\tilde{f}(x^p), \tilde{f}(y^p)\right)$ i.e. that $\tilde{f} : \tilde{F} \to G$ is the desired homomorphism. **TODO How do we remove the ^{p}? I think it follows if we don't have nilpotents..** □

Definition. The *height* of a formal group law F over R is defined as follows: if $[p]_F = 0$, the height is ∞, otherwise it is the unique $n \in \mathbb{N}$ such that $[p]_F(x) = g\left(x^{p^n}\right)$ with $g'(0) \neq 0$.

Lemma. *The height is an isomorphism invariant.*

Proof. Let $f : F \to G$ be an isomorphism. We've seen that in that case $f([n]_F(x)) = [n]_G(f(x))$. Since f is an isomorphism, $f'(0)$ is a unit, the least non-zero degree is conserved and the result follows. □

TODO Existence for each height over a field, uniqueness over an algebraically closed field.

4 The Lazard Ring

Definition. Given an homomorphism $\varphi : R \to S$, and a formal group law over R, $F(x,y) = \sum a_{ij} x^i y^j$, we define the *base change* by $\varphi^*(F)(x,y) = \sum \varphi(a_{ij}) x^i y^j$. In fact, that is a functor, defined similarly for morphisms.

Theorem. *There is a ring L, called the* Lazard ring*, and a formal group law over it F_{univ}, called* the universal formal group law*, such that for every ring R the map*

$$\hom_{\text{Ring}}(L, R) \to \text{Ob}(\text{FGL}(R)) \qquad \varphi \mapsto \varphi^*(F_{\text{univ}})$$

is one-to-one and onto.

Proof. Look at the ring $\tilde{L} = \mathbb{Z}[c_{ij}]$, and $\tilde{F}_{\mathrm{univ}}(x,y) = \sum c_{ij} x^i y^j \in \tilde{L}[[x,y]]$. There are various relations obtained from the definition of a formal group law, e.g. $c_{0j} = 0 = c_{i0}$. Denote by I the ideal generated by these relations, and define $L = \tilde{L}/I$, and $F_{\mathrm{univ}}(x,y) = \sum (c_{ij} + I) x^i y^j \in L[[x,y]]$, which satisfies the definition of a formal group law over L by construction. The map being one-to-one is trivial. Given a formal group law $F(x,y) = \sum a_{ij} x^i y^j$, we can define $\tilde{\varphi} : \tilde{L} \to R$ by $\tilde{\varphi}(c_{ij}) = a_{ij}$, It is clear that if factors through L, to a map $\varphi : L \to R$, and that the base w.r.t $\varphi^*(F_{\mathrm{univ}}) = F$, therefore it is onto. $\square$

TODO Lazard's theorem?