メモ (形式的冪級数)

hos

2019 年 9 月 17 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]．

1　形式的冪級数環

R を可換環とする[*2]．

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 $a_0 + a_1 X + a_2 X^2 + \cdots$) 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．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

$$\sum_{i\in\mathbb{N}} a_i X^i + \sum_{i\in\mathbb{N}} b_i X^i := \sum_{i\in\mathbb{N}} (a_i + b_i) X^i,$$

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

で定めると，可換環になることを示す．加法の単位元は $0 = 0 + 0X + 0X^2 + \cdots$，乗法の単位元は $1 = 1 + 0X + 0X^2 + \cdots$．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 $r + 0X + 0X^2 + \cdots \in R[[X]]$ とみれるので，包含 $R \longrightarrow R[[X]]$ により $R[[X]]$ は R 代数でもある．

> **例．** $(1+X)(1+X+X^2+X^3+\cdots) = 1 + 2X + 2X^2 + 2X^3 + \cdots$．

[*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のですが，$\sum$ の下にたくさん書くので仕方なく．

[*2] 環と言ったら乗法の単位元の存在を仮定します．

$a(X) \in R[[X]]$ 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，$\bmod X^n$ 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． □

2　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. $\displaystyle\sum_{i\in\mathbb{N}} a_i X^i \in R[[X]]$ 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）$\displaystyle\sum_{i\in\mathbb{N}} b_i X^i \in R[[X]]$ が $\displaystyle\left(\sum_{i\in\mathbb{N}} a_i X^i\right)\left(\sum_{i\in\mathbb{N}} b_i X^i\right) = 1$ を満たすとすると，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，$\displaystyle\sum_{i\in\mathbb{N}} b_i X^i \in R[[X]]$ を

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

として定めると，$\displaystyle\left(\sum_{i\in\mathbb{N}} a_i X^i\right)\left(\sum_{i\in\mathbb{N}} b_i X^i\right) = 1$ 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 $\dfrac{1}{a(X)}$ と書く．

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

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，$(1-X)^{-n} = \sum_{i \in \mathbb{N}} \binom{i+n-1}{n-1} X^i$.

3　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

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

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 a_0 である．

$(b \circ a)(X)$ 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，

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

である. □

合成を「代入」と考えたとき成り立ってほしい性質たちを確認していく.

命題 4. $a(X) \in XR[[X]]$ は R 代数の準同型 $a^* \colon R[[X]] \longrightarrow R[[X]];\, b(X) \longmapsto (b \circ a)(X)$ 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) $a(X) = \sum_{i \in \mathbb{N}} a_i X^i$, $b(X) = \sum_{i \in \mathbb{N}} b_i X^i$, $c(X) = \sum_{i \in \mathbb{N}} c_i X^i$ とする．$n \in \mathbb{N}$ を任意にとる．命題 3 より，

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

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，$(b\circ a)(X)=\displaystyle\sum_{i\in\mathbb{N}}\left(\sum_{0=i}1\right)X^i=1$.

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

□

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).

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

例. $a(X)=\dfrac{X}{1-X}=\displaystyle\sum_{i\in\mathbb{N}}X^{i+1}\in R[[X]]$ と $n\in\mathbb{N}$ に対し，$(\underbrace{a\circ\cdots\circ a}_{n})(X)=\dfrac{X}{1-nX}=\displaystyle\sum_{i\in\mathbb{N}}n^iX^{i+1}$ (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).

4　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 $D_X\colon R[[X]] \longrightarrow R[[X]]$ を，$a(X) = \sum_{i\in\mathbb{N}} a_i X^i \in R[[X]]$ に対し，

$$D_X a(X) = \sum_{i\in\mathbb{N},\, i\geq 1} i a_i X^{i-1}$$

として定める．$D_X a(X)$ を $a'(X)$ とも書く．D_X を X による **形式微分**と呼ぶ.

D_X 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，$D_X(a(X)b(X)) = (D_X a(X))b(X) + a(X)(D_X b(X))$.

証明. D_X が R 加群の準同型なので，R 加群としての基底についてのみ示せばよい．$a(X) = 1$ または $b(X) = 1$ のときは $D_X(1) = 0$ よりよい．$a(X) = X^m$, $b(X) = X^n$ $(m, n \in \mathbb{N},\, m, n > 0)$ のとき，

$$(D_X(X^m))b(X^n) + X^m(D_X(X^n)) = mX^{m-1}\cdot X^m + X^m \cdot nX^{n-1} = (m+n)X^{m+n-1} = D_X(X^{m+n})$$

より成り立つ. □

以下はいわゆる chain rule である.

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

証明. D_X が R 加群の準同型であることと命題 4 より，$b(X) = X^n$ $(n \in \mathbb{N})$ のときについて示せばよい．このとき命題 4 より $(b\circ a)(X) = a(X)^n$ である．$n = 0$ のときはよい．$n \geq 1$ のとき，命題 6 を繰り返し用いて，

$$D_X(b\circ a)(X) = D_X(a(X)^n) = na(X)^{n-1}a'(X) = b'(a(X))a'(X)$$

となりよい. □

例. $a(X) = \sum_{i\in\mathbb{N}} a_i X^i$ に対し，$D_X a(0) = a_1$ である．より一般に，n 階微分を考えると，$D_X^n a(0) = \underbrace{D_X \cdots D_X}_{n} a(0) = n! a_n$ である.

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

5 形式積分

6 exp

7 log

8 合成逆

9 多変数

10 形式的 Laurent 級数

11 アルゴリズム

12 数え上げ