Algebra II

Nicholas Schwab & Ferdinand Wagner

Wintersemester 2017/18

This text consists of notes of the lecture Algebra II, taught at the University of Bonn by Professor Jens Franke in the winter term (Wintersemester) 2017/18.

Please report bugs, typos etc. through the *Issues* feature of github.

Contents

Introduction

After a slight delay due to the Professor being confused by the large attendance to his lecture, Franke briefly recaps the contents of his lecture course Algebra I. Our notes to this lecture can be found here [1]. He mentions specifically

- Hilbert's Basissatz and Nullstellensatz,
- the Noether Normalization Theorem,
- the Zariski-topology on k^n,
- irreducible topological spaces and their correspondence to the prime ideals of $k[X_1, \ldots, X_n]$,
- Noetherian topological spaces and their unique decomposition into irreducible subsets,
- the dimension of topological spaces and codimension of their irreducible subsets,
- catenary topological spaces,
- the fact that k^n is catenary and $\dim(k^n) = n$,
- quasi-affine varieties,
- structure sheaves,
- the fact that quasi-affine varieties X are catenary and $\dim(X) = \deg \operatorname{tr}(K(X)/k)$, where $K(X)$ is the quotient field of $\mathcal{O}(X)$. By the way, there is a nice alternative characterization as a direct limit (or colimit)

$$K(X) = \varinjlim_{\substack{\emptyset \neq U \subseteq X \\ U \text{ open}}} \mathcal{O}(U) \, .$$

- going up and going down for integral ring extensions,
- localizations.

Exercises will be held on Wednesday from 16 to 18 and Friday from 12 to 14 in Room 0.008. It is necessary to have achieved at least half the points on the exercise sheets in order to attend the exams.

Professor Franke recommends the following literature:

- Hartshorne, R.: *Algebraic Geometry*
- Mumford, D.: *The Red Book of Varieties and Schemes*
- Matsumura, H.: *Commutative Ring Theory* [2]

- Atiyah, M. & MacDonald, I.: *Introduction to Commutative Algebra*

The oh-so-humble authors of these notes want to use this opportunity to recommend

- Schwab, N. & Wagner, F.: *Algebra I by Jens Franke* [1].

as well. **Warning!** Somewhere in the middle of the last-mentioned text, the term *irreducible* is redefined as irreducible *and closed*. So don't let yourself get confused.

1. Krull's principal ideal theorem

1.1. Formulation

Theorem 11 (Krull's principal ideal theorem)**.** *Let R be Noetherian, $f \in R$, $\mathfrak{p} \in \operatorname{Spec} R$ minimal among all prime ideals containing f. Then $\operatorname{ht}(\mathfrak{p}) \leq 1$. In other words, $\mathfrak{p}$ is a minimal prime ideal (if $\operatorname{ht}(\mathfrak{p}) = 0$) or all prime ideals strictly contained in $\mathfrak{p}$ are minimal.*

Remark. (a) The *height* of a prime ideal is defined as

$$\operatorname{ht}(\mathfrak{p}) = \sup \left\{ \ell \;\middle|\; \begin{array}{c} \text{there is a strictly descending chain} \\ \mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_\ell \text{ of prime ideals } \mathfrak{p}_i \in \operatorname{Spec} R \end{array} \right\} .$$

(b) Recall the *Zariski topology* on $\operatorname{Spec} R$: For any ideal $I \subseteq R$, let

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\} \ .$$

We have the following relations (which we are supposed to prove on exercise sheet #1)

$$\begin{aligned} V(I) &= V\left(\sqrt{I}\right) \\ V(I \cdot J) &= V(I) \cup V(J) \\ V\Big(\sum_{\lambda \in \Lambda} I_\lambda\Big) &= \bigcap_{\lambda \in \Lambda} V(I_\lambda) \ . \end{aligned}$$

This implies (together with $V(0) = \operatorname{Spec} R$ and $V(R) = \emptyset$) that $\operatorname{Spec} R$ can be equipped with a topology in which the closed subsets are precisely the subsets of them for $V(I)$ where I is some ideal in R. This topology is Noetherian when R is, hence any closed subset can be decomposed into irreducible components. For $V(f) = V(f \cdot R)$, they are precisely those $V(\mathfrak{p})$ for which $\mathfrak{p}$ is minimal among all prime ideals containing f. Theorem 11 thus states that all irreducible components of $V(f)$ have codimension smaller or equal to 1 in $\operatorname{Spec} R$.

Corollary 1. *If $X \subseteq k^n$ is quasi-affine in k^n (with k algebraically closed) and $f \in \mathcal{O}(X) \setminus \{0\}$ then every irreducible component of $V(f)$ has codimension 1 in X.*

Remark 1. (a) Let $U \subseteq X$ be open, then there is a bijective correspondence

$$\begin{aligned} \{\text{irreducible closed subsets } B \subseteq U\} &\xrightarrow{\sim} \left\{ \begin{array}{c} \text{irreducible closed subsets } A \subseteq X \\ \text{such that } A \cap U \neq \emptyset \end{array} \right\} \\ A \cap U &\longleftarrow\!\shortmid\ A \\ B &\longmapsto \overline{B} \end{aligned}$$

(this is more or less a tedious calculation – and guess what: we have the pleasure to do it on exercise sheet #2). This shows that $\operatorname{codim}(A \cap U, U) = \operatorname{codim}(A, X)$ whenever $A \subseteq X$ is irreducible, closed and $U \subseteq X$ open and not disjoint from A. This is known as the *locality of codimension* (cf. [1, Remark 2.1.3]).

(*b*) In particular, the X from Corollary 1 may be replaced by any open subset meeting the irreducible component under consideration.

(*c*) If $Y \subseteq k^n$ is an affine algebraic variety in k^n and $\lambda \in \mathcal{O}_Y(Y)$, then $Y \setminus V(\lambda)$ is affine (that is, isomorphic to an affine algebraic variety, cf. [1, Proposition 2.2.4] for more details and a proof). Because of this, we may assume X to be affine: Let $Y = \overline{X} \subseteq k^n$ and let C be the irreducible component of $V(f)$ under consideration. Then there is a $\lambda \in k[X_1, \ldots, X_n]$ vanishing on $Y \setminus X$, but not on all of C. Indeed, $A = Y \setminus X$ and $B = Y \setminus X \cup \overline{C}$ are closed subsets and $A \subsetneq B$. Then we may choose λ such that it vanishes on A but not on all of B, hence not on all of $\overline{C}$. But then λ can't be identically zero on C since otherwise $\lambda = 0$ on $\overline{C}$ by continuity. Replacing X by $Y \setminus V(\lambda)$ we may then assume X to be affine according to (*b*).

(*d*) Let now X be an affine variety. We saw in Algebra I (cf. [1, Corollary 2.2.2]) that there is a bijection

$$\begin{aligned} \{\text{closed subsets } A \subseteq X\} &\xrightarrow{\sim} \left\{\text{ideals } I \subseteq \mathcal{O}(X) \text{ such that } I = \sqrt{I}\right\} \\ A &\longmapsto I = \{f \in \mathcal{O}(X) \mid f|_A = 0\} \\ V(I) &\longmapsfrom I\ . \end{aligned} \tag{$*$}$$

Under this correspondence, A is irreducible iff the corresponding ideal is prime. ($*$) follows from the special case $X = k^n$, $\mathcal{O}(X) = k[X_1, \ldots, X_n] =: R$ using the (nontrivial!) fact that, for closed $X = V(I) \subseteq k^n$ (with $I = \sqrt{I} \subseteq R$ an ideal), $\mathcal{O}(X) = R/I$. For I a prime ideal, this was proved in [1, Proposition 2.2.2]. For arbitrary I, one can just copy-paste the proof given there (the primality condition is not used at all) or expand the idea outlined after Proposition A.1.2 using that $R \to \mathcal{O}(X)$ (by the Nullstellensatz, cf. [1, Proposition 1.7.1]) has kernel I.

Proof Corollary 1 (using Theorem 11). Let $C_1, \ldots, C_m$ be the irreducible components of $V(f)$ and $\mathfrak{p}_i \in \mathcal{O}(X)$ the corresponding prime ideals. Then $f \in \mathfrak{p}_i$ (as $\mathfrak{p}_i$ is the ideal of functions vanishing on $C_i \subseteq V(f)$). Let $\mathfrak{q} \in \operatorname{Spec} \mathcal{O}(X)$ such that $f \in \mathfrak{q} \subseteq \mathfrak{p}_i$, then $V(f) \supseteq V(\mathfrak{q}) \supseteq V(\mathfrak{p}_i)$, hence $\mathfrak{q} = \mathfrak{p}_i$ because the decomposition of X into maximal irreducible subsets is unique (Proposition A.1.1 or (recommended) [1, Proposition 2.1.1]). Hence, each $\mathfrak{p}_i$ is a minimal prime ideal containing f.

On the other hand (this was missing in the lecture), if $\mathfrak{q} \ni f$ is a minimal prime ideal containing f, then $V(\mathfrak{q}) \subseteq V(f)$ is a maximal irreducible subset, hence among the C_i by [1, Proposition 2.1.1], hence $\mathfrak{q}$ is among the the $\mathfrak{p}_i$. We conclude that the $\mathfrak{p}_i$ are the minimal prime ideals containing f. By ($*$) and the principal ideal theorem, $\operatorname{codim}(C_i, X) = \operatorname{ht}(\mathfrak{p}_i) \leq 1$. But $\operatorname{codim}(C_i, X) > 0$ as X is irreducible and $f \neq 0$. *q.e.d.*

Standalone proof of Corollary 1. Step 1. We reduce to the case where X is affine and $V(f)$ is irreducible. Indeed, by Remark 1(*c*), X may be assumed to be affine. Let $V(f) = C_1 \cup \cdots \cup C_m$ be its decomposition into irreducible components. Since $C_1 \not\subseteq B := C_2 \cup \cdots \cup C_m$, there is a

$\lambda \in \mathcal{O}(X)$ vanishing on B but not on C_1. By Remark 1(b), we may replace X by $\widetilde{X} = X \setminus V(\lambda)$. Denote $\widetilde{f} = f|_{\widetilde{X}} \in \mathcal{O}(\widetilde{X})$, then $V(f) \cap \widetilde{X} = V(\widetilde{f}) = C_1 \setminus V(\lambda)$ is irreducible and we may replace X and f by their tilded versions $\widetilde{X}$ and $\widetilde{f}$.

Step 2. Let R be a factorial domain and $p \in R$ prime. Then $\operatorname{ht}(p) = 1$. Indeed, $\operatorname{ht}(p) > 0$ as $(0) \in \operatorname{Spec} R$ and $p \neq 0$. Suppose there is a prime ideal $(0) \subsetneq \mathfrak{q} \subsetneq (p)$. Let $g \in \mathfrak{q} \setminus \{0\}$ and $g = q_1 \cdots q_k$ its decomposition into prime factors. We may assume that k is minimal. Since $p \mid q_1 \cdots q_k$, we have w.l.o.g. $p \mid q_1$, hence p and q differ only by a unit of R as they are both primes. But $q_2 \cdots q_k \notin \mathfrak{q}$ by minimality of k, hence $q_1 \in \mathfrak{q}$ as $\mathfrak{q}$ is prime. Then also $p \in \mathfrak{q}$, hence $(p) \subseteq \mathfrak{q}$, contradiction!

Step 3. The principal ideal theorem holds when R is factorial. Indeed, let $f \in R \setminus \{0\}$ and $f = p_1 \cdots p_k$ its prime factorization. Then any prime ideal containing f contains some p_i, hence the (p_i) are the minimal prime ideals containing f. Step 2 does the rest.

Step 4. To reduce Corollary 1 to a situation where Step 3 can be applied, one uses the *Noether normalization theorem* (cf. [1, Theorem 3]). Suppose that $V(f)$ is irreducible (we can do that by Step 1) and let $\mathfrak{p} = \sqrt{(f)}$ be the prime ideal of functions vanishing on $V(f)$. By Noether normalization, the finite-type k-algebra $A = \mathcal{O}(X)$ contains algebraically independent elements $\lambda_1, \ldots, \lambda_n$ such that A is integral over $B = k[\lambda_1, \ldots, \lambda_n]$. The latter is factorial, because $B \simeq k[X_1, \ldots, X_n]$, the λ_i being algebraically independent. Denote by L and K the quotient fields of A and B and let $\mathfrak{q} = \mathfrak{p} \cap B$, $f_0 = N_{L/K}(f)$. We claim

$$f_0 \in B \quad \text{and} \quad \mathfrak{q} = \sqrt{(f_0)}\,. \tag{\#}$$

Note that $\mathfrak{q} = \sqrt{(f_0)}$ is a (actually, *the*) minimal prime ideal containing f_0 since prime ideals coincide with their radicals. By Step 3 and Step 2, this implies $\operatorname{ht}(\mathfrak{q}) = 1$. But $\operatorname{ht}(\mathfrak{p}) \leq \operatorname{ht}(\mathfrak{q})$ holds by the *going-up theorem* (cf. [1, Theorem 7] or [1, Fact 2.6.2] for this particular result), hence $\operatorname{codim}(V(f), X) \leq 1$. However, as $f \neq 0$ and X is irreducible, $V(f)$ cannot have codimension 0.

Step 5. We are left to prove (#). Let B be a domain integrally closed in its field of quotients K (i.e. $x \in K$ is integral over B iff $x \in B$). Such B are called *normal*. For instance, factorial rings are always normal and we may apply the following to the situation of Step 4.

If L/K is a finite field extension and $f \in L$ is integral over B, then so are all its images under the K-linear embeddings $L \hookrightarrow \overline{L}$ (they satisfy the same equation as f). As the elements of $\overline{L}$ which are integral over B form a subring of $\overline{L}$, all coefficients of the characteristic polynomial $P_{f,L/K}$ (cf. Definition A.3.1) and the minimal polynomial $\operatorname{Min}_{f/K}$ are integral over B by Theorem C(d). But, by definition, these two have their coefficients in K as well, hence $P_{f,L/K}, \operatorname{Min}_{f/K} \in B[T]$. In particular, $f_0 = N_{L/K}(f) \in B$.

Now let $\sigma = \sigma_1, \sigma_2, \ldots, \sigma_r$ be the different K-embeddings and $n = [L : K]$. Then

$$f_0 = \pm\Big(\prod_{i=1}^{r} \sigma_i(f)\Big)^{n/r}$$

by Theorem C(d). We know that f is among the $\sigma_i(f)$, say, $f = \sigma_1(f)$. Replacing A by the integral closure $\widetilde{A}$ of B in L (which is possible thanks to the going-up theorem), we may assume

$\sigma_2(f)\cdots\sigma_r(f) \in A$, hence $f_0 \in \mathfrak{p}$ as it contains $f \in \mathfrak{p}$ as a factor. Then $f_0 \in \mathfrak{p} \cap B$, hence also $\sqrt{(f_0)} \subseteq \mathfrak{q}$, as prime ideals coincide with their radicals.

To prove $\mathfrak{q} \subseteq \sqrt{(f_0)}$ let $q \in \mathfrak{q}$. Then $q^m \in (f)$ for sufficiently large m as $q \in \mathfrak{p} = \sqrt{(f)}$. Let $q^m = fa$, $a \in A$. Since $q^m \in B$, we have

$$q^{mn} = N_{L/K}(q^m) = N_{L/K}(f)N_{L/K}(a) = f_0 b \in (f_0)$$

for some $b = N_{L/K}(a) \in B$. This proves $q \in \sqrt{(f_0)}$. *q.e.d.*

Theorem 12 (Krull's height theorem)**.** *Let A be a Noetherian ring, $f_1, \ldots, f_r \in A$ and $\mathfrak{p}$ any prime ideal minimal among the prime ideals containing all the f_i. Then* $\operatorname{ht}(\mathfrak{p}) \leq r$.

The following corollary can be derived in the same way as Corollary 1 from Theorem 11.

Corollary 2. *Let X be a quasi-affine variety in k^n, and let $f_1, \ldots, f_r \in \mathcal{O}(X)$ and let Z be any irreducible component of $\bigcap_{i=1}^r V(f_i) = V(f_1, \ldots, f_r)$. Then* $\operatorname{codim}(Z, X) \leq r$.

The derivation from Corollary 1 by induction on r is significantly easier then the similar inductive derivation of Theorem 12 from Theorem 11 due to the fact that k^n is catenary. We will eventually prove Theorem 12 by Hilbert polynomial arguments.

Proof of Corollary 2. We use Corollary 1 and induction on r. The case $r = 0$ is trivial. Now let $r \geq 1$ and the assertion be true for for fewer than r equations. If $f_r = 0$ we drop f_r and apply the induction assumption: $\operatorname{codim}(Z, X) \leq r - 1 < r$.

Otherwise, let $V(f_r) = \bigcup_{i=1}^N Y_i$, be the decomposition into irreducible components. Then $Z = \bigcup_{i=1}^N (Z \cap Y_i)$ and, as Z is irreducible, there is an $i \leq N$ such that $Z \subseteq Y_i$ (cf. [1, Proposition 2.1.1]). By Corollary 1, $\operatorname{codim}(Y_i, X) = 1$. Now Z is an irreducible component of $\bigcap_{j=1}^{r-1} V(f_j|_{Y_i})$. Indeed, it is possible to obtain a decomposition of $\bigcap_{j=1}^r V(f_j)$ into irreducible subsets by forming the union over $1 \leq i \leq N$ of the decompositions of $\bigcap_{j=1}^{r-1} V(f_j|_{Y_i})$. Removing the non-maximal elements gives the decomposition of $\bigcap_{j=1}^r V(f_j)$ into irreducible components, which is unique (to be *the* unique decomposition into irreducible components, it actually suffices, that no component is contained in another, cf. [1, Proposition 2.1.1]). As Z occurs in it, it is not a strict subset of any irreducible component of $\bigcap_{j=1}^{r-1} V(f_j|_{Y_i})$, hence it is an irreducible component of that. Applying the induction assumption we obtain $\operatorname{codim}(Z, Y_i) \leq r - 1$. As X is catenary, we have

$$\operatorname{codim}(Z, X) = \operatorname{codim}(Z, Y_i) + \operatorname{codim}(Y_i, X) \leq r - 1 + 1 = r \ ,$$

as claimed. *q.e.d.*

Corollary 3. *If R is any Noetherian ring and $\mathfrak{p} \in \operatorname{Spec} R$, then* $\operatorname{ht}(\mathfrak{p}) < \infty$. *In particular, any local Noetherian ring is finite-dimensional.*

Remark. The dimension of R (or $\operatorname{Spec} R$) may still be infinite for lack of a finite common bound for the heights of the maximal ideals.

Proposition 1 ([1, Concluding remarks, Proposition 1]). *Let $X \subseteq k^m$ and $Y \subseteq k^n$ be affine algebraic varieties of codimensions a resp. b. Then $X \times Y$ is an affine algebraic variety in k^{m+n} and*

$$\operatorname{codim}(X \times Y, k^{m+n}) = a + b \quad \textit{and} \quad \dim(X \times Y) = \dim(X) + \dim(Y) \ .$$

Proof. Let's first prove that $X \times Y$ is an affine algebraic variety (this was done in [1, proof of Proposition 2.2.6] as well). Let $X = V(\mathfrak{p})$, $Y = V(\mathfrak{q})$ with $\mathfrak{p}, \mathfrak{q}$ prime ideals in their respective polynomial rings. Then $X \times Y = V(I)$ where $I \subseteq k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ is the ideal generated by $\{f(X_1, \ldots, X_m) \mid f \in \mathfrak{p}\}$ and $\{g(Y_1, \ldots, Y_n) \mid g \in \mathfrak{q}\}$. Hence, $X \times Y$ is closed. To prove it's irreducible, let $X \times Y = Z_1 \cup Z_2$ where Z_1, Z_2 are closed. For every $x \in X$ we have $\{x\} \times Y \subseteq Z_1$ or $\{x\} \times Y \subseteq Z_2$, as Y is irreducible and isomorphic to $\{x\} \times Y$. Thus

$$X = X_1 \cup X_2 \ , \quad \text{where} \quad X_i = \{x \in X \mid \{x\} \times Y \subseteq Z_i\} = \bigcap_{y \in Y} \{x \in X \mid (x, y) \in Z_i\}$$
$$= \bigcap_{y \in Y} \Big((X \times \{y\}) \cap Z_i \Big)$$

are closed (as every *slice* $(X \times \{y\}) \cap Z_i$ on the right-hand side is closed), hence $X = X_1$ or $X = X_2$ and consequently $X \times Y = Z_1$ or $X \times Y = Z_2$.

Let $X = X_0 \subsetneq \ldots \subsetneq X_a = k^m$ and $Y = Y_0 \subsetneq \ldots \subsetneq Y_b = k^n$ be chains of irreducible closed subsets, then (using the that $X_i \times Y_j$ is irreducible closed again by the above)

$$X \times Y = X_0 \times Y_0 \subsetneq X_0 \times Y_1 \subsetneq \ldots \subsetneq X_0 \times Y_b \subsetneq X_1 \times Y_b \subsetneq \ldots \subsetneq X_a \times Y_b = k^{m+n}$$

is a such a chain for $X \times Y$, showing $\operatorname{codim}(X \times Y, k^{m+n}) \geq a + b$.

Denote $\dim(X) = d$ and $\dim(Y) = e$. Let $X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_d = X$ and $Y_0 \subsetneq Y_1 \subsetneq \ldots \subsetneq Y_e = Y$ be chains of irreducible closed subsets, then

$$X_0 \times Y_0 \subsetneq X_0 \times Y_1 \subsetneq \ldots \subsetneq X_0 \times Y_e \subsetneq X_1 \times Y_e \subsetneq \ldots \subsetneq X_d \times Y_e = X \times Y$$

is a similar chain. Hence $\dim(X \times Y) \geq d + e$.

Now observe that $a + d = m$, $b + e = n$, and $\dim(X \times Y) + \operatorname{codim}(X \times Y, k^{m+n}) = m + n$, because, by Theorem A, equality occurs in (A.1.2). We conclude

$$m + n = a + d + b + e \leq \dim(X \times Y) + \operatorname{codim}(X \times Y, k^{m+n}) = m + n$$

showing that the inequalities of the previous two steps are actually equalities. *q.e.d.*

Theorem 13 ([1, Concluding remarks, Corollary 3]). *Let $X, Y \subseteq k^n$ be irreducible and closed, then any irreducible component Z of $X \cap Y$ has codimension*

$$\operatorname{codim}(Z, k^n) \leq \operatorname{codim}(X, k^n) + \operatorname{codim}(Y, k^n) \ .$$

Remark. It follows that the dimension of any irreducible component of $X \cap Y$ is greater then or equal to $\dim(X) + \dim(Y) - n$. Note that the assumption *does not* imply $X \cap Y \neq \emptyset$ unless $X = k^n$ or $Y = k^n$ (or, unless one takes the intersection in $\mathbb{P}^n(k)$).

Proof. The intersection $X \cap Y$ is homeomorphic to $(X \times Y) \cap \Delta$ where

$$\Delta = \left\{(x,y) \in k^{n+n} \;\middle|\; x = y\right\} = \bigcap_{i=1}^{n} V(D_i)\ , \quad D_i = X_i - Y_i \in \mathcal{O}(k^{n+n})$$

denotes the *diagonal* in k^{2n}. Thus, if Z is any irreducible component of $(X \times Y) \cap \Delta$ we have $\operatorname{codim}(Z, X \times Y) \leq n$ by Corollary 2. Now Proposition 1 yields

$$\dim(Z) = \dim(X \times Y) - \operatorname{codim}(Z, X \times Y) \geq \dim(X) + \dim(Y) - n$$

and hence

$$\operatorname{codim}(Z, k^n) = n - \dim(Z) \leq 2n - \dim(X) - \dim(Y) = \operatorname{codim}(X, k^n) + \operatorname{codim}(Y, k^n)\ ,$$

proving the assertion. *q.e.d.*

Theorem 14. *Let R be a Noetherian domain.*

(*a*) *Every $r \in R \setminus (R^\times \cup \{0\})$ can be written as a product $r = \prod_{i=1}^{k} r_i$ of irreducible factors r_i.*

(*b*) *The following conditions are equivalent:*

(α) *The above decomposition is unique up to permutation and multiplicative equivalence of the factors.*

(β) *For any irreducible $p \in R$, $(p) = pR$ is a prime ideal.*

(γ) *Any $\mathfrak{p} \in \operatorname{Spec} R$ such that $\operatorname{ht}(\mathfrak{p}) = 1$ is principal, i.e. $\mathfrak{p} = (p)$ for some $p \in R$.*

1.2. The nilradical, the Jacobson radical and the Lemma of Nakayama(-Azumaya-Krull)

Proposition 1. *If R is any ring, then*

$$\bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p} = \operatorname{nil}(R) := \{f \in R \mid f^n = 0 \text{ for some } n \in \mathbb{N}\} = \sqrt{(0)}\ .$$

The ideal $\operatorname{nil}(R)$ is called the **nilradical** *of R.*

Proof. If f is nilpotent, i.e. $f^n = 0$ for some n, then $f^n \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$, hence also $f \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$.

Let $f^n \neq 0$ for all $n \in \mathbb{N}$, then R_f (the localization of R at $f^{\mathbb{N}} = \{1, f, f^2, \ldots\}$) is not the null ring, hence there is a prime ideal $\mathfrak{q} \in \operatorname{Spec}(R_f)$. Its preimage $\mathfrak{p} = \mathfrak{q} \sqcap R$ is in $\operatorname{Spec}(R)$ and $f \notin \mathfrak{p}$ as f becomes a unit in R_f. *q.e.d.*

Corollary 1. *There is a canonical bijection*

$$\begin{aligned}\{\textit{Zariski-closed subsets } A \subseteq \operatorname{Spec} R\} &\xrightarrow{\sim} \left\{\textit{ideals } I \subseteq R \textit{ such that } I = \sqrt{I}\right\} \\ A \subseteq \operatorname{Spec} R &\longmapsto I = \bigcap_{\mathfrak{p} \in A} \mathfrak{p} \\ \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\} = V(I) &\longmapsfrom I\end{aligned}$$

in which the irreducible sets correspond to the prime ideals.

Proof. For the first assertion, the only non-trivial part is that going from the right to the left and back again equals the identity. This can be seen from

$$\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}\,, \tag{1}$$

which follows from applying Proposition reffprop:nilradicalCapPrimeIdeals to R/I. The assertion about prime ideals is left as an exercise (and you should have done this on exercise sheet #2!). *q.e.d.*

Proposition 2. *The intersection of the maximal ideals of R, called the* **Jacobson-radical**, *is*

$$\bigcap_{\mathfrak{m} \in \mathfrak{m}\text{-Spec } R} \mathfrak{m} = \operatorname{rad}(R) = \{r \in R \mid 1 + xr \in R^\times \textit{ for all } x \in R\}\,. \tag{2}$$

Proof. Let $r \in \bigcap_{\mathfrak{m} \in \mathfrak{m}\text{-Spec}} \mathfrak{m}$ and $x \in R$. If $1 + xr \notin R^\times$ it must be contained in some maximal ideal $\mathfrak{m}$ or R. Since $r \in \mathfrak{m}$ and $1 = 1 + xr - xr \in \mathfrak{m}$, which is a contradiction.

Conversely, let $\mathfrak{m}$ be maximal and $r \notin \mathfrak{m}$. Then $\mathfrak{K}(\mathfrak{m}) = R/\mathfrak{m}$ is a field. Let $-x \mod \mathfrak{m}$ be inverse to $r \mod \mathfrak{m}$ (that being non-zero due to $r \notin \mathfrak{m}$) in that field. Then $xr + 1 \in \mathfrak{m}$ and $xr + 1 \notin R^\times$, so r is not an element of the right hand side. *q.e.d.*

Example 1. If R is a local ring and $\mathfrak{m}$ its maximal ideal, then $\operatorname{rad}(R) = \mathfrak{m} = R \setminus R^\times$.

The following is usually known under the name *Nakayama's lemma*. However, Professor Franke rather would like to attribute it to Azumaya and Krull (as Matsumura does in [2]). Making a compromise, it will, from now on, be cited as [NAK].

Proposition 3 (Nakayama's lemma)**.** *Let R ba any ring, M a finitely generated R-module such that $\operatorname{rad}(R) \cdot M = M$. Then $M = 0$.*

Proof. Let $m = (m_1, \ldots, m_k)^t$ be generators of M. As $M = \operatorname{rad}(R) \cdot M$ there are $\rho_{i,j} \in \operatorname{rad}(R)$ such that $m_i = \sum_{j=1}^k \rho_{i,j} m_j$. In other words $(\mathrm{id}_k - \rho) \cdot m = 0$ where ρ is the matrix formed by the $\rho_{i,j}$. But $\det(\mathrm{id}_k - \rho) \equiv 1 \mod \operatorname{rad}(R)$ by the Leibniz formula as $\operatorname{rad}(R)$ is an ideal containing the $\rho_{i,j}$. By (2), we conclude $\det(\mathrm{id}_k - \rho) \in R^\times$. Hence, by Cramers rule, $\mathrm{id}_k - \rho$ has an inverse matrix. Therefore $(\mathrm{id}_k - \rho) \cdot m = 0$ implies $m = 0$ and thus $M = 0$. *q.e.d.*

Applying Proposition 3 to M/N, we obtain the following corollary.

Corollary 2. *If M is finitely generated R-module and $N \subseteq M$ any submodule such that $M = N + \operatorname{rad}(R) \cdot M$ then $M = N$ (actually, it suffices M/N to be finitely generated).*

Remark. [NAK] is typically applied to local rings R: If $\mathfrak{m}$ denotes the maximal ideal, then $M = \mathfrak{m} \cdot M + N$ implies $M = N$ if M is finitely generated.

1.3. Regular rings

Proposition 1. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$, then $\mathfrak{m}/\mathfrak{m}^2$ is a k-vector space of finite dimension and*

$$\dim(R) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2) \ .$$

Proof. If $\mu_1, \ldots, \mu_n$ generate the ideal $\mathfrak{m}$, then their images $\overline{\mu}_1, \ldots, \overline{\mu}_n$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space, proving finite dimensionality.

Conversely, let $\mu_1, \ldots, \mu_n \in \mathfrak{m}$ such that their images $\overline{\mu}_1, \ldots, \overline{\mu}_n$ form a basis of $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space. Then $\mathfrak{m} \subseteq \mu_1 R + \ldots + \mu_n R + \mathfrak{m}^2$ hence $\mathfrak{m} = \mu_1 R + \ldots + \mu_n R$ by Corollary 1.2.2 applied to $M = \mathfrak{m}$, $N = \mu_1 R + \ldots + \mu_n R$. By Theorem 12, $\mathrm{ht}(\mathfrak{m}) \leq n$. Thus,

$$\dim(R) = \mathrm{ht}(\mathfrak{m}) \leq n = \dim_k \mathfrak{m}/\mathfrak{m}^2 \ ,$$

finishing the proof. *q.e.d.*

Definition 1 (Regularity)**.** (*a*) A Noetherian local ring is called **regular** if equality occurs in $\dim(R) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

(*b*) For algebraic varieties X, we call X **regular at $x \in X$** if $\mathcal{O}_{X,x}$ is regular. X is called **regular** if it is regular at all $x \in X$.

Remark 1. If R is any Noetherian ring and $\mathfrak{p} \in \operatorname{Spec} R$, then $(\mathfrak{p}R_\mathfrak{p})/(\mathfrak{p}R_\mathfrak{p})^2 \simeq (\mathfrak{p}/\mathfrak{p}^2)_\mathfrak{p}$ and $R_\mathfrak{p}$ is regular (or R is *regular at* $\mathfrak{p}$) iff $\mathfrak{p}/\mathfrak{p}^2$ has dimension $\mathrm{ht}(\mathfrak{p})$ as a $k(\mathfrak{p})$-vector space. In particular, R is regular at $\mathfrak{m} \in \mathfrak{m}\text{-Spec}\, R$ iff $\dim(R_\mathfrak{m}) = \mathrm{ht}(\mathfrak{m})$ equals $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. By a result by Serre (which has an easier proof in the classical situation $R = \mathcal{O}_{X,x}$), a regular local ring is regular at all of its prime ideals, i.e. if R is a regular local ring, then so is $R_\mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Spec} R$.

A Noetherian ring R is called *regular* iff $R_\mathfrak{p}$ is regular for all $\mathfrak{p} \in \operatorname{Spec} R$ or (equivalently) iff $R_\mathfrak{m}$ is regular for any $\mathfrak{m} \in \mathfrak{m}\text{-Spec}\, R$. These two definitions are equivalent as $R_\mathfrak{p} \simeq (R_\mathfrak{m})_\mathfrak{p}$ if $\mathfrak{p} \in \operatorname{Spec} R$ is prime and $\mathfrak{m}$ a maximal ideal containing $\mathfrak{p}$. Hence, if $R_\mathfrak{m}$ is regular then so is $R_\mathfrak{p}$ by Serre's result.

Note that despite Serre's theorem there are Noetherian rings R such that

$$\{\mathfrak{p} \in \operatorname{Spec} R \mid R_\mathfrak{p} \text{ is } \textit{not} \text{ regular}\}$$

fails to be closed in $\operatorname{Spec} R$.

Remark. In other words, a Noetherian local ring R with maximal ideal $\mathfrak{m}$ is regular at $\mathfrak{m}$ iff $\mathfrak{m}$ may be generated by $\dim(R)$ elements. In general, R is regular at its maximal ideal $\mathfrak{m}$ if (this *if* intentionally contains only one *f*!) $\mathfrak{m}$ may be generated by $\mathrm{ht}(\mathfrak{m})$ elements.

Example. (*a*) $R = k[X_1, \ldots, X_n]$ is regular. Indeed, let $\mathfrak{m} \subseteq R$ be a maximal ideal. If corresponds to some $x \in k^n$ (its only zero) and has the form $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)_R$, hence may be generated by n elements. But $\mathrm{ht}(\mathfrak{m}) = n$ by [1, Theorem 10] from Algebra I.

(*b*) $X = k^n$ is regular at all of its points, since $\mathcal{O}_{X,x} \simeq R_\mathfrak{m}$ ([1, Proposition 2.3.4]).

(*c*) Any field is regular.

Proposition 2 (Jacobian criterion of regularity)**.** *Let $X \subseteq k^n$ be a quasi-affine variety in k^n. Let $\mathfrak{p} \subseteq R = k[X_1, \dots, X_n]$ be the ideal of functions vanishing on X. Then X is regular at $x \in X$ iff*

$$\dim_k \left\{ \nabla f(x) = \left(\frac{\partial f}{\partial X_i}(x) \right)_{i=1}^{n} \;\middle|\; f \in \mathfrak{p} \right\} = \operatorname{codim}(X, k^n) \,.$$

Proof. Since $\dim(\overline{X}) = \dim(X)$ and $\mathcal{O}_{\overline{X},x} = \mathcal{O}_{X,x}$, we may replace X by its closure $\overline{X} = V(\mathfrak{p})$ and assume X to be affine. Let $R = k[X_1, \dots, X_n]$, $\mathfrak{m} \subseteq R$ the ideal of functions vanishing at x. The homomorphism

$$\begin{aligned} \varphi \colon \mathfrak{m} &\longrightarrow k^n \\ f &\longmapsto \nabla f(x) \end{aligned}$$

of k-vector spaces is surjective since $\mathfrak{m}$ is generated by $(X_1 - x_1), \dots, (X_n - x_n)$ and $\varphi(X_i - x_i)$ is the i^{th} unit vector in k^n. We have $\mathfrak{m}^2 \subseteq \ker \varphi$ (which can be easily checked on the generators $(X_i - x_i)(X_j - x_j)$ of $\mathfrak{m}^2$). On the other hand, $\dim_k \mathfrak{m}/\mathfrak{m}^2 = n$ as k^n is regular at x. Therefore,

$$\begin{aligned} \mathfrak{m}/\mathfrak{m}^2 &\xrightarrow{\sim} k^n \\ (f \mod \mathfrak{m}^2) &\longmapsto \nabla f(x) \end{aligned} \tag{1}$$

is (well-defined and) an isomorphism of k-vector spaces. Under this isomorphism, the image of $\mathfrak{p}$ in $\mathfrak{m}/\mathfrak{m}^2$ is mapped to $\mathcal{N} = \{\nabla f(x) \mid f \in \mathfrak{p}\}$.

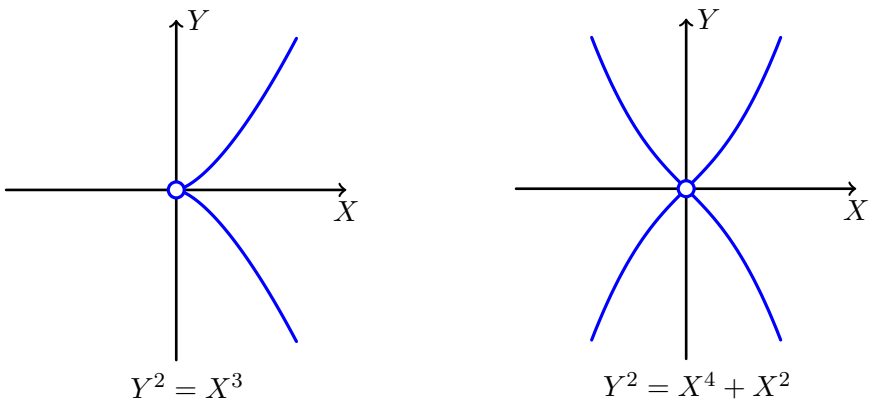
Denote by $\mathfrak{n} \subseteq \mathcal{O}(X) = R/\mathfrak{p}$ the ideal of regular functions on X vanishing at x. Then $\mathfrak{n} = \mathfrak{m}/\mathfrak{p}$. We have $\mathcal{O}_{X,x} \simeq \mathcal{O}(X)_{\mathfrak{n}}$, hence X is regular at x iff $\dim_k(\mathfrak{n}/\mathfrak{n}^2) = \dim(X)$. As $\mathfrak{n}/\mathfrak{n}^2 \simeq \mathfrak{m}/(\mathfrak{p} + \mathfrak{m}^2)$, this implies that (1) maps $\mathfrak{n}/\mathfrak{n}^2$ isomorphically to $k^n/\mathcal{N}$ (as a quotient of k-vector spaces) and X is regular at x iff

$$n - \dim \mathcal{N} = \dim(X) \,, \quad \text{or equivalently} \quad \dim \mathcal{N} = n - \dim(X) = \operatorname{codim}(X, k^n) \,.$$

This shows the assertion. *q.e.d.*

Remark. The derivatives occurring are the usual formal derivatives used in algebra. Inseparability does not play a role here as k is algebraically closed. When $k \neq \overline{k}$ has positive characteristic and $x \in \overline{k}^n$ has some x_i which is inseparable, the above argument collapses and X may be regular (but not *smooth*) at x even if the Jacobian criterion of regularity is violated.

Example. For $\mathfrak{p} = (X^2 - X^3)$ and $\mathfrak{q} = (Y^2 - X^4 - X^2)$ (both ideals in $k[X, Y]$), $V(\mathfrak{p})$ and $V(\mathfrak{q})$ have *singular points* precisely in the origin, provided that $\operatorname{char} k$ is 0 or greater than 3.



$Y^2 = X^3$ $\qquad$ $Y^2 = X^4 + X^2$

Remark. By Proposition 1 and the proof of Proposition 2,

$$\dim \{\nabla f(x) \mid f \in \mathfrak{p}\} \leq \operatorname{codim}(X, k^n) .$$

Remark 2. The k-vector space $\mathcal{N} = \{\nabla f(x) \mid f \in \mathfrak{p}\}$ may be viewed as the *conormal space* to X at x (at least if X is regular at x) and its complement

$$\mathcal{N}^\perp = \left\{ \xi = (\xi_i)_{i=1}^n \in k^n \;\middle|\; \sum_{i=1}^n \frac{\partial f}{\partial X_i}(x) \cdot \xi_i = 0 \text{ for all } f \in \mathfrak{p} \right\}$$

as the *tangent space* at x of X.

Theorem 15. *Let $X \subseteq k^n$ be quasi-affine and $Y, Z \subseteq X$ be irreducible closed subsets and C be any irreducible component of $Y \cap Z$. If there is at least one point $x \in C$ such that X is regular at x, then*

$$\operatorname{codim}(C, X) \leq \operatorname{codim}(Z, X) + \operatorname{codim}(Y, X) .$$

Remark 3. Let $n = 4$, identify k^4 with the space of 2×2-matrices and let $X = \{A \mid \det A = 0\}$. This has dimension 3 (where X turns out to be irreducible), and

$$Y = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \;\middle|\; a, b \in k \right\} , \quad Z = \left\{ \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \;\middle|\; c, d \in k \right\}$$

are irreducible closed subsets of codimension 1 and (thus) dimension 2. But $Y \cap Z = \{0\}$ has codimension 3 in X.

Proof of Theorem 15. First of all, passing to the respective closures (which doesn't change codimension, e.g. by the *locality of codimension*, cf. Remark 1.1.1(*a*)), we may assume that X, Y, Z are affine.

Step 1. As in the proof of Theorem 13, let Δ be the diagonal in k^{2n}. We will show the following: If $f_1, \ldots, f_d \in \mathcal{O}_{X,x}$ generate the maximal ideal $\mathfrak{m}_{X,x}$ of $\mathcal{O}_{X,x}$, then there exists an affine open neighbourhood U of x in X and preimages of the f_i in $\mathcal{O}(U)$ (which we will also call f_i) such that

$$\Delta \cap (U \times U) = \{(y, z) \in U \times U \mid f_i(y) = f_i(z) \text{ for } 1 \leq i \leq d\} = V(g_1, \ldots, g_d) \qquad (*)$$

(where $g_i(y, z) = f_i(y) - f_i(z)$), possibly after shrinking U. As U is required to be *affine open*, i.e. $U = X \setminus V(h)$ for some $h \in \mathcal{O}(X)$, we obtain that $Y \cap U = Y \setminus V(h|_Y) =: Y'$ and $Z \cap U = Z \setminus V(h|_Z) =: Z'$ are affine open as well, hence isomorphic to affine varieties ([1, Proposition 2.2.4]) and it makes sense to talk about vanishing sets of regular functions on Y' and Z' – which we will do now.

Consider $\gamma_1, \ldots, \gamma_d \in \mathcal{O}(Y' \times Z')$, $\gamma_i(y, z) = f_i|_{Y'}(y) - f_i|_{Z'}(z)$ (this essentially restricts $g_1, \ldots, g_d$ to $Y' \times Z'$). We identify $Y \cap Z$ with $\Delta \cap (Y \times Z)$ and thus C with its respective image, as we did in the proof of Theorem 13. Hence C is an irreducible component of $\Delta \cap (Y \times Z)$. Then $C' = C \cap (U \times U)$ is an irreducible component of $\Delta \cap (Y' \times Z') = V(\gamma_1, \ldots, \gamma_d)$ (here we used $(*)$) and Theorem 12 together with *locality of codimension* yields

$$\operatorname{codim}(C, Y \times Z) = \operatorname{codim}(C', Y' \times Z') \leq d .$$

We silently went over an important detail: $U \times U \subseteq X \times X$ is open again. This is easily seen as $(X \setminus U) \times X$ and $X \times (X \setminus U)$ are closed (using e.g. the argument from the proof of Proposition 1.1.1), but don't be fooled: this *does not* follow from *product topology stuff*; the Zariski topology on k^{2n} and $X \times X$ is *not* the product of the Zariski topologies on k^n or X.

Enough of that. From Proposition 1.1.1 we get

$$\begin{aligned}\operatorname{codim}(Y \times Z, X \times X) &= \dim(X \times X) - \dim(Y \times Z) \\ &= (\dim(X) - \dim(Y)) + (\dim(X) - \dim(Z)) \\ &= \operatorname{codim}(Y, X) + \operatorname{codim}(Z, X)\end{aligned}$$

and hence,

$$\begin{aligned}\operatorname{codim}(C, X) &= \dim(X) - \dim(C) \\ &= \dim(X) - (\dim(X) + \dim(X) - \operatorname{codim}(C, X \times X)) \\ &= \operatorname{codim}(C, X \times X) - \dim(X) \\ &= \operatorname{codim}(C, Y \times Z) + \operatorname{codim}(Y \times Z, X \times X) - \dim(X) \\ &\leq \operatorname{codim}(Y, X) + \operatorname{codim}(Z, X) + d - \dim(X) \\ &= \operatorname{codim}(Y, X) + \operatorname{codim}(Z, X),\end{aligned}$$

provided that $d = \dim(X)$, which is possible for an appropriate choice of the f_i when X is regular at x (by [NAK], $\mathfrak{m}_{X,x}$ can be generated by $\dim(X)$ elements, cf. the proof of Proposition 1 or [1, Concluding remarks, Lemma 1(c)]).

Step 2. Let $R = k[X_1, \ldots, X_m]$ and $\mathfrak{p}, \mathfrak{m} \subseteq R$ be the prime ideal defining $k^\ell \times \{0\}^{m-\ell}$ respectively the maximal ideal defining $\{0\}^m$. Then $\mathfrak{m}^2 \cap \mathfrak{p} \subseteq \mathfrak{m} \cdot \mathfrak{p}$. This can be shown as follows. Since $\mathfrak{m}$ is generated by $X_1, \ldots, X_m$, $\mathfrak{m}^2$ is generated by the $X_i X_j$ (with i, j not necessarily distinct). Similarly, $\mathfrak{p}$ is the ideal generated by $X_{\ell+1}, \ldots, X_m$. If $f \in R$ lies in both $\mathfrak{m}^2$ and $\mathfrak{p}$, each monomial of f must be divisible by some $X_i X_j$ as well as by some $X_{\ell+r}$. Then this monomial is divisible by $X_i X_{\ell+r}$ or $X_j X_{\ell+r}$, hence contained in $\mathfrak{m} \cdot \mathfrak{p}$. Now $f \in \mathfrak{m} \cdot \mathfrak{p}$ because each monomial lies in that ideal.

Step 3. Let $\xi \in k^m$, $L \subseteq k^m$ an affine subspace containing ξ. Let $\mathfrak{p}$ be the prime ideal defining L and $\mathfrak{m}$ the maximal ideal defining $\{\xi\}$. Then $\mathfrak{p} \cap \mathfrak{m}^2 \subseteq I \cdot \mathfrak{m}$. This can be reduced to the previous step by an affine automorphism of k^m.

Step 4. Let $x \in k^n$, $\mathfrak{m}_x \subseteq S = k[X_1, \ldots, X_n]$ the maximal ideal defined by x, $f_1, \ldots, f_n \in S$ such that their images generate $\mathfrak{m}_x/\mathfrak{m}_x^2$. Then there is $h \in R = k[X_1, \ldots, X_n, Y_1, \ldots Y_n]$ such that $h(x, x) \neq 0$ and $h \cdot \mathfrak{p}_\Delta \subseteq (g_1, \ldots, g_n)_R$ where $g_i(y, z) = f_i(y) - f_i(z)$ and $\mathfrak{p}_\Delta \subseteq R$ is the prime ideal of functions vanishing on $\Delta = \{(y, y) \mid y \in k^n\}$. To see this, let $\xi = (x, x)$ and $\mathfrak{q} = \mathfrak{p}_\Delta \cdot R_{\mathfrak{m}_\xi}$, where $\mathfrak{m}_\xi \subseteq R$ denotes the maximal ideal of functions vanishing on ξ. Let $\mathfrak{n} = \mathfrak{m}_\xi \cdot R_{\mathfrak{m}_\xi}$ denote the maximal ideal of the local ring $R_{\mathfrak{m}_\xi}$. From the previous step it follows that

$$\mathfrak{n}^2 \cap \mathfrak{q} \subseteq \mathfrak{q} \cdot \mathfrak{n}. \tag{2}$$

Let $\mathfrak{g} \subseteq \mathfrak{q}$ be the ideal generated by the images of the g_i. Our long-term goal is to show $\mathfrak{g} = \mathfrak{p}$. Let $f \in \mathfrak{p}_\Delta$. We claim that there are $c_1, \ldots, c_n$ such that $g = f - \sum_{i=1}^n c_i g_i$ is in $\mathfrak{m}_\xi^2$. Indeed, by

the isomorphism (1) this is equivalent to $\nabla g(\xi) = 0$. Since $f|_\Delta = 0$, we have $\frac{\partial f}{\partial X_i}(\xi) + \frac{\partial f}{\partial Y_i}(\xi) = 0$ at $\xi \in \Delta$ and the same for the g_i. Thus, it is sufficient to have

$$\frac{\partial f}{\partial X_i}(\xi) = \sum_{j=1}^{n} c_j \frac{\partial g_j}{\partial X_i}(\xi) = \sum_{j=1}^{n} c_j \frac{\partial f_j}{\partial X_i}(x) \quad \text{for all } i = 1, \dots, n$$

(the second equality is tautological), which is possible since the f_i generate $\mathfrak{m}_x/\mathfrak{m}_x^2$, hence the $\nabla f_i(x)$ generate k^n by the isomorphism (1). It follows that $\mathfrak{p}_\Delta \subseteq (g_1, \dots, g_n)_R + (\mathfrak{p}_\Delta \cap \mathfrak{m}_\xi^2) = (g_1, \dots, g_n) + \mathfrak{p}_\Delta \cdot \mathfrak{m}_\xi$ (the second equality follows from Step 3). This is still true in the localization at $\mathfrak{m}_\xi$, i.e. $\mathfrak{q} \subseteq \mathfrak{g} + \mathfrak{q} \cdot \mathfrak{n}$. By Corollary 1.2.2, we have $\mathfrak{q} = \mathfrak{g}$.

Now let $\varphi_1, \dots, \varphi_N$ generate $\mathfrak{p}_\Delta$. Since $\mathfrak{q} = \mathfrak{p}_\Delta \cdot R_{\mathfrak{m}_\xi}$ is generated by the images of the g_i, there are $h_i \notin \mathfrak{m}_\xi$ and such that $h_i \cdot \varphi_i \in (g_1, \dots, g_n)_R$. Then $h = h_1 \cdots h_N$ fulfills $h(\xi) = h(x, x) \neq 0$ and $h \cdot \mathfrak{p}_\Delta \subseteq (g_1, \dots, g_n)_R$.

Step 5. Let $f_1, \dots, f_d$ be elements of $S = k[X_1, \dots, X_n]$ such that their images in $\mathcal{O}_{X,x}$ form a base of $\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2$ (again, $\mathfrak{m}_{X,x}$ is the maximal ideal of the local ring $\mathcal{O}_{X,x}$, which Professor Franke would like to express as $\mathfrak{m}_{X,x} = \operatorname{rad} \mathcal{O}_{X,x}$). Let $f_{d+1}, \dots, f_n$ be chosen in such a way that the images of $f_1, \dots, f_n$ form a base of $\mathfrak{m}_x/\mathfrak{m}_x^2$. Why is this possible? We have $\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2 = \mathfrak{n}/\mathfrak{n}^2$, $\mathfrak{n} \subseteq \mathcal{O}(X)$ denoting the maximal ideal of $\mathcal{O}(X)$ of functions vanishing at x. Then $\mathfrak{n}/\mathfrak{n}^2$ is a quotient of $\mathfrak{m}_x/\mathfrak{m}_x^2$ (as we saw in the proof of Proposition 2). If h is as in the previous step, $U = X \setminus V(h)$ has the required property. *q.e.d.*

Remark 4 (on (2))**.** Let R be an arbitrary ring, $S \subseteq R$ a multiplicative subset, I and J ideals in R. Then

$$\begin{aligned}(I + J) \cdot R_S &= I \cdot R_S + J \cdot R_S \\ (I \cap J) \cdot R_S &= I \cdot R_S \cap J \cdot R_S \\ (I \cdot J) \cdot R_S &= (I \cdot R_S) \cdot (J \cdot R_S) \\ \sqrt{I \cdot R_S} &= \sqrt{I} \cdot R_S\end{aligned}$$

Proof. We will only prove the second equality, they are all quite similar. The image of $I \cap J$ is contained in both $I \cdot R_S$ and $J \cdot R_S$, hence so is $(I \cap J) \cdot R_S$, proving $(I \cap J) \cdot R_S \subseteq I \cdot R_S \cap J \cdot R_S$. Conversely, let $\rho \in (I \cdot R_S) \cap (J \cdot R_S)$. Since $\rho \in I \cdot R_S$, $\rho = \frac{i}{s}$ where $i \in I$ and $s \in S$. Since $\rho \in J \cdot R_S$, $\rho = \frac{j}{t}$ where $j \in J$ and $t \in S$. Since $\frac{i}{s} = \frac{j}{t}$ in R_S, there is $\sigma \in S$ such that $\sigma i t = \sigma j s$. Then $\rho = \frac{\sigma i t}{\sigma s t} = \frac{\sigma j s}{\sigma s t} \in (I \cap J) \cdot R_S$. *q.e.d.*

1.4. Derivations and the module of Kähler differentials

Definition 1 (Derivations)**.** Let A be a ring, M an A-module, $d\colon A \to M$ a homomorphism of the additive group. We say that d is a **derivation** of A with values in M if it satisfies the *Leibniz rule*

$$d(a \cdot b) = b \cdot d(a) + a \cdot d(b) \ .$$

If A is an R-algebra and $A \xrightarrow{d} M$ a derivation of A, we call d *R-linear* if the following equivalence conditions hold:

(a) $d(r) = 0$ for all $r \in R$.

(b) $d(r \cdot a) = r \cdot d(a)$ for all $r \in R, a \in A$.

Let $\mathrm{Der}(A, M)$ denote the set of derivations with values in M. This can be given a canonical A-module structure via $(a \cdot d)(b) = a \cdot d(b)$.

Proof. Let $d \in \mathrm{Der}(A, M)$. Note that we always have $d(1) = 0$ as $d(1) = d(1 \cdot 1) = d(1) + d(1)$ by the Leibniz rule. Now, assuming $d(r \cdot a) = r \cdot d(a)$ for all $r \in R, a \in A$, we obtain $d(r) = d(r \cdot 1) = 0$. Conversely, if $d(r) = 0$ for all $r \in R$, then $d(a \cdot r) = a \cdot d(r) + r \cdot d(a) = r \cdot d(a)$ by the Leibniz rule. Hence, (a) and (b) are indeed equivalent. *q.e.d.*

Remark 1. The set $\mathrm{Der}_R(A, M)$ of R-linear derivations forms an A-submodule of $\mathrm{Der}(A, M)$.

Example 1. A derivation $d \in \mathrm{Der}_R(R[X_1, \ldots, X_n], M)$ is uniquely determined by the tuple $(m_1, \ldots, m_n) \in M^n$ via

$$\begin{aligned} d &\longmapsto (dX_1, \ldots, dX_m) \\ \left(P \mapsto \sum_{i=1}^{n} \frac{\partial P}{\partial X_i} \cdot m_i\right) &\longmapsto\!\shortmid\ (m_1, \ldots, m_n)\ . \end{aligned}$$

Note that the left hand side is indeed a derivation:

$$d(PQ) = \sum_{i=1}^{n} \frac{\partial (PQ)}{\partial X_i} \cdot m_i = \sum_{i=1}^{n} \left(P \cdot \frac{\partial Q}{\partial X_i} + Q \cdot \frac{\partial P}{\partial X_i}\right) m_i = P \cdot d(Q) + d(P) \cdot Q\ .$$

It is easy to see that the two maps are inverse to each other.

Remark. $\mathrm{Der}(A, -)$ and $\mathrm{Der}_R(A, -)$ are functors: If $M \xrightarrow{\mu} N$ is a homomorphism of A-modules then

$$\begin{aligned} \mathrm{Der}(A, M) &\longrightarrow \mathrm{Der}(A, N) \\ d &\longmapsto \mu \circ d \end{aligned}$$

is a morphism of A-modules and similar for $\mathrm{Der}_R(A, M)$ and $\mathrm{Der}_R(A, N)$.

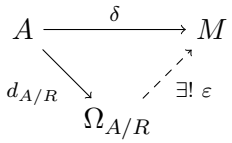
The previous Example 1 can be re-formulated as saying that

$$\begin{aligned} d\colon A = R[X_1, \ldots, X_n] &\longrightarrow A^n \\ P &\longmapsto \nabla P = \left(\frac{\partial P}{\partial X_1}, \ldots, \frac{\partial P}{\partial X_n}\right) \end{aligned}$$

is the *universal* R-linear derivation of A: Any $\delta \in \mathrm{Der}_R(A, M)$ can be uniquely expressed as $\delta = \mu \circ d$ where $A^n \xrightarrow{\mu} M$ is a uniquely determined A-linear homomorphism.

Definition 2 (Kähler differentials)**.** Let A be an R-algebra. A **module of Kähler differentials** for A/R is an A-module $\Omega_{A/R}$ together with $d_{A/R} \in \mathrm{Der}_R(A, \Omega_{A/R})$ satisfying the following universal property:

> For any A-module M and any $\delta \in \mathrm{Der}_R(A, M)$ there is a unique A-homomorphism $\Omega_{A/R} \xrightarrow{\varepsilon} M$ such that



It is worth pointing out that we thus defined $\Omega_{A/R}$ by an (ε, δ)-*definition*!

Remark. (*a*) The universal property characterizes $\Omega_{A/R}$ up to unique isomorphism (if it exists): If $\widetilde{d}_{A/R} \in \mathrm{Der}_R(A, \widetilde{\Omega}_{A/R})$ has the same universal property, there is a unique isomorphism $\Omega_{A/R} \xrightarrow[i]{\sim} \widetilde{\Omega}_{A/R}$ such that $\widetilde{d}_{A/R} = i \circ d_{A/R}$. In fact, the universal property of $d_{A/R}$ shows the existence and uniqueness of a homomorphism i with this property. Reversing the roles of $d_{A/R}$ and $\widetilde{d}_{A/R}$ we also obtain $\widetilde{\Omega}_{A/R} \xrightarrow{j} \Omega_{A/R}$ such that $d_{A/R} = j \circ \widetilde{d}_{A/R}$. Then $\alpha = j \circ i$ satisfies $d_{A/R} = \alpha \circ d_{A/R}$ which implies $\alpha = \mathrm{id}_{\Omega_{A/R}}$ by the universal property of $\Omega_{A/R}$. Exchanging $d_{A/R}$ and $\widetilde{d}_{A/R}$ gives $i \circ j = \mathrm{id}_{\widetilde{\Omega}_{A/R}}$. Thus, i is an isomorphism.

(*b*) For $A = R[X_1, \ldots, X_n]$, $\Omega_{A/R} = \bigoplus_{i=1}^n A \cdot dX_i \simeq A^n$ with $d_{A/R}(P) = \sum_{i=1}^n \frac{\partial P}{\partial X_i} \cdot dX_i$ is a module of Kähler differentials.

(*c*) If A is a quotient of R (i.e. $R \to A$ is surjective) then $\mathrm{Der}_R(A, M) = 0$ for all M, hence $\Omega_{A/R} = 0$.

Definition 3 (Free module)**.** The free A-module F with generating set M, $F = \bigoplus_{m \in M} A$, is the A-module of functions $f \colon M \to A$ with finite support. We define $\delta_x \in F$ by $\delta_x(y) = \delta_{x,y}$ (i.e. $\delta_x(x) = 1$ and $\delta_x(y) = 0$ for $y \neq x$).

Remark. (*a*) One often thinks of F as the module of formal (finite) A-linear combinations of M with $f = \sum_{x \in M} f(x)x$ instead of $f = \sum_{x \in M} = f(x)\delta_x$.

(*b*) We have a bijection, for any A-module N,

$$\begin{aligned} \mathrm{Hom}_{\mathrm{Set}}(M, N) &\xrightarrow{\sim} \mathrm{Hom}_A(F, N) \\ \upsilon &\longmapsto \left(f \mapsto \sum_{m \in M} f(m)\upsilon(m) \right) \\ (m \mapsto \varphi(\delta_m)) &\longmapsto \varphi \ . \end{aligned}$$

In other words, mapping X to the free A-module generated by X as a functor from Set to the category of A-modules is *left-adjoint* to the forgetful functor from the category of A-modules to Set.

Proposition 1. *A module $\Omega_{A/R}$ of Kähler differentials exists for any R-algebra A.*

Proof. We follow the *brute-force* approach to constructing $\Omega_{A/R}$. Let F_A be the free A-module generated by the set A itself and let $K \subseteq F_A$ the submodule generated by the following three types of elements:

(*a*) $\{\delta_x + \delta_y - \delta_{x+y} \mid x, y \in A\}$

(*b*) $\{\delta_r \mid r \in R\}$

(*c*) $\{x\delta_y + y\delta_x - \delta_{xy} \mid x, y \in A\}$

Let $\Omega_{A/R} = F_A/K$, $F \xrightarrow{\pi} \Omega_{A/R}$ be the projection to the quotient and put $d_{A/R}(a) = \pi(\delta_a)$. It is easy to see that $d_{A/R} \in \mathrm{Der}_R(A, M)$ e.g.

$$d_{A/R}(ab) = \pi(\delta_{ab}) = \pi(\delta_{ab} - a\delta_b - \delta_a) + a\pi(\delta_b) + b\pi(\delta_a) = a \cdot d_{A/R}(b) + b \cdot d_{A/R}(a)$$

as $\delta_{ab} - a\delta_b - \delta_a \in K$ and by the definition of $d_{A/R}$.

Let $(A \xrightarrow{d} M) \in \mathrm{Der}_R(A, M)$. By the universal property of F_A there is a unique morphism $c \in \mathrm{Hom}_A(F_A, M)$ such that $d(a) = c(\delta_a)$. We claim that c vanishes on K.

- $c(\delta_a + \delta_b - \delta_{a+b}) = c(\delta_a) + c(\delta_b) - c(\delta_{a+b}) = d(a) + d(b) - d(a+b) = 0$ as d is additive.
- $c(\delta_r) = d(r) = 0$ when $r \in R$ as d is R-linear.
- $c(a\delta_b + b\delta_a - \delta_{ab}) = a \cdot d(b) + b \cdot d(a) - d(ab) = 0$ by the Leibniz rule.

Consequently, due to the universal property of quotient modules, there is a unique $\delta \in \mathrm{Hom}_A(F_A/K, M)$ such that

$$\begin{array}{ccc} F_A & \xrightarrow{\quad d \quad} & M \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle \exists!\ \delta} & \\ & F_A/K & \end{array}$$

commutes. Therefore, $F_A/K = \Omega_{A/R}$ satisfies the universal property. *q.e.d.*

In many cases, the module of Kähler differentials can be calculated using $\Omega_{R[X_1,\ldots,X_n]} \simeq \bigoplus_{i=1}^n R[X_1, \ldots, X_n]dX_i$ and two exact sequences which follow in a straight forward way from

Fact 1. Let R be a ring, A an R-algebra.

(*a*) Let $I \subseteq A$ be any ideal, M any A/I-module, $A \xrightarrow{\pi} A/I$ the projection, then

$$0 \longrightarrow \mathrm{Der}_R(A/I, M) \longrightarrow \mathrm{Der}_R(A, M) \longrightarrow \mathrm{Hom}_{A/I}(I/I^2, M) \tag{1}$$

is exact. Herein, the morphism $\mathrm{Der}_R(A/I, M) \to \mathrm{Der}_R(A, M)$ is defined by $d \mapsto \delta = d \circ \pi$ and $\mathrm{Der}_R(A, M) \to \mathrm{Hom}_{A/I}(I/I^2, M)$ by $\delta \mapsto \varphi = \big(i \mod I^2 \mapsto \delta(i)\big)$.

(*b*) Let B be an A-algebra, M an B-module, then we have the exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Der}_A(B, M) \hookrightarrow \mathrm{Der}_R(B, M) &\longrightarrow \mathrm{Der}_R(A, M) \\ d &\longmapsto d|_A\ . \end{aligned} \tag{2}$$

Proof. We will first proof (*b*). The exactness on the left end is obvious, as is the vanishing of the composition $\mathrm{Der}_A(B, M) \hookrightarrow \mathrm{Der}_R(B, M) \to \mathrm{Der}_R(A, M)$. Let $d \in \mathrm{Der}_R(B, M)$ such that $0 = d|_A$, then d is A-linear, i.e. $d \in \mathrm{Der}_A(B, M)$.

Now about (*a*). That $\mathrm{Der}_R(A/I, M) \to \mathrm{Der}_R(A, M)$ is well-defined is obvious, as derivations are compatible with applying ring homomorphisms on the right. To show that the rightmost

arrow is well-defined, we first need to show that $\delta \in \mathrm{Der}_R(A, M)$ vanishes on I^2. If $i, j \in I$, then $\delta(i \cdot j) = i \cdot \delta(j) + j \cdot \delta(i) = 0$ as $I \cdot M = 0$, hence δ indeed vanishes on I^2 as I^2 is generated by the ij where $i, j \in I$. It follows that φ is indeed a homomorphism of abelian groups. Let $\alpha = a \mod I \in A/I$ and $i \in I$, then $\varphi(\alpha \cdot (i \mod I^2)) = \delta(a \cdot i) = i \cdot \delta(a) + a \cdot \delta(i) = \alpha \cdot \delta(i)$ showing that φ is (A/I)-linear as stated.

Exactness on the left end follows from the surjectivity of $A \xrightarrow{\pi} A/I$. The fact that the composition $d \in \mathrm{Der}_R(A/I, M) \mapsto \delta \in \mathrm{Der}_R(A, M) \mapsto \varphi \in \mathrm{Hom}_{A/I}(I/I^2, M)$ is zero is also obvious: $\varphi(i \mod I^2) = \delta(i) = d(\pi(i)) = d(0) = 0$. Finally, let δ be such that $\varphi = 0$. For $i \in I$, $\delta(i) = \varphi(i \mod I^2) = 0$. Hence there exists a unique group homomorphism $A/I \xrightarrow{d} M$ such that $\delta = d \circ \pi$. The Leibniz rule for d follows from the analogous rule for δ and the surjectivity of π. *q.e.d.*

Fact. Let A be any ring, $M' \to M \to M'' \to 0$ a sequence of A-homomorphisms, then this sequence is exact iff $0 \to \mathrm{Hom}_A(M'', T) \to \mathrm{Hom}_A(M, T) \to \mathrm{Hom}_A(M', T)$ is exact for any A-module T.

Corollary 1. *Let R be a ring, A an R-algebra.*

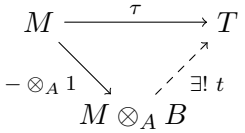
(*a*) *If $I \subseteq A$ is any ideal, we have a canonical short exact sequence of (A/I)-modules*

$$I/I^2 \xrightarrow{\alpha} \Omega_{A/R} \otimes_A A/I \xrightarrow{\beta} \Omega_{(A/I)/R} \longrightarrow 0 \,. \tag{3}$$

(*b*) *If B is any A-algebra, we have a canonical short exact sequence of B-modules*

$$\Omega_{A/R} \otimes_A B \xrightarrow{\kappa} \Omega_{B/R} \xrightarrow{\lambda} \Omega_{B/A} \longrightarrow 0 \,. \tag{4}$$

Remark. (*a*) Tensor products as occuring above are used for change of base: $M \otimes_A B$ is a B-module together with a morphism $M \to M \otimes_A B$, $m \mapsto m \otimes_A 1$ with the following universal property:

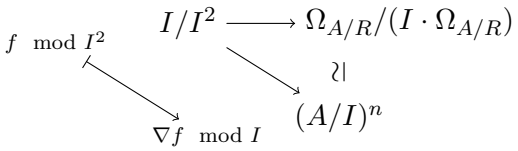
> If T is any B-module and $M \xrightarrow{\tau} T$ any A-linear homomorphism, then there is a unique homomorphism $M \otimes_A B \xrightarrow{t} T$ such that
>
> 
>
>
> commutes, i.e. $\tau(m) = t(m \otimes_A 1)$. In particular, there is an isomorphism $\mathrm{Hom}_A(M, T) \simeq \mathrm{Hom}_B(M \otimes_A B, T)$ of B-modules.

For instance, $V \otimes_{\mathbb{R}} \mathbb{C}$ is the complexification of the $\mathbb{R}$-vector space V. We put $m \otimes_A b = b \cdot (m \otimes_A 1)$. One easy special case is $B = A/I$ in which case

$$M \otimes_A (A/I) = M/(I \cdot M) \,, \quad m \otimes_A (a \mod I) \coloneqq (a \cdot m) \mod (I \cdot M)$$

has the desired universal property.

(*b*) Using and 3 the calculation of $\Omega_{R[T_1,\ldots,T_n]/R}$ it is possible to calculate $\Omega_{(A/I)/R}$ (where $A = R[T_1, \ldots, T_n]$) as the cokernel of



Since any R-algebra of finite type has the form A/I, this provides a way to calculate $\Omega_{B/R}$ for such R-algebras B. Since Example 1 is not (really) limited to case of finitely many variables, other R-algebras could be treated as well.

Proof of Corollary 1. Let us first construct the involved canonical homomorphisms.

- By the universal property of $d_{B/R}$, the derivation $d_{B/A}\colon B \to \Omega_{B/A}$ (which is R-linear) hence has a unique representation

$$d_{B/A} = \lambda \circ d_{B/R} \,,$$

in which λ is an B-homomorphism $\Omega_{B/R} \xrightarrow{\lambda} \Omega_{B/A}$.

- Composing $d_{B/R}\colon B \to \Omega_{B/R}$ with $A \to B$ gives us an element of $\mathrm{Der}_R(A, \Omega_{B/R})$, which, by the universal property of $\Omega_{A/R}$, is given by a unique A-module-homomorphism

$$\Omega_{A/R} \xrightarrow{\kappa'} \Omega_{B/R} \,.$$

By the universal property of $- \otimes_A B$, κ' is given by a unique B-module-homomorphism

$$\Omega_{A/R} \otimes_A B \xrightarrow{\kappa} \Omega_{B/R} \,.$$

In other words, κ is the unique B-module-homomorphism such that $\kappa(d_{A/R}(a) \otimes_A b) = b \cdot d_{B/R}(a)$.

- The A/I-homomorphism β is uniquely determined by

$$\beta\left(d_{A/R}(a) \mod (I \cdot \Omega_{A/R})\right) = d_{(A/I)/R}(a) \,.$$

In other words, this is the special case $B = A/I$ of κ.

- We put

$$\alpha(i \mod I^2) = d_{A/R}(i) \mod (I \cdot \Omega_{A/R}) \,.$$

In other words, α is obtained by applying $\mathrm{Der}_R(A, M) \to \mathrm{Hom}_{A/I}(I/I^2, M)$ from Fact 1 to the derivation $A \xrightarrow{d_{A/R}} \Omega_{A/R} \to \Omega_{A/R}/I \cdot \Omega_{A/R} =: M$.

It remains to show exactness. By this unnamed fact, it is sufficient to show that exactness holds after applying the functor $\mathrm{Hom}_B(-, T)$ for any B-module T (where in (a) we have the special case $B = A/I$). Note that

$$\mathrm{Hom}_A\left(\Omega_{A/R}, T\right) \simeq \mathrm{Der}_R(A, T) \quad \text{and} \quad \mathrm{Hom}_B\left(\Omega_{A/R} \otimes_A B, T\right) \simeq \mathrm{Hom}_A\left(\Omega_{A/R}, T\right)$$

by the universal properties of $\Omega_{A/R}$ and $- \otimes_A B$. Hence, applying $\mathrm{Hom}_B(-, T)$ transforms (3) and (4) into (1) and (2) respectively, thus showing exactness by Fact 1. *q.e.d.*

Fact 1a. This should actually be in Fact 1, but we refuse to change a fact that was stated two lectures ago.

(*c*) When $X \subseteq R$ is multiplicative and M an A_X-module, then we have an isomorphism of A_X-modules

$$\mathrm{Der}_{R_X}(A_X, M) \xrightarrow{\sim} \mathrm{Der}_R(A, M). \tag{5}$$

(*d*) When $S \subseteq A$ is multiplicative and M an A_S-module, then we have an isomorphism of A_S-modules

$$\mathrm{Der}_R(A_S, M) \xrightarrow{\sim} \mathrm{Der}_R(A, M). \tag{6}$$

Proof. Both maps are defined by composition of derivations with the ring homomorphisms $A \to A_X$ respectively $A \to A_S$, so they are well-defined.

To prove (*c*), take any element $d \in \mathrm{Der}_R(A, M)$. This is R-linear and hence defines a unique homomorphism $A_X \xrightarrow{d} M$ of R_X modules, by our assumption on M and the universal property of the localization. To confirm the Leibniz rule, look at

$$d\left(\frac{a}{x}\cdot\frac{\alpha}{\xi}\right) = \frac{d(a\cdot\alpha)}{x\cdot\xi} = \frac{\alpha\cdot d(a) + a\cdot d(\alpha)}{x\cdot\xi} = \frac{\alpha}{\xi}\frac{d(a)}{x} + \frac{a}{x}\frac{d(\alpha)}{\xi} = \frac{\alpha}{\xi}d\left(\frac{a}{x}\right) + \frac{a}{x}d\left(\frac{\alpha}{\xi}\right).$$

This proves surjectivity and injectivity follows from the uniqueness of d.

To show (*d*), let $d \in \mathrm{Der}_R(A_S, M)$ be an element of the kernel, then $d(a)$ when a is in the image of A in A_S. Let $\alpha \in A_S$, then there is σ in the image of S in A_S such that $\sigma\cdot\alpha$ is in the image of A in A_S. Then

$$0 = d(\sigma\cdot\alpha) = \sigma\cdot d(\alpha) + \alpha\cdot d(\sigma) = \sigma\cdot d(\alpha)$$

implies $d(\alpha) = 0$ since $\sigma \in (A_S)^\times$. This shows injectivity of the map. For surjectivity, let $\delta \in \mathrm{Der}_R(A, M)$ and put $d\left(\frac{a}{s}\right) = \frac{s\cdot\delta(a) - a\cdot\delta(s)}{s^2}$ (the *quotient rule*). We have

$$d\left(\frac{\sigma\cdot a}{\sigma\cdot s}\right) = \frac{\sigma\cdot s\cdot\delta(\sigma\cdot a) - \sigma\cdot a\cdot\delta(\sigma\cdot s)}{\sigma^2\cdot s^2} = \frac{s\cdot\delta(a) - a\cdot\delta(s)}{s^2}$$

showing that $d\colon A_S \to M$ is well-defined. That $d(R) = 0$ is trivial, as is the additivity and the Leibniz rule is easily verified. *q.e.d.*

Corollary 1a. *Same as Fact 1a, this should have been stated a long time ago.*

(*c*) *When $X \subseteq R$ is multiplicative, there is a canonical isomorphism of A_X-modules*

$$\Omega_{A_X/R_X} \xleftarrow[\iota]{\sim} (\Omega_{A/R})_X = \Omega_{A/R}\otimes_A A_X \tag{7}$$

(as $A_X = A\otimes R_X$, we could have taken the tensor product $-\otimes_R R_X$ as well).

(*d*) *When $S \subseteq A$ is multiplicative, there is a canonical isomorphism of A_S-modules*

$$\Omega_{A_S/R} \xleftarrow{\sim} (\Omega_{A/R})_S = \Omega_{A/R}\otimes_A A_S\,. \tag{8}$$

Proof. As in the proof of Corollary 1, we should first agree on how the morphisms are supposed to look like.

- As $A \to A_X \xrightarrow{d_{A_X/R_X}} \Omega_{A_X/R_X}$ is an R-linear derivative of A, there is a unique morphism $\Omega_{A/R} \xrightarrow{\alpha} \Omega_{A_X/R_X}$ of A-modules such that the left of the below diagrams commutes. By the universal property of the localization $\Omega_{A/R} \to (\Omega_{A/R})_X = \Omega_{A/R} \otimes_A A_X$ there is a unique A_X-module homomorphism ι such that the right diagram commutes.

$$\begin{array}{ccc} A & \longrightarrow & A_X \\ {\scriptstyle d_{A/R}}\downarrow & & \downarrow{\scriptstyle d_{A_X/R_X}} \\ \Omega_{A/R} & \overset{\exists!\ \alpha}{\dashrightarrow} & \Omega_{A_X/R_X} \end{array} \qquad \begin{array}{ccc} \Omega_{A/R} & \xrightarrow{\alpha} & \Omega_{A_X/R_X} \\ & {\scriptstyle -\otimes_A 1}\searrow \quad \nearrow{\scriptstyle \exists!\ \iota} & \\ & \Omega_{A/R} \otimes_A A_X & \end{array}$$

- Similarly, since $A \to A_S \xrightarrow{d_{A_S/R}} \Omega_{A_S/R}$ is an element of $\mathrm{Der}_R(A, \Omega_{A_S/R})$ there is a unique morphism $\Omega_{A/R} \xrightarrow{\alpha} \Omega_{A_S/R}$ of A-modules such that the left of the below diagrams commutes. By the universal property of $\Omega_{A/R} \to (\Omega_{A/R})_S = \Omega_{A/R} \otimes_A A_S$ there is a unique ι such that the tight diagram commutes.

$$\begin{array}{ccc} A & \longrightarrow & A_S \\ {\scriptstyle d_{A/R}}\downarrow & & \downarrow{\scriptstyle d_{A_S/R}} \\ \Omega_{A/R} & \overset{\exists!\ \alpha}{\dashrightarrow} & \Omega_{A_S/R} \end{array} \qquad \begin{array}{ccc} \Omega_{A/R} & \xrightarrow{\alpha} & \Omega_{A_S/R} \\ & {\scriptstyle -\otimes_A 1}\searrow \quad \nearrow{\scriptstyle \exists!\ \iota} & \\ & \Omega_{A/R} \otimes_A A_S & \end{array}$$

To show that ι is an isomorphism in (c), it is sufficient to show that we have an isomorphism after applying $\mathrm{Hom}_{A_X}(-, T)$ to both sides for every A_X–module T. This is so because of this unfortunately unnamed fact applied to the sequence $0 \to \Omega_{A/R} \otimes_A A_X \xrightarrow{\iota} \Omega_{A_X/R_X} \to 0$ (which is exact iff ι is an isomorphism). But

$$\mathrm{Hom}_{A_X}(\Omega_{A_X/R_X}, T) \simeq \mathrm{Der}_{R_X}(A_X, T)$$

and

$$\mathrm{Hom}_{A_X}(\Omega_{A/R} \otimes_A A_X, T) \simeq \mathrm{Hom}_A(\Omega_{A/R}, T) \simeq \mathrm{Der}_R(A, T)$$

by various universal properties, hence (c) reduces to Fact 1a(c).

Part (d) works just the same. *q.e.d.*

An alternative construction of $\Omega_{A/R}$. Consider the map $A \otimes_R A \xrightarrow{m} A$, $a \otimes \alpha \mapsto a \cdot \alpha$. It turns out that this morphism of R-modules is a ring morphism. Let I denote its kernel. Let $\Omega_{A/R} = I/I^2$, turned into an A-module using $A \to A \otimes_R A$, $a \mapsto a \otimes 1$. Let $d\colon A \to \Omega_{A/R}$ be given by $a \to (a \otimes 1 - 1 \otimes a) \mod I^2$. It turns out that the Leibniz rule holds and that the universal property for R-linear derivatives of A is satisfied.

1.5. Kähler-differentials and regularity

Definition 1 (Locally free)**.** Let R be a ring, M an R-module. We say that M is **locally free** at $\mathfrak{p} \in \operatorname{Spec} R$ if there is $f \in R \setminus \mathfrak{p}$ such that M_f is a free R_f-module. When M_f is free of rank d we call M *locally free of rank d at $\mathfrak{p}$*. We simply call M a *locally free R-module (of rank d)* if it is locally free (of rank d) at every prime ideal.

Remark. (a) Since each prime ideal $\mathfrak{p}$ is contained in a maximal ideal, it is sufficient to require M being locally free at every maximal ideal in Definition 1.

(b) When $\operatorname{Spec} R$ is disconnected, there may be R-modules M which are locally free but not of a rank d for any fixed d. In this situation, there is a locally constant function d on $\operatorname{Spec} R$ such that M is locally free of rank $d(\mathfrak{p})$ at every $\mathfrak{p} \in \operatorname{Spec} R$.

Indeed, suppose that $f, g \in R \setminus \mathfrak{p}$ such that $M_f \simeq R_f^d$. Localizing the rest of $R \setminus \mathfrak{p}$ as well, we get

$$M_{\mathfrak{p}} = M_f \otimes_R R_{\mathfrak{p}} \simeq R_f^d \otimes_R R_{\mathfrak{p}} = (R_f \otimes_R R_{\mathfrak{p}})^d = R_{\mathfrak{p}}^d \,.$$

In particular, $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module and its rank obviously doesn't depend on f. Thus, in the above situation the rank function $d(\mathfrak{p})$ is well-defined. Moreover, our argument shows that it is constant on the open set $\operatorname{Spec} R \setminus V(f) \subseteq \operatorname{Spec} R$ for any f such that M_f is free over R_f, hence d is indeed locally constant.

(c) Probably this definition is not quite what you would expect from a *locally free* module and rather one would like to have an R-module M locally free if every localization $M_{\mathfrak{p}}$ at a prime ideal $\mathfrak{p}$ is free over $R_{\mathfrak{p}}$. For *finitely presented* modules M (in particular, every finitely generated module over a Noetherian ring) this is indeed equivalent. It even suffices to have the $M_{\mathfrak{m}}$ free over $R_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R. If you a brave enough to face The Stacks Project, a proof of this can be found in [Stacks, Tag 00NX]. If not, have a look at Corollary 1.

Proposition 1. *Let X be an affine algebraic variety. For a finitely generated $\mathcal{O}(X)$-module M, the following conditions are equivalent:*

(a) *For all $x \in X$, $\dim_k(M/\mathfrak{m}_x M) = n$ where $\mathfrak{m}_x \subseteq \mathcal{O}(X)$ is the maximal ideal of functions vanishing at x.*

(b) *M is locally free of rank n.*

Remark. The k-vector spaces appearing here (and also in Proposition 2) come from the fact that the residue field $\mathfrak{K}(\mathfrak{m}_x) = \mathcal{O}(X)/\mathfrak{m}_x$ is canonically isomorphic to k. However, the k-vector space structure (or actually $\mathfrak{K}(\mathfrak{m}_x)$-vector space structure) of $M/\mathfrak{m}_x M$ *does* depend on $\mathfrak{m}_x$, so keep that in mind when we write k for short instead of $\mathfrak{K}(\mathfrak{m}_x)$.

Lemma 1. *Let R be a ring, M a finitely generated R-module, $\mathfrak{p} \in \operatorname{Spec} R$. If $\mu_1, \dots, \mu_k \in M$ are such that their images in $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$ generate this $\mathfrak{K}(\mathfrak{p})$-vector space, then there is $f \in R \setminus \mathfrak{p}$ such that their images generate M_f as an R_f-module.*

Proof. Let $m_1, \dots, m_\ell$ be generators of M as an R-module. Their images in M_f generate M_f as an R_f-module for every f. Moreover, their images generate $M_\mathfrak{p}$. Since the images of μ_i generate $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ as a $\mathfrak{K}(\mathfrak{p})$-vector space, we have $M_\mathfrak{p} \subseteq \mathfrak{p}M_\mathfrak{p} + N$ where $N \subseteq M_\mathfrak{p}$ is the $R_\mathfrak{p}$-submodule generated by the image of the μ_i. By [NAK] we have $M_\mathfrak{p} = N$. In particular, the μ_i generate $M_\mathfrak{p}$ as an $R_\mathfrak{p}$-module, thus there are $\rho_{i,j} \in R_\mathfrak{p}$ such that $m_j = \sum_{i=1}^k \rho_{i,j}\mu_i$ holds in $M_\mathfrak{p}$. Taking a common denominator of the $\rho_{i,j}$, we find $f \in R \setminus \mathfrak{p}$ and $r_{i,j} \in R_f$ such that $m_j = \sum_{i=1}^k r_{i,j}\mu_i$ in M_f. Then the images of the μ_i generate M_f as an R_f-module. *q.e.d.*

The following wasn't treated in the lecture but we include it anyway (at the prize of post-poning the proof of Proposition 1) because we think it really helps understanding the notion of local freeness.

Corollary 1. *If R is Noetherian, M a finitely generated R-module and $\mathfrak{p} \in \operatorname{Spec} R$ a prime ideal such that $M_\mathfrak{p}$ is free over $R_\mathfrak{p}$, then there is an $f \in R \setminus \mathfrak{p}$ such that M_f is already free over R_f.*

Proof. Let $\mu_1, \dots, \mu_n \in M$ be such that their images generate $M_\mathfrak{p} \otimes_R \mathfrak{K}(\mathfrak{p})$. By Lemma 1, there is an $f \in R \setminus \mathfrak{p}$ such that their images generate M_f. We then obtain a surjective map $R_f^n \xrightarrow{\varphi} M_f$ and thus an exact sequence

$$0 \longrightarrow \ker\varphi \longrightarrow R_f^n \xrightarrow{\varphi} M_f \longrightarrow 0\ .$$

Localizing at $\mathfrak{p}$ turns φ into an isomorphism $R_\mathfrak{p}^n \xrightarrow{\sim} M_\mathfrak{p}$, hence $(\ker\varphi)_\mathfrak{p} = 0$ as localization is an exact functor. Then $0 = \ker\varphi \otimes_R \mathfrak{K}(\mathfrak{p})$ can be generated by zero elements, hence so can $(\ker\varphi)_g$ for some $g \in R \setminus \mathfrak{p}$ by Lemma 1. Then also $(\ker\varphi)_{fg} = (\ker\varphi)_g \otimes R_f = 0$ and localizing the above exact sequence at fg we obtain an isomorphism $R_{fg}^n \xrightarrow{\sim} M_{fg}$. *q.e.d.*

Proof of Proposition 1. We first prove that (b) implies (a). Let $R = \mathcal{O}(X)$, if (b) holds, then for any $\mathfrak{m}_x$ as in (a) there are $\mu_1, \dots, \mu_n \in M_f$, for some $f \in R \setminus \mathfrak{m}_x$ which freely generate M_f as an R_f-module. Then their images in $M/\mathfrak{m}_x M$ generate this as a k-vector space and from

$$k^n = (R/\mathfrak{m}_x R)^n = (R/\mathfrak{m}_x R)_f^n = (R_f/\mathfrak{m}_x R_f)^n \simeq M_f/\mathfrak{m}_x M_f = (M/\mathfrak{m}_x M)_f = M/\mathfrak{m}_x M$$

we conclude that the images of $\mu_1, \dots, \mu_n$ then indeed must form a basis. Here we used some well-known facts about the behaviour of quotients under localizations (cf. [1, Proposition 2.3.2(e)]) and $R/\mathfrak{m}_x R = (R/\mathfrak{m}_x R)_f$ and $(M/\mathfrak{m}_x M)_f = M/\mathfrak{m}_x M$ since f is already invertible in k.

Let (a) be satisfied, $\mathfrak{p} \in \operatorname{Spec} R$, $\mathfrak{m} = \mathfrak{m}_x$ any maximal ideal containing $\mathfrak{p}$. Applying (a) at x we obtain, $\mu_1, \dots, \mu_n \in M$ such that their images in $M/\mathfrak{m}_x M$ form a base of that k-vector space. By applying Lemma 1, there is $f \in R \setminus \mathfrak{m}_x \subseteq R \setminus \mathfrak{p}$ such that the μ_i generate M_f as an R_f module. We claim that they do so freely. Suppose that

$$0 = \sum_{i=1}^n r_i\mu_i \quad \text{in } M_f\ ,$$

where $r_i \in R_f$ not all zero. Multiplying by a suitable power of f we may assume $r_i \in R$ and

$$0 = \sum_{i=1}^n r_i\mu_i \quad \text{in } M\ .$$

Without losing generality let $r_1 \neq 0$. As X is irreducible, there is $y \in X \setminus (V(f) \cup V(r_1))$. Then the μ_i generate $M/\mathfrak{m}_y M$ because they generate M_f as an R_f-module and $f(y) \neq 0$. But we have

$$0 \equiv \sum_{i=1}^{n} r_i(y)\mu_i \mod \mathfrak{m}_y M$$

in $M/\mathfrak{m}_y M$ with the first coefficient $r_1(y) \neq 0$. Hence the images of $\mu_2, \ldots, \mu_n$ already generate $M/\mathfrak{m}_y M$, hence $\dim_k(M/\mathfrak{m}_y M) < n$, which is a contradiction to (a). *q.e.d.*

Remark. (a) A natural generalization of Proposition 1 would be

> If M is a finitely generated R-module and there is a natural number ℓ such that
>
> $$\dim_{\mathfrak{K}(\mathfrak{p})} ((M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}) = \dim_{\mathfrak{K}(\mathfrak{p})} (M \otimes_R \mathfrak{K}(\mathfrak{p})) = \ell \quad \text{for all } \mathfrak{p} \in \operatorname{Spec} R\,,$$
>
> then M is locally free of rank ℓ.

However, this is *wrong*! For example, if R is such that $\#\operatorname{Spec} R = 1$ but fails to be a field (e.g. $R = \mathbb{Z}/p^2\mathbb{Z}$ for p prime or $k[X]/(X^{2017})$), then there are modules which are finitely generated but not free (e.g. $R/\mathfrak{m}$ where $\mathfrak{m}$ is the only maximal ideal), hence not locally free (since $R \setminus \mathfrak{m} \subseteq R^\times$). But the function $\mathfrak{p} \mapsto \dim_{\mathfrak{K}(\mathfrak{p})}(M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p})$ has no choice but to be constant as $\#\operatorname{Spec} R = 1$.

However again, if R has no nilpotent elements, the generalization is true and the proof of Proposition 1 works. Instead of $y \in X \setminus (V(f) \cup V(r_1))$ in the last step of the above proof we now need to find a prime ideal $\mathfrak{q} \in \operatorname{Spec} R$ such that $r_1, f \in R \setminus \mathfrak{q}$ to arrive at the same contradiction. Equivalently, we need to assure that $r_1 f \in R \setminus \mathfrak{q}$. But $r_1 f \neq 0$ (as otherwise r_1 would be 0 in M_f) and the intersection of all prime ideals is the nilradical $\operatorname{nil}(R)$ which is (0) in our case, hence such a $\mathfrak{q}$ may be found.

(b) The closest analogue to Proposition 1 probably is

> If M is a finitely generated R-module and there is a natural number ℓ such that
>
> $$\dim_{\mathfrak{K}(\mathfrak{m})} (M/\mathfrak{m}M) = \dim_{\mathfrak{K}(\mathfrak{m})} (M \otimes_R \mathfrak{K}(\mathfrak{m})) = \ell \quad \text{for any maximal ideal } \mathfrak{m}\,,$$
>
> then M is a locally free R-module of rank ℓ.

but this fails unless R is, in addition to $\operatorname{nil}(R) = (0)$, a *Jacobson ring*: The maximal ideals of R form a dense subset of every closed subset of $\operatorname{Spec} R$. For instance, algebras of finite type over $\mathbb{Z}$ or any field or any principal ideal domain with infinitely many prime ideals may be taken (when $\operatorname{nil}(R) = (0)$), but not local rings which are not fields (as $M = R/\mathfrak{m}$ is a counterexample).

Proposition 2. *Let X be an affine algebraic variety of dimension $\dim(X) = n$ over the algebraically closed field k. Then the following conditions are equivalent:*

(a) *X is regular.*

(b) *$\Omega_{R/k}$ is a locally free module of rank n over $R = \mathcal{O}(X)$.*

Remark. (*a*) If $\Omega_{R/k}$ is locally free at $x \in X$ (i.e. it is locally free at $\mathfrak{m}_x$) then X is regular in some neighbourhood of x an in particular at x. This holds since, if $(\Omega_{R/k})_f$ is free and $f(x) \neq 0$,

- $\Omega_{R_f/k} \simeq (\Omega_{R/k})_f$ is a free R_f-module, hence so is any further localization.
- $X \setminus V(f)$ is an affine open neighbourhood of x and $\mathcal{O}(X \setminus V(f)) \simeq R_f$.

(*b*) It turns out (in Section 1.6) that $\Omega_{R/k}$ is locally free of rank $\dim(X)$ if it is locally free at all.

(*c*) When k is an arbitrary field, an R-algebra of finite type is called *smooth* if $\Omega_{R/k}$ is locally free of rank $\dim(R_\mathfrak{m})$ at every maximal ideal $\mathfrak{m}$. When k is perfect this is equivalent to the regularity of R.

Lemma 2. *When A/R is of finite type, $\Omega_{A/R}$ is a finitely generated A-module.*

Proof. Since A is of finite type, $A \simeq B/I$ with $B = R[X_1, \dots, X_n]$ and some ideal $I \subseteq B$. We have seen that $\Omega_{B/R} \simeq B^n$ is finitely generated. But the exact sequence

$$I/I^2 \longrightarrow \Omega_{B/R} \otimes_R A \longrightarrow \Omega_{A/R} \longrightarrow 0$$

from Corollary 1.4.1 expresses $\Omega_{A/R}$ as a quotient of $\Omega_{B/R} \otimes_R A \simeq A^n$ which is finitely generated over $B/I \simeq A$. Hence $\Omega_{A/R}$ is finitely generated over A. *q.e.d.*

Proof of Proposition 2. Let $x \in X$. Let X be realized as a closed irreducible subset $V(I) \subseteq k^m$, where I is a prime ideal in $S = k[X_1, \dots, X_m]$. Then $R \simeq S/I$ and by Corollary 1.4.1 we have a short exact sequence

$$I/I^2 \longrightarrow \Omega_{S/k} \otimes_k R \longrightarrow \Omega_{R/k} \longrightarrow 0,$$

where $\Omega_{S/k} \otimes_k R \simeq S^m \otimes_k R \simeq R^m$. Denote by $\mathfrak{m}_x \subseteq R$ the maximal ideals of functions vanishing at x. Taking tensor products over R with $\mathfrak{K}(\mathfrak{m}_x) \simeq k$ (as we pointed out before: although $\mathfrak{K}(\mathfrak{m}_x)$ is canonically isomorphic to k, the k-vector space structures involved do depend on $\mathfrak{m}_x$) gives a sequence

$$\begin{array}{ccccccc} I/I^2 \otimes_R k & \longrightarrow & R^m \otimes_R k & \longrightarrow & \Omega_{R/k} \otimes_R k & \longrightarrow & 0 \\ \downarrow \wr & & \downarrow \wr & & \| & & \\ I/(\mathfrak{m}_x I + I^2) & \longrightarrow & k^m & \longrightarrow & \Omega_{R/k} \otimes_R k & \longrightarrow & 0 \\ & & f \longmapsto \nabla f(x) & & & & \end{array}$$

which is exact since the functor $- \otimes_R M$ is *right-exact* for any R-module M (cf. Fact A.4.1). By Proposition 1 $\Omega_{R/k}$ being locally free is equivalent to $\dim_k(\Omega_{R/k}/\mathfrak{m}_x\Omega_{R/k}) = \dim_k(\Omega_{R/k} \otimes k) = n$ for all $x \in X$. By exactness of the above sequences of k-vector spaces, this is equivalent to the image of $I/I^2 \otimes_R k \to k^n$ having dimension $m - n$. But by the bottom row, this image is given by $\mathcal{N} = \{\nabla f(x) \mid f \in I\}$ and by the Jacobian criterion (Proposition 1.3.2), X is regular at $x \in X$ iff $\dim_k \mathcal{N} = m - n$, thus proving the assertion. *q.e.d.*

1.6. Kähler differentials for field extensions

In this section Professor Franke presented some nice-to-know results but without any proofs. However, we try our best to sketch most of the proofs.

Proposition 1. (*a*) *If L/k is a separable (algebraic) field extension, $\Omega_{L/k} = 0$.*

(*b*) *More generally, if L/k is separable in the sense that L is algebraic and separable over $K = k(x_1, \ldots, x_n)$ with $(x_1, \ldots, x_n)$ a transcendence basis of L/k, then*

$$\dim_L \Omega_{L/k} = \deg \operatorname{tr}(L/k)$$

and $dx_1, \ldots, dx_n$ form a basis of the L-vector space $\Omega_{L/k}$.

Remark. (*a*) If $K = k$, $L = K(X)$ (the field of rational functions, where X is an affine algebraic variety of dimension n over k) this implies that $\Omega_{K(X)/k} \simeq \Omega_{\mathcal{O}(X)/k} \otimes_{\mathcal{O}(X)} K(X)$ (note that Ω commutes with localization) has dimension $\deg \operatorname{tr}(K(X)/k) = \dim(X)$. Hence $\Omega_{\mathcal{O}(X)/k}$ must be locally free of rank $\dim(X)$ if it is locally free at all.

(*b*) In characteristic 0, the condition in Proposition 1(*b*) is automatically fulfilled.

(*c*) Finiteness of n actually isn't necessary.

Proof of Proposition 1. Part (*a*) appeared as problem 3 on sheet #5 and we consider it an easy exercise.

For part (*b*), recall that any K-valued derivation of K can be uniquely extended to an L-valued derivation of L (that was also part of the exercise) and Professor Franke immediately remarks, that this generalizes to V-valued K-derivations being uniquely extendible to $L \otimes_K V$-valued L-derivations (choose a basis, then every component of a derivation is again a derivation).

In particular, $K \xrightarrow{d_{K/k}} \Omega_{K/k}$ uniquely extends to a derivation $L \xrightarrow{\delta} \Omega_{K/k} \otimes_K L$ which is k-linear since $d_{K/k}$ already vanishes on k. By the universal property of $\Omega_{L/k}$, the derivation δ factors over a unique homomorphism $\Omega_{L/k} \to \Omega_{K/k} \otimes_K L$.

On the other hand, we have the canonical exact sequence

$$\Omega_{K/k} \otimes_K L \longrightarrow \Omega_{L/k} \longrightarrow \Omega_{L/K} \longrightarrow 0$$

in which $\Omega_{L/K} = 0$ by (*a*) and the left-most arrow is inverse to homomorphism $\Omega_{L/k} \to \Omega_{K/k} \otimes_K L$ we just constructed. By exercise 1 of sheet #6, $\Omega_{K/k}$ is the K-vector space freely generated by $dx_1, \ldots, dx_n$ and we're done. *q.e.d.*

Proposition 2. *Let L/k be a finitely generated field extension of char $p > 0$.*

(*a*) *$\Omega_{L/k} = 0$ iff L/k is algebraic separable.*

(*b*) *If $k^p = k$ (i.e. k is perfect) then $\dim_L \Omega_{L/k} = \deg \operatorname{tr}(L/k)$.*

Proof. Assertion (a) is not so trivial and we refer to [3, Proposition 5.6].

For (b), a result due to F.K. Schmidt says that every extension (algebraic or not) of a perfect field is separable. For finitely generated field extensions we use the notion of separability from Proposition 1. In general, *separable* means that every finitely generated subextension is separable. To prove Schmidt's result, consider a maximal separable subextension Z/k, then L/Z is algebraic and purely inseparable and we also may assume it is finite. Then $L^{p^e} \subseteq Z$ for some $e \in \mathbb{N}_0$, hence L^{p^e} is a separable extension of k. Now $k = k^{p^e}$ as k is perfect (i.e. the Frobenius is bijective), hence L/k is separable since L/k is isomorphic to L^{p^e}/k^{p^e} via the Frobenius. Also cf. [3, Proposition 5.18]. *q.e.d.*

Proposition 3. *If A is an algebra of finite type over a perfect field k and $\mathfrak{m} \in \mathfrak{m}\text{-Spec}\, A$ then the following conditions are equivalent:*

(a) *$A_\mathfrak{m}$ is regular, i.e. A is regular at $\mathfrak{m}$.*

(b) *$\Omega_{A/k}$ locally free at $\mathfrak{m}$.*

(c) *$\Omega_{A/k}$ is locally free of rank $\dim(A_\mathfrak{m})$ at $\mathfrak{m}$.*

We will be quite sketchy and only give a full prove in the case that A is a domain.

Lemma 1. *Let k be a field and R a Noetherian local k-algebra with maximal ideal $\mathfrak{m}$ such that the residue field $A/\mathfrak{m} = \mathfrak{K}(\mathfrak{m})$ is finitely generated and separable over k. Then the canonical homomorphism*

$$\mathfrak{m}/\mathfrak{m}^2 \longrightarrow \Omega_{R/k} \otimes_R \mathfrak{K}(\mathfrak{m})$$

is injective.

Proof. Replacing R by $R/\mathfrak{m}^2$ doesn't change $\mathfrak{m}/\mathfrak{m}^2$. Moreover, we have the exact sequence

$$0 \longrightarrow \mathfrak{m}^2/\mathfrak{m}^4 \longrightarrow \Omega_{R/k} \otimes_R R/\mathfrak{m}^2 \longrightarrow \Omega_{(R/\mathfrak{m}^2)/k} \longrightarrow 0\,,$$

which tensored by $\mathfrak{K}(\mathfrak{m})$ (tensoring is right-exact) becomes

$$0 \longrightarrow \mathfrak{m}^2/\mathfrak{m}^3 \longrightarrow \Omega_{R/k} \otimes_R \mathfrak{K}(\mathfrak{m}) \longrightarrow \Omega_{(R/\mathfrak{m}^2)/k} \otimes_R \mathfrak{K}(\mathfrak{m}) \longrightarrow 0\,.$$

The left-most arrow is obtained by applying $d_{R/k}$ to a representative $\mu \in \mathfrak{m}^2$ of $(\mu \mod \mathfrak{m}^3)$ and we know that $\mathfrak{m} \to \Omega_{R/k} \otimes_R \mathfrak{K}(\mathfrak{m})$ factors over $\mathfrak{m}^2$ (becoming the morphism we would like to show is surjective). Hence the left-most arrow is the 0-morphism, which proves $\Omega_{R/k} \otimes_R \mathfrak{K}(\mathfrak{m}) \simeq \Omega_{(R/\mathfrak{m}^2)/k} \otimes \mathfrak{K}(\mathfrak{m})$ and we may indeed replace R by $R/\mathfrak{m}^2$, thus assuming $\mathfrak{m}^2 = 0$.

Our strategy now is first to show that $\mathfrak{K}(\mathfrak{m})$ can be embedded into R leading to a (non-canonical) isomorphism $R \simeq \mathfrak{K}(\mathfrak{m}) \oplus \mathfrak{m}$. Using this, we will construct a left-inverse of the above map.

Let $\mathfrak{K}(\mathfrak{m}) = k(\xi_1, \ldots, \xi_r, \zeta)$ with $\xi_1, \ldots, \xi_r$ a transcendence base of $\mathfrak{K}(\mathfrak{m})/k$ and ζ separable over $k(\xi_1, \ldots, \xi_r)$ with minimal polynomial P. Let $x_i \in R$ be any lifts of the ξ_i. We need to find a lift z of ζ such that $P(z) = 0$. Let z be arbitrary at first. Surely, $P(z) \in \mathfrak{m}$ if $\delta \in \mathfrak{m}$, then

$$P(z + \delta) = P(z) + \delta P'(z)$$

since $\delta^2 \in \mathfrak{m}^2 = 0$. As ζ is separable, $P'(z)$ is not in $\mathfrak{m}$ and thus invertible in the local ring R. Therefore we can choose δ appropriately and replace z by $z + \delta$ such that $P(z) = 0$.

We thus have $R \simeq \mathfrak{K}(\mathfrak{m}) \oplus \mathfrak{m}$ (we just constructed a split of the exact sequence $0 \to \mathfrak{m} \to R \to \mathfrak{K}(\mathfrak{m}) \to 0$). We want to construct a homomorphism $\Omega_{R/k} \otimes_R \mathfrak{K}(\mathfrak{m}) \to \mathfrak{m}/\mathfrak{m}^2$ of $\mathfrak{K}(\mathfrak{m})$-vector spaces which is left-inverse to the to-be-injective map. Forgetting about left-inverseness at first, we may equivalently give a map $\Omega_{R/k} \to \mathfrak{m}/\mathfrak{m}^2$ of R-modules, that is, a derivation $R \xrightarrow{d} \mathfrak{m}/\mathfrak{m}^2$. Define d by $d(x + \mu) = \mu$ for $x \in \mathfrak{K}(\mathfrak{m})$, $\mu \in \mathfrak{m}$. It's a straightforward check that d fulfills the Leibniz rule and is left-inverse to $\mathfrak{m}/\mathfrak{m}^2 \to \Omega_{R/k} \otimes_R \mathfrak{K}(\mathfrak{m})$. We're done. *q.e.d.*

Let's see how this applies to our situation. Since A is Noetherian and of finite type, $\mathfrak{K}(\mathfrak{m})/k$ is a field extension of finite type, hence finite by the Nullstellensatz (cf. [1, Theorem 4]). Then $\mathfrak{K}(\mathfrak{m})$ must be separable, k being perfect. We thus obtain an exact sequence

$$0 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \Omega_{A_\mathfrak{m}/k} \otimes_A \mathfrak{K}(\mathfrak{m}) \longrightarrow \Omega_{\mathfrak{K}(\mathfrak{m})/k} \longrightarrow 0$$

(exactness on the left follows from the lemma we just showed, the rest is the first standard sequence from Corollary 1.4.1) in which $\Omega_{\mathfrak{K}(\mathfrak{m})/k} = 0$ as $\mathfrak{K}(\mathfrak{m})/k$ is algebraic and separable. Also note that $\Omega_{A_\mathfrak{m}/k} \otimes_A \mathfrak{K}(\mathfrak{m}) = (\Omega_{A/k})_\mathfrak{m} \otimes_A \mathfrak{K}(\mathfrak{m}) = \Omega_{A/k} \otimes_A \mathfrak{K}(\mathfrak{m})$. Then

$$\dim_{\mathfrak{K}(\mathfrak{m})} \left(\Omega_{A/k} \otimes_A \mathfrak{K}(\mathfrak{m})\right) = \dim_{\mathfrak{K}(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2 \geq \dim(A_\mathfrak{m}) = \dim(A)$$

and equality holds, by definition, iff A is regular at $\mathfrak{m}$.

To see local freeness in the case of A a domain, we need another tiny lemma.

Lemma 2. *Let R be a noetherian local domain with maximal ideal $\mathfrak{m}$, residue field $\mathfrak{K}(\mathfrak{m})$ and field of quotients K. Then a finitely generated R-module M is free iff*

$$\dim_{\mathfrak{K}(\mathfrak{m})} M \otimes_R \mathfrak{K}(\mathfrak{m}) = \dim_K M \otimes_R K \,.$$

Proof. If M is free, this is immediate. So let's assume the other direction. By [NAK], M can be generated by $d = \dim_{\mathfrak{K}(\mathfrak{m})} M \otimes_R \mathfrak{K}(\mathfrak{m})$ elements. Let thus $R^d \xrightarrow{\varphi} M$ be surjective, hence the sequence $0 \to \ker\varphi \to R^d \xrightarrow{\varphi} M \to 0$ is exact. Tensoring with K and $\mathfrak{K}(\mathfrak{m})$, we obtain exact sequences

$$0 \longrightarrow \ker\varphi \otimes_R K \longrightarrow K^d \longrightarrow M \otimes_R K \longrightarrow 0$$

and

$$0 \longrightarrow \ker\varphi \otimes_R \mathfrak{K}(\mathfrak{m}) \longrightarrow \mathfrak{K}(\mathfrak{m})^d \longrightarrow M \otimes_R \mathfrak{K}(\mathfrak{m}) \longrightarrow 0 \,.$$

Here we tricked the right-exactness of the tensor product in the following ways: Tensoring with K is exact because it is the same as localizing at $R \setminus \{0\}$. Then $\ker\varphi \otimes_R \mathfrak{K}(\mathfrak{m}) \to \mathfrak{K}(\mathfrak{m})^d$ is injective by a dimension count argument for which we need the hypothesis. Thus $\ker\varphi \otimes_R \mathfrak{K}(\mathfrak{m}) = 0$, hence $\ker\varphi = 0$ by [NAK]. *q.e.d.*

Proof of Proposition 3 if A is a domain. By Lemma 2, $\Omega_{A/k}$ is locally free at $\mathfrak{m}$ iff

$$\dim_{\mathfrak{K}(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2 = \dim_{\mathfrak{K}(\mathfrak{m})} \left(\Omega_{A/k} \otimes_A \mathfrak{K}(\mathfrak{m})\right) = \dim_K \left(\Omega_{A/k} \otimes_A K\right) \,.$$

But $\Omega_{A/k} \otimes_A K$ equals $\Omega_{K/k}$, which by Proposition 1 has dimension $\deg\mathrm{tr}(K/k)$ over K. But $\deg\mathrm{tr}(K/k) = \dim(A)$ by [1, Theorem 10] and we're done. *q.e.d.*

2. Projective spaces and graded rings

2.1. The projective space of a vector space

Definition 1 (Projective space)**.** Let V be a vector space over a field k, the **projective space** $\mathbb{P}(V)$ is the set of one-dimensional subspaces of V. Equivalently, $\mathbb{P}(V) = (V \setminus \{0\})/\sim$ where $x \sim y$ iff $x = \lambda y$ for some $\lambda \in k^\times$. Let $\mathbb{P}^n(k) \coloneqq \mathbb{P}(k^{n+1})$. In particular

$$\mathbb{P}^n(k) = \{[x_0, \dots, x_n] \mid x_i \in k, \text{ not all } x_i = 0\}$$

where $[x_0, \dots, x_n] = [y_0, \dots, y_n]$ iff there is $\lambda \in k^\times$ such that $x_i = \lambda y_i$ for $0 \le i \le n$. The tuple $(x_0, \dots, x_n)$ is called a *tuple of homogenous coordinates* for $[x_0, \dots, x_n]$.

Let $V(X_i) = \{[x_0, \dots, x_n] \mid x_i = 0\}$, or more generally $V(\ell) = \{[x] \mid x \in V \setminus \{0\}, \ell(x) = 0\} \subseteq \mathbb{P}(V)$ for some linear functional $\ell \colon V \to k$. We have $\mathbb{P}^n(k) = \bigcup_{i=0}^n (\mathbb{P}^n(k) \setminus V(X_i))$ and we have a bijection

$$\begin{aligned} V(X_i) &\xrightarrow{\sim} \mathbb{P}^{n-1}(k) \\ [x_0, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n] &\longmapsto [x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n] \end{aligned}$$

and

$$\begin{aligned} \mathbb{P}^n(k) \setminus V(X_0) &\xrightarrow{\sim} k^n = \mathbb{A}^n(k) \\ [1, y_1, \dots, y_n] &\longmapsto (y_1, \dots, y_n) \\ [x_0, \dots, x_n] &\longmapsto \left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right). \end{aligned}$$

In this sense, one can view $\mathbb{P}^n(k)$ as a compactification of $\mathbb{A}^n$.

For a more geometric description of this construction one can look at it as follows: Let $H \subseteq V$ be a hyperplane, $\widetilde{H} \subseteq V$ be an affine subspace parallel to H such that $0 \notin \widetilde{H}$. Then $\mathbb{P}(H) \subseteq \mathbb{P}(V)$ and $\mathbb{P}(V) \setminus \mathbb{P}(H) \to \widetilde{H}$, where we map a line ℓ to its intersection (a single point) with $\widetilde{H}$. This is a bijection (a central projection, the reason why it has been called *projective space*).

Elements of $\mathrm{GL}(V)$ operate onv $\mathbb{P}(V)$, with $g \in \mathrm{GL}(V)$ sending $\ell \in \mathbb{P}(V)$ to $g\ell = \{g(v) \mid v \in \ell\}$. On homogenous coordinates the action is given by matrix multiplication (where we treat $(x_0, \dots, x_n)$ as a column vector).

Example 1 (Riemann sphere)**.** Let $k = \mathbb{C}$, V a two-dimensional k-vector space, L a one-dimensional subspace, $W \supseteq L$ a real subspace of real dimension 3, S a sphere in W containing

0 and having L as the tangent plane there. Then

$$\begin{aligned}\mathbb{P}(V) &\longrightarrow S \\ \ell &\longmapsto \begin{cases} 0 & \text{if } \ell = L \\ \text{the non-zero element of } \ell \cap S & \text{otherwise} \end{cases} .\end{aligned}$$

The sphere S is the Riemann sphere of classical complex function theory.

2.2. Graded rings and homogenous ideals

To have an unambiguous definition of the vanishing set in $\mathbb{P}^n(k)$ of $P \in R = k[X_0, \ldots, X_n]$ (i.e. a definition of *vanishing* which does not depend on the choice of homogenous coordinates) one has to restrict to the case where P is homogenous of some degree $d \in \mathbb{N}$. This leads to

Definition 1 (Graded ring)**.** A ($\mathbb{N}$)-**graded ring** is a ring R with a decomposition $R = \bigoplus_{i=0}^{\infty} R_i$ of its additive group as a direct sum of subgroups R_i, such that $R_i \cdot R_j \subseteq R_{i+j}$. Every $r \in R$ thus has a unique decomposition $r = \sum_{i=0}^{\infty} r_i$ where $r_i \in R_i$ and only finitely many r_i are non-zero. The r_i are called the *homogenous components* of r. An element $r \in R$ is *homogenous* of degree n iff $r \in R_n$.

Example 1. For $\alpha, \beta \in \mathbb{N}^{n+1}$, let

$$\alpha + \beta = (\alpha_i + \beta_i)_{i=0}^{n} , \quad \alpha! = \prod_{i=0}^{n} \alpha_i! , \quad |\alpha| = \sum_{i=0}^{n} \alpha_i , \quad \text{and} \quad x^{\alpha} = \prod_{i=0}^{n} x_i^{\alpha_i} .$$

Let $R = k[X_0, \ldots, X_n]$, $R_k = \left\{ \sum_{|\alpha|=k} p_\alpha X^\alpha \;\middle|\; p_\alpha \in k \right\}$. Then R is a graded ring and the corresponding notion of *homogenous element* (i.e. *homogenous polynomial*) is the well-known one.

Remark. Sometimes $\mathbb{Z}$-graded rings are also considered. The definitions are unchanged unless indicated otherwise.

Definition 2 (Homogenous ideals)**.** Let R be a ($\mathbb{N}$-, $\mathbb{Z}$-) graded ring, $I \subseteq R$ and ideal. We say that I is **homogenous** if for every $f \in I$ the homogenous components f_i of f all belong to I.

Example 2. If R is a graded ring, the **augmentation ideal** is $R_+ = \bigoplus_{i=1}^{\infty} R_n$. In the case $R = k[X_0, \ldots, X_n]$ (graded as in Example 1) we have $R_+ = \{f \in R \mid f(0) = 0\}$.

For now on let k be an algebraically closed field.

Definition 3 (Projective vanishing set)**.** If $I \subseteq R = k[X_0, \ldots, X_n]$ is a homogenous ideal we put $V(I) = V_{\text{proj}}(I) = \{[x_0, \ldots, x_n] \mid f(x_0, \ldots, x_n) = 0 \text{ for all } f \in I\}$ as the **projective vanishing set** of I.

Remark 1. (*a*) In this section let $V(I) = V_{\text{proj}}(I)$ and $V_{\text{aff}}(U) \subseteq k^{n+1}$ denote affine vanishing set as studied before.

(*b*) As I is homogenous, for any given $x \in k^{n+1}$ then condition "$f(x) = 0$ for all $f \in I$" is equivalent to "$f(x) = 0$ for all homogenous $f \in I$" which is invariant under replacing x by λx for some $\lambda \in k^\times$. The condition to $[x_0, \ldots, x_n] \in \mathbb{P}^n(k)$ used in the above definition is therefore independent of the choice of homogenous coordinates and depends on the point $[x_0, \ldots, x_n]$ alone.

(*c*) We have, as in the affine case,

$$\begin{aligned} V\Big(\sum_{\lambda\in\Lambda} I_\lambda\Big) &= \bigcap_{\lambda\in\Lambda} V(I_\lambda) \\ V(I_1 \cdot I_2) &= V(I_1 \cap I_2) = V(I_1) \cup V(I_2) \\ V\left(\sqrt{I}\right) &= V(I)\ . \end{aligned} \tag{1}$$

Also, all the ideal constructions give homogeneous ideals provided that I, I_1, I_2 and the $(I_\lambda)_{\lambda\in\Lambda}$ are homogeneous (only for $\sqrt{I}$ this is not completely immediate).

Proposition 1. *For an $\mathbb{N}$-graded ring R the following conditions are equivalent:*

(*a*) *R is Noetherian.*

(*b*) *Any homogenous ideal of R is finitely generated.*

(*c*) *Any set $\mathfrak{M} \neq \emptyset$ of homogenous ideals in R has an $I \in \mathfrak{M}$ such that $I \not\subseteq J$ for $J \in \mathfrak{M}$ and $J \neq I$.*

(*d*) *Any ascending chain $I_0 \subseteq I_1 \subseteq \ldots$ of homogenous ideals in R becomes stationary for some $N \in \mathbb{N}$, i.e. $I_n = I_N$ for all $n \geq N$.*

(*e*) *R_0 is a Noetherian ring and R_+ is a finitely generated ideal in R.*

(*f*) *R_0 is a Noetherian ring and R is an R_0-algebra of finite type.*

Remark 2. Note that a homogenous ideal in R is finitely generated iff it can be generated by finitely many homogenous elements.

Proof of Proposition 1. The implication $(f) \Rightarrow (a)$ follows from Hilbert's Basissatz. That (a) implies (b) to (d) is trivial since these are special cases of the definitions of Noetherianness. We conclude (d) from (c) by applying (c) to $\mathfrak{M} = \{I_0, I_1, \ldots\}$. For the implication $(d) \Rightarrow (b)$ the proof for the ungraded case still applies, as the ideal generated by a set of homogenous elements of R is homogenous and for every inclusion $J \subsetneq I$ of ideals in R with homogenous I there is some homogenous $f \in I \setminus J$.

We obtain (e) from (b) since R_+ is a homogenous ideal in R and for any ideal I of R_0 the sum $I + R_+$ is a homogenous ideal of R and when $I + R_+$ is generated by $f_1, \ldots, f_d \in R_0$ and $f_{d+1}, \ldots, f_e$ (homogenous of positive degree) then I is generated by $f_{d+1}, \ldots, f_e$.

The implication $(e) \Rightarrow (f)$ can be seen as follows: Let R_+ be generated by homogenous elements $g_1, \ldots, g_d$ and let $S \subseteq R$ be the R_0-subalgebra generated by $g_1, \ldots, g_d$. Then any $f \in R$ belongs to S which can be proved by induction on the largest i for which the homogenous component f_i of f does not vanish. If this i is zero or non-existent then $f \in R_0$. Otherwise, let $f_i = \sum_{j=1}^d \lambda_j g_j$. We may assume that λ_j is homogenous of degree $i - \deg(g_j)$ as dropping the other homogenous

components only changes homogenous components of $\lambda_j g_j$ of degree not equal to i. By the induction assumption, $\lambda_j \in S$ and $f - f_i = f - \sum_{j=1}^{d} \lambda_j g_j \in S$. Since the g_j are in S, also $f \in S$. *q.e.d.*

Proposition 2. *Let I be any homogenous ideal of $R = k[X_0, \ldots, X_n]$ such that $\sqrt{I} \subsetneq R_+$. Then $V(I) \neq \emptyset$ and*

$$\sqrt{I} = \{f \in R \mid f(x_0, \ldots, x_n) = 0 \text{ when } (x_0, \ldots, x_n) \neq 0 \text{ and } [x_0, \ldots, x_n] \in V(I)\} \ . \tag{2}$$

Remark. (*a*) Another description of the right hand side of (2) is the ideal generated by all homogenous f such that $f(x_0, \ldots, x_n) = 0$ when $[x_0, \ldots, x_n] \in V(I)$. This is so because if $f = \sum_{i=0}^{\infty} f_i$ is an element of the right hand side of (2) and $[x_0, \ldots, x_n] \in V(I)$ then $\sum_{i=0}^{\infty} \lambda^i f_i(x_0, \ldots, x_n) = 0$ for all $\lambda \in k^\times$ as the condition of (2) may be applied to $(\lambda x_0, \ldots, \lambda x_n)$ Since there are infinitely many $\lambda \in k^\times$, all $f_i(x_0, \ldots, x_n) = 0$.

(*b*) The condition $\sqrt{I} \subsetneq R_+$ for homogenous ideals $I \subseteq R$ can also be expressed as $\dim_k(R/I) = \infty$.

Proof of Proposition 2. Recall that by the affine version of the Nullstellensatz

$$\sqrt{J} = \{f \in R \mid f(x) = 0 \text{ for all } x \in V_{\text{aff}}(J)\}$$

and $V(J) \neq \emptyset$ for $J \subsetneq R$. Since we assume $\sqrt{I} \subsetneq R_+ = \sqrt{R_+}$ this implies that there is $x \in V_{\text{aff}}(I) \setminus V_{\text{aff}}(R_+) = V_{\text{aff}}(I) \setminus \{0\}$. Let $x = (x_0, \ldots, x_n)$, then $[x_0, \ldots, x_n] \in V(I)$.

Moreover, let $f \in R$ be such that $f(x) = 0$ when $x \neq 0$ and $[x_0, \ldots, x_n] \in V(I)$. Then $f(x) = 0$ when $x \in V_{\text{aff}}(I) \setminus \{0\}$. For such x (which exist as $V(I) \neq 0$) and $\lambda \neq 0$ we have $f(\lambda x) = 0$. Since the Zariski closure of $k^\times \cdot x$ in k^{n+1} is $k \cdot x$, we also have $f(0) = 0$. It follows that $0 \in V_{\text{aff}}(f)$, hence $V_{\text{aff}}(f) \supseteq V_{\text{aff}}(I)$ and $f \in \sqrt{I}$ by the affine Nullstellensatz. *q.e.d.*

Remark. The only homogenous ideals $I \subseteq R$ such that $\sqrt{I} = I$ and $V(I) = \emptyset$ are $I = R_+$ and $I = R$. Also, any homogenous ideal of R equals R or is contained in R_+.

Definition 4 (Topology on $\mathbb{P}^n(k)$)**.** The Zariski topology of $\mathbb{P}^n(k)$ is the topology for which the closed sets of the form $V(I)$, for a homogenous ideal $I \subseteq R$.

Remark. By (1) and since $V(0) = \mathbb{P}^n(k)$ and $V(R) = V(R_+) = \emptyset$ this a topology, and the definition does not change when only ideals in R_+ are allowed.

Proposition 3. *There is a bijective correspondence between the closed subsets of $\mathbb{P}^n(k)$ and the homogeneous ideals $I = \sqrt{I} \subseteq R_+$ given by*

$$Z \mapsto \{I \in R_+ \mid f(x_0, \ldots, x_n) = 0 \text{ when } [x_0, \ldots, x_n] \in Z\}$$
$$I \mapsto Z = V(I).$$

This is an immediate consequence of Proposition 2.

Remark (Separation axioms for topological spaces)**.** Recall the following separation axioms for a topological space X:

- T_0: For all $x \neq y \in X$ we have $\overline{x} \neq \overline{y}$ (in other words, x has a neighbourhood not containing y or y has a neighbourhood not containing x) (occasionally attributed to Kolmogorov).
- T_1: For all $x \neq y \in X$, $y \notin \overline{x}$ (in other words, x has a neighbourhood not containing y; resp. $\{x\}$ is closed).
- T_2: Two points $x \neq y \in X$ have disjoint neighbourhoods (inother words, $\Delta \subseteq X \times X$ is closed) (the Hausdorff axiom).

Proposition 4. *$\mathbb{P}^n(k)$ is a Noetherian T_1-space. There is a bijection between the points of $\mathbb{P}^n(k)$ and the homogeneous ideals $I = \sqrt{I} \subsetneq R_+$ maximal with this property, obtained as a special case of Proposition 3 applied to closed subsets with precisely one point. Under the coorespondence of Proposition 3, the irreducible closed subsets correpond to the homogeneous prime ideals $\mathfrak{p} \neq R_+$.*

Proof. $\{\xi\} = \{[\xi_0, \ldots, \xi_n]\}$ is closed as it equals $\bigcap_{0 \leq i < j \leq n} V(\xi_i X_j - \xi_j X_i)$. The fact that $\mathbb{P}^n(k)$ is Noetherian follows from R from Proposition 3 as an infinite strictly decreasing chain of closed subsets becomes a strictly increasing chain of ideals in R. But R is Noetherian

The correspondence between points and ideals also follows from Proposition 3, and the last is checked as in the affine case. *q.e.d.*

Corollary. *$\mathbb{P}^n(k) = V(\{0\})$ is irreducible.*

Proposition 5. *The topology on $\mathbb{A}^n \simeq \mathbb{P}^n \setminus V(X_0)$ induced fro the Zariski topology on $\mathbb{P}^n(k)$ is the Zariski topology on k^n.*

Remark. The same, of course, holds for $\mathbb{P}^n \setminus V(X_j)$.

Proof of Proposition 5. Let $k^n \xrightarrow{i} \mathbb{P}^n(k)$, $i(x_1, \ldots, x_n) = [1, x_1, \ldots, x_n]$, be the inclusion to investigate. Since $i^{-1}(V(I)) = \{(x_1, \ldots, x_n) \mid f(1, x_1, \ldots, x_n) = 0 \text{ for all } f \in I\}$, it is continuous. To show that any closed $A \subseteq k^n$ can be represented as $i^{-1}(B)$ for some closed $B \subseteq k^{n+1}$, we first construct, for any $f \in S = k[X_1, \ldots, X_n]$, a homogeneous polynomial $\tilde{f} \in R$ such that $i^{-1}(V_{\text{proj}}(\tilde{f})) = V_{\text{aff}}(f)$. This can be done by putting

$$\tilde{f}(X_0, \ldots, X_n) = X_0^d f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right) \in R_d$$

where d is large enough. If $A = V_{\text{aff}}(I)$ and J denotes the ideal generated by the $\tilde{f}$, for all $f \in I$, then $B = V_{\text{proj}}(J)$ has the desired property. *q.e.d.*

Corollary 1.
- *The closed subsets of $\mathbb{P}^1(k)$ are $\mathbb{P}^1(k)$ and the finite subsets.*
- $\operatorname{codim}(x, \mathbb{P}^n(k)) = n$ *for any $x \in \mathbb{P}^n(k)$ (use the bijection between irreducible closed $B \subseteq \mathbb{P}^n(k)$ such that $B \cap \mathbb{A}^n \neq \emptyset$ and irreducible closed $A \subseteq k^n$, by $A = B \cap \mathbb{A}^n$, resp. B being the closure of A in $\mathbb{P}^n(k)$).*
- $\dim(\mathbb{P}^n) = n$.
- *$\mathbb{P}^n(k)$ is catenary (*$\operatorname{codim}(Y, Z) = \operatorname{codim}(Y \cap \mathbb{A}^n, Z \cap \mathbb{A}^n)$ *when $Y \cap \mathbb{A}^n \neq \emptyset$ by the argument used before, i.e. locality of codimension).*

Definition 5. The *affine cone* $C(Z)$ over a closed subset $Z \subseteq \mathbb{P}^n(k)$ is

$$C(Z) := \{0\} \cup \{(x_0, \dots, x_n) \neq (0, \dots, 0) \mid [x_0, \dots, x_n] \in Z\}.$$

Proposition 6. *$C(Z)$ is Zariski-closed in k^{n+1} and homogeneous in the sense that $\lambda z \in C(Z)$ for all $z \in C(Z)$ and $\lambda \in k$. One obtains a correspondence as follows:*

$$\begin{array}{ccc} (\textit{closed homogeneous non-empty } C \subseteq k^{n+1}) & \overset{\sim}{\longleftrightarrow} & (\textit{closed } Z \subseteq \mathbb{P}^n) \\ C = C(Z) & \longmapsto & Z \\ C & \longmapsto & Z = \{[x_0, \dots, x_n] \mid (x_0, \dots, x_n) \in C \setminus \{0\}\} \end{array}$$

Z is irreducible $\iff$ $C(Z)$ is irreducible and $\neq \{0\}$. Moreover, $\dim(C(Z)) = \dim(Z) + 1$ *and* $\operatorname{codim}(C(Y), C(Z)) = \operatorname{codim}(Y, Z)$ *when $Y \subseteq Z$ is irreducible.*

Proof. The assertions about the correspondences (everything except "Moreover") all follow from Propositions 3 and 4 and the correspondence

$$\begin{array}{ccc} (\text{ideals } I = \sqrt{I} \subseteq R) & \overset{\sim}{\longleftrightarrow} & (\text{closed } C \subseteq k^{n+1}) \\ I = \{f \mid f \equiv 0 \text{ on } C\} & \longmapsto & C \\ I & \longmapsto & C = V(I) \end{array}.$$

One must of course check that an ideal $I = \sqrt{I} \subseteq R$ is homogeneous iff $V(I)$ is homogeneous, but this is easy. (In particular, $C(Z)$ is irreducible as it equals $V_{\text{aff}}(\mathfrak{p})$ for some $\mathfrak{p} \in \operatorname{Spec} R$ with $Z = V_{\text{proj}}(\mathfrak{p})$).

We have $\dim(C(Z)) \geq \dim(Z) + 1$ because every chain $Z = Z_0 \supsetneqq Z_1 \supsetneqq \cdots \supsetneqq Z_d$ of irreducible subsets yields a chain

$$C(Z) = C(Z_0) \supsetneqq \cdots \supsetneqq C(Z_d) \supsetneqq \{0\}.$$

We have $\operatorname{codim}(C(Y), C(Z)) \geq \operatorname{codim}(Y, Z)$ by applying the cone construction of irreducibles between Y and Z. As $\mathbb{P}^n(k)$ is catenary of dimension n, we have $\dim(Z) + \operatorname{codim}(Z, \mathbb{P}^n) = n$, hence we obtain

$$n + 1 \leq \dim(C(Z)) + \operatorname{codim}(C(Z), C(\mathbb{P}^n)) = \dim(C(Z)) + \operatorname{codim}(C(Z), \mathbb{A}^{n+1}) = n + 1 \quad (*)$$

by affine dimension theory from Algebra 1, cf. [1]. If one of the inequalities $\dim(C(Z)) \geq \dim(Z) + 1$ or $\operatorname{codim}(Z, \mathbb{P}^n) \leq \operatorname{codim}(C(Z), C(\mathbb{P}^n))$ was strict, the above inequality $(*)$ would be strict, which is impossible. It follows that

$$\operatorname{codim}(Y, Z) = \dim(Y) - \dim(Z) = \dim(C(Y)) - \dim(C(Z)) = \operatorname{codim}(C(Y), C(Z)),$$

as both $\mathbb{P}^n$ and $\mathbb{A}^{n+1}$ are catenary. *q.e.d.*

Corollary 2. *Every irreducible subset of codimension 1 in $\mathbb{P}^n$ has the form $Z = V(P)$ where $P \neq 0$ is a homogeneous polynomial of positive degree.*

Proof. If Z is ireducible of codimension 1 in $\mathbb{P}^n$, then $C(Z)$ has codimension 1 in $\mathbb{A}^{n+1}$. Hence $C(Z) = V(P)$ for some prime element $P \in R = k[X_0, \dots, X_n]$, where P is uniquely determined up to multiplicative equivalence in R, i.e., up to $k^\times$ (existence was shown in Proposition 2.1.3 in [1], uniqueness up to multiplicative equivalence is rather clear). Since P and $P(\lambda \cdot)$, for any $\lambda \in K^\times$, have the same vanishing set, it follows that $P(z) = c_\lambda P(\lambda z)$ for any $\lambda \in k^\times$. But any such polynomial must be homogeneous (choose $\lambda \in k^\times \setminus \bigcup_{d \leq \deg P} \mu_d$, i.e. λ not a root of unity). *q.e.d.*

A. Appendix

A.1. Introduction to Krull dimension and all that

Professor Franke recapitulated on some topics of his previous lecture, Algebra I (of which detailed lecture notes may be found in [1]). Note that although the numbering of theorems in the following might seem messy, it is *intentionally* messy at least.

Definition 1 ([1, Definition 2.1.2])**.** A topological space X is called **quasi-compact** if every open cover $X = \bigcup_{\lambda\in\Lambda} U_\lambda$ admits a finite subcover.

X is **Noetherian** if it satisifies the following equivalent conditions:

(*a*) Every open subset is quasi-compact.

(*b*) There is no infinite properly descending chain of closed subsets.

(*c*) Every set of closed subsets of X has a $\subseteq$-minimal element.

Definition 2 ([1, Definition 2.1.3])**.** A topological space $X \neq \emptyset$ is **irreducible** if it satisifies the following equivalent conditions:

(*a*) If $X = X_1 \cup X_2$ where X_1 and X_2 are closed subsets, then $X = X_1$ or $X = X_2$. Also, $X \neq \emptyset$.

(*b*) Any two non-empty open subsets of X have non-empty intersection.

(*c*) Every non-empty open subset of X is dense.

Condition (a) implies, by induction, the following more general property: For any finite cover $X = \bigcup_{i=1}^n X_i$ by closed subsets, there is $1 \leq i \leq n$ such that $X = X_i$.

Proposition 1. (*a*) *Any subset of a Noetherian topological space is Noetherian with it's induced subspace topology* (cf. [1, Remark 2.2.1]).

(*b*) *If X is Noetherian, there is a unique (that is, up to permutation of the X_i) decomposition $X = \bigcup_{i=1}^n X_i$ into irreducible closed subsets $X_i \subseteq X$ such that $X_i \not\subseteq X_j$ for $i \neq j$* (cf. [1, Proposition 2.1.1]).

Definition 3 ([1, Definition 2.1.4])**.** Let X be a topological space, $Z \subseteq X$ irreducible and closed. We put

$$\operatorname{codim}(Z, X) = \sup\left\{ \ell \;\middle|\; \begin{array}{c}\text{there is a strictly ascending chain} \\ Z = Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_\ell \subseteq X \text{ of irreducible closed } Z_i \subseteq X\end{array} \right\}$$

$$\dim(X) = \sup\{\operatorname{codim}(Z, X) \mid Z \subseteq X \text{ irreducible and closed}\}$$

Example 1 ([1, Section 1.7 and 2.1])**.** Let $k = \overline{k}$ be an algebraically closed field. For an ideal $I \subseteq R = k[X_1, \ldots, X_n]$ let

$$V(I) = \{x \in k^n \mid f(x) = 0 \ \forall f \in I\}$$

be the set of zeroes of I. By the Hilbert Nullstellensatz, $V(I) \neq \emptyset$ when $I \subsetneq R$. Moreover

$$\begin{aligned} V(I) &= V\left(\sqrt{I}\right) \\ V(I \cdot J) &= V(I) \cup V(J) \\ V\Big(\sum_{\lambda \in \Lambda} I_\lambda\Big) &= \bigcap_{\lambda \in \Lambda} V(I_\lambda) \ . \end{aligned}$$

It follows that there is a topology (called the *Zariski topology*) on k^n containing precisely the subsets of the form $V(I)$ as closed subsets. A version of the Nullstellensatz ([1, Proposition 1.7.1]) says

$$\{f \in R \mid f(x) = 0 \ \forall f \in I\} = \{f \in R \mid V(f) \supseteq V(I)\} = \sqrt{I} \ .$$

This means that there is strictly antimonotonic bijective correspondence between the ideals I of R with $I = \sqrt{I}$ and the Zariski-closed subsets $A \subseteq k^n$ via

$$\begin{aligned} \Big\{\text{ideals } I \subseteq R \text{ such that } I = \sqrt{I}\Big\} &\xrightarrow{\sim} \{\text{Zariski-closed subsets } A \subseteq k^n\} \\ \{f \in R \mid V(f) \supseteq A\} &\longmapsfrom A \\ I &\longmapsto V(I) \ . \end{aligned}$$

(cf. [1, Remark 2.1.1]). As R is Noetherian, any strictly ascending chain of ideals in R terminates, implying that k^n is a Noetherian topological space. Under the above correspondence prime ideals correspond to irreducible subsets and vice versa (cf. [1, Proposition 2.1.2]).

Remark 1 ([1, Remark 2.1.3])**.** In general, for $A \subseteq B \subseteq C \subseteq X$

$$\operatorname{codim}(A, B) + \operatorname{codim}(B, C) \leq \operatorname{codim}(A, C) \tag{1}$$

$$\operatorname{codim}(A, X) + \dim(A) \leq \dim(X) \ . \tag{2}$$

may be strict. A Noetherian topological space is called *catenary* if (1) is an equality whenever A, B and C are irreducible.

Theorem A ([1, Theorem 5])**.** *The space $X = k^n$ is catenary and in this case equality always occurs in (2).*

Example 2. For $n = 1$, the closed subsets of k are k itself and the finite subsets. Since k is infinite, the points and k are the irreducible subsets, implying $\dim(k) = 1$ and the other assertions for $n = 1$.

Example 3. The irreducible subsets of k^2 are k^2 itself, single points, and $V(f)$ where $f \in k[X, Y]$ is a prime element.

Definition 4 (Transcendence degree)**.** Let $K \subseteq L$ be a field extension. A set $S \subseteq L$ is called *algebraically independent* over K if for all polynomials $P \in K[X_1, \dots, X_n]$ and pairwise different $s_1, \dots, s_n \in S$,

$$P(s_1, \dots, s_n) = 0 \quad \text{implies} \quad P = 0 \,.$$

A *transcendence basis* of L/K is a subset $S \subseteq L$ which is algebraically independent over K and such that $L/K(s_1, \dots, s_n)$ is algebraic. The **transcendence degree** $\deg \operatorname{tr} L/K$ of L/K is the cardinality of any transcendence basis.

Example. The empty set is a transcendence basis of K/K.

Definition 5 (regular functions, [1, Definition 2.2.2])**.** Let $X \subseteq k^n$ be closed, $U \subseteq X$ open. A function $f\colon U \to k$ is called *regular* at $x \in U$ if x has a neighbourhood $\Omega \subseteq k^n$ for which there are polynomials $p, q \in k[X_1, \dots, X_n]$ such that $V(q) \cap \Omega = \emptyset$ and

$$f(y) = \frac{p(y)}{q(y)} \quad \text{for all } y \in U \cap \Omega$$

The ring $\mathcal{O}(U)$ of **regular functions** on U consists of all functions $U \xrightarrow{f} k$ which are regular at every $x \in U$.

Proposition 2. *If $X \subseteq k^n$ is closed then $R = k[X_1, \dots, X_n] \to \mathcal{O}(X)$ is surjective.*

In [1, Proposition 2.2.2], we actually proved a stronger result: If $X \subseteq k^n$ is irreducible closed, i.e. $X = V(\mathfrak{p})$ for some prime ideal $\mathfrak{p} \subseteq R$, then $\mathcal{O}(X) \simeq R/\mathfrak{p}$. Proposition 2 immediately follows from this, as any closed subset decomposes into irreducible closed subsets according to Proposition 1 (it is crucial that each X_i occuring in such a contains a non-empty open subset of X, cf. [1, Proposition 2.1.1]).

Remark 2. When $X \subseteq k^n$ is an irreducible open-closed subset (that is, an open subset of an irreducible closed subset – a.k.a. a *quasi-affine variety*, cf. [1, Definition 2.2.1]) then $\mathcal{O}(X)$ is a domain.

Remark 3. Let T be any topological space, $A \subseteq T$ such that every $t \in T$ has an open neighbourhood $U \subseteq T$ such that $A \cap U$ is closed in U, then A is closed in T (we suspect that this is mentioned only because Professor Franke ~~mistook this class for Algebraic Geometry I~~ recently used this in Algebraic Geometry I). If the condition is required only for $t \in A$, then A is called *locally closed*.

If X is irreducible, let $K(X)$ be the quotient field of $\mathcal{O}(X)$. This is called the *field of rational functions* on X.

Theorem B ([1, Theorem 6])**.** *If $X \subseteq k^n$ is locally closed and irreducible, then*

$$\dim(X) = \deg \operatorname{tr}(K(X)/k) \,.$$

Moreover, X is catenary and equality always holds in (2), i.e. $\dim(Y) + \operatorname{codim}(Y, X) = \dim(X)$ whenever $Y \subseteq X$ is closed, irreducible.

One may check that locally closed sets are precisely the open subsets of closed sets. In particular, X from the above theorem is a quasi-affine variety, as we used to call it in Algebra I.

Remark 4. It is easy to see that $\dim k^n \geq n$ since we have the chain

$$\{0\}^n \subsetneq k \times \{0\}^{n-1} \subsetneq \ldots \subsetneq k^{n-1} \times \{0\} \subsetneq k^n$$

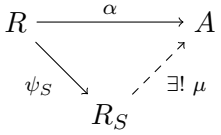
of irreducible closed subsets. To prove $\dim(k^n) \leq n$, and $\dim(X) \leq \deg \mathrm{tr}(K(X)/k)$, one proves $\deg \mathrm{tr}(\mathfrak{K}(\mathfrak{p})/k) > \deg \mathrm{tr}(\mathfrak{K}(\mathfrak{q})/k)$ whenever A/k is an algebra of finite type over k, $\mathfrak{q} \supsetneq \mathfrak{p}$ are prime ideals and $\mathfrak{K}(\mathfrak{p})$ denotes the quotient field of $A/\mathfrak{p}$.

For general affine X one uses the Noether Normalization theorem to get a finite morphism $X \xrightarrow{(f_1,\ldots,f_d)} \mathbb{A}^d(k) = k^d$ (i.e., $\mathcal{O}(X)$ is integral over $k[f_1, \ldots, f_d]$ and $f_1, \ldots, f_d$ are k-algebraically independent). One then uses the going-up (going-down) for (certain) integral ring extensions to lift chains of irreducible subsets of $\mathbb{A}^d(k) = k^d$ to chains of irreducible subsets of X (all of this may be found in much more detail in [1, Section 2.4-2.6]).

A.2. Localization of rings

Definition 1 (Multiplicative subsets)**.** Let R be any ring (commutative, with 1). A subset $S \subseteq R$ is called a **multiplicative subset** of R if it is closed under finite products (in particular $\prod_{s \in \emptyset} s = 1 \in S$).

Definition 2 (Localization of a ring)**.** A **localization** R_S of R with respect to S is a ring R_S with a ring morphism $R \xrightarrow{\psi_S} R_S$ such that $\psi_S(S) \subseteq R_S^\times$ (the group of units of R_S) and such that ψ_S has the universal property (on the left) for such ring morphisms:

> If $R \xrightarrow{\alpha} A$ is any ring morphism such that $\alpha(S) \subseteq A^\times$ then there is a unique ring morphism $R_S \xrightarrow{\mu} A$ such that the diagram
>
> 
>
>
> commutes.

It turns out (by a Yoneda-style argument) that this universal property characterizes R_S uniquely up to unique isomorphism. One constructs R_S (and thereby proves its existence) by $R_S = (R \times S)/_\sim$ where $(r, s) \sim (\rho, \sigma)$ iff there is $t \in S$ such that $t \cdot r \cdot \sigma = t \cdot \rho \cdot s$ (note that since R is not necessarily a domain the factor t on both sides cannot be omitted). One thinks of $(r, s)/_\sim$ as $\frac{r}{s}$ and introduces the ring operations in an obvious way.

If $I \subseteq R$ is any ideal then $I_S = I \cdot R_S = \left\{ \frac{i}{s} \;\middle|\; i \in I, s \in S \right\}$ is an ideal in R_S, and any ideal in R_S can be obtained in this way: $J = (J \sqcap R) \cdot R_S$ for any ideal $J \subseteq R_S$ where $J \sqcap R$ denotes

the preimage of J in R under ψ_S. It follows then R_S is Noetherian when R is. For prime ideals one obtains a bijection (cf. [1, Corollary 2.3.1(e)])

$$\begin{aligned} \operatorname{Spec} R_S &\xrightarrow{\sim} \{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \cap S = \emptyset\} \\ \mathfrak{p} &\longmapsto \mathfrak{p} \sqcap R \\ \mathfrak{q} \cdot R_S &\longmapsto \mathfrak{q} \ . \end{aligned}$$

We have an equivalence of categories between the category of R_S-modules and the category of R-modules M on which $M \xrightarrow{s\cdot} M$ acts bijectively for every $s \in S$. For every R-module M there is an R-module M_S belonging to the right hand side together with a morphism of R-modules $M \to M_S$, which has the universal property (on the left) for all morphisms from M to some R_S-module. It can be constructed as $\{\frac{m}{s} \mid m \in Ma, s \in S\}/_\sim$ with $\frac{m}{s} \sim \frac{\mu}{\sigma}$ iff $m \cdot \sigma \cdot t = \mu \cdot s \cdot t$ for some $t \in S$. $M = I$ is an ideal in R, one can take $M_S = I_S = I \cdot R_S$. As for rings, we call M_S the *localization* of M (cf. [1, Proposition 2.3.2]).

A.3. "Advanced" Galois theory: trace and norm

Let L/K be a finite field extension, $\overline{L}$ an algebraic closure of L. Let $x \in L$. There is a unique monic generator $\operatorname{Min}_{x/K}$ of the ideal $\{P \in K[T] \mid P(x) = 0\}$ in the principal ideal domain $K[T]$. Recall that

$$d = [K(x) : K] = \deg \operatorname{Min}_{x/K} =: \deg(x/K)$$

is called the *degree* and $\operatorname{Min}_{x/K}$ the *minimal polynomial* of x over K.

Definition 1 (Characteristic polynomial, trace and norm)**.** Let $x \in L$. Consider the corresponding endomorphism $L \xrightarrow{x\cdot(-)} L$ of the K-vector space L. Then the **characteristic polynomial** $P_{x,L}$, the **trace** $\operatorname{Tr}_{L/K}(x)$ and the **norm** $N_{L/K}(x)$ of x with respect to L/K are defined as the corresponding invariants of the endomorphism $x \cdot (-)$. In particular,

$$\begin{aligned} P_{x,L/K} &= \det(T \cdot \mathrm{id} - x) = T^n + \sum_{i=0}^{n-1} p_i T^i \ , \\ \operatorname{Tr}_{L/K}(x) &= -p_{n-1} \ , \quad \text{and} \quad N_{L/K}(x) = (-1)^n p_0 \ . \end{aligned}$$

Theorem C. *(a) If V is any finite dimensional L-vector space and $f \in \operatorname{End}_L(V)$, then*

$$\det_K(f) = N_{L/K}(\det_L(f)) \quad \textit{and} \quad \operatorname{Tr}_K(f) = \operatorname{Tr}_{L/K}(\operatorname{Tr}_L(f)) \ ,$$

where, for M a field, $\operatorname{Tr}_M(f)$ and $\det_M(f)$ are trace and determinant of the f regarded as an endomorphism of the M-vector space V.

(b) If M/L is a finite field extension and $x \in M$, then

$$\operatorname{Tr}_{M/K}(x) = \operatorname{Tr}_{L/K}(\operatorname{Tr}_{M/L}(x)) \quad \textit{and} \quad N_{M/K}(x) = N_{L/K}(N_{M/L}(x)) \ .$$

Let $x \in L$ and let $x = x_1, \ldots, x_e$ be the pairwise different images of x under the K-linear embeddings $L \hookrightarrow \overline{L}$. Also, let $d = \deg(x/K)$ and $n = [L : K]$ as before.

(c) *Suppose that* $e = 1$. *If* $\operatorname{char} K = 0$, *then* $x \in K$. *If* $\operatorname{char} K = p > 0$, *then* $x^{p^k} \in K$ *for some non-negative integer* k.

(d) *We have*

$$\operatorname{Min}_{x/K} = \prod_{i=1}^{e} (T - x_i)^{d/e} \quad \text{and} \quad P_{x,L/K} = \prod_{i=1}^{e} (T - x_i)^{n/e} = \prod_{\sigma} (T - \sigma(x))^{n/r}$$

where σ *runs over the different embeddings* $L \hookrightarrow \overline{L}$ *and* r *is their number.*

(e) *We have* $P_{x,L/K} = \operatorname{Min}_{x/K}^{[L:K(x)]}$. *More general, for any intermediate field* $K \subseteq E \subseteq L$ *we have* $P_{x,L/K} = P_{x,L/E}^{[L:E]}$ $\forall x \in E$.

Proof. Let's prove (e) first. Choose bases $(\ell_1, \ldots, \ell_k)$ of L/E and $(e_1, \ldots, e_m)$ of E/K and let M be the matrix representation of $E \xrightarrow{x\cdot} E$ in that basis. It is known from basic Galois theory that $(e_i m_j)_{i,j}$ form a basis of L/K. The matrix representation of $L \xrightarrow{x\cdot} L$ in that basis is a block diagonal matrix

$$\begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix}$$

with $k = [L : E]$ times the block M on the diagonal. This shows that $P_{x,L/K} = P_{x,E/K}^k$ as stated. If $E = K(x)$ then $P_{x,E/K} = \operatorname{Min}_{x/K}$ since x is a zero of the left hand side by Cayley-Hamiltion and $\deg P_{x,E/K} = [E : K] = [K(x) : K] = \deg(x/K) = \deg \operatorname{Min}_{x/K}$ and both polynomials are normed. This shows (e).

Now we prove part (a). Let $\mathcal{C} = (\ell_1, \ldots, \ell_k)$ is a basis of L/K and $\mathcal{B} = (v_1, \ldots, v_m)$ a basis of V as an L-vector space. Denote by $\operatorname{Mat}_{\mathcal{B}}(f) = (f_{i,j})_{i,j=1}^m$ the matrix representing f in basis $\mathcal{B}$. Then $\widetilde{\mathcal{B}} = (\ell_i v_j)_{i,j}$ is a basis of V as a K-vector space and

$$\operatorname{Mat}_{\widetilde{\mathcal{B}}}(f) = \begin{pmatrix} \operatorname{Mat}_{\mathcal{C}}(f_{1,1}) & \cdots & \operatorname{Mat}_{\mathcal{C}}(f_{1,m}) \\ \vdots & \ddots & \vdots \\ \operatorname{Mat}_{\mathcal{C}}(f_{m,1}) & \cdots & \operatorname{Mat}_{\mathcal{C}}(f_{m,m}) \end{pmatrix}.$$

Since the trace of a matrix is the sum of its diagonal elements, the assertion about traces follows. The assertion about determinants would be immediate too by

$$\begin{aligned} \det_K(f) = \det \operatorname{Mat}_{\widetilde{\mathcal{B}}}(f) &= \prod_{i=1}^{m} \det \operatorname{Mat}_{\mathcal{C}}(f_{i,i}) = \prod_{i=1}^{m} N_{L/K}(f_{i,i}) = N_{L/K}\Big(\prod_{i=1}^{m} f_{i,i}\Big) \\ &= N_{L/K} \det_L(f) \end{aligned}$$

if $f_{i,j} = 0$ for all $i > j$, as in that case, $\operatorname{Mat}_{\mathcal{B}}(f)$ and hence also $\operatorname{Mat}_{\widetilde{\mathcal{B}}}(f)$ are upper triangular (block) matrices . But that's no problem since we can always choose $\mathcal{B}$ in such a way that $\operatorname{Mat}_{\mathcal{B}}(f)$ is upper triangular. Part (b) is just the special case $V = M$, so we proved (a) and (b).

Let's prove the first assertion of (d). If $\operatorname{char} K = 0$, then $\operatorname{Min}_{x/K}$ is separable. Thus, $d = e$ and $\operatorname{Min}_{x/K} = (T - x_1) \cdots (T - x_e)$ since the zeros of $\operatorname{Min}_{x/K}$ are precisely the possible images of x under the K-linear embeddings $L \hookrightarrow \overline{L}$.

Now let $\operatorname{char} K = p > 0$. There is a separable polynomial $\mu \in K[T]$ and a non-negative integer k such that $\operatorname{Min}_{x/K} = \mu(T^{p^k})$. Indeed, if $\operatorname{Min}_{x/K}$ is irreducible but not separable, then its derivative must be the zero polynomial, hence each monomial of $\operatorname{Min}_{x/K}$ is a power of T^p and $\operatorname{Min}_{x/K} = \mu_1(T^p)$ for some polynomial $\mu \in K[T]$. Iterating this argument, we finally arrive at a separable polynomial μ (note that in each step the degree strictly decreases).

Let $y_1, \ldots, y_{e'}$ be the zeros of μ in $\overline{L}$. Then $0 = \operatorname{Min}_{x/K}(x_i) = \mu(x_i^{p^k})$, hence $x_i^{p^k}$ must be some of the y_j for each $i \leq e$. Note that $x_i^{p^k} - x_j^{p^k} = (x_i - x_j)^{p^k} \neq 0$ for $i \neq j$, hence $x_1^{p^k}, \ldots, x_e^{p^k}$ are pairwise different. On the other hand, $\overline{L}$ being algebraically closed, each y_i has a $p^k{}^{\text{th}}$ root $\eta \in \overline{L}$. Then $\operatorname{Min}_{x/K}(\eta) = \mu(y_i) = 0$ and η must be among the x_i. Summarizing, we get $e = e'$ and $x_1^{p^k}, \ldots, x_e^{p^k}$ are $y_1, \ldots, y_e$ in some order. Since μ factorizes into linear factors,

$$\operatorname{Min}_{x/K} = \mu\left(T^{p^k}\right) = \prod_{i=1}^{e}\left(T^{p^k} - y_i\right) = \prod_{i=1}^{e}\left(T^{p^k} - x_i^{p^k}\right) = \prod_{i=1}^{e}(T - x_i)^{p^k}$$

and comparison of degrees yields $p^k = \frac{d}{e}$. This shows the first assertion of (d). The second one immediately follows from this and (e). For the third one, let $\psi_1, \ldots, \psi_e$ be the different K-linear embeddings $K(x) \hookrightarrow \overline{L}$, $\psi_i(x) = x_i$. It is easy to see, that each of the ψ_i has the same number b of extensions to a K-linear embedding $\sigma\colon L \hookrightarrow \overline{L}$. Then by the previous step the left hand side is

$$\prod_{i=1}^{e}(T - x_i)^{n/e} = \prod_{\sigma}\left(T - \sigma(x)\right)^{n/(be)} = \prod_{\sigma}\left(T - \sigma(x)\right)^{n/r}.$$

Last thing we have to do is part (c). If $\operatorname{char} K = 0$, then $\operatorname{Min}_{x/K}$ is separable and thus $\operatorname{Min}_{x/K} = T - x$ as $e = 1$. Then $x \in K$. By (d), in characteristic $p > 0$, there is a non-negative integer k such that $\operatorname{Min}_{x/K} = (T - x)^{p^k} = T^{p^k} - x^{p^k}$, hence $x^{p^k} \in K$. *q.e.d.*

A.4. Construction and basic properties of tensor products of modules over a ring

Definition 1. Let M and N be modules over the (commutative) ring R. Let $\operatorname{Bil}_R(M, N; T)$ be the R-module of R-bilinear maps $f\colon M \times N \to T$. A **tensor product** $M \otimes_R N$ is an R-module together with an R-bilinear map

$$\begin{aligned} M \times N &\longrightarrow M \otimes_R N \\ (m, n) &\longmapsto m \otimes_R n = m \otimes n \end{aligned}$$

which has the *universal property* for R-bilinear maps $M \times N \xrightarrow{\tau} T$:

> If τ is any such map, there is a unique $t \in \operatorname{Hom}_R(M \otimes_R N, T)$ such that the following diagram commutes.

$$\begin{array}{ccc} M \times N & \xrightarrow{\quad\tau\quad} & T \\ & {\scriptstyle -\otimes -}\searrow \quad \nearrow{\scriptstyle t} & \\ & M \otimes_R N & \end{array}$$

Remark 1. (*a*) It is easy to see that this characteristizes $M \otimes_R N$ uniquely up to unique isomorphism.

(*b*) $M \otimes_R N$ is generated as an R-module by $\{m \otimes n \mid m \in M, n \in N\}$. To see this, let T be the quotient of $M \otimes_R N$ by the submodule generated by elements of this form, and consider $\tau = 0$. Then both $t_1 = 0$, and t_2 the projection $M \otimes_R N \twoheadrightarrow T$ would make the above diagram commute, which forces $0 = t_1 = t_2$, hence the quotient is 0.

Thus, a morphism $M \otimes_R N \xrightarrow{f} X$ of R-modules is uniquely determined by giving $f(m \otimes n)$ for $m \in M$, $n \in N$. Existence is guaranteed by the universal property, provided that the expression given for $f(m \otimes n)$ is bilinear in m and n.

Proposition 1. *$M \otimes_R N$ exists.*

Proof. $M \otimes_R N$ can be constructed by F/K and $m \otimes n$ by the image of $\delta_{(m,n)}$ in F/K. Here $F = \bigoplus_{(m,n) \in M \times N} R$ is the free R-module generated by $M \times N$ and K the submodule generated by elements of the form

$$\begin{aligned} \delta_{(m+m',n)} - \delta_{(m,n)} - \delta_{(m',n)} \ , \quad \delta_{(m,n+n')} - \delta_{(m,n)} - \delta_{(m,n')} \ , \\ \delta_{(rm,n)} - r\delta_{(m,n)} \ , \quad \delta_{(m,rn)} - r\delta_{(m,n)} \ . \end{aligned}$$

It's easy to check that this works. *q.e.d.*

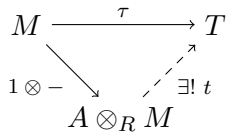
A.4.1. Use of the tensor product to basis-change a module

Let R be a ring, A an R-algebra, M an R-module. Then $A \otimes_R M$ has a unique structure of an A-module such that

$$\alpha \cdot (a \otimes m) = (\alpha \cdot a) \otimes m.$$

In fact, the right hand side is R-bilinear in a and m, showing the existence. There is a unique morphism $\alpha \cdot (-) = \mu_\alpha \colon A \otimes_R M \to A \otimes_R M$ such that $\mu_\alpha(a \otimes m) = (\alpha \cdot a) \otimes m$ for all $a \in A$, $m \in M$. We have $\mu_{\alpha+\alpha'} = \mu_\alpha + \mu_{\alpha'}$. Also, $\mu_\alpha = \rho \cdot (-)$ (in the R-module structure) when α is the image of $\rho \in R$ in A. In particular, $\mu_1 = \mathrm{id}_{A \otimes_R M}$. It follows that we have obtained an A-module-structure on $A \otimes_R M$.

We have a homomorphism $M \to A \otimes_R M$ sending m to $1 \otimes m$. This is a morphism of R-modules by the R-bilinearity of $- \otimes -$. Let T be any A-module and $\tau \in \mathrm{Hom}_R(M, T)$, then there is a unique homomorphism $t \colon A \otimes_R M \to T$ of R-modules such that $t(a \otimes m) = a\tau(m)$, i.e.



commutes. Also, t is A-linear:

$$\alpha \cdot t(a \otimes m) = \alpha \cdot (a \cdot \tau(m)) = t((\alpha \cdot a) \otimes m) = t(\alpha \cdot (a \otimes m)) \ .$$

As the $a \otimes m$ generate $A \otimes M$ as an R-module this implies A-linearity of τ. Also, if t makes the above diagram commutative and is A-linear then t is R-linear and $t(a \otimes m) = a \cdot t(1 \otimes m) = a \otimes \tau(m)$ hence t is uniquely determined.

It can be shown that

$$\begin{aligned}(M \otimes_R A) \otimes_A (A \otimes_R N) &\xrightarrow{\sim} (M \otimes_R N) \otimes_R A \\ (m \otimes a) \otimes (1 \otimes n) = (m \otimes 1) \otimes (a \otimes n) &\longmapsto (m \otimes n) \otimes a \\ (m \otimes a') \otimes (a'' \otimes n) &\longmapsto (m \otimes n) \otimes (a' \cdot a'').\end{aligned}$$

Furthermore, we have

$$\begin{aligned}(M \oplus N) \otimes_R A &\xrightarrow{\sim} (M \otimes_R A) \oplus (N \otimes_R A) \\ (m, n) \otimes a &\longmapsto (m \otimes a, n \otimes a)\end{aligned}$$

and

$$\operatorname{coker}\left(M \otimes_R A \xrightarrow{\mu \otimes \mathrm{id}_A} N \otimes_R A\right) \xrightarrow{\sim} \operatorname{coker}\left(M \xrightarrow{\mu} N\right) \otimes_R A\,.$$

In the case where $R = k$ is a field, we also have

$$\ker\left(M \otimes_k A \xrightarrow{\mu \otimes \mathrm{id}_A} N \otimes_k A\right) \xrightarrow{\sim} \ker\left(M \xrightarrow{\mu} N\right) \otimes_k A\,,$$

but this does not hold in general. The last two isomorphisms are just a non-abstract nonsense way of stating the following

Fact 1. If N is any R-module (not necessarily an R-algebra), then $- \otimes_R N \colon R\text{-mod} \to R\text{-mod}$ is a *right-exact* functor (i.e. if $M' \to M \to M'' \to 0$ is an exact sequence of R-modules, then so is $M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$) but it need not be *exact*. Those R-modules N for which it is exact are called **flat**.

The above assertion about cokernels is an immediate consequence. Moreover, when $R = k$ is a field, then an k-module N is a k-vector space, hence free, hence *projective* and thus flat (by some standard facts from commutative algebra), proving that in this case the above assertion about kernels holds.

Also, note that if $A = R/I$ where $I \subseteq R$ is some ideal, then

$$\begin{aligned}M \otimes_R A &\xrightarrow{\sim} M/(I \cdot M) \\ m \otimes (r \mod I) &\longmapsto (r \cdot m) \mod (I \cdot M).\end{aligned}$$

In the case where B is another R-algebra, $A \otimes_R B$ has a unique ring structure such that $(a \otimes b) \cdot (\alpha \otimes \beta) = (a \cdot \alpha) \otimes (b \cdot \beta)$. The construction is done by steps: First construct multiplication maps $\mu_{\alpha,\beta} \colon A \otimes_R B \to A \otimes_R B$ such that $\mu_{\alpha,\beta}(a \otimes b) = (a \cdot \alpha) \otimes (b \cdot \beta)$. Then show

$$\begin{aligned}\mu_{\alpha+\alpha',\beta} &= \mu_{\alpha,\beta} + \mu_{\alpha',\beta} \\ \mu_{\alpha,\beta+\beta'} &= \mu_{\alpha,\beta} + \mu_{\alpha,\beta'} \\ r \cdot \mu_{\alpha,\beta} &= \mu_{r\cdot\alpha,\beta} = \mu_{\alpha,r\cdot\beta}\end{aligned}$$

using the analogous properties of $(a \cdot \alpha) \otimes (b \cdot \beta)$ and the uniqueness part of the universal property to get $\mu_{\alpha,\beta}$. Once this is done, $\mu_{\alpha,\beta}(c)$ is R-bilinear in α and β, for fixed $c \in A \otimes_R B$. Then it follows that there is a unique map

$$\begin{aligned} \mu \colon (A \otimes_R B) \times (A \otimes_R B) &\longrightarrow A \otimes_R B \\ (\alpha \otimes \beta, c) &\longmapsto \mu_{\alpha,\beta}(c) \end{aligned}$$

and we can say $c \cdot d = \mu(c, d)$ for $c, d \in A \otimes_R B$.

There are morphisms $A \to A \otimes_R B$, $a \mapsto a \otimes 1$ and $B \to A \otimes_R B$, $b \mapsto 1 \otimes b$ of R-algebras and the universal property

$$\begin{aligned} \mathrm{Hom}_{R\text{-Alg}}(A, T) &\simeq \mathrm{Hom}_{B\text{-Alg}}(A \otimes_R B, T) \\ \mathrm{Hom}_{R\text{-Alg}}(B, S) &\simeq \mathrm{Hom}_{A\text{-Alg}}(A \otimes_R B, S) \end{aligned}$$

hold for any A-algebra S and any B-algebra T.

Bibliography

[1] Nicholas Schwab; Ferdinand Wagner. *Algebra I by Jens Franke (lecture notes)*. GitHub: https://github.com/Nicholas42/AlgebraFranke/tree/master/AlgebraI.

[2] H. Matsumura and M. Reid. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1989. ISBN: 978-0-521-36764-6. URL: http://www.math.unam.mx/javier/Matsumura.pdf.

[Stacks] The Stacks Project Authors. *The Stacks Project*.

[3] E. Kunz. *Kähler Differentials*. Advanced Lectures in Mathematics. Vieweg+Teubner Verlag, 1986. ISBN: 978-3-528-08973-3. URL: http://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/kunz/kaehler/paragraph1.pdf.