On 1-dimensional formal group laws in characteristic zero

Harald Fripertinger & Jens Schwaiger

June 5, 2014

Abstract

Let $\mathbb{K}$ be a field of characteristic zero or, more general, a $\mathbb{Q}$-algebra. A formal power series $F(x,y) = x+y+\sum_{i,j\geq 1} a_{i,j}x^iy^j \in \mathbb{K}[\![x,y]\!]$ is called a 1-dimensional formal group law if $F(F(x,y),z) = F(x,F(y,z))$. Using some elementary methods, we prove that for every 1-dimensional formal group law $F(x,y)$ there exists a formal power series $f(x) = x+\sum_{n\geq 2} f_nx^n \in \mathbb{K}[\![x]\!]$ so that $F(x,y) = f^{-1}(f(x)+f(y))$.

Formal group laws are completely described in Hazewinkel's monograph [2]. Consider a commutative ring A. A formal power series $F(x,y) \in A[\![x,y]\!]$ is called a 1-dimensional formal group law if

$$F(x,0) = x, \quad F(0,y) = y, \quad F(F(x,y),z) = F(x,F(y,z))$$

are satisfied. It is called commutative if $F(x,y) = F(y,x)$. Two formal group laws $F(x,y)$ and $G(x,y)$ are called strictly isomorphic, if there exists an invertible series $f(x) = x + \sum_{n\geq 2} f_nx^n \in A[\![x]\!]$, so that $f(F(x,y)) = G(f(x),f(y))$.

Using some elementary methods similar to those used in [1], we prove that every 1-dimensional formal group law $F(x,y)$ over $\mathbb{K}$, a field of characteristic zero or a $\mathbb{Q}$-algebra, is strictly isomorphic to $G(x,y) = x+y$. In other words, there exists a formal series $f(x) = x + \sum_{n\geq 2} f_nx^n \in \mathbb{K}[\![x]\!]$ so that $F(x,y) = f^{-1}(f(x)+f(y))$. Consequently, formal group laws over $\mathbb{K}$ of dimension 1 are all commutative. Using only elementary methods, we present two different proofs.

Remark 1 For the situation of formal group laws over $\mathbb{Q}$-algebras Hazewinkel's approach seems to be rather complicated. Here we present a short outline of his method. Let A be a ring of characteristic zero. This means that the natural map $A \to A\otimes\mathbb{Q}$ is injective. The series $f(x) = x + f_2x^2 + \ldots \in A\otimes\mathbb{Q}[\![x]\!]$ has an inverse f^{-1} with respect to substitution. Then $F(x,y) = f(f^{-1}(x)+f^{-1}(y))$ is a formal group law over $A\otimes\mathbb{Q}$. If $f(x)$ satisfies a certain functional equation, he calls it the functional equation-integrality lemma, the coefficients of F belong to A. Actually for each prime number p which is not invertible in A the series $f(x)$ must satisfy a certain equation. Solutions of the functional equation can be constructed in a recursive way.

Based on this method Hazewinkel first determines a universal group law $F_U(x,y)$ over $\mathbb{Z}[\![U]\!] := \mathbb{Z}[\![U_2, U_3, \ldots]\!]$ in indeterminates $U_2, U_3, \ldots$ The attribute "universal" means that for each formal group law $G(x,y)$ over a ring A there exists a unique ring-homomorphism $\phi\colon \mathbb{Z}[\![U]\!] \to A$, so that $G(x,y) = \phi_*(F_U(x,y)) = x + y + \sum_{i,j\geq 1} \phi(c_{i,j}) x^i y^j$, where $F_U(x,y) = x + y + \sum_{i,j\geq 1} c_{i,j} x^i y^j$. Then the tensor product with $\mathbb{Q}$ yields a homomorphism $\tilde{\phi}\colon \mathbb{Q}[U] \to A \otimes \mathbb{Q}$. Hazewinkel proves that there exists a power series $f_U(X) \in \mathbb{Q}[\![U]\!]$ so that $F_U(x,y) = f_U^{-1}(f_U(x) + f_U(y))$. Let $f(x) = \tilde{\phi}_*(f_U(x))$, then $f(x) \in A \otimes \mathbb{Q}$. Moreover, $F(x,y) = f^{-1}(f(x) + f(y))$ and $f(x) \equiv x \bmod x^2$. The power series f is uniquely determined by the last two properties. Therefore, the formal group laws in a $\mathbb{Q}$-algebra $\mathbb{K}$ are commutative and of the form $F(x,y) = f^{-1}(f(x) + f(y))$ for some $f(x) \in \mathbb{K}[\![x]\!]$ with $f(x) \equiv x \bmod x^2$.

We start with some preparatory lemmata. If $F(x,y)$ is a formal group law, then F can be written as

$$F(x,y) = \sum_{\substack{p,q\geq 0 \\ p+q\geq 1}} a_{p,q} x^p y^q$$

with suitable coefficients $a_{p,q} \in \mathbb{K}$, $a_{1,0} = a_{0,1} = 1$.

Lemma 2 *If $F(x,y) = \varphi_1(x) + \varphi_2(y) + xy\tilde{F}(x,y)$ is a 1-dimensional formal group law over $\mathbb{K}$, then $\varphi_1(x) = x = \varphi_2(x)$.*

Proof. From the associativity equation

$$F(F(x,y),z) = F(x,F(y,z)) \tag{AE}$$

we deduce that on the left hand side the subseries depending only on x is $\varphi_1(\varphi_1(x))$ and on the right hand side $\varphi_1(x)$. Hence $\varphi_1(\varphi_1(x)) = \varphi_1(x)$. Let $\psi(x) = \varphi_1(x) - x$, then $\psi(\varphi_1(x)) = 0$. Since $\varphi_1(x) \equiv x \bmod x^2$ we obtain $\psi(x) = 0$ which means that $\varphi_1(x) = x$. A similar proof can be done for $\varphi_2(x) = x$. □

Consequently $a_{n,0} = a_{0,n} = 0$ for $n \geq 2$ for all 1-dimensional formal group laws over $\mathbb{K}$.

Let k be a positive integer, then

$$F(x,y)^k = \sum_{\substack{p,q\geq 0 \\ p+q\geq 1}} A_{p,q}^{(k)} x^p y^q$$

where

$$A_{p,q}^{(k)} = \sum_{\substack{(p_1,\ldots,p_k) \\ (q_1,\ldots,q_k) \\ \sum p_\nu = p \\ \sum q_\nu = q \\ p_\nu + q_\nu > 0 \ \forall \nu}} \prod_{\nu=1}^{k} a_{p_\nu, q_\nu}$$

and where p_ν and q_ν are non-negative integers for $1 \le \nu \le k$. In the sequel we denote this sum as $\sum_{(p_\nu),(q_\nu)}^{k}$.

The situation $k = p+q$ implies that $p_\nu, q_\nu \in \{0,1\}$ and $p_\nu + q_\nu = 1$ for all $1 \le \nu \le k$. For $k < p+q$ the $A_{p,q}^{(k)}$ vanish, thus $F(x,y)^k = \sum_{\substack{p,q\ge 0\\ p+q\ge k}} A_{p,q}^{(k)} x^p y^q$.

Comparing the coefficients of $x^i y^j z$, $\min\{i,j\} \ge 1$, in (AE) we obtain

$$\sum_{p=1}^{i+j} a_{p,1} \sum_{(i_\nu),(j_\nu)}^{p} \prod_{\nu=1}^{p} a_{i_\nu,j_\nu} = \sum_{q=1}^{j+1} a_{i,q} \sum_{(j_\nu),(\sigma_\nu)}^{q} \prod_{\nu=1}^{q} a_{j_\nu,\sigma_\nu}$$

where $\sum_\nu \sigma_\nu = 1$.

Since $A_{j+1,1}^{(j+1)} = \binom{j+1}{1} = j+1$ we have

$$a_{i,j+1} = \frac{1}{j+1}\left(\sum_{p=1}^{i+j} a_{p,1} \sum_{(i_\nu),(j_\nu)}^{p} \prod_{\nu=1}^{p} a_{i_\nu,j_\nu} - \sum_{q=1}^{j} a_{i,q} \sum_{(j_\nu),(\sigma_\nu)}^{q} \prod_{\nu=1}^{q} a_{j_\nu,\sigma_\nu} \right). \tag{1}$$

Lemma 3 *All coefficients $a_{r,s}$ of a 1-dimensional formal group law over $\mathbb{K}$ with $s \ge 1$ are uniquely determined by $(a_{n,1})_{n\ge 1}$.*

Proof. For $s = 1$ there is nothing to prove. Assume that $s = 2$, then with $j = 1$ from (1) we get that

$$a_{r,2} = \frac{1}{2}\left(\sum_{p=1}^{r+1} a_{p,1} \sum_{(r_\nu),(j_\nu)}^{p} \prod_{\nu=1}^{p} a_{r_\nu,j_\nu} - a_{r,1}a_{1,1} \right)$$

and all coefficients $a_{n,m}$ on the right side satisfy $m \in \{0,1\}$.

If $s > 2$, then $j = s-1 > 1$. From (1) we get that

$$a_{r,s} = \frac{1}{j+1}\left(\sum_{p=1}^{r+j} a_{p,1} \sum_{(r_\nu),(j_\nu)}^{p} \prod_{\nu=1}^{p} a_{r_\nu,j_\nu} - \sum_{q=1}^{j} a_{r,q} \sum_{(j_\nu),(\sigma_\nu)}^{q} \prod_{\nu=1}^{q} a_{j_\nu,\sigma_\nu} \right)$$

and all coefficients $a_{n,m}$ on the right side satisfy $m \le j = s-1$. By induction they are uniquely determined by $(a_{n,1})_{n\ge 1}$. □

Lemma 4 *Consider an invertible power series $f(x) = x + \sum_{n\ge 2} f_n x^n \in \mathbb{K}[\![x]\!]$, then*

$$F(x,y) = f^{-1}(f(x) + f(y)) \tag{2}$$

is a formal group law $F(x,y) = \sum_{\substack{p,q\ge 0\\ p+q\ge 1}} a_{p,q} x^p y^q$ over $\mathbb{K}$. If we set $f_1 = 1$, then for $n \ge 2$ the coefficients f_n of f satisfy

$$0 = \sum_{j=1}^{n-1} j f_j a_{n-j,1} + n f_n. \tag{3}$$

Proof. Let $F(x,y)$ be given by (2), then $F(x,0) = f^{-1}(f(x)+0) = x$ and similarly $F(0,y) = y$. Moreover (AE) is satisfied since

$$\begin{aligned} F(F(x,y),z) &= f^{-1}\big(f(F(x,y)) + f(z)\big) \\ &= f^{-1}\big(f(f^{-1}(f(x)+f(y))) + f(z)\big) \\ &= f^{-1}\big(f(x)+f(y)+f(z)\big) \\ &= \ldots = F(x,F(y,z)). \end{aligned}$$

(2) is equivalent to

$$f(x)+f(y) = f(F(x,y)), \tag{2'}$$

whence

$$\sum_{n\geq 1} f_n(x^n+y^n) = \sum_{n\geq 1} f_n \sum_{\substack{p,q\geq 0\\ p+q\geq n}} A_{p,q}^{(n)} x^p y^q.$$

Comparison of all terms homogeneous of order n for $n \geq 1$ yields

$$f_n(x^n+y^n) = \sum_{j=1}^{n} f_j \sum_{p=0}^{n} A_{p,n-p}^{(j)} x^p y^{n-p}.$$

For $n \geq 2$ the coefficient of $x^{n-1}y$ in this expression is given by

$$0 = \sum_{j=1}^{n} f_j A_{n-1,1}^{(j)}.$$

Since $A_{n-1,1}^{(j)} = j a_{n-j,1} a_{1,0}^{j-1}$ and $a_{1,0} = a_{0,1} = 1$ we obtain (3). This formula allows to compute the coefficients f_n, $n \geq 2$, recursively from the coefficients $a_{n,1}$, $n \geq 1$, by

$$f_n = -\frac{1}{n} \sum_{j=1}^{n-1} j f_j a_{n-j,1}, \qquad n \geq 2 \tag{4}$$

and the proof is finished. □

Theorem 5 *The series $F(x,y) = \sum_{\substack{p,q\geq 0\\ p+q\geq 1}} a_{p,q} x^p y^q$ is a formal group law over $\mathbb{K}$, if and only if there exists some $f(x) = x + \sum_{n\geq 2} f_n x^n \in \mathbb{K}[\![x]\!]$ so that $F(x,y) = f^{-1}(f(x)+f(y))$. Moreover, f is uniquely determined by F.*

Proof. Let $F(x,y)$ be a formal group law. Then by (4) we determine the coefficients f_n, $n \geq 2$, of an invertible series $f(x) = x + \sum_{n\geq 2} f_n x^n \in \mathbb{K}[\![x]\!]$. According to Lemma 4 the series $G(x,y) = \sum_{\substack{p,q\geq 0\\ p+q\geq 1}} b_{p,q} x^p y^q = f^{-1}(f(x)+f(y))$ is a formal group law. Due to (3) the coefficients $a_{n,1}$ and $b_{n,1}$ coincide for all $n \geq 1$. According to Lemma 3 the coefficients of F and G are uniquely determined by the coefficients $(a_{n,1})_{n\geq 1}$ whence $a_{p,q} = b_{p,q}$ for all $p,q \geq 0$ and $F(x,y) = G(x,y) = f^{-1}(f(x)+f(y))$.

Conversely, according to Lemma 4 the series $f^{-1}(f(x)+f(y)$ is a formal group law.

If $F(x,y) = f^{-1}(f(x)+f(y)$ is a formal group law, then again by Lemma 4 the coefficients of f are uniquely determined by F. □

Another proof can be given as follows.

2nd Proof. We (only) show that any given 1-dimensional group law F is of the form (2) with some $f(x) = x + \sum_{n\geq 2} f_n x^n \in \mathbb{K}[\![x]\!]$ uniquely determined by F. As for the uniqueness assume that (2′) holds true. For $G \in \mathbb{K}[\![x,y]\!]$ we denote the partial derivatives with respect to x and y by D_1G and D_2G respectively. Then, using the chain rule for formal power series, differentiating (2′) with respect to x gives $f'(x) = f'(F(x,y))D_1F(x,y)$ which for $x = 0$ results in $1 = f'(y)D_1F(0,y)$ since $F(0,y) = y$ and $f'(0) = 1$. Observe that $D_1F(0,y)$ is a unit in $\mathbb{K}[\![y]\!]$. Thus $f'(y) = \frac{1}{D_1F(0,y)}$ and $f := \int \frac{1}{D_1F(0,y)}dy$ as that primitive series (integral) of $\frac{1}{D_1F(0,y)}$ which satisfies $f(0) = 0$, is uniquely determined.

Using this f, we have to show that $G(x,y) := f(F(x,y)) - f(x) - f(y) = 0$. To this aim we differentiate the associativity equation (AE) with respect to x:

$$D_1F(F(x,y),z)D_1F(x,y) = D_1F(x,F(y,z))$$

and (with $x = 0$) $D_1F(y,z)D_1F(0,y) = D_1F(0,F(y,z))$. Since $f'(y) = \frac{1}{D_1F(0,y)}$ this implies $D_1F(y,z)f'(F(y,z)) = f'(y)$. Now we differentiate G with respect to x:

$$D_1G(x,y) = f'(F(x,y))D_1F(x,y) - f'(x).$$

Thus $D_1G = 0$ and $G(x,y) = g(y) \in \mathbb{K}[\![y]\!]$. But $g(y) = G(0,y) = f(y) - f(y) = 0$. So $G = 0$ which means that (2) is satisfied. □

Remark 6 Theorem 5 becomes false if the characteristic p of $\mathbb{K}$ is greater than 0. $F(x,y) := x + y + xy$ is a 1-dimensional group law. If $f = \sum_{i=1}^{\infty} a_i x^i \in \mathbb{K}[\![x]\!], a_1 \neq 0$, satisfied (2′), f' would satisfy $f'(y)(1+y) = a_1$, implying $(i+1)a_{i+1} = (-1)^i a_1$ for all i. But this for $i = p-1$ would imply that $a_1 = 0$.

Acknowledgement. The authors want to thank Ludwig Reich for pointing their attention to this question and Franz Halter-Koch for fruitful discussion.

References

[1] Harald Fripertinger, Ludwig Reich, Jens Schwaiger, and Jörg Tomaschek. Associative formal power series in two indeterminates. *Semigroup Forum*, pages 1–12, 2013.

[2] Michiel Hazewinkel. *Formal groups and applications*. Academic Press, New York, San Francisco, London, 1978.

Institut für Mathematik und Wissenschaftliches Rechnen
Karl-Franzens-Universität Graz
Heinrichstr. 36/4
A–8010 Graz, AUSTRIA
harald.fripertinger@uni-graz.at
jens.schwaiger@uni-graz.at