Formal Groups

Niki Myrto Mavraki

Contents

Abstract. In this note we give an introduction to the theory of formal group laws.

1. Introduction

Assume you want to define a group operation without some underlying set. Then, one might want to define the product z of x and y. One could try doing this by setting $z = F(x, y)$ for some power series F. We also want our group law to be associative, which translates into requiring the power series to satisfy $F(X, F(Y, Z)) = F(F(X, Y), Z)$. Lastly, we need an identity element, which means that we should also assume that $F(X, 0) = X$ and $F(0, Y) = Y$. It appears that we can assume that $F(X, Y) = X + Y +$(terms of degree ≥ 2). Then, our group law automatically guarantees that inverses exist.

Formal groups arise in Number Theory, Algebraic Topology and Lie Theory. In fact their origin lies in the theory of Lie groups. A Lie group is an n dimensional manifold endowed with a group structure. Once we choose coordinates around the identity element of the Lie group, the multiplication on the Lie group can be expressed using power series. This procedure gives us a formal group law. In characteristic 0, the formal group law and the Lie algebra happen to carry the same information, but this is not the case in characteristic p. In number theory, formal group laws play a crucial role in the study of elliptic curves and Dirichlet series of L-functions.

2. Some preliminaries

We will denote by $R[[T]]$ the ring of formal power series in T over a commutative ring R. Next we define a metric on $R[[T]]$.

Definition 2.1. *We define the following metric in* $R[[T]]$. *If* $f(T) = \sum_{i\geq 0} a_i T^i$ *and* $g(T) = \sum_{i\geq 0} b_i T^i$, *we set*

$$d(f,g) = \frac{1}{2^k},$$

where k *is the first* $k \in \mathbb{N}$ *so that* $a_k \neq b_k$. *We let* $\frac{1}{2^\infty} = 0$.

Remark 2.2. *It is easy to check that* $d : R[[T]] \times R[[T]] \to \mathbb{Z}_{\geq 0}$ *is actually a metric. In fact,* $(R[[T]], d)$ *is a complete metric space.*

3. Formal Groups (1 dimensional)

We denote by R a commutative ring with identity.

Definition 3.1. *A (one parameter) formal group* $\mathscr{F}$ *defined over* R *is a power series* $F(X,Y) \in R[[X,Y]]$ *satisfying:*

1. $F(X,Y) = X + Y +$*(terms of degree* ≥ 2*)*
2. $F(X, F(Y,Z)) = F(F(X,Y),Z)$ *(associativity)*

We call F *the formal group law of* $\mathscr{F}$. *If in addition we have that* $F(X,Y) = F(Y,X)$, *we say that* $\mathscr{F}$ *is a commutative formal group.*

Remark 3.2. *It is true that* (1) *and* (2) *imply that* $\mathscr{F}$ *is commutative, provided that* R *has no torsion nilpotents, meaning there is no element* $r \in R \setminus \{0\}$ *for which there exist* $n, m \in \mathbb{N}$ *so that* $r^n = mr = 0$. *We will see a proof of this fact when* R *has no non zero torsion elements in section 6. We say that* $r \in R$ *is a torsion element if there exists some* $n \in \mathbb{Z} \setminus \{0\}$ *so that* $nr = 0$.

Lemma 3.3. *For a formal group* $\mathscr{F}$ *defined over* R, *given by a power series* $F(X,Y) \in R[[X,Y]]$, *we also have*

1. $F(X,0) = X$ *and* $F(0,Y) = Y$.

(2) *There is a unique power series $i(T) \in R[[T]]$ such that $F(T, i(T)) = 0$.*

Proof. Part 1: Consider

$$F(X,Y) = X + Y + \sum_{i+j\geq 2} c_{ij}X^iY^j = f(X) + g(Y) + XYH(X,Y), \tag{1}$$

where

$$f(X) := F(X,0) = X + \sum_{i\geq 2} c_{i0}X^i,$$
$$g(Y) := F(0,Y) = Y + \sum_{j\geq 2} c_{0j}Y^j.$$

By associativity, we have that $F(X, F(0,Y)) = F(F(X,0), Y)$. Equivalently,

$$f(X) + g(g(Y)) + Xg(Y)H(X, g(Y)) = f(f(X)) + g(Y) + f(X)YH(f(X), Y).$$

Note here that the compositions of the power series above are still power series, since $f(0) = g(0) = 0$. Equating parts independent of X and parts independent of Y in this equation, we get that

$$f(X) = f(f(X)) \text{ and } g(Y) = g(g(Y)). \tag{2}$$

We will now see that this implies that $f(X) = X$. Similarly, we can get that $g(Y) = Y$. Assume the contrary, i.e. that there exists a smallest non zero $n \geq 2$ so that $c_{n0} \neq 0$. Then, equation (2) yields that

$$\sum_{i\geq 2} c_{i0}f(X)^i = 0, \tag{3}$$

or equivalently that

$$c_{n0}(X + c_{n0}X^n + \text{ terms of degree } \geq n+1)^n \tag{4}$$
$$+ \sum_{i\geq n+1} c_{i0}(X + \text{ terms of degree } \geq n)^i = 0.$$

Equating the coefficients of X^n on both sides of the above equation yields that $c_{n0} = 0$, contradicting its definition. Hence, $f(X) = X$. This finishes the proof.

Part 2:

Proof of existence of $i(T)$:

In view of part (1) above, we know that $F(X,Y)$ has the form

$$F(X,Y) = X + Y + \sum_{i\geq 1, j\geq 1} c_{ij} X^i Y^j. \tag{5}$$

Throughout this proof, we will denote by (T^n) the ideal of $R[[T]]$ generated by T^n, for $n \in \mathbb{N}$.

We will construct inductively a sequence of polynomials $\{g_n\}_{n\in\mathbb{N}}$, so that

$$g_{n+1}(T) - g_n(T) \in (T^{n+1}), \text{ and} \tag{6}$$

$$F(T, g_n(T)) \in (T^{n+1}). \tag{7}$$

Then, one can see that (6) yields $d(g_{n+1}, g_n) \leq \frac{1}{2^{n+1}}$. Using the usual telescopic trick then yields that $\{g_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence in the complete metric space $R[[T]]$. Hence, the limit $\lim\limits_{n\to\infty} g_n$ exists, and we will denote this by $i(T)$. Moreover, (7) implies that $d(F(T, g_n(T)), 0) \leq \frac{1}{2^{n+1}}$. Taking the limit as $n \to \infty$ in the last inequality gives that $d(F(T, \lim\limits_{n\to\infty} g_n(T)), 0) = 0$, or that $F(T, i(T)) = 0$, as desired.

We are now left to construct the sequence of polynomials $\{g_n\}_{n\in\mathbb{N}}$ with the desired properties.

For $n = 1$, we must have $g_1(T) = -T$. Then, we get that $F(T, g_1(T)) = \sum\limits_{i\geq 1, j\geq 1} c_{ij} T^i (-T)^j \in (T^2)$, as wanted. For the inductive step, assume that we have defined $g_n(T)$ so that $F(T, g_n(T)) \in (T^{n+1})$. We will now find some $\lambda \in R$, so that $g_{n+1}(T) = g_n(T) + \lambda T^{n+1}$ satisfies the property that $F(T, g_{n+1}(T)) \in (T^{n+2})$. Then obviously, we will have that $g_{n+1}(T) - g_n(T) \in (T^{n+1})$. Therefore, the inductive step will be done.

Notice that

$$\begin{aligned}F(T, g_n(T) + \lambda T^{n+1}) = \quad & T + g_n(T) + \lambda T^{n+1} \\ & + \sum_{i \geq 1, j \geq 1} c_{ij} T^i (g_n(T) + \lambda T^{n+1})^j \\ = \quad & T + g_n(T) + \lambda T^{n+1} + \sum_{i \geq 1, j \geq 1} c_{ij} T^i g_n(T)^j \\ & + \sum_{i \geq 1} c_{ij} T^i \sum_{j \geq k \geq 1} \binom{j}{k} g_n(T)^{j-k} (\lambda T^{n+1})^k \\ & = F(T, g_n(T)) + \lambda T^{n+1} \\ & + \sum_{i \geq 1} c_{ij} T^i \sum_{j \geq k \geq 1} \binom{j}{k} g_n(T)^{j-k} (\lambda T^{n+1})^k \quad (8)\end{aligned}$$

This in turn implies that

$$F(T, g_n(T) + \lambda T^{n+1}) - F(T, g_n(T)) - \lambda T^{n+1} \in (T^{n+2}). \quad (9)$$

Now, in light of the induction hypothesis, we have that there exists unique $a \in R$ so that

$$F(T, g_n(T)) - aT^{n+1} \in (T^{n+2}). \quad (10)$$

Adding (9) and (10), yields that

$$F(T, g_n(T) + \lambda T^{n+1}) - (\lambda + a)T^{n+1} \in (T^{n+2}). \quad (11)$$

We must now choose $\lambda = -a$ and define $g_{n+1}(T) = g_n(T) - aT^{n+1}$.

By induction, the proof is done.

Proof of uniqueness:

First note that by construction in the proof of existence there is a unique sequence of polynomials $\{g_n\}_{n \in \mathbb{N}}$ so that (6) and (7) are satisfied. Assume that for $a(T) = \sum_{i \geq 0} a_i T^i \in R[[T]]$ we have that $F(T, a(T)) = 0$. We will show that $a(T)$ is the unique power series satisfying this relation. Consider $a_n(T) = \sum_{0 \leq i \leq n} a_i T^i$ and note that $a(T) = \lim_{n \to \infty} a_n(T)$, where the limit is taken with respect to the metric d. We will see that the sequence of polynomials $\{a_n\}_{n \in \mathbb{N}}$ satisfies (6) and (7). Indeed, obviously from its definition $a_{n+1}(T) - a_n(T) = a_{n+1} T^{n+1}$ so (6) is satisfied. Moreover, using $F(X, Y)$

as defined in (5), we have

$$\begin{aligned} F(T, a_n(T)) &= F(T, a(T) - \sum_{s \geq n+1} a_s T^s) \\ &= T + a(T) - \sum_{s \geq n+1} a_s T^s + \sum_{i \geq 1, j \geq 1} c_{ij} T^i \left(a(T) - \sum_{s \geq n+1} a_s T^s \right)^j . \end{aligned}$$

This yields that there exists $h(T) \in R[[T]]$ such that

$$F(T, a_n(T)) = T + a(T) - \sum_{s \geq n+1} a_s T^s + \sum_{i \geq 1, j \geq 1} c_{ij} T^i (a(T))^j + T^{n+1} h(T).$$

This is equivalent to

$$F(T, a_n(T)) = T + a(T) - \sum_{s \geq n+1} a_s T^s + F(T, a(T)) - T - a(T) + T^{n+1} h(T).$$

Since $F(T, a(T)) = 0$ we get

$$F(T, a_n(T)) = - \sum_{s \geq n+1} a_s T^s + T^{n+1} h(T) \in (T^{n+1}).$$

Therefore, $\{a_n\}_{n \in \mathbb{N}}$ satisfies (7). Hence, as noted in the beginning of this proof $\{a_n\}_{n \in \mathbb{N}}$ is unique. Therefore, its limit $a(T) \in R[[T]]$ is the unique power series satisfying $F(T, a(T)) = 0$. □

Remark 3.4. *Note that in proposition 3.3 we do not need to assume that $\mathscr{F}$ is commutative.*

We proceed to provide some examples of formal groups.

Example 3.5. *$F(x, y) = x + y + cxy \in R[[x, y]]$ for some $c \in R$ is a formal group (associativity can be easily checked), whereas $F(x, y) = x + y + x^2 + y^2$ is not a formal group (even though $F(x, y) = F(y, x)$).*

One could ask the question whether there are other $F(x, y) \in R[x, y]$ that give rise to a formal group. It turns out the ones given in the preceding example are actually all such formal groups. We will establish this fact next.

Theorem 3.6. *If $F(x, y)$ is a formal group for some $F(x, y) \in R[x, y]$, then $F(x, y) = x + y + cxy$ for some $c \in R$.*

Proof. Assume that the greatest power of x appearing in $F(x, y)$ is n, whereas the greatest power of y is k, where $F(x, y) = x + y+$(terms of degree ≥ 2). Associativity forces $F(x, F(y,z)) = F(F(x,y),z)$. Notice that the greatest power of z appearing in the left hand side of this equation is k^2, whereas in the right hand side it is k. This yields that $k = k^2$. Similarly, the greatest power of x appearing in the left hand side of this equation is n, whereas in the right hand side it is n^2. This yields that $n = n^2$. Moreover $n + k \geq 2$. Therefore, $n = k = 1$. This now implies that $F(x,y)$ has the desired form. □

Example 3.7. *The formal additive group, denoted by $\hat{\mathbb{G}}_a$, is given by the formal group law $F(X,Y) = X + Y$.*

Example 3.8. *The formal multiplicative group, denoted by $\hat{\mathbb{G}}_m$, is given by the formal group law $F(X,Y) = X + Y + XY$.*

Definition 3.9. *Let $(\mathscr{F}, F)$ and $(\mathscr{G}, G)$ be formal groups defined over R. A* ***homomorphism*** *from $\mathscr{F}$ to $\mathscr{G}$ defined over R, is a power series (with no constant term) $f(T) \in R[[T]]$ satisfying*

$$f(F(X,Y)) = G(f(X), f(Y)).$$

Definition 3.10. *Two formal groups $(\mathscr{F}, F)$ and $(\mathscr{G}, G)$ defined over R are* ***isomorphic*** *over R, if there are homomorphisms $f : \mathscr{F} \to \mathscr{G}$ and $g : \mathscr{G} \to \mathscr{F}$ defined over R with*

$$f(g(T)) = g(f(T)) = T.$$

Example 3.11. *Let $(\mathscr{F}, F)$ be a formal group. We can define a map $[m] : \mathscr{F} \to \mathscr{F}$ for $m \in \mathbb{Z}$ inductively, as follows:*

$$[0](T) = 0 \text{ and } [m+1](T) = F([m]T, T).$$

Moreover, assuming $i(T)$ is the unique power series satisfying $F(T, i(T)) = 0$ as in Lemma 3.3, we define $[m-1](T) = F([m](T), i(T))$. We call $[m]$ the ***multiplication by m map****.*

We will see that the multiplication by m map is a formal group homomorphism. Actually $[m]$ is an $\mathscr{F}$ isomorphism, provided that $m \in R^*$. In that direction, we will prove the following Lemma.

Lemma 3.12. *Let $\alpha \in R^*$ and $f(T) \in R[[T]]$ a power series given as*

$$f(T) = \alpha T + (\text{ terms of degree} \geq 2).$$

Then, there is a unique power series $g(T) \in R[[T]]$ such that $f(g(T)) = T$. Moreover $g(f(T)) = T$.

Proof. Throughout the proof we denote by (T^n) the ideal of $R[[T]]$ generated by T^n, for $n \in \mathbb{N}$.

We will construct inductively a sequence of polynomials $\{g_n\}_{n\in\mathbb{N}}$ so that for all $n \in \mathbb{N}$

$$f(g_n(T)) - T \in (T^{n+1}). \tag{12}$$

$$g_{n+1}(T) - g_n(T) \in (T^{n+1}). \tag{13}$$

Then, (13) implies that $d(g_{n+1}, g_n) \leq \frac{1}{2^{n+1}}$, and using the usual telescopic tric this yields that $\{g_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence in the complete metric space $(R[[T]], d)$. Hence, the limit $\lim\limits_{n\to\infty} g_n = g$ exists. Now (12) yields that for all $n \in \mathbb{N}$, $d(f(g_n), T) \leq \frac{1}{2^{n+1}}$. Hence, letting $n \to \infty$ we get that $f(g(T)) = T$. This will finish the proof of the first statement of the lemma.

We will now construct $\{g_n\}_{n\in\mathbb{N}}$. For $n = 1$, we define $g_1(T) = \alpha^{-1}T$. Suppose now that g_{n-1} is defined. We will proceed to construct $g_n(T)$. In particular we will find a $\mu \in R$, so that $g_{n-1} + \mu T^n$ has the property $f(g_{n-1}(T) + \mu T) - T \in (T^{n+1})$. Then, we will set $g_n(T) = g_{n-1} + \mu T^n$.

Hence, we are left to find $\mu \in R$ so that

$$f(g_{n-1}(T) + \mu T) - T \in (T^{n+1}). \tag{14}$$

Notice that

$$f(g_{n-1}(T) + \mu T^n) - f(g_{n-1}(T)) - \alpha\mu T^n \in (T^{n+1}). \tag{15}$$

Moreover, in light of the induction hypothesis, we get that

$$f(g_{n-1}(T)) - T - \beta T^n \in (T^{n+1}), \tag{16}$$

for some $\beta \in R$. Adding now (15) and (16), we get that

$$f(g_{n-1}(T) + \mu T^n) - (\alpha\mu + \beta)T^n - T \in (T^{n+1}). \tag{17}$$

Leting now $\mu = -\beta \cdot \alpha^{-1} \in R$, we get that

$$f(g_{n-1}(T) + \mu T^n) - T \in (T^{n+1}). \tag{18}$$

This finishes the inductive step. By induction, the construction is done.

We will now see that also $g(f(T)) = T$.

Indeed note that by our construction $g(0) = 0$. Moreover we proved that $f(g(T)) = T$, which implies that $f'(0)g'(0) = 1$. Hence, since $f'(0) \in R^*$, we also have that $g'(0) \in R^*$. This now implies that $g(T) = bT +$

(terms of degree ≥ 2), for some $b \in R^*$. Therefore, as we proved, there exist some $h(T) \in R[[T]]$ so that $g(h(T)) = T$. Applying now f in this equation, we get that $f(g(h(T))) = f(T)$. This in turn implies that $h(T) = f(T)$. Therefore, $g(f(T)) = T$.

Next we will establish the uniqueness of $g(T)$.

Assume that there exists some $q(T)$ so that $f(q(T)) = T$. Applying g to this equation, yields that $g(f(q(T)) = g(T)$. This, in light of the fact that $g(f(T)) = T$, implies that $q(T) = g(T)$, yielding the uniqueness of the inverse. □

Proposition 3.13. *Let $\mathscr{F}$ be a formal group over R, and let $m \in \mathbb{Z}$. The following statements are true:*

(1) $[m]T = mT +$ (*higher order terms*).
(2) *If $m \in R^*$, then $[m] : \mathscr{F} \to \mathscr{F}$ is an isomorphism.*

Proof. Part 1: We will prove this statement inductively on m. First, we will prove for $m \in \mathbb{N}$. For $m = 0$, we have that $[0](T) = 0 = 0 \cdot T$ and the statement holds. Assume now that the statement holds for some $m \geq 1$. We will see that it also holds for $m + 1$. By definition,

$$[m+1](T) = F([m]T, T) = [m]T + T + (\text{ terms of degree} \geq 2).$$

The induction hypothesis now, yields that

$$\begin{aligned} [m+1](T) &= mT + (\text{ terms of degree} \geq 2) + T + (\text{ terms of degree} \geq 2) \\ &= (m+1)T + (\text{ terms of degree} \geq 2). \end{aligned}$$

Hence, by induction the statement is true. Similarly, using the recursive definition of the multiplication by m map, we get that the statement is also true all $m \in \mathbb{Z}$.

Part 2: This now is an immediate result of Part 1 and Lemma 3.12. □

4. Groups associated to formal groups

Generally a formal group resembles a group operation, with no actual underlying group. However, if the ring R is local and complete and the variables are assigned values from the maximal ideal, then the power series defining the formal group will converge in R, thus giving rise to a group. In this section we will talk about this group.

We will use the following notation:

Notation 4.1. *R a complete local ring*
$\mathcal{M}$ the maximal ideal of R
k the residue field $R/\mathcal{M}$
$\mathscr{F}$ a formal group defined over R with formal group law $F(x,y)$.

Definition 4.2. *The group associated to $\mathscr{F}/R$, denoted $\mathscr{F}(\mathcal{M})$, is the set $\mathcal{M}$ with the group operations*

$$x \oplus_{\mathscr{F}} y = F(x,y) \ (addition) \ for \ x, y \in \mathcal{M},$$

$$\ominus_{\mathscr{F}} x = i(x) \ (inverse) \ for \ x \in \mathcal{M}$$

The identity element of this group is 0, since Proposition 3.3, yields that

$$x \oplus_{\mathscr{F}} 0 = x, 0 \oplus_{\mathscr{F}} y = y$$

Remark 4.3.
(1) *For $n \geq 1$, we denote $\mathscr{F}(\mathcal{M}^n)$ the subset of $\mathscr{F}(\mathcal{M})$ consisting of the set $\mathcal{M}^n$.*
(2) *Note that since R is complete the power series $F(x,y)$ and $i(x)$ converge in R for $x, y \in \mathcal{M}$. The axioms of a formal group now imply that $\mathscr{F}(\mathcal{M})$ is a group and $\mathscr{F}(\mathcal{M}^n)$ a subgroup.*

Proposition 4.4.
(1) *For each $n \geq 1$, the map*

$$\mathscr{F}(\mathcal{M}^n)/\mathscr{F}(\mathcal{M}^{n+1}) \to \mathcal{M}^n/\mathcal{M}^{n+1}$$

induced by the identity map on sets is an isomorphism of groups.
(2) *Let p be the characteristic of k ($p = 0$ is allowed). Then every torsion element of $\mathscr{F}(\mathcal{M})$ has order a power of p.*

Proof. Part 1:

The fact that the given map is bijective is an immediate consequence of the fact that the underlying sets are the same (with different group operation). Hence, it suffices to prove that it is a group homomorphism. Equivalently, we have to show that for $x, y \in \mathcal{M}^n$

$$x \oplus y - (x + y) \in \mathcal{M}^{n+1}.$$

Recall that $x \oplus y = F(x,y) = x + y + ($ terms of order $\geq 2)$ Therefore for $x, y \in \mathcal{M}^n$

$$x \oplus y - (x + y) \in \mathcal{M}^{2n} \subseteq \mathcal{M}^{n+1}$$

This proves the statement.

Part 2:

Consider $x \in \mathscr{F}(\mathcal{M})$ a torsion element. Then, there exists $m \geq 1$ so that $[m]x = 0$. Without loss of generality we can assume that m is coprime with p, since otherwise, we can consider the torsion element $p^n x$, for an appropriate n, instead. We have to show that $x = 0$. Note that if $m = 1$, we have $x = 0$ and the statement is trivial. Therefore, we may assume that $m > 1$. Equivalently, we have to show that the group homomorphism

$$[m] : \mathscr{F}(\mathcal{M}) \to \mathscr{F}(\mathcal{M})$$

has kernel 0. Recall that p is characteristic of the residue field and note that since m is coprime with p by our assumption, we have that $m \notin \mathcal{M}$. Therefore, $m \in R^*$. Now, the result follows from Proposition 3.13. □

5. The Invariant Differential

In this section R is an arbitrary ring as in the beginning. We will introduce the notion of an invariant differential associated with the formal group $\mathscr{F}/R$. We will use the invariant differential to give a description for the multiplication by p map on $\mathscr{F}$, where $p \in \mathbb{Z}$ prime. In section 6 we will use the invariant differential to introduce the formal logarithm.

Definition 5.1. *An invariant differential on $\mathscr{F}/R$ is a differential form*

$$\omega(T) = P(T)dT \in R[[T]]dT$$

satisfying

$$\omega \circ F(T, S) = \omega(T).$$

Equivalently, this can be restated as

$$P(F(T, S))F_X(T, S) = P(T),$$

where $F_X(X, Y)$ is the partial derivative of F with respect to the first variable.

In the case when $P(0) = 1$, we say that the invariant differential is normalized.

Example 5.2. *On the additive formal group, an invariant differential is $\omega(T) = dT$.*

The following Proposition ensures the existence of an invariant differential in a formal group $\mathscr{F}/R$. Furthermore, it shows that if the invariant differential is normalized it is actually unique and has a prescribed form.

Proposition 5.3. *Consider $\mathscr{F}/R$ a formal group. Then, there* ***exists*** *a* ***unique*** *normalized invariant differential on $\mathscr{F}/R$. It is given as*

$$\omega(T) = F_X(0,T)^{-1}dT.$$

Moreover, every other invariant differential on $\mathscr{F}/R$ is of the form $a\omega$ for some $a \in R$.

Proof. Consider $\omega(T) = F_X(0,T)^{-1}dT \in R[[T]]dT$. We will show that it is an invariant differential. We have to check that

$$F_X(0,F(T,S))^{-1}F_X(T,S) = F_X(0,T)^{-1},$$

or equivalently that

$$F_X(0,F(T,S)) = F_X(T,S)F_X(0,T).$$

To see this recall that the formal group is associative, hence

$$F(U,F(T,S)) = F(F(U,T),S).$$

Differentiating this with respect to U and setting $U = 0$, we obtain

$$F_X(0,F(T,S)) = F_X(F(0,T),S)F_X(0,T).$$

This in light of the fact that $F(0,T) = T$ as seen in Lemma 3.3, yields the desired equality. Moreover, ω is normalized since $F_X(0,S) = 1 +$ (terms of degree ≥ 1).

Hence, we have seen that ω as defined in the Proposition is a normalized invariant differential on $\mathscr{F}/R$.

It remains to see that any invariant differential on $\mathscr{F}/R$ is of the form $a\omega$ for some $a \in R$. Note that this also yields that ω is the unique normalized invariant differential on $\mathscr{F}/R$.

Consider $\omega(T) = P(T)dT \in R[[T]]dT$ an invariant differential on $\mathscr{F}/R$. Then,

$$P(F(T,S))F_X(T,S) = P(T).$$

Setting $T = 0$ yields in light of Lemma 3.3 that

$$P(S)F_X(0,S) = P(0),$$

or, since $F_X(0,S) = 1 +$ (terms of degree ≥ 1) and hence invertible, that

$$P(S)dS = P(0)F_X(0,S)^{-1}dS.$$

Therefore, $\omega(S) = aF_X(0,S)^{-1}dS$, where $a = P(0) \in R$, as desired. This yields the result. □

The following Corollary of this Proposition will come in hand later.

Corollary 5.4. *Consider $\mathscr{F}/R$, $\mathscr{G}/R$ formal groups with normalized invariant differentials $\omega_{\mathscr{F}}$ and $\omega_{\mathscr{G}}$. Let $f : \mathscr{F} \to \mathscr{G}$ be a formal group homomorphism. Then,*

$$\omega_{\mathscr{G}} \circ f = f'(0)\omega_{\mathscr{F}}$$

Proof. Let $F(x,y)$, $G(x,y)$ be the formal group laws associated with $\mathscr{F}$ and $\mathscr{G}$ respectively. We will see that $\omega_{\mathscr{G}} \circ f$ is an invariant differential of $\mathscr{F}$. Then, in light of Proposition 5.3, since $\omega_{\mathscr{F}}$ is the normalized invariant differential of $\mathscr{F}$, we have that $\omega_{\mathscr{G}} \circ f = a\omega_{\mathscr{F}}$ for some $a \in R$. Comparing then initial terms, we get that $f'(0) = a$. This will imply the result.

To see that $\omega_{\mathscr{G}} \circ f$ is an invariant differential of $\mathscr{F}$, note that since f is a formal group homomorphism, we know that

$$\omega_{\mathscr{G}} \circ f(F(T,S)) = \omega_{\mathscr{G}}(G(f(T), f(S)).$$

Now since $\omega_{\mathscr{G}}$ is an invariant differential for $\mathscr{G}$, the latest equality implies that

$$(\omega_{\mathscr{G}} \circ f)(F(T,S)) = (\omega_{\mathscr{G}} \circ f)(T).$$

This in turn yields that $\omega_{\mathscr{G}} \circ f$ is an invariant differential for $\mathscr{F}$ as claimed. □

We will now provide a description for the multiplication by p map, where p is prime, associated to the formal group $\mathscr{F}$.

Corollary 5.5. *Let $\mathscr{F}/R$ be a formal group and $p \in \mathbb{Z}$ a prime number. Then, there exist power series $f(T), g(T) \in R[[T]]$ with $f(0) = g(0) = 0$ so that*

$$[p](T) = pf(T) + g(T^p).$$

Proof. In view of Proposition 3.13, we have that $[p]'(0) = p$. Combining this fact with Corollary 5.4, we get that

$$p\omega(T) = \omega \circ [p](T).$$

This in turn, yields that

$$p\omega(T) = (1 + ...)[p]'(T)dT.$$

Notice now that the series $(1 + ...)$ is invertible in $R[[T]]$. Therefore, the last equation implies that $[p]'(T) \in pR[[T]]$. Thus every term aT^n in the series of $[p](T)$ satisfies either $a \in pR$ or $p|n$, yielding the desired form for $[p](T)$. □

6. The Formal Logarithm

Let us first introduce a definition.

Definition 6.1. *We call a ring R torsion-free if it has no torsion elements, i.e. if $n \in \mathbb{Z}$ and $a \in R$ satisfy $na = 0$, then either $n = 0$ or $a = 0$.*

Recall from Example 3.7 that the formal additive group is given by the formal group law $F(X, Y) = X + Y$ and is denoted by $\hat{\mathbb{G}}_a$. In this section we will introduce the formal logarithm. This way we will get an isomorphism of a formal group defined over a torsion-free ring R with the additive group. As an application this yields that every one parameter formal group over a torsion-free ring is commutative.

In this section, R will be a torsion-free ring, commutative, with identity.

Definition 6.2. *Let R be a ring of characteristic 0, $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathscr{F}/R$ a formal group. Let*

$$\omega(T) = (1 + c_1 T + c_2 T^2 + c_3 T^3 + ...)dT$$

be the normalized invariant differential on $\mathscr{F}/R$. The ***formal logarithm*** *of $\mathscr{F}/R$ is the power series*

$$\int \omega(T) = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + ... \in K[[T]].$$

The ***formal exponential*** *of $\mathscr{F}/R$ is the unique power series $\exp_{\mathscr{F}}(T) \in K[[T]]$ satisfying*

$$\log_{\mathscr{F}} \circ \exp_{\mathscr{F}}(T) = \exp_{\mathscr{F}} \circ \log_{\mathscr{F}}(T) = T.$$

Note that the existence and uniqueness of the formal exponential is justified by Lemma 3.12.

Remark 6.3. *By its definition the formal logarithm of $\mathscr{F}/R$ is unique, since in view of Proposition 5.3, the normalized invariant differential of a formal group is unique.*

We will now prove the main Proposition of this section.

Proposition 6.4. *Let $\mathscr{F}/R$ be a formal group over a ring R with characteristic 0. Then,*

$$\log_{\mathscr{F}} : \mathscr{F} \to \hat{\mathbb{G}}_a$$

is an isomorphism of formal groups over $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proof. As noted in view of Lemma 3.12, there exists an inverse of $\log_{\mathscr{F}}$, namely $\exp_{\mathscr{F}}$. Therefore to prove that the map given in the statement of this proposition is an isomorphism of formal groups, it suffices to prove that it is a homomorphism. To see this, consider $\omega(T)$ the normalized invariant differential on $\mathscr{F}/R$. Then,

$$\omega(F(T,S)) = \omega(T).$$

Integrating this relation with respect to T, yields that

$$\log_{\mathscr{F}} F(T,S) = \log_{\mathscr{F}}(T) + f(S)$$

for some $f(S) \in K[[S]]$. Taking $T = 0$ and using Proposition 3.3, implies that $f(S) = \log_{\mathscr{F}}(S)$. Therefore,

$$\log_{\mathscr{F}} F(T,S) = \log_{\mathscr{F}}(T) + \log_{\mathscr{F}}(S).$$

Equivalently, we have seen that $\log_{\mathscr{F}} : \mathscr{F} \to \hat{\mathbb{G}}_a$ is a formal group homomorphism as claimed. □

We are now in shape to prove that formal groups over a torsion-free ring are commutative. This is the main application of this section.

Theorem 6.5. *Suppose that R is a torsion-free ring and $F(X,Y) \in R[X,Y]$ is a formal group law satisfying only axioms $(1), (2)$ in definition 3.1. Then, axiom (3) is also true, i.e.*

$$F(X,Y) = F(Y,X).$$

Proof. Note that in constructing the invariant differential, formal logarithm and formal exponential and proving their basic properties, we have only used the associativity of the formal group law and the fact that

$$F(X,0) = X \text{ and } F(0,Y) = Y.$$

This follows using only the first two axioms of the formal group, as presented in Proposition 3.3. Thus, as shown in Proposition 6.4, letting $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$ there exist $\log_{\mathscr{F}}, \exp_{\mathscr{F}} \in K[[T]]$ so that

$$F(X,Y) = \exp_{\mathscr{F}}^{(\log_{\mathscr{F}}(X) + \log_{\mathscr{F}}(Y))}.$$

In particular, $F(X,Y) = F(Y,X)$ in $K[[X,Y]]$. Note now that R is a torsion free ring as defined in 6.1, therefore it is embedded into $R \otimes_{\mathbb{Z}} \mathbb{Q}$ by the natural map mapping r to $r \otimes 1$. Moreover, $F(X,Y) \in R[[X,Y]]$. Therefore, $F(X,Y) = F(Y,X)$ in $R[[X,Y]]$ and $\mathscr{F}$ is commutative. □

Lemma 6.6. *Let R be a ring with characteristic 0 and let $f(T) = \sum_{n=1}^{\infty} \frac{a_n}{n!} T^n$ be a power series with $a_n \in R$ and $a_1 \in R^*$. Then, in light of proposition 3.12, there exists a unique power series satisfying $f(g(T)) = T$. We claim that it can be written as*

$$g(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!} T^n,$$

with $b_1 \in R^*$, $b_n \in R$.

Proof. Differentiating $f(g(T)) = T$ yields $f'(g(T))g'(T) = 1$. Letting $T = 0$ implies that

$$b_1 = g'(0) = \frac{1}{f'(0)} = \frac{1}{a_1} \in R^*.$$

Differentiating for a second time yields that

$$f'(g(T))g''(T) + f''(g(T))g'(T)^2 = 0$$

Letting $T = 0$ expresses $a_1 b_2$ as a polynomial a_1, a_2, b_1. Repeating this process shows that for every $n \geq 2$, $f'(g(T))g^{(n)}(T)$ can be expressed as a polynomial with integer coefficients in $f^{(i)}(g(T))$ and $g^{(j)}(T)$ for $1 \leq i \leq n$ and $1 \leq j \leq n-1$. Evaluating at $T = 0$ expresses $a_1 b_n$ as a polynomial in $a_1, ..., a_n, b_1, ..., b_{n-1}$. Since $a_1, b_1 \in R^*$ we see inductively that $b_n \in R$ for all $n \in \mathbb{N}$, as claimed. □

In view of this Lemma and the definition of the formal logarithm, we get the following proposition:

Proposition 6.7. *Let R be a ring with characteristic 0 and let $\mathscr{F}/R$ be a formal group. Then*

$$\log_{\mathscr{F}}(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n \text{ and } \exp_{\mathscr{F}}(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!} T^n,$$

with $a_n, b_n \in R$ and $a_1 = b_1 = 1$.

7. The n-dimensional formal group law

In this section we will see how to define a Lie bracket on the $n-$dimensional affine space using the n-dimensional formal group.

A formal group law of dimension n is given by a set of n power series $F_{(i)}$ of $2n$ variables $x_1, , x_n, y_1, , y_n$, satisfying $F_{(i)}(x,y) = x_i + y_i +$ (higher order terms). Moreover, letting $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$ and $F(x,y) = (F_{(1)}(x,y), \ldots, F_{(n)}(x,y))$, we demand further that $F(x, F(y,z)) = F(F(x,y),z)$.

We can now write

$$F(x,y) = x + y + B(x,y) + \text{terms of degree} \geq 3,$$

where $B(x,y) = (B_{(1)}(x,y), ..., B_{(n)}(x,y))$ is an n-tuple of quadratic polynomials in $x_1, ..., x_n, y_1, ..., y_n$. As in Lemma 3.3, we see that $B_{(i)}$ have the form

$$B_{(i)}(x,y) = \sum_{1 \leq p,q \leq n} c^i_{pq} x_p y_q.$$

Theorem 7.1. *We can define a Lie Algebra structure on the n dimensional affine space by means of this formula, as*

$$[x,y] = B(x,y) - B(y,x).$$

Proof. Obviously $[x,x] = 0$. Moreover, the fact that $B(x,y)$ has only degree 2 terms of the form $X_i Y_j$, ensures that it is bilinear. Hence, the Lie bracket as defined in the theorem is bilinear. It remains to check that the Jacobi identity is satisfied. Consider x, y, z in the $n-$dimensional affine space. We have to check that

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0.$$

Throughout the proof we will use ,without explicit mention, the fact that $B(x,y)$ is bilinear. Note that

$$\begin{aligned} [x,[y,z]] &= B(x,[y,z]) - B([y,z],x) \\ &= B(x,B(y,z)) - B(x,B(z,y)) - B(B(y,z),x) + B(B(z,y),x). \end{aligned} \tag{19}$$

For ease of notation, we write $C(x,y)$ for the degree 3 terms in $F(x,y)$. More specifically, $F(x,y) = x + y + B(x,y) + C(x,y) + \text{terms of degree} \geq 4$.

Associative of the formal group law, yields that

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

Equating now terms of degree < 4 in this equation, yields that

$$x + y + z + B(y, z) + B(x, y) + B(x, z) + B(x, B(y, z)) + C(y, z) + C(x, y + z)$$
$$= x + y + z + B(x, y) + B(x, z) + B(y, z) + B(B(x, y), z) + C(x, y) + C(x + y, z).$$

or equivalently that

$$B(x, B(y, z)) + C(y, z) + C(x, y + z) = B(B(x, y), z) + C(x, y) + C(x + y, z).$$

Thus,

$$s_1 = B(B(x, y), z) - B(x, B(y, z)) = C(y, z) - C(x, y) + C(x, y + z) - C(x + y, z). \tag{20}$$

Moreover

$$s_2 = B(B(z, y), x) - (B(z, B(y, x)) = C(y, x) - C(z, y) + C(z, y + x) - C(z + y, x). \tag{21}$$

$$s_3 = B(B(x, z), y) - (B(x, B(z, y)) = C(z, y) - C(x, z) + C(x, y + z) - C(x + z, y). \tag{22}$$

$$s_4 = B(B(y, x), z) - (B(y, B(x, z)) = C(x, z) - C(y, x) + C(y, x + z) - C(y + x, z). \tag{23}$$

$$s_5 = B(B(z, x), y) - (B(z, B(x, y)) = C(x, y) - C(z, x) + C(z, x + y) - C(z + x, y). \tag{24}$$

$$s_6 = B(B(y, z), x) - (B(y, B(z, x)) = C(z, x) - C(y, z) + C(y, x + z) - C(y + z, x). \tag{25}$$

An easy calculation shows that the Jacobi identity is equivalent to verifying that

$$-s_1 + s_2 + s_3 + s_4 - s_5 - s_6 = 0.$$

This is true and seen by adding the terms from (20), (21), (22), (23), (24), (25) with the appropriate signs and noting carefully all cancelations that occur.

□

Definition 7.2. *The Lie algebra defined as in Theorem 7.1 is called the* ***Lie algebra of the formal group law*** *$F(x, y)$.*

References

[1] Hazewinkel, M. Formal groups and applications, *AMS Chelsea Publishing, Providence, RI*, 2012.

[2] Silverman, J. H. The arithmetic of elliptic curves, *GTM 106, Springer*, 2009.