

# 正標数の環における導分

七条 彰紀

2017 年 10 月 25 日

## 1 準備

定義 1.1 (Derivation,  $k$ -Derivation.)

$A :: \text{ring}$ ,  $M :: \text{module}$  とする. 任意の  $a, b \in A$  に対して次を満たす写像  $D : A \rightarrow M$  を derivation とよぶ.

- (i)  $D(a + b) = D(a) + D(b)$ .
- (ii)  $D(ab) = D(a) \cdot b + a \cdot D(b)$ .

(ii) は Leibniz Formula (or Rule) と呼ばれる. 以下, 必要に応じて  $D(a)$  を  $Da$  と表記する.

準同型  $f : k \rightarrow A$  によって  $A$  を  $k$ -module とみなせる時,  $D \circ f = 0$  を満たす derivation  $D$  を  $k$ -derivation と呼ぶ.

$\text{Der}(A, M)$  で  $A \rightarrow M$  の derivation 全体を表す.  $\text{Der}(A, A)$  は  $\text{Der}(A)$  と略す.  $\text{Der}_k(A, M)$  で  $A \rightarrow M$  の  $k$ -derivation 全体を表す.  $\text{Der}_k(A, A)$  は  $\text{Der}_k(A)$  と略す.

$\text{Der}(A, M), \text{Der}_k(A, M)$  が  $A$ -module になることは明らか.  $a \in A, n \geq 0$  について  $Da^n = na^{n-1}Da$  が成り立つことは帰納法を用いて簡単に示せる.

次が成り立つ.

命題 1.2

$A :: \text{ring}$ ,  $D \in \text{Der}(A)$ ,  $a, b \in A$ ,  $n \in \mathbb{Z}_{\geq 0}$  とする.

$$D^n(ab) = \sum_{i=0}^n \binom{n}{i} (D^i a)(D^{n-i} b).$$

ただし  $D^0 = \text{id}_A$  とする.

証明は  $n$  についての帰納法に拠る.

今,  $A :: \text{ring}$  が正標数  $n > 0$ <sup>†1</sup> を持つとしよう.  $n$  が素数ならば,  $\binom{n}{i}$  は  $i = 1, \dots, n-1$  について  $n$  の倍数であるから, 次が成り立つ.

$$D^n(ab) = (D^n a) \cdot b + a \cdot (D^n b). \quad (*)$$

すなわち,  $D^n \in \text{Der}(A)$  となる.

---

<sup>†1</sup>  $f : \mathbb{Z} \rightarrow A$  を唯一の写像  $1_{\mathbb{Z}} \mapsto 1_A$  とすると,  $f^{-1}((0)) = \ker f \subseteq \mathbb{Z}$  は  $\mathbb{Z}$  のイデアルであり, したがって  $\ker f = (n)$  となる  $n \in \mathbb{Z}_{\geq 0}$  が存在する. この  $n$  を  $A$  の標数と呼ぶ.  $A$  が整域, すなわち  $(0) \subseteq A$  が素イデアルならば,  $\ker f$  も素イデアルになり (可換環論の基本的命題), したがって標数  $n$  は素数になる.

## 2 (\*) の反例

一方,  $n$  が素数でない, すなわち合成数でない時には (\*) が成り立たないことがある.

### 例 2.1

$A = (\mathbb{Z}/4\mathbb{Z})[x], D = x \frac{d}{dx}$  とする. この場合,  $A$  の標数は 4. ただし  $\frac{d}{dx}$  は  $x$  についての通常の微分であり, 明示すれば  $\frac{d}{dx}x = 1, \frac{d}{dx}1 = 0$  を満たす.  $\frac{d}{dx} \in \text{Der}(A)$  と  $\text{Der}(A) \ni A\text{-module より } D \in \text{Der}(A)$ .  $Dx = x \cdot 1 = x$  だから,  $D^4(x^2)$  は次のように成る.

$$D^4(x^2) = D^3(D(x^2)) = D^3(2x^{2-1}(Dx)) = D^3(2x^2) = \cdots = 2^4x^2 = 0.$$

一方,  $D^4(x^2) = D^4(x \cdot x)$  と考えて (\*) の右辺を計算すると, 次のよう.

$$(D^4x) \cdot x + x \cdot (D^4x) = 2x^2 \neq 0.$$

なので (\*) は成立しない.

### 例 2.2

$n$  に加えて文字  $a, b$  を加えて更に一般化する.  $A = (\mathbb{Z}/n\mathbb{Z})[x], D = x \frac{d}{dx}$  とする. ある  $a, b > 0$  について  $(a+b)^n \neq a^n + b^n$  であるとしよう. この時, (\*) の反例がある:

$$D^n(x^a \cdot x^b) = (a+b)^n x^{a+b} \neq (a^n + b^n) x^{a+b} = D^n(x^a) \cdot x^b + x^a \cdot D^n(x^b).$$

一方, 次の命題が成立する.

### 命題 2.3

$n$  を正整数とする. 次は同値<sup>†2</sup>.

(1)  $\forall a, b \in \mathbb{Z}/n\mathbb{Z}, (a+b)^n = a^n + b^n.$

(2)  $\forall x \in \mathbb{Z}/n\mathbb{Z}, x^n = x.$

(3)  $n$  は素数または Carmichael 数.

(証明). (1)  $\implies$  (2) の証明は  $x = 1 + 1 + \cdots + 1$  とすれば出来るし, (2)  $\implies$  (1) の証明は  $x = a + b$  とすれば出来る. (2)  $\iff$  (3) は Fermat の小定理と Carmichael 数の定義である. ■

したがって, 以上の方法では  $n$  が Carmichael 数 (561, 1105, 1729, 2465, 2821, ...) であるときの (\*) の反例が作れない. しかし, 環  $A$  を多変数にすれば容易に (\*) の反例が作れる. というよりも, 一般の設定を具体的な環で再現できる.

### 例 2.4

$n$  を正整数とする.

$$A = (\mathbb{Z}/n\mathbb{Z})[x_0, \dots, x_n], \quad D = \sum_{i=0}^{n-1} x_{i+1} \frac{\partial}{\partial x_i}.$$

<sup>†2</sup> Pratibha Ghatage and Brian Scott(2005), *Exactly When Is  $(a+b)^n \equiv a^n + b^n \pmod{n}$ ?*, <http://www.jstor.org/stable/30044877>.

このようにすると,  $i = 0, \dots, n$  について  $D^i x_0 = x_i$  となる. したがって  $D^n(x_0 \cdot x_0)$  は次のようになる.

$$D^n(x_0 \cdot x_0) = x_0 x_n + \sum_{i=1}^{n-1} \binom{n}{i} x_i x_{n-i} + x_n x_0.$$

当然,  $i \neq j$  ならば  $x_i x_{n-i} \neq x_j x_{n-j}$  となる. したがって  $\sum$  の部分が 0 になるのは,  $i = 1, \dots, n-1$  について  $\binom{n}{i} \bmod n = 0$  となる時のみである. このことは, 次の主張の通り,  $n$  が素数であることと同値である.

### 命題 2.5

正整数  $n$  を考える.  $i = 1, \dots, n-1$  について次式が成り立つことと,  $n$  が素数であることは同値である.

$$\binom{n}{i} \bmod n = \frac{n!}{i!(n-i)!} \bmod n = 0.$$

(証明).

■( $\Rightarrow$ ).  $n$  を合成数とし,  $p$  をその素因数<sup>†3</sup> とする. また  $m = n/p$  とする.

$$\binom{n}{p} = \frac{n(n-1) \cdots (n-p+1)}{p!} = m \cdot \frac{(n-1) \cdots (n-p+1)}{(p-1)!}.$$

これが  $n$  の倍数であると仮定しよう.  $n = m \cdot p$  なので, 仮定により,  $\frac{(n-1) \cdots (n-p+1)}{(p-1)!}$  は  $p$  の倍数である. 特に  $(n-1) \cdots (n-p+1)$  が  $p$  の倍数. しかし  $p-1$  個の整数  $n-1, \dots, n-(p-1)$  はいずれも  $p$  と互いに素であるから, これはありえない.

■( $\Leftarrow$ ).  $n$  が素数であるとする. すると  $1 \leq i \leq n-1$  より,  $i!$  は  $n$  の倍数ではない.  $1 \leq i \leq n-1$  ならば  $1 \leq n-i \leq n-1$  だから,  $(n-i)!$  も同様. したがって  $i!(n-i)!$  は  $n$  の倍数ではなく,  $\binom{n}{i} = \frac{n!}{i!(n-i)!}$  は  $n$  の倍数. ■

## 3 (\*) の成立

標数  $n$  が合成数であっても (\*) が成り立つのはどんな場合か, という問に対しては次がひとつの答えを与える.

### 命題 3.1

$A, k :: \text{ring}, D \in \text{Der}_k(A)$  とする.  $A$  の標数  $n$  は合成数であるとする.  $A$  は次を満たすとする.

- (1)  $A$  の任意の元が  $G \subseteq A$  の元の積の  $k$  線型結合として書ける.
- (2)  $G$  の任意の元  $g$  について  $D^2 g = 0$ .

この時,  $D^n = 0$ . したがって任意の  $a, b \in A$  について (\*) の等号が成り立つ.

この命題の仮定のうち, 条件 (2) 以外は次のような環で成り立つ:  $k$  上の多項式環・形式的べき級数環, 及びその剰余環,  $k$  の元による局所化, テンソル積, 直積.

これは次の補題から得られる.

<sup>†3</sup> <https://www.anothermathblog.com/?p=72> では  $p$  を特に最小のものとしているが, 以下の通り, この仮定は不要である

**補題 3.2**

$A, k :: \text{ring}, D \in \text{Der}_k(A)$  とする.  $x \in A$  と  $n, k \in \mathbb{Z}_{\geq 0}$  について, 次が成り立つ.

$$D^k x^n = \sum_{i=0}^{k-1} \binom{k-1}{i} n^{i+1} x^{n-(i+1)} (Dx)^i (D^{k-i} x).$$

ここで  $n^{i+1} = n(n-1)\cdots(n-(i+1)+1)$  は降下階乗べきである.

$D \in \text{Der}_k(A)$  は  $k$  線形写像であること, 及び  $n^{i+1}$  が  $i = 0, \dots, k-1$  で  $(i+1)!$  の倍数に成ることに気をつければ, この補題から上の命題はすぐに出る.