

# 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  $F(x, y) \in R[[x, y]]$ , 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  $b_n = -a_0^{-1} (\sum_{k=1}^n a_k b_{n-k})$  (so the second part follows).  $\square$

**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  $\text{FGL}(R)$ .

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

**Claim.**  $f : F \rightarrow G$  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  $h(x) = h(g(f(x))) = f(x)$ .  $\square$

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

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

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

(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  $F_2 = \frac{\partial F}{\partial y}$ . Since  $F(x, y) = x + y + \dots$ , we know that  $F_2(0, 0) = 1$ , thus it is (multiplicatively) invertible. Since each  $0 \neq n \in \mathbb{Z}$  is invertible, we can define the following:

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

We claim that it is a logarithm. We already know that  $f'(0) = F_2(0, 0) = 1$ . 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  $w(x, y) = \sum c_{ij} x^i y^j$ . 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  $j c_{ij} = 0$ , 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.  $\square$

*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:

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

Clearly, for  $f : F \rightarrow G$  we get  $f([n]_F(x)) = [n]_G(f(x))$ .

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  $f : F_m \rightarrow F_a$  is an homomorphism then

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

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

**Definition.** Given an homomorphism  $\varphi : R \rightarrow S$ , 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  $F_{\text{univ}}$ , called the universal formal group law, such that for every ring  $R$  the map

$$\text{hom}_{\text{Ring}}(L, R) \rightarrow \text{Ob}(\text{FGL}(R)) \quad \varphi \mapsto \varphi^*(F_{\text{univ}})$$

is one-to-one and onto.

*Proof.* Look at the ring  $\tilde{L} = \mathbb{Z}[c_{ij}]$ , and  $\tilde{F}_{\text{univ}}(x, y) = \sum c_{ij} x^i y^j \in \tilde{L}[[x, y]]$ . 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  $F_{\text{univ}}(x, y) = \sum (c_{ij} + I) x^i y^j \in L[[x, y]]$ , 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  $\tilde{\varphi} : \tilde{L} \rightarrow R$  by  $\tilde{\varphi}(c_{ij}) = a_{ij}$ . It is clear that if factors through  $L$ , to a map  $\varphi : L \rightarrow R$ , and that the base w.r.t  $\varphi^*(F_{\text{univ}}) = F$ , therefore it is onto.  $\square$