

メモ (形式的冪級数) (書きかけ)

hos

2019 年 10 月 5 日

大事なこと：収束のことは考えない．その代わり，知らない演算をしない．

\mathbb{N} は非負整数全体の集合とする^{*1}．環と言ったら乗法の単位元の存在を仮定する．

1 形式的冪級数環

以降， R を可換環とする．

X を不定元として， R の加算個の直積 $\prod_{i \in \mathbb{N}} R$ の元 $(a_i)_{i \in \mathbb{N}}$ を形式的に $\sum_{i \in \mathbb{N}} a_i X^i$ (あるいは $a_0 + a_1 X + a_2 X^2 + \dots$) と書いたものの集合を $R[[X]]$ とする．この元を $a(X)$ のように書くこともある^{*2}． a_i を $a(X)$ の i 次の係数 (あるいは X^i の係数) と呼び， $[X^i]a(X)$ のように書く． 0 次の係数を定数項と呼ぶ．

$\sum_{i \in \mathbb{N}} a_i X^i, \sum_{i \in \mathbb{N}} b_i X^i \in R[[X]]$ に対し，加法と乗法を

$$\begin{aligned} \sum_{i \in \mathbb{N}} a_i X^i + \sum_{i \in \mathbb{N}} b_i X^i &:= \sum_{i \in \mathbb{N}} (a_i + b_i) X^i, \\ \left(\sum_{i \in \mathbb{N}} a_i X^i \right) \left(\sum_{i \in \mathbb{N}} b_i X^i \right) &:= \sum_{k \in \mathbb{N}} \left(\sum_{i, j \in \mathbb{N}, i+j=k} a_i b_j \right) X^k \end{aligned}$$

で定めると，可換環になることを示す．加法の単位元は $0 = 0 + 0X + 0X^2 + \dots$ ，乗法の単位元は $1 = 1 + 0X + 0X^2 + \dots$ ．乗法の結合法則のみやや非自明で， $\left(\left(\sum_{i \in \mathbb{N}} a_i X^i \right) \left(\sum_{i \in \mathbb{N}} b_i X^i \right) \right) \left(\sum_{i \in \mathbb{N}} c_i X^i \right)$ の m 次の係数が

$$\sum_{l, k \in \mathbb{N}, l+k=m} \left(\sum_{i, j \in \mathbb{N}, i+j=k} a_i b_j \right) c_k = \sum_{i, j, k \in \mathbb{N}, i+j+k=m} a_i b_j c_k$$

となることから従う．この可換環 $R[[X]]$ を， R 係数形式的冪級数環と呼ぶ．

さらに， $r \in R$ はそのまま $r + 0X + 0X^2 + \dots \in R[[X]]$ とみれるので，包含 $R \hookrightarrow R[[X]]$ により $R[[X]]$ は R 代数でもある．

例． $(1 + X)(1 + X + X^2 + X^3 + \dots) = 1 + 2X + 2X^2 + 2X^3 + \dots$ ．

^{*1} 普段は $\mathbb{Z}_{\geq 0}$ とかを使って \mathbb{N} という記号を避けようと思っているが， \sum の下にたくさん書くので仕方なく．

^{*2} 不定元を書かず単に a のように書くのも綺麗だが，今回は積と合成が混同しないことを重視．

$a(X) \in R[[X]]$ に対し, 集合 $a(X)R[[X]] := \{a(X)b(X) \mid b(X) \in R[[X]]\} \subseteq R[[X]]$ は $R[[X]]$ のイデアルである. $b(X), c(X) \in R[[X]]$ が $b(X) - c(X) \in a(X)R[[X]]$ を満たすことを $b(X) \equiv c(X) \pmod{a(X)}$ と書く. $n \in \mathbb{N}$ に対し, $\text{mod } X^n$ での合同は, n 次未満の係数が等しいことを表す.

例. $0 + 1X + 2X^2 + 3X^3 + 4X^4 + \cdots \equiv X + 2X^2 \pmod{X^3}$.

次の命題は, 突き詰めると環の位相の話になるが, 本稿では技術的な補題として用いる.

命題 1. $a(X), b(X) \in R[[X]]$ について, $a(X) = b(X)$ である必要十分条件は, 任意の $n \in \mathbb{N}$ に対して $a(X) \equiv b(X) \pmod{X^n}$ であること.

証明. (必要性) 明らか.

(十分性) 任意の $i \in \mathbb{N}$ に対し, $n = i + 1$ ととって $a(X) \equiv b(X) \pmod{X^{i+1}}$ なので, $a_i = b_i$ となる. \square

2 形式的 Laurent 級数環

$S = \{X^n \mid n \in \mathbb{N}\}$ は $R[[X]]$ の積閉集合であるから, 局所化 $S^{-1}R[[X]]$ が考えられる. これを $R((X))$ と書き, R 係数形式的 **Laurent** 級数環という. S は零因子を含まないので自然な $R[[X]] \rightarrow R((X))$ は単射であり, $R[[X]] \subseteq R((X))$ とみなせる.

局所化の構成を確認すれば, $R((X))$ の元は形式的に $\frac{\sum_{i \in \mathbb{N}} a_i X^i}{X^n} = \sum_{i \in \mathbb{N}} a_i X^{i-n}$ と書いてよく,

$$R((X)) = \left\{ \sum_{i \in \mathbb{Z}} a_i X^i \mid a_i \neq 0 \text{ なる } i \in \mathbb{Z}_{\leq 0} \text{ は有限個} \right\} = \left\{ \sum_{i \in \mathbb{Z}, i \geq m} a_i X^i \mid m \in \mathbb{Z} \right\}$$

である^{*3}. 環の演算は, $\sum_{i \in \mathbb{Z}, i \geq m} a_i X^i, \sum_{i \in \mathbb{Z}, i \geq n} b_i X^i \in R((X))$ に対し,

$$\begin{aligned} \sum_{i \in \mathbb{Z}, i \geq m} a_i X^i + \sum_{i \in \mathbb{Z}, i \geq n} b_i X^i &= \sum_{i \in \mathbb{Z}, i \geq \min\{m, n\}} (a_i + b_i) X^i, \\ \left(\sum_{i \in \mathbb{Z}, i \geq m} a_i X^i \right) \left(\sum_{i \in \mathbb{Z}, i \geq n} b_i X^i \right) &= \sum_{k \in \mathbb{Z}, k \geq m+n} \left(\sum_{i, j \in \mathbb{Z}, i \geq m, j \geq n, i+j=k} a_i b_j \right) X^k \end{aligned}$$

となる (1 式目では $i < m$ のとき $a_i = 0$, $i < n$ のとき $b_i = 0$ とする. 2 式目では内側の \sum が有限和となる).

$a(X) = \sum_{i \in \mathbb{Z}} a_i X^i \in R((X))$ に対し, $a_i \neq 0$ なる最小の $i \in \mathbb{Z}$ を $\text{ord}(a(X))$ で表す. ただし $\text{ord}(0) = \infty$ とする. $\text{ord}(a(X))$ 次を最低次と呼ぶ.

^{*3} 以降, $\sum_{i \in \mathbb{Z}} a_i X^i \in R((X))$ と書いたら $a_i \neq 0$ なる $i \in \mathbb{Z}_{\leq 0}$ は有限個であることも主張する.

R が整域ならば, $R[[X]]$ や $R((X))$ も整域であり (最低次の係数に注目する), $\text{ord}: R((X)) \rightarrow \mathbb{Z} \cup \{\infty\}$ は付値を与える.

3 乗法の逆元

環の単元とは, 乗法の逆元をもつ元のこと. 可逆元. 1 の約数.

命題 2. $\sum_{i \in \mathbb{N}} a_i X^i \in R[[X]]$ が単元であるための必要十分条件は, a_0 が R の単元であること.

証明. (必要性) $\sum_{i \in \mathbb{N}} b_i X^i \in R[[X]]$ が $\left(\sum_{i \in \mathbb{N}} a_i X^i\right) \left(\sum_{i \in \mathbb{N}} b_i X^i\right) = 1$ を満たすとする, 定数項を比較して, $a_0 b_0 = 1$ である.

(十分性) a_0 が単元のとき, $\sum_{i \in \mathbb{N}} b_i X^i \in R[[X]]$ を

$$\begin{aligned} b_0 &= a_0^{-1}, \\ b_i &= -a_0^{-1} \sum_{j \in \mathbb{N}, 1 \leq j \leq i} a_j b_{i-j} \quad (i \geq 1) \end{aligned}$$

として定めると, $\left(\sum_{i \in \mathbb{N}} a_i X^i\right) \left(\sum_{i \in \mathbb{N}} b_i X^i\right) = 1$ を満たす. □

$a(X) \in R[[X]]$ の乗法の逆元が存在するとき, それは一意なので, $a(X)^{-1}$ や $\frac{1}{a(X)}$ と書く.

例. $r \in R$ に対し, $(1 - rX)^{-1} = \sum_{i \in \mathbb{N}} r^i X^i$.

$a(X) = \sum_{i \in \mathbb{Z}} a_i X^i \in R((X)) \setminus \{0\}$ が単元であるための必要十分条件は, 最低次の係数が可逆であることで

ある. $m = \text{ord}(a(X))$ として, 逆元は $a(X)^{-1} = X^{-m} \left(\sum_{i \in \mathbb{Z}} a_i X^{i-m}\right)^{-1}$ で与えられる.

とくに, R が体ならば, $R((X))$ も体である.

ここまでで定めた加減乗除については, 一般の R 代数で成り立つことを用いて普通の計算ができるし, 普通の表記をする.

例. $a(X) \in R((X))$ に対して, $a(X)^2$ とは $a(X)a(X)$ のことであり, $a(X)^2$ の逆元は $(a(X)^{-1})^2$ であり $a(X)^{-2}$ と書く.

例. 正の整数 n に対し, $(1 - X)^{-n} = \sum_{i \in \mathbb{N}} \binom{i+n-1}{n-1} X^i$.

例. $\mathbb{Q}((X))$ において, $\frac{X}{X^2 + X^3} = X^{-1} - 1 + X - X^2 + X^3 - \dots$.

4 合成

形式的冪級数の合成は, X の部分に「代入」していいものは定数項が 0 でなければならない (すなわち, イデアル $XR[[X]]$ の元である) ことに注意を要する.

定義. $a(X) = \sum_{i \in \mathbb{N}, i \geq 1} a_i X^i \in XR[[X]]$ と $b(X) = \sum_{i \in \mathbb{N}} b_i X^i \in R[[X]]$ に対し, $b(X)$ と $a(X)$ の合成 $(b \circ a)(X)$ を

$$(b \circ a)(X) := \sum_{i \in \mathbb{N}} \left(\sum_{k \in \mathbb{N}, j_1, \dots, j_k \in \mathbb{N}, j_1, \dots, j_k \geq 1, j_1 + \dots + j_k = i} b_k a_{j_1} \cdots a_{j_k} \right) X^i$$

で定める. 内側の \sum について, $k \leq i$ が従うためこれは有限和である. 特に, $(b \circ a)(X)$ の定数項は b_0 である.

4 次以下の項を書き下すと

$$(b \circ a)(X) = b_0 + b_1 a_1 X + (b_1 a_2 + b_2 a_1^2) X^2 + (b_1 a_3 + 2b_2 a_1 a_2 + b_3 a_1^3) X^3 \\ + (b_1 a_4 + b_2(a_1 a_3 + a_2^2) + 3b_3 a_1^2 a_2 + b_4 a_1^4) X^4 + \dots$$

となる.

$(b \circ a)(X)$ の i 次の係数は, $b_k a(X)^k$ の i 次の係数を $k \in \mathbb{N}$ について足したものである. つまり, 形式的に $(b \circ a)(X) = \sum_{k \in \mathbb{N}} b_k a(X)^k$ と書きたいが, 右辺は $R[[X]]$ の元の無限和であり定義されておらず, 各係数ごとに有限和として定義できるための条件が $a(X)$ の定数項が 0 であることに他ならない. このとき, $k > i$ の項は i 次の係数に影響を与えない. 言い換えると,

命題 3. $a(X) = \sum_{i \in \mathbb{N}, i \geq 1} a_i X^i \in XR[[X]]$ と $b(X) = \sum_{i \in \mathbb{N}} b_i X^i \in R[[X]]$ に対し,

$$(b \circ a)(X) \equiv \sum_{k \in \mathbb{N}, k < n} b_k a(X)^k \pmod{X^n}$$

が成り立つ.

証明. $i \in \mathbb{N}$, $i < n$ に対し, $k \leq i$ ならば $k < n$ であるから,

$$\begin{aligned}
(b \circ a)(X) &\equiv \sum_{i \in \mathbb{N}, i < n} \left(\sum_{k \in \mathbb{N}, j_1, \dots, j_k \in \mathbb{N}, j_1, \dots, j_k \geq 1, j_1 + \dots + j_k = i} b_k a_{j_1} \cdots a_{j_k} \right) X^i \\
&= \sum_{i \in \mathbb{N}, i < n} \left(\sum_{k \in \mathbb{N}, k < n, j_1, \dots, j_k \in \mathbb{N}, j_1, \dots, j_k \geq 1, j_1 + \dots + j_k = i} b_k a_{j_1} \cdots a_{j_k} \right) X^i \\
&= \sum_{i \in \mathbb{N}, i < n} \left(\sum_{k \in \mathbb{N}, k < n} [X^i] b_k a(X)^k \right) X^i \\
&= \sum_{k \in \mathbb{N}, k < n} \left(\sum_{i \in \mathbb{N}, i < n} [X^i] b_k a(X)^k \right) X^i \\
&\equiv \sum_{k \in \mathbb{N}, k < n} b_k a(X)^k \pmod{X^n}
\end{aligned}$$

である. □

とくに, $a(X) = X$ ならば $(b \circ a)(X) = b(X)$ であることが命題 1 よりわかる.
合成を「代入」と考えたとき成り立ってほしい性質たちをさらに確認していく.

命題 4. $a(X) \in XR[[X]]$ は R 代数の準同型 $a^*: R[[X]] \rightarrow R[[X]]$; $b(X) \mapsto (b \circ a)(X)$ を定め, これは $a^*(X) = a(X)$ を満たす. すなわち, $b(X), c(X), d(X) \in R[[X]]$ に対し,

- (1) $b(X) + c(X) = d(X)$ ならば $(b \circ a)(X) + (c \circ a)(X) = (d \circ a)(X)$.
- (2) $b(X)c(X) = d(X)$ ならば $(b \circ a)(X)(c \circ a)(X) = (d \circ a)(X)$.
- (3) $b(X) = 1$ ならば $(b \circ a)(X) = 1$.
- (4) $b(X) = X$ ならば $(b \circ a)(X) = a(X)$.

証明. (1) 合成の定義から明らか.

(2) $a(X) = \sum_{i \in \mathbb{N}, i \geq 1} a_i X^i$ および $b(X) = \sum_{i \in \mathbb{N}} b_i X^i$, $c(X) = \sum_{i \in \mathbb{N}} c_i X^i$ とする. $n \in \mathbb{N}$ を任意にとる. 命題

3 より,

$$\begin{aligned}
(b \circ a)(X)(c \circ a)(X) &\equiv \left(\sum_{i \in \mathbb{N}, i < n} b_i a(X)^i \right) \left(\sum_{j \in \mathbb{N}, j < n} c_j a(X)^j \right) \\
&= \sum_{k \in \mathbb{N}, k < 2n} \left(\sum_{i, j \in \mathbb{N}, i, j < n, i+j=k} b_i c_j \right) a(X)^k \\
&\equiv \sum_{k \in \mathbb{N}, k < n} \left(\sum_{i, j \in \mathbb{N}, i+j=k} b_i c_j \right) a(X)^k \\
&= \sum_{k \in \mathbb{N}, k < n} d_k a(X)^k \\
&\equiv (d \circ a)(X) \pmod{X^n}
\end{aligned}$$

である. よって, 命題 1 より $(a \circ d)(X)(b \circ d)(X) = (c \circ d)(X)$ が従う.

(3) b_0 のみ 1 なので, $(b \circ a)(X) = \sum_{i \in \mathbb{N}} \left(\sum_{0=i} 1 \right) X^i = 1.$

(4) b_1 のみ 1 なので, $(b \circ a)(X) = \sum_{i \in \mathbb{N}} \left(\sum_{k_1 \in \mathbb{N}, k_1 \geq 1, k_1=i} a_{k_1} \right) X^i = \sum_{i \in \mathbb{N}} a_i X^i = a(X).$

□

命題 5. $a(X), b(X) \in XR[[X]]$ と $c(X) \in R[[X]]$ に対し, $(c \circ (b \circ a))(X) = ((c \circ b) \circ a)(X).$

証明. $c(X) = X$ のとき, 命題 4 (4) より,

$$(c \circ (b \circ a))(X) = (b \circ a)(X) = ((c \circ b) \circ a)(X)$$

である. すなわち $(b \circ a)^*(X) = (a^* \circ b^*)(X)$ である ($(b \circ a)(X)$ は形式的冪級数の合成, $a^* \circ b^*$ は R 代数の準同型の合成であることに注意する).

TODO ↓嘘!!! 生成されてない. 位相を入れて連続準同型なら決まる

$R[[X]]$ は X で生成されるので, 準同型は X の行き先で定まる. よって $(b \circ a)^* = a^* \circ b^*$ であり, 任意の $c(X)$ に対し

$$(c \circ (b \circ a))(X) = (b \circ a)^*(c(X)) = (a^* \circ b^*)(c(X)) = ((c \circ b) \circ a)(X)$$

となる.

□

これらの理解のもと, $(b \circ a)(X)$ を $b(a(X))$ とも書く. とくに, $b(0)$ は $b(X)$ の定数項に等しい.

例. $a(X) = \sum_{i \in \mathbb{N}} a_i X^i \in R[[X]]$ と正の整数 n に対し, $a(X^n) = \sum_{i \in \mathbb{N}} a_i X^{ni}.$

例. $a(X) = \frac{X}{1-X} = \sum_{i \in \mathbb{N}} X^{i+1} \in R[[X]]$ と $n \in \mathbb{N}$ に対し, $(\underbrace{a \circ \cdots \circ a}_n)(X) = \frac{X}{1-nX} = \sum_{i \in \mathbb{N}} n^i X^{i+1}$ (n 回合成を a^n と書くと $a^n(X)$ か $a(X)^n$ かかなり紛らわしいため避けている).

5 形式微分

多項式の微分を拡張して形式微分が定義できる. 記法についてはいくつかの流儀・用途がある.

定義. R 加群の準同型 $D: R((X)) \rightarrow R((X))$ を, $a(X) = \sum_{i \in \mathbb{Z}} a_i X^i \in R((X))$ に対し,

$$D(a(X)) = \sum_{i \in \mathbb{Z}} i a_i X^{i-1}$$

として定める. $D(a(X))$ を $a'(X)$ と書く. D を (X による) 形式微分と呼ぶ.

$0a_0X^{-1} = 0$ なので, D を $R[[X]]$ に制限すると R 加群の準同型 $D: R[[X]] \rightarrow R[[X]]$ が得られる.

D は R 加群としては準同型である (線型性を満たす) が R 代数の準同型ではない (積は保たない) ことに注意する. 積に関しては, 以下のいわゆる Leibniz rule を満たす:

命題 6. $a(X), b(X) \in R((X))$ に対し, $D(a(X)b(X)) = D(a(X))b(X) + a(X)D(b(X))$.

証明. $a(X) = \sum_{i \in \mathbb{Z}, i \geq m} a_i X^i, b(X) = \sum_{i \in \mathbb{Z}, i \geq n} b_i X^i$ ($m, n \in \mathbb{Z}$) とすると,

$$\begin{aligned} D(a(X)b(X)) &= D\left(\sum_{k \in \mathbb{Z}, k \geq m+n} \left(\sum_{i, j \in \mathbb{Z}, i \geq m, j \geq n, i+j=k} a_i b_j\right) X^k\right) \\ &= \sum_{k \in \mathbb{Z}, k \geq m+n} k \left(\sum_{i, j \in \mathbb{Z}, i \geq m, j \geq n, i+j=k} a_i b_j\right) X^{k-1} \\ &= \sum_{k \in \mathbb{Z}, k \geq m+n} \left(\sum_{i, j \in \mathbb{Z}, i \geq m, j \geq n, i+j=k} (i a_i b_j + j a_i b_j)\right) X^{k-1} \\ &= \left(\sum_{i \in \mathbb{Z}, i \geq m} i a_i X^{i-1}\right) \left(\sum_{j \in \mathbb{Z}, j \geq n} b_j X^j\right) + \left(\sum_{i \in \mathbb{Z}, i \geq m} a_i X^i\right) \left(\sum_{j \in \mathbb{Z}, j \geq n} j b_j X^{j-1}\right) \\ &= D(a(X))b(X) + a(X)D(b(X)) \end{aligned}$$

より成り立つ. □

合成に関しては、以下のいわゆる chain rule を満たす^{*4}：

命題 7. $a(X) \in XR[[X]]$ と $b(X) \in R[[X]]$ に対し、 $D((b \circ a)(X)) = b'(a(X))a'(X)$.

証明. $k \in \mathbb{N}$ に対し、 $D(a(X)^k) = ka(X)^{k-1}a'(X)$ である。これは、 $k = 0$ のときはよく、 $k \geq 1$ のときは命題 6 を $k - 1$ 回用いる。

$n \in \mathbb{N}$ を任意にとる。命題 3 より、 $(b \circ a)(X) \equiv \sum_{k \in \mathbb{N}, k < n} b_k a(X)^k \pmod{X^{n+1}}$ なので、

$$\begin{aligned} D((b \circ a)(X)) &\equiv D\left(\sum_{k \in \mathbb{N}, k < n} b_k a(X)^k\right) \\ &= \sum_{k \in \mathbb{N}, k < n} b_k D(a(X)^k) \\ &= \sum_{k \in \mathbb{N}, k < n} b_k \cdot ka(X)^{k-1}a'(X) \\ &= \left(\sum_{k \in \mathbb{N}, k < n} kb_k a(X)^{k-1}\right) a'(X) \pmod{X^n} \end{aligned}$$

となる。よって命題 1 より $D((b \circ a)(X)) = b'(a(X))a'(X)$ が従う。 □

例. $a(X) = \sum_{i \in \mathbb{Z}} a_i X^i \in R((X))$ に対し、 $a'(0) = a_1$ である。より一般に、 n 階微分 ($n \in \mathbb{Z}$) を考えると、 $a^{(n)}(X) = \underbrace{D(\cdots D(a(X)) \cdots)}_n$ として $a^{(n)}(0) = n!a_n$ である。

例. $(1 - X)^{-1} = \sum_{i \in \mathbb{N}} X^i$ について、 $D((1 - X)^{-1}) = \sum_{i \in \mathbb{N}, i \geq 1} iX^{i-1} = (1 - X)^{-2}$.

6 形式積分

この節では K を標数 0 の体とする。

微分の「逆操作」として積分を考えることができる。

^{*4} $b'(a(X))$ が $D(b(X))$ と $a(X)$ の合成であることに注意 (記法のせいで D で綺麗に書けない)。

定義. $a(X) = \sum_{i \in \mathbb{Z}} a_i X^i \in K((X))$ が $a_{-1} = 0$ を満たすとき,

$$I(a(X)) = \sum_{i \in \mathbb{Z}, i \neq -1} \frac{1}{i+1} a_i X^{i+1}$$

と定める. $I(a(X))$ を $\int a(X)dx$ とも書く. I を $(X$ による) 形式積分と呼ぶ.

I は部分 K 加群間の準同型 $\{a(X) \in K((X)) \mid [X^{-1}]a(X) = 0\} \longrightarrow \{a(X) \in K((X)) \mid [X^0]a(X) = 0\}$ を与える. また, I を $K[[X]]$ に制限すると K 加群の準同型 $I: K[[X]] \longrightarrow XK[[X]]$ が得られる.

命題 8. $a(X) \in K((X))$ に対し,

- (1) $I(D(a(X))) = a(X) - a(0)$.
- (2) $[X^{-1}]a(X) = 0$ ならば, $D(I(a(X))) = a(X)$.

証明. 定義より明らか. □

7 形式留数

微分で情報が落ちる部分に名前がついている.

定義. $a(X) \in R((X))$ に対し, $[X^{-1}]a(X)$ を $\text{Res}(a(X))$ とも書き, $a(X)$ の形式留数という.

$\text{Res}: R((X)) \longrightarrow R$ は R 準同型である.

命題 9. $a(X), b(X) \in XR[[X]]$ が $b(a(X)) = X, a(b(X)) = X$ を満たすとき, $m, n \in \mathbb{N}$ に対し,

$$m[X^m]b(X)^n = n[X^{-n}]a(X)^{-m}$$

が成り立つ.

証明. TODO: 体じゃなくて大丈夫? □

8 exp

この節では K を標数 0 の体とする.

定義. $\exp(X) \in R[[X]]$ を,

$$\exp(X) = \sum_{i \in \mathbb{N}} \frac{1}{i!} X^i$$

で定める.

定義から, $D(\exp(X)) = \exp(X)$ がわかる.

\exp を左から合成する写像 $\exp: XK[[X]] \rightarrow 1 + XK[[X]]$; $a(X) \mapsto \exp(a(X))$ は指数法則を満たす:

命題 10. $a(X), b(X) \in XK[[X]]$ に対し, $\exp(a(X) + b(X)) = \exp(a(X)) \exp(b(X))$.

証明. $a(X) = \sum_{i \in \mathbb{N}, i \geq 1} a_i X^i$, $b(X) = \sum_{i \in \mathbb{N}, i \geq 1} b_i X^i$ とする. $n \in \mathbb{N}$ を任意にとる. 命題 3 より,

$$\begin{aligned} \exp(a(X) + b(X)) &\equiv \sum_{k \in \mathbb{N}, k < n} \frac{1}{k!} (a(X) + b(X))^k \\ &= \sum_{k \in \mathbb{N}, k < n} \sum_{i, j \in \mathbb{N}, i+j=k} \frac{1}{i!j!} a(X)^i b(X)^j \\ &\equiv \left(\sum_{i \in \mathbb{N}, i < n} \frac{1}{i!} a(X)^i \right) \left(\sum_{j \in \mathbb{N}, j < n} \frac{1}{j!} b(X)^j \right) \\ &\equiv \exp(a(X)) \exp(b(X)) \pmod{X^n} \end{aligned}$$

となる (2 つ目の \equiv は $a(X)^i \equiv 0 \pmod{X^i}$, $b(X)^j \equiv 0 \pmod{X^j}$ を用いた). よって命題 1 より $\exp(a(X) + b(X)) = \exp(a(X)) \exp(b(X))$ が従う. \square

9 形式積分

10 log

11 合成逆

12 多変数

13 アルゴリズム

14 数え上げ