TAYLOR SERIES AND DIVISIBILITY

BY

A. A. EVYATAR† AND O. E. VILLAMAYOR

ABSTRACT

Let A be an augmented K-algebra; define $T: A \to A \otimes_K A$ by $T(a) = 1 \otimes a - a \otimes 1$, $a \in A$. We prove, under some conditions, that g is in the subalgebra $K[f]$ of A generated by f if and only if $T(g)$ is in the principal ideal generated by $T(f)$ in $A \otimes_K A$. When $A = K[[X]]$, $T(f)$ is a multiple of $T(X)$ if and only if f belongs to the ring L obtained by localizing $K[X]$ at (X).

Introduction

This paper is a sequel of [1].

We want to relate, by means of the Taylor series T, as defined in (1.1), the problem of studying the subalgebra generated by an element f to the study of the principal ideal generated by Tf.

We will consider commutative augmented K-algebras with unit. Denote such an algebra by A.

We can prove, under some conditions, that g is in the K-subalgebra $K[f]$ of A generated by f if and only if $T(g)$ is in the principal ideal generated by Tf in $A \otimes A$, which generalizes the result of [1].

In general, if S is the subalgebra of A of elements g such that $T(g)$ is in the ideal generated by $T(f)$, then S contains $K[f]$ and S is contained in the f-adic completion of such a subalgebra. We show an example in which both inclusions are proper: in the case $A = K[[X]]$, $T(f)$ is a multiple of $T(X)$ if and only if f belongs to the ring L obtained by localizing $K[X]$ at the prime ideal (X).

1. Notation

We fix, once and for all, a commutative ring with unit K, our "scalar ring" and will work in the category C of commutative K-algebras with unit element. Hence a map is a morphism in the category of K-algebras, unlabeled tensor products are taken over K, and so on.

† The work on this paper was done while A. Evyatar was in Buenos Aires under the auspices of the Mathematic Multinational Program of OAS.

Received June 5, 1973

If A is an augmented K-algebra, we will denote by $\gamma : A \to K$ the augmentation map. (Since γ is a K-algebra map, if $i : K \to A$ is the structure map, $\gamma i =$ identity.)

If $A \in \mathrm{Ob}C$, call $\epsilon_0 : A \to A \otimes A$ the map defined by $\epsilon_0(x) = 1 \otimes x$, let $\epsilon_1 : A \otimes A$ be defined by $\epsilon_1(x) = x \otimes 1$ and let $\mu : A \otimes A \to A$ be given by $\mu(x \otimes y) = xy$ (the multiplication map).

If A is augmented, define $\delta : A \otimes A \to A$ as $\delta = \mu \circ (i \otimes i) \circ (\gamma \otimes 1)$. Hence $\delta(1 \otimes a) = a$, $\delta(a \otimes 1) = i\gamma a$.

For $a \in A$, call $\tilde{a} = a - i\gamma a$, then $\tilde{a} \in \mathrm{Ker}\, \gamma$.

$A \otimes A$ will be considered on an A-module by left multiplication, i.e., $a \cdot (x \otimes y) = ax \otimes y$.

Definition 1.1. If $A \in \mathrm{Ob}C$, call $I = \mathrm{Ker}\, \mu$, then the (K-linear) map $T : A \to I$ given by $T(a) = 1 \otimes a - a \otimes 1$ satisfies the following conditions:

(a) T is K-linear,

(b) $T(xy) = xT(y) + yT(x) + T(x)T(y)$,

(c) T is universal for maps satisfying (a) and (b).

T will be called the canonical K-Taylor series of A.

For the properties of K-Taylor series, see [2], [3], and [4].

Remark 1.2. If $a \in A$, then $T(a) = T(\tilde{a})$. Indeed, since T is linear, and $\tilde{a} = a - i\gamma a$, and $i\gamma a \in iK$ we have $T(i\gamma a) = 0$.

2. Divisibility

Theorem 2.1. *Let A be a commutative K-algebra. Assume $f, g \in A$. If g is in the K-subalgebra $K[f]$ generated by f, then Tf divides Tg.*

Proof. Since for any $x, y \in A$ we have

$$T(xy) = xT(y) + y(Tx) + T(x)T(y), \text{ then}$$

$$T(x^n) = \sum \binom{n}{n-i} x^{n-i} [T(x)]^i,$$

and the statement follows.

Corollary 2.2. *Let $p, h \in K[f]$, h invertible in A. If $g = h^{-1} \cdot p$ then $T(f) | T(g)$.*

Proof. Write $hg = p$. Then $T(p) = hT(g) + gT(h) + T(h)T(g)$. By the previous theorem $T(p)-gT(h)-T(h)T(g)$ is divisible by $T(f)$. Hence

$$hT(g)=\alpha T(f) \text{ for some } \alpha\in A\otimes A.$$

So $T(g)=h^{-1}\alpha T(f)$.

THEOREM 2.3. *Let A be a commutative augmented K-algebra. Consider $f,g\in A$ and assume the following properties are satisfied:*

(1) A is a free K-module,

(2) f is not a zero divisor in A,

(3) $\tilde f$ is not a zero divisor in A,

(4) A/fA is a free K-module,

(5) Tf divides Tg.

Then $\tilde g=g_1\tilde f$ for some $g_1\in A$ and Tf divides Tg_1.

PROOF. Since $Tf|Tg$, then $T\tilde f|T\tilde g$, or

$$\epsilon_0\tilde g-\epsilon_1\tilde g=p(\epsilon_0\tilde f-\epsilon_1\tilde f) \text{ for some } p\in A\otimes A. \tag{2.4}$$

By applying $\delta: A\otimes A\to A$ and using that $\gamma(\tilde g)=\gamma(\tilde f)=0$, we obtain $\tilde g=g_1\tilde f$ where $g_1=\delta p$. By replacing in (2.4), we obtain

$$(p-\epsilon_0g_1)\epsilon_0\tilde f=(p-\epsilon_1g_1)\epsilon_1\tilde f \text{ and} \tag{2.5}$$

$$T(g_1)\epsilon_0\tilde f=(p-\epsilon_1g_1)T\tilde f. \tag{2.6}$$

Since A and A/fA are free over K we can choose bases for both over K. Let $(t_1,\cdots,t_r)$ be a basis for A over K; then $(ft_1,\cdots,ft_r)$ is a basis for fA. Let $(\bar u_1,\cdots,\bar u_s)$ be a basis for A/fA over K, and $(u_1,\cdots,u_s)$ a set of representatives of $(\bar u_1,\cdots,\bar u_s)$ in A.

Then (2.6) can be written

$$\sum_{i\in I}a_i\otimes b_i\tilde f=\sum_{j\in J}c_j\tilde f\otimes d_j \tag{2.7}$$

for suitable finite indexing sets I and J and appropriate elements a_i, b_i, c_j, d_j in A.

We now express the elements d_j as combinations of the basis-elements $(u_1,\cdots,u_s)$ and $(ft_1,\cdots,ft_r)$.

Likewise we express the elements $b_i\tilde f$ in the base $(ft_1,\cdots,ft_r)$. Then the coefficients of the basis-elements $(u_1,\cdots,u_s)$ turn out to be all zero, and it follows that the elements d_j all have $\tilde f$ as a factor.

Therefore $$T(\tilde{f})|T(g_1).$$

THEOREM 2.8. *Let A be a commutative augmented K-algebra. Assume that $f, g \in A$ and that the conditions of Theorem 2.3 are satisfied; then from $T(f)|T(g)$ it follows that g is in the f-adic completion of the K-subalgebra generated by f in A.*

PROOF. The conditions of the theorem are the same as in Theorem 2.3, therefore we have $\tilde{g} = g_1\tilde{f}$, for some $g_1 \in A$ and $T(f)|T(g_1)$. Hence we can write

$$g = g_1\tilde{f} + d_1$$

where $d_1 = i\gamma g, d_1 \in iK$. Now the pair (f, g_1) again satisfies all the conditions of theorem 2.3. Therefore $\tilde{g}_1 = g_2\tilde{f}$, for some $g_2 \in A$ and $T(f)|T(g_2)$ which means that

$$g = (g_2\tilde{f} + d_2)\tilde{f} + d_1; \quad d_1, d_2 \in iK.$$

The same process can be started again with the pair (f, g_2).

We go on this way. Two things can happen. Either at a certain stage we obtain an element g_i which is in iK (in that case g turns out to be a polynomial in $\tilde{f}$, or for that matter in f) or the process goes on indefinitely. In the latter eventuality g is in the f-adic completion of the subalgebra generated by f in A.

3.

From now on we restrict ourselves to the case where K is a field.

THEOREM 3.1. *Let A be a graded K-algebra which is an integral domain. If $f, g \in A$ and $T(f)|T(g)$, then g is a polynomial in f.*

PROOF. $A \in \mathrm{Ob}C$. Moreover the conditions of Theorem 2.8 are satisfied.

In this case the inductive process described in the proof of Theorem 2.8 is finite, since the sequence of elements $g_1, g_2, \cdots, g_r$ thus obtained is made up of elements of strictly decreasing degrees. Eventually we reach a non-zero element of K, which we suppose to be g_r. Then g is a polynomial in f of degree r.

THEOREM 3.2. *Let $A \otimes_K A$ be a graded K-algebra. If $f, g \in A$, $T(f)|T(g)$ and $T(f)$ is not a zero-divisor in $A \otimes_K A$, then g is a polynomial in f.*

PROOF. $A \in \mathrm{Ob}C$, and the conditions of Theorem 2.3 are satisfied. Therefore, from $T(g) = p_1 T(f)$, $p_1 \in A \otimes_K A$ it follows that

$$\tilde{g} = (\delta p_1)\tilde{f} \text{ and } T(f) | T(\delta p_1) \tag{3.3}$$

so that

$$T(\delta p_1) = p_2 T(f) \quad p_2 \in A \otimes_K A. \tag{3.4}$$

From (3.3) we obtain, by Definition (1.1),

$$T(\tilde{g}) = (\delta p_1)T(\tilde{f}) + \tilde{f}T(\delta p_1) + T(\delta p_1)T(\tilde{f}); \tag{3.5}$$

substituting from (3.4) in (3.5) we obtain

$$T(\tilde{g}) = (\delta p_1)T(\tilde{f}) + \tilde{f}p_2 T(\tilde{f}) + p_2[T(\tilde{f})]^2; \tag{3.6}$$

since $T(g) = p_1 T(f)$ and $T(\tilde{f}) = T(f)$ we obtain

$$\begin{aligned} p_1 &= p_2 T(\tilde{f}) + \tilde{f}p_2 + (\delta p_1)\otimes 1 \\ &= p_2(1\otimes_K \tilde{f} - \tilde{f}\otimes_K 1) + \tilde{f}p_2 + (\delta p_1)\otimes 1 \\ &= p_2(1\otimes_K \tilde{f}) + (\delta p_1)\otimes 1. \end{aligned}$$

Since $A\otimes_K A$ is graded, it follows that degree $p_2 <$ degree p_1.

From here on we proceed in a way which is similar to the end of the proof of the preceeding theorem. This time the sequence of elements $p_1, p_2, \cdots$ is of strictly descending degrees.

THEOREM 3.7. *Let $A \in \mathrm{Ob}C$, K be a field, $f \in A$. The set of elements g in A such that $T(f) | T(g)$ is a sub-K-algebra of A.*

PROOF. Since T is linear, we have only to prove that if $T(f)|T(g_1)$ and $T(f)|T(g_2)$ then $T(f)|T(g_1 g_2)$. This follows from Definition (1.1):

$$T(g_1 g_2) = g_1 T(g_2) + g_2 T(g_1) + T(g_1)T(g_2).$$

4. Power series rings

In order to show that the subalgebra S we obtained in Theorem 3.7 can be strictly between the subalgebra generated by f in A and its completion, we will consider the case $A = K[[X]]$, K a field of characteristic zero. The finiteness conditions imposed by the tensor product (i.e., in $A\otimes A$) show that, in general, not for every $f \in A$ we have $TX | Tf$.

First of all, we consider the inclusion $A \otimes A \to B = K[[y_1, y_2]]$ by writing $1 \otimes (\Sigma_0^\infty a_i X^i) = \Sigma_0^\infty a_i y_1^i$, $(\Sigma_0^\infty a_i X^i) \otimes 1 = \Sigma_0^\infty a_i y_2^i$. Then, for $f = \Sigma_0^\infty a_i X^i$ we have

$$T(f) = \left(\sum_0^\infty a_i y_1^i\right) - \left(\sum_0^\infty a_i y_2^i\right)$$

$$= \sum_0^\infty a_i (y_1^i - y_2^i)$$

$$= (y_1 - y_2) \sum_0^\infty a_i \left(\sum_{j=0}^i y_1^j y_2^{i-j}\right)$$

$$= T(X) \sum_0^\infty a_i \left(\sum_{j=0}^i y_1^j y_2^{i-j}\right).$$

So, we can write $T(f) = T(X)h$ with $h \in B$.

Our interest is, then, to know under which conditions (to be imposed on f) we have $h \in A \otimes A$. We will prove that $h \in A \otimes A$ if and only if $f \in L$ (see introduction for the definition of L).

Call $h = T(f)/T(X)$. Since we use the A-module structure of $A \otimes A$ by multiplication on the left, and $T(X) = y_1 - y_2$, we will denote $y_1 = X$, $y_2 = X - T(X)$, hence every polynomial in y_1, y_2 can be written in terms of X and $T(X)$.

EXAMPLE 4.1. We compute $T(f)/T(X)$ when f is a geometric series in X. Let $f = \Sigma_0^\infty a^i X^i$. Then

$$T(f) = \sum_{i=1}^\infty a^i T(X^i)$$

$$\sum_{i=1}^\infty a^i \sum_{j=1}^i \binom{i}{j} (T(X))^j X^{i-j}.$$

For a given j the coefficient of $(TX)^j$ is

$$\sum_{i>j} a^i \binom{i}{j} X^{i-j} = \frac{1}{j!} \frac{d^j f}{dX^j}.$$

Therefore

$$\frac{T(f)}{T(X)} = \sum_{i>j}^\infty a^i \sum_{j=1}^i \binom{i}{j} (T(X))^{j-1} X^{i-j}.$$

Let $k = i - j$; then the coefficient of $(T(X))^{j-1}$ is

$$\sum_{k=0}^\infty a^{k+j} \binom{k+j}{j} X^k.$$

If $H \in K[[y_1 y_2]]$, define H_{ij} as the coefficient of $X^i(T(X))^j$ in the development of H. Then

$$\left(\frac{T(f)}{T(X)}\right)_{ij} = \left(\frac{i+j+1}{j+1}\right)a^{i+j+1} \qquad (0 \leq i, j \leq \infty).$$

Similarly $(T(f))_{rj} = \binom{r+j}{j} a^{r+j}$ and

$$(fT(f))_{ij} = \sum_{r+s=i} a^r \binom{s+j}{j} a^{s+j} = \sum_{s=0}^{i} \binom{s+j}{j} a^{i+j} \text{ but}$$

$$\sum_{s=0}^{i} \binom{s+j}{j} = \binom{i+j+1}{j+1}, \text{ hence}$$

$$(fT(f))_{ij} = \binom{i+j+1}{j+1} a^{i+j} \qquad 0 \leq i, 1 \leq j.$$

Comparing $\left(\frac{T(f)}{T(X)}\right)_{ij}$ with $a(fT(f))_{ij}$ it is clear that the difference is given by the terms in $j = 0$ or $\Sigma_{i=1}^{\infty} i a^i X^{i-1}$.

Therefore, denoting by $\frac{d}{dX}$ the continuous derivation $A \xrightarrow{\delta} A$ defined by $\delta(x) = 1$,

$$\frac{T(f)}{T(X)} = \frac{df}{dX} + afT(f) = g \in A \otimes A, \quad \text{so that}$$

$$Tf = gT(X) \quad \text{in} \quad A \otimes A.$$

THEOREM 4.2. *Let* $f = \Sigma d_i X^i$, $g_\alpha = \Sigma g_{\alpha i} X^i$, $h_\theta = \Sigma h_{\alpha i} X^i$ *be elements of* $K[[X]]$, $\alpha \in J$, J *a finite indexing set. Then, if*

$$\frac{T(f)}{T(X)} = \frac{df}{dX} + \sum_\alpha g_\alpha T(h_\alpha) \text{ we have}$$

$$\sum_\alpha g_{\alpha i} h_{\alpha j} = a_{i+j+1}.$$

PROOF.

$$\left(\frac{T(f)}{T(X)}\right)_{ij} = \binom{i+j+1}{j+1} a_{i+j+1}$$

$$(T(h_\alpha))_{rj} = \binom{r+j}{j} h_{\alpha r+j}$$

$$(g_\alpha T(h_\alpha))_{ij} = \sum_{r+s=i} \binom{r+j}{j} g_{\alpha s} h_{\alpha r+j}$$

$$= \sum_{r=0}^{i} \binom{r+j}{j} g_{\alpha i-r} h_{\alpha r+j}.$$

Or

$$\left[\sum_{\alpha} g_{\alpha} T(h_{\alpha})\right]_{ij} = \sum_{r=0}^{i} \binom{r+j}{j} \left(\sum_{\alpha} g^{\alpha}_{i-r} h^{\alpha}_{j+r}\right).$$

Putting $i = 0$ we have

$$\sum_{\alpha} g_{\alpha 0} h_{\alpha j} = a_{j+1} \qquad j \geq 1.$$

Assume, as an induction hypothesis that

$$\sum_{\alpha} g_{\alpha l} h_{\alpha j} = a_{j+l+1} \text{ for all } l < i.$$

Then

$$\left[\sum_{\alpha} g_{\alpha} T(h_{\alpha})\right]_{ij} = \sum_{\alpha} g_{\alpha i} h_{\alpha j} + \sum_{r=1}^{i} \binom{r+j}{j} a_{i+j+1}.$$

But

$$\left[\sum_{\alpha} g_{\alpha} T(h_{\alpha})\right]_{ij} = \left(\frac{T(f)}{T(X)}\right)_{ij} = \binom{i+j+1}{j+1} a_{i+j+1}.$$

Since

$$\sum_{r=0}^{i} \binom{r+j}{j} = \binom{i+j+1}{j+1}, \text{ then } \sum_{r=1}^{i} \binom{r+j}{j} = \binom{i+j+1}{j+1} - 1$$

hence

$$\sum_{\alpha} g_{\alpha i} h_{\alpha j} = a_{i+j+1}.$$

Denote by $N = (i_1, \cdots, i_m)$ an m-tuple of natural numbers, and let an N-row of f ($f = \sum_{i=0}^{\infty} a_i x^i$) be the m-tuple $(a_{j+i_1}, \cdots, a_{j+i_m})$ for any j. We will call N-matrix of f an $m \times m$ matrix whose rows are N-rows, i.e., a matrix

$$M = (b_{ik}) \text{ with } b_{ik} = a_{j(i)+k}.$$

THEOREM 4.3. *Let $A = K[[X]]$ and $f \in A$. Then $T(X) | T(f)$ if and only if there exists an m-tuple N such that all N-matrices of f have zero determinant.*

PROOF. Suppose that

$$\frac{T(f)}{T(X)}=\frac{df}{dX}+\sum_{\alpha} g_\alpha T(h_\alpha) \tag{4.4}$$

and among all possible such decompositions select a shortest one, say $1 \leqslant \alpha \leqslant m$.

Consider the $(m \times \infty)$-matrix $\|g_{\alpha i}\|$. If its rank is smaller than m, then there is a g, say g_m, which is a k-linear combination of the previous ones; since T is K-linear we can find an expression (4.4) with less than m terms, contradicting our hypothesis.

Therefore $\|g_{\alpha i}\|$ must have rank m, i.e., there exist indices $i_1, \cdots, i_m$ such that $|g_{ki_l}|$ is invertible.

Consider the equations

$$\sum_{\alpha} g_{\alpha i_1} h_{\alpha j} = a_{j+i_1+1}$$

$$\sum_{\alpha} g_{\alpha i_m} h_{\alpha j} = a_{j+i_m+1}.$$

Now consider any new equation

$$\sum_{\alpha} g_{\alpha i_0} h_{\alpha j} = a_{j+i_0+1}.$$

Then the determinant

$$\begin{vmatrix} g_{1i_0} & \cdots & g_{mi_0} & a_{j+i_0+1} \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ g_{1i_m} & \cdots & g_{mi_m} & a_{j+i_m+1} \end{vmatrix}$$

must be zero for all j. Since $|g_{ki_l}|$ is invertible, a_{j+i_0+1} is a fixed linear combination of $a_{j+i_1+1}, \cdots, a_{j+i_m+1}$ with respect to j (= independent of j), $l \neq 0$.

Hence, if $N=(i_0, \cdots, i_m)$, every N-matrix has zero determinant, and i_0 turns out to be arbitrary!

To prove the converse, assume that there is an $N_0=(i_1, \cdots, i_m)$ and an N_0-matrix with non-zero determinant and an $N=(i_0, i_1, \cdots, i_m)=(i_0, N_0)$ such that all N-matrix have zero determinant, i.e.,

$$\begin{vmatrix} a_{i_1+j_1} & \cdots & a_{i_1+j_n} \\ a_{i_n+j_1} & & a_{i_n+j_n} \end{vmatrix} \neq 0$$

and, for every j,

$$\begin{vmatrix} a_{i_1+j_1} & \cdots & a_{i_1+j_n} & a_{i_1+j} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ a_{i_0+j_1} & \cdots & & a_{i_0+j} \end{vmatrix} = 0.$$

Then $a_{i_0+j_s}$ is a linear combination

$$a_{i_0+j_s} = \sum_{k=1}^{m} c_k a_{i_k+j_0}, \text{ independent of } j$$

$$a_{i_0+j} = \sum d_l a_{i_0+j_l}, \text{ independent of } i_0.$$

Notice that since i_0 is arbitrary, we can choose i_0 so that $i_0 + j_1$ is the smallest integer not appearing in $(i_1 \cdots i_n)$.

Take $g_{ri} = a_{i+j_r}, \qquad 1 \le r \le n.$

Then there exists an i_0 such that

$$g_{r\, i_0+l} = \sum_{k=1}^{m} c_k g_{r\, i_k+l}.$$

Hence, if we solve the systems

$$\sum_{\alpha} g_{\alpha i_s} h_{\alpha j} = a_{j+i_s+1} \qquad i_s \in N_0$$

the unique solutions $h_{\alpha j}$ will satisfy all the equations $\Sigma_\alpha g_{\alpha i} h_{\alpha i} = a_{j+i+1}$ and, hence we have

$$\frac{T(f)}{T(X)} = \frac{df}{dX} + \sum g_\alpha T(h_\alpha).$$

Consider $K[X] \subset K[[X]]$ and call L the ring obtained from $K[X]$ by localizing at the ideal (X). Hence $L \subset K[[X]]$. (Actually, $K[[X]]$ is the X-adic completion of L.)

According to Corollary 2.2, if $\alpha \in L$, $T(X)|T(\alpha)$. We want to prove the converse.

According to Theorem 4.3, if $\alpha = \Sigma_0^\infty a_i X^i$, $T(X)|T(\alpha)$ implies the existence of an N such that, for every $j \geq 0$, $a_{N+j} = \Sigma_0^{N-1} c_i a_{i+j}$.

Call $p = 1 - \Sigma_0^{N-i} c_i X^{N-i}$; hence all coefficients of $p \cdot \alpha$ are zero for degrees higher than N hence $p\alpha = q \in K[X]$, and p is invertible in $K[[X]]$, hence $\alpha \in L$.

So, we have proved the following theorem.

THEOREM 4.5. *Let $A = K[[X]]$; then for $\alpha \in A$, $T(X)|T(\alpha)$ if and only if $\alpha \in L$.*

REFERENCES

1. A. A. Evyatar and D. B. Scott, *On polynomials in a polynomial*, Bull. London Math. Soc. 4 (1972), 176–178.

2. K. R. Mount O. F. Villamayor, *Taylor-Series and Higher Derivations*, Serie Impresiones previas No. 18. Departamento de Matemáticas, Universidad de Buenos Aires, 1969.

3. K. R. Mount and O. E. Villamayor, *Weierstrass points as singularities of maps in arbitrary characteristic*, to appear in J. of Algebra.

4. P. Torelli, *The theory of higher order M-adic differentials*, Thesis, Northwestern University (1970), to appear in J. of Algebra.

DEPARTMENT OF MATHEMATICS
TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY
HAIFA, ISRAEL