

Appendix A

Algebra à la carte

A.1 Introduction

In what follows, rings are always commutative with 1. The proofs of the results below are contained in most Algebra textbooks (e.g. Lang [?]).

A.2 Unique factorization

Theorem A.2.1. *Let R be a UFD. Then $R[t]$ is a UFD. Moreover a polynomial $p = a_0t^d + a_1t^{d-1} + \dots + a_d$ is prime if and only if*

1. p is prime when viewed as element of $K[t]$, where K is the field of fractions of R ,
2. and the greatest common divisor of a_0, a_1, \dots, a_d is 1.

Corollary A.2.2. *The ring $\mathbb{K}[x_1, \dots, x_n]$ is a unique factorization domain.*

Proof. By induction on n . If $n = 0$, the ring is a field, and hence it is trivially a UFD. The inductive step follows from Theorem A.2.2, because $\mathbb{K}[x_1, \dots, x_n] \cong \mathbb{K}[x_1, \dots, x_{n-1}][t]$. \square

A.3 Noetherian rings

Definition A.3.1. A (commutative unitary) ring R is *Noetherian* if every ideal of R is finitely generated.

Example A.3.2. A field K is Noetherian, because the only ideals are $\{0\} = (0)$ and $K = (1)$. The ring \mathbb{Z} is Noetherian, because every ideal has a single generator.

Lemma A.3.3. *A (commutative unitary) ring R is Noetherian if and only if every ascending chain*

$$I_0 \subset I_1 \subset \dots \subset I_m \subset \dots$$

of ideals of R (here I_m is defined for all $m \in \mathbb{N}$, and $I_m \subset I_{m+1}$ for all $m \in \mathbb{N}$) is stationary, i.e. there exists $m_0 \in \mathbb{N}$ such that $I_m = I_{m_0}$ for $m \geq m_0$.

Proof. Suppose that R is Noetherian. The union $I := \bigcup_{m \in \mathbb{N}} I_m$ is an ideal because the $\{I_m\}$ form a chain. By Noetherianity I is finitely generated, say $I = (a_1, \dots, a_r)$. There exists m_0 such that $a_j \in I_{m_0}$ for $j \in \{1, \dots, r\}$, and hence $I = I_{m_0}$. Let $m \geq m_0$; then $I_m \subset I$ and $I \subset I_m$, hence $I = I_m$. Thus $I_{m_0} = I_m$ for $m \geq m_0$.

Now suppose that every ascending chain of ideals of R is stationary. Let $I \subset R$ be an ideal. Suppose that I is *not* finitely generated. Let $a_1 \in I$. Then $(a_1) \subsetneq I$ because I is not finitely generated; let

$a_2 \in (I \setminus (a_1))$. Then $(a_1, a_2) \subsetneq I$ because I is not finitely generated. Iterating, we get a non stationary chain of ideals (contained in I)

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \dots \subsetneq (a_1, \dots, a_m) \subsetneq$$

This is a contradiction. □

Example A.3.4. The ring $\text{Hol}(\mathbb{K})$ of entire functions of one variable is *not* Noetherian. In fact let $f_m \in \text{Hol}(\mathbb{K})$ be defined by

$$f_m(z) := \prod_{n=m}^{\infty} \left(1 - \frac{z^2}{n^2}\right), \quad m \geq 1.$$

Then $(f_m) \subsetneq (f_{m+1})$. Thus $(f_1) \subset (f_2) \subset \dots \subset (f_m) \subset \dots$ is a non-stationary ascending chain of ideals, and hence $\text{Hol}(\mathbb{K})$ is not Noetherian by Lemma A.3.3.

Theorem A.3.5. *Let R be a Noetherian commutative ring. Then $R[t]$ is Noetherian.*

Proof. For a non zero $f \in R[t]$, we let $\ell(f)$ be the *leading coefficient* of f , i.e. if $f = \sum_{i=0}^m c_i t^i$ with $c_m \neq 0$, then $\ell(f) = c_m$.

Let $I \subset R[t]$. We must prove that I is finitely generated. If $I = (0)$ there is nothing to prove and hence we may assume $I \neq (0)$. Thus the set

$$\ell(I) := \{\ell(f) \mid 0 \neq f \in I\}$$

is non-empty and it makes sense to define

$$J := \langle \ell(I) \rangle \subset R$$

as the ideal of R generated by $\ell(I)$. By hypothesis J is finitely generated: $J = (c_1, \dots, c_s)$. Since J is generated by $\ell(I)$ we may assume that each generator is the leading coefficient of a polynomial in I , i.e. for each $1 \leq i \leq s$ there exists $f_i \in I$ such that $\ell(f_i) = c_i$. Let

$$d := \max_{1 \leq i \leq s} \{\deg f_i\}.$$

Let $H := I \cap \{f \in R[t] \mid \deg f \leq d\}$. Then H is a submodule of $\{f \in R[t] \mid \deg f \leq d\} \simeq R^{d+1}$ (as R -modules). Since R is Noetherian every submodule of R^{d+1} is finitely generated (argue by induction on d ; if $d = 0$ it holds by definition of Noetherian ring, if $d > 0$ consider the projection $R^{d+1} \rightarrow R$) and hence

$$H = (g_1, \dots, g_t).$$

Let us prove that

$$I = (f_1, \dots, f_s, g_1, \dots, g_t).$$

In fact let $f \in I$. If $\deg f \leq d$ then $f \in H$ and hence $f \in (g_1, \dots, g_t) \subset (f_1, \dots, f_s, g_1, \dots, g_t)$. Now suppose that $\deg f > d$. Then $\ell(f) = \sum_{i=1}^s a_i c_i$. Let

$$h := f - \sum_{i=1}^s a_i t^{\deg f - \deg f_i} f_i.$$

Then $\deg h < \deg f$. Since $\sum_{i=1}^s a_i t^{\deg f - \deg f_i} f_i \in (f_1, \dots, f_s, g_1, \dots, g_t)$ it suffices to prove that $h \in I$. If $\deg h \leq d$ we are done, otherwise we iterate until we get down to a polynomial of degree less or equal to d . □

Theorem A.3.6 (Hilbert's basis Theorem). *Every ideal of $\mathbb{K}[x_1, \dots, x_n]$ is finitely generated.*

Proof. By induction on n . If $n = 0$, the ring is a field, and hence is Noetherian. The inductive step follows from Theorem A.3.5, because $\mathbb{K}[x_1, \dots, x_n] \cong \mathbb{K}[x_1, \dots, x_{n-1}][t]$. □

A.4 Extensions of fields

An extension of fields $F \subset E$ is *algebraic* if every $\alpha \in E$ is the root of a non zero polynomial $\psi \in F[z]$. If this is the case, the set of polynomials vanishing on α is a non zero ideal $F[z]$, and hence it is generated by a unique monic polynomial φ , which is the *minimal polynomial of α over F* . Of course φ is irreducible, hence prime. The subfield of F generated by F and α is isomorphic to the quotient $F[z]/(\varphi)$.

An extension is an *algebraic closure of F* , if it is algebraic over F , and every polynomial in $F[z]$ has a root in E .

Theorem A.4.1 (Chapter VII in [?]). *An algebraic closure exists, and is unique up to isomorphism, i.e. if E_1, E_2 are two algebraic closures, there exists an isomorphism $E_1 \xrightarrow{\sim} E_2$ which is the identity on F .*

One denotes “the” algebraic closure of F by F^a , or by \overline{F} . Notice that a non constant polynomial in $F[z]$ decomposes in \overline{F} as a product of polynomials of degree 1 (it has a root, hence it is divisible by a linear term, if the quotient is not constant it has a root hence it is divisible...)

Let $[E : F]$ be the dimension of E as vector space over F - the *degree of E over F* . Notice that if $[E : F]$ is finite, then E is an algebraic extension of F . Suppose that E is algebraic over F . One defines another degree of E over F as follows. Let $\sigma : F \hookrightarrow L$ be an embedding into a field which is an algebraic closure of $\sigma(F)$. An extension of σ to E is an embedding $\tilde{\sigma} : E \hookrightarrow L$ such that $\tilde{\sigma}|_F = \sigma$. The number of such extensions is independent of the embedding $\sigma : F \hookrightarrow L$, and is the *separable degree of E over F* - one denotes it by $[E : F]_s$.

Example A.4.2. Let $\varphi \in F[z]$ be an irreducible monic polynomial, and let $E = F[z]/(\varphi)$. Let $\alpha \in E$ be the class of z : by construction the minimal polynomial of α is equal to φ .

Let $\sigma : F \hookrightarrow L$ be an embedding into a field which is an algebraic closure of $\sigma(F)$. An extension of σ to E is determined by its value on α , and moreover such value can be chosen to be any root of φ in L . Hence the separable degree of E over F is the number of roots of φ in \overline{F} (not counted with multiplicity).

If the formal derivative $\frac{d\varphi}{dz}$ is not the zero polynomial, then since its degree is strictly smaller than $\deg \varphi$, and φ is prime, the ideal $(\varphi, \frac{d\varphi}{dz})$ is equal to $F[z]$, and thus $\varphi, \frac{d\varphi}{dz}$ have no common roots. It follows that all the roots of φ have multiplicity 1, and the separable degree of E over F is equal to $\deg \varphi$, which is also the degree of E over F . Hence in this case $[E : F] = [E : F]_s$.

The formal derivative $\frac{d\varphi}{dz}$ is the zero polynomial only if $\text{char } F = p > 0$, and $\varphi = \psi(z^p)$, where $\psi \in F[z]$, i.e. all monomials appearing in φ have exponent a multiple of p . Iterating, we may write $\varphi = \rho(z^{p^r})$, where $\rho \in F[z]$ is such that $\frac{d\rho}{dz}$ is not the zero polynomial. Hence the number of roots of φ is equal to the degree of $h\rho$, and thus $[E : F]_s = \deg \rho$.

Since $[E : F] = \deg \varphi = p^r \cdot \deg \rho = [E : F]_s$, we see (at least in this case) that the separable degree divides the degree. Moreover, let $\beta = \alpha^{p^r}$. Then $E^s := F[\beta]$ is a separable extension of F such that $[E^s : F] = [E : F]_s$, and the extension $E \supset E^s$ is obtained by adjoining p -th roots, and iterating.

The result below states that the example given above is typical.

Theorem A.4.3 (Chapter VII in [?]). *Let $E \supset F$ be a finite extension of fields, i.e. $[E : F]$ is finite. There exists a maximal separable extension $E^s \supset F$, containing all subfields of E over F which are separable. The separable degree $[E : F]_s$ is equal to the degree of the extension $E^s \supset F$. The extension $E^s \supset F$ has a primitive element, i.e. there exists $\beta \in E^s$ generating E^s over F . Suppose that $E^s \neq E$; then $\text{char } F = p > 0$, and if $\alpha \in E$, the minimal polynomial of α over E^s is equal to $z^{p^r} - \gamma$ for some $r \geq 0$, and $\gamma \in E^s$.*

Example A.4.4. Let $E = \mathbb{F}_p(w, z)$, and let $F = \mathbb{F}_p(w^p, z^p)$. Then $E^s = F$ (in this case one says that $E \supset F$ is a *purely inseparable* extension, and there is no primitive element of E over F).

Elements $\alpha_1, \dots, \alpha_n \in E$ are *algebraically dependent* over F if there exists a non zero polynomial $\Phi \in F[z_1, \dots, z_n]$ such that $\Phi(\alpha_1, \dots, \alpha_n) = 0$ (strictly speaking, we should say that the set $\{\alpha_1, \dots, \alpha_n\}$

is algebraically dependent over F). A collection $\{\alpha_i\}_{i \in I}$ of elements of E is *algebraically independent* over F if there does *not* exist a non empty finite $\{i_1, \dots, i_n\} \subset I$ such that $\alpha_{i_1}, \dots, \alpha_{i_n}$ are algebraically dependent (with the usual abuse of language, we also say that the α_i 's are algebraically independent). A *transcendence basis* of E over F is a maximal set of algebraically independent elements of E over F . There always exists a transcendence basis, by Zorn's Lemma. One proves that any two transcendence bases have the same cardinality, which is the *transcendence degree* of E over F ; we denote it by $\text{Tr. deg}_F(E)$. An extension is algebraic if and only if its transcendence degree is zero.

Every finitely generated extension $E \supset F$ can be obtained as a composition of extensions $F \subset K$ and $K \subset E$, where $F \subset K$ is a *purely transcendental extension*, i.e. there exists a transcendence basis $\{\alpha_1, \dots, \alpha_n\}$ of K over F such that $K = F(\alpha_1, \dots, \alpha_n)$ (thus $F(\alpha_1, \dots, \alpha_n)$ is isomorphic to the field of rational functions in n indeterminates with coefficients in F), and $F \subset K$ is a finitely generated algebraic extension.

Definition A.4.5. Let $E \supset F$ be an extension of fields. A transcendence basis $\{\alpha_1, \dots, \alpha_n\}$ of E over F is *separating* if E is a separable extension of the subfield $F(\alpha_1, \dots, \alpha_n)$. The extension $E \supset F$ is *separably generated* if there exists a separating transcendence basis of E over F .

Theorem A.4.6 (Thm 26.2 in [?]). *If \mathbb{K} is an algebraically closed field, any finitely generated extension $E \supset \mathbb{K}$ is separably generated.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be a transcendence basis of E over \mathbb{K} . Hence the field $F := \mathbb{K}(\alpha_1, \dots, \alpha_n)$ is isomorphic to the field of rational functions in n indeterminates, and $E \supset F$ is a finite extension. Let β_1, \dots, β_r be elements of E algebraic over F , which generate E over F . If all such β_i 's are separable over F (i.e. the subfield of E generated by F and β_i is separable over F), then E is separable over F (see Chapter VII in [?]).

Suppose that one of the β_i 's is not separable over F . Then $\text{char } F = \text{char } \mathbb{K} = p > 0$. We may reorder the β_i 's so that each of β_1, \dots, β_s is separable over F , and each of the $\beta_{s+1}, \dots, \beta_r$ is not separable over F . We find suitable replacements of the α_j 's so that E is a separable extension of the subfield generated by the new transcendence basis. Since β_{s+1} is algebraic over F , there exists a polynomial $\Phi \in \mathbb{K}[z_1, \dots, z_{n+1}]$ such that

$$\Phi(\alpha_1, \dots, \alpha_n, \beta_{s+1}) = 0.$$

We may, and will, assume that Φ is irreducible. We claim that there exists $i \in \{1, \dots, n\}$ such that $\frac{\partial \Phi}{\partial z_i} \neq 0$. In fact, suppose the contrary. Then all partial derivatives of Φ are zero, because β_{s+1} is not separable over F (see Example A.4.2). Write

$$\Phi = \sum_{I \in \mathcal{I}} a_I z^I,$$

where \mathcal{I} is a set of multiindices, and we assume that $a_I \neq 0$ for every $I \in \mathcal{I}$. Since $\frac{\partial \Phi}{\partial z_i} \neq 0$ for all $i \in \{1, \dots, n+1\}$, it follows that each $I \in \mathcal{I}$ is equal to pJ , for a multiindex J . On the other hand there exists a (unique) p -th root of a_I , because \mathbb{K} is algebraically closed. It follows that $\Phi = \Psi^p$. This is a contradiction because Φ is irreducible, and hence we have proved that there exists $i \in \{1, \dots, n\}$ such that $\frac{\partial \Phi}{\partial z_i} \neq 0$. Then α_i is algebraic and separable over $F' := \mathbb{K}(\alpha_1, \dots, \hat{\alpha}_i, \dots, \alpha_n, \beta_{s+1})$. Thus $\alpha_1, \dots, \hat{\alpha}_i, \dots, \alpha_n, \beta_{s+1}$ is a new transcendence basis of E over \mathbb{K} , and E is generated over F' by $\beta_1, \dots, \beta_s, \alpha_i, \beta_{s+2}, \dots, \beta_r$. Moreover, each of $\beta_1, \dots, \beta_s, \alpha_i$ is separable over F' . Iterating, we get the Theorem. \square

Corollary A.4.7. *Let $E \supset \mathbb{K}$ be a finitely generated extension of fields, and suppose that \mathbb{K} is algebraically closed. Let m be the transcendence degree of E over \mathbb{K} . Then there exists a prime polynomial $P \in \mathbb{K}(z_1, \dots, z_m)[z_{m+1}]$ such that E (as extension of \mathbb{K}) is isomorphic to the field $\mathbb{K}(z_1, \dots, z_m)[z_{m+1}]/(P)$.*

A.5 The key to the Nullstellensatz

We prove the key result needed for Hilbert's Nullstellensatz. Note: in the present section fields are not necessarily algebraically closed.

Theorem A.5.1. *Let $K \supset F$ be an extension of fields, and assume that K is a finitely generated F -algebra. Then K is an algebraic extension of F .*

Proof (by D. Allcock and O. Zariski). We must prove that if $K \supset F$ is not an algebraic extension, then it is not finitely generated as an F -algebra. First assume that K has transcendence degree 1 over F (this is the key case). Let $x \in K$ be transcendental over F . Thus the subfield of K generated by x (over F) is isomorphic to $F(x)$, the field of rational functions in x with coefficients in F . Since K is a finitely generated F -algebra it is also a finitely generated vector space over $F(x)$. Let $\{\xi_1, \dots, \xi_r\}$ be a basis of K as vector space over $F(x)$. Let $z_1, \dots, z_d \in K$ be generators of K as F -algebra. We may (and will) assume that $z_1 = 1$. For $i \in \{1, \dots, d\}$ we have

$$z_i = \sum_{j=1}^r \frac{f_{ij}(x)}{g_{ij}(x)} \xi_j, \quad (\text{A.5.1})$$

where $f_{ij}(x), g_{ij}(x) \in F[x]$ are polynomials (of course $g_{ij}(x) \neq 0$). For $s, t \in \{1, \dots, r\}$ we have

$$\xi_s \cdot \xi_t = \sum_{j=1}^r \frac{l_{stj}(x)}{m_{stj}(x)} \xi_j \quad (\text{A.5.2})$$

where $l_{stj}(x), m_{stj}(x) \in F[x]$ are polynomials. Let $a \in K$. Since K is a finitely generated F -algebra, we have $a = P(z_1, \dots, z_d)$, where P is a polynomial with coefficients in F . Applying the formulae in (A.5.1) and in (A.5.2) we get that a is a linear combination of ξ_1, \dots, ξ_r with coefficients rational functions whose denominators are products of the polynomials $g_{ij}(x)$'s and $m_{stj}(x)$'s (this is the key point). Now let $h(x) \in F[x]$ be a prime polynomial which is not among the (finite) prime factors of the $g_{ij}(x)$'s and the $m_{stj}(x)$'s. Then $a := h(x)^{-1} \xi_1$ is an element of K which is not equal to such a linear combination. This is a contradiction, and hence $K \supset F$ is an algebraic extension.

Now assume that K has transcendence degree greater than 1 over F . There exists an intermediate subfield $K \supset F' \supset F$ such that K has transcendence degree greater 1 over F' . We have just proved that K is not finitely generated as F' algebra, and hence K is not finitely generated as F algebra. \square

Corollary A.5.2. *Let F be a field, and let $\mathfrak{m} \subset F[z_1, \dots, z_n]$ be a maximal ideal. Then $F[z_1, \dots, z_n]/\mathfrak{m}$ is a finite algebraic extension of F .*

Proof. Let $K := F[z_1, \dots, z_n]/\mathfrak{m}$. Then K is a field because \mathfrak{m} is a maximal ideal, and it is generated as F algebra by the equivalence classes $\bar{z}_1, \dots, \bar{z}_n$. By Theorem A.5.1 it follows that K is an algebraic extension of F (obviously finitely generated). \square

A.6 Derivations

Let R be a ring (commutative with unit), and let M be an R -module.

Definition A.6.1. A *derivation from R to M* is a map $D: R \rightarrow M$ such that additivity and Leibnitz' rule hold, i.e. for all $a, b \in R$,

$$D(a + b) = D(a) + D(b), \quad D(ab) = bD(a) + aD(b).$$

If k is a field and R is a k -algebra a *k -derivation* (or *derivation over k*) $D: R \rightarrow M$ is a derivation such that $D(c) = 0$ for all $c \in k$. We let $\text{Der}(R, M)$ be the set of derivations from R to M . If R is a k -algebra we let $\text{Der}_k(R, M) \subset \text{Der}(R, M)$ be the subset of k -derivations.

Example A.6.2. Let k be a field, and let $f = \sum_I a_I z^I$ be a polynomial in $k[z_1, \dots, z_n]$, where the summation is over multiindices I , $a_I \in \mathbb{K}$ for every I , and a_I is almost always zero. The formal derivative of f with respect to z_m is defined by the familiar formula

$$\frac{\partial f}{\partial z_m} = \sum_{I \text{ s.t. } i_m > 0} i_m a_I z_1^{i_1} \cdots z_{m-1}^{i_{m-1}} \cdot z_m^{i_m-1} \cdot z_{m+1}^{i_{m+1}} \cdots z_n^{i_n}. \quad (\text{A.6.3})$$

The map

$$\begin{array}{ccc} k[z_1, \dots, z_n] & \xrightarrow{\frac{\partial}{\partial z_m}} & k[z_1, \dots, z_n] \\ f & \mapsto & \frac{\partial f}{\partial z_m} \end{array} \quad (\text{A.6.4})$$

is a k -derivation of the k algebra to itself. We claim that $\text{Der}_k(k[z_1, \dots, z_n], k[z_1, \dots, z_n])$ is freely generated (as $k[z_1, \dots, z_n]$ module) by $\frac{\partial}{\partial z_1}, \dots, \frac{\partial}{\partial z_n}$. In fact there is no relation between $\frac{\partial}{\partial z_1}, \dots, \frac{\partial}{\partial z_n}$ because $\frac{\partial z_j}{\partial z_m} = \delta_{jm}$, and moreover, given a k derivation

$$D: k[z_1, \dots, z_n] \rightarrow k[z_1, \dots, z_n]$$

we have $D = \sum_{m=1}^n \alpha_m \frac{\partial}{\partial z_m}$, where $\alpha_m := D(z_m)$.

Example A.6.3. Let $D: R \rightarrow M$ be a derivation.

1. By Leibniz we have $D(1) = D(1 \cdot 1) = D(1) + D(1)$ and hence $D(1) = 0$.
2. Suppose that $g \in R$ is invertible. Then

$$0 = D(1) = D(g \cdot g^{-1}) = g^{-1} Dg + f D(g^{-1}) \quad (\text{A.6.5})$$

and hence $D(g^{-1}) = -g^{-2} D(g)$.

3. Suppose that $f, g \in R$ and that g is invertible. By Item (2) we get that the following familiar formula holds:

$$D(f \cdot g^{-1}) = g^{-2} (D(f) \cdot g - f \cdot D(g)). \quad (\text{A.6.6})$$

Let $D, D' \in \text{Der}(R, M)$ and $z \in R$ we let

$$\begin{array}{ccc} R & \xrightarrow{D+D'} & M \\ a & \mapsto & D(a) + D'(a) \end{array} \quad (\text{A.6.7})$$

and

$$\begin{array}{ccc} R & \xrightarrow{zD} & M \\ a & \mapsto & zD(a) \end{array} \quad (\text{A.6.8})$$

Both $D + D'$ and zD are derivations and with these operations $\text{Der}(R, M)$ is an R -module. If R is a k -algebra then $\text{Der}_k(R, M)$ is an R -submodule of $\text{Der}(R, M)$.

Next we suppose that $E \supset F$ is an extension of fields, and we consider $\text{Der}_F(E, E)$. Notice that $\text{Der}_F(E, E)$ is a vector space over F .

Proposition A.6.4. *Suppose that $E \supset F$ is a finitely and separably generated extension of fields. Let $\alpha_1, \dots, \alpha_n$ be a separating transcendence basis of E over F . Then the map of E -vector spaces*

$$\begin{array}{ccc} \text{Der}_F(E, E) & \longrightarrow & E^n \\ D & \mapsto & (D(\alpha_1), \dots, D(\alpha_n)) \end{array} \quad (\text{A.6.9})$$

is an isomorphism.

Proof. Let $K := F(\alpha_1, \dots, \alpha_n) \subset E$. Since $\alpha_1, \dots, \alpha_n$ is a separating transcendence basis of E over F , and E is finitely generated (over F), there exists an element $\beta \in E$ primitive over K . Let $P \in K[z]$ be the minimal polynomial of β . In particular

$$P(\beta) = 0, \quad \frac{dP}{dz}(\beta) \neq 0. \quad (\text{A.6.10})$$

(The inequality holds because E is a separable extension of K .)

Since K is a purely transcendental extension of F we have an isomorphism of E -vector spaces

$$\begin{array}{ccc} \text{Der}_F(K, E) & \xrightarrow{\sim} & E^n \\ D & \mapsto & (D(\alpha_1), \dots, D(\alpha_n)). \end{array}$$

Equivalently every $D \in \text{Der}_F(K, E)$ is given by

$$D(\phi) = \sum_{i=1}^n c_i \frac{\partial \phi}{\partial \alpha_i}, \quad \alpha_i \in E,$$

and the c_i 's may be chosen arbitrarily. Thus we must show that the restriction map

$$\begin{array}{ccc} \text{Der}_F(E, E) & \longrightarrow & \text{Der}_F(K, E) \\ D & \mapsto & D|_K \end{array} \quad (\text{A.6.11})$$

defines an isomorphism of E -vector spaces.

Let us prove that the restriction map is injective. Let $P = \sum_{i=0}^d a_i z^{d-i}$, where $a_0 = 1$ (recall that P is the minimal polynomial of β over K). Suppose that $D \in \text{Der}_F(E, E)$; by the equality in (A.6.10) we get that

$$0 = D(P(\beta)) = \sum_{i=0}^d D(a_i) \beta^{d-i} + \sum_{i=0}^{d-1} D(\beta) a_i (d-i) \beta^{d-i-1} = \sum_{i=0}^d D(a_i) \beta^{d-i} + D(\beta) \frac{dP}{dz}(\beta).$$

By the inequality in (A.6.10), we can divide and we get

$$D(\beta) = - \left(\sum_{i=1}^m D(a_i) \beta^{m-i} \right) \cdot \frac{dP}{dz}(\beta)^{-1}. \quad (\text{A.6.12})$$

This proves that the map in (A.6.11) is injective.

In order to prove surjectivity, we extend a derivation $D \in \text{Der}_F(K, E)$ to a derivation in $\text{Der}_F(E, E)$ by *defining* its value on β via (A.6.12). \square

Corollary A.6.5. *Keep hypotheses and notation as above. Then $\text{Tr deg}_k K = \dim_K \text{Der}_k(K, K)$.*

A.7 Nakayama's Lemma

Let R be a ring, M be an R -module, and $I \subset R$ be an ideal. We let $IM \subset M$ be the submodule of finite sums $\sum_{k \in K} f_k m_k$, where $f_k \in I$ and $m_k \in M$ for every $k \in K$.

Lemma A.7.1 (Nakayama's Lemma). *Let R be a ring and M a finitely generated R -module. Let $I \subset R$ be an ideal and suppose that $M \subset IM$ (i.e. $M = IM$). Then there exists $\varphi \in I$ such that $(1 + \varphi)M = 0$ i.e. $(1 + \varphi)m = 0$ for all $m \in M$.*

Proof. Let m_1, \dots, m_r be generators of M . By hypothesis there exist $a_{ij} \in I$ for $1 \leq i, j \leq r$ such that

$$m_i = \sum_{j=1}^r a_{ij} m_j.$$

Let A be the $r \times r$ -matrix with entries in R given by $A := (\delta_{ij} - a_{ij})$, where δ_{ij} is the Kronecker symbol i.e. $\delta_{ij} = 1$ if $i = j$ and is 0 otherwise. Let B be the $r \times 1$ -matrix with entries m_1, \dots, m_r . Then $A \cdot B = 0$: multiplying by the matrix of cofactors A^c we get that $\det A \cdot m_i = 0$ for $i = 1, \dots, r$. Expanding $\det A$ we get that $\det A = 1 + \varphi$ where $\varphi \in I$. \square

Corollary A.7.2. *Let R be a local ring with maximal ideal \mathfrak{m} and M a finitely generated R -module. Suppose that the quotient module $M/\mathfrak{m}M$ is generated by the classes of $m_1, \dots, m_r \in M$. Then M is generated by m_1, \dots, m_r .*

Proof. Let $N \subset M$ be the submodule generated by m_1, \dots, m_r and $P := M/N$ be the quotient module. We must prove that $P = 0$. The module P is finitely generated over R because M is, and moreover $P \subset \mathfrak{m}P$ by hypothesis. By Nakayama's Lemma there exists $\varphi \in \mathfrak{m}$ such that $(1 + \varphi)P = 0$. Since $(1 + \varphi)$ does not belong to \mathfrak{m} it is invertible (it generates all of R because \mathfrak{m} contains all non-trivial ideals of R) and hence it follows that $P = 0$. \square

A.8 Order of vanishing

The prototype of a Noetherian local ring (R, \mathfrak{m}) is the ring $\mathcal{O}_{X,x}$ of germs of regular functions of a quasi projective variety X at a point $x \in X$, with maximal ideal \mathfrak{m}_x , see Proposition 4.2.4. The following result of Krull can be interpreted as stating that a non zero element of $\mathcal{O}_{X,x}$ can not vanish to arbitrary high order at x . In other words, elements of $\mathcal{O}_{X,x}$ behave like analytic functions (as opposed to C^∞ functions).

Theorem A.8.1 (Krull). *Let (R, \mathfrak{m}) be a Noetherian local ring. Then*

$$\bigcap_{i \geq 0} \mathfrak{m}^i = \{0\}.$$

Proof. Since R is Noetherian the ideal \mathfrak{m} is finitely generated; say $\mathfrak{m} = (a_1, \dots, a_n)$. Let $b \in \bigcap_{i \geq 0} \mathfrak{m}^i$. Let $i \geq 0$; since $b \in \mathfrak{m}^i$ there exists $P_i \in R[X_1, \dots, X_n]_i$ such that $P_i(a_1, \dots, a_n) = b$. Let $J \subset R[X_1, \dots, X_n]$ be the ideal generated by the P_i 's. Since R is Noetherian so is $R[X_1, \dots, X_n]$. Thus J is finitely generated and hence there exists $N > 0$ such that $J = (P_0, \dots, P_N)$. Thus there exists $Q_{N+1-i} \in R[X_1, \dots, X_n]_{N+1-i}$ for $i = 0, \dots, N$ such that $P_{N+1} = \sum_{i=0}^N Q_{N+1-i} P_i$. It follows that

$$b = P_{N+1}(a_1, \dots, a_n) = \sum_{i=0}^N Q_{N+1-i}(a_1, \dots, a_n) P_i(a_1, \dots, a_n) = b \sum_{i=0}^N Q_{N+1-i}(a_1, \dots, a_n). \quad (\text{A.8.13})$$

Now $Q_{N+1-i}(a_1, \dots, a_n) \in \mathfrak{m}$ for $i = 0, \dots, N$ and hence $\epsilon := \sum_{i=0}^N Q_{N+1-i}(a_1, \dots, a_n) \in \mathfrak{m}$. Equality (A.8.13) gives that $(1 - \epsilon)b = 0$: since $\epsilon \in \mathfrak{m}$ the element $(1 - \epsilon)$ is invertible and hence $b = 0$. \square

Corollary A.8.2. *Let (R, \mathfrak{m}) be a Noetherian local ring, and let $\mathfrak{J} \subset R$ be an ideal. Then*

$$\bigcap_{i \geq 0} (\mathfrak{J} + \mathfrak{m}^i) = \{0\}.$$

Proof. Let $S := R/\mathfrak{J}$. Then S is a Noetherian local ring, with maximal ideal $\mathfrak{m}_S := \mathfrak{J} + \mathfrak{m}$. The corollary follows by applying Theorem A.8.2 to (S, \mathfrak{m}_S) . \square