Direct definition of the formal power series $\mathbb{K}$-algebra

Hiroyuki Yammae (24/4/2025)

We use notations as follows:

For sets A and B, let
$A \cup B := \{x \,|\, x \in A \text{ or } x \in B\}$ (the union)
$A \cap B := \{x \,|\, x \in A \text{ and } x \in B\}$ (the intersection)
$A^1 := A$, $A^2 := A \times A$, $A^3 := A \times A \times A = A^2 \times A$, ...

$A \setminus B := \{x \,|\, x \in A \text{ and } x \notin B\}$ (the set difference)
$A \times B := \{(a, b) \,|\, a \in A, b \in B\}$ (the Cartesian product)
If $A \cap B = \emptyset$, let $A \coprod B$ mean $A \cup B$ (the disjoint union (the direct union)).

As for sets of (some) numbers, we use the following notations

$\mathbb{N} := \{1, 2, 3, \ldots\}$ (the set of natural numbers)
$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ (the set of integers)
$\mathbb{Z}_{\geq 0} := \{z \in \mathbb{Z} \,|\, z \geq 0\} = \mathbb{N} \coprod \{0\}$ (the set of non-negative integers)
$\mathbb{Q} := \{\frac{m}{n} \,|\, m, n \in \mathbb{Z},\, n \neq 0\}$ (the set of rational numbers)
$\mathbb{R} := \{\lim_{n\to\infty} a_n \,|\, a_n \in \mathbb{Q}\,(n \in \mathbb{N}) \text{ and } \lim_{n\to\infty} a_n \text{ converges}\}$ (the set of rational numbers)
$\mathbb{R} := \{\lim_{n\to\infty} a_n \,|\, a_n \in \mathbb{Q}\,(n \in \mathbb{N}) \text{ and } \lim_{n\to\infty} a_n \text{ converges}\}$
$\mathbb{C} := \{a + ib \,|\, a, b \in \mathbb{R}\}$ (the set of complex numbers, where $i = \sqrt{-1}$)

We also use the following notations. For $x, y \in \mathbb{R}$, let $J_{x,y} := \{n \in \mathbb{Z} \,|\, x \leq n \leq y\}$.
For $x \in \mathbb{R}$, let $J_{x,\infty} := \{n \in \mathbb{Z} \,|\, n \geq x\}$ and $J_{-\infty,x} := \{n \in \mathbb{Z} \,|\, n \leq x\}$.

1 Elementary proof of the associative law of $A[[x]]$

For a set A, let

$$A^{\mathbb{Z}_{\geq 0}} := \{(a_k)_{k=0}^{\infty} = (a_0, a_1, a_2, \ldots) \,|\, a_k \in A\,(k \in \mathbb{Z}_{\geq 0})\}$$

(the set of infinite sequences in A whose first element is called the 0-th one).

Definition 1.1. Let $\mathbb{K}$ be a non-empty set. We call $\mathbb{K}$ *field* if the following maps $+$ and $\cdot$ are given and the following axioms ($\mathbb{K}$1)-($\mathbb{K}$10) are fulfilled, where $+$ and

$\cdot$ are called the sum and the multiplication respectively.

$$+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, (a, b) \mapsto a + b$$
$$\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, (a, b) \mapsto ab$$

($\mathbb{K}1$) $\forall a, \forall b, \forall c \in \mathbb{K}, \ (a + b) + c = a + (b + c)$
($\mathbb{K}2$) $\forall a, \forall b \in \mathbb{K}, \ a + b = b + a$
($\mathbb{K}3$) $\exists 0 \in \mathbb{K}, \ \forall a \in \mathbb{K}, \ a + 0 = a$
($\mathbb{K}4$) $\forall a \in \mathbb{K}, \ \exists - a \in \mathbb{K}, \ a + (-a) = 0$
($\mathbb{K}5$) $\forall a, \forall b, \forall c \in \mathbb{K}, \ (ab)c = a(bc)$
($\mathbb{K}6$) $\forall a, \forall b \in \mathbb{K}, \ ab = ba$
($\mathbb{K}7$) $\forall a, \forall b, \forall c \in \mathbb{K}, \ a(b + c) = ab + ac$
($\mathbb{K}8$) $\exists 1 \in \mathbb{K}, \ \forall a \in \mathbb{K}, \ 1a = a$
($\mathbb{K}9$) $\forall a \in \mathbb{K} \setminus \{0\}, \ \exists a^{-1} \in \mathbb{K}, \ aa^{-1} = 1$
($\mathbb{K}10$) $1 \neq 0$

Definition 1.2. Let $\mathbb{K}$ be a field. Let V be a non-empty set. We say thet V is a linear space over $\mathbb{K}$ if the following maps $+$ and $\cdot$ are given and the following axioms $(V1)$-$(V8)$ are fulfilled, where $+$ and $\cdot$ are called the sum and the scolor-product respectively.

$$+ : V \times V \to V, (x, y) \mapsto x + y$$
$$\cdot : \mathbb{K} \times V \to V, (a, x) \mapsto ax$$

$(V1)$ $\forall x, \forall y \in V, \ x + y = y + x$
$(V2)$ $\forall x, \forall y, \forall z \in V, \ (x + y) + z = x + (y + x)$
$(V3)$ $\exists 0 \in V, \ \forall x \in V, \ x + 0 = x$
$(V4)$ $\forall x \in V, \ \exists - x \in V, \ x + (-x) = 0$
$(V5)$ $\forall a \in \mathbb{K}, \ \forall x, \forall y \in V, \ a(x + y) = ax + ay$
$(V6)$ $\forall a, \forall b \in \mathbb{K}, \ \forall x \in V, \ (a + b)x = ax + bx$
$(V7)$ $\forall a, \forall b \in \mathbb{K}, \ \forall x \in V, \ (ab)x = a(bx)$
$(V8)$ $\forall x \in V, \ 1x = x$ ($1 = 1_{\mathbb{K}} \in \mathbb{K}$ is a unit of $\mathbb{K}$.)

Definition 1.3. Let $\mathbb{K}$ be a field.

(1) Let A be a linear space over $\mathbb{K}$. Let $+ : A \times A \to A$, $(a, b) \mapsto a + b$ and $\cdot : \mathbb{K} \times A \to A$, $(\lambda, a) \mapsto \lambda a$ be the sum and the scolor-product respectively. We say that A is an *associative* $\mathbb{K}$*-algebra* if the map $\cdot : A \times A \to A$, $(a, b) \to ab$, called the multiplication, is given and fulfills the following axioms $(A1)$-$(A5)$, where the symbol $\cdot$ is the same as that of the scolor-product.

$(A1)$ $\forall a, \ \forall b, \ \forall c \in A, \ (ab)c = a(bc)$
$(A2)$ $\forall a, \ \forall b, \ \forall c \in A, \ a(b + c) = ab + ac$
$(A3)$ $\forall a, \ \forall b, \ \forall c \in A, \ (a + b)c = ac + bc$
$(A4)$ $\exists 1 = 1_A \in A, \ \forall a \in A, \ 1a = a1 = a$

(A5) $\forall \lambda \in \mathbb{K}$, $\forall a$, $\forall b \in A$, $\lambda(ab) = (\lambda a)b = a(\lambda b)$

(2) Let A be an associative $\mathbb{K}$-algebra. Let B be a subset of A. We say that B is a $\mathbb{K}$-*subalgebra* of A if B is a linear $\mathbb{K}$-subspace of A, $1 \in B$, and $uv \in B$ for all u, $v \in B$.

(3) Let A and B be associative $\mathbb{K}$-algebras. Let $f : A \to B$ be a $\mathbb{K}$-linear homomorphism. We say that f is a $\mathbb{K}$-*algebra homomorphism* if $f(1_A) = 1_B$ and $f(uv) = f(u)f(v)$ $(u, v \in A)$. For a $\mathbb{K}$-linear homomorphism $f : A \to B$ is a $\mathbb{K}$-linear homomorphism, if f is bijective, we say that f is a $\mathbb{K}$-*algebra isomorphism*. Notice that for a $\mathbb{K}$-algebra isomorphism $f : A \to B$, $f^{-1} : B \to A$ is also a $\mathbb{K}$-algebra isomorphism.

(4) Let $f : A \to B$ be a $\mathbb{K}$-algebra homomorphism. Let $\mathrm{Im}(f) := \{f(u) | u \in A\}$. We call $\mathrm{Im}(f)$ the *image of* f. Notice that $\mathrm{Im}(f)$ is the $\mathbb{K}$-subalgebra of A. If f is injective, then we often identify A with $\mathrm{Im}(f)$. Whenever identify A and $\mathrm{Im}(f)$, we identify u and $f(u)$ for $u \in A$.

Definition 1.4. Let $\mathbb{K}$ be a field. Let A be an associative $\mathbb{K}$-algebra. For m, $n \in \mathbb{Z}$ and $a_k \in A$ $(k \in J_{m,n})$, let

$$\sum_{k=m}^{n} a_k := \begin{cases} 0 & \text{if } m > n, \\ a_m & \text{if } m = n, \\ (\sum_{k=m}^{n-1} a_k) + a_n & \text{if } m < n. \end{cases}$$

We can easily see the following Lemma 1.5.

Lemma 1.5. *Let $\mathbb{K}$ be a field. Let A be an associative $\mathbb{K}$-algebra. Let $n \in \mathbb{N}$ and a_i, $b_i \in A$ $(i \in J_{1,n})$.*

(1) *For $m \in J_{1,n}$, we have $(\sum_{i=1}^{m} a_i) + \left(\sum_{j=m+1}^{n} a_j\right) = \sum_{k=1}^{n} a_k$.*

(2) *For a bijection $\sigma : J_{1,n} \to J_{1,n}$, we have $\sum_{k=1}^{n} a_{\sigma(k)} = \sum_{i=1}^{n} a_i$.*

(3) *We have $\sum_{i=1}^{n}(a_i + b_i) = \left(\sum_{j=1}^{n} a_j\right) + (\sum_{k=1}^{n} b_k)$.*

(4) *For $c \in A$, we have $c \cdot (\sum_{i=1}^{n} a_i) = \sum_{i=1}^{n} ca_i$ and $(\sum_{i=1}^{n} a_i) \cdot c = \sum_{i=1}^{n} a_i c$.*

The following Lemma 1.6 is the most essential in this note.

Lemma 1.6. *Let $\mathbb{K}$ be a field. Let A be an associative $\mathbb{K}$-algebra.*

Let a_i, b_i, $c_i \in A$ $(i \in \mathbb{Z}_{\geq 0})$

For $n \in \mathbb{Z}_{\geq 0}$, we have the equation $(\#)_n$ below.

$$(\#)_n \qquad \sum_{k=0}^{n} a_k \left(\sum_{r=0}^{n-k} b_r c_{n-k-r}\right) = \sum_{s=0}^{n} \left(\sum_{t=0}^{s} a_t b_{s-t}\right) c_{n-s}$$

Proof. If $n = 0$, we have $a_0(b_0c_0) = (a_0b_0)c_0$ by ($\mathbb{K}$5) of Definition 1.1 whence $(\#)_0$ holds.

Assume $n \geq 1$. Let $c'_i := c_{i+1}$ ($i \in \mathbb{Z}_{\geq 0}$). Then we have:

$$
\begin{aligned}
&\textstyle\sum_{k=0}^{n} a_k \left(\sum_{r=0}^{n-k} b_r c_{n-k-r}\right) \\
&= \left(\textstyle\sum_{k=0}^{n-1} a_k \left(\sum_{r=0}^{n-k} b_r c_{n-k-r}\right)\right) + a_n(b_0c_0) \quad \text{(by the definition of } \Sigma) \\
&= \left(\textstyle\sum_{k=0}^{n-1} a_k \left(\left(\sum_{r=0}^{n-k-1} b_r c_{n-k-r}\right) + b_{n-k}c_0\right)\right) + a_n(b_0c_0) \quad \text{(by the definition of } \Sigma) \\
&= \left(\textstyle\sum_{k=0}^{n-1} \left(a_k \left(\sum_{r=0}^{n-k-1} b_r c_{n-k-r}\right) + a_k(b_{n-k}c_0)\right)\right) + a_n(b_0c_0) \\
&\qquad \text{(By (}\mathbb{K}\text{7) of Definition 1.1)} \\
&= \left(\left(\textstyle\sum_{k=0}^{n-1} \left(a_k \left(\sum_{r=0}^{n-k-1} b_r c_{n-k-r}\right)\right)\right) + \left(\sum_{k=0}^{n-1} a_k(b_{n-k}c_0)\right)\right) + a_n(b_0c_0) \\
&\qquad (\because \text{公式 } \textstyle\sum_{i=0}^{n-1}(\alpha_i + \beta_i) = (\sum_{i=0}^{n-1} \alpha_i) + (\sum_{i=0}^{n-1} \beta_i)) \\
&= \left(\textstyle\sum_{k=0}^{n-1} \left(a_k \left(\sum_{r=0}^{n-k-1} b_r c_{n-k-r}\right)\right)\right) + \left(\left(\sum_{k=0}^{n-1} a_k(b_{n-k}c_0)\right) + a_n(b_0c_0)\right) \\
&\qquad \text{(by (}\mathbb{K}\text{1) of Definition 1.1)} \\
&= \left(\textstyle\sum_{k=0}^{n-1} \left(a_k \left(\sum_{r=0}^{n-k-1} b_r c_{n-k-r}\right)\right)\right) + \left(\sum_{k=0}^{n} a_k(b_{n-k}c_0)\right) \quad \text{(by the definition of } \Sigma) \\
&= \left(\textstyle\sum_{k=0}^{n-1} \left(a_k \left(\sum_{r=0}^{(n-1)-k} b_r c_{((n-1)-k-r)+1}\right)\right)\right) + \left(\sum_{k=0}^{n} a_k(b_{n-k}c_0)\right) \\
&= \left(\textstyle\sum_{k=0}^{n-1} \left(a_k \left(\sum_{r=0}^{(n-1)-k} b_r c'_{(n-1)-k-r}\right)\right)\right) + \left(\sum_{k=0}^{n} a_k(b_{n-k}c_0)\right) \quad \text{(by the definition of } c'_i) \\
&= \left(\textstyle\sum_{k=0}^{n-1} \left(a_k \left(\sum_{r=0}^{(n-1)-k} b_r c'_{(n-1)-k-r}\right)\right)\right) + \left(\sum_{k=0}^{n} (a_kb_{n-k})c_0\right) \quad \text{(By (}\mathbb{K}\text{5) of Definition 1.1)} \\
&= \left(\textstyle\sum_{s=0}^{n-1} \left(\sum_{t=0}^{s} a_t b_{s-t}\right) c'_{(n-1)-s}\right) + \left(\sum_{k=0}^{n} (a_kb_{n-k})c_0\right) \quad \text{(by induction, i.e., } (\sharp)_{n-1}) \\
&= \left(\textstyle\sum_{s=0}^{n-1} \left(\sum_{t=0}^{s} a_t b_{s-t}\right) c_{n-s}\right) + \left(\sum_{k=0}^{n} (a_kb_{n-k})c_0\right) \quad \text{(by the definition of } c'_i) \\
&= \textstyle\sum_{s=0}^{n} \left(\sum_{t=0}^{s} a_t b_{s-t}\right) c_{n-s} \quad \text{(by the definition of } \Sigma)
\end{aligned}
$$

□

By Lemma 1.6, we can easily obtain the following Theorem 1.7.

Theorem 1.7. *Let $\mathbb{K}$ be a field, and let A be a $\mathbb{K}$-algebra. Then $A^{\mathbb{Z}_{\geq 0}}$ is regarded as the $\mathbb{K}$-algebra by:*

(Sum)	$(a_i)_{i=0}^{\infty} + (b_i)_{i=0}^{\infty} = (a_i + b_i)_{i=0}^{\infty} \quad ((a_i)_{i=0}^{\infty}, (b_i)_{i=0}^{\infty} \in A^{\mathbb{Z}_{\geq 0}})$,
(Scalar product)	$\lambda(a_i)_{i=0}^{\infty} = (\lambda a_i)_{i=0}^{\infty} \quad (\lambda \in \mathbb{K}, (a_i)_{i=0}^{\infty} \in A^{\mathbb{Z}_{\geq 0}})$,
(Product)	$(a_i)_{i=0}^{\infty} \cdot (b_i)_{i=0}^{\infty} = (\sum_{j=0}^{i} a_j b_{i-j})_{i=0}^{\infty} \quad ((a_i)_{i=0}^{\infty}, (b_i)_{i=0}^{\infty} \in A^{\mathbb{Z}_{\geq 0}})$.

Definition 1.8. Keep the notation of Lemma 1.6.

(1) We write $A[[x]] := A^{\mathbb{Z}_{\geq 0}}$. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i \in A[[x]]$ ($a_i \in A$) mean the element $(a_i)_{i=0}^{\infty} \in A^{\mathbb{Z}_{\geq 0}} = A[[x]]$. We call such $f(x)$ the *formal power series* in A. We call $A[[x]]$ the *formal power series $\mathbb{K}$-algebra in A*.

(2) Define $\mathbb{K}$-algebra homomorphism $\iota : A \to A[[x]]$ by $\iota(u) := \sum_{i=0}^{\infty}(\delta_{i0}u)x^i$. We identify A and $\mathrm{Im}(\iota)$. We identify u and $\iota(u)$ for $u \in A$. For $n \in \mathbb{Z}_{\geq 0}$, let $x^n := \sum_{i=0}^{\infty}(\delta_{in})x^i$. Note $x^0 = 1_A = 1_{A[[x]]}$. Let $x := x^1$. Note $x^m x^n = x^{m+n}$

$(m, n \in \mathbb{Z}_{\geq 0})$. Define the $\mathbb{K}$-subalgebra $A[x]$ of $A[[x]]$ by

$$A[x] := \{\sum_{i=0}^{n} a_i x^i \,|\, n \in \mathbb{Z}_{\geq 0},\, a_i \in A\,(i \in J_{0,n})\}.$$

We call an element of $A[x] \setminus \mathbb{K} \cdot 1$ a *polynomial in A*. We we call $A[x]$ a *polynomial $\mathbb{K}$-algebra in A*.