正標数の環における導分

七条 彰紀

2017 年 10 月 20 日

定義 0.1 (Derivation, k-Derivation.)
A :: ring, M :: module とする．任意の $a, b \in A$ に対して次を満たす写像 $D : A \to M$ 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 $f : k \to A$ 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．

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

$\mathrm{Der}(A, M), \mathrm{Der}_k(A, M)$ 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 0.2
A :: ring, $D \in \mathrm{Der}(A)$, $a, b \in A$, $n \in \mathbb{Z}_{\geq 0}$ とする．

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

ただし $D^0 = \mathrm{id}_A$ とする．

証明は n についての帰納法に拠る．

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

$$D^c(ab) = (D^c a) \cdot b + a \cdot (D^c b). \tag{$*$}$$

すなわち，$D^c \in \mathrm{Der}(A)$ となる．

一方，c 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 0.3
$A = (\mathbb{Z}/4\mathbb{Z})[x], D = x\frac{d}{dx}$ 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

[†1] $f : \mathbb{Z} \to A$ 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 $\ker f = (c)$ となる $c \in \mathbb{Z}_{\geq 0}$ が存在する．この c を A の標数と呼ぶ．

り，明示すれば $\frac{d}{dx}x = 1, \frac{d}{dx}1 = 0$ を満たす．$\frac{d}{dx} \in \mathrm{Der}(A)$ と $\mathrm{Der}(A)$ :: A-module より $D \in \mathrm{Der}(A)$. $Dx = x \cdot 1 = x$ 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 0.4
文字 c を導入して一般化を試みる．$A = (\mathbb{Z}/c\mathbb{Z})[x], D = x\frac{d}{dx}$ とする．

$$D^c(x^2) = 2^cx^2, \quad 2x^2 = D^c(x) \cdot x + x \cdot D^c(x).$$

この二つはほとんどの c で異なり，そのとき $(*)$ の反例と成る．しかし，よく知られている通り，Fermat の小定理の逆には反例が存在する．なので，ここで与えた A, D は，例えば c が Carmichael 数 $(561, 1105, 1729, 2465, 2821, \dots)$ である場合についての $(*)$ の反例にならない．（他に例がないか探してみると，$c = 341(= 11 \cdot 31), 645, 1387, 1905, 2047$ でも反例にならない．）

例 0.5
$c > 0$ を **square-free** でない合成数とし，c の互いに異なる素因数の積を r とする．（r は c の radical と呼ばれる．）$c > r$ に注意せよ．$A = (\mathbb{Z}/c\mathbb{Z})[x], D = x^{r+1}\frac{d}{dx}$ とする．この時，$Dx = x^{r+1}$．$t \geq 1$ とすると，$D^c(x^t)$ は次のように成る．

$$D^c(x^t) = \delta_t x^{cr+t}, \quad \delta_t = \prod_{i=0}^{c-1}(ir + t).$$

したがって $D^c(x^r)$ は $\delta_r x^{(c+1)r} = c!r^c \cdot x^{(c+1)r}$．一方，$(*)$ の右辺は次のように成る．

$$D^c(x \cdot x^{r-1}) = D^c(x) \cdot x^{r-1} + x \cdot D(x^{r-1}) = (\delta_1 + \delta_{r-1})x^{(c+1)r}.$$

$c > r$ より $\delta_1 + \delta_{r-1}$ が c の倍数でないことが示される．（この証明は難しいと思われる．計算機で $c < 100$ の範囲で正しいことを確かめた．）よって $(*)$ が成立しない．

残念ながら，Carmichael 数は square-free である[†2]．上で挙げたその他の c も square-free である．標数が Carmichael 数ならば常に $(*)$ が成り立つ可能性もあるが，それは Future Work としよう．

標数 c 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 0.6
A, k :: ring, $D \in \mathrm{Der}_k(A)$ とする．A の標数 c 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 $D^2g = 0$.

[†2] `http://mathworld.wolfram.com/CarmichaelNumber.html` などを参照せよ．

この時，$D^c = 0$．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・形式的ベキ級数環，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．

補題 0.7

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

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

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

$D \in \mathrm{Der}_k(A)$ は k 線形写像であること，及び $n^{\underline{i+1}}$ が $i = 0, \ldots, k-1$ 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．