

In this handout we discuss the use of modules of differentials to find a separating transcendence basis for a finitely generated extension K/k of a field k of characteristic $p > 0$ assuming $k' \otimes_k K$ is reduced for all purely inseparable finite extensions k'/k (a condition we have seen is necessary anyway). It was seen in class that under this latter assumption, $K' := k_p \otimes_k K$ is a field finitely generated over the perfect closure k_p and satisfying $\text{trdeg}(K'/k_p) = \text{trdeg}(K/k)$. Moreover, by perfectness of k_p we have seen in class that K'/k_p does admit a separating transcendence basis. The problem is how to use this information to build a separating transcendence basis for K/k .

1. SUMMARY OF PROPERTIES OF $\Omega_{B/A}^1$

Let $A \rightarrow B$ be a map of rings. Let $\mu : B \otimes_A B \rightarrow B$ be the ring map satisfying $b \otimes b' \mapsto bb'$, and define $I = \ker \mu$. In class we saw that for the B -module $\Omega_{B/A}^1 := I/I^2$ equipped with the A -linear derivation

$$d = d_{B/A} : B \rightarrow \Omega_{B/A}^1$$

defined by $b \mapsto 1 \otimes b - b \otimes 1 \pmod{I^2}$, every A -linear derivation $D : B \rightarrow M$ to any B -module M factors linearly through d : that is, there exists a B -linear map $T_D : \Omega_{B/A}^1 \rightarrow M$ satisfying $D = T_D \circ d$. To establish the universality of $(\Omega_{B/A}^1, d)$, and that $\Omega_{B/A}^1$ is spanned over B by the elements $d(b_i)$ for any set $\{b_i\}$ of A -algebra generators of B , it remains to show:

Proposition 1.1. *The map T_D is uniquely determined by D , and if $\{b_i\}$ is a set of A -algebra generators of B then $\{d(b_i)\}$ spans $\Omega_{B/A}^1$ over B .*

Proof. To prove uniqueness of T_D , we have to show that there is at most one B -linear map $T : \Omega_{B/A}^1 \rightarrow M$ satisfying $T(db) = D(b)$ for all $b \in B$. If the elements $db \in \Omega_{B/A}^1$ for $b \in B$ span $\Omega_{B/A}^1$ over B then obviously an B -linear map $T : \Omega_{B/A}^1 \rightarrow M$ is determined uniquely by its values on the B -module spanning set $\{db\}_{b \in B}$. (This just says that any linear map between modules is determined by its values on a spanning set.) Thus, it suffices to show that I/I^2 is spanned over B by the classes of the elements $1 \otimes b - b \otimes 1 \in I$.

Since I/I^2 is a module over $B = (B \otimes_A B)/I$, it suffices to show that I is generated as a $B \otimes_A B$ module (i.e., as an ideal!) by such differences $1 \otimes b - b \otimes 1$. Letting $J \subset B \otimes_A B$ denote the ideal generated by those differences, so $J \subset I$ (due to the definition $I = \ker \mu$), clearly in the quotient ring $(B \otimes_A B)/J$ the class of $b \otimes b' = (b \otimes 1)(1 \otimes b')$ is equivalent to that of $(b \otimes 1)(b' \otimes 1) = bb' \otimes 1$. Hence, in the factorization

$$B \rightarrow (B \otimes_A B)/J \twoheadrightarrow (B \otimes_A B)/I = B$$

of id_B using as first map $b \mapsto b \otimes 1 \pmod{J}$, we see that the first map is surjective. But the composite map id_B is injective (even an isomorphism), so the first step is injective and thus is an isomorphism. This forces the second map to also be an isomorphism, and thus $J = I$ as desired.

It remains to show rather generally that if $\{b_i\}$ is a set of A -algebra generators of B then $\{d(b_i)\}$ spans $\Omega_{B/A}^1$ as a B -module. Letting N denote the B -span of the elements $d(b_i)$, the quotient $M := \Omega_{B/A}^1/N$ is a B -module and the natural quotient map $T : \Omega_{B/A}^1 \rightarrow M$ defines an A -linear derivation $D := T \circ d : B \rightarrow M$ satisfying $D(b_i) = T(db_i) = 0$ for all i since T kills N by design of T . This forces $D = 0$; i.e., $D(b) = 0$ for all $b \in B$. Indeed, any $b \in B$ can be written as $b = f(b_{i_1}, \dots, b_{i_m})$ for some b_{i_1}, \dots, b_{i_m} in our set of A -algebra generators and some

$f \in A[T_1, \dots, T_m]$, so

$$D(b) = \sum_j (\partial f / \partial T_j)(b_{i_1}, \dots, b_{i_m}) D(b_{i_j}) = 0$$

(as all $D(b_i) = 0$).

By the uniqueness aspect of the established universal property, the vanishing of D forces the vanishing of T . But T was defined as projection to the quotient modulo N , so the vanishing of T forces $\Omega_{B/A}^1 = N$; this is exactly the desired property that $\{d(b_i)\}$ spans $\Omega_{B/A}^1$ as a B -module. ■

There are some further properties of Ω^1 recorded in class and worked out on HW3:

- (1) (HW3, #3(iii)) For any multiplicative set $S \subset B$, there is a unique $S^{-1}B$ -linear isomorphism $\Omega_{S^{-1}B/A}^1 \simeq S^{-1}\Omega_{B/A}^1$ satisfying $d(b/s) \mapsto (sdb - bds)/s^2 = db/s - b(ds/s)$ for $b \in B$, $s \in S$.
- (2) (HW3, #4(i)) For any A -algebra A' and $B' := A' \otimes_A B$, there is a unique isomorphism $A' \otimes_B \Omega_{B/A}^1 \simeq \Omega_{B'/A'}^1$ of B' -modules satisfying $1 \otimes db \mapsto d(1 \otimes b)$ for all $b \in B$.
- (3) (HW3, #4(ii)) For any quotient ring $\bar{B} = B/J$ and set $\{f_i\}$ of generators of J ,

$$\Omega_{B/A}^1 / (J\Omega_{B/A}^1 + \sum B \cdot df_i) \simeq \Omega_{\bar{B}/A}^1$$

via $db \mapsto d(b \bmod J)$ for all $b \in B$.

- (4) (HW3, #4(iii)) For any pair of ring maps $A \rightarrow A' \rightarrow B$, $\Omega_{B/A}^1 / \langle da' \rangle_{a' \in A'} \simeq \Omega_{B/A'}^1$ as B -modules via $d_{B/A}(b) \mapsto d_{B/A'}(b)$ for $b \in B$.

Example 1.2. For any field k and field $K := k(T_1, \dots, T_n)$ that is the localization of $B = k[T_1, \dots, T_n]$ at the multiplicative set $S = B - \{0\}$, we have

$$\Omega_{K/k}^1 = S^{-1}\Omega_{B/k}^1 = S^{-1}(\oplus_{j=1}^n B dT_j) = \bigoplus_{j=1}^n K dT_j$$

as K -vector spaces.

2. CONSTRUCTION OF SEPARATING TRANSCENDENCE BASIS

Now consider K/k a finitely generated extension in characteristic $p > 0$ with $m := \text{trdeg}(K/k)$, and assume $K' := k_p \otimes_k K$ is a field (this being the step that encodes that $k' \otimes_k K$ is reduced for any finite purely inseparable extension k'/k). As we have already reviewed at the start, K'/k_p is a finitely generated extension with transcendence degree m as well. The crucial point is this:

Lemma 2.1. $\dim_K \Omega_{K/k}^1 = \text{trdeg}(K/k)$.

This equality fails badly already for K/k finite when K/k is not separable (which cannot happen when $k_p \otimes_k K$ is reduced). Indeed, in such cases the transcendence degree is 0 but always $\Omega_{K/k}^1 \neq 0$ in such cases, as seen in class.

Proof. To compute the K -dimension, we will calculate the K' -dimension after extension of scalars: by associativity of tensor products we have $K' \otimes_{K'} \Omega_{K/k}^1 = k_p \otimes_k \Omega_{K/k}^1$, and the good behavior of Ω^1 with respect to extension of the ground ring identifies this with $\Omega_{(k_p \otimes_k K)/k_p}^1 = \Omega_{K'/k_p}^1$. We know that K'/k_p is finitely generated with transcendence degree m , and it admits a separating transcendence basis $\{Y_1, \dots, Y_m\}$ since k_p is perfect. Since K' is finite *separable* over $E := k_p(Y_1, \dots, Y_m)$, it follows from HW3 Exercise 5 that the natural K' -linear map $K' \otimes_E \Omega_{E/k_p}^1 \rightarrow \Omega_{K'/k_p}^1$ (induced by the map $\Omega_{E/k_p}^1 \rightarrow \Omega_{K'/k_p}^1$ arising from functoriality of $\Omega_{B/A}^1$ in B as an A -algebra) is an isomorphism. Thus,

to show $\dim_K \Omega_{K/k}^1 = m$ it is the same to show Ω_{E/k_p}^1 has E -dimension equal to m . But Example 1.2 applied to $E = k_p(Y_1, \dots, Y_m)$ over the base field k_p gives exactly that result. ■

Since $\Omega_{K/k}^1$ is spanned as a K -vector space by the elements df for $f \in K$ (just as $\Omega_{B/A}^1$ is spanned over B by the elements db for $b \in B$), it admits a K -basis consisting of some elements df_i for $1 \leq i \leq \dim_K \Omega_{K/k}^1 = m$. We claim that $\{f_1, \dots, f_m\}$ is a separating transcendence basis. (Note that we are *not* directly using a separating transcendence basis for K'/k_p to make one for K/k ; rather, we used the former to prove Lemma 2.1, from which we got f_1, \dots, f_m that we will show do the job.)

The key is to show that $\{f_1, \dots, f_m\}$ inside K is algebraically independent over k , or even that these f_j 's are algebraically independent over k_p (when we view each f_j as an element of $K' = k_p \otimes_k K$). Indeed, once this is proved then since $m = \text{trdeg}(K/k)$ it follows that $\{f_1, \dots, f_m\}$ is a transcendence basis for K/k . This is even a separating transcendence basis, which is to say the finite extension $K/k(f_1, \dots, f_m)$ is separable, because

$$\Omega_{K/k(f_1, \dots, f_m)}^1 = \Omega_{K/k}^1 / \left(\sum K df_j \right) = 0$$

(as the df_j 's span $\Omega_{K/k}^1$ over K by design) and we saw in class that a finite extension of fields is separable if and only if its Ω^1 vanishes!

Finally, it remains to show $\{f_1, \dots, f_m\}$ is algebraically independent over k_p when viewed inside the field $K' = k_p \otimes_k K$. Since $K' \otimes_K \Omega_{K/k}^1 \simeq \Omega_{K'/k_p}^1$ and $\{df_j\}$ is a K -basis of $\Omega_{K/k}^1$ by design, it follows that these df_j 's also constitute a K' -basis of Ω_{K'/k_p}^1 . Thus, we may rename K'/k_p as K/k to reduce to showing that if k is *perfect* then for any collection elements $\{f_j\}$ in K such that $\{df_j\}$ is K -linearly independent inside $\Omega_{K/k}^1$, the f_j 's are algebraically independent over k inside K .

Suppose to the contrary that $g(f_1, \dots, f_m) = 0$ for some nonzero $g \in k[T_1, \dots, T_m]$. Using the usual lexicographical ordering on exponents of monomials in T_1, \dots, T_m (with the zero polynomial considered to be a constant and hence assigned degree equal to the ordered m -tuple $(0, 0, \dots, 0)$), we may and do choose g to be minimal with respect to the lexicographical ordering of its “degree” (i.e., the largest m -tuple exponent for a monomial that occurs in g). This forces g to be irreducible (since any product of non-constant elements of $k[T_1, \dots, T_n]$ has degree that is strictly larger for the lexicographical order than the degree of either of the factors). Thus, by perfectness of k with characteristic $p > 0$, *some* variable T_{i_0} does not occur in g only through $T_{i_0}^p$ (i.e., some variable occurs in some monomial term of g with an exponent in \mathbf{Z}^+ not divisible by p) because g is irreducible yet $k[T_1^p, \dots, T_m^p] = k[T_1, \dots, T_m]^p$ due to perfectness of k . Hence, $\partial g / \partial T_{i_0} \neq 0$.

Applying the universal $d = d_{K/k} : K \rightarrow \Omega_{K/k}^1$ to both sides of the equation $g(f_1, \dots, f_m) = 0$ gives

$$(2.1) \quad 0 = d(g(f_1, \dots, f_m)) = \sum_{j=1}^m (\partial g / \partial T_j)(f_1, \dots, f_m) df_j.$$

But $\{df_j\}$ is K -linearly independent inside $\Omega_{K/k}^1$ by the way we chose the f_j 's, so the vanishing of the right side of (2.1) forces all coefficients to vanish; i.e., $(\partial g / \partial T_j)(f_1, \dots, f_m) = 0$ for all j . But we saw that some $\partial g / \partial T_{i_0}$ is nonzero, yet *all* partial derivatives of the non-constant g clearly have degree smaller than that of g for the lexicographical order (recall our convention about the meaning of the m -tuple degree for the zero polynomial, for cases when a partial derivative vanishes). Thus, the vanishing of $(\partial g / \partial T_{i_0})(f_1, \dots, f_m)$ violates the degree-minimality by which g was chosen! This completes the proof that $\{f_j\}$ is algebraically independent over k .