# 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 [Lan02]).

## A.2 Unique factorization

**Theorem A.2.1.** *Let $R$ be a UFD. Then $R[t]$ is a UFD. Moreover a polynomial $p = a_0 t^d + a_1 t^{d-1} + \ldots + a_d$ 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 $a_0, a_1, \ldots, a_d$ is 1.*

**Corollary A.2.2.** *The ring $\mathbb{K}[x_1, \ldots, x_n]$ 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 $\mathbb{K}[x_1, \ldots, x_n] \cong \mathbb{K}[x_1, \ldots, x_{n-1}][t]$. □

## 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*

$$I_0 \subset I_1 \subset \ldots \subset I_m \subset \ldots$$

*of ideals of $R$ (here $I_m$ is defiend 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 hat $I_m = I_{m_0}$ for $m \geqslant m_0$.*

*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 $I = (a_1, \ldots, a_r)$. There exists $m_0$ such that $a_j \in I_{m_0}$ for $j \in \{1, \ldots, r\}$, and hence $I = I_{m_0}$. Let $m \geqslant m_0$; then $I_m \subset I$ and $I \subset I_m$, hence $I = I_m$. Thus $I_{m_0} = I_m$ for $m \geqslant m_0$.

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

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

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

This is a contradiction. $\square$

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

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

Then $(f_m) \subsetneq (f_{m+1})$. Thus $(f_1) \subset (f_2) \subset \ldots \subset (f_m) \subset \ldots$ is a non-stationary ascending chain of ideals, and hence $\mathrm{Hol}(\mathbb{K})$ 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: $J = (c_1, \ldots, c_s)$. 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 $1 \leqslant i \leqslant s$ there exists $f_i \in I$ such that $\ell(f_i) = c_i$. Let

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

Let $H := I \cap \{f \in R[t] \mid \deg f \leqslant d\}$. Then $H$ is a submodule of $\{f \in R[t] \mid \deg f \leqslant d\} \simeq R^{d+1}$ (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 $R^{d+1} \to R$) and hence

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

Let us prove that

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

In fact let $f \in I$. If $\deg f \leqslant d$ then $f \in H$ and hence $f \in (g_1, \ldots, g_t) \subset (f_1, \ldots, f_s, g_1, \ldots, g_t)$. 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 $\sum_{i=1}^{s} a_i t^{\deg f - \deg f_i} f_i \in (f_1, \ldots, f_s, g_1, \ldots, g_t)$ it suffices to prove that $h \in I$. If $\deg h \leqslant d$ we are done, otherwise we iterate until we get down to a polynomial of degree less or equal to $d$. $\square$

**Theorem A.3.6** (Hilbert's basis Theorem)**.** *Every ideal of $\mathbb{K}[x_1, \ldots, x_n]$ 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 $\mathbb{K}[x_1, \ldots, x_n] \cong \mathbb{K}[x_1, \ldots, x_{n-1}][t]$. $\square$

## 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 $\alpha$ is a non zero ideal $F[z]$, and hence it is generated by a unique monic poylnomial $\varphi$, which is the *minimal polynomial of $\alpha$ over $F$*. Of course $\varphi$ is irreducible, hence prime. The subfield of $F$ generated by $F$ and $\alpha$ 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 [Lan02])**.** *An algebraic closure exists, and is unique up to isomorphism, i.e. if $E_1$, $E_2$ are two algebriac 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 costant 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 $\sigma\colon F \hookrightarrow L$ be an embedding into a field which is an algebraic closure of $\sigma(F)$. An extension of $\sigma$ to $E$ is an embedding $\widetilde{\sigma}\colon E \hookrightarrow L$ such that $\widetilde{\sigma}_{|F} = \sigma$. The number of such extensions is independent of the embedding $\sigma\colon F \hookrightarrow L$, 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 $\alpha$ is equal to $\varphi$.

Let $\sigma\colon F \hookrightarrow L$ be an embedding into a field which is an algebraic closure of $\sigma(F)$. An extension of $\sigma$ to $E$ is determined by its value on $\alpha$, and moreover such value can be chosen to be any root of $\varphi$ in $L$. Hence the separable degree of $E$ over $F$ is the number of roots of $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\operatorname{char} F = p > 0$, and $\varphi = \psi(z^p)$, where $\psi \in F[z]$, i.e. all monomials appearing in $f$ 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 numer of roots of $\varphi$ 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 [Lan02])**.** *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* $\operatorname{char} F = p > 0$, *and if $\alpha \in E$, the minimal polynomial of $\alpha$ over $E^s$ is equal to $z^{p^r} - \gamma$ for some $r \geqslant 0$, 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 elemnt of $E$ over $F$.

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

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 $\{i_1, \ldots, i_n\} \subset I$ such that $\alpha_{i_1}, \ldots, \alpha_{i_n}$ are algebraically dependent (with the usual abuse of language, we also say that the $\alpha_i$'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 $\mathrm{Tr.deg}_F(E)$. 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 $\{\alpha_1, \ldots, \alpha_n\}$ of $K$ over $F$ such that $K = F(\alpha_1, \ldots, \alpha_n)$ (thus $F(\alpha_1, \ldots, \alpha_n)$ 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 $\{\alpha_1, \ldots, \alpha_n\}$ of $E$ over $F$ is *separating* if $E$ is a separable extension of the subfield $F(\alpha_1, \ldots, \alpha_n)$. 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 [Mat89]). *If $\mathbb{K}$ is an algebrically closed field, any finitely generated extension $E \supset \mathbb{K}$ is separably generated.*

*Proof.* Let $\alpha_1, \ldots, \alpha_n$ be a transcendence basis of $E$ over $\mathbb{K}$. Hence the field $F := \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ is isomorphic to the field of rational functions in $n$ indeterminates, and $E \supset F$ is a finite extension. Let $\beta_1, \ldots, \beta_r$ be elements of $E$ algebraic over $F$, which generate $E$ over $F$. If all such $\beta_i$'s are separable over $F$ (i.e. the subfield of $E$ generated by $F$ and $\beta_i$ is separable over $F$), then $E$ is separable over $F$ (see Chapter VII in [Lan02]).

Suppose that one of the $\beta_i$'s is not separable over $F$. Then $\mathrm{char}\, F = \mathrm{char}\, \mathbb{K} = p > 0$. We may reorder the $\beta_i$'s so that each of $\beta_1, \ldots, \beta_s$ is separable over $F$, and each of the $\beta_{s+1}, \ldots, \beta_r$ is not separable over $F$. We find suitable replacements of the $\alpha_j$'s so that $E$ is a separable extension of the subfield generated by the new transcendence basis. Since $\beta_{s+1}$ is algebraic over $F$, there exists a polynomial $\Phi \in \mathbb{K}[z_1, \ldots, z_{n+1}]$ such that

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

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

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

where $\mathscr{I}$ is a set of multiindices, and we assume that $a_I \neq 0$ for every $I \in \mathscr{I}$. Since $\frac{\partial \Phi}{\partial z_i} \neq 0$ for all $i \in \{1, \ldots, n+1\}$, it follows that each $I \in \mathscr{I}$ 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 $\Phi$ is irreducible, and hence we have proved that there exists $i \in \{1, \ldots, n\}$ such that $\frac{\partial \Phi}{\partial z_i} \neq 0$. Then $\alpha_i$ is algebraic and separable over $F' := \mathbb{K}(\alpha_1, \ldots, \widehat{\alpha}_i, \ldots, \alpha_n, \beta_{s+1})$. Thus $\alpha_1, \ldots, \widehat{\alpha}_i, \ldots, \alpha_n, \beta_{s+1}$ is a new transcendence basis of $E$ over $\mathbb{K}$, and $E$ is generated over $F$ by $\beta_1, \ldots, \beta_s, \alpha_i, \beta_{s+2}, \ldots, \beta_r$. Moreover, each of $\beta_1, \ldots, \beta_s, \alpha_i$ is separable over $F'$. Iterating, we get the Theorem. □

**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 $P \in \mathbb{K}(z_1, \ldots, z_m)[z_{m+1}]$ such that $E$ (as extension of $\mathbb{K}$) is isomorphic to the field $\mathbb{K}(z_1, \ldots, z_m)[z_{m+1}]/(P)$.*

## 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** (Zariski's Lemma [Zar47], [All05])**.** *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 $\{\xi_1, \ldots, \xi_r\}$ be a basis of $K$ as vector space over $F(x)$. Let $z_1, \ldots, z_d \in K$ be generators of $K$ as $F$-algebra. We may (and will) assume that $z_1 = 1$. For $i \in \{1, \ldots, d\}$ we have

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

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

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

where $l_{stj}(x), g_{stj}(x) \in F[x]$ are polynomials. Let $a \in K$. Since $K$ is a finitely generated $F$-algebra, we have $a = P(z_1, \ldots, z_d)$, 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 $\xi_1, \ldots, \xi_r$ 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. □

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

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

## A.6 Descent

Let $F \subset K$ be an inclusion of fields, and let $\mathrm{Aut}(K/F)$ be the group of automorphisms of $K$ which are the identity on $F$. If $V$ is an $F$ vector space, then $\mathrm{Aut}(K/F)$ acts on the $K$ vector space

$$W := K \otimes_F V \tag{A.6.3}$$

via its action on $K$. Explicitly: if $v \in W$ is given by $v = c_1 \otimes v_1 + \ldots + c_n \otimes v_n \in V$ where $c_i \in K$ and $v_i \in V$, then $\sigma \in \mathrm{Aut}(K/F)$ acts as

$$\sigma(v) = \sigma(c_1) \otimes v_1 + \ldots + \sigma(c_n) \otimes v_n.$$

*Example* A.6.1. Let $F = \mathbb{R} \subset \mathbb{C} = K$ and $V = \mathbb{R}^n$. Then we may identify $W = \mathbb{C} \otimes \mathbb{R}^n$ with $\mathbb{C}^n$ in such a way that the generator $\sigma$ of the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/(2)$ acts as $\sigma(z_1, \ldots, z_n) = (\overline{z}_1, \ldots, \overline{z}_n)$.

*Example* A.6.2. Let $p$ a prime and $q = p^r$, where $r \in \mathbb{N}_+$. Let $F = \mathbb{F}_q \subset \mathbb{F}_{q^m} = K$, and let $F \colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ be the Frobenius automorphism defined by $F(a) := a^q$. Thus $F$ is a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Let $V = \mathbb{F}_q$. Then we may identify $W = \mathbb{F}_{q^m} \otimes \mathbb{F}_q^n$ with $\mathbb{F}_{q^m}^n$ in such a way that $F$ acts as $F(z_1, \ldots, z_n) = (z_1^q, \ldots, z_n^q)$.

Suppose that $V_0 \subset V$ is an $F$ sub vector space. Then $W_0 := K \otimes_F V_0$ is mapped to itself by $\mathrm{Aut}(K/F)$. If the fixed field of $\mathrm{Aut}(K/F)$ is $F$ then the converse is true.

**Proposition A.6.3.** *Keep notation as above, and assume that the fixed field of* $\mathrm{Aut}(K/F)$ *is* $F$*. Suppose that* $W_0 \subset W = K \otimes_F V$ *is a* $K$ *subvector space which is mapped to itself by* $\mathrm{Aut}(K/F)$*. Then there exists an* $F$ *sub vector space* $V_0 \subset V$ *such that* $W_0 = K \otimes_F V_0$

Before proving Proposition A.6.3 we go through a special case. To simplify notation let $G := \mathrm{Aut}(K/F)$. Assume that the fixed field $K^G$ of $G = \mathrm{Aut}(K/F)$ is $F$. Then

$$W^G := \{w \in W \mid \sigma(w) = w \ \forall \sigma \in \mathrm{Aut}(K/F)\} = V, \tag{A.6.4}$$

where $V$ stands for $F \otimes_F V \subset W$. It follows that if $W_0 \subset W$ is a $K$ vector space then $W_0^G = (W_0 \cap V)$. Hence the following is a special case of Proposition A.6.3: if $W_0$ is mapped to itself by $G$ and $W_0^G = \{0\}$, then $W_0 = \{0\}$. The Lemma below proves the validity of the latter statement.

**Lemma A.6.4.** *Keep notation as above, and assume that* $K^G = F$*. Suppose that* $W_0 \subset W$ *is a* $K$ *subvector space which is mapped to itself by* $G$ *and such that* $W_0^G = \{0\}$*. Then* $W_0 = \{0\}$*.*

*Proof.* We prove that if $W_0 \neq \{0\}$ then $W_0^G \neq \{0\}$. Since $W_0 \neq \{0\}$ there exists a minimal $n \geqslant 1$ for which there exist $n$ linearly independent vectors $v_1, \ldots, v_n \in V$ and non zero $c_1, \ldots, c_n \in K$ (meaning that $c_i \neq 0$ for all $i \in \{1, \ldots, n\}$) such that $w = \sum_{i=1}^n c_i \otimes v_i$ is an element of $W_0$. Multiplying $w$ by $c_1^{-1}$ we may (and will) assume that $c_1 = 1$. Let $\sigma \in G$. Then $(\sigma(w) - w) \in W_0$ because $W_0$ is mapped to itself by $G$. Since $\sigma(c_1) = \sigma(1) = 1 = c_1$ we get that for all $\sigma \in G$ we have

$$(\sigma(w) - w) = \sum_{i=2}^{n} (\sigma(c_i) - c_i) \otimes v_i \in W_0. \tag{A.6.5}$$

By minimality of $n$ it follows that $\sigma(c_i) = c_i$ for all $i \in \{1, \ldots, n\}$ and hence $c_i \in F$ for all $i$ because $K^G = F$. Thus $w$ is a non zero vector in $W_0^G$. □

*Proof of Proposition A.6.3.* Let $V_0 = V \cap W_0 = W_0^G$. Let $U := V/V_0$ and let

$$W = K \otimes_F V \xrightarrow{\pi} K \otimes_F U \tag{A.6.6}$$

be the quotient map of $K$ vector spaces. Of course the action of $G$ on $K$ induces an action of $K$ on $K \otimes_F U$. The kernel of $\pi$ is $K \otimes V_0$ which is contained in $W_0$. It suffices to prove that $\pi(W_0) = \{0\}$. Now $\pi(W_0)^G = \pi(W_0) \cap U = \pi(W_0 \cap V) = \pi(V_0) = \{0\}$.

□

## A.7 Derivations

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

**Definition A.7.1.** A *derivation from* $R$ *to* $M$ is a map $D \colon R \to M$ such that additivity and Leibinitz' 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* $k$) $D \colon R \to M$ is a derivation such that $D(c) = 0$ for all $c \in k$. We let $\mathrm{Der}(R, M)$ be the set of derivations from $R$ to $M$. If $R$ is a $k$-algebra we let $\mathrm{Der}_k(R, M) \subset \mathrm{Der}(R, M)$ be the subset of $k$-derivations.

*Example* A.7.2. Let $k$ be a field, and let $f = \sum_I a_I z^I$ be a polynomial in $k[z_1, \ldots, z_n]$, 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 familar formula

$$\frac{\partial f}{\partial z_m} = \sum_{I \text{ s.t. } i_m > 0} i_h a_I z_1^{i_1} \cdot \ldots \cdot z_{m-1}^{i_{m-1}} \cdot z_m^{i_m - 1} \cdot z_{m+1}^{i_{m+1}} \cdot \ldots z_n^{i_n}. \tag{A.7.7}$$

The map

$$\begin{array}{ccc} k[z_1, \ldots, z_n] & \xrightarrow{\frac{\partial}{\partial z_m}} & k[z_1, \ldots, z_n] \\ f & \mapsto & \frac{\partial f}{\partial z_m} \end{array} \tag{A.7.8}$$

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

$$D \colon k[z_1, \ldots, z_n] \to k[z_1, \ldots, z_n]$$

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

*Example* A.7.3. Let $D \colon R \to M$ 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

$$0 = D(1) = D(g \cdot g^{-1}) = g^{-1} Dg + f D(g^{-1}) \tag{A.7.9}$$

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

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

$$D(f \cdot g^{-1}) = g^{-2}(D(f) \cdot g - f \cdot D(g)). \tag{A.7.10}$$

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

$$\begin{array}{ccc} R & \xrightarrow{D+D'} & M \\ a & \mapsto & D(a) + D'(a) \end{array} \tag{A.7.11}$$

and

$$\begin{array}{ccc} R & \xrightarrow{zD} & M \\ a & \mapsto & zD(a) \end{array} \tag{A.7.12}$$

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

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

**Proposition A.7.4.** *Suppose that $E \supset F$ is a finitely and separably generated extension of fields. Let $\alpha_1, \ldots, \alpha_n$ be a separating transcendence basis of $E$ over $F$. Then the map of $E$-vector spaces*

$$\begin{array}{ccc} \mathrm{Der}_F(E, E) & \longrightarrow & E^n \\ D & \mapsto & (D(\alpha_1), \ldots, D(\alpha_n)) \end{array} \tag{A.7.13}$$

*is an isomorphism.*

*Proof.* Let $K := F(\alpha_1, \ldots, \alpha_n) \subset E$. Since $\alpha_1, \ldots, \alpha_n$ 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 $\beta$. In particular

$$P(\beta) = 0, \quad \frac{dP}{dz}(\beta) \neq 0. \tag{A.7.14}$$

(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

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

Equivalently every $D \in \mathrm{Der}_F(K, E)$ 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

$$\begin{array}{ccc} \mathrm{Der}_F(E, E) & \longrightarrow & \mathrm{Der}_F(K, E) \\ D & \mapsto & D_{|K} \end{array} \tag{A.7.15}$$

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 polynomila of $\beta$ over $K$). Suppose that $D \in \mathrm{Der}_F(E, E)$; by the equality in (A.7.14) 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.7.14), we can divide and we get

$$D(\beta) = -\left(\sum_{i=1}^{m} D(a_i)\beta^{m-i}\right) \cdot \frac{dP}{dz}(\beta)^{-1}. \tag{A.7.16}$$

This proves that the map in (A.7.15) is injective.

In order to prove surjectivity, we extend a derivation $D \in \mathrm{Der}_F(K, E)$ to a derivation in $\mathrm{Der}_F(E, E)$ by *defining* its value on $\beta$ via (A.7.16). □

**Corollary A.7.5.** *Keep hypotheses and notation as above. Then* $\mathrm{Tr\,deg}_k K = \dim_K \mathrm{Der}_k(K, K)$.

## A.8 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.8.1** (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 $m_1, \ldots, m_r$ be generators of $M$. By hypothesis there exist $a_{ij} \in I$ for $1 \leqslant i, j \leqslant r$ 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 $\delta_{ij}$ 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 $m_1, \ldots, m_r$. Then $A \cdot B = 0$: multiplying by the matrix of cofactors $A^c$ we get that $\det A \cdot m_i = 0$ for $i = 1, \ldots, r$. Expanding $\det A$ we get that $\det A = 1 + \varphi$ where $\varphi \in I$. □

**Corollary A.8.2.** *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 $m_1, \ldots, m_r \in M$. Then $M$ is generated by $m_1, \ldots, m_r$.*

*Proof.* Let $N \subset M$ be the submodule generated by $m_1, \ldots, m_r$ 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 $P = 0$. □

## A.9 Order of vanishing

The prototype of a Noetherian local ring $(R, \mathfrak{m})$ is the ring $\mathscr{O}_{X,x}$ 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 $\mathscr{O}_{X,x}$ can not vanish to arbitrary high order at $x$. In other words, elements of $\mathscr{O}_{X,x}$ behave like analytic functions (as opposed to $C^\infty$ functions).

**Theorem A.9.1** (Krull)**.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then*

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

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

$$b = P_{N+1}(a_1, \ldots, a_n) = \sum_{i=0}^N Q_{N+1-i}(a_1, \ldots, a_n) P_i(a_1, \ldots, a_n) = b \sum_{i=0}^N Q_{N+1-i}(a_1, \ldots, a_n). \quad \text{(A.9.17)}$$

Now $Q_{N+1-i}(a_1, \ldots, a_n) \in \mathfrak{m}$ for $i = 0, \ldots, N$ and hence $\epsilon := \sum_{i=0}^N Q_{N+1-i}(a_1, \ldots, a_n) \in \mathfrak{m}$. Equality (A.9.17) gives that $(1 - \epsilon)b = 0$: since $\epsilon \in \mathfrak{m}$ the element $(1 - \epsilon)$ is invertible and hence $b = 0$. □

**Corollary A.9.2.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let $\mathfrak{I} \subset R$ be an ideal. Then*

$$\bigcap_{i \geqslant 0} (\mathfrak{I} + \mathfrak{m}^i) = \{0\}.$$

*Proof.* Let $S := R/\mathfrak{I}$. Then $S$ is a Noetherian local ring, with maximal ideal $\mathfrak{m}_S := \mathfrak{I} + \mathfrak{m}$. The corollary follows by applying Theorem A.9.2 to $(S, \mathfrak{m}_S)$. □

# Bibliography


[All05] D. Allcock, *Hilbert's Nullstellensatz*, https://web.ma.utexas.edu/users/allcock/expos/nullstellensatz3.pdf (2005).

[Lan02] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

[Mat89] Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid. MR 1011461

[Zar47] Oscar Zariski, *A new proof of Hilbert's Nullstellensatz*, Bull. Amer. Math. Soc. **53** (1947), 362–368.