Differentials and the Trace

Arthur Ogus

November 2, 2007

Let A be a commutative ring and let B be a finite flat A-algebra. For each element b of B, let $b_B\colon B \to B$ denote multiplication by b and let $\mathrm{Tr}_{B/A}\colon B \to A$ denote the map sending b to the trace of b_B. Thus

$$\mathrm{Tr}_{B/A} \in \omega_{B/A} := \mathrm{Hom}_A(B, A).$$

We endow $\omega_{B/A}$ with the B-module structure defined by $b\phi(b') := \phi(b'b)$.

Lemma: If B has basis $(e_1, \dots, e_n)$ and $(e_1^*, \dots, e_n^*)$ is the dual basis, then

$$\mathrm{Tr}_{B/A} = \sum e_i e_i^* \in \omega_{B/A}.$$

Proof: In fact, if η is any A-linear endomorphism of B, the ijth entry of matrix for η in the basis $(e_1, \dots e_n)$ is $e_i^*(\eta(e_j))$. Thus the trace of η is $\sum e_i^*(\eta(e_i))$. If $b \in B$ and $\eta = b_\beta$, we find $\mathrm{Tr}_{B/A}(b) = \sum e_i^*(be_i) = \sum e_i e_i^*(b)$. $\square$

Theorem: Let $f \in A[X]$ be a monic polynomial of degree n, let $B := A[X]/(f)$, and let β be the image of X in B.

1. B is a free A-module of rank n, with basis $(1, \beta, \dots \beta^{n-1})$.
2. $\omega_{B/A}$ is a free B-module of rank 1, with basis $\tau := \partial_{n-1}$, where $(\partial_0, \dots, \partial_{n-1})$ is the dual basis to $(1, \beta, \dots \beta^{n-1})$.
3. $\mathrm{Tr}_{B/A} = f'(\beta)\tau \in \omega_{B/A}$.

Proof: [1] The key point is the following.

Lemma: Write $f(X) = (X - \beta)g(X)$, where $g(X) = \sum_i b_i X^i \in B[X]$. Then

$$\partial_i = b^i \tau \text{ for } i = 0, \dots n-1.$$

[1] This discussion is based on the exposition in the book *Anneaux Locaux Henseliens* by M. Raynaud, which is in turn based on notes by J. Tate.

Note that this lemma implies that the element τ generates $\omega_{B/A}$ as a B-module: the map $B \to \omega_{B/A}$ it defines is surjective. Since both the source and target of this map are free A-modules of the same rank, it is an isomorphism, and (2) of the theorem follows. Moreover, if we combine the two lemmas, we find

$$\begin{aligned} \mathrm{Tr}_{B/A} &= \sum \beta^i \partial_i \\ &= \sum \beta^i b_i \tau \\ &= g(\beta)\tau \end{aligned}$$

But $g(\beta) = f'(\beta)$ since $f(X) = (X - \beta)g(X)$.

It remains only to prove the lemma. Let us write $f(X) = \sum a_i X^i$, so that

$$\beta^n = -\sum_{i=0}^{n-1} a_i \beta^i,$$

and

$$a_i = b_{i-1} - \beta b_i \quad \text{for } 0 \leq i \leq n.$$

We calculate:

$$\beta \partial_i(\beta^j) = \partial_i(\beta^{j+1}) = \begin{cases} 1 & \text{if } j = i-1 \\ -a_i & \text{if } j = n-1 \\ 0 & \text{otherwise.} \end{cases}$$

In other words, $\beta\partial_i = \partial_{i-1} - a_i\tau$, or

$$\partial_{i-1} = \beta\partial_i + a_i\tau.$$

We prove our claim that $\partial_i = b_i\tau$ by descending induction on i. Since $b_{n-1} = 1$, the result is true for $i = n-1$. Using the above formulas and the induction hypothesis, we find:

$$\begin{aligned} \partial_{i-1} &= \beta\partial_i + a_i\tau \\ &= \beta b_i \tau + (b_{i-1} - \beta b_i)\tau \\ &= b_{i-1}\tau \end{aligned}$$

□