Abdullah Naeem Malik

December 12, 2019

Notes:

- Unless specified otherwise, all references are from Paolo Aluffi's *Algebra: Chapter Zero*
- Symbols are conveniently recycled for each solution.

Q1 Let $k \subseteq K$ be a separable, finite extension. Show that $\Omega_{K/k} = 0$

Solution*

To show that $\Omega_{K/k} = 0$, we can show that the morphism $d : K \longrightarrow \Omega_{K/k}$ is trivial. The result will follow since $\Omega_{K/k} = \langle d(\alpha) : \alpha \in K \rangle$. We establish both statements.

We start off with the following observation: for any derivation $D : K \longrightarrow M$ and $\forall \alpha \in K$,

$$D(\alpha^n) = n\alpha^{n-1} D(\alpha) \tag{1}$$

Proof. $D(\alpha^2) = D(\alpha\alpha) = \alpha D(\alpha) + \alpha D(\alpha) = 2\alpha D(\alpha)$. Assume that $D(\alpha^n) = n\alpha^{n-1} D(\alpha)$ holds for some n. Then, $D(\alpha^{n+1}) = D(\alpha\alpha^n) = \alpha D(\alpha^n) + \alpha^n D(\alpha) = \alpha(n\alpha^{n-1} D(\alpha)) + \alpha^n D(\alpha) = n\alpha^n D(\alpha) + \alpha^n D(\alpha)$ $= (n+1)\alpha D(\alpha)$ ■

Recall the formal derivative

$$f(x) = \sum_{i=0}^{n} a_i x^i \longmapsto f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$$

satisfies Liebniz rule, hence $(.)' : k[x] \longrightarrow k[x]$ is a derivation without deception, where the domain is treated as a natural k-algebra (courtesy of the canonical embedding $k \hookrightarrow k[x]$) and the codomain is treated as a $k[x]$-module (every ring is a module over itself).

Now, the (algebraic) extension $k \subseteq K$ gives us, in particular, a ring homomorphism $i : k \longrightarrow K$ so we are allowed to consider the evaluation map $\bar{i} : k[x] \longrightarrow K$ which sends x to any $\alpha \in K$ of choice. As an algebraic extension in general $\forall \alpha \in K$, $\exists$ minimal polynomial $f(x) \in k[x]$ such that $f(\alpha) = 0$. Since the extension is, in particular, separable, $f(x)$ must be separable so by **Lemma VII.4.14,** $f'(x) \neq 0$. In particular, $f'(\alpha) \neq 0$ since

$$\bar{i}\left(\sum_{i=0}^{d} b_i x^i\right) = \sum_{i=0}^{d} i(b_i)\alpha^i$$

defined using an injection i (Cf. **Example III.2.3**) for any polynomial $b_0 + b_1 x + \ldots + b_d x^d$.

With this background in order, we now show that d is trivial. From $f(\alpha) = 0$, we have $d(f(\alpha)) = 0$ since the k-linear d is (also) a morphism of the underlying abelian groups. Focusing on the LHS, we have

$$\begin{aligned} d(f(\alpha)) &= d\left(\sum_{i=0}^{n} i(a_i)\alpha^i\right) = d\left(\sum_{i=0}^{n} a_i \alpha^i\right) \stackrel{\dagger}{=} \sum_{i=0}^{n} a_i d(\alpha^i) \stackrel{\ddagger}{=} \sum_{i=0}^{n} i a_i \alpha^{i-1} d(\alpha) \\ &= d(\alpha)\sum_{i=0}^{n} i a_i \alpha^{i-1} = d(\alpha) f'(\alpha) \end{aligned}$$

where † holds because we have k-linearity and ‡ holds because of **Eq (1)**. Thus, we have $d(\alpha) f'(\alpha) = 0$. In particular, $f'(\alpha) \neq 0$ so we must have $d(\alpha) = 0$.

Showing $\Omega_{K/k} = \langle d(\alpha) : \alpha \in K \rangle$ requires us to stare at the diagram

*Solution taken from **Example 10.26.G** in *Commutative Algebra* by Hideyuki Matsumura

$$
\begin{tikzcd}
K \otimes_k K \arrow[r, "m"] & K \arrow[d, "d"] \\
J \arrow[u, hook] \arrow[r, two heads] & J/J^2 = \Omega_{K/k}
\end{tikzcd}
$$

Here, m is the multiplication map $a \otimes b \longmapsto ab$ and $J = \ker m$. Since J is defined relative to m, and m is defined relative to generators of $K \otimes_R K$, $\Omega_{K/k}$ can be defined in terms of images of generators of K.

Q2 Can you drop the separability hypothesis in **Q1**?

Solution

The hypothesis of separability is used to come up with the minimal, separable polynomial f and the fact $f'(\alpha) \neq 0$ coupled with $d(\alpha) f'(\alpha) = 0$, we concluded that $d(\alpha) = 0$. Thus, if we were to not focus on separability, we would want to preserve $f'(\alpha) \neq 0$ in order to surely arrive at $d(\alpha) = 0$. This fails in, e.g., when $f(x) \in k[x]$ is inseparable and irreducible, or in cases like $f(x) = x^p + 1$ with $char(k) = p > 0$, so let us focus our attention in a decent classification of fields we know of viz. $char(k) = 0$ and $char(k) \neq 0$. In the former, the field is perfect and by **Proposition VII.1.15,** all irreducible polynomials are separable. Hence to discard the notion of separability entirely, we need to restrict ourselves to the $char(k) \neq 0$ case. Even this case needs to be further refined since by **Corollary VII.4.18**, separability cannot fail if $|k| < \infty$.

Thus, if we were to drop the separability hypothesis, we would be left with an infinite field k with $char(k) \neq 0$. However, there are good chances that $f'(x) = 0$ for a non-zero polynomial f so there is no guarantee that $d(\alpha) = 0$. For example, consider $f(x) = x^p - t \in \mathbb{F}_p(t)[x]$, where $\mathbb{F}_p(t)$ is the field of rational functions with coefficients in $\mathbb{Z}/p\mathbb{Z}$. The extension $K = \frac{\mathbb{F}_p(t)[x]}{(f(x))}$ is not separable since $x^p - t = (x-u)^p$ where $u \in K$ is a root of $f(x)$. Yet, $f'(x) = 0$. In fact, since $K = \left\langle 1, u, u^2, ..., u^{p-1} \right\rangle$ (K is a $\mathbb{F}_p(t)$ vector space of dimension p), $d(u^i) = iu^{i-1} d(u)$, and the fact that $d(u)$ is nontrivial, we are justified in saying that $\Omega_{K/\mathbb{F}_p(t)} = \left\langle d(u^i) : 0 \leqslant i < p \right\rangle$ is non-trivial. Therefore, the hypothesis of separability is necessary.

Q3 Let k be a field with $char(k) = p > 0$, and let A be a k-algebra. Let $D : A \longrightarrow A$ be a derivation. Show that D^p is a derivation.

Solution

To make life easy, let us assume that A is commutative, to have $D(a) D(b) = D(b) D(a)$.
Using the base case $D(ab) = aD(b) + bD(a)$, for all n, the following can be easily verified:

$$
D^{(n)}(ab) = \sum_{k=0}^{n} \binom{n}{k} D^{(n-k)}(a) D^{(k)}(b) \tag{2}
$$

with the convention that $D^{(0)} = id_A$. We can, therefore, plug† $n = p$ in **Eq (2)** to give us

$$
D^{(p)}(ab) = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} D^{(p-k)}(a) D^{(k)}(b) \tag{3}
$$

Courtesy of the injection $i : k \longrightarrow A$, the ring A *per se* has characteristic p. Since we are in characteristic p, all coefficients in **Eq** (3), except those with $k = 0$ and $k = p$, are multiples of p, hence yield zero. Thus, $D^{(p)}(ab) = D^{(p)}(a) D^{(0)}(b) + D^{(0)}(a) D^{(p)}(b) = bD^p(a) + aD^p(b)$, making D^p a bona-fide derivation.

Q4 Assume the same hypothesis as Q3. Let $\sigma : A \longrightarrow A$ be the Frobenius homomorphism $a \longmapsto a^p$. Prove that there is an isomorphism $\Omega_{A/k} \cong \Omega_{A/A}$, where in the right-hand side A is considered as an A-algebra via σ.

†Observe that any repeated application of D would still land us in A.

Solution

Let M be any A-module and $\phi : k \longrightarrow A$ be the map giving A a k-algebra structure. This and the given information in the question summons the following commutative diagram:

$$\begin{tikzcd}
 & A \arrow[dr, "\sigma"] & & \Omega_{A/A} \arrow[d, dashed] \\
k \arrow[ur, "\phi"] \arrow[dr, "\sigma_k"'] & & A \arrow[ur, "d_A"] \arrow[r] \arrow[dr, "d_k"'] & M \\
 & k \arrow[ur, "\phi"'] & & \Omega_{A/k} \arrow[u, dashed]
\end{tikzcd}$$

The diamond on the left commutes simply because ϕ is a ring homomorphism: for any $x \in k$, $(\phi \circ \sigma_k)(x) = \phi(\sigma_k(x)) = \phi(x^p) = \phi(x)^p = \sigma(\phi(x)) = (\sigma \circ \phi)(x)$, where $\sigma_k(x) = x^p$ is the Frobenius homomorphism of k. The two triangles on the right commute by construction of the Kähler Differentials. This observation is enough to establish the required isomorphism via abstract nonsense.

To see this further, recall that the universal object $\left(d, \Omega_{A/k}\right)$ (respectively, $\left(d, \Omega_{A/A}\right)$), is initial in the coslice subcategory A/k-$\texttt{Alg}$ (respectively, A/A-$\texttt{Alg}$). The prefix "sub" stems from the fact that the objects are restricted to subobjects $\mathrm{Der}_k(A, M) \subset \mathrm{Hom}_k(A, M)$ (repectively, $\mathrm{Der}_A(A, M) \subset \mathrm{Hom}_A(A, M)$) of the respective coslice categories. So, to show that the Kähler differentials are isomorphic, we can show that they are essentially derived from the same categories. Thus, we need to focus on the categories A-$\texttt{Alg}$ and k-$\texttt{Alg}$.

Now, the category R-$\texttt{Alg}$ for any ring R is, again, a coslice category $R/\texttt{Rng}$. In our case, we can consider the category $\texttt{Rng}_p$, consisting of rings of characteristic p as objects. Consider the identity functors $\mathcal{F}, \mathcal{G}$:$\texttt{Rng}_p \longrightarrow \texttt{Rng}_p$ and the natural transformation $\eta : \mathcal{F} \rightsquigarrow \mathcal{G}$. The latter is defined as follows: for $\phi \in \mathrm{Hom}_{\texttt{Rng}_p}(X, Y)$, $\eta_\phi = \sigma_X$ where $\sigma_X : X \longrightarrow X$ is the map $x \longmapsto x^p$. This gives us the diagram in **Defition VIII.1.15**:

$$\begin{tikzcd}
\mathcal{F}(X) \arrow[r, "\mathcal{F}(\phi)"] \arrow[d, "\eta_X"'] & \mathcal{F}(Y) \arrow[d, "\eta_Y"] \\
\mathcal{G}(Y) \arrow[r, "\mathcal{G}(\phi)"] & \mathcal{G}(Y)
\end{tikzcd}$$

The diagram commutes by virtue of the fact that ϕ is a homomorphism of rings. Therefore, for our purposes, the choice of R for $R/\texttt{Rng}_p$ is immaterial and the result follows.

A more direct way is as follows: we know that both $\left(d_A, \Omega_{A/A}\right)$ and $\left(d_k, \Omega_{A/k}\right)$ exist and are both A-modules. Placing either instead of M in the commutative diagram in the start gives us morphisms $f : \Omega_{A/A} \longrightarrow \Omega_{A/k}$ and $g : \Omega_{A/k} \longrightarrow \Omega_{A/A}$.

$$\begin{tikzcd}
\Omega_{A/A} \arrow[d, dashed, "f"] & & \Omega_{A/A} \arrow[d, dashed, "id_{\Omega_{A/A}}"] \\
\Omega_{A/k} & A \arrow[l, dashed, "d_k"'] \arrow[r, dashed, "d_A"] \arrow[ul, "d_A"'] \arrow[ur, "d_A"] \arrow[dl, "d_k"] \arrow[dr, "d_k"'] & \Omega_{A/A} \\
\Omega_{A/k} \arrow[u, dashed, "id_k"] & & \Omega_{A/k} \arrow[u, dashed, "g"']
\end{tikzcd}$$

If we can show that $fg = id_{\Omega_{A/k}}$ and $gf = id_{\Omega_{A/A}}$, we will be done. The universal property tells us that $fd_A = d_k$ and $gd_k = d_A$. Thus, $fgd_k = d_k$ and $gfd_A = d_A$. Since d_k and d_A are unique, the result follows.

Q5 Assume R is a commutative ring and let R-$\texttt{Alg}$ be the category of commutative R-algebras. Let A be an R-algebra and M an A-module. For all $a, a' \in A$ and $m, m' \in M$, define a product structure $(a, m)(a', m') \longmapsto (aa', am' + am')$ on $D_A(M) = A \oplus M$. Show that (a) $D_A(M)$ is an augmented A-algebra; and (b) $\mathrm{Hom}_{R\text{-}\texttt{Alg}/A}(B, D_A(M)) \cong \mathrm{Hom}_B\left(\Omega_{B/R}, u_* M\right) \cong \mathrm{Hom}_A\left(A \otimes_B \Omega_{B/R}, M\right)$

Solution

(a) In order to show that $D_A(M)$ is an augmented A-algebra, we first need to show that $D_A(M)$ is an A-algebra. For this, we need to show the existence of a ring homomorphism $\alpha : A \longrightarrow D_A(M)$ such that $\alpha(A)$ is in the centre of $D_A(M)$.

$D_A(M)$ is necessarily an A-module, as it is the coproduct of two A-modules (the R-algebra A is an A-module). This means we have a homomorphism $\sigma_D : A \longrightarrow \mathrm{End}_{Ab}(D_A(M))$ given by $\sigma_A \oplus \sigma_M$ where $\sigma_A : A \longrightarrow \mathrm{End}_{Ab}(A)$ and $\sigma_M : A \longrightarrow \mathrm{End}_{Ab}(M)$ are, respectively, the A-module structures on A and M[‡].

Now, note that $D_A(M) = A \oplus M$ implies that the short exact sequence of A-modules

$$0 \longrightarrow A \xrightarrow{\alpha} A \oplus M \longrightarrow M \longrightarrow 0$$

splits. Thus, we have for ourselves at least a group homomorphism from A to $D_A(M)$ given by $a \longmapsto (a, 0)$. To show that this is, in addition, a ring homomorphism, we first show that with the given product operation, $D_A(M)$ is a ring with the obvious identity $1_{D_A(M)} = (1_A, 0)$ and the distributive identities.

Proof. $(a_1, m_1)[(a_2, m_2) + (a_3, m_3)] = (a_1, m_1)(a_2 + a_3, m_2 + m_3)$

$= (a_1a_2 + a_1a_3, a_1m_2 + a_1m_3 + a_2m_1 + a_3m_1)$

$= (a_1a_2, a_1m_2 + a_2m_1) + (a_1a_3, a_1m_3 + a_3m_1)$

$= (a_1, m_1)(a_2, m_2) + (a_1, m_1)(a_3, m_3)$

Furthermore, $(1_A, 0)(a, m) = (1_Aa, 1_Am + 0m) = (a, m)$ and $(a, m)(1_A, 0) = (a1_A, 0m + 1_Am) = (a, m)$. However, the multiplicative binary operation on $D_A(M)$ is easily seen to be commutative as

$$(a_1, m_1)(a_2, m_2) = (a_1a_2, a_1m_2 + a_2m_1) = (a_2a_1, a_2m_1 + a_1m_2) = (a_2, m_2)(a_1, m_1)$$

Thus, we are justified in verifying only one distributive identity and discarding the requirement that $\alpha(A)$ be contained in the centre of $D_A(M)$. ■

Clearly, $1_A \longmapsto 1_{D_A(M)}$ and $\alpha(ab) = (ab, 0) = (a, 0)(b, 0) = \alpha(a)\alpha(b)$. Thus, $D_A(M)$ is a bona-fide A-algebra.

Since the short exact sequence of A-modules

$$0 \longrightarrow A \xrightarrow{\alpha} D_A(M) \longrightarrow M \longrightarrow 0$$

splits, by the Splitting Lemma, we have an A-module homomorphism $\pi : D_A(M) \longrightarrow A$ such that $\pi \circ \alpha = id_A$. Since our R-algebra A is, in fact, an A-algebra via the ring homomorphism $\pi \circ \alpha = id_A : A \longrightarrow A$ and so is $D_A(M)$, we can view our A-module homomorphisms α and π as an A-algebra homomorphism.

(b) Let us first take care of the two terms on the right. $\mathrm{Hom}_B\left(\Omega_{B/R}, u_*M\right)$ is easily seen to be isomorphic to $\mathrm{Hom}_A\left(A \otimes_B \Omega_{B/R}, M\right)$ by **Proposition VII.3.6**. This isomorphism follows since the functor $u_* : A$-$\mathtt{Mod} \longrightarrow B$-$\mathtt{Mod}$ is right-adjoint to the functor $\_ \otimes_B A : B$-$\mathtt{Mod} \longrightarrow A$-$\mathtt{Mod}$. This opposition in the tensor can easily be reconciled: $\Omega_{B/R} \otimes_B A \cong A \otimes_B \Omega_{B/R}$ as B-modules by construction (Cf. §**VII.2.1**), where the B-module A exists since we have $B \xrightarrow{u} A \xrightarrow{\sigma_A} \mathrm{End}_{Ab}(A)$; and by **Exercise VII.3.9**, $\Omega_{B/R} \otimes_B A \cong A \otimes_B \Omega_{B/R}$ as A-modules. We, therefore, have the privilege of concluding that $\mathrm{Hom}_B\left(\Omega_{B/R}, u_*M\right) \cong \mathrm{Hom}_A\left(A \otimes_B \Omega_{B/R}, M\right)$.

To show the $\mathrm{Hom}_B\left(\Omega_{B/R}, u_*M\right) \cong \mathrm{Hom}_{R\text{-}\mathtt{Alg}/A}(B, D_A(M))$, we show a correspondence of morphisms in each hom-set and the isomorphism will follow from abstract nonsense. Consider the following diagram:

$$\begin{tikzcd}
 & R \arrow[r] \arrow[d] & A \\
\Omega_{B/R} \arrow[dr, dashed, "D"'] & B \arrow[l, "d"'] \arrow[r] \arrow[ur, "u"] \arrow[d, "\bar{D}"] & D_A(M) \arrow[u, "\pi"'] \arrow[d, two heads, "p"] \\
 & u_*(M) & M \arrow[l, "u_*"]
\end{tikzcd}$$

[‡]In fact, $\sigma_A(a) = \lambda_a$, where $\lambda_a : A \longrightarrow A$ is a ring homomorphism given by $\lambda_a(x) = ax$, is an embedding by **Proposition III.2.7**. This notation is carried on for Q8.

Given any $D \in \mathrm{Hom}_B\left(\Omega_{B/R}, u_*(M)\right)$, we can find an R-linear function (a derivation) $\overline{D} \in \mathrm{Hom}_R(B, u_*(M))$ and using this, we can form $u \oplus \overline{D}^* \in \mathrm{Hom}_{R\texttt{-Alg}/A}(B, D_A(M))$. To qualify the latter, we observe that $\pi \circ \left(u \oplus \overline{D}^*\right) = u$, where $\overline{D}^* \in \mathrm{Hom}_A(B, M)$ holds by definition of extension of scalars (here, B is treated as an A-module via $B \otimes_B A$). Conversely, given any $f \in \mathrm{Hom}_{R\texttt{-Alg}/A}(B, D_A(M))$, by axioms of a category, we can form $\overline{D} = u_* \circ p \circ f \in \mathrm{Hom}_R(B, u_*(M))$. If $\overline{D}$ is a derivation, we will have found our $D \in \mathrm{Hom}_B\left(\Omega_{B/R}, u_* M\right)$.

Q6 Same hypothesis as Q4.

- For $a \in A$, consider
$$C : a \longmapsto a^{p-1} da$$
Show that C gives a derivation
$$C : A \longrightarrow \sigma_* \Omega_{A/k}$$
- Verify that $a, b \in A$:
$$C(a+b) - C(a) - C(b) = d \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} a^i b^{p-i} \tag{4}$$
- Show that C factors through $H^1_{DR}\left(\sigma_* \Omega_{A/k}\right)$
- Obtain a homomorphism
$$\overline{C} : \Omega_{A/k} \longrightarrow \sigma_* H^1_{DR}(A)$$
- Show that $\overline{C}$ extends to a graded homomorphism
$$\overline{C} : \Omega^\bullet_{A/k} \longrightarrow \sigma_* H^\bullet_{DR}(A)$$

Solution

For the A-algebra A, we need to show that the map C is A-linear and satisfies the Leibniz Rule[§]: $C(ab) = a \cdot C(b) + b \cdot C(a)$. Assuming that d refers to the map $d : A \longrightarrow \Omega_{A/A}$ (in which case the codomain $\sigma_* \Omega_{A/k}$ makes sense), we first show that the definition satisfies Leibniz Rule:

$$\begin{aligned}
C(ab) &= (ab)^{p-1} \cdot d(ab) && (5)\\
&= a^{p-1} b^{p-1} \cdot (a \cdot d(b)) + a^{p-1} b^{p-1} \cdot (b \cdot d(a))\\
&= \left(a^{p-1} b^{p-1} a\right) \cdot d(b) + \left(a^{p-1} b^{p-1} b\right) \cdot d(a) && (6)\\
&= \left(a^p b^{p-1}\right) \cdot d(b) + \left(b^p a^{p-1}\right) \cdot d(a)\\
&= a \cdot \left(b^{p-1} \cdot d(b)\right) + b \cdot \left(a^{p-1} \cdot d(a)\right) = a \cdot C(b) + b \cdot C(a)
\end{aligned}$$

where **equality in (5)** follows from the fact that in an A-algebra, scalar multiplication is compatible with the multiplication structure of the scalars. Next, to show A-linearity, we establish scalar multiplication first:

$$\begin{aligned}
C(\alpha \cdot a) &= (\alpha \cdot a)^{p-1} \cdot d(\alpha \cdot a) \overset{\diamondsuit}{=} (\alpha \cdot a)^{p-1} \cdot (\alpha \cdot d(a)) = \left((\alpha a)^{p-1} \alpha\right) \cdot d(a)\\
&= \left((\alpha a)^{p-1} \alpha\right) \cdot d(a) = \left(\alpha^p a^{p-1}\right) \cdot d(a) = \alpha \cdot \left(a^{p-1} \cdot d(a)\right) = \alpha \cdot C(a)
\end{aligned}$$

where $\diamondsuit$ follows since d is A-linear.

To show $C(a+b) = C(a) + C(b)$, observe that the d applied to the sum on the right of **Eq (4)** is defined for scalars, hence is zero. This is because $(a+b)^p = a^p + b^p$ (because of Frobenius homomorphism) and we have

$$0 = (a+b)^p - a^p - b^p = \sum_{i=0}^{p} \binom{p}{i} \left(a^i\right) b^{p-i} - a^p - b^p = \sum_{i=1}^{p-1} \binom{p}{i} \left(a^i\right) b^{p-i}$$

[§]The scalar multiplication of a by scalar α is given by $\alpha \cdot a = \sigma(\alpha) a = \alpha^p a$.

In fact,

$$d\left((a+b)^p\right) = d\left(a^p + b^p\right) = d\left(a^p\right) + d\left(b^p\right) = \left(pa^{p-1}\right) \bullet d\left(a\right) + \left(pb^{p-1}\right) \bullet d\left(b\right) = 0$$

We, therefore, simply show the equality in **Eq (4)**. For this, we resort to Liebniz Rule.

$$\begin{aligned}
0 &= d\left((a+b)^p\right) = d\Big((a+b)(a+b)^{p-1}\Big) \\
&= (a+b)^{p-1} \bullet d(a+b) + (a+b) \bullet d\Big((a+b)^{p-1}\Big) \\
&= C(a+b) + a \bullet d\left(\sum_{i=0}^{p-1} \binom{p-1}{i} \left(a^i\right) b^{p-1-i}\right) + b \bullet d\left(\sum_{i=0}^{p-1} \binom{p-1}{i} \left(a^i\right) b^{p-1-i}\right) \\
&= C(a+b) + a \bullet d\left(\sum_{i=0}^{p} \binom{p}{i} \left(a^i\right) b^{p-1-i}\right) - a \bullet d\left(a^p\right) + b \bullet d\left(\sum_{i=1}^{p} \binom{p}{i} \left(a^i\right) b^{p-i}\right) - b \bullet d\left(b^p\right) \\
&= C(a+b) - d\left(\sum_{i=0}^{p-1} \binom{p-1}{i} \left(a^i\right) b^{p-i}\right) - a^{p-1} \bullet d(a) - b^{p-1} \bullet d(b) \\
&= C(a+b) - d\left(\sum_{i=0}^{p-1} \binom{p-1}{i} \left(a^i\right) b^{p-i}\right) - C(a) - C(b)
\end{aligned}$$

We now have the following diagram:

$$\begin{tikzcd}
 & \Omega_{A/A} \arrow[d, dashed] & \\
A \arrow[ur, "d_A"] \arrow[r, "C"] \arrow[dr, "d_k"'] & \sigma_*\Omega_{A/k} \arrow[r, hook] & \bigoplus_{n\geqslant 0} \sigma_*\Omega^n_{A/k} \\
 & \Omega_{A/k} \arrow[u, dashed] &
\end{tikzcd}$$

Q8 Let $\pi : B \longrightarrow A$ be a surjective homomorphism of commutative R-algebras. Let $M = \ker \pi$ and consider the short exact sequence

$$0 \longrightarrow M \longrightarrow B \longrightarrow A \longrightarrow 0 \tag{7}$$

Show that (a) if $M^2 = 0$, then M is an A-module and (b) if the underlying sequence of R-modules in (7) splits, under what condition is $B \cong D_A(M)$ as R-algebras, where $D_A(M)$ is as in $(Q5)$.

Solution
(a) We are given the following situation:

$$\begin{tikzcd}
 & \mathrm{End}_{\mathtt{Ab}}(M) & & \mathrm{End}_{\mathtt{Ab}}(B) & \mathrm{End}_{\mathtt{Ab}}(A) & \\
0 \arrow[r] & M \arrow[rr, hook, "i"'] & & B \arrow[ull, "\sigma_M"'] \arrow[u, "\sigma_B"] \arrow[r, two heads, "\pi"] & A \arrow[u, "\sigma_A"] \arrow[r] & 0
\end{tikzcd}$$

The ideal M is a B-module and the module structure is given by σ_M where $\sigma_M(b) = \lambda_b$ where $\lambda_b(x) = bx$ is the multiplication operation, making B a natural B-module. Similarly, $\sigma_A(a) = \lambda_a$. The composition $\sigma_A \circ \pi$ gives the abelian group A a B-module structure. This restriction of scalars makes $\pi_*(A)$ (effectively, A) a B-module, whence the short exact sequence of B-modules given in the question.

Thus, to show that M is an A-module, we would need a well-defined function $\sigma : A \longrightarrow \mathrm{End}_{\mathtt{Ab}}(M)$, which we propose to be $\sigma(a) = \sigma_M \pi^{-1}(a)$ where $\pi^{-1}(a) = b + M$. This, we establish.

Proof. $a_1 = a_2$

$\implies \pi^{-1}(a_1) = \pi^{-1}(a_2)$

$\implies b_1 + M = b_2 + M$

$\implies \sigma_M(b_1 + M) = \sigma_M(b_2 + M)$

$\implies \sigma_M(b_1) + \sigma_M(M) = \sigma_M(b_2) + \sigma_M(M)$

$\implies \lambda_{b_1} + \lambda_M = \lambda_{b_2} + \lambda_M$.

We also show that either one of these is an element in $\mathrm{End}_{\mathtt{Ab}}(M)$. Observe that $(\lambda_{b_1} + \lambda_M)(M) = b_1 M + M^2 \overset{\dagger}{=} b_1 M \overset{\dagger\dagger}{=} M$ where † follows since $M^2 = 0$ and †† follows since M is an ideal.

In fact, † tells us that λ_M is the trivial map and hence the additive identity in $\mathrm{End}_{\mathtt{Ab}}(M)$ so we may very well have $\sigma(a) = \lambda_b$ where $\pi(b) = a$. With this observation, verification of fact that $\sigma(a_1 + a_2) = \sigma(a_1) + \sigma(a_2)$ and $\sigma(a_1 a_2) = \sigma(a_1)\sigma(a_2)$ and $\sigma(1_A) = \lambda_{1_B} = id_B$ is a matter of routine ■

A more "frog" approach, as Freeman Dyson would say, would be to define the action $\cdot : A \times M \longrightarrow M$ by $\cdot(a, m) = a \cdot m = \pi^{-1}(a)\, m$ (because of commutativity of B, we can simply focus on one-side). This defines an A-module structure on M.

Proof. Since $\pi^{-1}(a) = b + M$, we have $\pi^{-1}(a)\, m = (b + M)\, m = bm + Mm$. Because M is an ideal $bm \in M$. Since $M^2 = 0$, we have $Mm = 0$ and so, the function is well-defined. Then, the following are easy consequences:

i) $(a_1 + a_2) \cdot m = \pi^{-1}(a_1 + a_2)\, m = (b_1 + b_2 + M)\, m = (b_1 + M + b_2 + M)\, m = (b_1 + M)\, m + (b_2 + M)\, m = a_1 \cdot m + a_2 \cdot m$

ii) $a \cdot (m_1 + m_2) = (b + M)(m_1 + m_2) = (b + M)\, m_1 + (b + M)\, m_2 = a \cdot m_1 + a \cdot m_2$

iii) $(a_1 a_2) \cdot m = \pi^{-1}(a_1 a_2)\, m = (b_1 b_2 + M)\, m = ((b_1 + M)(b_2 + M))\, m = (b_1 + M)((b_2 + M)\, m) = (b_1 + M)(a_2 \cdot m) = a_1 \cdot (a_2 \cdot m)$

iv) $1_A \cdot m = \pi^{-1}(1_A)\, m = (1_B + M)\, m = m + Mm = m$ ■

(b) We are only missing the multiplicative structure. For this to hold, the obvious route would be to ask for exact sequence to be that for rings, but this is too much to ask for:

$$\begin{tikzcd} & & R \arrow[dl, "\phi_M"'] \arrow[d, dashed, "\phi_B"] \arrow[dr, "\phi_A"] & & \\ 0 \arrow[r] & M \arrow[r, hook, "i"] & B \arrow[r, "\pi"] & A \arrow[r] & 0 \end{tikzcd}$$

Since π is a given morphism of R-algebras, we know that $\phi_A = \pi \circ \phi_B$, where ϕ_A and ϕ_B are the maps which, respectively, give A and B their R-algebra structure. If we can show that $\phi_B = i \circ \phi_M$, then we would have a short exact sequence of R-algebras. This requires R-algebra structure on M, which can only be possible if M were a ring in the first place i.e., have the identity. This would make the map π trivial.

A weaker requirement would be to ask for M to be an A-module and this is accomplished via $M^2 = 0$. By **Q5**, what this does for us is it allows us to view $D_A(M)$ as an (augmented) A-algebra and, by restriction of scalars via ϕ_{A*}, an R-algebra.

In another scenario, we could consider our final commutative diagram:

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, hook, "i"] \arrow[d, "id_M"] & B \arrow[r, "\pi"] & A \arrow[r] \arrow[d, "id_A"] & 0 \\ 0 \arrow[r] & M \arrow[r, hook, "i'"] & D \arrow[r, "\pi'"] & A \arrow[r] & 0 \end{tikzcd}$$

Here, i is the inclusion map of R-modules and π is the given morphism of R-algebras, which is, in particular, a morphism of R-modules. For the bottom short-exact sequence of A-modules, $i'(m) = (0, m)$ and $\pi'(a, m) = a$. Since $D_A(M)$ is canonically an R-module, so given an R-linear function $f : B \longrightarrow D$, we would have $B \cong D$ as R-modules, by **Exercise III.7.11**. Since both are, in addition rings, the existence of f gives us another condition.