The Algebraic Properties of Formal Group Laws

Shay Ben Moshe

20/06/2017

(All rings are commutative with unit.)

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

1. $F(x,0) = x = F(0,x)$
2. $F(x,y) = F(y,x)$ (commutativity)
3. $F(F(x,y),z) = F(x,F(y,x))$ (associativity)

Remark. The notation $x +_F y = F(x,y)$ is convenient sometimes.

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. $f(x +_F y) = f(x) +_G f(y)$

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 $f(x) = u^{-1}\log(1+ux) = \sum_{k=1}^{\infty} \frac{(-u)^{k-1}x^k}{k}$:

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

(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*.

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

Proof. Let F be such a formal group law, and denote $F_2 = \frac{\partial F}{\partial y}$. We claim that the following is a logarithm:

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

This is well-defined since each $0 \neq n \in \mathbb{Z}$ is invertible. We need to prove that $f(F(x,y)) = F_a(f(x), f(y))$, i.e. that $w(x,y) = f(F(x,y)) - f(x) - f(y)$ vanishes. Denote it's coefficients by $w(x,y) = \sum c_{ij} x^i y^j$. First, note that

$$\begin{aligned} w(x,0) &= f(F(x,0)) - f(x) - f(0) \\ &= f(x) - f(x) - 0 \\ &= 0 \end{aligned}$$

and it follows that $c_{i0} = 0$. If we prove that

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

then 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. $\square$