Algebra II

Lecturer: Jens Franke
Notes: 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 [Alg_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 $\dim(X) = \text{tr.deg}(K(X)/k)$, 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* [MR89]

- 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* [Alg_1].

as well. **Warning!** Somewhere in the middle of the last-mentioned text, the term *irreducible* is redefined as irreducible *and closed* when referring to subsets of a topological space. So don't let yourself get confused. Also, this lecture is intended by Professor Franke to be a continuation of Algebra I and that's why our theorem numbering will start with 11 on the next page.

1. Krull's principal ideal theorem

1.1. Formulation

Theorem 11 (Krull's principal ideal theorem)**.** *Let R be a noetherian ring, $f \in R$, $\mathfrak{p} \in \operatorname{Spec} R$ minimal among all prime ideals containing f. Then* $\operatorname{ht}(\mathfrak{p}) \leqslant 1$.

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. [Alg$_1$, 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. [Alg$_1$, 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. [Alg$_1$, Corollary 2.2.2]) that there is a bijection

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

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 [Alg$_1$, 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. [Alg$_1$, 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 $\mathfrak{p}_i \subseteq \mathcal{O}(X)$ 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) [Alg$_1$, Proposition 2.1.1]). Hence, each $\mathfrak{p}_i$ is a minimal prime ideal containing f. By ($*$) and the principal ideal theorem, $\operatorname{codim}(C_i, X) = \operatorname{ht}(\mathfrak{p}_i) \leqslant 1$. But $\operatorname{codim}(C_i, X) > 0$ as X is irreducible and $f \neq 0$. □

Remark. Actually, the minimal prime ideals containg f are precisely the $\mathfrak{p}_i$. We have seen that the $\mathfrak{p}_i$ are minimal. Conversely, 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 [Alg$_1$, Proposition 2.1.1], hence $\mathfrak{q}$ is among the the $\mathfrak{p}_i$.

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 $\widetilde{X} = X \setminus V(\lambda)$, which is affine again by Remark 1(c). 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 must have $k \geqslant 1$, otherwise g is a unit and $\mathfrak{q} = R$ would be no prime ideal. As $\mathfrak{q}$ is prime, one of the q_i must be contained in $\mathfrak{q}$, say, $q_1 \in \mathfrak{q}$. Hence $q_1 \in \mathfrak{q} \subseteq (p)$ and p and q_1 must differ only by a unit as $p \mid q_1$ and they are both primes. Then also $p \in (q_1) \subseteq \mathfrak{q}$, 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. [Alg$_1$, 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 $B \cong k[X_1, \ldots, X_n]$, 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 $\operatorname{ht}(\mathfrak{p}) \leqslant \operatorname{ht}(\mathfrak{q})$ holds by the *going-up theorem* (cf. [Alg$_1$, Theorem 7] or [Alg$_1$, Fact 2.6.2] for this particular result), hence $\operatorname{codim}(V(f), X) \leqslant 1$. 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 $q \in \sqrt{(f_0)}$. □

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* $\operatorname{ht}(\mathfrak{p}) \leqslant r$.

We'll eventually prove Theorem 11 and 12 in Section 3.4 (page 66) using Hilbert polynomial arguments. The following corollary can be derived in the same way as Corollary 1 from Theorem 11, but again we also give a standalone proof.

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

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.

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

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 $i \leqslant N$ such that $Z \subseteq Y_i$ (cf. [Alg$_1$, 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 $1 \leqslant i \leqslant N$ 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. [Alg$_1$, 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 $\operatorname{codim}(Z, Y_i) \leqslant r - 1$. As X is catenary, we have

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

as claimed. □

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 ([Alg$_1$, 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 [Alg$_1$, 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

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

(here $X \times Y \xrightarrow{p_X} X$ means the projection onto the X-coordinate) 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 $\operatorname{codim}(X \times Y, k^{m+n}) \geqslant a + b$.

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 $\dim(X \times Y) \geqslant d + e$.

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

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

showing that the inequalities of the previous two steps are actually equalities. □

Theorem 13 ([Alg$_1$, 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*

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

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

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

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

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

and hence

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

proving the assertion. □

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*

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

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. □

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 1 to R/I. The assertion about prime ideals is left as an exercise (and you should have done this on exercise sheet #2!). □

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 $\mathfrak{m}$ of R. Since $r \in \mathfrak{m}$ and $1 = 1 + xr - xr \in \mathfrak{m}$, we get 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 $-x \bmod \mathfrak{m}$ be inverse to $r \bmod \mathfrak{m}$ (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. □

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 [MR89]). Making a compromise, it will, from now on, be cited as [NAK].

Proposition 3 (Nakayama's lemma)**.** *Let R be 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 a vector of 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 $\rho = (\rho_{i,j})$ is the matrix formed by the $\rho_{i,j}$. But $\det(\mathrm{id}_k - \rho) \equiv 1 \bmod \operatorname{rad}(R)$ 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 Cramer's rule, $\mathrm{id}_k - \rho$ has an inverse matrix. Therefore $(\mathrm{id}_k - \rho) \cdot m = 0$ implies $m = 0$ and thus $M = 0$. □

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*

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

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.

Now 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, $\operatorname{ht}(\mathfrak{m}) \leqslant n$. Thus,

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

finishing the proof. □

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

(*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 $(\mathfrak{p}R_\mathfrak{p})/(\mathfrak{p}R_\mathfrak{p})^2 \cong (\mathfrak{p}/\mathfrak{p}^2)_\mathfrak{p}$ and $R_\mathfrak{p}$ is regular (or R is *regular at* $\mathfrak{p}$) iff $\mathfrak{p}/\mathfrak{p}^2$ has dimension $\operatorname{ht}(\mathfrak{p})$ as a $\mathfrak{K}(\mathfrak{p})$-vector space. In particular, R is regular at $\mathfrak{m} \in \mathfrak{m}\text{-Spec}\, R$ iff $\dim(R_\mathfrak{m}) = \operatorname{ht}(\mathfrak{m})$ 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 $R_\mathfrak{p} \cong (R_\mathfrak{m})_\mathfrak{p}$ 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*) If k is algebraically closed, $R = k[X_1, \dots, X_n]$ 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 $\mathfrak{m} = (X_1 - x_1, \dots, X_n - x_n)_R$, hence may be generated by n elements. But $\mathrm{ht}(\mathfrak{m}) = n$ by [Alg$_1$, Theorem 10] from Algebra I.

This result holds in more generality for arbitrary fields k, as we have seen on exercise sheet #4.

(*b*) $X = k^n$ is regular at all of its points, since $\mathcal{O}_{X,x} \cong R_{\mathfrak{m}}$ if $x \in X$ corresponds to the maximal ideal $\mathfrak{m} \subseteq R$ ([Alg$_1$, 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 $I \subseteq R = k[X_1, \dots, X_n]$ be the ideal of functions vanishing on X. Then X is regular at $x \in X$ iff*

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

Proof. Since $\dim(\overline{X}) = \dim(X)$ and $\mathcal{O}_{\overline{X},x} = \mathcal{O}_{X,x}$, we may replace X by its closure $\overline{X} = V(I)$ 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 R is regular at x. Therefore,

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

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

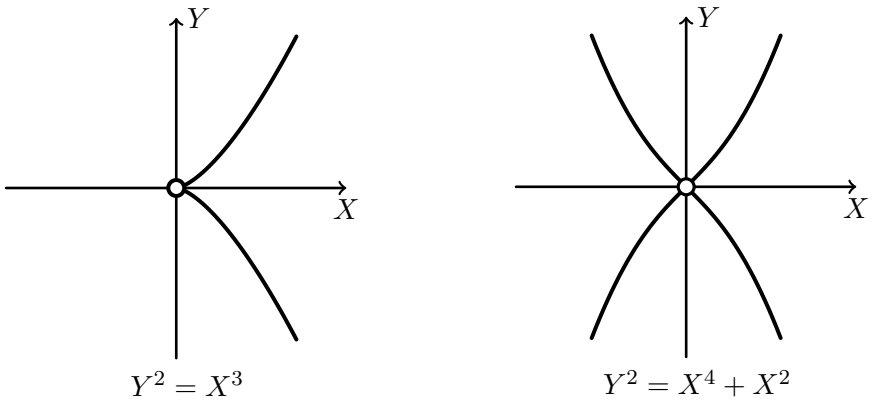
Denote by $\mathfrak{n} \subseteq \mathcal{O}(X) = R/I$ the ideal of regular functions on X vanishing at x. Then $\mathfrak{n} = \mathfrak{m}/I$. We have $\mathcal{O}_{X,x} \cong \mathcal{O}(X)_{\mathfrak{n}}$, hence X is regular at x iff $\dim_k(\mathfrak{n}/\mathfrak{n}^2) = \dim(X)$. As $\mathfrak{n}/\mathfrak{n}^2 \cong \mathfrak{m}/(I + \mathfrak{m}^2)$, 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

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

This shows the assertion. □

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. Consider the prime ideals $\mathfrak{p} = (X^2 - X^3)$ and $\mathfrak{q} = (Y^2 - X^4 - X^2)$ in $k[X, Y]$, where k may be assumed to be an algebraically closed field of characteristic 0 or greater than 3. The affine varieties $V(\mathfrak{p})$ and $V(\mathfrak{q})$ in k^2 have *singular points* precisely in the origin, as depicted in the following figures.



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

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

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

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

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

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*

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

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 dimension 2 and (thus) codimension 1 in X. But $Y \cap Z = \{0\}$ has codimension 3 in X and the inequality from Theorem 15 fails, due to the failure of regularity of X at 0.

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

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

(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 ([Alg$_1$, 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 Corollary 1.1.2 together with *locality of codimension* yields

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

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 topologies on k^{2n} and $X \times X$ are *not* the products 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,

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

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 [Alg$_1$, Concluding remarks, Lemma 1(c)]).

Step 2. Let $R = k[X_1, \dots, X_m]$ 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 $X_1, \dots, X_m$, $\mathfrak{m}^2$ is generated by the $X_i X_j$ (with i, j not necessarily distinct). Similarly, $\mathfrak{p}$ is the ideal generated by $X_{\ell+1}, \dots, X_m$. 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 $\mathfrak{m}^2 \cap \mathfrak{p} \subseteq \mathfrak{m} \cdot \mathfrak{p}$. This can be reduced to the previous step by an affine automorphism of k^m.

Step 4. Let $x \in k^n$, $\mathfrak{m}_x \subseteq S = k[X_1, \dots, X_n]$ the maximal ideal defined by x, $f_1, \dots, f_n \in S$ such that their images generate $\mathfrak{m}_x/\mathfrak{m}_x^2$. Then there is $h \in R = k[X_1, \dots, X_n, Y_1, \dots Y_n]$ such that $h(x, x) \neq 0$ and $h \cdot \mathfrak{d} \subseteq (g_1, \dots, g_n)_R$ where $g_i(y, z) = f_i(y) - f_i(z)$ and $\mathfrak{d} \subseteq R$ is the prime ideal of functions vanishing on $\Delta = \{(y, y) \mid y \in k^n\}$. To see this, let $\xi = (x, x)$ and $\mathfrak{q} = \mathfrak{d} \cdot R_{\mathfrak{m}_\xi}$, 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 $f \in \mathfrak{d}$. We claim that there are $c_1, \dots, c_n$ 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 $\mathfrak{d} \subseteq (g_1, \dots, g_n)_R + (\mathfrak{d} \cap \mathfrak{m}_\xi^2) = (g_1, \dots, g_n)_R + \mathfrak{d} \cdot \mathfrak{m}_\xi$ (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 $\mathfrak{d}$. Since $\mathfrak{q} = \mathfrak{d} \cdot R_{\mathfrak{m}_\xi}$ 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 $h \cdot \mathfrak{d} \subseteq (g_1, \dots, g_n)_R$.

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 basis 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 basis 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.

We're finally done. □

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 $\sigma it = \sigma js$. Then $\rho = \frac{\sigma it}{\sigma st} = \frac{\sigma js}{\sigma st} \in (I\cap J)\cdot R_S$. □

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 equivalent 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. □

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

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

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

The ∂s occurring here are of course formal derivatives in $R[X_1, \ldots, X_n]$ and for the products $\frac{\partial P}{\partial X_i} \cdot m_i$ we use the usual multiplication in the $R[X_1, \ldots, X_n]$-module M. 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

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

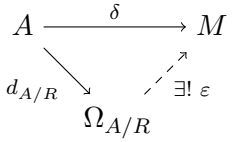
is a morphism of A-modules and similar for $\mathrm{Der}_R(A, M)$ and $\mathrm{Der}_R(A, N)$.

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
>
> 
>
>
> commutes. In other words, $\mathrm{Der}_R(A, M) \cong \mathrm{Hom}_A(\Omega_{A/R}, M)$ is a natural bijection – or in category theory language, $\Omega_{A/R}$ together with $d_{A/R}$ *represents* the functor $\mathrm{Der}_R(A, -)$ from the category of A-modules to the category of sets.

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

Remark. (*a*) By the usual argument, the universal property characterizes $\Omega_{A/R}$ up to unique isomorphism (if it exists).

(*b*) For $A = R[X_1, \ldots, X_n]$, $\Omega_{A/R} = \bigoplus_{i=1}^{n} A \cdot dX_i \cong A^n$ 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. For $x \in M$ 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,

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

In other words, the functor $\mathbf{Set} \to \mathbf{Mod}(A)$ from the category of sets to the category of A-modules mapping X to the free A-module generated by X is *left-adjoint* to the forgetful functor from the category of A-modules to **Set**, the category of sets.

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

- $c(\delta_a + \delta_b - \delta_{a+b}) = c(\delta_a) + c(\delta_b) - c(\delta_{a+b}) = d(a) + d(b) - d(a+b) = 0$ 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. □

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

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 $\delta \mapsto \varphi = \big(i \bmod I^2 \mapsto \delta(i)\big)$.

(*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 prove (*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 $\alpha = a \bmod I \in A/I$ and $i \in I$, then $\varphi(\alpha \cdot (i \bmod I^2)) = \delta(a \cdot i) = i \cdot \delta(a) + a \cdot \delta(i) = \alpha \cdot \delta(i)$ 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: $\varphi(i \bmod I^2) = \delta(i) = d(\pi(i)) = d(0) = 0$. Finally, let δ be such that $\varphi = 0$. For $i \in I$, $\delta(i) = \varphi(i \bmod I^2) = 0$. 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. □

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.*

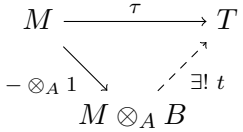
(*a*) *If $I \subseteq A$ is any ideal, we have a canonical short exact sequence of (A/I)-modules*

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

(*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 occurring 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:

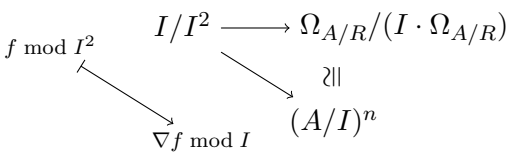
> If T is any B-module and $M \xrightarrow{\tau} T$ any A-linear homomorphism, then there is a unique homomorphism of B-modules $M \otimes_A B \xrightarrow{t} T$ such that
>
> 
>
>
> commutes, i.e. $\tau(m) = t(m \otimes_A 1)$. In particular, there is an isomorphism $\mathrm{Hom}_A(M, T) \cong \mathrm{Hom}_B(M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

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

has the desired universal property. More about tensor products may be found in the appendix, section A.4.

(*b*) Using (3) and the calculation of $\Omega_{R[T_1,\ldots,T_n]/R}$ in Example 1 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

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

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

- We put

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

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 the unnamed fact from page 19, 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

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

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. □

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 $d(a) = 0$ 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. □

As we did with Fact 1 and Corollary 1, results about the module of derivatives can be directly translated into results about Kähler differentials by Hom-ing them appropriately.

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.

(*c*) 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.

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

(*d*) 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 right 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 the unfortunately unnamed fact from page 19 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

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

and

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

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

Part (*d*) works just the same. □

Remark. There is an alternative construction of $\Omega_{A/R}$ and it is given as follows: Consider the multiplication map $A \otimes_R A \xrightarrow{m} A$, $a \otimes b \mapsto a \cdot b$. 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 $a \mapsto (a \otimes 1 - 1 \otimes a) \bmod I^2$. 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 $f \in R \setminus \mathfrak{p}$ such that $M_f \cong R_f^d$. Localizing the rest of $R \setminus \mathfrak{p}$ as well, we get

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

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 are 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 over the algebraically closed field k. 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 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. □

The following wasn't treated in the lecture but we include it anyway (at the price of postponing 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 and $\ker\varphi$ is finitely generated as R is noetherian, hence $(\ker\varphi)_g$ can be generated by zero elements as well 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 $R_{fg}^n \xrightarrow{\sim} M_{fg}$. □

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

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

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. [Alg$_1$, 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

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

with coefficients $r_i \in R_f$ 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

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

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). □

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 $f(x) \neq 0$,

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

(*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, $A \cong B/I$ with $B = R[X_1, \ldots, X_n]$ and some ideal $I \subseteq B$. We have seen that $\Omega_{B/R} \cong B^n$ 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 $\Omega_{B/R} \otimes_R A \cong A^n$ which is finitely generated over $B/I \cong A$. Hence $\Omega_{A/R}$ is finitely generated over A. □

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 $S = k[X_1, \ldots, X_m]$. Then $R \cong S/I$ 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 $\Omega_{S/k} \otimes_k R \cong S^m \otimes_k R \cong R^m$. Denote by $\mathfrak{m}_x \subseteq R$ the maximal ideals of functions vanishing at x. Taking tensor products over R with $\mathfrak{K}(\mathfrak{m}_x) \cong k$ (as we pointed out before: although $\mathfrak{K}(\mathfrak{m}_x)$ is 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. □

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.

It should be mentioned, though, that an exhaustive, self-contained, and very readable treatment of Kähler differentials can be found in Eisenbud, [Eis95, Chapter 16]. A more general version of the Jacobi criterion (cf. Proposition 1.3.2) may also be found there – we recommend having a look at this.

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*

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

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 $\Omega_{K(X)/k} \cong \Omega_{\mathcal{O}(X)/k} \otimes_{\mathcal{O}(X)} K(X)$ (note that Ω commutes with localization) has dimension $\mathrm{tr.deg}(K(X)/k) = \dim(X)$. 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. □

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

Proof. Assertion (a) is not so trivial and we refer to Eisenbud, [Eis95, Corollary 16.17], or [Kun86, 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. Together with Proposition 1(b) this implies the assertion.

For finitely generated field extensions Schmidt uses 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. [Kun86, Proposition 5.18]. □

Proposition 3. *If A is an algebra of finite type over a perfect field k and $\mathfrak{p} \in \operatorname{Spec} A$ then $A_\mathfrak{p}$ is a regular local ring iff $\Omega_{A/k}$ is locally free of rank $\dim(A_\mathfrak{p}) + \operatorname{tr.deg}(\mathfrak{K}(\mathfrak{p})/k)$ at $\mathfrak{p}$. If A is reduced or $\operatorname{char} k = 0$, we only need that $\Omega_{A/k}$ is locally free at $\mathfrak{p}$.*

Remark. Note that Proposition 3 is not quite what it was in the lecture. Franke formulated the result only for maximal ideals of A (but it holds for every prime ideal) and didn't mention the additional conditions in the case where $\Omega_{A/k}$ is only locally free at $\mathfrak{p}$ but we do not yet know its rank. However, Eisenbud, cf. [Eis95, Corollary 16.22], and The Stacks Project, cf. [Stacks, Tag 00TX], believe this is necessary, and when it comes down to facts Franke casually mentions without proving them because they are "perhaps worthwhile to know" I trust them more than I trust him.

Proof of Proposition 3. We start with the following lemma, which together with its proof is taken from [Stacks, Tag 00TU].

Lemma 1. *Let k be a field and R a noetherian local k-algebra with maximal ideal $\mathfrak{m}$ such that the residue field $R/\mathfrak{m} = \mathfrak{K}(\mathfrak{m})$ 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

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

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

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

The left-most arrow is obtained by applying $d_{R/k}$ to a representative $\mu \in \mathfrak{m}^2$ of ($\mu \bmod \mathfrak{m}^3$) 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 injective). Hence the left-most arrow is the 0-morphism, which proves $\Omega_{R/k} \otimes_R \mathfrak{K}(\mathfrak{m}) \cong \Omega_{(R/\mathfrak{m}^2)/k} \otimes \mathfrak{K}(\mathfrak{m})$ 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 $R \cong \mathfrak{K}(\mathfrak{m}) \oplus \mathfrak{m}$. 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 $R \cong \mathfrak{K}(\mathfrak{m}) \oplus \mathfrak{m}$ (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. □

Let's see how this applies to our situation. Since A is noetherian and of finite type, $\mathfrak{K}(\mathfrak{p})/k$ is a field extension of finite type, hence finite by the Nullstellensatz (cf. [Alg$_1$, Theorem 4]). Then $\mathfrak{K}(\mathfrak{p})$ must be separable over k since k is perfect. We thus obtain an exact sequence

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

(exactness on the left follows from Lemma 1, the rest is the first standard sequence from Corollary 1.4.1) in which $\dim_{\mathfrak{K}(\mathfrak{p})} \Omega_{\mathfrak{K}(\mathfrak{p})/k} = \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k)$ by Proposition 2(b) as k is perfect and so $\mathfrak{K}(\mathfrak{p})/k$ is separable. Also note that $\Omega_{A_\mathfrak{p}/k} \otimes_A \mathfrak{K}(\mathfrak{p}) = (\Omega_{A/k})_\mathfrak{p} \otimes_A \mathfrak{K}(\mathfrak{p}) = \Omega_{A/k} \otimes_A \mathfrak{K}(\mathfrak{p})$. Then we deduce

$$\dim_{\mathfrak{K}(\mathfrak{p})} \left(\Omega_{A/k} \otimes_A \mathfrak{K}(\mathfrak{p})\right) = \dim_{\mathfrak{K}(\mathfrak{p})} \mathfrak{p}/\mathfrak{p}^2 + \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k) \geqslant \dim(A_\mathfrak{p}) + \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k) \quad (*)$$

in which equality holds, by definition, iff A is regular at $\mathfrak{p}$. In particular, we see that $\Omega_{A/k}$ being locally free at $\mathfrak{p}$ of rank $\dim(A_\mathfrak{p}) + \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k)$ implies that $A_\mathfrak{p}$ is regular.

Conversely, suppose that $A_\mathfrak{p}$ is regular. Then we may assume that A is a domain. Indeed, let $\mathfrak{q}$ be a minimal prime ideal of A contained in $\mathfrak{p}$. Then $\mathfrak{q}$ has height 0, hence so has $\mathfrak{q}A_\mathfrak{p} \in \operatorname{Spec} A_\mathfrak{p}$. But every regular local ring is a domain by Corollary 3.4.9(b), hence $\mathfrak{q}A_\mathfrak{p} = 0$.

Then $A_\mathfrak{p} \cong A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p} \cong (A/\mathfrak{q})_\mathfrak{p}$ and we may replace A by $A/\mathfrak{q}$. This is also compatible with the assertion we want to prove, that is, $(\Omega_{A/k})_\mathfrak{p} \cong \Omega_{A_\mathfrak{p}/k}$ being free, since the left-hand side doesn't change when A is replaced by $A/\mathfrak{q}$ (as we have just shown).

To see local freeness of $\Omega_{A/k}$ at $\mathfrak{p}$ 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 we obtain an exact sequence

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

Since tensoring with K is the same as localization at $R\setminus\{0\}$ (and localization is exact), we were able to trick the right-exactness of the tensor product on the left end of the above sequence. Since $\dim_K K^d = d = \dim_K M \otimes_R K$ we obtain $\ker\varphi \otimes_R K = 0$. Hence $\ker\varphi = 0$ as R^d is torsion-free. □

Note that $A_\mathfrak{p}$ and A have the same field of quotients K. By Lemma 2, what we need to check for $\Omega_{A/k}$ being locally free at $\mathfrak{p}$ is

$$\dim_{\mathfrak{K}(\mathfrak{p})} \mathfrak{p}/\mathfrak{p}^2 + \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k) \overset{(*)}{=} \dim_{\mathfrak{K}(\mathfrak{p})} \Big(\Omega_{A/k} \otimes_A \mathfrak{K}(\mathfrak{p})\Big) = \dim_K \Big(\Omega_{A/k} \otimes_A K\Big) \ . \qquad (\#)$$

Now $\Omega_{A/k} \otimes_A K$ equals $\Omega_{K/k}$ (tensoring with K is localization at $A \setminus \{0\}$), which by Proposition 1(b) has dimension $\mathrm{tr.deg}(K/k)$ over K. But $\mathrm{tr.deg}(K/k) - \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k) = \mathrm{ht}(\mathfrak{p}) = \dim(A_\mathfrak{p})$ by [Alg$_1$, Theorem 10] and we're done.

Now assume that $\Omega_{A/k}$ is locally free at $\mathfrak{p}$ and A is reduced or $\mathrm{char}\, k = 0$. We will show that the rank of $\Omega_{A/k}$ at $\mathfrak{p}$ is necessarily equal to $\dim(A_\mathfrak{p}) + \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k)$. To do this, let $\mathfrak{q}$ be a minimal prime of A which is contained in $\mathfrak{p}$ and such that $\mathfrak{q}A_\mathfrak{p}$ is part of a maximal ascending chain of prime ideals in $A_\mathfrak{p}$ (i.e., to find $\mathfrak{q}$ we choose such a maximal chain in $A_\mathfrak{p}$ and take the preimage of the smallest prime ideal in that chain). Then $\dim(A_\mathfrak{p}) = \dim(A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p})$ and our goal is to reduce everything to $A/\mathfrak{q}$. This is done in two steps.

Step 1. We first show that $\mathfrak{q}/\mathfrak{q}^2 = 0$. To do so, we'll give an argument that works both when A is reduced and when $\mathrm{char}\, k = 0$ – but for different reasons, so we start with some case work.

Case 1. If A is reduced, so is the localization $A_\mathfrak{q}$. Hence from $\dim(A_\mathfrak{q}) = \mathrm{ht}(\mathfrak{q}) = 0$ we deduce that $A_\mathfrak{q}$ is a field. Then $A_\mathfrak{q} \cong A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q}$ can be no other than the quotient field $\mathfrak{K}(\mathfrak{q})$ of $A/\mathfrak{q}$ and we have $\dim_{\mathfrak{K}(\mathfrak{q})} \Omega_{\mathfrak{K}(\mathfrak{q})/k} = \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{q})/k)$ by Proposition 2(b).

Case 2. Now suppose that $\mathrm{char}\, k = 0$ and let $x \in \mathfrak{q}A_\mathfrak{q}$. Since $\mathfrak{q}A_\mathfrak{q}$ is the only prime ideal of $A_\mathfrak{q}$, every element $x \in \mathfrak{q}A_\mathfrak{q}$ is nilpotent by Proposition 1.2.1. Choose n such that $x^n = 0$ but $x^{n-1} \neq 0$. Denoting $d_{A_\mathfrak{q}/k}$ the derivation associated to $\Omega_{A_\mathfrak{q}/k}$, we have $0 = d_{A_\mathfrak{q}/k}x^n = nx^{n-1}d_{A_\mathfrak{q}/k}x$ by the Leibniz rule. Since k has characteristic 0, n is invertible in k and thus also in the k-algebra

$A_\mathfrak{q}$. Hence $x^{n-1} d_{A_\mathfrak{q}/k} x = 0$. Also $\Omega_{A_\mathfrak{q}/k} = (\Omega_{A_\mathfrak{p}/k})_{\mathfrak{q}A_\mathfrak{p}}$ is a free $A_\mathfrak{q}$-module since $\Omega_{A_\mathfrak{p}/k}$ is a free $A_\mathfrak{p}$-module. Hence we must have $d_{A_\mathfrak{q}/k} x \in \mathfrak{q}\Omega_{A_\mathfrak{q}/k}$ and therefore $d_{A_\mathfrak{q}/k}$ descends to a morphism

$$\overline{d_{A_\mathfrak{q}/k}} \colon \mathfrak{K}(\mathfrak{q}) \longrightarrow \Omega_{A_\mathfrak{q}/k}/\mathfrak{q}\Omega_{A_\mathfrak{q}/k} \ .$$

Clearly $\overline{d_{A_\mathfrak{q}/k}}$ is a k-linear derivation, hence induces a morphism $\Omega_{\mathfrak{K}(\mathfrak{q})/k} \xrightarrow{\delta} \Omega_{A_\mathfrak{q}/k}/\mathfrak{q}\Omega_{A_\mathfrak{q}/k}$ by the universal property of $\Omega_{\mathfrak{K}(\mathfrak{q})/k}$. It's easy to check that δ is left-inverse to the canonical morphism $\Omega_{A_\mathfrak{q}/k}/\mathfrak{q}\Omega_{A_\mathfrak{q}/k} \to \Omega_{\mathfrak{K}(\mathfrak{q})/k}$ (indeed, their composition must be $\mathrm{id}_{\Omega_{\mathfrak{K}(\mathfrak{q})/k}}$ by the universal property of $\Omega_{\mathfrak{K}(\mathfrak{q})/k}$). Thus $\Omega_{A_\mathfrak{q}/k}/\mathfrak{q}\Omega_{A_\mathfrak{q}/k} \to \Omega_{\mathfrak{K}(\mathfrak{q})/k}$ is injective and it follows that

$$\dim_{\mathfrak{K}(\mathfrak{q})} \Omega_{A_\mathfrak{q}/k}/\mathfrak{q}\Omega_{A_\mathfrak{q}/k} \leqslant \dim_{\mathfrak{K}(\mathfrak{q})} \Omega_{\mathfrak{K}(\mathfrak{q})/k} \ .$$

In either case, we can conclude that

$$\dim_{\mathfrak{K}(\mathfrak{q})} \left(\Omega_{A/k} \otimes_A \mathfrak{K}(\mathfrak{q})\right) = \dim_{\mathfrak{K}(\mathfrak{q})} \Omega_{A_\mathfrak{q}/k}/\mathfrak{q}\Omega_{A_\mathfrak{q}/k} \leqslant \dim_{\mathfrak{K}(\mathfrak{q})} \Omega_{\mathfrak{K}(\mathfrak{q})/k} = \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{q})/k) \ .$$

Comparing with (∗), this can only happen if $\dim_{\mathfrak{K}(\mathfrak{q})} \mathfrak{q}/\mathfrak{q}^2 = 0$, i.e., $\mathfrak{q}/\mathfrak{q}^2 = 0$.

Step 2. We can finish the reduction to $A/\mathfrak{q}$ as follows. From the sequence

$$\mathfrak{q}/\mathfrak{q}^2 \longrightarrow \Omega_{A/k} \otimes_A A/\mathfrak{q} \longrightarrow \Omega_{(A/\mathfrak{q})/k} \longrightarrow 0$$

we thus get $\Omega_{A/k} \otimes_A A/\mathfrak{q} \cong \Omega_{(A/\mathfrak{q})/k}$. Hence $\Omega_{A/k}$ being locally free at $\mathfrak{p}$ implies that $\Omega_{(A/\mathfrak{q})/k}$ is locally free of the same rank at $\mathfrak{p}/\mathfrak{q}$.

Hence, by Lemma 2 we see that (#) holds for $A/\mathfrak{q}$ and its quotient field $\mathfrak{K}(\mathfrak{q})$ instead of A and K. By Proposition 2(b) and [Alg$_1$, Theorem 10],

$$\begin{aligned}\dim_{\mathfrak{K}(\mathfrak{q})} \left(\Omega_{(A/\mathfrak{q})/k} \otimes_A \mathfrak{K}(\mathfrak{q})\right) &= \dim_{\mathfrak{K}(\mathfrak{q})} \Omega_{\mathfrak{K}(\mathfrak{q})/k} = \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{q})/k) = \dim(A/\mathfrak{q}) \\ &= \dim(A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p}) + \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p}/\mathfrak{q})/k) \ .\end{aligned}$$

But $A_\mathfrak{p}$ and $A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p}$ have the same dimension (by construction of $\mathfrak{q}$) and the same residue field $\mathfrak{K}(\mathfrak{p}) = \mathfrak{K}(\mathfrak{p}/\mathfrak{q})$, hence the last line of the above equation equals $\dim(A_\mathfrak{p}) + \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k)$. This shows that equality holds in (∗), proving that $A_\mathfrak{p}$ is indeed regular. □

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 $0 \leqslant i \leqslant n$. The tuple $(x_0, \dots, x_n)$ is called a *tuple of homogeneous 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 homogeneous 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 there is a map

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

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

2.2. Graded rings and homogeneous 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 homogeneous coordinates) one has to restrict to the case where P is homogeneous 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 *homogeneous components* of r. An element $r \in R$ is *homogeneous* 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 *homogeneous element* (i.e. *homogeneous polynomial*) is the well-known one.

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

Definition 2 (Homogeneous ideals)**.** Let R be a ($\mathbb{N}$-, $\mathbb{Z}$-) graded ring, $I \subseteq R$ and ideal. We say that I is **homogeneous** if for every $f \in I$ the homogeneous 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 homogeneous 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, $V(I) = V_{\text{proj}}(I) \subseteq \mathbb{P}^n(k)$ always means projective vanishing sets, whereas our good old affine vanishing sets are denoted $V_{\text{aff}}(U) \subseteq k^{n+1}$.

(*b*) As I is homogeneous, 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 homogeneous $f \in I$" 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 homogeneous 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 homogeneous ideal of R is finitely generated.*

(*c*) *Any set $\mathfrak{M} \neq \emptyset$ of homogeneous 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 homogeneous ideals in R becomes stationary for some $N \in \mathbb{N}$, i.e. $I_n = I_N$ for all $n \geqslant N$.*

(*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 homogeneous ideal in R is finitely generated iff it can be generated by finitely many homogeneous 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 homogeneous elements of R is homogeneous and for every inclusion $J \subsetneq I$ of ideals in R with homogeneous I there is some homogeneous $f \in I \setminus J$.

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

The implication $(e) \Rightarrow (f)$ can be seen as follows: Let R_+ be generated by homogeneous 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 homogeneous 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 homogeneous of degree $i - \deg(g_j)$ as dropping the other homogeneous components only changes homogeneous 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 $f \in S$. □

Proposition 2. *Let I be any homogeneous 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 homogeneous 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 homogeneous 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. □

Remark. The only homogeneous ideals $I \subseteq R$ such that $\sqrt{I} = I$ and $V(I) = \emptyset$ are $I = R_+$ and $I = R$. Also, any homogeneous 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 homogeneous 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*

$$\begin{aligned} \{\text{closed subsets } Z \subseteq \mathbb{P}^n(k)\} &\xrightarrow{\sim} \left\{\text{homogeneous ideals } I \subseteq R_+ \text{ such that } I = \sqrt{I}\right\} \\ Z &\longmapsto \{f \in R_+ \mid f(x_0, \ldots, x_n) = 0 \text{ when } [x_0, \ldots, x_n] \in Z\} \\ Z = V(I) &\longleftarrow\!\shortmid I \ . \end{aligned}$$

Proof. 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). This is 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 (equivalently, $\Delta \subseteq X \times X$ is closed). Such spaces X are called *Hausdorff*.

Proposition 4. *$\mathbb{P}^n(k)$ is a noetherian T_1-space. The correspondence from Proposition 3 induces a bijection between the points of $\mathbb{P}^n(k)$ and the homogeneous ideals $I = \sqrt{I} \subsetneq R_+$ maximal with this property, as well as between irreducible closed subsets and homogeneous prime ideals $\mathfrak{p} \subsetneq R_+$.*

Proof. A point $\{\xi\} = \{[\xi_0, \ldots, \xi_n]\}$ is closed as

$$\{\xi\} = \bigcap_{0 \leqslant i < j \leqslant n} V(\xi_i X_j - \xi_j X_i) \, .$$

The fact that $\mathbb{P}^n(k)$ is noetherian follows from noetherianness of R and Proposition 3 as an infinite strictly decreasing chain of closed subsets becomes a strictly increasing chain of ideals in R.

The correspondence between points and maximal homogeneous ideals also follows from Proposition 3. For the last one, note that a homogeneous ideal I is prime iff $fg \in I$ implies $f \in I$ or $g \in I$ for all *homogeneous* elements $f, g \in R$. Indeed, suppose that I has this property and $f, g \in R$ (not necessarily homogeneous) are such that $fg \in I$. Assume that $f, g \notin I$. Hence, if $f_i, g_i \in R_i$ are their homogeneous components, there are minimal indices k and ℓ such that $f_k, g_\ell \notin I$. Since I is homogeneous, the $(k+\ell)^{\text{th}}$-degree homogeneous component of fg must be contained in I as well. However, $(fg)_{k+\ell} = \sum_{i+j=k+\ell} f_i g_j \notin I$ as only $f_k g_\ell$ in this sum is not contained in I. Having established this, the arguments from the affine case may be used. □

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

Proposition 5. *For all $j = 0, \ldots, n$ the topology on $\mathbb{A}^n(k) \cong \mathbb{P}^n \setminus V(X_j)$ induced from the Zariski topology on $\mathbb{P}^n(k)$ is the Zariski topology on $\mathbb{A}^n(k)$.*

Proof. W.l.o.g. let $j = 0$. Then $\mathbb{A}^n(k) \xrightarrow{i} \mathbb{P}^n(k)$, $i(x_1, \ldots, x_n) = [1, x_1, \ldots, x_n]$, is the inclusion to investigate. The task is to show that i is an immersion, i.e., a homeomorphism onto its image.

Let $k[X_0,\dots,X_n] \xrightarrow{\pi} k[X_1,\dots,X_n]$ be the ring homomorphism induced by $X_0 \mapsto 1$. Then

$$i^{-1}(V(I)) = \{(x_1,\dots,x_n) \mid f(1,x_1,\dots,x_n) = 0 \text{ for all } f \in I\} = V(\pi(I))$$

and $\pi(I) \subseteq k[X_1,\dots,X_n]$ is an ideal by surjectivity of π, hence i is continuous.

To show that any closed $A \subseteq \mathbb{A}^n(k)$ can be represented as $i^{-1}(B)$ for some closed $B \subseteq \mathbb{P}^n(k)$, we first construct, for any $f \in S = k[X_1,\dots,X_n]$, a homogeneous polynomial $\widetilde{f} \in R$ such that $i^{-1}(V_{\text{proj}}(\widetilde{f})) = V_{\text{aff}}(f)$. This can be done by putting

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

where d is large enough (so that all exponents in $\widetilde{f}$ are non-negative). If $A = V_{\text{aff}}(I)$ and J denotes the ideal generated by the $\widetilde{f}$, for all $f \in I$, then $B = V_{\text{proj}}(J)$ has the desired property. □

Corollary 1. *(a) The closed subsets of $\mathbb{P}^1(k)$ are $\mathbb{P}^1(k)$ and the finite subsets.*

(b) $\operatorname{codim}(\{x\}, \mathbb{P}^n(k)) = n$ for any $x \in \mathbb{P}^n(k)$.

(c) $\dim(\mathbb{P}^n) = n$.

(d) $\mathbb{P}^n(k)$ is catenary.

Proof. For (a), let $Z \subseteq \mathbb{P}^1(k)$ be closed, then $Z \cap \mathbb{P}^1(k) \setminus V(X_0)$ and $Z \cap \mathbb{P}^1(k) \cap V(X_1)$ are closed, hence finite (by the affine case), thus so is Z. Conversely, if Z is finite, then it is closed by Remark A.1.3.

Parts (b), (c), and (d) follow from the *locality of codimension* (cf. Remark 1.1.1(a)) and the corresponding results in the affine case. □

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

$$C(Z) \coloneqq \{0\} \cup \{(x_0,\dots,x_n) \neq 0 \mid [x_0,\dots,x_n] \in Z\} \subseteq k^{n+1}\ .$$

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:*

$$\left\{\begin{array}{c}\textit{non-empty closed homogeneous}\\ \textit{subsets } C \subseteq k^{n+1}\end{array}\right\} \xrightarrow{\sim} \{\textit{closed subsets } Z \subseteq \mathbb{P}^n(k)\}$$
$$C = C(Z) \longleftarrow\!\shortmid\ Z$$
$$C \longmapsto Z = \{[x_0,\dots,x_n] \mid (x_0,\dots,x_n) \in C \setminus \{0\}\}\ .$$

Under this correspondence, Z is irreducible iff $C(Z)$ is irreducible and $\neq \{0\}$. Moreover,

$$\dim(C(Z)) = \dim(Z) + 1 \quad \textit{and} \quad \operatorname{codim}(C(Y), C(Z)) = \operatorname{codim}(Y, Z)$$

when $Y \subseteq Z$ is irreducible and closed.

Proof. The assertions about the correspondences (everything before *moreover*) all follow from Propositions 3 and 4 and the correspondence

$$\begin{aligned}\left\{\text{ideals } I \subseteq R \text{ such that } I = \sqrt{I}\right\} &\xrightarrow{\sim} \left\{\text{Zariski-closed subsets } C \subseteq k^{n+1}\right\}\\ \{f \in R \mid f(x) = 0 \text{ for all } x \in C\} &\longleftarrow\!\shortmid C\\ I &\longmapsto C = V(I)\,.\end{aligned}$$

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

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

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

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

$$n + 1 \leqslant \dim(C(Z)) + \operatorname{codim}\left(C(Z), C(\mathbb{P}^n(k))\right) = \dim(C(Z)) + \operatorname{codim}\left(C(Z), k^{n+1}\right) = n + 1 \qquad (*)$$

by affine dimension theory from Algebra 1, cf. [Alg$_1$, Theorem 5]. If one of the inequalities $\dim(C(Z)) \geqslant \dim(Z) + 1$ or $\operatorname{codim}\left(Z, \mathbb{P}^n(k)\right) \leqslant \operatorname{codim}\left(C(Z), C(\mathbb{P}^n(k))\right)$ 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 $\mathbb{P}^n(k)$ and k^{n+1} are catenary. □

Corollary 2. *An irreducible closed subset $Z \subseteq \mathbb{P}^n(k)$ has codimension 1 in $\mathbb{P}^n(k)$ iff it has the form $Z = V(p)$ where $p \neq 0$ is an irreducible homogeneous polynomial of positive degree in $R = k[X_0, \ldots, X_n]$.*

Proof. An irreducible closed subset Z has codimension 1 in $\mathbb{P}^n(k)$ iff $C(Z)$ has codimension 1 in $\mathbb{A}^{n+1}(k)$ by Proposition 6. By [Alg$_1$, Proposition 2.1.3], this is the case iff $C(Z) = V(p)$ for some prime element $p \in R = k[X_0, \ldots, X_n]$, where the prime ideal $(p) \in \operatorname{Spec} R$ is uniquely determined, hence so is its generator p up to multiplicative equivalence in R, i.e. up to $k^\times$.

We show that such p must necessarily be homogeneous, which will establish the equivalence. Since $p(X)$ and $p(\lambda X)$, for any $\lambda \in k^\times$, have the same vanishing set $C(Z)$ (as this is homogeneous), it follows (from uniqueness up to $k^\times$) that for any $\lambda \in k^\times$ there is some $c_\lambda \in k^\times$ such that $p(X) = c_\lambda p(\lambda X)$. But any such polynomial must be homogeneous (choose $\lambda \in k^\times \setminus \bigcup_{d \leqslant \deg p} \mu_d$, i.e. λ not a d^{th} root of unity for all $d \leqslant \deg p$). □

2.3. Projective algebraic varieties

Definition 1 (Projective algebraic variety)**.** A **projective algebraic variety** in $\mathbb{P}^n(k)$ is an irreducible closed subset Z of $\mathbb{P}^n(k)$. A **quasi-projective algebraic variety** is a non-empty open subset in a projective variety.

Definition 2 (Regular functions)**.** Let $Z \subseteq \mathbb{P}^n(k)$ be a quasi-projective algebraic variety.

(*a*) A function $Z \xrightarrow{f} k$ is called **regular** at $x \in Z$ if x has an open neighbourhood U in $\mathbb{P}^n(k)$ such that there are $p, q \in R = k[X_0, \ldots, X_n]$ which are homogeneous of the same degree, such that $q(y_0, \ldots, y_n) \neq 0$ for $[y_0, \ldots, y_n] \in U$ and

$$f([y_0, \ldots, y_n]) = \frac{p(y_0, \ldots, y_n)}{q(y_0, \ldots, y_n)} \quad \text{whenever} \quad [y_0, \ldots, y_n] \in U \cap Z \ .$$

We say that f is regular, or $f \in \mathcal{O}(Z)$, if it is regular at every $x \in Z$.

(*b*) Let $\pi \colon k^{n+1} \setminus \{0\} \to \mathbb{P}^n(k)$ be the projection and let, for $d \in \mathbb{Z}$, $\mathcal{O}(d)(Z)$ be the set of all functions $f \colon \pi^{-1}(Z) = C(Z) \setminus \{0\} \to k$ which are homogeneous of degree d, i.e.

$$f(\lambda y_0, \ldots, \lambda y_n) = \lambda^d f(y_0, \ldots, y_n) \quad \text{for all } y \in C(Z) \setminus \{0\} \text{ and } \lambda \in k^\times \ ,$$

and such that for every $x \in C(Z) \setminus \{0\}$, there are an open neighbourhood $U \subseteq k^{n+1}$ and $p \in R_{d+e}$, $q \in R_e$ (for some $e \in \mathbb{N}_0$) such that $U \cap V(q) = \emptyset$ and such that

$$f(y_0, \ldots, y_n) = \frac{p(y_0, \ldots, y_n)}{q(y_0, \ldots, y_n)} \quad \text{whenever} \quad (y_0, \ldots, y_n) \in U \cap C(Z) \setminus \{0\} \ .$$

Remark 1. (*a*) The condition $[y_0, \ldots, y_n] \in U$ has to be read as including that not all y_i are 0, i.e. that $[y_0, \ldots, y_n]$ is well-defined.

(*b*) The condition $U \cap V(q) = \emptyset$ could be weakened to $Z \cap U \cap V(q) = \emptyset$ or strengthened to $U = \mathbb{P}^n(k) \setminus V(q)$ without altering the definition. For the $\mathcal{O}(\ell)$, we may always choose a neighbourhood of the form $U = C(V) \setminus \{0\}$ with $V \subseteq \mathbb{P}^n(k)$ open as we won't hit the vanishing set of q by "conifying" U.

(*c*) $\mathcal{O}(Z)$ is a k-algebra, where $+$ and $\cdot$ are defined pointwise. If (U, p, q) above are for f, and $(\widetilde{U}, \widetilde{p}, \widetilde{q})$ for $\widetilde{f}$ witness their respective regularity condition at $[x]$, then

$$(f + \widetilde{f})([y]) = \frac{p(y)\widetilde{q}(y) + q(y)\widetilde{p}(y)}{(q\widetilde{q})(y)} \ , \quad (f \cdot \widetilde{f})([y]) = \frac{(p\widetilde{p})(y)}{(q\widetilde{q})(y)} \quad \text{for } [y] \in Z \cap U \cap \widetilde{U} \ .$$

(*d*) The set of units $\mathcal{O}(Z)^\times$ is $\{f \in \mathcal{O}(Z) \mid V(f) \cap Z = \emptyset\}$. Indeed, if this happens, then in the above situation we have $p(y) \neq 0$ for all $y \in U \cap Z$. Let $\widetilde{U} = U \setminus V(p)$, then $\widetilde{U} \cap Z = U \cap Z$ and the equality $\frac{1}{f} = \frac{q}{p}$ holds there.

(*e*) We have $\mathcal{O}(0) = \mathcal{O}$. If $f \in \mathcal{O}(d)(Z)$ and $\varphi \in \mathcal{O}(\delta)(Z)$ then $f\varphi \in \mathcal{O}(d + \delta)(Z)$ and $\frac{1}{f} \in \mathcal{O}(-d)(Z)$ if $f(y) \neq 0$ for $y \in Z$. Moreover, $(f + \varphi) \in \mathcal{O}(d)(Z)$ if $d = \delta$. The $\mathcal{O}(d)$ are *line bundles* (locally free modules of rank 1) over the *sheaf of rings* $\mathcal{O}$ (cf. Definition A.5.2 and A.5.3).

Example 1. Let $Y \subseteq \mathbb{P}^n(k)$ be a quasi-projective variety. We have $Y = \bigcup_{i=0}^n (Y \setminus V(X_i))$ and for $U \subseteq Y \setminus V(X_i)$

$$\begin{aligned} \mathcal{O}(U) &\longrightarrow \mathcal{O}(\ell)(U) \\ f &\longmapsto ((x_0, \ldots, x_n) \mapsto x_i^\ell f([x_0, \ldots, x_n])) \end{aligned}$$

defines an isomorphism $\mathcal{O}|_U \xrightarrow{\cdot X_i^\ell} \mathcal{O}(\ell)|_U$ of sheaves of (abelian groups or) $\mathcal{O}$-modules. Thus, $\mathcal{O}(\ell)$ is indeed a line bundle on Y.

Proposition 1. *Let $Z \subseteq \mathbb{P}^n(k)$ be a quasi-projective algebraic variety, then $Z \cap \mathbb{A}^n(k) = Z \setminus V(X_0)$ is quasi-affine or empty, and a function $f\colon Z \cap \mathbb{A}^n(k) \to k$ is regular in the sense of Definition 2(a) if and only if it is regular in the sense of the quasi-affine counterpart of that definition.*

Proof. The first part is obvious by Proposition 2.2.5. For the comparison of the structure sheaves use X_0 to homogenize (quasi-affine) regular functions; the details will be left as an exercise. □

Corollary. *Quasi-projective varieties are prevarieties in the sense Definition A.5.4.*

Corollary 1. *If $f_1, \ldots, f_n \in \mathcal{O}(Z)$ then $Z \xrightarrow{(f_1,\ldots,f_n)} \mathbb{A}^n(k)$ is Zariski-continuous.*

Remark. This holds when Z is any prevariety, and follows from the corresponding assertion about quasi-affine varieties.

Corollary 2. *If $U \subseteq Z$ is a non-empty open subset, $\mathcal{O}(Z) \to \mathcal{O}(U)$, $f \mapsto f|_U$ is injective.*

Proof. If $f \in \mathcal{O}(Z)$, $V(f) = \{z \in Z \mid f(z) = 0\}$ is closed in Z. If $f|_U = 0$, then $U \subseteq V(f)$. As Z is irreducible, U is dense in it. Hence $V(f)$ is closed and dense in Z, which implies $V(f) = Z$ and $f = 0$. □

Definition 3 (Field of rational functions)**.** If Z is any *prevariety* (cf. Definition A.5.4), let the **field of rational functions** K be the set of all pairs (U, f) where U is a non-empty open subset, $f \in \mathcal{O}_Z(U)$ modulo the equivalence relation $(U, f) \sim (V, \varphi)$ iff there is a non-empty $W \subseteq U \cap V$ such that $f|_W = \varphi|_W$.

Remark 2. (a) By Corollary 2, $f|_W = \varphi|_W$ is equivalent to $f|_{U\cap V} = \varphi|_{U\cap V}$. One may think of $K = \bigcup_{U\neq\emptyset,\text{ open}} \mathcal{O}(U)$ but of course that would be imprecise. However, by the sheaf axiom and Corollary 2 it follows that for any $f \in K$ there are a largest open subset U and $\varphi \in \mathcal{O}_Z(U)$ such that $f = (U, \varphi)/_\sim$, and φ is uniquely determined by f. This U is called the *domain of definition* of the rational function f.

(b) If Z had a point η_Z which is dense in Z (a *generic* point), we would have $K = \mathcal{O}_{Z,\eta_Z}$ as any open $U \neq \emptyset$ must contain η_Z.

(*c*) To show that K is a field, let $f \in K \setminus \{0\}$. Let $f = (U, \varphi)/_\sim$, then $\varphi \neq 0$. By Corollary 1, $V(\varphi) \subseteq U$ is closed and $\left(U \setminus V(\varphi), \frac{1}{\varphi}\right)/_\sim \in K$ is an inverse to f in K.

(*d*) If $U \subseteq Z$ is non-empty, the fields $K(U)$ and $K(Z)$ of rational functions on the respective spaces are canonically isomorphic as any $f \in K(Z)$ has a representative (W, φ) with $W \subseteq U$ (if $(V, \widetilde{\varphi})$ is any representative of f, $W = V \cap U$ and $\varphi = \widetilde{\varphi}|_W$ will do).

This enables us to derive the relation between dimension and transcendence degree from the quasi-affine case.

Proposition 2. *If $Z \subseteq \mathbb{P}^n(k)$ is quasi-projective (or, more generally, if Z is any prevariety) then $\dim(Z) = \operatorname{tr.deg}(K(Z)/k)$ and $\operatorname{codim}(\{z\}, Z) = \dim(Z)$ for any point $z \in Z$. Moreover, Z is catenary, i.e.*

$$\operatorname{codim}(A, B) + \operatorname{codim}(B, C) = \operatorname{codim}(A, C)$$

when $A \subseteq B \subseteq C$ are irreducible closed subsets of Z. Furthermore we have

$$\dim(A) + \operatorname{codim}(A, B) = \dim(B) \,.$$

Proof. By permutation of the X_i, we may assume $z \in Z \cap (\mathbb{P}^n(k) \setminus V(X_0)) = Z \cap \mathbb{A}^n(k) \neq \emptyset$. Then $U = Z \cap \mathbb{A}^n(k)$ is an open subset of Z, thus $K(U) \cong K(Z)$ and $\operatorname{codim}(\{z\}, U) = \operatorname{codim}(\{z\}, Z)$ (and moreover $\operatorname{codim}(X \cap U, Y \cap U) = \operatorname{codim}(X, Y)$ whenever $X \subseteq Y \subseteq Z$ are irreducible and $X \cap U \neq \emptyset$) by *locality of codimension*, cf. Remark 1.1.1(*a*) or [Alg$_1$, Remark 2.1.3]). By [Alg$_1$, Theorem 6], $\operatorname{codim}(\{z\}, Z) = \operatorname{codim}(\{z\}, U) = \operatorname{tr.deg}(K(U)/k) = \operatorname{tr.deg}(K(Z)/k)$ and the other assertions also follow from their counterparts in the affine case. □

Corollary 3. *The Krull dimension of $\mathbb{P}^n(k)$ equals n.*

Proof. We have $K(\mathbb{P}^n(k)) \cong K(\mathbb{A}^n(k)) \cong k(X_1, \ldots, X_n)$ by Remark 2(*d*), hence the transcendence degree considered in the above Proposition 2 equals n. □

Proposition 3. *Let Z be quasi-projective variety and $Y \subseteq Z$ irreducible closed, then*

$$\dim(C(Z)) = \dim(Z) + 1 \quad \textit{and} \quad \operatorname{codim}(Y, Z) = \operatorname{codim}(C(Y), C(Z)) \,.$$

Proof. Hello there. I'm Proposition 2.2.6 again. □

Theorem 16. *When X and Y are irreducible closed subsets of $\mathbb{P}^n(k)$, of codimension ξ and υ in $\mathbb{P}^n(k)$, then every irreducible component of $X \cap Y$ has codimension smaller or equal to $\xi + \upsilon$ in $\mathbb{P}^n(k)$. If we have $\xi + \upsilon \leqslant n$, it follows $X \cap Y \neq \emptyset$.*

Remark. For instance, if C and D are curves in $\mathbb{P}^2(k)$ (given by $P(x, y, z) = 0$ or $Q(x, y, z) = 0$ where P and Q are homogeneous of degree c and d) it follows that $C \cap D \neq \emptyset$. When the intersection is finite, it has $c \cdot d$ elements counted by multiplicity, by Bézout's Theorem (as we will see, cf. Theorem 19).

Proof of Theorem 16. We have $C(X) \cap C(Y) = C(X \cap Y)$. If $X \cap Y \neq \emptyset$, then it has a decomposition $X \cap Y = \bigcup_{i=1}^{\ell} C_i$ into irreducible components, and $C(X) \cap C(Y) = \bigcup_{i=1}^{\ell} C(C_i)$. If $X \cap Y = \emptyset$, then $C(X) \cap C(Y) = \{0\}$. By the previous Proposition 3 and Theorem 13,

$$\begin{aligned}\operatorname{codim}(C_i, \mathbb{P}^n(k)) &= \operatorname{codim}\left(C(C_i), \mathbb{A}^{n+1}(k)\right) \\ &\leqslant \operatorname{codim}\left(C(X), \mathbb{A}^{n+1}(k)\right) + \operatorname{codim}\left(C(Y), \mathbb{A}^{n+1}(k)\right) = \xi + \upsilon\end{aligned}$$

and the first assertion follows. Also, in the case $X \cap Y = \emptyset$ we have

$$n+1 = \operatorname{codim}\left(\{0\}, \mathbb{A}^{n+1}(k)\right) \leqslant \operatorname{codim}\left(C(X), \mathbb{A}^{n+1}(k)\right) + \operatorname{codim}\left(C(Y), \mathbb{A}^{n+1}(k)\right) = \xi + \upsilon\,,$$

proving the second assertion. □

Definition 4. The graded ring defined by a projective variety $X = V(\mathfrak{p}) \subseteq \mathbb{P}^n(k)$ with $\mathfrak{p} \subseteq k[X_0, \ldots, X_n]$ a homogeneous prime ideal is defined as $S(X) = k[X_0, \ldots, X_n]/\mathfrak{p}$.

As $\mathfrak{p}$ is homogeneous, $S(X)$ inherits a grading $S(X) = \bigoplus_{d \geqslant 0} S_d(X)$ (Professor Franke puts a dot in the index to indicate this, but we think this is ugly). Unlike to the affine case, we don't have $\mathcal{O}(X) \cong k[X_0, \ldots, X_n]/\mathfrak{p} = S(X)$ here, but nevertheless we would like to compare $S(X)$ to the structure sheaf or the line bundles $\mathcal{O}(\ell)$ on X.

Theorem 17. *Let X be a projective algebraic variety.*

(*a*) *For any $f \in S(X)$ which is homogeneous of positive degree, the localization $S(X)_f$ admits a grading $S(X)_f = \bigoplus_{d \geqslant 0} (S(X)_f)_d$ and we have*

$$\begin{aligned}(S(X)_f)_0 &\xrightarrow{\sim} \mathcal{O}(X \setminus V(f)) \\ \frac{g}{f^s} &\longmapsto \left([x_0, \ldots, x_n] \mapsto \frac{g(x_0, \ldots, x_n)}{f(x_0, \ldots, x_n)^s}\right)\,.\end{aligned}$$

Moreover

$$\begin{aligned}(S(X)_f)_\ell &\xrightarrow{\sim} \mathcal{O}(\ell)(X \setminus V(f)) \\ \frac{g}{f^s} &\longmapsto \left((x_0, \ldots, x_n) \mapsto \frac{g(x_0, \ldots, x_n)}{f(x_0, \ldots, x_n)^s}\right)\,.\end{aligned}$$

(*b*) *If $\lambda \in \mathcal{O}(\ell)(X)$, then for sufficiently large N we have $\lambda \cdot S_N(X) \subseteq S_{N+\ell}(X) \subseteq \mathcal{O}(N+\ell)(X)$ where the product should be viewed as a product of homogeneous functions on $C(X) \setminus \{0\}$.*

(*c*) *We have $k \cong S_0(X) \cong \mathcal{O}(X)$.*

Remark. (*a*) The grading is given by $(S(X)_f)_d = \{g f^{-s} \mid g \in S_{d+s\cdot\delta}(X)\}$ when $f \in S_\delta(X)$. For $\delta > 0$ we obtain a $\mathbb{Z}$-graded ring.

(*b*) When $f \in S_\delta(X)$ has the form $f = \varphi \bmod \mathfrak{p}$ for $\varphi \in R = k[X_0, \ldots, X_n]$ homogeneous of degree δ, then $V(f) \coloneqq V(\varphi) \cap X$ does not depend on the choice of φ.

Proof of Theorem 17. The proof of (a) is similar to what was done in the affine case, that is, in [Alg$_1$, Proposition 2.2.2]. Professor Franke's proof even contained the same unnecessary technical step, which we will – again – avoid. As they were before, well-definedness and injectivity are easy again so surjectivity is what we need to worry about.

Let $\eta \in \mathcal{O}(\ell)(X \setminus V(f))$ (the case $\ell = 0$ corresponds to the study of $\mathcal{O}(X \setminus V(f))$), where $f \neq 0$ is homogeneous of degree $\delta > 0$. Denote $X^\circ = X \setminus V(f)$ for short. By Definition 2(b) and Remark 1(b), every $x \in X^\circ$ has an open neighbourhood $U_x \subseteq X^\circ$ such that there are polynomials $p_x, q_x \in R = k[X_0, \ldots, X_n]$ where q_x is homogeneous of degree b_x, p_x of degree $a_x = b_x + \ell$ and $V(q_x) \cap U_x = \emptyset$ and such that

$$\eta(y_0, \ldots, y_n) = \frac{p_x(y_0, \ldots, y_n)}{q_x(y_0, \ldots, y_n)}$$

when $(y_0, \ldots, y_n) \in C(U_x) \setminus \{0\} \subseteq C(X^\circ) \setminus \{0\} = C(X) \setminus V_{\mathrm{aff}}(f)$. The topological space $\mathbb{P}^n(k)$, and thus also X, being noetherian, the open subset $X^\circ = X \setminus V(f)$ is quasi-compact, hence covered by finitely many $U_{x_i} = U_i$ for $i = 1, \ldots, N$. Let $p_i = p_{x_i}$ and $q_i = q_{x_i}$ for brevity. Since $V(q_i) \cap U_i = \emptyset$, we have $X^\circ \cap V(q_i) \subseteq X^\circ \setminus U_i$, hence $\emptyset = X^\circ \cap \bigcap_{i=1}^N V(q_i)$. Then

$$V(\varphi) \supseteq X \cap \bigcap_{i=1}^n V(q_i) = V\big(\mathfrak{p} + (q_1, \ldots, q_N)_R\big)$$

where $\mathfrak{p}$ is the homogeneous prime ideal corresponding to X and φ is some homogeneous representative of $f \in S(X) = R/\mathfrak{p}$. Since $\delta > 0$, $\varphi \in R_+$ and by the projective version of Hilbert's Nullstellensatz,

$$\varphi^s \in \mathfrak{p} + (q_1, \ldots, q_N)_R \qquad \text{for some } s \geqslant 1\ .$$

In other words, there are $h_i \in R_{s\cdot\delta - b_i}$ (with $b_i = b_{x_i}$) such that $\varphi^s \equiv \sum_{i=1}^N h_i q_i \bmod \mathfrak{p}$. Let

$$h = f^{-s} \sum_{i=1}^N h_i p_i \in (S(X)_f)_\ell\ .$$

We have $(p_i q_j)(x) = (p_j q_i)(x)$ for all $x = [x_0, \ldots, x_n] \in X$ because this holds as an equation in $\mathbb{A}^{n+1}(k)$ on the dense open subset $C(X) \setminus V(q_i q_j)$ of $C(X)$ and thus by continuity on all of $C(X)$. Then, for $[x_0, \ldots, x_n] \in X \setminus V(f)$

$$(g_j h)(x_0, \ldots, x_n) = f^{-s} \sum_{i=1}^N (h_i p_i q_j)(x) = f^{-s} \sum_{i=1}^N (h_i q_i p_j)(x) = p_j(x)$$

and thus $\eta(x) = h(x)$ when $x \in X \setminus V(q_j)$. As the sets $X \setminus V(q_j)$ cover $X \setminus V(f)$, the asserted surjectivity follows.

For (b), apply (a) in the case $f = X_i$. We thereby obtain the existence of $N_i \in \mathbb{N}$ such that $\lambda X_i^{N_i} \in S_{N_i+\ell}(X)$. If $N = \sum_{i=0}^n N_i$ the assertion follows as any monomial $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ of degree greater or equal to N contains an exponent $\alpha_i \geqslant N_i$.

To see (c), let $\lambda \in \mathcal{O}(X)$. By (b) there is $N \geqslant 0$ such that $\lambda \cdot S_N(X) \subseteq S_N(X)$ in $\mathcal{O}(N)(X)$. Let $P = \prod_{j=1}^d (T - \lambda_j)^{e_j}$, with $\lambda_j \in k$ and all $e_j > 0$, be the characteristic polynomial of $\lambda\cdot$ (the

linear map given by multiplication with λ) on $S_N(X)$. Then

$$\vartheta(x) \cdot \prod_{j=1}^{d} (\lambda(x) - \lambda_j)^{e_j} = 0$$

for all $\vartheta \in S_N(X)$ and all $x \in C(X) \setminus \{0\}$ by Cayley–Hamilton. As it is always possible to choose $\vartheta \in S_N(X)$ such that $\vartheta(x) \neq 0$ for a given $x \in C(X) \setminus \{0\}$ (indeed, if the i^{th} coordinate of x is non-zero, then $X_i^N \bmod \mathfrak{p}$ will do) we have $\prod_{j=1}^{d}(\lambda(x) - \lambda_j) = 0$, hence

$$X = \bigcup_{j=1}^{d} V(\lambda - \lambda_j) \, .$$

As X is irreducible, there is j such that $X = V(\lambda - \lambda_j)$. Then $\lambda = \lambda_j$ is constant on X. □

Corollary 4. *When* $\dim(X) > 0$ *and* $\ell < 0$ *we have* $\mathcal{O}(\ell)(X) = 0$.

Proof. First consider $\ell = -1$. Let $\lambda \in \mathcal{O}(-1)(X)$. By Theorem 17($c$) there are constants c_j such that $x_j\lambda(x) = c_j$ for $x \in C(X) \setminus \{0\}$ as all functions $X_j\lambda$ must be constant. If $\lambda \neq 0$ then not all c_i are 0. We have $x_i c_j = x_i x_j \lambda(x) = x_j c_i$ for $[x_0, \ldots, x_n] \in X$. If follows that the vectors $(x_0, \ldots, x_n)$ and $(c_0, \ldots, c_n)$ are proportional, $[x_0, \ldots, x_n] = [c_0, \ldots, c_n]$. Hence X has only one point, a contradiction to our assumption.

If $\ell < -1$ we use $X_i^{-1-\ell}\lambda \in \mathcal{O}(-1)(X)$ must vanish by the previous consideration. As for all $[x_0, \ldots, x_n] \in X$ one x_i must be non-zero, it follows that $\lambda = 0$. □

Remark. (a) When $X = \{x\}$ with $x_i \neq 0$ then X_i^ℓ gives a non-vanishing global section of $\mathcal{O}(\ell)$, for arbitrary ℓ. Thus $\dim(X) > 0$ is necessary in the corollary.

(b) Theorem 17(c) may be motivated from Liouville's Theorem from function theory.

(c) It is clear that $\lambda \in \mathcal{O}(\ell)(X)$ defines an element of $\mathcal{O}(C(X) \setminus \{0\})$. If it extends to all of $C(X)$ then it is given by a polynomial in $X_0, \ldots, X_n$ by results of Algebra I, cf. [Alg$_1$, Proposition 2.2.2]. In this case, it follows that $\lambda \in S_\ell(X)$.

One would expect that for ℓ sufficiently large, λ "vanishes to a very high order" at 0, hence extends to an element of $\mathcal{O}(C(X))$ and this turns out to be correct, as is shown on the 10^{th} exercise sheet. It follows that $S_\ell(X) \xrightarrow{\sim} \mathcal{O}(\ell)(X)$ when ℓ is sufficiently large.

(d) In general, $\mathfrak{p}$ defines a sheaf of ideals $\mathcal{J}$ on $\mathbb{P}^n = \mathbb{P}^n(k)$ and $\mathcal{O}_X(\ell)$ can be identified with $\mathcal{O}_{\mathbb{P}^n}(\ell)/\mathcal{J}\mathcal{O}_{\mathbb{P}^n}(\ell)$ and one obtains a part of a long exact cohomology sequence

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0\left(\mathbb{P}^n, \mathcal{J}\mathcal{O}_{\mathbb{P}^n}(\ell)\right) & \longrightarrow & H^0\left(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(\ell)\right) & \longrightarrow & H^0\left(\mathbb{P}^n, \mathcal{O}_X(\ell)\right) & \xrightarrow{\delta} & H^1\left(\mathbb{P}^n, \mathcal{J}\mathcal{O}_{\mathbb{P}^n}(\ell)\right) \\
 & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\
0 & \longrightarrow & \mathfrak{p}_\ell & \longrightarrow & k[X_0, \ldots, X_n]_\ell & \longrightarrow & \mathcal{O}_X(\ell)(X) & &
\end{array}$$

where the right end can be shown to be finite-dimensional and to vanish when ℓ is sufficiently large.

(*e*) When $n+1>1$ it follows that $\mathcal{O}(k^{n+1}\setminus\{0\})\cong\mathcal{O}(k^{n+1})$ as shown in Algebra I, cf. [Alg$_1$, Proposition 2.2.5]. Then $\mathcal{O}(\ell)(\mathbb{P}^n(k))\cong k[X_0,\dots,X_n]_\ell$. Another argument to see this is that when $\lambda\in\mathcal{O}(\ell)(\mathbb{P}^n(k))$ there there is $N\in\mathbb{N}$ such that $X_i^N\lambda=f_i\in R=k[X_0,\dots,X_n]$ for $i=0,\dots,n$. We have $X_i^Nf_j=X_j^Nf_i$. It follows that f_i is divisible by X_i^N (taking $j\neq i$, that's what we need $n\geqslant 1$ for), then $\lambda\in R$ (and thus $\in R_\ell$). The same argument only works for general X if $S(X)$ is factorial, which is usually not the case.

(*f*) It can be shown that $\mathcal{O}_X(\ell)(X)$ is finite-dimensional over k when $X\subseteq\mathbb{P}^n(k)$ is closed (and irreducible).

Remark. When $X=\{x\}$, $\dim_k\mathcal{O}_X(\ell)(X)=1$ is given by a polynomial of degree 0 in ℓ.

$$\mathcal{O}(\ell)(\mathbb{P}^1(k))=k[X_0,X_1]_\ell=\bigoplus_{i=0}^{\ell}\left(k\cdot X_0^iX_1^{\ell-1}\right)$$

has dimension $\ell+1$ over k when $\ell\geqslant-1$, hence the dimension is given by by a polynomial of degree 1 in ℓ. Is $\dim_k\left(\mathcal{O}_X(\ell)(X)\right)$ always given by a polynomial of degree $\dim(X)$ when $\ell\gg 0$? The answer is *yes* and this brings us to *Hilbert polynomials*.

It may be remarked that the seemingly artificial condition $\ell\gg 0$ can be removed (thus unfolding the deeper truth behind this) considering cohomology. There is always a polynomial P such that

$$\sum_{i=0}^{\dim(X)}\dim_k H^i(X,\mathcal{O}_X(\ell))=P(\ell)\quad\text{for all }\ell\,.$$

Note from the future: And we did this in *Algebraic Geometry II* [AG$_2$, Proposition 2.2.4]!

3. Applications of the Hilbert polynomial

Lemma 1. *For a field k the dimension of the space of homogeneous polynomials of degree d in n variables is given by $\binom{n+d-1}{n-1}$.*

Corollary 1. *For $\ell \geqslant -m$,*

$$\dim_k \mathcal{O}_{\mathbb{P}^m(k)}(\ell)(\mathbb{P}^m(k)) = \binom{m+\ell}{m} = \frac{(m+\ell)\cdots(1+\ell)}{m!} .$$

Remark. Again, there is a deeper cohomological truth behind this, and that deeper truth is

$$\dim_k H^p\left(\mathbb{P}^m(k), \mathcal{O}_{\mathbb{P}^m(k)}(\ell)\right) = \begin{cases} \text{the above (or 0 for } \ell < 0) & \text{if } p = 0 \\ 0 & \text{if } 0 < p < m \\ \dim_k H^0\left(\mathbb{P}^m(k), \mathcal{O}_{\mathbb{P}^m(k)}(-1-m-\ell)\right) & \text{if } p = m \end{cases} .$$

Proof of Lemma 1. Putting $n-1$ separators into $\{1, 2, \ldots, n+d-1\}$ produces n intervals of integers of lengths $\alpha_1, \ldots, \alpha_n$ (possibly 0) such that $\alpha_1 + \ldots + \alpha_n = d$. Sending such a set of intervals to $\prod_{i=1}^n X_i^{\alpha_i}$ is a bijection between the set of sets of separators an the monomials of degree d in n variables. Thus their number is $\binom{n+d-1}{n-1}$. □

Another proof. Induction on n, the case $n = 1$ being trivial. Let $n > 1$ and the assertion be true for less than n variables. For n variables we use induction on d. When $d = 0$, both sides equal 1. Otherwise a monomial of degree d in n variables has the form $X^\alpha = X^\beta X_n$ or $\alpha_n = 0$ in which case it is a monomial in $n-1$ variables. Thus their number is

$$\binom{n+d-2}{n-1} + \binom{n+d-2}{n-2} = \binom{n+d-1}{n-1} ,$$

as claimed □

Definition 1 (Graded module)**.** A **graded module** M over a graded ring R is an R-module M with a decomposition $M = \bigoplus_{d=-\infty}^{\infty} M_d$ of its additive group such that $R_k \cdot M_\ell \subseteq M_{k+\ell}$. We call M *finitely generated* (respectively *noetherian*) if it is finitely generated (respectively noetherian) as an ungraded R-module.

Remark 1. If M is finitely generated, it may be generated by finitely many homogeneous elements.

Definition 2 (Graded submodule)**.** (*a*) If $N \subseteq M$ is a **graded submodule** of a graded R-module M (i.e. for $n \in N$, the decomposition $n = \sum_{i=-\infty}^{\infty} h_i$ into homogeneous elements of M is a decomposition into elements of N), then M/N is the **graded quotient** with the grading $(M/N)_d = M_d/N_d$.

(*b*) The graded R-module $M[k]$ with $M[k]_\ell \coloneqq M_{k+\ell}$ is called the *shift* of M by k.

3.1. The Hilbert polynomial of a module over a graded ring

Definition 1 (Simple module, finite length)**.** (*a*) A module M over any ring R is called **simple** if it is not 0 and 0 and M are the only R-submodules of M.

(*b*) An R-module M is called **finite length** if it has a filtration $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_\ell = M$ such that M_i/M_{i-1} is simple for $1 \leqslant i \leqslant \ell$. Then ℓ is called *length* of M and denoted $\ell = \operatorname{length}_R(M)$ (sometimes the index is dropped).

Remark 1. (*a*) By a theorem of Artin–Schreier, the number ℓ is determined uniquely by M, as are the isomorphism classes of M_i/M_{i-1} up to permutation. We did not prove this in the lecture, but the proof is not too hard so it shall be sketched here.

Let $0 = M_0 \subsetneq \ldots \subsetneq M_\ell = M$ and $0 = N_0 \subsetneq \ldots \subsetneq N_k = M$ be two filtrations with simple quotients. We do induction on $\ell + k$. The case $\ell + k = 0$ is trivial. Now let w.l.o.g. $\ell \geqslant 1$ and choose a minimal m such that $M_1 \subseteq N_m$. Clearly $m \geqslant 1$, and using that $M_1 \nsubseteq N_{m-1}$ and that M_1 is simple as well as N_m/N_{m-1} we deduce that $N_{m-1} + M_1 = N_m$ and $N_{m-1} \cap M_1 = 0$. Then $N_m \cong N_{m-1} \oplus M_1$. In particular, $N_m/N_{m-1} \cong M_1$.

Now replace M by $M' = M/M_1$, each M_i for $i = 1, \ldots, \ell$ by $M'_{i-1} = M_i/M_1$, each N_j for $j = m+1, \ldots, k$ by $N'_{j-1} = N_j/M_1$ and finally each N_j for $j = 0, \ldots, m-1$ by $N'_j = (N_j + M_1)/M_1 \cong (N_j \oplus M_1)/M_1 \cong N_j$. Then $0 = M'_0 \subsetneq \ldots \subsetneq M'_{\ell-1} = M'$ and $0 = N'_0 \subsetneq \ldots \subsetneq N'_{k-1} = M'$ are filtrations of M' with the same quotients as the original filtrations of M except for a quotient isomorphic to M_1 we deleted from both filtrations. Induction does the rest. □

(*b*) The length of a k-vector space is its dimension. Indeed, as the quotients mustn't be 0, the dimension must strictly increase in each step of a filtration with simple quotients. Conversely, if the quotients are to be simple, it can only increase by 1 in each step.

(*c*) The length of $\mathbb{Z}/N\mathbb{Z}$ is the number of prime factors of N with respect to their multiplicity. Indeed, if $N = p_1 \cdots p_n$ is its decomposition into prime factors, then

$$0 = (p_1 \cdots p_n \mathbb{Z})/N\mathbb{Z} \subsetneq (p_1 \cdots p_{n-1}\mathbb{Z})/N\mathbb{Z} \subsetneq \ldots \subsetneq p_1\mathbb{Z}/N\mathbb{Z} \subsetneq \mathbb{Z}/N\mathbb{Z}$$

is a filtration with simple quotients, hence the claim follows from Artin–Schreier.

(*d*) The zero module has length 0.

(*e*) Any submodule or quotient module of an R-module M of finite length has again finite length, and for any strictly increasing chain $M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_d$ of submodules of M, the sequence $\operatorname{length}_R(M_i)$ is strictly increasing. Thus $d \leqslant \operatorname{length}_R(M)$, and any module of finite length is noetherian.

(*f*) If $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ is a short exact sequence then $\operatorname{length}_R(M) = \operatorname{length}_R(M') + \operatorname{length}_R(M'')$. This is an easy consequence of Artin–Schreier. Indeed, if $0 = M'_0 \subsetneq \dots M'_{\ell'} = M'$ and $0 = M''_0 \subsetneq \dots \subsetneq M''_{\ell''} = M''$ are filtrations of M' and M'' with simple quotients M'_i/M'_{i-1} and M''_j/M''_{j-1}, then

$$0 = \alpha(M'_0) \subsetneq \dots \subsetneq \alpha(M'_{\ell'}) = \beta^{-1}(M''_0) \subsetneq \dots \subsetneq \beta^{-1}(M''_{\ell''}) = M$$

is a filtration of M of length $\ell' + \ell''$ with simple quotients.

(*g*) Inductively, one can deduce from (*f*) that for any R-module M and any filtration $0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_k = M$ we have

$$\operatorname{length}_R(M) = \sum_{i=1}^{k} \operatorname{length}_R(M_i/M_{i-1}) \,.$$

Also note that all of this still works if some of the involved lengths are infinite.

Proposition 1 (Akizuki–Hopkins)**.** *For a ring R the following conditions are equivalent:*

(*a*) *R is noetherian of Krull dimension 0.*

(*b*) *R has finite length as an R-module.*

(*c*) *There is no strictly descending infinite chain $I_0 \supsetneq I_1 \supsetneq \dots$ of ideals in R.*

(*d*) *Any finitely generated R-module has finite length.*

(*e*) *In any finitely generated R-module M, there is no strictly descending infinite chain $M_0 \supsetneq M_1 \supsetneq \dots$ of submodules.*

We postpone the quite lengthy proof of Proposition 1 to after Proposition 2.

Proposition 2. (*a*) *Let R be a noetherian ring, M a finitely generated R-module. Then there is a finite filtration $0 = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_k = M$ such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in \operatorname{Spec} R$.*

(*b*) *If R and M are graded (R being $\mathbb{N}$-graded), we may chose this filtration in such a way that the M_i are graded submodules and the $\mathfrak{p}_i$ homogeneous and $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)[t_i]$ (this is the shift from Definition 3.0.2 and not some polynomial ring thingy), where $t_i \in \mathbb{N}_0$ and the isomorphism respects the grading.*

Lemma 1. *Let $M \neq 0$ be a module over a noetherian ring R, then it contains a submodule isomorphic to $R/\mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} R$. If M and R are graded, then $\mathfrak{p}$ may be chosen homogeneous and such that the isomorphism respects the grading up to shift.*

Proof. The set of ideals $\{\operatorname{Ann}_R(m) = \{r \in R \mid r \cdot m = 0\} \mid m \in M \setminus \{0\}\}$ in R has a $\subseteq$-maximal element, as R is noetherian. Let $m \neq 0$ such that $\operatorname{Ann}_R(m) = \mathfrak{p}$ is $\subseteq$-maximal in the above set of ideals. Then the submodule $R \cdot m \subseteq M$ is isomorphic to $R/\mathfrak{p}$. We have $1 \notin \mathfrak{p}$ as $m \neq 0$. Let $ab \in \mathfrak{p}$. If $a \notin \mathfrak{p}$, then $a \cdot m \neq 0$ and $\operatorname{Ann}_R(a \cdot m) \supseteq \operatorname{Ann}_R(m)$, and equality must occur by our choice of m. Thus $b \in \operatorname{Ann}_R(a \cdot m)$ implies $b \in \operatorname{Ann}_R(m)$, and $\mathfrak{p}$ is prime.

In the graded case, consider $\{\mathrm{Ann}_R(m) \mid m \in M \setminus \{0\} \text{ homogeneous}\}$, then the ideals of this set are automatically homogeneous and thanks to Proposition 2.2.1, the arguments for the ungraded can be recycled. □

Proof of Proposition 2. Part (a). By our assumption, M is noetherian. Hence the set $\mathfrak{M}$ of submodules of M with such a filtration has an $\subseteq$-maximal element M'. If $M' \neq M$ we could find a submodule $Q \subseteq M/M'$ which is isomorphic to $R/\mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} R$ by Lemma 1. Then the preimage of Q in M also has a filtration of the desired kind, contradicting maximality of M'.

The graded version (b) follows in the exact same way from the graded case of Lemma 1. □

Remark. (a) Note that $R/\mathfrak{p}$ is simple iff $\mathfrak{p}$ is maximal. Otherwise $\mathrm{length}_R(R/\mathfrak{p}) = \infty$. Indeed, any element $x \neq 0$ which is not a unit induces an infinite chain $(x) \supsetneq (x^2) \supsetneq \ldots$ of ideals of R.

(b) In particular, M in Proposition 2 is of finite length iff the $\mathfrak{p}_i$ are maximal. In this case, the length of the filtration equals $\mathrm{length}_R(M)$ and the $R/\mathfrak{p}_i$ are unique up to permutation and isomorphism. Otherwise, the length of the filtration may be non-unique, e.g. $0 \subsetneq \mathbb{Z}$ or $0 \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$ when $M = R = \mathbb{Z}$.

Proof of Proposition 1. Assume (a) and consider a filtration of the finitely generated R-module R as in Proposition 2. Given the Krull dimension is 0, the prime ideals $\mathfrak{p}_i$ occurring there are maximal and so $R/\mathfrak{p}_i$ is simple and thus R has finite length by Artin–Schreier. This shows that $(a) \Rightarrow (b)$.

Let R be of finite length as an R-module, i.e. (b) holds. We use induction on the minimal number k of generators of M to prove (d). If $k = 1$, M is isomorphic to R/I for some ideal $I \subseteq R$ and its length is smaller or equal to $\mathrm{length}_R(R)$. Now let $k \geqslant 2$. If M is generated by $m_1, \ldots, m_k$ and the assertion is known for $k-1$ generators, then, if $M' \subseteq M$ denotes the submodule generated by $m_1, \ldots, m_{k-1}$, we have $\mathrm{length}_R(M') < \infty$ by the induction assumption and M/M' is generated by the image of m_k, hence has finite length by the previous consideration. By Remark 1(f), $\mathrm{length}_R(M) = \mathrm{length}_R(M') + \mathrm{length}_R(M/M')$ is finite.

To show $(d) \Rightarrow (e)$, note that the length of the members of such sequence as in (e) form a strictly decreasing sequence. Hence the length of the sequence is bounded by $\mathrm{length}_R(M)$ assuming that M is of finite length, which is given by (d).

Taking $M = R$, (c) is a special case of (e).

To close the circle we have to prove that (c) implies (a). For this we will not need the famous prime avoidance lemma, but it is pretty neat so I will let it stand here:

Lemma 2 (Prime avoidance)**.** *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be ideals of a ring R such that there at most two among them which are not prime. If I is an ideal of R not contained in any $\mathfrak{p}_i$, then it is also not contained in the union of all the $\mathfrak{p}_i$.*

Professor Franke does not want to prove this here and recommends the appropriate chapter in Eisenbud, [Eis95, Section 3.2]. You can also find a proof by Franke himself in [Alg$_1$, Lemma 2.5.1].

Back to $(c) \Rightarrow (a)$. *Step 1.* First we prove that any prime ideal is maximal, i.e. the Krull dimension is 0. If $x \in R/\mathfrak{p}$ and $x \neq 0$, $x^n \cdot (R/\mathfrak{p})$ would form a strictly descending chain of ideals in the domain $R/\mathfrak{p}$ if x failed to be a unit, so any $x \in R/\mathfrak{p} \setminus \{0\}$ is a unit, hence $R/\mathfrak{p}$ a field and $\mathfrak{p}$ thus maximal.

Step 2. If R had infinitely many prime ideals (in other words, infinitely many maximal ideals), there would be a sequence $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ of distinct maximal ideals and the sequence

$$\mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supsetneq \ldots \supsetneq \bigcap_{i=1}^{k} \mathfrak{m}_i \supsetneq \ldots$$

is strictly descending, a contradiction to (c). Indeed, take $f_i \in \mathfrak{m}_i \setminus \mathfrak{m}_{k+1}$, then the product $f_1 \cdots f_k$ is in $\bigcap_{i=1}^{k} \mathfrak{m}_i$ but not in $\mathfrak{m}_{k+1}$.

Step 3. Now assume there are only finitely many distinct prime (and thus maximal) ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ of R. Then the nilradical $\operatorname{nil}(R) = \bigcap_{i=1}^{k} \mathfrak{m}_i = \operatorname{rad}(R)$ equals the Jacobson radical, and the sequence

$$\operatorname{nil}(R) \supseteq \operatorname{nil}(R)^2 \supseteq \ldots \supseteq \operatorname{nil}(R)^i \supseteq \ldots$$

must terminate at some point by (c). Thus, let $n \in \mathbb{N}$ such that $\operatorname{nil}(R)^n = \operatorname{nil}(R)^i$ for all $i \geqslant n$. Let $N = \operatorname{nil}(R)^n$. We would like to show $N = 0$. If $N \neq 0$, the annihilator K of N would be an ideal of R strictly contained in R. From (c) and Zorn's lemma it follows that any set of ideals of R contains a $\subseteq$-minimal element. Thus, there is an ideal $K \subsetneq I \subseteq R$ minimal among all such ideals. If $x \in I \setminus K$ we have $I = K + x \cdot R$ by the minimality of I. We have $K \subseteq x \cdot \operatorname{nil}(R) + K \subseteq I$, hence $x \cdot \operatorname{nil}(R) + K = K$ or $x \cdot \operatorname{nil}(R) + K = I$ by the minimality of I. In the second case $(I/K) = \operatorname{nil}(R) \cdot (I/K)$ and $I = K$ by [NAK], a contradiction to our choice of I. In the first case, $x \cdot \operatorname{nil}(R) \subseteq K$, hence $x \cdot \operatorname{nil}(R)^{n+1} \subseteq K \cdot N = 0$. But $\operatorname{nil}(R)^{n+1} = \operatorname{nil}(R)^n = N$, hence $x \in K$, a contradiction to our choice of I.

Step 4. We want to show that, if $I \supseteq J$ are ideals of R and I/J is annihilated by one of the $\mathfrak{m}_i$, then the length $\operatorname{length}_R(I/J)$ is finite. Otherwise this quotient would be a vector space of infinite dimension over the field $R/\mathfrak{m}_i$, hence has an infinite descending chain of subvector spaces whose preimages under $I \to I/J$ form an infinite descending chain of ideals in R, contradicting (c).

Step 5. We conclude that $\operatorname{nil}(R)^i / \operatorname{nil}(R)^{i+1}$ has finite length. Indeed, consider the (downwards indexed) filtration $0 = N_k \subsetneq N_{k-1} \subsetneq \ldots \subsetneq N_0 = \operatorname{nil}(R)^i / \operatorname{nil}(R)^{i+1}$ of $\operatorname{nil}(R)^i / \operatorname{nil}(R)^{i+1}$ given by

$$N_j \coloneqq \left(\bigcap_{l=1}^{j} \mathfrak{m}_l \cdot \operatorname{nil}(R)^i \right) / \operatorname{nil}(R)^{i+1} \quad \text{for } j = 0, \ldots, k\,.$$

Then each N_j/N_{j+1} is annihilated by $\mathfrak{m}_{j+1}$, hence has finite length by Step 4. Using Remark 1(g), we deduce that $\operatorname{nil}(R)^i / \operatorname{nil}(R)^{i+1}$ has finite length as well.

As $\operatorname{nil}(R)^n = 0$, this shows that $\operatorname{length}_R(R) < \infty$ (again by Remark 1(g)). In particular, R must be noetherian and this finishes our proof. □

Definition 2 (Artinian)**.** Rings with these equivalent properties are called **Artinian**.

Theorem 18. *Let R be an $\mathbb{N}$-graded ring satisfying the following equivalent conditions:*

(*a*) *R is noetherian and R_0 is Artinian and R_+ is generated by R_1 as an ideal.*

(*b*) *R_0 is Artinian, R is generated by R_0 and R_1, and R_1 is a finitely generated R_0-module.*

Let M be a finitely generated graded R-module. Then there are a polynomial $P_M \in \mathbb{Q}[T]$ and $k_0 \in \mathbb{Z}$ such that $\operatorname{length}_{R_0}(M_k) = P_M(k)$ for all $k \geqslant k_0$. This polynomial is uniquely determined and if R_1 may be generated by d elements as an R_0-module then its degree is less than d.

Remark. (*a*) We use the convention that the zero polynomial 0 has degree $-\infty$. When $d = 0$, the condition $\deg(P_M) < d$ is thus equivalent to $P_M = 0$.

(*b*) Here, we are considering the length $\operatorname{length}_{R_0}(M_k)$ of M_k as an R_0-module and not as an R-module. In fact, it wouldn't make sense to consider the length M_k as an R-module since it is most likely *not* an R-module, e.g. since $R_1 \cdot M_k \subseteq M_{k+1}$.

Definition 3 (Hilbert polynomial)**.** P_M is called the **Hilbert polynomial** of M.

Definition 4 (Hilbert polynomial of projective algebraic variety)**.** If $M = R = k[X_0, \ldots, X_n]/\mathfrak{p}$ is the graded coordinate ring of a projective algebraic variety $Z = V(\mathfrak{p})$, the polynomial P_M is called the **Hilbert polynomial** of Z.

Proof of Theorem 18. It is easy to see that (*a*) and (*b*) are equivalent; the arguments are similar to Proposition 2.2.1, except for noetherianness in (*a*) if (*b*) is given. This can be seen as follows: As R_1 is a finitely generated R_0-module and R is generated by R_0 and R_1, R must be a R_0-algebra of finite type. As R_0 is (Artinian and thus) noetherian, so is R by Hilbert's Basissatz. Also it's clear that P_M is unique.

For existence we use induction on d. *Step 1.* If $d = 0$, $R = R_0$. As M is finitely generated, $M_k = 0$ when $k \gg 0$ and $P_M = 0$ does it.

Step 2. When $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules and the assertion is valid for M' and M'', then it is valid for M and $P_M = P_{M'} + P_{M''}$, since we have $\operatorname{length}_{R_0}(M_k) = \operatorname{length}_{R_0}(M'_k) + \operatorname{length}_{R_0}(M''_k)$ for $k \gg 0$ (Remark 1(f)), and the sum has degree smaller than d if both summands are of degree smaller than d. Using an induction similar to Remark 1(g), we deduce that

$$P_M = \sum_{i=1}^{k} P_{M_i/M_{i-1}}$$

(and in particular, the assertion holds for M) for any filtration $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_k = M$ such that the assertion is valid for all subquotients M_i/M_{i-1}.

Step 3. Also, if the assertion is valid for M then it is clearly valid for the shift $M[\ell]$ (with $\ell \in \mathbb{Z}$) and $P_{M[\ell]}(T) = P_M(T + \ell)$.

Step 4. Let $d \geqslant 1$ and the assertion be valid if R_1 may be generated by fewer than d elements as an R_0-module. By Proposition 2(*b*) and by Step 2 and 3, we may assume $M = R/\mathfrak{p}$ where $\mathfrak{p}$ is a homogeneous prime ideal. Let $x_1 = x, x_2, \ldots, x_d$ generate R_1 as an R_0-module. If $x \in \mathfrak{p}$ then M is a module over R/xR to which the induction assumption may be applied as $(R/xR)_1 \cong R_1/xR_0$ is generated over R_0 by the images of $x_2, \ldots, x_d$. Otherwise we have short exact sequences

$$0 \longrightarrow M[-1] \xrightarrow{x\cdot} M \longrightarrow M/xM \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow M_{k-1} \xrightarrow{x\cdot} M_k \longrightarrow M_k/xM_{k-1} \longrightarrow 0$$

and the induction assumption may be applied to M/xM (with grading $(M/xM)_k = M_k/xM_{k-1}$) which is a module over R/xR. When k is large enough, we thus obtain

$$\operatorname{length}_{R_0}(M_k) = \operatorname{length}_{R_0}(M_{k-1}) + \operatorname{length}_{R_0}(M_k/xM_{k-1}) = \operatorname{length}_{R_0}(M_{k-1}) + P_{M/xM}(k)\ ,$$

where the polynomial $P_{M/X\cdot M}$ has degree smaller than $d-1$. The assertion thus follows from the following elementary fact. □

Fact 1. (*a*) *If $f\colon \mathbb{Z} \to \mathbb{Q}$ is a function such that there is a polynomial $P \in \mathbb{Q}[T]$ such that $f(k) - f(k-1) = P(k)$ for k sufficiently large, i.e. $k \geqslant k_0$ for some k_0, then there exists a (unique) polynomial $Q \in \mathbb{Q}[T]$ such that $f(k) = Q(k)$ for $k \geqslant k_0 - 1$.*

(*b*) *If $P \neq 0$ then $\deg Q = \deg P + 1$. If $\deg P = \delta$, then we have $(\delta+1) \cdot q_{\delta+1} = p_\delta$ for the leading coefficients $q_{\delta+1}$ and p_δ of Q respectively P.*

Proof. We would like to present a proof different from the one presented in the lecture. W.l.o.g. we may assume $k_0 = 0$. For any $i \geqslant 0$, the binomial coefficient $\binom{n}{i}$ for $n \geqslant 0$ extends to a polynomial

$$\binom{T}{i} = \frac{T(T-1)\cdots(T-i+1)}{i!} \in \mathbb{Q}[T]\ .$$

As $\binom{T}{i}$ has degree i, the $\binom{T}{i}$ form a $\mathbb{Q}$-basis of $\mathbb{Q}[T]$ which is more suitable for our purposes than the standard basis. If $P(T) = \widetilde{p}_0\binom{T}{0} + \widetilde{p}_1\binom{T}{1} + \ldots + \widetilde{p}_\delta\binom{T}{\delta}$, then $Q(T) = f(0) + \widetilde{p}_0\binom{T+1}{1} + \widetilde{p}_2\binom{T+1}{2} + \ldots + \widetilde{p}_\delta\binom{T+1}{\delta+1}$. Indeed, this follows from the well-known identity

$$\sum_{j=0}^{k} \binom{j}{i} = \binom{k+1}{i+1} \quad \text{for all } i, k \geqslant 0$$

which has a nice combinatorial proof by double counting: There are $\binom{k+1}{i+1}$ ways to select $i+1$ numbers from $\{1, \ldots, k+1\}$. On the other hand, for every $j \leqslant k$ there are $\binom{j}{i}$ choices such that $j+1$ is the largest selected number (we have to choose the remaining i from $\{1, \ldots, j\}$). Summing over all $j \leqslant k$ gives the above identity.

From this, assertion (*a*) is immediate. For (*b*) one just needs to note that $\widetilde{p}_\delta = \delta! \cdot p_\delta$ and $\widetilde{p}_\delta = (\delta+1)! \cdot q_{\delta+1}$. □

Fact 2. *Let M be an R-module with a filtration $0 = M_0 \subsetneq \ldots \subsetneq M_k = M$ such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$, where $\mathfrak{p}_i \in \operatorname{Spec} R$. Let $\operatorname{Ann}(M) = \{r \in R \mid r \cdot M = 0\}$, then $\sqrt{\operatorname{Ann}(M)} = \bigcap_{i=1}^{k} \mathfrak{p}_i$.*

Proof. If $r \in \bigcap_{i=1}^{k} \mathfrak{p}_i$ then $r \cdot M_i/M_{i-1} = 0$ for all i, hence $r \cdot M_i \subseteq M_{i-1}$ and thus $r^k \cdot M = 0$. This shows $r^k \in \operatorname{Ann}(M)$. On the other hand, if $r \notin \mathfrak{p}_i$, and $m \in M_i \setminus M_{i-1}$ then $r^\ell \cdot m \neq 0$ for arbitrary ℓ as the image of m in $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ is non-zero and $r \notin \mathfrak{p}_i$ is not a zero divisor in $R/\mathfrak{p}_i$. Thus, $r \notin \sqrt{\operatorname{Ann}(M)}$. □

Proposition 3. *Let k be an algebraically closed field.*

(*a*) *If $Z = V(\mathfrak{p})$ (where $\mathfrak{p} \subseteq k[X_0, \ldots, X_n]$ is a homogeneous prime ideal) is a projective algebraic variety, then the degree of its Hilbert polynomial equals* $\dim(Z)$.

(*b*) *If $R = k[X_0, \ldots, X_n]$ and M is a finitely generated graded R-module with a filtration $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_\ell = M$ with $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)[t_i]$ as in Proposition 2, then the degree of the Hilbert polynomial P_M equals*

$$\deg P_M = \max \{\dim V(\mathfrak{p}_i) \mid 1 \leqslant i \leqslant \ell\}$$

where the empty maximum and the dimension of $\emptyset$ are both taken to be $-\infty$.

Remark. The Hilbert polynomial is easily seen to be additive: $P_M = \sum_{i=1}^{\ell} P_{M_i/M_{i-1}}$. Moreover, Hilbert polynomials always have positive leading coefficients such that

$$\deg P_M = \max \left\{ \deg P_{M_i/M_{i-1}} \;\middle|\; 1 \leqslant i \leqslant \ell \right\} .$$

Proof of Proposition 3. It suffices to show (*b*) as (*a*) is just the special case $M = R/\mathfrak{p}$. We use induction on

$$d = \max \{\dim V(\mathfrak{p}_i) \mid 1 \leqslant i \leqslant \ell\} .$$

By the previous remark, we only have to consider the case $M = R/\mathfrak{p}$ for a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$. When $d = -\infty$, we have $\mathfrak{p} = R_+$ by the projective Nullstellensatz (Proposition 2.2.2) and $P_M = 0$ as $M = R/R_+ = k$ is concentrated in degree 0. Then both sides are $-\infty$.

Now let $d \geqslant 0$ and suppose that (*b*) holds for all smaller d. Again, we may restrict to $M = R/\mathfrak{p}$ with $\mathfrak{p} \subsetneq R_+$ this time. As R_+ is generated by R_1 as an ideal, it follows that there is $x \in R_1 \setminus \mathfrak{p}$. As $\mathfrak{p}$ is prime, the sequence

$$0 \longrightarrow M[-1] \xrightarrow{x\cdot} M \longrightarrow M/xM \longrightarrow 0$$

is exact. Thus $P_M(T) - P_M(T-1) = P_N$ by the additivity of the Hilbert polynomial, where $N = M/xM$. Let $0 = N_0 \subsetneq \ldots \subsetneq N_m = N$ with $N_i/N_{i-1} \cong (R/\mathfrak{q}_i)[s_i]$ for homogeneous prime ideals $\mathfrak{q}_i \in \operatorname{Spec} R$ and $s_i \in \mathbb{N}_0$ be a filtration as in Proposition 2. By Fact 2, $\bigcup_{i=1}^{m} V(\mathfrak{q}_i) = V(\operatorname{Ann}_R(N))$ and $\operatorname{Ann}_R(N) = \mathfrak{p} + xR$ as $N \cong R/(\mathfrak{p} + xR)$. Thus, $\bigcup_{i=1}^{m} V(\mathfrak{q}_i) = V(\mathfrak{p}) \cap V(x)$ is a proper subset of $V(\mathfrak{p})$.

In particular, each irreducible closed set $V(\mathfrak{q}_i)$ must have a smaller dimension than $d = \dim V(\mathfrak{p})$. Then the induction hypothesis may be applied to N and it follows that

$$\deg P_N = \max \{\dim V(\mathfrak{q}_i) \mid 1 \leqslant i \leqslant m\} < d .$$

If $d = 0$, it follows that $\deg P_N = -\infty$ and $P_N = 0$ and P_M is constant. On the other hand, $P_M = 0$ would imply the vanishing of $M = R/\mathfrak{p}$ in large homogeneous degrees. Then $R_+ \subseteq \sqrt{\mathfrak{p}}$

and $\sqrt{\mathfrak{p}} = \mathfrak{p}$ for $\mathfrak{p}$ being prime, thus $d = \dim(\emptyset) = -\infty$, but we are assuming $d = 0$. Thus, in this case P_M is a non-zero constant polynomial, i.e. of degree 0.

Now consider the case $d \geqslant 1$. Note that $x \in R_1$ is necessarily an irreducible polynomial. Then $V(x)$ is irreducible closed and has codimension $\operatorname{codim}(V(x), \mathbb{P}^n(k)) = 1$ by Corollary 2.2.2. By Theorem 16, the irreducible components of $V(\mathfrak{p}) \cap V(x)$ thus have codimension $\leqslant n - d + 1$. However, their dimension is bounded from above by $d-1$, hence equals $d-1$. As the irreducible components of $V(\mathfrak{p}) \cap V(x)$ must be among the $V(\mathfrak{q}_i)$ we obtain

$$\deg P_N = \max\{\dim(V(\mathfrak{q}_i)) \mid 1 \leqslant i \leqslant m\} = d - 1 \,.$$

By Fact 1(*b*), $P_N(T) = P_M(T) - P_M(T-1)$ implies $\deg P_M = d$. □

Lemma 3 (a.k.a. Lemma 1)**.** *Let $P \in \mathbb{Q}[T]$ be of degree $d \in \mathbb{N}_0$ such that $P(k) \in \mathbb{Z}$ for all sufficiently large $k \in \mathbb{Z}$. Then $P(k) \in \mathbb{Z}$ for all $k \in \mathbb{Z}$ and*

$$P(T) = \sum_{k=0}^{d} \widetilde{p}_k \binom{T}{k}$$

where $\widetilde{p}_k = \Delta^k P(0)$ (with Δ the difference operator $\Delta P(T) = P(T) - P(T-1)$, $\Delta^k P = \Delta\Delta^{k-1}P$). In particular, $\widetilde{p}_k \in \mathbb{Z}$ for all k and $d! \cdot p_d = \widetilde{p}_d$ for p_d the leading coefficient of P.

Proof. Let $P(T) = \frac{Q(T)}{N}$ where $Q \in \mathbb{Z}[T]$ and N is a positive integer. Then $Q(k) \bmod N$ only depends on $k \bmod N$, hence vanishes for all $k \in \mathbb{Z}$ if it does for sufficiently large $k \in \mathbb{Z}$. Thus $P(k) \in \mathbb{Z}$ for all $k \in \mathbb{Z}$. The formula for $\widetilde{p}_k$ is the Newton interpolation formula and follows from the *Pascal triangle identity*

$$\Delta\binom{T}{k} = \binom{T}{k} - \binom{T-1}{k} = \begin{cases} \binom{T}{k-1} & \text{if } k > 0 \\ 0 & \text{if } k = 0 \end{cases}$$

together with $\binom{0}{k} = 0$ for $k > 0$. □

Definition 5. Let $Z = V(\mathfrak{p}) \subseteq \mathbb{P}^n(k)$ be a projective algebraic variety of dimension d. The **degree** of Z is $\deg Z = d! \cdot p_d$ where $P(T) = \sum_{i=0}^{d} p_i T^i$ is the Hilbert polynomial of Z.

Example 1. (*a*) For $Z = \mathbb{P}^n(k)$ we have $P_Z(T) = \binom{T+n}{n}$ (by Lemma 3.0.1) which has leading coefficient $\frac{1}{n!}$. Hence $\deg \mathbb{P}^n(k) = 1$.

(*b*) Let $Z = V(p)$ where $p \in R = k[X_0, \ldots, X_n]$ be an irreducible homogeneous polynomial of degree d. Then $S(Z) = R/pR$ admits an obvious grading and by the short exact sequence

$$0 \longrightarrow R[-d] \xrightarrow{\cdot p} R \longrightarrow S(Z) \longrightarrow 0$$

we have $P_R(T) - P_R(T-d) = P_{S(Z)}(T)$. But $P_R(T) = \binom{T+n}{n}$ hence

$$P_Z = \frac{T^n - (T-d)^n}{n!} + \text{lower powers} = \frac{d \cdot n \cdot T^{n-1}}{n!} + \text{lower powers}$$

and $\deg Z = (n-1)! \cdot \frac{n \cdot d}{n!} = d$. Hence $\deg Z = \deg p$ when $Z = V(p)$ and p is s homogeneous irreducible polynomial, motivating the term *degree*.

Remark. This degree depends on Z as a subset of some $\mathbb{P}^n(k)$, not the isomorphism class of the abstract algebraic variety Z. For instance, with $p = XZ - Y^2$,

$$\begin{aligned} \mathbb{P}^1(k) &\xrightarrow{\sim} V(p) \subseteq \mathbb{P}^2(k) \\ [S,T] &\longrightarrow [S^2, ST, T^2] \end{aligned}$$

is an isomorphism of algebraic varieties. But the left hand side has degree 1 while the right hand side has degree 2.

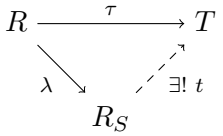
Remark. Bézout's Theorem in the general from states

$$\deg Z \cdot \deg p = \sum_{i=1}^{\ell} i(Z,p;Y_i) \cdot \deg(Y_i)$$

if $Z \subseteq \mathbb{P}^n(k)$ is a projective algebraic variety of positive dimension, $p \in k[X_0,\ldots,X_n]$ a homogeneous polynomial not identically vanishing on Z, moreover $Z \cap V(p) = \bigcup_{i=1}^{\ell} Y_i$ is the decomposition into irreducible components and $i(Z,p;Y_i)$ the (yet to define) *intersection multiplicity* of Z with $V(p)$ in Y_i.

3.2. Remarks on localization in the graded case

Proposition 1. (*a*) *Let R be a $\mathbb{Z}$-graded ring and $S \subseteq R$ a multiplicative set consisting of homogeneous elements. Then there is a unique (up to unique isomorphism) graded ring R_S with a morphism $R \xrightarrow{\lambda} R_S$ of graded rings such that $\lambda(S) \subseteq R_S^\times$ and such that the universal property for such morphisms holds:*

> *For any morphism $R \xrightarrow{\tau} T$ of graded rings with $\tau(S) \subseteq T^\times$, there is a unique morphism $R_S \xrightarrow{t} T$ such that the diagram*
>
> 
>
>
> *commutes.*

As an ungraded ring, R_S is the ordinary localization and the grading is given by

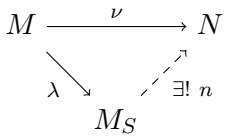
$$(R_S)_d = \left\{ \frac{r}{s} \;\middle|\; s \in S \cap R_e, r \in R_{d+e} \right\} .$$

(*b*) *We have a bijection*

$$\begin{aligned} \operatorname{Spec}(R_S) &\xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S \neq \emptyset\} \\ \mathfrak{p} &\longrightarrow \mathfrak{p} \cdot R_S \\ \lambda^{-1}(\mathfrak{q}) &\longleftarrow \mathfrak{q} . \end{aligned}$$

(c) *Every graded R_S-module defines a graded R-module on which S acts invertibly, and every graded R-module on which S acts invertibly module is obtained in this fashion.*

(d) *For every graded R-module M there is a unique (up to unique isomorphism) R_S-module M_S with a morphism $M \xrightarrow{\mu} M_S$ of graded R-modules, which has the universal property for such morphisms:*

> *For any morphism $M \xrightarrow{\nu} N$ of graded R-modules M to graded R_S-modules N, there is a unique morphism $M_S \xrightarrow{n} N$ such that*
>
> 
>
>
> *commutes.*

As an ungraded module, M_S is the ordinary localization, and the grading is

$$(M_S)_d = \left\{ \frac{m}{s} \;\middle|\; s \in S \cap R_e,\ r \in M_{e+d} \right\} .$$

The functor $M \mapsto M_S$ commutes with kernels of morphisms, quotients, direct sums and the shift operator $[-]$, i.e. $M[t]_S \cong M_S[t]$ for any $t \in \mathbb{Z}$.

(e) *Under the correspondence from (b), the homogeneous prime ideals correspond to each other.*

Proof. Parts (a) to (d) are tedious calculation. We are too lazy to copy them and you should be *grateful* we are!

Let's prove (e). Let $\mathfrak{p} \in \operatorname{Spec} R$ be homogeneous and $f \in \mathfrak{p}R_S$. Then $f = \frac{\varphi}{\sigma}$ for some $\varphi \in \mathfrak{p}$, $\sigma \in S$. As the elements of S are homogeneous, $\sigma \in S \cap R_e$ for some $e \in \mathbb{Z}$. As $\mathfrak{p}$ is homogeneous, we have $\varphi = \sum_{i=-\infty}^{\infty} \varphi_i$ with $\varphi_i \in \mathfrak{p} \cap R_i$ (and all but finitely many $\varphi_i = 0$). Put $f_i = \frac{\varphi_{i+e}}{\sigma}$, then $f = \sum_{i=-\infty}^{\infty} f_i$ and $f_i \in \mathfrak{p}R_S \cap (R_S)_i$. Hence $\mathfrak{p}R_S$ is homogeneous.

Conversely, let $\mathfrak{q} \in \operatorname{Spec} R_S$ be homogeneous and $f \in \mathfrak{p} = \lambda^{-1}(\mathfrak{q})$. Let $f = \sum_{i=-\infty}^{\infty} f_i$ with $f_i \in R_i$ (and only finitely many $f_i \neq 0$) be its decomposition into homogeneous components in R. Then $\lambda(f) = \sum_{i=-\infty}^{\infty} \lambda(f_i)$ and $\lambda(f_i) \in (R_S)_i$. By homogeneousness of $\mathfrak{q}$ we obtain $\lambda(f_i) \in \mathfrak{q}$ and thus $f_i \in \mathfrak{p}$, proving that $\mathfrak{p}$ is homogeneous. □

Convention 1. If R is a graded ring and $\mathfrak{p}$ a homogeneous prime ideal, $R_{\mathfrak{p}}$ is defined as the graded localization of R with respect to $S = \bigcup_{i \in \mathbb{Z}} (R_i \setminus \mathfrak{p})$. That is, we invert **only the homogeneous elements and not all of** $R \setminus \mathfrak{p}$. The same convention is applied to $M_{\mathfrak{p}}$ where M is a graded R-module.

3.3. Intersection multiplicities and Bézout's theorem

Definition 1. Let X be an algebraic variety (e.g. quasi-affine or quasi-projective, cf. Definition A.5.4), $\mathcal{O}_X$ its structure sheaf and $Z \subseteq X$ irreducible closed. We put

$$\mathcal{O}_{X,Z} \coloneqq \varinjlim_{U} \mathcal{O}_X(U) \ ,$$

where the colimit is taken over all open subsets $U \subseteq X$ such that $U \cap Z \neq \emptyset$, ordered by inclusion. Similarly, when $\mathcal{L}$ is a line bundle on X (e.g. $\mathcal{O}_X(\ell)$ when $X \subseteq \mathbb{P}^n(k)$ is projective) we put

$$\mathcal{L}_Z \coloneqq \varinjlim_{U} \mathcal{L}(U)$$

(U running over the same subsets as above) which is a free $\mathcal{O}_{X,Z}$-module of rank 1.

Explicitly, $\mathcal{O}_{X,Z}$ can be described as

$$\mathcal{O}_{X,Z} = \left\{ (U,f)/_\sim \;\middle|\; \begin{array}{c} U \subseteq X \text{ open}, U \cap Z \neq \emptyset, f \in \mathcal{O}_X(U) \text{ and } (U,f) \sim (V,g) \text{ iff there is} \\ \text{an open subset } W \subseteq U \cap V \text{ such that } W \cap Z \neq \emptyset \text{ and } f|_W = g|_W \end{array} \right\} .$$

By irreducibility of X (which is, after all, a variety), any open subsets U and V as above intersect (even inside Z by irreducibility of Z). Moreover, $U \cap V \subseteq X$ is nonempty open and thus irreducible as well, hence the W from above is dense in $U \cap V$ and by Zariski-continuity we may as well require that $W = U \cap V$. Also, we don't need Z to be closed, as replacing an irreducible set Z by its closure in X doesn't change the above definition.

$\mathcal{O}_{X,Z}$ has a natural ring structure (it is, in fact, a colimit in the category of rings). The operations $+$ and $\cdot$ are defined representative-wise, i.e. via

$$((U,f)/_\sim) * ((V,g)/_\sim) = (U \cap V, (f|_{U\cap V}) * (g|_{U\cap V}))/_\sim$$

for $* \in \{+,\cdot\}$ (one may check that this is well-defined). $\mathcal{O}_{X,Z}$ is a local ring with maximal ideal

$$\mathfrak{m} = \{(U,f)/_\sim \mid f \text{ vanishes identically on } U \cap Z\}$$

since for f not identically zero on $U \cap Z$, we have $(U,f) \sim \left(U \setminus V(f), f|_{U\setminus V(f)}\right)$ in $\mathcal{O}_{X,Z}$ and the latter is clearly invertible.

Proposition 1. (*a*) *When $Z = \{x\}$, $\mathcal{O}_{X,Z} = \mathcal{O}_{X,x}$ and $\mathcal{L}_Z = \mathcal{L}_x$.*

(*b*) *We have a bijective correspondence*

$$\left\{ \begin{array}{l} \textit{irreducible closed subsets} \\ Y \subseteq X \textit{ such that } Z \subseteq Y \end{array} \right\} \xrightarrow{\sim} \operatorname{Spec} \mathcal{O}_{X,Z}$$
$$Y \longmapsto \mathfrak{p} = \{(U,f)/_\sim \mid f_{U\cap Y} = 0\} \ .$$

(*c*) *When $X \subseteq \mathbb{P}^n(k)$ is a projective algebraic variety (over the algebraically closed field k), $X = V(\mathfrak{p})$ for some homogeneous prime ideal $\mathfrak{p} \subseteq k[X_0, \dots, X_n]$, and $Z = V(\mathfrak{q})$ where $\mathfrak{q} \subseteq S(X) = k[X_0, \dots, X_n]/\mathfrak{p}$ is a homogeneous prime ideal, then*

$$\begin{aligned}(S(X)_{\mathfrak{q}})_0 &\xrightarrow{\sim} \mathcal{O}_{X,Z}\\ \frac{f}{s} &\longmapsto \left(X \setminus V(s), \frac{f}{s}|_{X\setminus V(s)}\right)/\sim\end{aligned}$$

is an isomorphism. More generally,

$$\begin{aligned}(S(X)_{\mathfrak{q}})_\ell &\xrightarrow{\sim} \mathcal{O}_X(\ell)_Z\\ \frac{f}{s} &\longmapsto \left(X \setminus V(s), \frac{f}{s}|_{X\setminus V(s)}\right)/\sim\end{aligned}$$

is an isomorphism for all $\ell \in \mathbb{Z}$.

Proof. Point (*a*) follows directly from the definitions.

Part (*c*) follows from Theorem 17 as the open subsets $X \setminus V(\lambda)$ for homogeneous $\lambda \in S(X)$ form a topology base on X. Indeed, an open set $X \setminus V(I)$ (for $I \subseteq S(X)$ a homogeneous ideal) is the union of all $X \setminus V(\lambda)$ where λ goes over all homogeneous $\lambda \in I$. Therefore, open subsets $U = X \setminus V(s)$ for non-constant homogeneous s such that $U \cap Z \neq \emptyset$ (or equivalently, $s \notin \mathfrak{q}$) are *cofinal* in the set of open subsets over which the direct limit is taken in Definition 1 and it does not change if the direct limit is instead taken over all such homogeneous $s \in S(X) \setminus \mathfrak{q}$ of positive degree ordered by divisibility. Then one obtains

$$\mathcal{O}_{X,Z} = \varinjlim_s \mathcal{O}_X(\ell)(X \setminus V(s)) \cong \varinjlim_s (S(X)_s)_\ell \cong (S(X)_{\mathfrak{q}})_\ell$$

(recall our Convention 3.2.1 that we only invert homogeneous elements).

The question (*b*) is local because for any open subset $U \subseteq X$, we have a bijection between the irreducible closed subsets $A \subseteq U$ and the irreducible closed subsets $B \subseteq X$ such that $B \cap U \neq \emptyset$ (cf. Remark 1.1.1(*a*)) and because $(\mathcal{O}_X|_V)_Z) \cong \mathcal{O}_{X,Z}$ when $V \cap Z \neq \emptyset$ and $V \subseteq X$ is open, as the open $U \subseteq V$ such that $U \cap Z \neq \emptyset$ are cofinal in the open subsets over which the direct limit is taken.

Therefore it is possible to assume without loss of generality that X is affine. As $Z \subseteq X$ is irreducible closed, by [Alg$_1$, Corollary 2.2.2] we have $Z = V(\mathfrak{q})$ for some prime ideal $\mathfrak{q} \subseteq \mathcal{O}_X(X)$. As $\mathcal{O}_X(X \setminus V(f)) \cong \mathcal{O}_X(X)_f$ by [Alg$_1$, Proposition 2.3.3], we have

$$\mathcal{O}_{X,Z} = \varinjlim_{f \notin \mathfrak{q}} \mathcal{O}_X(X \setminus V(f)) \cong \varinjlim_{f \notin \mathfrak{q}} \mathcal{O}_X(X)_f \cong \mathcal{O}_X(X)_{\mathfrak{q}}$$

and we have bijections

$$\begin{array}{ccc}
\left\{\begin{array}{c}\text{irreducible closed subsets}\\ Y \subseteq X \text{ such that } Z \subseteq Y\end{array}\right\} & & \\
\Big\downarrow \wr & \overset{\sim}{\searrow} & \\
\left\{\begin{array}{c}\text{prime ideals } \mathfrak{p} \subseteq \mathcal{O}_X(X) \text{ such that } \mathfrak{p} \subseteq \mathfrak{q}\\ \text{(or in other words } \mathfrak{p} \cap (\mathcal{O}_X \setminus \mathfrak{q}) = \emptyset)\end{array}\right\} & \xrightarrow{\sim} & \operatorname{Spec} \mathcal{O}_X(X)_{\mathfrak{q}} \cong \operatorname{Spec} \mathcal{O}_{X,Z}
\end{array}$$

(the vertical bijection from [Alg$_1$, Corollary 2.2.2], the horizontal from [Alg$_1$, Corollary 2.3.1(e)]) inducing the bijective correspondence we want. □

Definition 2 (Intersection multiplicity)**.** Let $X \subseteq \mathbb{P}^n(k)$ be a projective algebraic variety over an algebraically closed field k, $H \in k[X_0, \ldots, X_n]$ a homogeneous polynomial of degree $d > 0$ not identically zero on X, and Z an irreducible component of $X \cap V(H)$. We define the intersection multiplicity $i(X, H, Z)$ by

$$i(X, H; Z) = \text{length}_{\mathcal{O}_{X,Z}} \left(\mathcal{O}_{X,Z} \Big/ \left(\frac{H}{F} \cdot \mathcal{O}_{X,Z} \right) \right) = \text{length}_{\mathcal{O}_{X,Z}} \left(\mathcal{O}_X(d)_Z / H \cdot \mathcal{O}_{X,Z} \right)$$

where the length is of $\mathcal{O}_{X,Z}$-modules and in the middle term, F is any element of $k[X_0, \ldots, X_n]_d$ not identically vanishing on Z.

You know you are attending a Franke lecture when a definition needs a proof. By the same argument as in Example 2.3.1, F is a free generator of $\mathcal{O}_X(d)|_{X \setminus V(F)}$. Moreover, $X \setminus V(F)$ intersects Z, hence $(X \setminus V(F), F)/_\sim$ is a free generator of $\mathcal{O}_X(d)_Z$. Therefore, multiplication by F defines an isomorphism

$$\mathcal{O}_{X,Z} \Big/ \left(\frac{H}{F} \cdot \mathcal{O}_{X,Z} \right) \xrightarrow[\cdot F]{\sim} \mathcal{O}_X(d)_Z / H \cdot \mathcal{O}_{X,Z} \, .$$

This shows that the middle term is independent of F. □

Corollary 1 (of Definition 2)**.** *When $Z = V(\mathfrak{q})$ we have*

$$\begin{aligned} i(X, H; Z) &= \text{length}_{(S(X)_\mathfrak{q})_0} \left((S(X)_\mathfrak{q})_0 \Big/ \left(\frac{H}{F} \cdot (S(X)_\mathfrak{q})_0 \right) \right) \\ &= \text{length}_{(S(X)_\mathfrak{q})_0} \left((S(X)_\mathfrak{q})_d / H \cdot (S(X)_q)_0 \right) . \end{aligned}$$

Proof. Follows directly from Proposition 1(c). □

Remark 1. (a) It follows from the second equality that the middle term in Definition 2 and Corollary 1 is independent of F.

(b) When $Z \not\subseteq V(H)$, then $\frac{H}{F} \in \mathcal{O}_{X,Z}^\times$ and the above definition of i gives zero. When $Z \subseteq X \cap V(H)$ is not an irreducible component of $X \cap V(H)$, the length can be shown to be infinite.

(c) The definition can be generalized to $i(A, B; Z)$ (containing ours for irreducible H as the special case when $B = V(H) \subseteq \mathbb{P}^n(k)$) the multiplicity of an irreducible component in $Z \subseteq A \cap B$, where A and B are irreducible and of arbitrary codimension. This was done by Serre and is much more complicated. Our

$$\text{length}_{\mathcal{O}_{\mathbb{P}^n(k),Z}} \left(\mathcal{O}_{A,Z} \otimes_{\mathcal{O}_{\mathbb{P}^n(k),Z}} \mathcal{O}_{B,Z} \right)$$

becomes

$$\sum_{j=0}^{\infty} (-1)^j \, \text{length}_{\mathcal{O}_{\mathbb{P}^n(k),Z}} \left(\text{Tor}_j^{\mathcal{O}_{\mathbb{P}^n(k),Z}} (\mathcal{O}_{A,Z}, \mathcal{O}_{B,Z}) \right) \, .$$

(*d*) Ok, hang on a minute. Why is $\operatorname{length}_{\mathcal{O}_{\mathbb{P}^n(k),Z}}\left(\mathcal{O}_{A,Z}\otimes_{\mathcal{O}_{\mathbb{P}^n(k),Z}}\mathcal{O}_{B,Z}\right)$ *our* intersection multiplicity? I've never seen that guy before! Well, here is why: Let Z intersect $\mathbb{P}^n(k)\setminus V(X_i)$ (as these sets cover $\mathbb{P}^n(k)$, Z must intersect one of them). Then X_i doesn't vanish identically on Z and we have $Z=V(\mathfrak{q})$ with $\mathfrak{q}\subseteq R=k[X_0,\dots,X_n]$ a prime ideal such that $X_i\notin\mathfrak{q}$. Let d be the degree of H, which we assume to be irreducible (and homogeneous of course). Then $S(V(H))_{\mathfrak{q}}=(R/HR)_{\mathfrak{q}}$ is a graded ring and

$$\bigoplus_{\ell\in\mathbb{Z}}\left((R/HR)_{\mathfrak{q}}\right)_\ell=(R/HR)_{\mathfrak{q}}=R_{\mathfrak{q}}/HR_{\mathfrak{q}}\cong R_{\mathfrak{q}}\Big/\left(\frac{H}{X_i^d}\cdot R_{\mathfrak{q}}\right)$$

as $X_i\notin\mathfrak{q}$ is a unit in $R_{\mathfrak{q}}$. Now the left-hand side has the big advantage that $\frac{H}{X_i^d}$ is homogeneous of degree 0 and we deduce that

$$\mathcal{O}_{V(H),Z}\cong\left((R/HR)_{\mathfrak{q}}\right)_0\cong(R_{\mathfrak{q}})_0\Big/\left(\frac{H}{X_i^d}\cdot(R_{\mathfrak{q}})_0\right)\cong\mathcal{O}_{\mathbb{P}^n(k),Z}\Big/\left(\frac{H}{X_i^d}\cdot\mathcal{O}_{\mathbb{P}^n(k),Z}\right)$$

in which we used Proposition 1(*c*) twice. Hence, tensoring $\mathcal{O}_{X,Z}$ with $\mathcal{O}_{V(H),Z}$ is the same as modding out $\frac{H}{X_i^d}\cdot\mathcal{O}_{X,Z}$ (cf. Fact A.4.2), hence gives the same as the middle term in Definition 2, except that we are taking the length as an $\mathcal{O}_{\mathbb{P}^n(k),Z}$-module instead of as an $\mathcal{O}_{X,Z}$-module. However, if $X=V(\mathfrak{p})$ for $\mathfrak{p}\subseteq R$ a homogeneous prime ideal, we have that

$$\mathcal{O}_{X,Z}\cong((R/\mathfrak{p})_{\mathfrak{q}})_0\cong(R_{\mathfrak{q}})_0/(\mathfrak{p}R_{\mathfrak{q}})_0$$

(by Proposition 1(*c*)) is a quotient of $(R_{\mathfrak{q}})_0\cong\mathcal{O}_{\mathbb{P}^n(k),Z}$ and $\mathcal{O}_{X,Z}\otimes_{\mathcal{O}_{\mathbb{P}^n(k),Z}}\mathcal{O}_{V(H),Z}$ has $(\mathfrak{p}R_{\mathfrak{q}})_0$-torsion (well, we tensored with $\mathcal{O}_{X,Z}$), hence any $\mathcal{O}_{\mathbb{P}^n(k),Z}$-submodule of it is an $\mathcal{O}_{X,Z}$-submodule as well and the lengths agree.

Theorem 19 (Bézout's theorem in a more general version)**.** *Let $X\subseteq\mathbb{P}^n(k)$ be a projective algebraic variety, $H\in k[X_0,\dots,X_n]$ a polynomial of degree d not identically vanishing on X, then*

$$\sum_Z i(X,H;Z)\cdot\deg(Z)=d\cdot\deg(X)$$

where the intersection multiplicities are finite and the sum is taken over all irreducible components Z of $X\cap V(H)$.

Remark. As $\mathcal{O}_{X,Z}$ is a domain and the $\mathcal{O}_X(\ell)_Z$ are free modules of rank 1 over it, we have a short exact sequence

$$0\longrightarrow\mathcal{O}_X(e)_Z/G\cdot\mathcal{O}_{X,Z}\xrightarrow{\cdot F}\mathcal{O}_X(e+d)_Z/(GF)\cdot\mathcal{O}_{X,Z}\longrightarrow\mathcal{O}_X(e+d)_Z/F\cdot\mathcal{O}_X(e)_Z\longrightarrow 0$$

when $F,G\in k[X_0,\dots,X_n]$ are homogeneous polynomials of degree e respectively d not identically vanishing on X. If i is chosen such that Z intersects $\mathbb{P}^n(k)\setminus V(X_i)$, i.e. X_i doesn't vanish identically on Z, we have an isomorphism

$$\mathcal{O}_X(d)_Z/F\cdot\mathcal{O}_{X,Z}\xrightarrow[\cdot X_i^e]{\sim}\mathcal{O}_X(e+d)_Z/F\cdot\mathcal{O}_X(e)_Z$$

showing that $i(X, GF; Z) = i(X, F; Z) + i(X, G; Z)$ by the right term of Definition 2 and Artin–Schreier (cf. Remark 3.1.1(f)). For this reason, Theorem 19 can be reduced to the case where H is irreducible. In this case, H is a generator of the prime ideal $\mathfrak{r} = (H)$ such that $V(\mathfrak{r}) = C = V(H)$, hence, one can interpret the result as

$$\sum_Z i(X, C; Z) \cdot \deg(Z) = \deg(X) \cdot \deg(C)$$

where the sum is taken over the irreducible components of $X \cap C$, provided $X \not\subseteq C$, which holds when $\operatorname{codim}(X, \mathbb{P}^n(k)) = 1$. With Serre's definition of $i(X, C; Z)$ the equality hold in full generality when the intersection is *proper*, i.e., all occurring Z have codimension in $\mathbb{P}^n(k)$ equal to $\operatorname{codim}(X, \mathbb{P}^n(k)) + \operatorname{codim}(C, \mathbb{P}^n(k))$.

When X also has codimension 1, $V = V(P)$ with $P \in k[X_0, \ldots, X_n]$ irreducible and homogeneous of some degree e (by Corollary 2.2.2), then

$$i(X, C; Z) = \operatorname{length}_{\mathcal{O}_{\mathbb{P}^n(k),Z}} \left(\mathcal{O}_{\mathbb{P}^n(k),Z} \Big/ \left(\frac{P}{X_i^e}, \frac{H}{X_i^d} \right)_{\mathcal{O}_{\mathbb{P}^n(k),Z}} \right)$$

since $\mathcal{O}_{X,Z} \cong \mathcal{O}_{\mathbb{P}^n(k),Z} \Big/ \left(\frac{P}{X_i^e} \cdot \mathcal{O}_{\mathbb{P}^n(k),Z} \right)$ by the argument from Remark 1(e).This is symmetric in P and H, hence our definition of $i(X, C; Z)$ is symmetric in X and C when both are of codimension 1. Serre's i is always symmetric in the first two operands.

It seems that Bézout treated the case $n = 2$, $\dim(X) = 1$ in the 18^{th} century.

Proof of Bézout's Theorem. Let $R = S(X)$ and $M = (R/HR)$ then we have

$$P_M(T) = P_X(T) - P_X(T - d)$$

where P_M, P_X are the Hilbert polynomials of M and X) by Remark 3.1.1(f) and the short exact sequence

$$0 \longrightarrow R[-d] \xrightarrow{\cdot H} R \longrightarrow M \longrightarrow 0\,.$$

If ξ is the dimension and e the degree of X and $P_X = \frac{e}{\xi!} T^\xi + \sum_{i=0}^{\xi-1} c_i T^i$ this equals

$$\begin{aligned} P_M(T) = \frac{e}{\xi!}(T^\xi - (T-d)^\xi) + \sum_{i=0}^{\xi-1} c_i (T^i - (T-d)^i) &= \frac{e \cdot d \cdot \xi}{\xi!} \cdot T^{\xi-1} + \text{ lower powers} \\ &= \frac{e \cdot d}{(\xi-1)!} \cdot T^{\xi-1} + \text{ lower powers } . \end{aligned} \tag{\#}$$

Let $0 = M_0 \subsetneq \ldots \subsetneq M_n = M$ be a filtration as in Proposition 3.1.2, with $M_i/M_{i-1} \cong (R/\mathfrak{q}_i)[t_i]$, $\mathfrak{q}_i \in \operatorname{Spec} R$ being homogeneous prime ideals and t_i some integers. By Fact 3.1.2 we have

$$\sqrt{(H)_R} = \sqrt{\operatorname{Ann}_R(M)} = \bigcap_{i=1}^n \mathfrak{q}_i$$

showing that $V(H) \cap X = \bigcup_{i=1}^n V(\mathfrak{q}_i)$. In particular, the $\subseteq$-minimal elements of $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ correspond to the irreducible components of $V(H) \cap X$. Let $Z = V(\mathfrak{q})$ be such an irreducible component, we claim that

Claim 1. The intersection multiplicity $i(X, H; Z)$ equals the number of occurrences of $\mathfrak{q}$ in the sequence $(\mathfrak{q}_1, \ldots, \mathfrak{q}_n)$.

Believing Claim 1 for the moment, this proves in particular the finiteness if $i(X, H; Z)$. The irreducible components of $X \cap V(H)$ have codimension 1 in X by Corollary 1.1.2, hence dimension $\xi - 1$. The contribution of the $\mathfrak{q}_i$ such that $V(\mathfrak{q}_i)$ is an irreducible component of $X \cap V(H)$ to the leading coefficient of $P_M(T) = \sum_{i=1}^n P_{M_i/M_{i-1}}(T) = \sum_{i=1}^n P_{R/\mathfrak{q}_i}(T - t_i)$ therefore is given by

$$\sum_Z i(X, H; Z) \cdot \frac{\deg(Z)}{(\xi - 1)!} \cdot T^{\xi - 1} \ . \tag{$*$}$$

If $V(\mathfrak{q}_i)$ is not an irreducible component of $X \cap V(H)$, it is strictly contained in an irreducible component of $X \cap V(H)$, hence of dimension $\leqslant \xi - 2$, and its Hilbert polynomial (by Proposition 3.1.3) is of degree $\leqslant \xi - 2$ and thus doesn't contribute to the $(\xi - 1)^{\text{st}}$ coefficient of P_M. Therefore, $(*)$ is equal to the leading term of P_M. Bézout's theorem follows by comparison of leading coefficients with (#).

It remains to prove Claim 1. We have $M_\mathfrak{q} \cong (R_\mathfrak{q}/HR_\mathfrak{q})$ by the exactness of localization. By more properties of localization, the $R_\mathfrak{q}$-modules $0 = (M_0)_\mathfrak{q} \subseteq \ldots \subseteq (M_k)_\mathfrak{q} = M_\mathfrak{q}$ form a filtration of $M_\mathfrak{q}$ with filtration quotients

$$(M_i)_\mathfrak{q}/(M_{i-1})_\mathfrak{q} \cong (M_i/M_{i-1})_\mathfrak{q} \cong (R/\mathfrak{q}_i[t_i])_\mathfrak{q} \cong (R_\mathfrak{q}/\mathfrak{q}_i R_\mathfrak{q})[t_i]$$

which is zero unless $\mathfrak{q}_i \subseteq \mathfrak{q}$ (using Proposition 3.2.1(b); as $\mathfrak{q}_i$ is homogeneous, it doesn't matter that we only localize at the homogeneous elements of $R \setminus \mathfrak{q}$, which we do by Convention 3.2.1). If $\mathfrak{q}_i \subseteq \mathfrak{q}$ we have $V(\mathfrak{q}_i) \supseteq Z = V(\mathfrak{q})$ and equality occurs as Z is an irreducible component of $X \cap V(H) = \bigcup_{i=1}^k V(\mathfrak{q}_i)$. Hence, $\mathfrak{q} = \mathfrak{q}_i$, when $(M_i/M_{i-1})_\mathfrak{q} \neq 0$ and in this case

$$(M_i/M_{i-1})_\mathfrak{q} \cong (R_\mathfrak{q}/\mathfrak{q}R_\mathfrak{q})[t_i] \ .$$

But $(\mathfrak{q}R_\mathfrak{q})_0$ is the maximal ideal of the local ring $\mathcal{O}_{X,Z} \cong (R_\mathfrak{q})_0$ (using Proposition 1(c)), and $(R_\mathfrak{q})_\ell$ is a free $(R_\mathfrak{q})_0$-module with generator X_j^ℓ if j is chosen such that $X_j \notin \mathfrak{q}$. Therefore,

$$\begin{aligned} i(X, H; Z) \overset{\text{Prop. } 1(c)}{=} \operatorname{length}_{\mathcal{O}_{X,Z}}((M_\mathfrak{q})_d) &= \sum_{i=1}^n \operatorname{length}_{\mathcal{O}_{X,Z}}(((M_i/M_{i-1})_\mathfrak{q})_d) \\ &= \sum_{\mathfrak{q}_i = \mathfrak{q}} \operatorname{length}_{\mathcal{O}_{X,Z}}((R_\mathfrak{q}/\mathfrak{q}R_\mathfrak{q})_{d+t_i}) \\ &= \#\{\mathfrak{q}_i = \mathfrak{q}\} \cdot \operatorname{length}_{(R_\mathfrak{q})_0}((R_\mathfrak{q})_0/(\mathfrak{q}R_\mathfrak{q})_0) \\ &= \#\{\mathfrak{q}_i = \mathfrak{q}\} \end{aligned}$$

using $\operatorname{length}_{(R_\mathfrak{q})_0}((R_\mathfrak{q})_0/(\mathfrak{q}R_\mathfrak{q})_0) = 1$ as the residue field of a local ring is a simple module over that ring. This proves Claim 1. □

3.4. The Samuel polynomial and the principal ideal theorem

Let R be a noetherian ring, M a finitely generated R-module. By Proposition 3.1.2, M has a filtration

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_k = M \ , \tag{1}$$

where $M_i/M_{i+1} \cong R/\mathfrak{p}_i$ with $\mathfrak{p}_i \in \operatorname{Spec} R$ some prime ideals. We'll investigate some properties of such filtrations.

Lemma 1. *Let M be a finitely generated module over any (not necessarily noetherian) ring R, then we have*

$$V(\operatorname{Ann}_R(M)) = \{\mathfrak{p} \in \operatorname{Spec} R \mid M_\mathfrak{p} \neq 0\} \ .$$

Proof. If $\mathfrak{p} \not\supseteq \operatorname{Ann}_R(M)$, there is a $r \in R \setminus \mathfrak{p}$ such that $r \cdot M = 0$, hence $M_\mathfrak{p} = 0$ as r gets inverted in $R_\mathfrak{p}$. Thus the right-hand side is a subset of $V(\operatorname{Ann}_R(M))$ for arbitrary M. Conversely, let $m_1, \ldots, m_k$ generate M. If $M_\mathfrak{p} = 0$, then the image of each m_i in $M_\mathfrak{p}$ is 0. Therefore, there is $r_i \in R \setminus \mathfrak{p}$ such that $r_i m_i = 0$. let $r = \prod_{i=1}^k r_i$, then $r \in R \setminus \mathfrak{p}$ and $r \cdot M = 0$. Hence $\mathfrak{p} \not\supseteq \operatorname{Ann}_R(M)$, showing the inclusion in the other direction. □

Definition 1 (Support)**.** (*a*) The set characterized in the above Lemma 1 is called the **support** $\operatorname{supp}(M)$.

(*b*) For the duration of the next 1 or 2 lectures or so, we set

$$\dim(M) \coloneqq \dim(\operatorname{supp}(M)) \ .$$

Remark. (*a*) As always, let $\dim \emptyset = -\infty$.

(*b*) If $R = k$ is a field, M is a k-vector space and we have

$$\dim(M) = \begin{cases} -\infty & \text{if } M = 0 \\ 0 & \text{otherwise} \end{cases} \ .$$

From now on, let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated R-module.

Fact 1. *The set $\operatorname{supp}(M)$ is Zariski-closed. Let $\operatorname{supp}(M) = \bigcup_{i=1}^\ell V(\mathfrak{q}_i)$ be its decomposition into irreducible components (cf. Proposition A.1.1(b)) and $\mathfrak{Q}_M = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell\}$. Then*

$$\sqrt{\operatorname{Ann}_R(M)} = \bigcap_{\mathfrak{q} \in \mathfrak{Q}_M} \mathfrak{q} \tag{2}$$

hence we have

$$\dim(M) = \max\{\dim(R/\mathfrak{q}) \mid \mathfrak{q} \in \mathfrak{Q}_M\} = \max\{\dim(R/\mathfrak{p}_1), \ldots, \dim(R/\mathfrak{p}_k)\} \ . \tag{3}$$

For any filtration like (1), $\mathfrak{Q}_M$ is equal to the set of $\subseteq$-minimal elements of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$.

Proof. Zariski-closedness follows from $\operatorname{supp}(M) = V(\operatorname{Ann}_R(M))$ by Lemma 1. For any filtration like (1), Fact 3.1.2 gives

$$\sqrt{\operatorname{Ann}_R(M)} = \bigcap_{i=1}^k \mathfrak{p}_k = \bigcap_{\mathfrak{q} \in \mathfrak{Q}} \mathfrak{q} \ ,$$

where $\mathfrak{Q}$ is the set of $\subseteq$-minimal elements of $\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$. Hence $\operatorname{supp} M = \bigcup_{\mathfrak{q}\in\mathfrak{Q}} V(\mathfrak{q})$ where no member of this union contains another, hence it is the decomposition into irreducible components and $\mathfrak{Q} = \mathfrak{Q}_M$ and (2) follows, as well as the right equality of (3).

Moreover, any chain of irreducible subsets of $\operatorname{supp} M$ must be contained in one irreducible component $V(\mathfrak{q})$, hence it must be of the form $V(\mathfrak{q}_0) \subsetneq \dots \subsetneq V(\mathfrak{q}_m)$ with $\mathfrak{q}_i \supseteq \mathfrak{q}$, and such $\mathfrak{q}_i$ define elements $\mathfrak{q}_0/\mathfrak{q} \supsetneq \dots \supsetneq \mathfrak{q}_m/\mathfrak{q}$ of $\operatorname{Spec} R/\mathfrak{q}$. This correspondence can clearly be reversed, showing (3). □

Remark. By the usual correspondence between prime ideals and irreducible subsets, we have

$$\dim M = \sup\{m \mid \text{there is a chain of prime ideals } \operatorname{Ann}_R(M) \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_m\} \ . \quad (4)$$

Fact 2. *If $x \in R \setminus \bigcap_{\mathfrak{q}\in\mathfrak{Q}_M} \mathfrak{q}$, then $\dim(M/xM) < \dim(M)$, unless $\dim(M) = \infty$.*

Proof. We have $\operatorname{Ann}_R(M/xM) \supseteq \operatorname{Ann}_R(M)$, hence $\operatorname{supp}(M/xM) \subseteq \operatorname{supp}(M)$ and therefore $\dim(M/xM) \leqslant \dim(M)$. Moreover, if $\operatorname{Ann}(M/xM) \subseteq \mathfrak{q}_0 \subsetneq \dots \subsetneq \mathfrak{q}_\ell$ is any chain of prime ideals, then $\mathfrak{q}_0 \in \operatorname{supp}(M/xM) \subseteq \operatorname{supp} M$, hence $\mathfrak{q}_0 \in V(\mathfrak{q})$ for some $\mathfrak{q} \in \mathfrak{Q}_M$ but $\mathfrak{q} \subsetneq \mathfrak{q}_0$ as $x \in \mathfrak{q}_0$ but $x \notin \mathfrak{q}$ by our assumption, hence $\dim(M) \geqslant \ell + 1$. □

Definition 2 (Ideal of definition)**.** An **ideal of definition** of R is any ideal I with $\sqrt{I} = \mathfrak{m}$ (the maximal ideal of the local ring R).

Remark. That I is an ideal of definition is equivalent to $V(I) = \{\mathfrak{m}\}$, which is equivalent to $\dim(V(I)) = 0$ which is equivalent to $\dim(R/I) = 0$, which is equivalent to R/I being Artinian (by Proposition 3.1.1(a)) and not equal to 0 (the zero ring).

Fact 3. *If $I \subseteq R$ is any ideal of definition there is a unique polynomial $Q = Q_{M,I}$ such that $\operatorname{length}_R(M/I^kM) = Q(k)$ for any large enough $k \in \mathbb{N}$.*

Proof. Consider the graded ring associated to R and I, i.e.

$$\operatorname{gr}(R, I) = \bigoplus_{k=0}^{\infty} I^k/I^{k+1} \ .$$

Then $\operatorname{gr}_0(R, I) = R/I$ is Artinian (by the previous remark) and $\operatorname{gr}(R, I)$ is generated by $\operatorname{gr}_0(R, I)$ and $\operatorname{gr}_1(R, I)$. Since $\operatorname{gr}_1(R, I)$ is finitely generated over R/I (indeed, as R is noetherian, $I = (x_1, \dots, x_n)_R$ and the x_i mod I^2 generate I/I^2 as an R/I-module), therefore Theorem 18 can be applied to any finitely generated graded $\operatorname{gr}(R, I)$-module. We apply it to the graded module associated to M and I, i.e.

$$\operatorname{gr}(M, I) = \bigoplus_{k=0}^{\infty} I^kM/I^{k+1}M$$

which is generated by the $(\mu_i \bmod IM) \in \operatorname{gr}_0(M, I)$, when M is generated by $\mu_1, \dots, \mu_m$ over R. Hence, there is $P \in \mathbb{Q}[T]$ such that $P(k) = \operatorname{length}_{R/I}(I^kM/I^{k+1}M) = \operatorname{length}_R(I^kM/I^{k+1}M)$, hence

$$\operatorname{length}_R(M/I^{k+1}M) - \operatorname{length}_R(M/I^kM) = \operatorname{length}_R(I^kM/I^{k+1}M) = P(k)$$

when k is sufficiently large. Here we used that by Remark 3.1.1(f), the length behaves additively on the short exact sequence

$$0 \longrightarrow I^k M/I^{k+1}M \longrightarrow M/I^{k+1}M \longrightarrow M/I^k M \longrightarrow 0\ .$$

The assertion now follows from Fact 3.1.1(a). □

Definition 3 (Samuel polynomial)**.** This polynomial $Q = Q_{M,I}$ is called the **Samuel polynomial** of M with respect to I and its degree is denoted by $d(M, I)$. Moreover, let

$$\delta(M, I) = \min\left\{k \;\middle|\; \text{there are } x_1, \ldots, x_k \in I \text{ such that } \operatorname{length}_R\left(M/(x_1 M + \ldots x_k M)\right) < \infty\right\}\ .$$

Remark. (a) We have that $\operatorname{length}_R(N) = \operatorname{length}_{R/J}(N)$, whenever N is an R/J-module and $J \subseteq R$ any ideal. Indeed, each R-submodule of N has J-torsion as well, hence is also an R/J-submodule and conversely any R/J-submodule is automatically an R-submodule (we have seen this argument before at the end of Remark 3.3.1(d)). This was used in the proof of Fact 3 and you should keep it in mind in Definition 3.

(b) In particular, $\operatorname{length}_R(M/IM) = \operatorname{length}_{R/I}(M/IM) < \infty$ by Proposition 3.1.1(d) as R/I is Artinian and M finitely generated over it. Hence $\delta(M, I) < \infty$ as we may e.g. take $x_1, \ldots, x_k$ to be generators of I.

(c) Obviously, $d(M, I) < \infty$.

Theorem 20. *For any ideal of definition I of any noetherian local ring R with maximal ideal $\mathfrak{m}$ and any finitely generated R-module M, we have*

$$\dim(M) = d(M, I) = \delta(M, I)\ .$$

Of course, before proving this, we will give some corollaries.

Corollary 1. *We have* $\dim(M) < \infty$. *In particular, with* $M = R$, $\operatorname{supp} R = V(0) = \operatorname{Spec} R$, *we have* $\dim(R) < \infty$, *when R is a noetherian local ring.*

Corollary 2. *The dimension of any noetherian local ring* $(R, \mathfrak{m})$ *is equal to dimension of its associated graded ring* $\operatorname{gr}(R, \mathfrak{m})$.

Proof. This proof captures only the case where $k = R/\mathfrak{m}$ is algebraically closed and $\operatorname{gr}(R, \mathfrak{m})$ is a domain. For an unconditional proof, cf. Eisenbud, [Eis95, Corollary 12.5].

If $\operatorname{gr}(R, \mathfrak{m})$ has no zero divisors, then it is a graded domain of finite type over $k = R/\mathfrak{m} = \operatorname{gr}_0(R, \mathfrak{m})$, hence $\operatorname{gr}(R, \mathfrak{m}) = k[X_0, \ldots, X_n]/\mathfrak{p}$ with $\mathfrak{p} \subseteq k[X_0, \ldots, X_n]$ a homogeneous prime ideal and $\operatorname{gr}(R, \mathfrak{m})$ corresponds to the graded ring of some projective variety $Y \subseteq \mathbb{P}^n(k)$. Then $\dim \operatorname{gr}(R, \mathfrak{m}) = \dim(C(Y)) = \dim(Y) + 1 = \deg P + 1$ where P is the Hilbert polynomial of Y (using Proposition 3.1.3), hence the same P as in Fact 3 and $\deg Q_{R,\mathfrak{m}} = \deg P + 1$ by Fact 3.1.1(b) and $\deg Q_{R,\mathfrak{m}} = d(R, \mathfrak{m}) = \dim R$ by Theorem 20. □

Corollary 3. *If R is a noetherian local ring and* $\mathfrak{m} = (x_1, \ldots, x_n)_R$, *then* $\dim(R) \leqslant n$.

Proof. We have $\operatorname{length}_R(R/(x_1R + \ldots + x_nR)) = \operatorname{length}_R(R/\mathfrak{m}) = 1 < \infty$, hence $\delta(R, \mathfrak{m}) \leqslant n$ and $\dim(R) \leqslant n$ by Theorem 20. □

Corollary 4. *If R is noetherian local,* $\dim(R)$ *is the minimal number of elements of R generating an ideal of definition J.*

Proof. If $J = (x_1, \ldots, x_n)_R$ is an ideal of definition then $\dim(R) = \delta(R, J) \leqslant n$ as before. Vice versa, if $d = \dim(R) = \delta(R, \mathfrak{m})$, there are $x_1, \ldots, x_d \in R$ such that $\operatorname{length}_R(R/(x_1, \ldots, x_d)_R)$ is finite, hence $J = (x_1, \ldots, x_d)_R$ is an ideal of definition. □

And finally, we are able to prove Theorem 12 and thus also Krull's (who, as we all know from [Alg$_1$], was a *n00b* compared to Grothendieck) principal ideal theorem, Theorem 11, at last!

Corollary 5 (Krull's height theorem)**.** *If R is any noetherian ring and $\mathfrak{p}$ minimal among all prime ideals containing $x_1, \ldots, x_k \in R$, then* $\operatorname{ht}(\mathfrak{p}) \leqslant k$.

Proof. As the prime ideals of the localization $R_\mathfrak{p}$ correspond to the prime ideals contained in $\mathfrak{p}$, its maximal ideal $\mathfrak{m} = \mathfrak{p}R_\mathfrak{p}$ is the only prime ideal containing the images of the x_i in $R_\mathfrak{p}$. Then $V(x_1, \ldots, x_k) = \{\mathfrak{m}\}$ in $\operatorname{Spec} R_\mathfrak{p}$ and $\sqrt{(x_1, \ldots, x_k)_{R_\mathfrak{p}}} = \mathfrak{m}$ hence $I = (x_1, \ldots, x_k)_{R_\mathfrak{p}}$ is an ideal of definition and $\operatorname{ht}(\mathfrak{p}) = \dim R_\mathfrak{p} \leqslant k$ by the previous Corollary 4. □

We now start proving Theorem 20. To do this, we will invoke the famous *Artin–Rees lemma*, which had almost been upgraded to a theorem itself.

Proposition 1 (Artin–Rees)**.** *If R is an noetherian ring, $I \subseteq R$ an ideal, $N \subseteq M$ a submodule of a finitely generated R-module M, then there exists a number $c \in \mathbb{N}_0$ such that*

$$N \cap I^{k+c}M \subseteq I^k N \quad \text{for all } k \geqslant 0\,.$$

Proof. Let

$$B_I R = \left\{ \sum_{k=0}^{\infty} a_k T^k \in R[T] \;\middle|\; a_k \in I^k \right\} \cong R \oplus I \oplus I^2 \oplus \cdots = R \oplus \bigoplus_{n=1}^{\infty} I^n$$

be the *Rees-algebra* (or *blowup-algebra*). One may note, that due to $B_I R$ being a subset of the polynomial ring, in each element all but finitely many a_k have to be 0. This is an R-algebra of finite type, hence noetherian by Hilbert's Basissatz. Indeed, if I is generated by $i_1, \ldots, i_n$ then A is generated over R by $i_1T, \ldots, i_nT$. The module

$$B_I M = \left\{ \sum_{k=0}^{\infty} \mu_k T^k \in M[T] \;\middle|\; \mu_k \in I^k M \right\} \cong M \oplus IM \oplus I^2M \oplus \cdots = \bigoplus_{n=0}^{\infty} I^n M$$

is finitely generated (by $m_1T^0, \ldots, m_\ell T^0$ when $m_1, \ldots, m_\ell$ generate M as an R-module) as an $B_I R$-module. As $B_I R$ is noetherian, $\widehat{N} = N[T] \cap B_I M \subseteq B_I M$ is also finitely generated. Let $n_1T^{c_1}, \ldots, n_sT^{c_s}$ be generators of $\widehat{N}$ over $B_I R$ (decomposing arbitrary generators into

homogeneous components, we may assume that we have generators which are all homogeneous). We claim that the assertion holds for $c = \max\{c_1, \ldots, c_s\}$.

The set of homogeneous elements of degree $k+c$ of $\widehat{N}$ equals $(I^{k+c}M \cap N) \cdot T^{k+c}$ and its elements must be of the form

$$\sum_{j=1}^{s} (a_j T^{k+c-c_j})(n_j T^{c_j})$$

where $a_j \in I^{k+c-c_j} \subseteq I^k$ as $c \geqslant c_j$. The result follows as $a_j n_j \in I^k N$. □

Corollary 6 (This is not Corollary 3)**.** *Let $0 \to M' \to M \to M'' \to 0$ be short exact sequence of finitely generated modules over a noetherian local ring R in which some ideal I of definition has been fixed. Then*

$$d(M, I) = \max\{d(M', I), d(M'', I)\}$$

and if the Samuel polynomials of M' and M have the same degrees and leading coefficients (e.g. because they are isomorphic), then $d(M'', I) < d(M, I)$.

Proof. We have $M'/(I^k M \cap M') \cong (I^k M + M')/I^k M$ by the second isomorphism theorem, which gives a short exact sequence

$$0 \longrightarrow M'/(I^k M \cap M') \longrightarrow M/I^k M \longrightarrow M''/I^k M'' \longrightarrow 0$$

by an easy diagram chase. Hence

$$\operatorname{length}_R(M/I^k M) = \operatorname{length}_R(M''/I^k M'') + \operatorname{length}_R\left(M'/(I^k M \cap M')\right)$$

by Remark 3.1.1(f) and an application of the Artin–Rees lemma (Proposition 1) gives the existence of some constant $c \in \mathbb{N}_0$ such that $I^k M' \subseteq I^k M \cap M' \subseteq I^{k-c} M'$. Then there are surjective maps $M'/I^k M' \twoheadrightarrow M'/(I^k M \cap M') \twoheadrightarrow M'/I^{k-c} M'$, hence their lengths over R must be decreasing in that order and we obtain $Q_{M',I}(k-c) \leqslant \operatorname{length}_R\left(M'/(I^k M \cap M')\right) \leqslant Q_{M',I}(k)$ for k sufficiently large by Fact 3. Thus, for k sufficiently large,

$$Q_{M',I}(k-c) + Q_{M'',I}(k) \leqslant Q_{M,I}(k) \leqslant Q_{M',I}(k) + Q_{M'',I}(k)$$

and if $d = \max\{d(M', I), d(M'', I)\}$, then both the left-hand and the right-hand side are polynomials of degree d. It follows that $\deg Q_{M,I} = d$ as well.

If $Q_{M,I}$ and $Q_{M',I}$ have the same degree and leading coefficient, then so have the polynomials $Q_{M',I}(T-c)$ and $Q_{M,I}(T)$, hence $Q_{M'',I}(k) \leqslant Q_{M,I}(k) - Q_{M',I}(k-c) = O(k^{d-1})$ as $k \to \infty$ (note that this O is *Landau notation* and no structure sheaf thingy). Then the degree of $Q_{M'',I}$ must be $\leqslant d-1$. □

Corollary 7 (This is also not Corollary 4)**.** *Applying this to (1) we obtain*

$$d(M, I) = \max\left\{d(R/\mathfrak{q}, I) \mid \mathfrak{q} \in \mathfrak{Q}_M\right\} .$$

Proof. By (1) and an inductive application of Corollary 6 the left hand side equals

$$\max\{d(R/\mathfrak{p}_i, I) \mid 1 \leqslant i \leqslant k\}$$

(as in (1)) but the $\mathfrak{q} \in \mathfrak{Q}_M$ are the $\subseteq$-minimal elements of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ and if $\mathfrak{p}_i \supseteq \mathfrak{q}$ we have $R/\mathfrak{q} \twoheadrightarrow R/\mathfrak{p}_i$, hence $\operatorname{length}_R(R/(I^k + \mathfrak{q})) \geqslant \operatorname{length}_R(R/(I^k + \mathfrak{p}_i))$, hence $d(R/\mathfrak{p}_i, I) \leqslant d(R/\mathfrak{q}, I)$. □

Corollary 8 (Krull's intersection theorem)**.** *If R is a local noetherian ring with maximal ideal $\mathfrak{m}$, $I \subseteq R$ a proper ideal and M a finitely generated R-module, then*

$$\bigcap_{k=0}^{\infty} I^k M = 0\,.$$

Proof. Let N be this intersection. By Artin–Rees (Proposition 1), there is a $c \in \mathbb{N}_0$ such that $\mathfrak{m}N \supseteq IN \supseteq I^{c+1}M \cap N = N$. Then $N = 0$ by [NAK]. □

Remark. In particular, $\bigcap_{k=0}^{\infty} \mathfrak{m}^k = 0$, which is the version we proved in the lecture. However, we need it in full generality for the proof of Theorem 20, which follows now.

Proof of Theorem 20. Step 1. First we show $\dim(M) \leqslant d(M, I)$ by induction on $d(M, I)$. When $d(M, I) = 0$ the lengths of M/I^kM are bounded as $k \to \infty$ by some constant C independent of k, hence $\operatorname{length}_R(M) \leqslant C$.

Well, the last assertion is not so trivial as it seems at first glance. The problem here is that $\operatorname{length}_R(M/I^kM) = Q_{M,I}(k) \leqslant C$ only holds for k sufficiently large. So a priori there's no control over $\operatorname{length}_R(M)$, i.e. $k = 0$. The following elegant workaround was suggested to us by `jckt`. First note that $\operatorname{length}_R(M/I^kM)$ is monotonic in k. Indeed, $I^kM \supseteq I^{k+1}M$, hence M/I^kM is a quotient of $M/I^{k+1}M$ and $\operatorname{length}_R(M/I^kM) \leqslant \operatorname{length}_R(M/I^{k+1}M)$. Moreover, as long as $I^kM \supsetneq I^{k+1}M$ this inequality is strict. So we deduce that $I^kM = I^{k+1}M$ for k sufficiently large. Then we also have $I^kM = \mathfrak{m}I^kM$, hence $I^kM = 0$ by [NAK]. Thus $\operatorname{length}_R(M) = \operatorname{length}_R(M/I^kM) \leqslant C$, as was claimed.

Hence $\operatorname{length}_R(R/\mathfrak{p}_i) \leqslant C$ in (1), hence all $R/\mathfrak{p}_i$ are Artinian and thus zero-dimensional by Proposition 3.1.1. Therefore $\dim(M) = \max\{\dim(R/\mathfrak{p}_i) \mid 1 \leqslant i \leqslant k\} = 0$ using (3).

Now let $d(M, I) \geqslant 1$ and let the assertion be proved for all R-modules N with $d(N, I) < d(M, I)$. By (3) and Corollary 7 it is sufficient to deal with the case $M = R/\mathfrak{p}$ with $\mathfrak{p} \in \operatorname{Spec} R$ a prime ideal. Let $\mathfrak{p} \subseteq \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_s$ a chain of prime ideals contained in $\operatorname{supp}(M)$, then we may select $x \in \mathfrak{q}_1 \setminus \mathfrak{q}_0 \subseteq \mathfrak{q}_1 \setminus \mathfrak{p}$. Then x is no zero-divisor in $M = R/\mathfrak{p}$ and $\mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_s$ are still contained in $\operatorname{supp}(M/xM)$ hence $\dim(M/xM) \geqslant s - 1$, but the short exact sequence $0 \to M \xrightarrow{\cdot x} M \to M/xM \to 0$ and Corollary 6 show $d(M/xM, I) < d(M, I)$. Thus $s \leqslant d(M, I)$.

Corollary (*Yes*, a corollary inside a proof, deal with it, I also have to)**.** *The finite-dimensionality of R has now been established.*

Step 2. We now show $d(M,I) \leqslant \delta(M,I)$. We do induction on $\delta(M,I)$. If $\delta(M,I) = 0$, then $\operatorname{length}_R(M) < \infty$ and $Q_{M,I}(k) \leqslant \operatorname{length}_R(M)$ for sufficiently large k, proving that $Q_{M,I}$ must be constant and $d(M,I) \leqslant 0$.

Now let $\delta(M,I) = n \geqslant 1$ and the assertion be valid for finitely generated R-modules N with $\delta(N,I) < n$. We have $x_1, \ldots, x_n \in I$ such that $\operatorname{length}_R\left(M/(x_1M + \ldots + x_nM)\right) < \infty$. Hence $\operatorname{length}_R\left(N/(x_1N + \ldots + x_{n-1}N)\right) < \infty$ where $N = M/x_nM$. It follows that $\delta(N,I) \leqslant n-1$. But

$$0 \longrightarrow x_nM/(x_nM \cap I^kM) \longrightarrow M/I^kM \longrightarrow N/I^kN \longrightarrow 0$$

is a short exact sequence and $\operatorname{length}_R\left(x_nM/(x_nM \cap I^kM)\right) \leqslant \operatorname{length}_R(M/I^{k-1}M)$ as $M \xrightarrow{\cdot x_n} x_nM$ induces a surjective map $M/I^{k-1}M \twoheadrightarrow x_nM/(x_nM \cap I^kM)$. It follows that

$$Q_{N,I}(k) \geqslant Q_{M,I}(k) - Q_{M,I}(k-1) \quad \text{for } k \text{ sufficiently large}$$

and if $Q_{M,I}(k) = \gamma k^d + O(k^{d-1})$ with $\gamma \neq 0$ then $Q_{M,I}(k) - Q_{M,I}(k-1) = \gamma d k^{d-1} + O(k^{d-2})$. Hence $d(N,I) \geqslant d(M,I) - 1$ and $d(M,I) \leqslant d(N,I) + 1 \leqslant \delta(N,I) + 1 \leqslant n = \delta(M,I)$.

Corollary (*facepalm*)**.** *The principal ideal theorem of Krull and its consequences follow.*

Step 3. To end the proof, we have to show $\delta(M,I) \leqslant \dim(M)$. We do induction on $\dim(M)$. If $\dim(M) = 0$, all $\mathfrak{p}_i$ in (1) are maximal, hence $\operatorname{length}_R(M) < \infty$ and $\delta(M,I) = 0$.

Now let $\dim(M) \geqslant 1$ and the assertion be valid for R-modules of lower dimension. Choose an element $x_1 \in I \backslash \bigcup_{\mathfrak{q} \in \mathfrak{Q}_M} \mathfrak{q}$. This is possible by prime avoidance (Lemma 3.1.2) as $I \subseteq \mathfrak{q}$ for $\mathfrak{q} \in \mathfrak{Q}_M$ would imply $\mathfrak{m} = \sqrt{I} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{q}$ which is impossible since $\dim M \geqslant 1$ and $\mathfrak{q}$ is $\subseteq$-minimal. Let $N = M/x_1M$ then $\sqrt{\operatorname{Ann}_R(N)} = \sqrt{x_1R + \bigcap_{\mathfrak{q} \in \mathfrak{Q}_M} \mathfrak{q}}$ (this is because ... well ... let's see after the proof), hence $\operatorname{supp}(N) \subseteq \operatorname{supp}(M)$, hence any $\mathfrak{r} \in \mathfrak{Q}_N$ contains some $\mathfrak{q} \in \mathfrak{Q}_M$ but $\mathfrak{r} \neq \mathfrak{q}$ as $x_1 \in \mathfrak{r}$ and $x_1 \notin \mathfrak{q}$. Thus, every irreducible component of $\operatorname{supp} N$ is strictly contained in some irreducible component of $\operatorname{supp} M$. Thus $\delta(N,I) \leqslant \dim(N) < \dim(M)$ and if $d = \dim(M)$ there are $x_2, \ldots, x_d \in I$ such that $\operatorname{length}_R\left(M/(x_1M + \ldots + x_dM)\right) = \operatorname{length}_R\left(N/(x_2N + \ldots + x_dN)\right) < \infty$, hence $\delta(M,I) \leqslant \dim(M)$. □

To finish the proof, we only need to note that $\operatorname{supp}(N) \subseteq \operatorname{supp}(M)$ is a trivial consequence of N being a quotient of M. But a more precise statement can be made and shall be made as it is – as Professor Franke would say – perhaps worthwhile to know.

Lemma 2. *Let R be an arbitrary ring (i.e. commutative, but neither necessarily noetherian nor local). Let $I \subseteq R$ be an ideal and M a finitely generated R-module. Then*

$$\sqrt{\operatorname{Ann}_R(M/IM)} = \sqrt{I + \operatorname{Ann}_R(M)}\,.$$

Remark. Note that the obvious-seeming stronger relation $\operatorname{Ann}_R(M/IM) = I + \operatorname{Ann}_R(M)$ may fail, even for well-behaved rings. Here's a counterexample[1].

[1] taken from https://math.stackexchange.com/questions/79538/annihilator-of-quotient-module-m-im

Let $R = k[x, y] \subseteq k[t]$ where k is a field, $x = t^2$, $y = t^3$. Let $M = k[t]$. It is finitely generated over R (a system of generators is $1, t$). Let $I = (x) \subseteq R$. Then $IM = t^2 k[t]$ and $yM = t^3 k[t] \subseteq IM$. So $y \in \operatorname{Ann}_R(M/IM)$. But $y \notin I$, contradiction!

Localizing everything at the maximal ideal $(x, y) \subseteq R$ should also give a counterexample in the local case, I think, but I haven't checked all details.

The following proof was suggested to us by Felix and is a lot shorter and more elegant than ours, so it shall be presented here.

Proof of Lemma 2. We may equivalently prove $V(\operatorname{Ann}_R(M/IM)) = V(I + \operatorname{Ann}_R(M))$. Applying Lemma 1 to the finitely generated R-module M/IM, we have

$$V(\operatorname{Ann}_R(M/IM)) = \{\mathfrak{p} \in \operatorname{Spec} R \mid (M/IM)_\mathfrak{p} \neq 0\} = \{\mathfrak{p} \in \operatorname{Spec} R \mid IM_\mathfrak{p} \subsetneq M_\mathfrak{p}\} \ .$$

Note that by Nakayama's Lemma in the form of Corollary 1.2.2 we have $IM_\mathfrak{p} \subsetneq M_\mathfrak{p}$ iff $(IR_\mathfrak{p} + \mathfrak{p}R_\mathfrak{p})M_\mathfrak{p} \subsetneq M_\mathfrak{p}$. Now this is the case iff $IR_\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p}$ (since $IR_\mathfrak{p} = R_\mathfrak{p}$ otherwise, $\mathfrak{p}R_\mathfrak{p}$ being the maximal ideal of the local ring $R_\mathfrak{p}$) and $\mathfrak{p}M_\mathfrak{p} \subsetneq M_\mathfrak{p}$. The first condition is equivalent to $I \subseteq \mathfrak{p}$. Indeed, if $I \subseteq \mathfrak{p}$, then clearly $IR_\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p}$. Conversely, if $IR_\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p}$, then $I \subseteq IR_\mathfrak{p} \cap R \subseteq \mathfrak{p}R_\mathfrak{p} \cap R = \mathfrak{p}$ (note that the first inclusion may be proper in general).

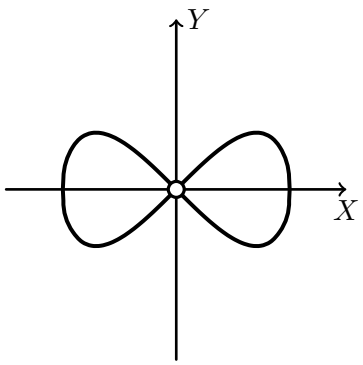
For the second condition, again by Nakayama's lemma (in its [NAK] version) we have $\mathfrak{p}M_\mathfrak{p} \subsetneq M_\mathfrak{p}$ iff $M_\mathfrak{p} \neq 0$. Thus, we get

$$\begin{aligned} V(\operatorname{Ann}_R(M/IM)) &= \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p} \text{ and } M_\mathfrak{p} \neq 0\} = V(I) \cap \operatorname{supp}(M) \\ &= V(I + \operatorname{Ann}_R(M)) \ , \end{aligned}$$

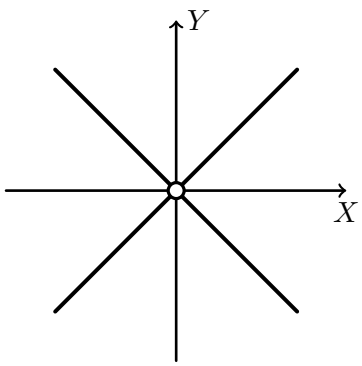
where we applied Lemma 1 to M. We are done. □

Recall that for a noetherian local ring R with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$, the dimension $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ equals the minimal number of generators of $\mathfrak{m}$ and $\dim(R) \leqslant \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ (cf. Proposition 1.3.1). If equality occurs, R is called *regular*.

Example. Consider the curves given by the ideals $(Y^2 - X^2 + X^4)$ and $(Y^2 - X^2)$ in $k[X, Y]$ over a field k of characteristic not equal to 2. Similar to the example on page 12, both have *singularities* in the origin.



$Y^2 = X^2 - X^4$



$Y^2 = X^2$

One would intuitively expect, that there are always singularities, where irreducible components meet or where the stalk of the structure sheaf has any non-zero zero-divisors. The following corollary shows that this is indeed the case

Corollary 9. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$. Suppose that R is regular of dimension d.*

(a) *If $\mu_1, \ldots, \mu_d$ generate $\mathfrak{m}$ then*

$$\begin{aligned} k[X_1, \ldots, X_d] &\longrightarrow \operatorname{gr}(R, \mathfrak{m}) \\ X_1^{\alpha_1} \cdots X_d^{\alpha_d} &\longmapsto \mu_1^{\alpha_1} \cdots \mu_d^{\alpha_d} \bmod \mathfrak{m}^{|\alpha|+1} \end{aligned}$$

(where $|\alpha| = \alpha_1 + \ldots + \alpha_d$ and $\alpha \in \mathbb{N}_0^d$) is an isomorphism.

(b) *R is a domain.*

Proof. Obviously the homomorphism from (a) is well-defined and it is surjective. Indeed, the μ_i generate $\mathfrak{m}$ as an ideal, hence the $\mu_1^{\alpha_1} \cdots \mu_d^{\alpha_d}$ for $|\alpha| = k$ generate $\mathfrak{m}^k$ as an ideal. If the map failed to be injective, there would be a homogeneous $P \in S = k[X_1, \ldots, X_n]$ contained in the kernel.

Let P be homogeneous of degree e and H denote the Hilbert polynomial of $S/(P)$. Multiplying by P gives an isomorphism $S_\ell \xrightarrow{\sim} P \cdot S_\ell = (P)_{\ell+e}$. Then the Hilbert polynomial of (P) equals that of S shifted by $-e$. In particular, both have the same degree $d-1$ (by Lemma 3.0.1) and the same leading coefficient. Then H, being the difference of these two via the short exact sequence $0 \to (P) \to S \to S/(P) \to 0$, has degree $\deg H < d-1$. As $S/(P) \twoheadrightarrow \operatorname{gr}(R, \mathfrak{m})$ is surjective, $\operatorname{length}_R(\mathfrak{m}^\ell/\mathfrak{m}^{\ell+1}) = \dim_k(\mathfrak{m}^\ell/\mathfrak{m}^{\ell+1}) \leqslant H(\ell)$ for large ℓ and it follows that the Samuel polynomial of R has degree smaller then d, a contradiction to Theorem 20 and $\dim(R) = d$. This shows (a).

To prove (b), first note that $R \neq 0$ as the zero ring is not local. Assume $f, g \in R \setminus \{0\}$ and $fg = 0$. By the Krull intersection lemma (Corollary 8) there are minimal exponents $n, \ell \geqslant 0$ such that $f \notin \mathfrak{m}^{n+1}$, $g \notin \mathfrak{m}^{\ell+1}$. Then $\overline{f} = f \bmod \mathfrak{m}^{n+1} \neq 0$ in $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ and $\overline{g} = g \bmod m^{\ell+1} \neq 0$ in $\mathfrak{m}^\ell/\mathfrak{m}^{\ell+1}$ and $fg \bmod \mathfrak{m}^{n+\ell+1} = \overline{f} \cdot \overline{g}$ in $\operatorname{gr}_{n+\ell}(R, \mathfrak{m})$. By (a) and because $k[X_1, \ldots, X_d]$ is a domain this does not vanish, a contradiction. □

3.5. One-dimensional regular rings

Definition 1 (Discrete valuation valuation ring)**.** A **discrete valuation valuation ring** (now with 100% more valuation!!) is a domain R with a function $v\colon R \to \mathbb{N}_0 \cup \{\infty\}$ (called the *valuation*) such that

(a) $v(x) = \infty$ iff $x = 0$.

(b) $v(xy) = v(x) + v(y)$

(c) $v(x+y) \geqslant \min\{v(x), v(y)\}$ (there should be a min even if Professor Franke is tenacious in using max)

(*d*) If $v(x) \geqslant v(y)$, then y divides x.

(*e*) There is $x \in R$ with $v(x) = 1$.

Remark 1. (*a*) Definition 1(*a*) can be deduced from the rest. Let $v(x) = 1$, then $v(0) = v(0 \cdot x) = v(0) + v(x) = v(0) + 1$, implying $v(0) \notin \mathbb{N}$.

(*b*) It easily follows $v(\varepsilon) = 0$ for $\varepsilon \in R^\times$. Hence $v(x) = v(-x)$ and $v(x) = v(x + y - y) \geqslant \min\{v(x + y), v(y)\}$ showing equality in (*c*), when $v(x) \neq v(y)$.

(*c*) Ordered groups other than $\mathbb{Z}$ (e.g $\mathbb{Z} \times \mathbb{Z}$ ordered lexicographically) may be considered as target of the valuation, giving a more general notion. But these will fail to be noetherian, unless they are discrete valuation rings.

Definition 2 (Normal ring)**.** A domain R is called **normal** if it is integrally closed in its field of quotients K.

Recall that $x \in K$ is in the integral closure of R in K iff there is a finitely generated R-submodule $M \neq 0$ of K such that $x \cdot M \subseteq M$ iff there is an R-subalgebra $C \subseteq K$ such that $x \in C$ and C is finitely generated as an R-module (we proved this on exercise sheet #10).

Definition 3 (Fractional ideal)**.** A **fractional ideal** of a domain R is an R-submodule $I \subseteq K$ with $aI \subseteq R$ for some $a \in R \setminus \{0\}$. We put $I^{-1} = \{x \in K \mid xI \subseteq R\}$. The ideal I is called **invertible** iff $I \cdot I^{-1} = R$.

If $0 \neq I \subseteq K$ is any R-submodule, then I^{-1} is a fractional ideal (in particular, this holds when I is fractional itself). Indeed, I always contains an element $r \in R \setminus \{0\}$ (take the numerator of any nonzero element of I) and then $rI^{-1} \subseteq R$ by definition of I^{-1}. The invertible fractional ideals thus form a group under ideal multiplication. If R is noetherian, the fractional ideals are precisely the finitely generated R-submodules of K.

Proposition 1. *A fractional ideal I is invertible iff it is finitely generated and $I_\mathfrak{p} = I \cdot R_\mathfrak{p}$ is a principal fractional ideal of $R_\mathfrak{p}$ (i.e. of the form $\alpha_\mathfrak{p} R_\mathfrak{p}$ for some $\alpha_\mathfrak{p} \in K$) for any $\mathfrak{p} \in \operatorname{Spec} R$.*

Proof. If I is invertible, there are $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in I^{-1}$ such that $\sum_{i=1}^n a_i b_i = 1$. If $J = (a_1, \ldots, a_n)$ denotes the ideal generated by $a_1, \ldots, a_n$, then also $JI^{-1} = R$, hence $J = JI^{-1}I = I$ and the a_i generate I (similarly, the b_i generate I^{-1}, so I^{-1} is also finitely generated). If $\mathfrak{p} \in \operatorname{Spec} R$ there is an i such that $a_i b_i \notin \mathfrak{p}$, hence $a_i b_i \in R_\mathfrak{p}^\times$. Thus $b_i I_\mathfrak{p}$ contains a unit, but is also contained in $R_\mathfrak{p}$ as $b_i \in I^{-1}$. Then $b_i I_\mathfrak{p} = R_\mathfrak{p}$ and $I_\mathfrak{p} = a_i b_i I_\mathfrak{p} = a_i R_\mathfrak{p} = (a_i)$, i.e. $I_\mathfrak{p}$ is a principal ideal.

Conversely, assume that I is finitely generated and all localizations $I_\mathfrak{p}$ are principal. We clearly have $I^{-1} \cdot R_\mathfrak{p} \subseteq I_\mathfrak{p}^{-1}$ where equality holds when I is finitely generated. Since $I_\mathfrak{p}$ is principal, clearly $I_\mathfrak{p} \cdot I_\mathfrak{p}^{-1} = R_\mathfrak{p}$, hence the inclusion $I \cdot I^{-1} \hookrightarrow R$ becomes an isomorphism after localization at any $\mathfrak{p} \in \operatorname{Spec} R$. But any such morphism of R-modules is an isomorphism. □

Lemma 1. *Let R be a normal local domain with finitely generated maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}$ is invertible or $\mathfrak{m}^{-1} = R$.*

Proof. Since $R \subseteq \mathfrak{m}^{-1}$ we have $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}^{-1} \subseteq R$. Hence $\mathfrak{m}$ is invertible or $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$. In the latter case, for any $x \in \mathfrak{m}^{-1}$, we have $x\mathfrak{m} \subseteq \mathfrak{m}$ hence x is in the integral closure of R by what was recalled before. □

Theorem 21. *For a noetherian local ring R of positive dimension, the following are equivalent:*

(*a*) *R is a discrete valuation ring (DVR from now on).*

(*b*) *R is a principal ideal domain (PID from now on).*

(*c*) *The maximal ideal $\mathfrak{m}$ is a principal ideal.*

(*d*) *R is one-dimensional regular.*

(*e*) *R is a one-dimensional normal domain.*

Proof. Assume (*a*). If $I \subseteq R$ is not 0 and $x \in I$ is such that $v(x)$ is minimal, then it is easy to see that $I = (x) = \{r \in R \mid v(r) \geqslant v(x)\}$. So every ideal in R is principal, hence (*a*) $\Rightarrow$ (*b*).

The implication from (*b*) to (*c*) is trivial.

Now assume (*c*), we want to show (*c*) $\Rightarrow$ (*a*). Let $v(x) = \sup\{k \in \mathbb{N} \mid x \in \mathfrak{m}^k\}$. By Krull's intersection theorem (Corollary 3.4.8), $v(x) = \infty$ iff $x = 0$. Let $\mathfrak{m} = (\pi)$, then $\mathfrak{m}^k = (\pi^k)$. In particular, π is not nilpotent, as otherwise $\mathfrak{m}$ would be nilpotent, i.e. $\mathfrak{m} = \mathrm{nil}(R)$. But $\mathrm{nil}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$ (by Proposition 1.2.1) shows that $\mathfrak{m}$ is the only prime ideal of R and $\dim R = 0$ – contradiction! Now v satisfies $x \in (\pi^{v(x)})$ for all $x \in R \setminus \{0\}$, and it follows that $v(xy) = v(x) + v(y)$, that R is a domain and all the further properties of a DVR are easily verified.

The points (*d*) and (*c*) are obviously equivalent as equality occurs in $1 \leqslant \dim(R) \leqslant \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ iff $\mathfrak{m}$ can be generated by a single element (cf. the proof of Proposition 1.3.1).

Now assume (*a*), we want to show (*a*) $\Rightarrow$ (*e*). The valuation v extends to a map $v\colon K \to \mathbb{Z} \cup \{\infty\}$ in the obvious way and still satisfies the conditions from Definition 1. Moreover, we will have $R = \{x \in K \mid v(x) \geqslant 0\}$. Let $x \in K$ be integral over R, say $x^n = \sum_{i=0}^{n-1} r_i x^i$ with $r_i \in R$. Then

$$nv(x) \geqslant \min\left\{v\left(r_i x^i\right) \;\middle|\; 0 \leqslant i \leqslant n\right\} \geqslant \min\{0, (n-1)v(x)\}$$

(as $r_i \in R$, hence $v(r_i) \geqslant 0$). Hence $v(x) \geqslant 0$, that is, $x \in R$, showing that R is normal. One-dimensionality follows as we already know (*a*) $\Leftrightarrow$ (*d*).

Finally, let's prove (*e*) $\Rightarrow$ (*c*). We will show that $\mathfrak{m}$ is invertible, which suffices thanks to Proposition 1. Assume not, then $\mathfrak{m}^{-1} = R$ by Lemma 1. Let $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. We deduce from the proof of Lemma 3.1.1 (applied to the R-module R/xR) that there is a $y \in R$ such that $v = y \bmod xR \in R/xR$ satisfies $\mathrm{Ann}_R(v) = \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} R$. Then $\mathfrak{p} = \{r \in R \mid ry \subseteq xR\}$ is not 0 as $x \in \mathfrak{p}$. As $\dim(R) = 1$ this implies $\mathfrak{p} = \mathfrak{m}$. Now let $a = y/x \in K$, then $a \notin R$ as $y \in (x)$ and $\mathrm{Ann}_R(v) = R$ otherwise. But $y \in \mathfrak{m}^{-1}$ because for $\mu \in \mathfrak{m} = \mathfrak{p}$ we have $\mu y \in (x)$ hence $\mu a = (\mu y)/x \in R$. This contradicts $\mathfrak{m}^{-1} = R$. □

Theorem 22. *For a domain R the following are equivalent.*

(*a*) *Any ideal $I \neq 0$ is invertible.*

(*b*) *Any fractional ideal is invertible.*

(*c*) *R is noetherian and for any non-zero $\mathfrak{p} \in \operatorname{Spec} R$, the localization $R_\mathfrak{p}$ is a field or a DVR.*

(*d*) *R is a field or one-dimensional noetherian normal.*

(*e*) *R is a field or one-dimensional noetherian regular.*

(*f*) *Any ideal of R may be written as a product of prime ideals.*

In fact, the decomposition in (f) is for ideals not equal to 0 unique up to reordering and the group of fractional ideals is free with the non-zero prime ideals as generators.

Definition 4 (Dedekind rings)**.** Such R are called **Dedekind domains**. If J_R is the group of fractional ideals of R and P_R its subgroup of principal fractional ideals, then $\mathrm{Cl}_R = J_R/P_R$ is called the **class group** of R.

Proof of Theorem 22. If R is a field, all assertions are more or less trivially fulfilled, so let us assume R is not a field.

The implication $(b) \Rightarrow (a)$ is trivial. For $(a) \Rightarrow (b)$, let I be any fractional ideal. Then there is some $r \in R \setminus \{0\}$ such that $rI \subseteq I$. Then $(rI)^{-1} = r^{-1}I^{-1}$ is easily checked, and the invertibility of rI implies

$$R = (rI)(rI)^{-1} = rIr^{-1}I^{-1} = rr^{-1}II^{-1} = II^{-1}.$$

Hence I is invertible.

Now for $(a) \Rightarrow (c)$. As invertibility for fractional ideals is equivalent to being finitely generated and locally principal (by Proposition 1), (a) implies that any ideal is finitely generated, hence R is noetherian. If $\mathfrak{p} \in \operatorname{Spec} R$ and $\mathfrak{p} \neq 0$, then $\mathfrak{p}R_\mathfrak{p}$ is principal again by Proposition 1, $\mathfrak{p}$ being invertible. Hence $R_\mathfrak{p}$ is a DVR by Theorem 21.

The converse implication $(c) \Rightarrow (a)$ also follows from Proposition 1 and the fact that DVRs are always PIDs.

Let's prove $(c) \Rightarrow (d)$. It is clear that R is noetherian, and $\dim R \leqslant 1$ follows easily from $\dim R_\mathfrak{p} \leqslant 1$ for all $\mathfrak{p} \in \operatorname{Spec} R$ (using (c) and Theorem 21). We still have to show R is normal.

We have seen that DVRs are normal. For any domain R, we have $R = \bigcap_{\mathfrak{m} \in \mathfrak{m}\text{-Spec}\, R} R_\mathfrak{m}$ (the intersection being taken in the field of fractions K). Indeed, if $x \in K$ is in the intersection, then $I = \{r \in R \mid rx \in R\}$ is an ideal of R not contained in any maximal ideal $\mathfrak{m}$ (as $x \notin R_\mathfrak{m}$ otherwise), hence $I = R$ and $x \in R$. Now if $x \in K$ is integral over R and R satisfies (c), it is integral over each localization $R_\mathfrak{m}$ hence contained in $R_\mathfrak{m}$ (as the $R_\mathfrak{m}$ are DVRs), hence contained in $\bigcap_\mathfrak{m} R_\mathfrak{m} = R$.

Now $(d) \Rightarrow (e)$. Normality is easily seen to be preserved under localization, hence the $R_\mathfrak{m}$ are normal, hence regular by Theorem 21. Similarly, $(e) \Rightarrow (c)$ is an immediate consequence of Theorem 21 as well.

We prove $(c) \Rightarrow (f)$. Let $I \neq 0$ be any ideal of R. For any maximal ideal $\mathfrak{p} \in \mathfrak{m}\text{-Spec}\, R$, we have $I \cdot R_\mathfrak{p} = aR_\mathfrak{p}$ for some $a \in R_\mathfrak{p}$. Put $v_\mathfrak{p}(I) = v_\mathfrak{p}(a)$ where $v_\mathfrak{p} \colon K \to \mathbb{Z} \cup \{\infty\}$ is the function on K defined by the valuation $v_\mathfrak{p}$ of $R_\mathfrak{p}$. We claim that $I = \prod_{\mathfrak{p} \in \mathfrak{m}\text{-Spec}\, R} \mathfrak{p}^{v_\mathfrak{p}(I)}$. Indeed, we only

have to check that both sides agree in any localization $R_\mathfrak{q}$ at a maximal prime $\mathfrak{q} \in \mathfrak{m}\text{-Spec}\, R$. To check this,

$$\left(\prod_{\mathfrak{p}\in\mathfrak{m}\text{-Spec}\, R} \mathfrak{p}^{e_\mathfrak{p}}\right) \cdot R_\mathfrak{q} = \prod_\mathfrak{p} (\mathfrak{p}R_\mathfrak{q})^{e_\mathfrak{p}} = (\mathfrak{q}R_\mathfrak{q})^{e_\mathfrak{q}}\,,$$

since $\mathfrak{p}R_\mathfrak{q} = R_\mathfrak{q}$ when $\mathfrak{p} \neq \mathfrak{q}$ because both $\mathfrak{p}$ and $\mathfrak{q}$ are maximal ideals, so $\mathfrak{p} \not\subseteq \mathfrak{q}$. It follows that $v_\mathfrak{q}\left(\prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}\right) = e_\mathfrak{q}$. As $I\cdot R_\mathfrak{p}$ is uniquely determined by $v_\mathfrak{p}(I)$, it follows that $I\cdot R_\mathfrak{q} = \left(\prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(I)}\right)\cdot R_\mathfrak{q}$ for any $\mathfrak{n} \in \mathfrak{m}\text{-Spec}\, R$ and we are done as explained above. Uniqueness of the decomposition also follows from these considerations.

In the lecture, we proved $(f) \Rightarrow (c)$ under the assumption that R is noetherian, but actually we also silently assumed R to be one-dimensional, for which there seems to be no quick proof from (f) directly. Instead, we will present a proof for $(f) \Rightarrow (a)$, which is taken from [MR89, pp. 83-84].

Step 1. First note that if I and J are fractional ideals such that $\mathfrak{a} = IJ$ is invertible, then so are I and J. Indeed, we have $I^{-1}J^{-1}\mathfrak{a} \subseteq R$, hence $I^{-1}J^{-1} \subseteq \mathfrak{a}^{-1}$. Moreover, from $\mathfrak{a}^{-1}IJ \subseteq R$ we get $\mathfrak{a}^{-1}I \subseteq J^{-1}$ and $\mathfrak{a}^{-1}J \subseteq I^{-1}$. Multiplying the latter equations together and using that $\mathfrak{a}$ is invertible, we see that $\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\left(\mathfrak{a}^{-1}IJ\right) \subseteq I^{-1}J^{-1}$, hence $\mathfrak{a}^{-1} = I^{-1}J^{-1}$. Then

$$R = \mathfrak{a}^{-1}IJ = (II^{-1})(JJ^{-1})$$

and this can't happen unless $II^{-1} = JJ^{-1} = R$.

Step 2 (this will be the most technical of all). Let $\mathfrak{p}$ be a non-zero prime ideal and $I \supsetneq \mathfrak{p}$ an ideal strictly containing $\mathfrak{p}$, then $\mathfrak{p}I = \mathfrak{p}$. Clearly, it suffices to consider the case $I = \mathfrak{p} + (\alpha)$ for some $\alpha \in R \setminus \mathfrak{p}$. The trick is to prove $I^2 = \mathfrak{p} + (\alpha^2)$, from which the claim can be deduced as follows. As $I^2 = (\alpha^2) + \alpha\mathfrak{p} + \mathfrak{p}^2$ and this equals $\mathfrak{p} + (\alpha^2)$, any $x \in \mathfrak{p}$ has a representation $x = y + \alpha z + \alpha^2 t$ with $y \in \mathfrak{p}^2$, $z \in \mathfrak{p}$ and $t \in R$. As $\alpha \notin \mathfrak{p}$, we must have $t \in \mathfrak{p}$, thus the right-hand side is an element of $\mathfrak{p}((\alpha) + \mathfrak{p}) = I\mathfrak{p}$. Since clearly $\mathfrak{p}I \subseteq \mathfrak{p}$, this shows $\mathfrak{p}I = \mathfrak{p}$.

To show $I^2 = \mathfrak{p} + (\alpha^2)$, let $I^2 = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ and $\mathfrak{p} + (\alpha^2) = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ be decompositions of them into (not necessarily distinct) prime ideals. Let $\overline{\alpha}$ and $\overline{\mathfrak{p}}_i, \overline{\mathfrak{q}}_j$ be the images of α and the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ in $R/\mathfrak{p}$, then

$$\overline{\mathfrak{p}}_1 \cdots \overline{\mathfrak{p}}_m = \overline{\alpha}^2 R/\mathfrak{p} = \overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_n\,. \tag{$*$}$$

Let w.l.o.g. $\overline{\mathfrak{p}}_1$ be $\subseteq$-minimal among the $\overline{\mathfrak{p}}_i$. By primality, some of the $\overline{\mathfrak{q}}_j$ must be contained in $\overline{\mathfrak{p}}_1$, say, $\overline{\mathfrak{q}}_1 \subseteq \overline{\mathfrak{p}}_1$. But $\overline{\mathfrak{q}}_1$ is prime as well, hence $\overline{\mathfrak{p}}_i \subseteq \overline{\mathfrak{q}}_1 \subseteq \overline{\mathfrak{p}}_1$ for some i and by $\subseteq$-minimality we must have $\overline{\mathfrak{p}}_i = \overline{\mathfrak{p}}_1$. Hence $\overline{\mathfrak{p}}_1 = \overline{\mathfrak{q}}_1$. Also note that the $\overline{\mathfrak{p}}_i$ and $\overline{\mathfrak{q}}_j$ are invertible, since the principal ideal $\overline{\alpha}^2 R/\mathfrak{p}$ is clearly invertible and we may apply Step 1. Multiplying $(*)$ by $\overline{\mathfrak{p}}_1^{-1} = \overline{\mathfrak{q}}_1^{-1}$ we get $\overline{\mathfrak{p}}_2 \cdots \overline{\mathfrak{p}}_m = \overline{\mathfrak{q}}_2 \cdots \overline{\mathfrak{q}}_n$. Iterating this process gives $m = n$ and the $\overline{\mathfrak{p}}_i$ and $\overline{\mathfrak{q}}_j$ coincide. Then so do the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ and $I^2 = \mathfrak{p} + (\alpha^2)$ follows.

Step 3. Let $\alpha \in R$ and $(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ be a decomposition into prime ideals. Then all occurring $\mathfrak{p}_i$ are maximal. Indeed, if $I \supsetneq \mathfrak{p}_i$ for some i and some ideal $I \subseteq R$, then $\mathfrak{p}_i I = \mathfrak{p}_i$ by Step 2. Now $\mathfrak{p}_i$ is invertible by Step 1 (since (α) clearly is) and multiplying by $\mathfrak{p}_i^{-1}$ yields $I = R$.

Step 4. Let $\mathfrak{p}$ be a non-zero prime ideal. Then $\mathfrak{p}$ is maximal and invertible. Indeed, take a $0 \neq \alpha \in \mathfrak{p}$ and consider its factorization $(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. By Step 3, each $\mathfrak{p}_i$ is maximal, but their

product is also contained in $\mathfrak{p}$, hence $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i which must be an equality by maximality of $\mathfrak{p}_i$. Since (α) is invertible, so is $\mathfrak{p}$ by Step 1. As every ideal of R can be decomposed into primes, every non-zero ideal is invertible and we obtain $(f) \Rightarrow (a)$. □

3.6. Relation with intersection multiplicities

Let $C \subseteq \mathbb{P}^2$ be a curve in the projective plane which is regular at $c \in C$: By Theorem 21, $\mathcal{O}_{C,c}$ is a DVR. Let $v_c : \mathcal{O}_{C,c} \to \mathbb{N}_0 \cup \{\infty\}$ be its valuation. If $\mathcal{L}$ is a line bundle on C and $l \in \mathcal{L}(U)$, where $U \subseteq C$ is an open neighbourhood of c, we put $v_c(l) = v_c\left(\frac{l}{\lambda}\right)$, where λ is any generator of the free $\mathcal{O}_{C,c}$-module $\mathcal{L}_c$ of rank 1 and the image of l in $\mathcal{L}_c$ was also denoted l.

Note that for any DVR R and $r \in R$, we have $\text{length}_R(R/rR) = v(r)$ (where v is the valuation of R). Indeed, if $r = 0$, both sides are ∞. Otherwise, we have $r = \varepsilon\pi^k$ where $\pi \in R$ is a *uniformizer* (i.e. $v(\pi) = 1$) and $\varepsilon \in R^\times$ and $k = v(r)$. Then $R/rR = R/\pi^k R$ has a filtration by the submodules $\pi^i R/\pi^k R$ for $i = 0, \dots k$. The filtration quotients $(\pi^i R/\pi^k R)/(\pi^{i+1} R/\pi^k R) \cong R/\pi R$ are simple R-modules (they are fields after all), thus proving $\text{length}_R(R/rR) = v(r)$.

For the above C and c, it follows that $v_c(f) = \text{length}_R(\mathcal{O}_{C,c}/f\mathcal{O}_{C,c})$ hence

$$v_c(l) = v_c\left(\frac{l}{\lambda}\right) = \text{length}_R\left(\mathcal{O}_{C,c} \Big/ \frac{l}{\lambda}\mathcal{O}_{C,c}\right) = \text{length}_R(\mathcal{L}_c/l\mathcal{O}_{C,c})$$

as multiplication by λ induces an isomorphism $\lambda\cdot\colon \mathcal{O}_{C,c}/\frac{l}{\lambda}\mathcal{O}_{C,c} \xrightarrow{\sim} \mathcal{L}_c/l\mathcal{O}_{C,c}$. It follows that

$$i(C, H; \{c\}) = v_c(H),$$

where H is any homogeneous polynomial of degree d, viewed as an element of $\mathcal{O}_{\mathbb{P}^2(k)}(d)(\mathbb{P}^2(k))$ and restricted to C, giving a section of $\mathcal{L} = \mathcal{O}_C(d)$. This can also be applied to any $C \subseteq \mathbb{P}^n(k)$ of codimension one at any $Z \subseteq C$ of codimension one in C such that $\mathcal{O}_{C,Z}$ is a DVR.

Theorem 23. (a) *If $C \subseteq \mathbb{P}^2(k)$ is a regular curve, then $k[X_0, X_1, X_2]_d \to \mathcal{O}_C(d)(C)$ is surjective.*

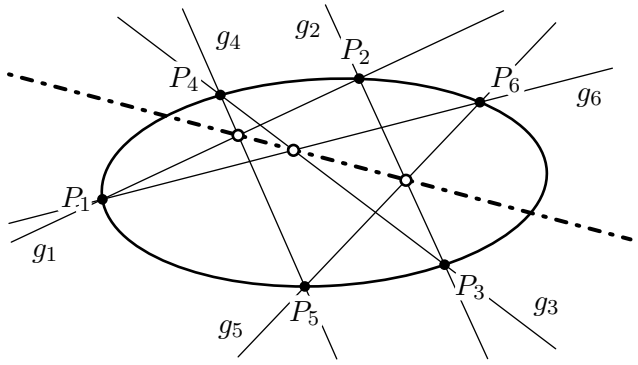
(b) (Restsatz, M. Noether) *Let $C \subseteq \mathbb{P}^2(k)$ be a curve and $H \in k[X_0, X_1, X_2]$ be a polynomial of homogeneous degree h not vanishing identically on C. Let moreover $c_1, \dots, c_{h \deg C}$ be the elements of $V(H) \cap C$ (occurring with the respective multiplicities).*

If $E \in k[X_0, X_1, X_2]_e$ with $0 < e < h$ is such that $c_1, \dots, c_{e \deg C}$ are the elements of $C \cap V(E)$ (by multiplicity), then there is some $F \in k[X_0, X_1, X_2]_f$ with $e + f = h$ and the remaining $f \deg C$ points $c_{1+e \deg C}, \dots, c_{h \deg C}$ are precisely the elements $V(F) \cap C$ (by multiplicity).

Example. Let $Q \subseteq \mathbb{P}^2(k)$ be a conic and $P_1, \dots, P_6$ different points and g_i the straight line connecting P_i with P_{i+1} (where $P_7 := P_1$). Then the intersections $g_1 \cap g_4, g_2 \cap g_5$ and $g_3 \cap g_6$ (which maybe do not exist in the *affine* plane, but do so in the *projective* plane) are on a line (the *Pascal line*).

To prove this, consider $C = g_1 \cup g_3 \cup g_5 \subseteq \mathbb{P}^2$ (this is not irreducible, hence not a variety, but nevermind) and H the polynomial of degree 3 defining $g_2 \cup g_4 \cup g_6$. Then $C \cap V(H) \supseteq \{P_1, \dots, P_6\}$

lying on Q, a curve on degree 2. By the Restsatz, Theorem 23(b), the remaining intersection points of C and H must be contained in a line.



The Pascal line of an ellipse.

Sketch of proof of Theorem 23, finishing the final lecture in a hurry and five minutes overtime. We first prove $(a) \Rightarrow (b)$. We have $v_c(H|_C) = i(C, H; \{c\}) \geqslant i(C, E; \{c\}) = v_c(E|_C)$ at all points where E fails to be a local generator of $\mathcal{O}_C(e)$ (i.e. at all points of $V(E) \cap C$, otherwise E is invertible on a small neighbourhood) by assumption. Hence there is a preimage $\frac{H|_C}{E|_C}$ of $H|_C \in \mathcal{O}_C(h)(C)$ under the map $\mathcal{O}_C(f) \xrightarrow{\cdot E} \mathcal{O}_C(f+e) = \mathcal{O}_C(h)$. By (a), there is a polynomial F in 3 variables such that $F|_C = \frac{H|_C}{E|_C}$, so $H = FE$ on C. Then F has the required properties and $i(C, H; \{c\}) = i(C, E; \{c\}) + i(C, F; \{c\})$ as the multiplicities depend only on $H|_C$.

To prove (a), one notes the the result can be shown to hold when d is large (cf. exercise sheet #10, exercise 6). We show that the result for $d+1$ implies the result for d. Let $\varphi \in \mathcal{O}_C(d)$ and let $L \neq 0$ be any linear polynomial such that $C \cap V(L)$ contains only regular points of C (this is where the proof becomes very sketchy. e.g. pick a regular point $p \in C$, then choose L such that $i(V(L), C; \{p\}) = \deg C$). Let, e.g., $L = X_0$ (this is possible after a suitable automorphism of $\mathbb{P}^2(k)$) and let $L\varphi = G|_C$ where $G \in k[X_0, X_1, X_2]_{d+1}$. Using the intersection multiplicities one shows that $i(V(L), G; \{l\}) \geqslant i(V(L), C; \{l\})$ for any $l \in V(L) = V(X_0) \cong \mathbb{P}^1(k)$. It follows that $G|_{V(L)}$ is divisible by $P|_{V(L)}$ (where P is the irreducible polynomial defining C) in $k[X_1, X_2] \cong k[X_0, X_1, X_2]/(X_0)$. Hence $G = AP + BX_0$ and $\varphi X_0 = BX_0$ on C, such that $\varphi = B$ there. □

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 [Alg$_1$] – and that's also where you should go if you want to see proofs for the below results).

Definition 1 ([Alg$_1$, 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 satisfies 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 ([Alg$_1$, Definition 2.1.3])**.** A topological space $X \neq \emptyset$ is **irreducible** if it satisfies 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 $1 \leqslant i \leqslant n$ such that $X = X_i$.

Proposition 1. (*a*) *Any subset of a noetherian topological space is noetherian with its induced subspace topology.*

(*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 $i \neq j$, called the* **irreducible components** *of X.*

Proof. Part (*a*) is [Alg$_1$, Remark 2.2.1] and (*b*) is [Alg$_1$, Proposition 2.1.1]. □

Definition 3 ([Alg$_1$, Definition 2.1.4])**.** Let X be a topological space, $Z \subseteq X$ irreducible and closed. We put

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

The number $\dim(X)$ is known as the **Krull dimension** of X.

Example 1 ([Alg$_1$, 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

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

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 ([Alg$_1$, 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

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

(cf. [Alg$_1$, 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. [Alg$_1$, Proposition 2.1.2]).

Remark 1 ([Alg$_1$, Remark 2.1.3])**.** In general, for $A \subseteq B \subseteq C \subseteq X$

$$\operatorname{codim}(A, B) + \operatorname{codim}(B, C) \leqslant \operatorname{codim}(A, C) \tag{1}$$
$$\operatorname{codim}(A, X) + \dim(A) \leqslant \dim(X) \ . \tag{2}$$

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

Theorem A ([Alg$_1$, 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 $P \in K[X_1, \ldots, X_n]$ and pairwise different $s_1, \ldots, s_n \in S$,

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

A *transcendence basis* of L/K is a subset $S \subseteq L$ which is algebraically independent over K and such that $L/K(s_1, \ldots, s_n)$ is algebraic. The **transcendence degree** $\operatorname{tr.deg} L/K$ 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, [Alg$_1$, 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 $p, q \in k[X_1, \ldots, X_n]$ 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 $R = k[X_1, \ldots, X_n] \to \mathcal{O}(X)$ is surjective.*

In [Alg$_1$, 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 $\mathcal{O}(X) \cong R/\mathfrak{p}$. 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 occurring in such a contains a non-empty open subset of X, cf. [Alg$_1$, 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. [Alg$_1$, 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 ([Alg$_1$, Theorem 6]). *If $X \subseteq k^n$ is locally closed and irreducible, then*

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

Moreover, X is catenary and equality always holds in (2), i.e. $\dim(Y) + \mathrm{codim}(Y, X) = \dim(X)$ 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 $\dim k^n \geqslant n$ since we have the chain

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

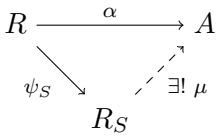
of irreducible closed subsets. To prove $\dim(k^n) \leqslant n$, and $\dim(X) \leqslant \mathrm{tr.deg}(K(X)/k)$, one proves $\mathrm{tr.deg}(\mathfrak{K}(\mathfrak{p})/k) > \mathrm{tr.deg}(\mathfrak{K}(\mathfrak{q})/k)$ whenever A/k is an algebra of finite type over k, $\mathfrak{q} \supsetneq \mathfrak{p}$ 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 [Alg$_1$, 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. [Alg$_1$, 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 $\left\{ \frac{m}{s} \mid m \in Ma, s \in S \right\}/_\sim$ 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. [Alg$_1$, 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*

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

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*

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

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*

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

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

(*e*) *We have $P_{x,L/K} = \mathrm{Min}_{x/K}^{[L:K(x)]}$. 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 $P_{x,E/K} = \mathrm{Min}_{x/K}$ since x is a zero of the left hand side by Cayley–Hamilton and $\deg P_{x,E/K} = [E : K] = [K(x) : K] = \deg(x/K) = \deg \mathrm{Min}_{x/K}$ 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 $\mathrm{Mat}_{\mathcal{B}}(f) = (f_{i,j})_{i,j=1}^m$ 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

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

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

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

if $f_{i,j} = 0$ for all $i > j$, as in that case, $\mathrm{Mat}_{\mathcal{B}}(f)$ and hence also $\mathrm{Mat}_{\widetilde{\mathcal{B}}}(f)$ are upper triangular (block) matrices . But that's no problem since we can always choose $\mathcal{B}$ in such a way that $\mathrm{Mat}_{\mathcal{B}}(f)$ 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 $\mathrm{Min}_{x/K}$ is separable. Thus, $d = e$ and $\mathrm{Min}_{x/K} = (T - x_1) \cdots (T - x_e)$ since the zeros of $\mathrm{Min}_{x/K}$ 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 $\mathrm{Min}_{x/K} = \mu(T^{p^k})$. Indeed, if $\mathrm{Min}_{x/K}$ is irreducible but not separable, then its derivative must be the zero polynomial, hence each monomial of $\mathrm{Min}_{x/K}$ is a power of T^p and $\mathrm{Min}_{x/K} = \mu_1(T^p)$ for some polynomial $\mu \in K[T]$. Iterating this argument, we eventually 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 $0 = \mathrm{Min}_{x/K}(x_i) = \mu(x_i^{p^k})$, hence $x_i^{p^k}$ must be some of the y_j for each $i \leqslant e$. 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 $\mathrm{Min}_{x/K}(\eta) = \mu(y_i) = 0$ 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,

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

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 $\mathrm{Min}_{x/K}$ is separable and thus $\mathrm{Min}_{x/K} = T - x$ as $e = 1$. Then $x \in K$. By (d), in characteristic $p > 0$, there is a non-negative integer k such that $\mathrm{Min}_{x/K} = (T - x)^{p^k} = T^{p^k} - x^{p^k}$, hence $x^{p^k} \in K$. □

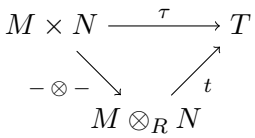
A.4. Tensor products of modules over a ring

Definition 1. Let M and N be modules over the (commutative) ring R. Let $\mathrm{Bil}_R(M, N; T)$ 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 $t \in \mathrm{Hom}_R(M \otimes_R N, T)$ such that the following diagram commutes.



Remark 1. (*a*) It is easy to see that this characterizes $M \otimes_R N$ 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

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

It's easy to check that this works. □

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.

$$\begin{array}{ccc} M & \xrightarrow{\quad\tau\quad} & T \\ & {\scriptstyle 1\otimes -}\searrow \quad \nearrow{\scriptstyle \exists!\, t} & \\ & A \otimes_R M & \end{array}$$

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

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

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 $- \otimes_R N\colon \mathbf{Mod}(R) \to \mathbf{Mod}(R)$ 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.

Fact 2. *Also, note that if $A = R/I$ where $I \subseteq R$ is some ideal, then*

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

is an isomorphism.

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

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

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

A.5. Sheaves

Definition 1 (Presheaf)**.** A **presheaf** $\mathcal{G}$ (with values in the category $\boldsymbol{A}$ of sets, groups, rings, etc.) on a topological space X associates

- every open subset $U \subseteq X$ with an object $\mathcal{G}(U) \in \mathrm{Ob}(\boldsymbol{A})$ (called the set (group, ring, etc.) of *sections* of $\mathcal{G}$ on U)
- and for every inclusion $V \subseteq U$ of open subsets, a morphism $(-)|_V \colon \mathcal{G}(U) \to \mathcal{G}(V)$ such that $g|_U = g$ when $g \in \mathcal{G}(U)$ and such that $(g|_V)|_W = g|_W$ for open $W \subseteq V \subseteq U$ and $g \in \mathcal{G}(U)$.

This can also be expressed as $\mathcal{G}$ being a *functor* from the category of open subsets of X (the inclusions being the morphisms) to the given category.

Definition 2 (Sheaf)**.** A presheaf $\mathcal{G}$ is called **sheaf** if it fulfills the so called *sheaf axiom*, i.e. if for any open cover $U = \bigcup_{i\in I} U_i$ of an open subset $U \subseteq X$,

$$\begin{aligned} \mathcal{G}(U) &\longrightarrow \left\{ (g_i)_{i\in I} \in \prod_{i\in I} \mathcal{G}(U_i) \;\middle|\; g_i|_{U_i\cap U_j} = g_j|_{U_i\cap U_j} \text{ for } i,j \in I \right\} \\ g &\longmapsto (g|_{U_i})_{i\in I} \end{aligned}$$

is bijective.

In general, this map is always well-defined but may fail to be bijective. If it is injective at least, $\mathcal{G}$ is called a **separated** presheaf.

Remark 1. (*a*) The sheaf axiom is interesting even if $I = \emptyset$ when it implies that $\mathcal{G}(\emptyset) = 0$ (if $\mathcal{G}$ is a sheaf of groups or rings).

(*b*) A typical example is the sheaf of k-valued functions on X, associating to any $U \subseteq X$ the rings of k-valued functions on U. Normally, one considers *subsheaves* defined by conditions like being locally constant, C^∞, holomorphic, regular in some sense and so on.

(*c*) Our definitions of $\mathcal{O}(Z)$ or $\mathcal{O}(d)(Z)$ can be applied to any subset $Z \subseteq \mathbb{P}^n(k)$. When $Z = \emptyset$, it gives $\mathcal{O}(Z) = 0$ (or $\mathcal{O}(d)(Z) = 0$) with the empty function as the only element. When Z is quasi-projective, $\mathcal{O}$ is sheaf of rings (a subsheaf of the sheaf of k-valued functions on Z) and $\mathcal{O}(d)\colon U \mapsto \mathcal{O}(d)(U)$ is a sheaf of modules.

Professor Franke would like to point out that the following definition being given here is in *no way*, by *any chance*, related to the recent appearance of this very definition in his other lecture Algebraic Geometry I.

Definition 3 (Sheaf of modules)**.** A **sheaf of modules** over a sheaf of rings $\mathcal{R}$ on X is a sheaf $\mathcal{M}$ on X of abelian groups together with maps

$$\begin{aligned} \mathcal{R}(U) \times \mathcal{M}(U) &\longrightarrow \mathcal{M}(U) \\ (\rho, \mu) &\longmapsto \rho \cdot \mu \end{aligned}$$

defining the structure of an $\mathcal{R}(U)$-module on $\mathcal{M}(U)$ and such that $(\rho\cdot\mu)|_V = (\rho|_V)\cdot(\mu|_V)$ when $V \subseteq U$ are open subsets of X, $\mu \in \mathcal{M}(U)$, $\rho \in \mathcal{R}(U)$. A sheaf of modules is **locally free** of rank n if every $x \in X$ has a neighbourhood U such that $\mathcal{M}|_U \cong (R|_U)^n$. When $n = 1$ this is called a *line bundle*.

Definition 4 (Prevariety)**.** A **prevariety** over an algebraically closed field k is a noetherian, irreducible topological space X together with a subsheaf $\mathcal{O}_X$ of the sheaf of k-valued functions on X such that

- any $x \in X$ has an open neighbourhood U for which there is a homeomorphism $U \xleftarrow[\varphi]{\sim} V \subseteq k^n$ where V is an affine variety in k^n
- and such that a k-valued function λ on the open subset $W \subseteq U$ satisfies $\lambda \in \mathcal{O}_X(W)$ if and only if $\varphi^*\lambda = (y \mapsto \lambda(\varphi(y))$ defines an element of $\mathcal{O}_V(\varphi^{-1}(W))$.

A **morphism** $X \xrightarrow{f} Y$ of prevarieties is a continuous map such that for any open $V \subseteq Y$ and any $\lambda \in \mathcal{O}_Y(V)$, $f^*\lambda$ is an element of $\mathcal{O}_X(f^{-1}V)$.

A **variety** is a prevariety X with the additional property that for any prevariety and any pair $X \overset{a}{\underset{b}{\rightrightarrows}} Y$ or morphisms, $\mathrm{Eq}(a,b) = \{x \in X \mid a(x) = b(x)\}$ is a closed subset of X.

Remark 2. The n in the above definition is *not* required to be constant, not even for a single $x \in X$. In fact, this wouldn't be a sensible thing to ask for, as e.g. $k \subseteq k^1$ and $k \times \{0\} \subseteq k^2$ are isomorphic affine varieties. However, the *Krull dimension* $\dim X$ (in the sense of Definition A.1.3) is a well-defined thing and one can show that $\dim X = \dim V$ in the above situation (this is a consequence of [Alg$_1$, Theorem 6] and the *locality of codimension*, cf. Remark 1.1.1(a) or [Alg$_1$, Remark 2.1.3]).

Remark 3. Recall that a topological space T is Hausdorff (of T_2) iff the following equivalent conditions hold

(a) Any two different points in T have disjoint open neighbourhoods.

(b) The *diagonal* $\Delta = \{(t,t) \mid t \in T\}$ is a closed subset of $T \times T$.

(c) For any pair $S \overset{a}{\underset{b}{\rightrightarrows}} T$ of continuous maps, $K = \mathrm{Eq}(a,b) = \{t \in T \mid a(t) = b(t)\}$ is closed in T.

Note that (c) reminds strongly of the *separateness* condition for varieties in Definition 4, except that we restrict S to be a prevariety and a, b morphisms of prevarieties there.

Definition 5 (Stalk)**.** The **stalk** at $x \in X$ of a presheaf $\mathcal{F}$ on the topological space X is $\mathcal{F}_x$ is the set of pairs (U, α) of open neighbourhoods U of x and $\alpha \in \mathcal{F}(U)$ modulo the equivalence relation $\sim$. This relation is defined by $(U,\alpha) \sim (V,\beta)$ iff there is an open neighbourhood $W \subseteq U \cap V$ of x such that $\alpha|_W = \beta|_W$. The group (ring) operations $* \in \{+, \cdot\}$ are given as follows: If $a = (U,\alpha)/_\sim$ and $b = (V,\beta)/_\sim$ are elements of $\mathcal{F}_x$, then

$$a * b = (W, (\alpha|_W) * (\beta|_W))/_\sim$$

where W is any open neighbourhood of x contained in $U \cap V$. This gives $\mathcal{F}_x$ a structure of a group (ring, etc.) if $\mathcal{F}$ is of the appropriate type of sheaves. When $\mathcal{M}$ is an $\mathcal{R}$-module, $\mathcal{M}_x$ gets the structure of an $\mathcal{R}_x$-module in the same way.

Remark 4. Let $X \subseteq k^n$ be quasi-affine and $\mathcal{O}$ be its structure sheaf. When $f = (U,\varphi)/_\sim \in \mathcal{O}_x$, $f(x) \coloneqq \varphi(x)$ is independent of its representative. When $f(x) \neq 0$, $f \in \mathcal{O}_x^\times$ as $U \setminus V(\varphi)$ is an open neighbourhood of x in U and $\varphi|_{U \setminus V(\varphi)} \in \mathcal{O}(U \setminus V(\varphi))^\times$. It follows that $\mathcal{O}_x \setminus \mathcal{O}_x^\times$ is the kernels of the homomorphism $\mathcal{O}_x \to k$, $f \mapsto f(x)$ an hence an ideal, i.e. $\mathcal{O}_x$ is a local ring.

As the construction of stalks is local[1], $\mathcal{O}_{X,x}$ is a local ring with maximal ideal $\mathfrak{m}_{X,x} = \{f \in \mathcal{O}_{X,x} \mid f(x) = 0\}$ for any prevariety X and any $x \in X$.

Remark 5. It turns out that the quasi-affine and quasi-projective varieties are varieties in the sens of Definition 4.

[1] Pun not intended.

Bibliography

[AG_2] F. Wagner. *Algebraic Geometry II by Jens Franke (lecture notes)*. GitHub: https://github.com/Nicholas42/AlgebraFranke/tree/master/AlgGeoII.

[Alg_1] N. Schwab and F. Wagner. *Algebra I by Jens Franke (lecture notes)*. GitHub: https://github.com/Nicholas42/AlgebraFranke/tree/master/AlgebraI.

[Eis95] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995. ISBN: 978-0-387-94269-8. URL: http://xavirivas.com/cloud/Commutative%20Algebra/Eisenbud%20-%20Commutative%20algebra,%20with%20a%20view%20toward%20algebraic%20geometry%20(Springer,%20GTM150)(T)(778s).pdf.

[Kun86] 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.

[MR89] 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.hawaii.edu/%7Epavel/cmi/References/Matsumura_Commutative_Theory.pdf.

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