4. Newton identities

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **31 (1985)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

form of the inductive hypothesis, so that $(\alpha A_1)(A_{p-1} \times B_q) \in J_{p+q-1}$; hence a second application of Lemma 3.5 gives

$$A_p \times B_q = (A_1 \times A_{p-1}) \times B_q \bmod J_{p+q-1} = A_1 \times (A_{p-1} \times B_q) \bmod J_{p+q-1}$$
$$= A_1 \cdot (A_{p-1} \times B_q) \bmod J_{p+q-1} .$$

Finally, the specific form $A_{p-1} \times B_q - A_{p-1} \cdot B_q \in J_{p+q-2} (\subset J_{p+q-1})$ of the inductive hypothesis permits one to conclude that

$$A_p \times B_q = A_1 \cdot (A_{p-1} \cdot B_q) \bmod J_{p+q-1} = (A_1 \cdot A_{p-1}) \cdot B_q \bmod J_{p+q-1}$$
$$= A_p \cdot B_q \bmod J_{p+q-1} ,$$

which completes the inductive step.

3.7 PROPOSITION. *For any module* V *over a commutative ring* R *with unit, the third product in* $\Pi_r \operatorname{End} \wedge^r V$ *restricts to a product in the sub-module of one-generated elements of the direct sum* $\amalg_r \operatorname{End} \wedge^r V$.

Proof. Immediate consequence of Lemma 3.6.

Lemma 3.6 and Proposition 3.7 are certainly valid under considerably weaker hypotheses; for example, one can easily combine the present versions with localization techniques to obtain greater generality. One can possibly establish entirely unrestricted versions of Lemma 3.6 and Proposition 3.7 by applying the identity of Lemma 3.1 directly to elements

$$x_1 \wedge \dots \wedge x_r \in \wedge^r V \quad \text{for} \quad r \geqslant p + q ;$$

however, such a computation would probably be very complicated.

Here is a simple application of the results of this section. Any endomorphisms $A \in \operatorname{End} V$ and $B \in \operatorname{End} V$ are trivially one-generated, so that Lemmas 3.2 and 3.6 imply $A \times B = AB + A \cdot B$ and $B \times A = BA + B \cdot A$; since $A \cdot B = B \cdot A$ it follows that $AB - BA = A \times B - B \times A$. If V is traceable Theorem 2.3 then implies the best-known elementary property of the trace:

$$\operatorname{tr} AB - \operatorname{tr} BA = (\operatorname{tr} A)(\operatorname{tr} B) - (\operatorname{tr} B)(\operatorname{tr} A) = 0 .$$

4. NEWTON IDENTITIES

Let A be any endomorphism of a module V over a commutative ring R with unit. The shuffle products of the compositions $I, A, A^2, \dots$ of A

generate a subalgebra R_A of one-generated elements of Π_r End $\wedge^r V$, and since the third product is defined in terms of shuffle products and composition products one expects various identities relating the three products in R_A. If V happens to be traceable one can then apply the trace and use Theorem 2.3 to obtain relations among the various trace-induced invariants of A, as indicated in the Introduction. In this section we develop those identities in R_A whose images under the trace are the Newton identities, relating the sums-of-powers invariants of A to the elementary invariants of A.

For convenience we henceforth impose an additional condition on the ground ring R itself: R will be a commutative algebra with unit over the field of rational numbers.

4.1 LEMMA. *For any* $p \geqslant 0$ *and any* $q > 0$ *the p-fold composition* $A^p \in \operatorname{End} V$ *and the q-fold shuffle product* $\frac{1}{q!} A^{\cdot q} \in \operatorname{End} \wedge^q V$ *satisfy*

$$(\alpha A^p)\left(\frac{1}{q!} A^{\cdot q}\right) = A^{p+1} \cdot \frac{1}{(q-1)!} A^{\cdot (q-1)} .$$

Proof. As in the proof of Lemma 3.4 one has

$$(\alpha A^p)(A^{\cdot q}) = (A^p \cdot I_{q-1})(A \cdot \ldots \cdot A) = \sum_{s=1}^{q} A \cdot \ldots \cdot A^p A \cdot \ldots \cdot A$$
$$= q\, A^{p+1} \cdot A^{\cdot (q-1)},$$

the s^{th} summand containing $A^p A$ $(= A^{p+1})$ as its s^{th} factor, $s = 1, \ldots, q$.

4.2 LEMMA. *Let* I_1 *be the identity endomorphism in* End V; *then for any* $r > 0$ *and any* $C_r \in \operatorname{End} \wedge^r V$ *one has*

$$I_1 \times C_r = I_1 \cdot C_r + r\, C_r \in \operatorname{End} \wedge^{r+1} V \oplus \operatorname{End} \wedge^r V .$$

Proof. By Lemma 3.5 one has $I_1 \times C_r = I_1 \cdot C_r + (\alpha I_1) C_r$, where the degree r component of αI_1 is given by $I_{r-1} \cdot I_1 = r\, I_r \in \operatorname{End} \wedge^r V$.

4.3 THEOREM. *Let* R *be a commutative algebra with unit over the rational numbers, let* V *be any R-module, and let* $A \in \operatorname{End} V$. *Then the p-fold compositions* $A^p \in \operatorname{End} V$ *and the q-fold shuffle products*

$$\frac{1}{q!} A^{\cdot q} \in \operatorname{End} \wedge^q V$$

are related for each $r > 0$ *by the identity*

$$r\left(\frac{1}{r!}A^{\cdot r}\right) + \sum_{p=1}^{r}(-1)^p A^p \times \frac{1}{q!}A^{\cdot q} = 0\,,$$

where $q = r - p$.

Proof. One applies Lemmas 3.5 and 4.1 to find

$$\begin{aligned} A^p \times \frac{1}{q!}A^{\cdot q} &= A^p \cdot \frac{1}{q!}A^{\cdot q} + (\alpha A^p)\left(\frac{1}{q!}A^{\cdot q}\right) \\ &= A^p \cdot \frac{1}{q!}A^{\cdot q} + A^{p+1} \cdot \frac{1}{(q-1)!}A^{\cdot (q-1)} \end{aligned}$$

for $q > 0$. Hence all summands of the alternating sum $\sum_{p+q=r}(-1)^p A^p \times \frac{1}{q!}A^{\cdot q}$ cancel except in the extreme cases $p = 0$ and $q = 0$. For $p = 0$ one uses Lemma 4.2 to find

$$A^0 \times \frac{1}{r!}A^{\cdot r} = A^0 \cdot \frac{1}{r!}A^{\cdot r} + r\left(\frac{1}{r!}A^{\cdot r}\right),$$

leaving the uncancelled term $r\left(\frac{1}{r!}A^{\cdot r}\right)$; for $q = 0$ one has $A^r \times \frac{1}{0!}A^{\cdot 0} = A^r \times I_0 = A^r$, for the third product unit element I_0, so that there are no further uncancelled terms.

Theorem 4.3 provides identities in the subalgebra $R_A \subset \Pi_r \operatorname{End} \wedge^r V$ generated by $A \in \operatorname{End} V$. In the next result $R_A[[t]]$ will be the formal power series algebra in a single indeterminate t over R_A. Observe that the element $I + tA = I_1 + tA \in R_A[[t]]$ has a composition-product inverse

$$(I+tA)^{-1} = I - tA + t^2A^2 - \ldots \in R_A[[t]]\,,$$

and that formal integration of $A(I+tA)^{-1}$ (from 0 to t) provides a composition-product logarithm

$$\ln(I+tA) = tA - \frac{t^2}{2}A^2 + \frac{t^3}{3}A^3 - \ldots \in R_A[[t]]$$

of $I + tA$. Similarly the shuffle-product exponentials

$$e^{\cdot tA} = I_0 + \frac{t}{1!}A + \frac{t^2}{2!}A \cdot A + \ldots \in R_A[[t]] \quad \text{and} \quad e^{\cdot (I+tA)^{-1}} \in R_A[[t]]$$

satisfy a composition-product identity

$$(\alpha e^{\cdot tA})e^{\cdot (I+tA)^{-1}} = (e^{\cdot (I+tA)})\,(e^{\cdot (I+tA)^{-1}}) = \mathbf{I} = e^{I};$$

hence

$$e^{\cdot tA} \times \alpha^{-1}e^{\cdot (I+tA)^{-1}} = \alpha^{-1}((\alpha e^{\cdot tA})\,(e^{\cdot (I+tA)^{-1}}) = \alpha^{-1}e^{I} = I_0$$

and similarly $\alpha^{-1}e^{\cdot (I+tA)^{-1}} \times e^{\cdot tA} = I_0$. Thus $\alpha^{-1}e^{\cdot (I+tA)^{-1}} \in R_A[[t]]$ is a two-sided third-product inverse $(e^{\cdot tA})^{-1}$ of $e^{\cdot tA}$, so that formal integration of the third-product $(A \cdot e^{\cdot tA}) \times (e^{\cdot tA})^{-1} \in R_A[[t]]$ (from 0 to t) provides a third-product logarithm $\ln^{\times}(e^{\cdot tA}) \in R_A[[t]]$ of the shuffle-product exponential $e^{\cdot tA} \in R_A[[t]]$.

4.4 THEOREM. *Let R be a commutative algebra with unit over the rational numbers, let V be any R-module, and let $A \in \operatorname{End} V$. Then the p-fold compositions $A^p \in \operatorname{End} V$ and the q-fold shuffle products*

$\frac{1}{q!}A^{\cdot q} \in \operatorname{End} \wedge^q V$ *are related in the formal power series ring $R_A[[t]]$ by the identity*

$$\ln(I+tA) = \ln^{\times}(e^{\cdot tA}).$$

Proof. For each $r > 0$ one can re-write Theorem 4.3 in the form

$$A\left(\sum_{p=0}^{r-1}(-1)^p A^p\right) \times \frac{1}{q!}A^{\cdot q} = A \cdot \frac{1}{(r-1)!}A^{\cdot (r-1)},$$

where $p + q = r - 1$. If one multiplies each such identity by t^{r-1} and computes formal sums over all values $0, 1, 2, \ldots$ of $r - 1$, the result is a formal power series identity

$$A(I+tA)^{-1} \times e^{\cdot tA} = A \cdot e^{\cdot tA} \in R_A[[t]].$$

Since $e^{\cdot tA}$ has a third-product inverse $(e^{\cdot tA})^{-1} \in R_A[[t]]$ it follows that

$$A(I+tA)^{-1} = (A \cdot e^{\cdot tA}) \times (e^{\cdot tA})^{-1};$$

that is,

$$\frac{d}{dt}\ln(I+tA) = \frac{d}{dt}\ln^{\times}(e^{\cdot tA}) \in R_A[[t]].$$

It remains only to integrate each power of t separately (from 0 to t) to complete the proof.

4.5 *Definition.* Let R be a commutative algebra with unit over the rational numbers, let V be a traceable R-module of rank n, and let $A \in \operatorname{End} V$.

Then the *elementary invariants* $\sigma_1, \sigma_2, \ldots, \sigma_n \in R$ of A and the *sums-of-powers invariants* $s_1, s_2, \ldots \in R$ of A are given by $\sigma_q = \sigma_q(A) = \operatorname{tr} \frac{1}{q!} A^{\cdot q}$ and $s_p = s_p(A) = \operatorname{tr} A^p$, respectively. Observe that since V is traceable of rank n one automatically has $A^{\cdot q} = 0$ hence $\sigma_q = 0$ whenever $q > n$; consequently the preceding hypotheses imply that

$$\operatorname{tr} e^{\cdot tA} = 1 + t\sigma_1 + \ldots + t^n \sigma_n \in R[[t]] .$$

4.6 COROLLARY (The Newton identities, more or less). *Let A be any endomorphism of a traceable module V of rank $n > 0$ over a commutative algebra R with unit over the rational numbers. Then for each $r > 0$ the invariants $\sigma_q = \sigma_q(A) \in R$ and $s_q = s_q(A) \in R$ satisfy the identity*

$$r\,\sigma_r + \textstyle\sum_{p=1}^{r} (-1)^p s_p\, \sigma_{r-p} = 0 ,$$

where $\sigma_q = 0$ for $q > n$.

Proof. By Theorem 2.3 the trace induces an algebra homomorphism $R_A \to R$ from the subalgebra R_A of the third-product algebra $\Pi_s \operatorname{End} \wedge^s V$ to the ground ring R; hence it suffices to apply the trace to the identities of Theorem 4.3.

4.7 COROLLARY. *Let A be any endomorphism of a traceable module V of rank $n > 0$ over a commutative algebra R with unit over the rational numbers. Then the elementary invariants $\sigma_1, \ldots, \sigma_n$ and sums-of-powers invariants $s_1, s_2, \ldots$ of A satisfy the identity*

$$t\, s_1 - \frac{t^2}{2} s_2 + \frac{t^3}{3} s_3 - \ldots = \ln(1 + t\sigma_1 + \ldots + t^n \sigma_n)$$

in the formal power series ring $R[[t]]$.

Proof. As in the preceding proof Theorem 2.3 implies that the trace induces an algebra homomorphism $R_A[[t]] \to R[[t]]$, products in $R_A[[t]]$ being defined in terms of third-products; hence it suffices to apply the trace to the identity of Theorem 4.4.

A special case of the third product and Theorem 2.3 appear briefly at the end of [2], somewhat fettered by the details of a specific application. The present article shows that the third product is a reasonable general feature of elementary linear algebra over any commutative ring with unit: it turns the trace into an algebra homomorphism, and it provides a natural setting for the study of invariants of module endomorphisms.