Algebra I

Lecturer
Prof. Dr. Jens Franke

Notes
Josia Pietsch

Version
October 21, 2023 20:35

Contents

Warning. *This is not an official script. There is no guarantee for completeness or correctness.*

$\mathfrak{k}$ is always an algebraically closed field and $\mathfrak{k}^n$ is equipped with the Zariski-topology. Fields which are not assumed to be algebraically closed have been renamed (usually to $\mathfrak{l}$).

1 Finiteness conditions

1.1 Finitely generated and Noetherian modules

Definition 1.1 (Generated submodule)**.** Let R be a ring, M an R-module, $S \subseteq M$. Then the following sets coincide

1. $$\left\{ \sum_{s \in S'} r_s \cdot s \mid S \subseteq S' \text{ finite}, r_s \in R \right\},$$

2. $$\bigcap_{\substack{S \subseteq N \subseteq M \\ N \text{submodule}}} N,$$

3. The $\subseteq$-smallest submodule of M containing S.

This subset of $N \subseteq M$ is called the **submodule of M generated by S**. If $N = M$ we say that **M is generated by S**. M is finitely generated $:\iff \exists S \subseteq M$ finite such that M is generated by S.

Definition 1.2 (Noetherian R-module)**.** M is a **Noetherian** R-module if the following equivalent conditions hold:

1. Every submodule $N \subseteq M$ is finitely generated.
2. Every sequence $N_0 \subseteq N_1 \subseteq \ldots$ of submodules terminates.
3. Every set $\mathfrak{M} \neq \varnothing$ of submodules of M has a $\subseteq$-largest element.

Proposition 1.3 (Hilbert's Basissatz)**.** If R is a Noetherian ring, then the polynomial rings $R[X_1, \ldots, X_n]$ in finitely many variables are Noetherian.

1.1.1 Properties of finite generation and Noetherianness

Fact 1.3.1 (Properties of Noetherian modules)**.**

1. Every Noetherian module over an arbitrary ring is finitely generated.
2. If R is a Noetherian ring, then an R-module is Noetherian iff it is finitely generated.
3. Every submodule of a Noetherian module is Noetherian.

Proof.

1. By definition, M is a submodule of itself. Thus it is finitely generated.
2. Since M is finitely generated, there exists a surjective homomorphism $R^n \to M$. As R is Noetherian, R^n is Noethrian as well.

3. trivial

□

Fact 1.3.2. Let M, M', M'' be R-modules.

1. Suppose $M \xrightarrow{p} M''$ is surjective. If M is finitely generated (resp. Noetherian), then so is M''.

2. Let $M' \xrightarrow{f} M \xrightarrow{p} M'' \to 0$ be exact. If M' and M'' are finitely generated (reps. Noetherian), so is M.

Proof. 1. Consider a sequence $M''_0 \subseteq M''_1 \subseteq \ldots \subseteq M''$. Then $p^{-1}M''_i$ yields a strictly ascending sequence. If M is generated by $S, |S| < \omega$, then M'' is generated by $p(S)$.

2. Because of 1. we can replace M' by $f(M')$ and assume $0 \to M' \xrightarrow{f} M \xrightarrow{p} M'' \to 0$ to be exact. The fact about finite generation follows from Einführung in die Algebra.

   If M', M'' are Noetherian, $N \subseteq M$ a submodule, then $N' := f^{-1}(N)$ and $N'' := p(N)$ are finitely generated. Since $0 \to N' \to N \to N'' \to 0$ is exact, N is finitely generated.

□

1.2 Ring extensions of finite type

Definition 1.4 (R-algebra)**.** Let R be a ring. An R-algebra (A, α) is a ring A with a ring homomorphism $R \xrightarrow{\alpha} A$. α will usually be omitted. In general α is not assumed to be injective.

An R-subalgebra is a subring $\alpha(R) \subseteq A' \subseteq A$.
A morphism of R-algebras $A \xrightarrow{f} \tilde{A}$ is a ring homomorphism with $\tilde{\alpha} = f\alpha$.

Definition 1.5 (Generated (sub)algebra, algebra of finite type)**.** Let (A, α) be an R-algebra.

$$\begin{aligned} \alpha : R[X_1, \ldots, X_m] &\longrightarrow A[X_1, \ldots, X_m] \\ P = \sum_{\beta \in \mathbb{N}^m} p_\beta X^\beta &\longmapsto \sum_{\beta \in \mathbb{N}^m} \alpha(p_\beta) X^\beta \end{aligned}$$

is a ring homomorphism. We will sometimes write $P(a_1, \ldots, a_m)$ instead of $(\alpha(P))(a_1, \ldots, a_m)$.

Fix $a_1, \ldots, a_m \in A^m$. Then we get a ring homomorphism $R[X_1, \ldots, X_m] \to$

A. The image of this ring homomorphism is the R-subalgebra of A **generated by the a_i**. A is **of finite type** if it can be generated by finitely many $a_i \in I$.

For arbitrary $S \subseteq A$ the subalgebra generated by S is the intersection of all subalgebras containing S
= the union of subalgebras generated by finite $S' \subseteq S$
= the image of $R[X_s | s \in S]$ under $P \mapsto (\alpha(P))(S)$.

1.3 Finite ring extensions

Definition 1.6 (Finite ring extension)**.** Let R be a ring and A an R-algebra. A is a module over itself and the ringhomomorphism $R \to A$ allows us to derive an R-module structure on A. A **is finite over** R / the R-algebra A is finite / A/R is finite if A is finitely generated as an R-module.

Fact 1.6.3 (Basic properties of finiteness)**.**

A Every ring is finite over itself.

B A field extension is finite as a ring extension iff it is finite as a field extension.

C A finite $\implies$ A of finite type.

D A/R and B/A finite $\implies$ B/R finite.

Proof.

A 1 generates R as a module

B trivial

C Let A be generated by $a_1, \ldots, a_n$ as an R-module. Then A is generated by $a_1, \ldots, a_n$ as an R-algebra.

D Let A be generated by $a_1, \ldots, a_m$ as an R-module and B by $b_1, \ldots, b_n$ as an A-module. For every b there exist $\alpha_j \in A$ such that $b = \sum_{j=1}^{n} \alpha_j b_j$. We have $\alpha_j = \sum_{i=1}^{m} \rho_{ij} a_i$ for some $\rho_{ij} \in R$ thus $b = \sum_{i=1}^{m} \sum_{j=1}^{n} \rho_{ij} a_i b_j$ and the $a_i b_j$ generate B as an R-module.

□

1.4 Determinants and Caley-Hamilton

This generalizes some facts about matrices to matrices with elements from commutative rings with 1. [1]

[1] Most of this even works in commutative rings without 1, since 1 simply can be adjoined.

Definition 1.7 (Determinant)**.** Let $A = (a_{ij}) \in \mathrm{Mat}(n, n, R)$. We define the determinant by the Leibniz formula

$$\det(A) := \sum_{\pi \in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)}.$$

Define $\mathrm{Adj}(A)$ by $\mathrm{Adj}(A)^T_{ij} := (-1)^{i+j} \cdot M_{ij}$, where M_{ij} is the determinant of the matrix resulting from A after deleting the i^{th} row and the j^{th} column.

Fact 1.7.4.

1. $\det(AB) = \det(A)\det(B)$.
2. Development along a row or column works.
3. Cramer's rule: $A \cdot \mathrm{Adj}(A) = \mathrm{Adj}(A) \cdot A = \det(A) \cdot \mathbf{1}_n$. A is invertible iff $\det(A)$ is a unit.
4. Caley-Hamilton: If $P_A = \det(T \cdot \mathbf{1}_n - A)$[a], then $P_A(A) = 0$.

[a] $T \cdot \mathbf{1}_n - A \in \mathrm{Mat}(n, n, A[T])$

Proof. All rules hold for the image of a matrix under a ring homomorphism if they hold for the original matrix. The converse holds in the case of injective ring homomorphisms. Caley-Hamilton was shown for algebraically closed fields in LA2 using the Jordan normal form. Fields can be embedded into their algebraic closure, thus Caley-Hamilton holds for fields. Every domain can be embedded in its field of quotients $\implies$ Caley-Hamilton holds for domains.

In general, A is the image of $(X_{i,j})_{i,j=1}^{n} \in \mathrm{Mat}(n, n, S)$ where $S := \mathbb{Z}[X_{i,j} | 1 \leqslant i, j \leqslant n]$ (this is a domain) under the morphism $S \to A$ of evaluation defined by $X_{i,j} \mapsto a_{i,j}$. Thus Caley-Hamilton holds in general. □

1.5 Integral elements and integral ring extensions

Proposition 1.8 (on integral elements)**.** Let A be an R-algebra, $a \in A$. Then the following are equivalent:

A $\exists n \in \mathbb{N}, (r_i)_{i=0}^{n-1}, r_i \in R : a^n = \sum_{i=0}^{n-1} r_i a^i$.

B There exists a subalgebra $B \subseteq A$ finite over R and containing a.

If $a_1, \ldots, a_k \in A$ satisfy these conditions, there is a subalgebra of A finite over R and containing all a_i.

Definition 1.9. Elements that satisfy the conditions from 1.8 are called **integral over** R. A/R is **integral**, if all $a \in A$ are integral over R. The set of elements of A integral over R is called the **integral closure** of R in A.

Proof.

B $\implies$ A Let $a \in A$ such that there is a subalgebra $B \subseteq A$ containing a and finite over R. Let $(b_i)_{i=1}^n$ generate B as an R-module.

$$\begin{aligned} q : R^n &\longrightarrow B \\ (r_1, \dots, r_n) &\longmapsto \sum_{i=1}^n r_i b_i \end{aligned}$$

is surjective. Thus there are $\rho_i = (r_{i,j})_{j=1}^n \in R^n$ such that $ab_i = q(\rho_i)$. Let $\mathfrak{A}$ be the matrix with the ρ_i as columns. Then for all $v \in R^n$: $q(\mathfrak{A} \cdot v) = a \cdot q(v)$. By induction it follows that $q(P(\mathfrak{A}) \cdot v) = P(a)q(v)$ for all $P \in R[T]$. Applying this to $P(T) = \det(T \cdot \mathbf{1}_n - \mathfrak{A})$ and using Caley-Hamilton, we obtain $P(a) \cdot q(v) = 0$. P is monic. Since q is surjective, we find $v \in R^n : q(v) = 1$. Thus $P(a) = 0$ and a satisfies A.

B $\implies$ A if R is Noetherian.[2] Let $a \in A$ satisfy B. Let B be a subalgebra of A containing b and finite over R. Let $M_n \subseteq B$ be the R-submodule generated by the a^i with $0 \leqslant i < n$. As a finitely generated module over the Noetherian ring R, B is a Noetherian R-module. Thus the ascending sequence M_n stabilizes at some step d and $a^d \in M_d$. Thus there are $(r_i)_{i=0}^{d-1} \in R^d$ such that $a^d = \sum_{i=0}^{d-1} r_i a^i$.

A $\implies$ B Let $a = (a_i)_{i=1}^n$ where all a_i satisfy A, i.e. $a_i^{d_i} = \sum_{j=0}^{d_i-1} r_{i,j} a_i^j$ with $r_{i,j} \in R$. Let $B \subseteq A$ be the sub-R-module generated by $a^\alpha = \prod_{i=1}^n a_i^{\alpha_i}$ with $0 \leqslant \alpha_i < d_i$. B is closed under $a_1 \cdot$ since

$$a_1 a^\alpha = \begin{cases} a^{(\alpha_1+1,\alpha')} & \text{if } \alpha = (\alpha_1, \alpha'), 0 \leqslant \alpha_1 < d_1 - 1, \\ \sum_{j=0}^{d_1-1} r_{i_1,j} a^{(j,\alpha')} & \text{if } \alpha_1 = d_1 - 1. \end{cases}$$

By symmetry, this hold for all a_i. By induction on $|\alpha| = \sum_{i=1}^n \alpha_i$, B is invariant under $a^\alpha \cdot$. Since these generate B as an R-module, B is multiplicatively closed. Thus A holds. Furthermore we have shown the final assertion of the proposition.

□

Corollary 1.10. Q Every finite R-algebra A is integral.

R The integral closure of R in A is an R-subalgebra of A.

S If A is an R-algebra, B an A-algebra and $b \in B$ integral over R, then it is integral over A.

T If A is an integral R-algebra and B any A-algebra, $b \in B$ integral

[2] This suffices in the exam.

over A, then b is integral over R.

Proof. Q Put $B = A$ in B.

R For every $r \in R$ $\alpha(r)$ is a solution to $T - r = 0$, hence integral over R. From B it follows, that the integral closure is closed under ring operations.

S trivial

T Let $b \in B$ such that $b^n = \sum_{i=0}^{n-1} a_i b^i$. Then there is a subalgebra $\tilde{A} \subseteq A$ finite over R, such that all $a_i \in \tilde{A}$. b is integral over $\tilde{A}$ Hence $\exists \tilde{B} \subseteq B$ finite over $\tilde{A}$ and $b \in \tilde{B}$. Since $\tilde{B}/\tilde{A}$ and $\tilde{A}/R$ are finite, $\tilde{B}/R$ is finite and b satisfies B.

□

1.6 Finiteness, finite generation and integrality

Fact 1.10.5 (Finite type and integral $\implies$ finite)**.** If A is an integral R-algebra of finite type, then it is a finite R-algebra.

Proof. Let A be generated by $(a_i)_{i=1}^n$ as an R-algebra. By the proposition on integral elements (1.8), there is a finite R-algebra $B \subseteq A$ such that all $a_i \in B$. We have $B = A$, as A is generated by the a_i as an R-algebra. □

Fact 1.10.6 (Finite type in tower)**.** If A is an R-algebra of finite type and B an A-algebra of finite type, then B is an R-algebra of finite type.

Proof. If A/R is generated by $(a_i)_{i=1}^m$ and B/A by $(b_j)_{j=1}^n$, then B/R is generated by the b_j and the images of the a_i in B. □

Fact 1.10.7 (About integrality and fields)**.** Let B be a domain integral over its subring A. Then B is a field iff A is a field.

Proof. Let B be a field and $a \in A \backslash \{0\}$. Then $a^{-1} \in B$ is integral over A, hence $a^{-d} = \sum_{i=0}^{d-1} \alpha_i a^{-i}$ for some $\alpha_i \in A$. Multiplication by a^{d-1} yields $a^{-1} = \sum_{i=0}^{d-1} \alpha_i a^{d-1-i} \in A$.

On the other hand, let B be integral over the field A. Let $b \in B \backslash \{0\}$. As B is integral over A, there is a sub-A-algebra $\tilde{B} \subseteq B$, $b \in \tilde{B}$ finitely generated as an A-module, i.e. a finite-dimensional A-vector space. Since B is a domain, $\tilde{B} \xrightarrow{b\cdot} \tilde{B}$ is injective, hence surjective, thus $\exists x \in \tilde{B} : b \cdot x \cdot 1$. □

1.7 Noether normalization theorem

Lemma 1.11. Let $S \subseteq \mathbb{N}^n$ be finite. Then there exists $\vec{k} \in \mathbb{N}^n$ such that $k_1 = 1$ and $w_{\vec{k}}(\alpha) \neq w_{\vec{k}}(\beta)$ for $\alpha \neq \beta \in S$, where $w_{\vec{k}}(\alpha) = \sum_{i=1}^n k_i \alpha_i$.

Proof. Intuitive: For $\alpha \neq \beta$ the equation $w_{(1,\vec{\kappa})}(\alpha) = w_{(1,\vec{\kappa})}(\beta)$ ($\kappa \in \mathbb{R}^{n-1}$) defines a codimension 1 affine hyperplane in $\mathbb{R}^{n-1}$. It is possible to choose κ such that all κ_i are $> \frac{1}{2}$ and with Euclidean distance $> \frac{\sqrt{n-1}}{2}$ from the union of these hyperplanes. By choosing the closest κ' with integral coordinates, each coordinate will be disturbed by at most $\frac{1}{2}$, thus at Euclidean distance $\leqslant \frac{\sqrt{n-1}}{2}$.

More formally:[3] Define $M := \max\{\alpha_i | \alpha \in S, 1 \leqslant i \leqslant n\}$. We can choose k such that $k_i > (i-1)Mk_{i-1}$. Suppose $\alpha \neq \beta$. Let i be the maximal index such that $\alpha_i \neq \beta_i$. Then the contributions of α_j (resp. β_j) with $1 \leqslant j < i$ to $w_{\vec{k}}(\alpha)$ (resp. $w_{\vec{k}}(\beta)$) cannot undo the difference $k_i(\alpha_i - \beta_i)$. □

Theorem 1.12 (Noether normalization)**.** Let K be a field and A a K-algebra of finite type. Then there are $a = (a_i)_{i=1}^n \in A$ which are algebraically independent over K, i.e. the ring homomorphism

$$\begin{aligned} \mathrm{ev}_a : K[X_1, \ldots, X_n] &\longrightarrow A \\ P &\longmapsto P(a_1, \ldots, a_n) \end{aligned}$$

is injective. n and the a_i can be chosen such that A is finite over the image of ev_a.

Proof. Let $(a_i)_{i=1}^n$ be a minimal number of elements such that A is integral over its K-subalgebra generated by $a_1, \ldots, a_n$. (Such a_i exist, since A is of finite type). Let $\tilde{A}$ be the K-subalgebra generated by the a_i. If suffices to show that the a_i are algebraically independent. Since A is of finite type over K and thus over $\tilde{A}$, by fact 1.10.5 (integral and finite type $\implies$ finite), A is finite over $\tilde{A}$. Thus we only need to show that the a_i are algebraically independent over K. Assume there is $P \in K[X_1, \ldots, X_n] \backslash \{0\}$ such that $P(a_1, \ldots, a_n) = 0$. Let $P = \sum_{\alpha \in \mathbb{N}^n} p_\alpha X^\alpha$ and $S = \{\alpha \in \mathbb{N}^n | p_\alpha \neq 0\}$. For $\vec{k} = (k_i)_{i=1}^n \in \mathbb{N}^n$ and $\alpha \in \mathbb{N}^n$ we define $w_{\vec{k}}(\alpha) := \sum_{i=1}^n k_i \alpha_i$.

By 1.11 it is possible to choose $\vec{k} \in \mathbb{N}^n$ such that $k_1 = 1$ and for $\alpha \neq \beta \in S$ we have $w_{\vec{k}}(\alpha) \neq w_{\vec{k}}(\beta)$.

Define $b_i := a_{i+1} - a_1^{k_{i+1}}$ for $1 \leqslant i < n$.

Claim 1. *A is integral over the subalgebra B generated by the b_i.*

[3] The intuitive version suffices in the exam.

Subproof. By the transitivity of integrality, it is sufficient to show that the a_i are integral over B. For $i > 1$ we have $a_i = b_{i-1} + a_1^{k_i}$. Thus it suffices to show this for a_1. Define $Q(T) := P(T, b_1 + T^{k_2}, \dots, b_{n-1} + T^{k_n}) \in B[T]$. We have $0 = P(a_1, \dots, a_n) = Q(a_1)$. Hence it suffices to show that the leading coefficient of Q is a unit.

We have
$$T^{\alpha_1} \prod_{i=1}^{n-1} (b_i + T^{k_i+1})^{\alpha_{i+1}} = T^{w_{\vec{k}}(\alpha)} + \sum_{l=0}^{w_{\vec{k}}(\alpha)-1} \beta_{\alpha,l} T^l$$
with suitable $\beta_{\alpha,l} \in B$.

By the choice of $\vec{k}$, we have

$$Q(T) = p_\alpha T^{w_{\vec{k}}(\alpha)} + \sum_{j=0}^{w_{\vec{k}}(\alpha)-1} q_j T^j$$

with $q_j \in B$ and α such that $w_{\vec{k}}(\alpha)$ is maximal subject to the condition $p_\alpha \neq 0$. Thus the leading coefficient of Q is a unit. ■

This contradicts the minimality of n, as B can be generated by $< n$ elements b_i. □

2 The Nullstellensatz and the Zariski topology

2.1 The Nullstellensatz

Let $\mathfrak{k}$ be a field, $R := \mathfrak{k}[X_1, \dots, X_n]$, $I \subseteq R$ an ideal.

Definition 2.1 (zero)**.** $x \in \mathfrak{k}^n$ is **a zero of I** if $\forall x \in I : P(x) = 0$. Let $V_{\mathbb{A}}(I)$ denote the set of zeros if I in $\mathfrak{k}^n$.

The **zero in a field extension $\mathfrak{i}$ of $\mathfrak{k}$** is defined similarly.

Remark 2.1.8 (Set of zeros and generators)**.** Let I be generated by S. Then $\{x \in R | \forall s \in S : s(x) = 0\} = V_{\mathbb{A}}(I)$. Thus zero sets of ideals correspond to solutions sets to systems of polynomial equations. If $S, \tilde{S}$ generate the same ideal I they have the same set of solutions. Therefore we only consider zero sets of ideals.

Theorem 2.2 (Hilbert's Nullstellensatz (1))**.** If $\mathfrak{k}$ is algebraically closed and $I \subsetneq R$ a proper ideal, then I has a zero in $\mathfrak{k}^n$.

Remark 2.2.9. Will be shown later (see proof of 2.4). It is trivial if $n = 1$: R is a PID, thus $I = pR$ for some $p \in R$. Since $I \neq R$ $p = 0$ or P is non-constant. $\mathfrak{k}$ algebraically closed $\rightsquigarrow$ there exists a zero of p.

If $\mathfrak{k}$ is not algebraically closed and $n > 0$, the theorem fails (consider $I = p(X_1)R$).

Equivalent[4] formulation:

Theorem 2.3 (Hilbert's Nullstellensatz (2))**.** Let L/K be an arbitrary field extension. Then L/K is a finite field extension ($\dim_K L < \infty$) iff L is a K-algebra of finite type.

Proof. $\Longrightarrow$ If $(l_i)_{i=1}^m$ is a base of L as a K-vector space, then L is generated by the l_i as a K-algebra.

$\Longleftarrow$ Apply the Noether normalization theorem (1.12) to $A = L$. This yields an injective ring homomorphism $\mathrm{ev}_a : K[X_1, \ldots, X_n] \to A$ such that A is finite over the image of ev_a. By the fact about integrality and fields (1.10.7), the isomorphic image of ev_a is a field. Thus $K[X_1, \ldots, X_n]$ is a field $\Longrightarrow$ $n = 0$. Thus L/K is a finite ring extension, hence a finite field extension.

□

Remark 2.3.10. We will see several additional proofs of this theorem. See 2.6 and 2.38. All will be accepted in the exam.

2.13 and 3.10 are closely related.

Theorem 2.4 (Hilbert's Nullstellensatz (1b))**.** Let $\mathfrak{l}$ be a field and $I \subseteq R = \mathfrak{l}[X_1, \ldots, X_m]$ a proper ideal. Then there are a finite field extension $\mathfrak{i}$ of $\mathfrak{l}$ and a zero of I in $\mathfrak{i}^m$.

Proof. (HNS2 (2.3) $\Longrightarrow$ HNS1b (2.4)) $I \subseteq \mathfrak{m}$ for some maximal ideal. $R/\mathfrak{m}$ is a field, since $\mathfrak{m}$ is maximal. $R/\mathfrak{m}$ is of finite type, since the images of the X_i generate it as a $\mathfrak{l}$-algebra. There are thus a field extension $\mathfrak{i}/\mathfrak{l}$ and an isomorphism $R/\mathfrak{m} \xrightarrow{\iota} \mathfrak{i}$ of $\mathfrak{l}$-algebras. By HNS2 (2.3), $\mathfrak{i}/\mathfrak{l}$ is a finite field extension. Let $x_i := \iota(X_i \mod \mathfrak{m})$.

$$P(x_1, \ldots, x_m) = \iota(P \mod \mathfrak{m})$$

Both sides are morphisms $R \to \mathfrak{i}$ of $\mathfrak{l}$-algebras. For for $P = X_i$ the equality is trivial. It follows in general, since the X_i generate R as a $\mathfrak{l}$-algebra.

[4] used in a vague sense here

Thus $(x_1, \dots, x_m)$ is a zero of I (since $P \mod \mathfrak{m} = 0$ for $P \in I \subseteq \mathfrak{m}$). HNS1 (2.2) can easily be derived from HNS1b. □

2.1.1 Nullstellensatz for uncountable fields

The following proof of the Nullstellensatz only works for uncountable fields, but will be accepted in the exam.

Lemma 2.5. If K is an uncountable field, then $\dim_K K(T)$ is uncountable.

Proof. We will show, that $S := \left\{\frac{1}{T-\kappa} | \kappa \in K\right\}$ is K-linearly independent. It follows that $\dim_K K(T) \geqslant \#S > \aleph_0$.

Suppose $(x_\kappa)_{\kappa \in K}$ is a selection of coefficients from K such that $I := \{\kappa \in K | x_\kappa \neq 0\}$ is finite and

$$g := \sum_{\kappa \in K} \frac{x_\kappa}{T - \kappa} = 0$$

Let $d := \prod_{\kappa \in I}(T - \kappa)$. Then for $\lambda \in I$ we have

$$0 = (dg)(\lambda) = x_\lambda \prod_{\kappa \in I \setminus \{\lambda\}} (\lambda - \kappa).$$

This is a contradiction as $x_\lambda \neq 0$. □

Theorem 2.6 (Hilbert's Nullstellensatz for uncountable fields)**.** If K is an uncountable field and L/K a field extension and L of finite type as a K-algebra, then this field extension is finite.

Proof. If $(x_i)_{i=1}^n$ generate L as an K-algebra, then the countably many monomials $x^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$ in the x_i with $\alpha \in \mathbb{N}^n$ generate L as a K-vector space. Thus $\dim_K L \leqslant \aleph_0$ and the same holds for any intermediate field $K \subseteq M \subseteq L$. If $l \in L$ is transcendent over K and $M = K(l)$, then $M \cong K(T)$ has uncountable dimension by 2.5. Thus L/K is algebraic, hence integral, hence finite (1.10.5). □

2.2 The Zariski topology

2.2.1 Operations on ideals and $V_{\mathbb{A}}(I)$

Let R be a ring and $I, J, I_\lambda \subseteq R$ ideals, $\lambda \in \Lambda$.

Definition 2.7 (Radical, product and sum of ideals)**.**

$$\sqrt{I} := \bigcap_{n=0}^{\infty} \{f \in R | f^n \in I\},$$

$$I \cdot J := \langle \{i \cdot j | i \in I, j \in J\} \rangle_R,$$

$$\sum_{\lambda \in \Lambda} I_\lambda := \left\{ \sum_{\lambda \in \Lambda'} i_\lambda | \Lambda' \subseteq \Lambda \text{ finite} \right\}.$$

Fact 2.7.11. The radical is an ideal in R and $\sqrt{\sqrt{I}} = \sqrt{I}$.
$I \cdot J$ is an ideal.
$\sum_{\lambda \in \Lambda} I_\lambda$ coincides with the ideal generated by $\bigcap_{\lambda \in \Lambda} I_\lambda$ in R.
$\bigcap_{\lambda \in \Lambda} I_\lambda$ is an ideal.

Let $R = \mathfrak{k}[X_1, \ldots, X_n]$ where $\mathfrak{k}$ is an algebraically closed field.

Fact 2.7.12. Let $I, J, (I_\lambda)_{\lambda \in \Lambda}$ be ideals in R. Λ may be infinite. Then

A $V_{\mathbb{A}}(I) = V_{\mathbb{A}}(\sqrt{I})$,

B $\sqrt{J} \subseteq \sqrt{I} \implies V_{\mathbb{A}}(I) \subseteq V_{\mathbb{A}}(J)$,

C $V_{\mathbb{A}}(R) = \emptyset, V_{\mathbb{A}}(\{0\} = \mathfrak{k}^n$,

D $V_{\mathbb{A}}(I \cap J) = V_{\mathbb{A}}(I \cdot J) = V_{\mathbb{A}}(I) \cup V_{\mathbb{A}}(J)$,

E $V_{\mathbb{A}}(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} V_{\mathbb{A}}(I_\lambda)$.

Proof. A-C trivial

D $I \cdot J \subseteq I \cap J \subseteq I$. Thus $V_{\mathbb{A}}(I) \subseteq V_{\mathbb{A}}(I \cap J) \subseteq V_{\mathbb{A}}(I \cdot J)$. By symmetry we have $V_{\mathbb{A}}(I) \cup V_{\mathbb{A}}(J) \subseteq V_{\mathbb{A}}(I \cap J) \subseteq V_{\mathbb{A}}(I \cdot J)$. Let $x \notin V_{\mathbb{A}}(I) \cup V_{\mathbb{A}}(J)$. Then there are $f \in I, g \in J$ such that $f(x) \neq 0, g(x) \neq 0$ thus $(f \cdot g)(x) \neq 0 \implies x \notin V_{\mathbb{A}}(I \cdot J)$. Therefore

$$V_{\mathbb{A}}(I) \cup V_{\mathbb{A}}(J) \subseteq V_{\mathbb{A}}(I \cap J) \subseteq V_{\mathbb{A}}(I \cdot J) \subseteq V_{\mathbb{A}}(I) \cup V_{\mathbb{A}}(J).$$

E $I_\lambda \subseteq \sum_{\lambda \in \Lambda} I_\lambda \implies V_{\mathbb{A}}(\sum_{\lambda \in \Lambda} I_\lambda) \subseteq V_{\mathbb{A}}(I_\lambda)$. Thus $V_{\mathbb{A}}(\sum_{\lambda \in \Lambda} I_\lambda) \subseteq \bigcap_{\lambda \in \Lambda} V_{\mathbb{A}}(I_\lambda)$. On the other hand if $f \in \sum_{\lambda \in \Lambda} I_\lambda$ we have $f = \sum_{\lambda \in \Lambda} f_\lambda$. Thus f vanishes on $\bigcap_{\lambda \in \Lambda} V_{\mathbb{A}}(I_\lambda)$ and we have $\bigcap_{\lambda \in \Lambda} V_{\mathbb{A}}(I_\lambda) \subseteq V_{\mathbb{A}}(\sum_{\lambda \in \Lambda} I_\lambda)$.

□

Remark 2.7.13. There is no similar way to describe $V_{\mathbb{A}}(\bigcap_{\lambda\in\Lambda} I_\lambda)$ in terms of the $V_{\mathbb{A}}(I_\lambda)$ when Λ is infinite. For instance if $n = 1, I_k := X_1^k R$ then $\bigcap_{k=0}^{\infty} I_k = \{0\}$ but $\bigcup_{k=0}^{\infty} V_{\mathbb{A}}(I_k) = \{0\}$.

2.2.2 Definition of the Zariski topology

Let $\mathfrak{k}$ be algebraically closed, $R = \mathfrak{k}[X_1, \ldots, X_n]$.

Corollary 2.8. (of 2.7.12) There is a topology on $\mathfrak{k}^n$ for which the set of closed sets coincides with the set $\mathfrak{A}$ of subsets of the form $V_{\mathbb{A}}(I)$ for ideals $I \subseteq R$. This topology is called the **Zariski-Topology**

Example 2.9. Let $n = 1$. Then R is a PID. Hence every ideal is a principal ideal and the Zariski-closed subsets of $\mathfrak{k}$ are the subsets of the form $V_{\mathbb{A}}(P)$ for $P \in R$. As $V_{\mathbb{A}}(0) = \mathfrak{k}$ and $V_{\mathbb{A}}(P)$ finite for $P \neq 0$ and $\{x_1, \ldots, x_n\} = V_{\mathbb{A}}(\prod_{i=1}^{n}(T - x_i))$ the Zariski-closed subsets of $\mathfrak{k}$ are $\mathfrak{k}$ and the finite subsets. Because $\mathfrak{k}$ is infinite, this topology is not Hausdorff.

2.2.3 Separation properties of topological spaces

Definition 2.10. Let X be a topological space. X satisfies the separation properties T_{0-2} if for any $x \neq y \in X$

- T_0 $\exists U \subseteq X$ open such that $|U \cap \{x, y\}| = 1$
- T_1 $\exists U \subseteq X$ open such that $x \in U, y \notin U$.
- T_2 There are disjoined open sets $U, V \subseteq X$ such that $x \in U, y \in V$. (Hausdorff)

Remark 2.10.14. Let $x \sim y :\iff$ the open subsets of X containing x are precisely the open subsets of X containing y. Then T_0 holds iff $x \sim y \implies x = y$.

Fact 2.10.15. $T_0 \iff$ every point is closed.

Fact 2.10.16. The Zariski topology on $\mathfrak{k}^n$ is T_1 but for $n \geqslant 1$ not Hausdorff. For $n \geqslant 1$ the intersection of two non-empty open subsets of $\mathfrak{k}^n$ is always non-empty.

Proof. $\{x\}$ is closed, as $\{x\} = V(\operatorname{Span} X_1 - x_1, \ldots, X_n - x_n{}_R)$. If $A = V(I), B = V(J)$ are two proper closed subsets of $\mathfrak{k}^n$ then $I \neq \{0\}$, $J \neq \{0\}$ and thus $IJ \neq \{0\}$. Therefore $A \cup B = V(IJ)$ is a proper closed subset of $\mathfrak{k}^n$. $\square$

2.2.4 Compactness properties of topological spaces

Let X be a topological space.

Definition 2.11 (Compact, quasi-compact)**.** X is called **quasi-compact** if every open covering of X has a finite subcovering. It is called **compact**, if it is quasi-compact and Hausdorff.

Definition 2.12 (Noetherian topological spaces)**.** X is called **Noetherian**, if the following equivalent conditions hold:

A Every open subset of X is quasi-compact.

B Every descending sequence $A_0 \supseteq A_1 \supseteq \dots$ of closed subsets of X stabilizes.

C Every non-empty set $\mathcal{M}$ of closed subsets of X has a $\subseteq$-minimal element.

Proof.

A $\implies$ B Let A_j be a descending chain of closed subsets. Define $A := \bigcap_{j=0}^{\infty} A_j$. If A holds, the covering $X \backslash A = \bigcup_{j=0}^{\infty}(X\backslash A_j)$ has a finite subcovering.

B $\implies$ C Suppose $\mathcal{M}$ does not have a $\subseteq$-minimal element. Using DC, one can construct a counterexample $A_1 \subsetneq A_2 \supsetneq \dots$ to B.

C $\implies$ A Let $\bigcup_{i\in I} V_i$ be an open covering of an open subset $U \subseteq X$. By C, the set $\mathcal{M} := \{X\backslash \bigcup_{i\in F} V_i | F \subseteq I \text{ finite}\}$ has a $\subseteq$-minimal element.

□

2.3 Another form of the Nullstellensatz and Noetherianness of $\mathfrak{k}^n$

Let $\mathfrak{k}$ be algebraically closed, $R = \mathfrak{k}[X_1, \dots, X_n]$. For $f \in R$ let $V(f) = V(fR)$.

Theorem 2.13 (Hilbert's Nullstellensatz (3))**.** Let $I \subseteq R$ be an ideal. Then $V(I) \subseteq V(f)$ iff $f \in \sqrt{I}$.

Proof. Suppose f vanishes on all zeros of I. Let $R' := \mathfrak{k}[X_1, \dots, X_n, T]$,

$$g(X_1, \dots, X_n, T) := 1 - T \cdot f(X_1, \dots, X_n)$$

and $J \subseteq R'$ the ideal generated by g and the elements of I (viewed as elements of R' which are constant in the T-direction).

If f vanishes on all zeros of I, then J has no zeros in $\mathfrak{k}^{n+1}$.

Thus there exist $p_i \in I, i = 1, \ldots, n,\ q_i \in \mathfrak{k}[X_1, \ldots, X_n, T], i = 1, \ldots, n$ and $q \in \mathfrak{k}[X_1, \ldots, X_n, T]$ such that

$$1 = g \cdot q + \sum_{i=1}^{n} p_i q_i.$$

Formally substituting $\frac{1}{f(x_1, \ldots, x_n)}$ for Y, one obtains:

$$1 = \sum_{i=1}^{n} p_i \left(x_1, \ldots, x_n\right) q_i \left(x_1, \ldots, x_n, \frac{1}{f(x_1, \ldots, x_n)}\right)$$

Multiplying by a sufficient power of f, this yields an equation in R :

$$f^d = \sum_{i=1}^{n} p_i(x_1, \ldots, _n) \cdot q_i'(x_1, \ldots, x_n) \in I$$

Thus $f \in \sqrt{I}$. □

Corollary 2.14.

$$\begin{aligned} f : \{I \subseteq R | I \text{ideal}, I = \sqrt{I}\} &\longrightarrow \{A \subseteq \mathfrak{k}^n | A \text{ Zariski-closed}\} \\ I &\longmapsto V(I) \\ \{f \in R | A \subseteq V(f)\} &\longleftarrow A \end{aligned}$$

is a $\subseteq$-antimonotonic bijection.

Corollary 2.15. The topological space $\mathfrak{k}^n$ is Noetherian.

Proof. Because the map from 2.14 is antimonotonic, strictly decreasing chains of closed subsets of $\mathfrak{k}^n$ are mapped to strictly increasing chains of ideals in R. By the Basissatz (1.3), R is Noetherian. □

2.4 Irreducible spaces

Let X be a topological space.

Definition 2.16. X is called **irreducible**, if $X \neq \varnothing$ and the following equivalent conditions hold:

A Every open $\varnothing \neq U \subseteq X$ is dense.

B The intersection of non-empty, open subsets $U, V \subseteq X$ is non-empty.

C If $A, B \subseteq X$ are closed, $X = A \cup B$ then $X = A$ or $X = B$.

D Every open subset of X is connected.

Proof.

$A \iff B$ by definition of denseness.

B $\iff$ C Let $U := X\backslash A, V := X\backslash B$.

B $\implies$ D Suppose W is a non-connected open subset. Then there exists a decomposition $W = U \cup V$ into disjoint open subsets.

D $\implies$ B If $U, V \neq \varnothing$ are disjoint open subsets, then $U \cup V$ is non-connected.

□

Corollary 2.17. Every irreducible topological space is connected.

Example 2.18. $\mathfrak{k}^n$ is irreducible as shown in 2.9.

Fact 2.18.17. A A single point is always irreducible.

B If X is Hausdorff then it is irreducible iff it has precisely one point.

C X is irreducible iff it cannot be written as a finite union of proper closed subsets.

D X is irreducible iff any finite intersection of non-empty open subsets is non-empty. ($\bigcap \varnothing := X$)

Proof. A,B trivial

C $\implies$: Induction on the cardinality of the union. $\impliedby$: $\bigcap \varnothing = X$ is non-empty and any intersection of two non-empty open subsets is non-empty.

D Follows from C.

□

2.4.1 Irreducible components

Fact 2.18.18. If $D \subseteq X$ is dense, then X is irreducible iff D is irreducible with its induced topology.

Proof. $X = \varnothing$ iff $D = \varnothing$. Suppose B is the union of its proper closed subsets A, B. Then $X = \overline{A} \cup \overline{B}$. These are proper closed subsets of X, as $\overline{A} \cap D = A \cap D$ (by closedness of D) and thus $\overline{A} \cap D \neq D$.

On the other hand, if U and V are disjoint non-empty open subsets of X, then $U \cap D$ and $V \cap D$ are disjoint non-empty open subsets of D. □

Definition 2.19 (Irreducible subsets)**.** A subset $Z \subseteq X$ is called **irreducible**, if it is irreducible with its induced topology. Z is called an **irreducible component** of X, if it is irreducible and if every irreducible subset $Z \subseteq Y \subseteq X$ coincides with Z.

Corollary 2.20.

1. $Z \subseteq X$ is irreducible iff $\overline{Z} \subseteq X$ is irreducible.
2. Every irreducible component of X is a closed subset of X.

Notation 2.20.19. From now on, irreducible means irreducible and closed.

2.4.2 Decomposition into irreducible subsets

Proposition 2.21. Let X be a Noetherian topological space. Then X can be written as a finite union $X = \bigcup_{i=1}^{n} Z_i$ of irreducible closed subsets of X. One may additionally assume that $i \neq j \implies Z_i \nsubseteq Z_i$. With this minimality condition, n and the Z_i are unique (up to permutation) and $\{Z_1, \ldots, Z_n\}$ is the set of irreducible components of X.

Proof. Let $\mathfrak{M}$ be the set of closed subsets of X which cannot be decomposed as a union of finitely many irreducible subsets. Suppose $\mathfrak{M} \neq \varnothing$. Then there exists a $\subseteq$-minimal $Y \in \mathfrak{M}$. Y cannot be empty or irreducible. Hence $Y = A \cup B$ where A, B are proper closed subsets of Y. By the minimality of Y, A and B can be written as a union of proper closed subsets $\lightning$.

Let $X = \bigcup_{i=1}^{n} Z_i$, where there are no inclusions between the Z_i. If Y is an irreducible subsets of X, $Y = \bigcup_{i=1}^{n}(Y \cap Z_i)$ and there exists $1 \leqslant i \leqslant n$ such that $Y = Y \cap Z_i$. Hence $Y \subseteq Z_i$. Thus the Z_i are irreducible components. Conversely, if Y is an irreducible component of X, $Y \subseteq Z_i$ for some i and $Y = Z_i$ by the definition of irreducible component. □

Remark 2.21.20. The proof of existence was an example of **Noetherian induction**: If E is an assertion about closed subsets of a Noetherian topological space X and E holds for A if it holds for all proper subsets of A, then $E(A)$ holds for every closed subset $A \subseteq X$.

Proposition 2.22. By 2.14 there exists a bijection

$$\begin{aligned} f : \{I \subseteq R | I \text{ ideal}, I = \sqrt{I}\} &\longrightarrow \{A \subseteq \mathfrak{k}^n | A \text{ Zariski-closed}\} \\ I &\longmapsto V(I) \\ \{f \in R | A \subseteq V(f)\} &\longleftarrow\!\shortmid A \end{aligned}$$

Under this correspondence $A \subseteq \mathfrak{k}^n$ is irreducible iff $I := f^{-1}(A)$ is a prime ideal. Moreover, $\#A = 1$ iff I is a maximal ideal.

Proof. By the Nullstellensatz (2.2), $A = \varnothing \iff I = R$. Suppose $A = B \cup C$ is a decomposition into proper closed subsets $A = V(J)$, $B = V(K)$ where $J = \sqrt{J}$, $K = \sqrt{K}$. Since $A \neq B$ and $A \neq C$, there are $f \in J \backslash I, g \in K \backslash I$. fg vanishes on $A = B \cup C$. By the Nullstellensatz (2.13) $fg \in \sqrt{I} = I$ and I fails to be prime.

On the other hand suppose that $fg \in I, f \notin I, g \notin I$. By the Nullstellensatz (2.13) and $I = \sqrt{I}$ neither f nor g vanishes on all of A. Thus $(A \cap V(f)) \cup (A \cap V(g))$ is a decomposition and A fails to be irreducible.

The remaining assertion follows from the fact, that the bijection is $\subseteq$-antimonotonic and thus maximal ideals correspond to minimal irreducible closed subsets, which are the one-point subsets as $\mathfrak{k}^n$ is T_1. ☐

2.5 Krull dimension

Definition 2.23. Let Z be an irreducible subset of the topological space X. Let $\operatorname{codim}(Z, X)$ be the maximum of the length n of strictly increasing chains

$$Z \subseteq Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_n$$

of irreducible closed subsets of X containing Z or ∞ if such chains can be found for arbitrary n. Let

$$\dim X := \begin{cases} -\infty & \text{if } X = \varnothing, \\ \sup\limits_{\substack{Z \subseteq X \\ Z \text{ irreducible}}} \operatorname{codim}(Z, X) & \text{otherwise.} \end{cases}$$

Remark 2.23.21.

- In the situation of the definition $\overline{Z}$ is irreducible. Hence $\operatorname{codim}(Z, X)$ is well-defined and one may assume without losing much generality that Z is closed.
- Because a point is always irreducible, every non-empty topological space has an irreducible subset and for $X \neq \varnothing$, $\dim X$ is ∞ or $\max_{x \in X} \operatorname{codim}(\{x\}, X)$.
- Even for Noetherian X, it may happen that $\operatorname{codim}(Z, X) = \infty$.
- Even for if X is Noetherian and $\operatorname{codim}(Z, X)$ is finite for all irreducible subsets Z of X, $\dim X$ may be infinite.

Fact 2.23.22. If $X = \{x\}$, then $\dim X = 0$.

Fact 2.23.23. For every $x \in \mathfrak{k}$, $\operatorname{codim}(\{x\}, \mathfrak{k}) = 1$. The only other irreducible closed subset of $\mathfrak{k}$ is $\mathfrak{k}$ itself, which has codimension zero. Thus $\dim \mathfrak{k} = 1$.

Fact 2.23.24. Let $Y \subseteq X$ be irreducible and $U \subseteq X$ an open subset such that $U \cap Y \neq \emptyset$. Then we have a bijection

$$
\begin{aligned}
f : &\{A \subseteq X | A \text{ irreducible, closed and } Y \subseteq A\} \\
&\longrightarrow \{B \subseteq U | B \text{ irreducible, closed and } Y \cap U \subseteq B\}
\end{aligned}
$$

given by

$$
\begin{aligned}
A &\longmapsto A \cap U \\
\overline{B} &\longleftarrow B
\end{aligned}
$$

where $\overline{B}$ denotes the closure in X.

Proof. If A is given and $B = A \cap U$, then $B \neq \emptyset$ and B is open hence (irreducibility of A) dense in A, hence $A = \overline{B}$. The fact that $B = \overline{B} \cap U$ is a general property of the closure operator. □

Corollary 2.24 (Locality of Krull codimension)**.** Let $Y \subseteq X$ be irreducible and $U \subseteq X$ an open subset such that $U \cap Y \neq \emptyset$. Then $\operatorname{codim}(Y, X) = \operatorname{codim}(Y \cap U, U)$.

Fact 2.24.25. Let $Z \subseteq Y \subseteq X$ be irreducible closed subsets of the topological space X. Then

$$
\operatorname{codim}(Z, Y) + \operatorname{codim}(Y, X) \leqslant \operatorname{codim}(Z, X) \tag{CD+}
$$

Proof. A chain of irreducible closed subsets between Z and Y and a chain of irreducible closed between Y and X can be spliced together. □

Taking the supremum over all Z we obtain:

Fact 2.24.26. If Y is an irreducible closed subset of the topological space X, then

$$
\dim(Y) + \operatorname{codim}(Y, X) \leqslant \dim(X) \tag{D+}
$$

In general, these inequalities may be strict.

Definition 2.25 (Catenary topological spaces)**.** A topological space T is called **catenary** if equality holds in (CD+) whenever X is an irreducible closed subset of T.

2.5.1 Krull dimension of $\mathfrak{k}^n$

Theorem 2.26. $\dim \mathfrak{k}^n = n$ and $\mathfrak{k}^n$ is catenary. Moreover, if X is an irreducible closed subset of $\mathfrak{k}^n$, then equality occurs in (D+).

Proof. Considering

$$\{0\} \subsetneq \mathfrak{k} \times \{0\} \subsetneq \mathfrak{k}^2 \times \{0\} \subsetneq \ldots \subsetneq \mathfrak{k}^n$$

it is clear that $\operatorname{codim}(\{0\}, \mathfrak{k}^n) \geqslant n$. Translation by $x \in \mathfrak{k}^n$ gives us

$$\operatorname{codim}(\{x\}, \mathfrak{k}^n) \geqslant n.$$

The opposite inequality follows from 2.50 ($Z = \mathfrak{k}^n$, $\dim \mathfrak{k}^n \leqslant \operatorname{trdeg}(\mathfrak{K}(Z)/\mathfrak{k}) = \operatorname{trdeg}(Q(\mathfrak{k}[X_1, \ldots, X_n])/\mathfrak{k}) = n$).

The theorem is a special case of 2.69. □

Lemma 2.27. Every non-zero prime ideal $\mathfrak{p}$ of a UFD R contains a prime element.

Proof. Let $p \in \mathfrak{p}\backslash\{0\}$ with the minimal number of prime factors, counted by multiplicity. If p was a unit, then $\mathfrak{p} \supseteq pR = R$. If $p = ab$ with non-units a, b, it follows that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ contradicting the minimality assumption. Thus p is a prime element of R. □

Proposition 2.28 (Irreducible subsets of codimension one)**.** Let $p \in R = \mathfrak{k}[X_1, \ldots, X_n]$ be a prime element. Then the irreducible subset $X = V(p) \subseteq \mathfrak{k}^n$ has codimension one, and every codimension one subset of $\mathfrak{k}^n$ has this form.

Proof. Since pR is a prime ideal, $X = V(p)$ is irreducible. Since $p \neq 0$, X is a proper subset of $\mathfrak{k}^n$. If $X \subseteq Y \subseteq \mathfrak{k}^n$ is irreducible and closed, then $Y = V(\mathfrak{q})$ for some prime ideal $\mathfrak{p} \subseteq pR$. If $Y \neq \mathfrak{k}^n$, then $\mathfrak{p} \neq \{0\}$. By 2.27 there exists a prime element $q \in \mathfrak{q}$. As $\mathfrak{q} \subseteq pR$ we have $p \mid q$. By the irreducibility of p and q it follows that $p \sim q$. Hence $\mathfrak{q} = pR$ and $X = Y$.

Suppose $X = V(\mathfrak{p}) \subseteq \mathfrak{k}^n$ is closed, irreducible and of codimension one. Then $\mathfrak{p} \neq \{0\}$, hence $X \neq \mathfrak{k}^n$. By 2.27 there is a prime element $p \in \mathfrak{p}$. If $\mathfrak{p} \neq pR$, then $X \subsetneq V(p) \subsetneq \mathfrak{k}^n$ contradicts $\operatorname{codim}(X, \mathfrak{k}^n) = 1$. □

2.6 Transcendence degree

2.6.1 Matroids

Definition 2.29 (Hull operator)**.** Let X be a set, $\mathcal{P}(X)$ the power set of X. A **Hull operator** on X is a map $\mathcal{P}(X) \xrightarrow{\mathcal{H}} \mathcal{P}(X)$ such that

H1 $\forall A \in \mathcal{P}(X)\ A \subseteq \mathcal{H}(A)$.

H2 $A \subseteq B \subseteq X \implies \mathcal{H}(A) \subseteq \mathcal{H}(B)$.

H3 $\mathcal{H}(\mathcal{H}(X)) = \mathcal{H}(X)$.

We call $\mathcal{H}$ **matroidal** if in addition the following conditions hold:

M If $m, n \in X$ and $A \subseteq X$ then

$$m \in \mathcal{H}(\{n\} \cup A)\backslash\mathcal{H}(A) \iff n \in \mathcal{H}(\{m\} \cup A)\backslash\mathcal{H}(A),$$

F $\mathcal{H}(A) = \bigcup_{F \subseteq A \text{ finite}} \mathcal{H}(F)$.

In this case, $S \subseteq X$ is called **independent subset**, if $s \notin \mathcal{H}(S\backslash\{s\})$ for all $s \in S$ and **generating** if $X = \mathcal{H}(S)$. S is called a **base**, if it is both generating and independent.

Theorem 2.30. If $\mathcal{H}$ is a matroidal hull operator on X, then a basis exists, every independent set is contained in a base and two arbitrary bases have the same cardinality.

Example 2.31. Let K be a field, V a K-vector space and $\mathcal{L}(T)$ the K-linear hull of T for $T \subseteq V$. Then $\mathcal{L}$ is a matroidal hull operator on V.

2.6.2 Transcendence degree

Lemma 2.32. Let L/K be a field extension and let $\mathcal{H}(T)$ be the algebraic closure in L of the subfield of L generated by K and T. [a] Then $\mathcal{H}$ is a matroidal hull operator.

[a] This is the intersection of all subfields of L containing $K \cup T$, or the field of quotients of the sub-K-algebra of L generated by T.

Proof. H1, H2 and F are trivial. For an algebraically closed subfield $K \subseteq M \subseteq L$ we have $\mathcal{H}(M) = M$. Thus $\mathcal{H}(\mathcal{H}(T)) = \mathcal{H}(T)$ (H3).

Let $x, y \in L$, $T \subseteq L$ and $x \in \mathcal{H}(T \cup \{y\})\backslash\mathcal{H}(T)$. We have to show that $y \in \mathcal{H}(T \cup \{x\})\backslash\mathcal{H}(T)$. If $y \in \mathcal{H}(T)$ we have $\mathcal{H}(T \cup \{y\}) \subseteq \mathcal{H}(\mathcal{H}(T)) = \mathcal{H}(T) \implies x \in \mathcal{H}(T)\backslash\mathcal{H}(T)\lightning$. Hence it is sufficient to show $y \in \mathcal{H}(T \cup \{x\})$. Without loss of generality loss of generality $T = \varnothing$ (replace K be the subfield generated by $K \cup T$). Then x is algebraic over the subfield M of L generated by $K \cup \{y\}$.

Thus there exists $0 \neq P \in M[T]$ with $P(x) = 0$. The coefficients p_i of P belong to the field of quotients of the K-subalgebra of L generated by y. There are thus polynomials $Q_i, R \in K[Y]$ such that $p_i = \frac{Q_i(y)}{R(y)}$, $R(y) \neq 0$. Let

$$Q(X,Y) := \sum_{i=0}^{\infty} X^i Q_i(Y) = \sum_{i,j=0}^{\infty} q_{i,j} X^i Y^j = \sum_{j=0}^{\infty} Y^j \hat{Q}_j(X) \in K[X,Y].$$

Then $Q(x,y) = 0$. Let $\hat{p_j} := \hat{Q}_j(x)$. Then $\hat{P}(y) = 0$. As $Q \neq 0$ there is $(i,j) \in \mathbb{N}^2$ such that $q_{i,j} \neq 0$ and then $\hat{p_j} \neq 0$ as $x \notin \mathcal{H}(\varnothing)$. Thus $\hat{P} \in \hat{M}[X] \backslash \{0\}$, where $\hat{M}$ is the subfield of L generated by K and x. Thus y is algebraic over $\hat{M}$ and $y \in \mathcal{H}(\{x\})$, □

Definition 2.33 (Transcendence Base)**.** Let L/K be a field extension and $\mathcal{H}(T)$ the algebraic closure in L of the subfield generated by K and T. A base for $(L, \mathcal{H})$ is called a **transcendence base** and the **transcendence degree** $\operatorname{trdeg}(L/K)$ is defined as the cardinality of any transcendence base of L/K.

Remark 2.33.27. L/K is algebraic iff $\operatorname{trdeg}(L/K) = 0$.

2.7 Inheritance of Noetherianness and of finite type by subrings and subalgebras / Artin-Tate

The following will lead to another proof of the Nullstellensatz, which uses the transcendence degree.

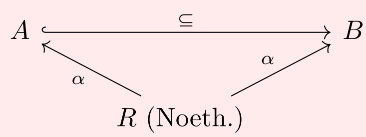
Remark 2.33.28. There exist non-Noetherian domains, which are subrings of Noetherian domains (namely the field of quotients is Noetherian).

Theorem 2.34 (Eakin-Nagata)**.** Let A be a subring of the Noetherian ring B. If the ring extension B/A is finite (i.e. B finitely generated as an A-module) then A is Noetherian.

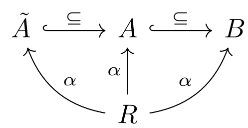
Fact† 2.34.29. Let R be Noetherian and let B be a finite R-algebra. Then every R-subalgebra $A \subseteq B$ is finite over R.

Proof. Since B a finitely generated R-module and R a Noetherian ring, B is a Noetherian R-module (this is a stronger assertion than Noetherian algebra). Thus the sub- R-module A is finitely generated. □

Proposition 2.35 (Artin-Tate)**.** Let A be a subalgebra of the R-algebra B, where R is Noetherian. If B/R is of finite type and B/A is finite, then A/R is also of finite type.



Proof. Let $(b_i)_{i=1}^m$ generate B as an A-module and $(\beta_j)_{j=1}^m$ as an R-algebra. There are $a_{ijk} \in A$ such that $b_i b_j = \sum_{k=1}^m a_{ijk} b_k$. And $\alpha_{ij} \in A$ such that $\beta_i = \sum_{j=1}^m \alpha_{ij} b_j$. Let $\tilde{A}$ be the sub- R-algebra of A generated by the a_{ijk} and α_{ij}. $\tilde{A}$ is of finite type over R, hence Noetherian. The $\tilde{A}$-submodule generated by 1 and the b_i is a sub-R-algebra containing the β_i and thus coincides with B. Hence $B/\tilde{A}$ is finite. Since $A \subseteq B, A/\tilde{A}$ is finite (2.34.29). Hence $A/\tilde{A}$ is of finite type. By the transitivity of "of finite type", it follows that A/R is of finite type.



□

2.7.1 Artin-Tate proof of the Nullstellensatz

Let K be a field and $R = K[X_1, \ldots, X_n]$.

Definition 2.36 (Rational functions)**.** Let $K(X_1, \ldots, X_n) := Q(R)$ be the field of quotients of R.

$K(X_1, \ldots, X_n)$ is called the **field of rational functions** in n variables over K.

Lemma 2.37 (Infinitely many prime elements)**.** There are infinitely many multiplicative equivalence classes of prime elements in R.

Proof. Suppose $(P_i)_{i=1}^m$ is a complete list of prime elements of R (up to multiplicative equivalence). Then $m > 0$, as X_1 is prime. The polynomial $f := 1 + \prod_{i=1}^m P_i$ is non-constant, hence not a unit in R. Hence there exists a prime divisor $P \in R$. As no P_i divides f, P cannot be multiplicatively equivalent to any P_i ↯. □

Lemma 2.38 (Ring of rational functions not of finite type)**.** If $n > 0$, then $K(X_1, \dots, X_n)/K$ is not of finite type.

Proof. Suppose $(f_i)_{i=1}^m$ generate $K(X_1, \dots, X_n)$ as a K-algebra. Let $f_i = \frac{a_i}{b}, a_i \in R, b \in R\backslash\{0\}$. Then $bf_i \in R$, and as the f_i generate $K(X_1, \dots, X_n)$ as a K-algebra, for every $g \in K(X_1, \dots, X_n)$ there is $N \in \mathbb{N}$ with

$$b^N g \in R \tag{+}$$

However, if $b = \varepsilon \prod_{i=1}^l P_i$ is a decomposition of b into prime factors P_i and a unit ε in R and $g = \frac{1}{P}$, where $P \in R$ is a prime element not multiplicatively equivalent to any P_i, then (+) fails for any $N \in \mathbb{N}$. □

The Nullstellensatz (2.3) can be reduced to the case of 2.38:

Proof. (Artin-Tate proof of HNS) Let $(l_i)_{i=1}^n$ be a transcendence base of L/K. If $n = 0$ then L/K is algebraic, hence an integral ring extension, hence a finite ring extension (1.10.5).

Suppose $n > 0$. Let $\tilde{R} \subseteq L$ be the K-subalgebra generated by the l_i. We have $\tilde{R} \cong R := K[X_1, \dots, X_n]$, as the l_i are algebraically independent. As they are a transcendence base, L is algebraic over the field of quotients $Q(\tilde{R})$, hence integral over $Q(\tilde{R})$.

As L/K is of finite type, so is $L/Q(\tilde{R})$ and it follows that $L/Q(\tilde{R})$ is a finite ring extension. By Artin-Tate (2.35), $Q(\tilde{K})$ is of finite type over K. This contradicts 2.38, as $R \cong \tilde{R} \implies K(X_1, \dots, X_n) \cong Q(\tilde{R})$. □

2.8 Transcendence degree and Krull dimension

Let $R = \mathfrak{k}[X_1, \dots, X_n]$.

Notation 2.38.30. Let $X \subseteq \mathfrak{k}^n$ be an irreducible closed subset. Then $X = V(\mathfrak{p})$ for a unique prime ideal $\mathfrak{p} \subseteq R$. Let $\mathfrak{K}(X) := Q(R/\mathfrak{p})$ denote the field of quotients of $R/\mathfrak{p}$.

Remark 2.38.31. As the elements of $\mathfrak{p}$ vanish on X, $R/\mathfrak{p}$ may be viewed as the ring of polynomials and $\mathfrak{K}(X)$ as the field of rational functions on X.

Theorem 2.39. If $X \subseteq \mathfrak{k}^n$ is irreducible, then $\dim X = \operatorname{trdeg}(\mathfrak{k}(X)/\mathfrak{k})$ and $\operatorname{codim}(X, \mathfrak{k}^n) = n - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$. More generally if $Y \subseteq \mathfrak{k}^n$ is irreducible and $X \subseteq Y$, then $\operatorname{codim}(X, Y) = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$.

Proof. One part will be shown in "A first result on dimension theory" (2.49) and other one in "Aplication to dimension theory: Proof of $\dim Y = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k})$" (2.13.2). The theorem is a special case of 2.69. ☐

Remark 2.39.32. Loosely speaking, the Krull dimension of X is equal to the maximal number of $\mathfrak{k}$-algebraically independent rational functions on X. This is yet another indication that the notion of dimension is the "correct" one.

Remark 2.39.33. 2.26 follows.

2.9 The spectrum of a ring

Definition 2.40 (Spectrum)**.** Let R be a commutative ring.

- Let $\operatorname{Spec} R$ denote the set of prime ideals and $\operatorname{MaxSpec} R \subseteq \operatorname{Spec} R$ the set of maximal ideals of R.
- For an ideal $I \subseteq R$ let $V(I) := \{\mathfrak{p} \in \operatorname{Spec} R | I \subseteq \mathfrak{p}\}$
- We equip $\operatorname{Spec} R$ with the **Zariski-Topology** for which the closed subsets are the subsets of the form $V(I)$, where I runs over the set of ideals in R.

Remark 2.40.34. When $R = \mathfrak{k}[X_1, \ldots, X_n]$, the notation $V(I)$ clashes with the previous notation. When several types of $V(I)$ will be in use, they will be distinguished using indices.

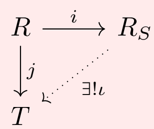
Remark 2.40.35. Let $(I_\lambda)_{\lambda \in \Lambda}$ and $(l_j)_{j=1}^n$ be ideals in R, where Λ may be infinite. We have $V(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} V(I_\lambda)$ and $V(\bigcap_{j=1}^n I_j) = V(\prod_{j=1}^n I_j) = \bigcup_{j=1}^n V(I_j)$. Thus, the Zariski topology on $\operatorname{Spec} R$ is a topology.

Remark 2.40.36. Let $R = \mathfrak{k}[X_1, \ldots, X_n]$. Then there exists a bijection (2.14, 2.22) between $\operatorname{Spec} R$ and the set of irreducible closed subsets of $\mathfrak{k}^n$ sending $\mathfrak{p} \in \operatorname{Spec} R$ to $V_{\mathfrak{k}^n}(\mathfrak{p})$ and identifying the one-point subsets with $\operatorname{MaxSpec} R$. This defines a bijection $\mathfrak{k}^n \cong \operatorname{MaxSpec} R$ which is a homeomorphism if $\operatorname{MaxSpec} R$ is equipped with the induced topology from the Zariski topology on $\operatorname{Spec} R$.

2.10 Localization of rings

Definition 2.41 (Multiplicative subset)**.** A **multiplicative subset** of a ring R is a subset $S \subseteq R$ such that $\prod_{i=1}^n f_i \in S$ when $n \in \mathbb{N}$ and all $f_i \in S$.

Proposition 2.42. Let $S \subseteq R$ be a multiplicative subset. Then there is a ring homomorphism $R \xrightarrow{i} R_S$ such that $i(S) \subseteq R_S^\times$ and i has the **universal property** for such ring homomorphisms: If $R \xrightarrow{j} T$ is a ring homomorphism with $j(S) \subseteq T^\times$, then there is a unique ring homomorphism $R_S \xrightarrow{\iota} T$ with $j = \iota i$.



Proof. The construction is similar to the construction of the field of quotients:

Let $R_S := (R \times S)/\sim$, where $(r,s) \sim (\rho,\sigma) :\iff \exists t \in S\ t\sigma r = ts\rho$. [5] $[r,s] + [\rho,\sigma] := [r\sigma + \rho s, s\sigma]$, $[r,s] \cdot [\rho,\sigma] := [r \cdot \rho, s \cdot \sigma]$.

In order proof the universal property define $\iota([r,s]) := \frac{j(r)}{j(s)}$. The universal property characterizes R_S up to unique isomorphism. □

Remark 2.42.37. i is often not injective and $\ker(i) = \{r \in R | \exists s \in S\ s \cdot r = 0\}$. In particular $(r = 1)$, R_S is the null ring iff $0 \in S$.

Notation 2.42.38. Let $S \subseteq R$ be a multiplicative subset of R. We write $\frac{r}{s}$ for $[r,s]$. The ring homomorphism $R \xrightarrow{i} R_S$ i given by $i(r) = \frac{r}{1}$. For $X \subseteq R_S$ let $X \sqcap R$ denote $i^{-1}(X)$.

Definition 2.43 (S-saturated ideal)**.** An ideal $I \subseteq R$ is called ***S*-saturated** if for all $s \in S, r \in R$ $rs \in I \implies r \in I$.

Fact 2.43.39. A prime ideal $\mathfrak{p} \subseteq \operatorname{Spec} R$ is S-saturated iff $\mathfrak{p} \cap S = \varnothing$.

Because the elements of S become units in R_S, $J \sqcap R$ is an S-saturated ideal in R when J is an ideal in R_S.

Fact 2.43.40. Let $I \subseteq R$ be an S-saturated ideal and let I_S denote the ideal $\{\frac{r}{s} | r \in R, s \in S\} \subseteq R_S$. Then for all $r \in R, s \in S$ we have $\frac{r}{s} \in I_S \iff r \in I$.

Proof. Clearly $i \in I \implies \frac{i}{s} \in I_S$. If $\frac{i}{s} \in J$ there are $\iota \in I$, $\sigma \in S$ such that $\frac{i}{s} = \frac{\iota}{\sigma}$ in R_S. This equation holds iff there exists $t \in S$ such that $ts\iota = t\sigma i$. But $ts\iota \in I$ hence $i \in I$, as I is S-saturated. □

[5] t does not appear in the construction of the field of quotients, but is important if S contains zero divisors.

Fact 2.43.41. The inverse image of a prime ideal under any ring homomorphism is a prime ideal.

Proposition 2.44.

$$\begin{aligned} f : \{I \subseteq R | I \text{ } S\text{-saturated ideal}\} &\longrightarrow \{J \subseteq R_S | J \text{ ideal}\} \\ I &\longmapsto I_S := \left\{\frac{i}{s} | i \in I, s \in S\right\} \\ J \sqcap R &\longleftarrow J \end{aligned}$$

is a bijection. Under this bijection I is a prime ideal iff $f(I)$ is.

Proof. Applying 2.43.40 to $s = 1$ gives $I_S \sqcap R = I$, when I is S-saturated.

Conversely, if J is given and $I = J \sqcap R$, $\frac{r}{s} \in R_S$, then by 2.43.40 $\frac{r}{s} \in IR_S \iff r \in I$. But as $\frac{r}{1} = s \cdot \frac{r}{s}$ and $s \in R_S^\times$, we have $r \in I \iff \frac{r}{1} \in J \iff \frac{r}{s} \in J$. We have thus shown that the two maps between sets of ideals are well-defined and inverse to each other.

By 2.43.41, $J \in \operatorname{Spec} R_S \implies f^{-1}(J) = J \cap R \in \operatorname{Spec} R_S$. Suppose $I \in \operatorname{Spec} R$, $\frac{a}{s} \cdot \frac{b}{t} \in I_S$ for some $a, b \in R, s, t \in S$. By 2.43.40 $ab \in I$. Thus $a \in I \vee b \in I$, hence $\frac{a}{s} \in I_S \vee \frac{b}{t} \in I_S$ and we have $I_S \in \operatorname{Spec} R_S$. □

Remark 2.44.42. Let R be a domain. If $S = R \backslash \{0\}$, then R_S is the field of quotients $Q(R)$. If $S \subseteq R\backslash\{0\}$, then

$$R_S \cong \left\{\frac{a}{s} \in K | a \in R, s \in S\right\}$$

In particular $Q(R) \cong Q(R_S)$.

Definition 2.45 (S-saturation)**.** Let R be any ring, $I \subseteq R$ an ideal. Even if I is not S-saturated, $J = I_S := \{\frac{i}{s} | i \in I, s \in S\}$ is an ideal in R_S, and $I_S \sqcap R = \{r \in R | s \cdot r \in I, s \in S\}$ is called the **S-saturation of I** which is the smallest S-saturated ideal containing I.

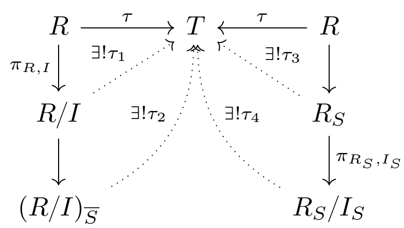
Lemma 2.46. In the situation of 2.45, if $\overline{S}$ denotes the image of S in R/I, there is a canonical isomorphism $R_S/I_S \cong (R/I)_{\overline{S}}$.

Proof. We show that both rings have the universal property for ring homomorphisms $R \xrightarrow{\tau} T$ with $\tau(I) = \{0\}$ and $\tau(S) \subseteq T^\times$. For such τ, by the fundamental theorem on homomorphisms[6] there is a unique $R/I \xrightarrow{\tau_1} T$ such that $\tau = \tau_1 \pi_{R,I}$.

[6] Homomorphiesatz

We have $\tau_1(\overline{S}) = \tau(S) \subseteq T^\times$, hence there is a unique $(R/I)_{\overline{S}} \xrightarrow{\tau_2} T$ such that the composition $R/I \to (R/I)_{\overline{S}} \xrightarrow{\tau_2} T$ equals τ_1. It is easy to see that this is the only one for which $R \to R/I \to (R/I)_{\overline{S}} \xrightarrow{\tau_2} T$ equals τ.

Similarly, by the universal property of R_S there is a unique $R_S \xrightarrow{\tau_3} T$ whose composition with $R \to R_S$ equals τ. $\tau_3(I_S) = 0$, hence a unique $R_S/I_S \xrightarrow{\tau_4} T$ whose composition with π_{R_S,I_S} equals τ_3 exists. This is the only one for which the composition $R \to R_S \to R_S/I_S \xrightarrow{\tau_4} T$ equals τ.



□

2.11 A first result of dimension theory

Notation 2.46.43. Let R be a ring, $\mathfrak{p} \in \operatorname{Spec} R$. Let $\mathfrak{k}(\mathfrak{p})$ denote the field of quotients of the domain $R/\mathfrak{p}$. This is called the **residue field** of $\mathfrak{p}$.

Proposition 2.47. Let $\mathfrak{l}$ be a field, A a $\mathfrak{l}$-algebra of finite type and $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} A$ with $\mathfrak{p} \subsetneq \mathfrak{q}$. Then

$$\operatorname{trdeg}(\mathfrak{k}(\mathfrak{p})/\mathfrak{l}) > \operatorname{trdeg}(\mathfrak{k}(\mathfrak{q})/\mathfrak{l})$$

Proof. Replacing A by $A/\mathfrak{p}$, we may assume $\mathfrak{p} = \{0\}$ and A to be a domain. Then $\mathfrak{k}(\mathfrak{p}) = Q(A/\mathfrak{p}) = Q(A)$.

If $\mathfrak{q}$ is a maximal ideal, $\mathfrak{k}(\mathfrak{q}) = A/\mathfrak{q}$ is of finite type over $\mathfrak{l}$, hence a finite field extension of $\mathfrak{l}$ by the Nullstellensatz (2.3). Thus, $\operatorname{trdeg}(\mathfrak{k}(\mathfrak{q})/\mathfrak{l}) = 0$. If $\operatorname{trdeg}(Q(A)/\mathfrak{l}) = 0$, A would be integral over $\mathfrak{l}$, hence a field (fact about integrality and fields, 1.10.7). But if A is a field, $\mathfrak{p} = \{0\}$ is a maximal ideal of A, hence $\mathfrak{q} = \mathfrak{p}$ ↯. This finishes the proof for $\mathfrak{q} \in \operatorname{MaxSpec} A$. We will use the following lemma to reduce the general case to this case:

Lemma 2.48. There are algebraically independent $a_1, \ldots, a_n \in A$ whose images in $A/\mathfrak{q}$ form a transcendence base for $\mathfrak{k}(\mathfrak{q})/\mathfrak{l}$.

Subproof. There exist $a_1, \dots, a_n \in A$ such that $\mathfrak{k}(\mathfrak{q})$ is algebraic over the subfield generated by $\mathfrak{l}$ and their images $\overline{a_i}$ (for instance generators of A as a $\mathfrak{l}$-algebra). We may assume that n is minimal. If the a_i are $\mathfrak{l}$-algebraically dependent, then w.l.o.g. $\overline{a_n}$ can be assumed to be algebraic over the subfield generated by $\mathfrak{l}$ and the $\overline{a_i}, 1 \leqslant i < n$. Thus, a_n could be removed, contradicting the minimality. ∎

Let $\mathfrak{q}$ be any prime ideal. Take $a_1, \dots, a_n \in A$ as in the lemma. As the a_i mod $\mathfrak{q}$ are $\mathfrak{l}$-algebraically independent, the same holds for the a_i themselves. Thus $\operatorname{trdeg}(Q(A)/\mathfrak{l}) \geqslant n$ and the inequality is strict, if it can be shown that the a_i fail to be a transcendence base of $Q(A)/\mathfrak{l}$. Let $R \subseteq A$ denote the $\mathfrak{l}$-subalgebra generated by $a_1, \dots, a_n$ and $S := R \backslash \{0\}$. We must show, that $Q(A)$ fails to be algebraic over $\mathfrak{l}_1 := R_S = Q(R)$. Let $A_1 := A_S$ and $\mathfrak{q}_S$ the prime ideal corresponding to $\mathfrak{q}$ as in 2.44. We have $\mathfrak{q}_S \neq \{0\}$ as $\{0_A\}_S = \{0_{A_S}\}$. A_1 is a domain with $Q(A_1) \cong Q(A)$ (2.44.42) and $A_1/\mathfrak{q}_S$ is isomorphic to the localization of $A/\mathfrak{q}$ with respect to the image of S in $A/\mathfrak{q}$ (2.46). $\mathfrak{k}(\mathfrak{q}_S)$ is algebraic over $\mathfrak{l}_1$ because the image of $\mathfrak{l}_1$ in $\mathfrak{k}(\mathfrak{q}_S)$ contains the images of $\mathfrak{l}$ and the a_i, and the images of the a_i form a transcendence base for $\mathfrak{k}(\mathfrak{q})/\mathfrak{l}$. By the fact about integrality and fields (1.10.7) it follows that $A_1/\mathfrak{q}_S$ is a field, hence $\mathfrak{q}_S \in \operatorname{MaxSpec}(A_1)$ and the special case of $\mathfrak{q} \in \operatorname{MaxSpec}(A)$ can be applied to $\mathfrak{q}_S$ and $A_1/\mathfrak{l}_1$ showing that $Q(A)$ cannot be algebraic over $\mathfrak{l}_1$. □

Corollary 2.49. Let $X, Y \subseteq \mathfrak{k}^n$ be irreducible and closed. Then $\operatorname{codim}(X, Y) \leqslant \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$.

Proof. Let $X = X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_c = Y$ be a chain of irreducible closed subsets between X and Y. Then $X_i = V(\mathfrak{p}_i)$ for prime ideals $\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \dots \supsetneq \mathfrak{p}_c$ in $R = \mathfrak{k}[X_1, \dots, X_n]$. By 2.47 we have $\operatorname{trdeg}(\mathfrak{k}(\mathfrak{p}_i)/\mathfrak{k}) < \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p}_{i+1})/\mathfrak{k})$ for all $0 \leqslant i < c$. Thus

$$c + \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k}) = c + \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p}_0)/\mathfrak{k}) \leqslant \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p}_c)/\mathfrak{k}) = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}).$$

As $\operatorname{codim}(X, Y) = \sup\{c \in \mathbb{N} | \exists X = X_0 \subsetneq \dots \subsetneq X_c = Y \text{ irreducible, closed}\}$ it follows that

$$\operatorname{codim}(X, Y) \leqslant \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$$

□

Corollary 2.50. Let $Z \subseteq \mathfrak{k}^n$ be irreducible and closed. Then

$$\dim Z \leqslant \operatorname{trdeg}(\mathfrak{K}(Z)/\mathfrak{k})$$

and

$$\operatorname{codim}(Z, \mathfrak{k}^n) \leqslant n - \operatorname{trdeg}(\mathfrak{K}(Z)/\mathfrak{k}.$$

Proof. Take $X = \{z\}$ and $Y = Z$ or $X = Z$ and $Y = \mathfrak{k}^n$ in 2.49. □

2.12 Local rings

Definition 2.51 (Local ring)**.** Let R be a ring. R is called a **local ring**, if the following equivalent conditions hold:

- $\# \operatorname{MaxSpec} R = 1$
- $R \backslash R^{\times}$ is an ideal.

If this holds, $\mathfrak{m}_R := R \backslash R^{\times}$ is the unique maximal ideal of R.

Proof. Suppose $\operatorname{MaxSpec} R = \{\mathfrak{m}\}$. If $x \in \mathfrak{m}$, then $x \notin R^{\times}$ as otherwise $xR = R \implies \mathfrak{m} = R$. If $x \notin R^{\times}$ then xR is a proper ideal, hence contained in some maximal ideal. Thus $x \in \mathfrak{m}$.

Assume that $\mathfrak{m} = R \backslash R^{\times}$ is an ideal in R. As $1 \in R^{\times}$ this is a proper ideal. If I is any proper ideal and $x \in I$, then $x \in \mathfrak{m}$. Hence $R = xR \subseteq I \subseteq \mathfrak{m}$. It follows that $\mathfrak{m}$ is the only maximal ideal of R. □

Remark 2.51.44.

- Any field is a local ring ($\mathfrak{m}_K = \{0\}$).
- The null ring is not local as it has no maximal ideals.

2.12.1 Localization at a prime ideal

Many questions of commutative algebra are easier in the case of local rings. Localization at a prime ideal is a technique to reduce a problem to this case.

Proposition 2.52 (Localization at a prime ideal)**.** Let A be a ring and $\mathfrak{p} \in \operatorname{Spec} A$. Then $S := A \backslash \mathfrak{p}$ is a multiplicative subset, A_S is a local ring with maximal ideal $\mathfrak{m} = \mathfrak{p}_S = \{\frac{p}{s} | p \in \mathfrak{p}, s \in S\}$.

We have a bijection

$$\begin{aligned} f : \operatorname{Spec} A_S &\longrightarrow \{\mathfrak{q} \in \operatorname{Spec} A | \mathfrak{q} \subseteq \mathfrak{p}\} \\ \mathfrak{r} &\longmapsto \mathfrak{r} \sqcap A \\ \mathfrak{q}_S := \left\{\frac{q}{s} | q \in \mathfrak{q}, s \in S\right\} &\longleftarrow \mathfrak{q} \end{aligned}$$

Proof. It is clear that S is a multiplicative subset and that $\mathfrak{p}_S$ is an ideal. By 2.43.40 $\frac{a}{s} \in \mathfrak{p}_S \iff a \in \mathfrak{p} \iff a \in A \backslash S$ for all $a \in A$, $s \in S$. Thus, if $\frac{a}{s} \notin \mathfrak{p}_S$ then it is a unit in A_S with inverse $\frac{s}{a}$. Hence A_S is a local ring with maximal ideal $\mathfrak{p}_S$.

The claim about $\operatorname{Spec} A_S$ follows from 2.44 using the fact (2.43.39) that a prime ideal $\mathfrak{r} \in \operatorname{Spec} A$ is S-saturated iff it is disjoint from $S = A \backslash \mathfrak{p}$ iff $\mathfrak{r} \subseteq \mathfrak{p}$. □

Definition 2.53. The ring A_S as in 2.52 is called the **localization of A at the prime ideal $\mathfrak{p}$** and denoted $A_{\mathfrak{p}}$.

Remark 2.53.45. This introduces no ambiguity because a prime ideal is never a multiplicative subset.

Remark 2.53.46. Let $B = \mathfrak{k}[X_1, \ldots, X_n]$, $x \in \mathfrak{k}^n$ and $\mathfrak{m}$ the maximal ideal such that $V(\mathfrak{m}) = \{x\}$. The elements of $B_{\mathfrak{m}}$ are the fractions $\frac{b}{s}$, $b \in B, s \in B \backslash \mathfrak{m}$, i.e. $s(x) \neq 0$. These are precisely the rational functions which are well-defined in some neighbourhood of x. This will be rigorously formulated in 4.28.

Remark 2.53.47. Let $Y = V(\mathfrak{p}) \subseteq \mathfrak{k}^n$ be an irreducible subset of $\mathfrak{k}^n$. Elements of $B_{\mathfrak{p}}$ are the fractions $\frac{b}{s}, s \notin \mathfrak{p}$, i.e. s does not vanish identically on Y. Thus, $B_{\mathfrak{p}}$ is the ring of rational functions on $\mathfrak{k}^n$ which are well defined on some open subset U intersecting Y. As Y is irreducible, the intersection of two such subsets still intersects Y.

Remark 2.53.48. For arbitrary A, we have a bijection $\operatorname{Spec} A_{\mathfrak{p}} \cong N = \{\mathfrak{q} \in \operatorname{Spec} A | \mathfrak{p} \subseteq \mathfrak{p}\}$. One can show that N is the intersection of all neighbourhoods of $\mathfrak{p}$ in $\operatorname{Spec} A$, confirming the intuition that "the localization sees things which go on in arbitrarily small neighbourhoods of $\mathfrak{p}$".

Remark 2.53.49. If A is a domain and $\mathfrak{p} = \{0\}$, then $A_{\mathfrak{p}} = Q(A)$.

2.13 Going-up and going-down

Definition 2.54 (Going-up and going-down)**.** Let R be a ring and A an R-algebra.

Going-up holds for A/R if for arbitrary $\mathfrak{q} \in \operatorname{Spec} A$ and arbitrary $\tilde{\mathfrak{p}} \in \operatorname{Spec} R$ with $\tilde{\mathfrak{p}} \supseteq \mathfrak{q} \sqcap R$ there exists $\tilde{\mathfrak{q}} \in \operatorname{Spec} A$ with $\mathfrak{q} \subseteq \tilde{\mathfrak{q}}$ and $\tilde{\mathfrak{p}} = \tilde{\mathfrak{q}} \sqcap R$.

(We are given $\mathfrak{p} \subseteq \tilde{\mathfrak{p}}$ and $\mathfrak{q}$ such that $\mathfrak{p} = \mathfrak{q} \sqcap R$ and must make $\mathfrak{q}$ larger).

$$\begin{array}{ccccc} \mathfrak{q} & \subseteq & \tilde{\mathfrak{q}} & \in \operatorname{Spec} A \\ \big\downarrow{\scriptstyle \cdot \sqcap R} & & \big\downarrow{\scriptstyle \cdot \sqcap R} & \\ \mathfrak{q} \sqcap R = \mathfrak{p} & \subseteq & \tilde{\mathfrak{p}} & \in \operatorname{Spec} R \end{array}$$

Going-down holds for A/R if for arbitrary $\tilde{\mathfrak{q}} \in \operatorname{Spec} A$ and arbitrary $\mathfrak{p} \in \operatorname{Spec} R$ with $\mathfrak{p} \subseteq \tilde{\mathfrak{q}} \sqcap R$, there exists $\mathfrak{q} \in \operatorname{Spec} A$ with $\mathfrak{q} \subseteq \tilde{\mathfrak{q}}$ and $\mathfrak{p} = \mathfrak{q} \sqcap R$.

(We are given $\mathfrak{p} \subseteq \tilde{\mathfrak{p}}$ and $\tilde{\mathfrak{q}}$ such that $\tilde{\mathfrak{p}} = \tilde{\mathfrak{q}} \sqcap R$ and must make $\tilde{\mathfrak{q}}$ smaller).

$$\begin{array}{ccccc} \mathfrak{q} & \subseteq & \tilde{\mathfrak{q}} & & \in \operatorname{Spec} A \\ \downarrow{\scriptstyle \cdot \sqcap R} & & \downarrow{\scriptstyle \cdot \sqcap R} & & \\ \mathfrak{p} & \subseteq & \tilde{\mathfrak{p}} = \tilde{\mathfrak{q}} \sqcap R & & \in \operatorname{Spec} R \end{array}$$

Remark 2.54.50. In the situation of 2.54, we say $\mathfrak{q} \in \operatorname{Spec} A$ **lies above** $\mathfrak{p} \in \operatorname{Spec} R$ if $\mathfrak{q} \sqcap R = \mathfrak{p}$.

2.13.1 Going-up for integral ring extensions

Theorem 2.55 (Krull, Cohen-Seidenberg)**.** Let A be a ring and $R \subseteq A$ a subring such that A is integral over R.

A The map $\operatorname{Spec} A \xrightarrow{\mathfrak{q} \mapsto \mathfrak{q} \cap R} \operatorname{Spec} R$ is surjective.

B For $\mathfrak{p} \in \operatorname{Spec} R$, there are no inclusions between the prime ideals $\mathfrak{p} \in \operatorname{Spec} A$ lying over $\mathfrak{p}$.

C Going-up holds for A/R.

D $\mathfrak{q} \in \operatorname{Spec} A$ is maximal iff $\mathfrak{p} := \mathfrak{q} \cap R$ is a maximal ideal of R.

Proof. D Consider the ring extension $A/\mathfrak{q}$ of $R/\mathfrak{p}$. Both rings are domains and the extension is integral. By the fact about integrality and fields (1.10.7) $A/\mathfrak{q}$ is a field iff $R/\mathfrak{p}$ is a field. Thus $\mathfrak{q} \in \operatorname{MaxSpec} A \iff \mathfrak{p} \in \operatorname{MaxSpec} R$.

A Suppose $\mathfrak{p} \in \operatorname{Spec} R$ and let $S := R \backslash \mathfrak{p}$. Then S is a multiplicative subset of both R and A, and we may consider the localizations $R \xrightarrow{\rho} R_{\mathfrak{p}}, A \xrightarrow{\alpha} A_{\mathfrak{p}}$ with respect to S. By the universal property of ρ, there exists a unique homomorphism $R_{\mathfrak{p}} \xrightarrow{i} A_{\mathfrak{p}}$ such that $i\rho = \alpha \upharpoonright_R$. We have $j(\frac{r}{s}) = \frac{r}{s}$ and j is easily seen to be injective.

$$\begin{array}{ccc} R & \xrightarrow{\rho} & R_{\mathfrak{p}} \\ \downarrow{\scriptstyle \subseteq} & & \downarrow{\scriptstyle \exists ! i} \\ A & \xrightarrow{\alpha} & A_{\mathfrak{p}} \end{array}$$

Claim 1. *$A_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$.*

Subproof. An element $x \in A_{\mathfrak{p}}$ has the form $x = \frac{a}{s}$ for some $s \in R \backslash \mathfrak{p}$ and where $a \in A$ is integral over R. Hence $a^n = \sum_{i=0}^{n-1} r_i a^i$ for some $r_i \in R$. Thus $x^n = \sum_{i=0}^{n-1} \rho_i x^i$ with $\rho_i := s^{i-n} r_i \in R_{\mathfrak{p}}$. ■

As i is injective and $R_\mathfrak{p} \neq \{0\}$ ($R_\mathfrak{p}$ is local!) $A_\mathfrak{p} \neq \{0\}$, there is $\mathfrak{m} \in \operatorname{MaxSpec} A_\mathfrak{p}$. D has already been shown and applies to $A_\mathfrak{p}/R_\mathfrak{p}$, hence $i^{-1}(\mathfrak{m}) = \mathfrak{p}_\mathfrak{p}$ is the only maximal ideal of the local ring $R_\mathfrak{p}$. Hence $\mathfrak{q} = \alpha^{-1}(\mathfrak{m})$ satisfies

$$\mathfrak{q} \cap R = \alpha^{-1}(\mathfrak{m}) \cap R = \rho^{-1}(i^{-1}(\mathfrak{m})) = \rho^{-1}(\mathfrak{p}_\mathfrak{p}) = \mathfrak{p}.$$

B The map $\operatorname{Spec} A_\mathfrak{p} \xrightarrow{\alpha^{-1}} \operatorname{Spec} A$ is injective with image equal to $\{\mathfrak{q} \in \operatorname{Spec} A | \mathfrak{q} \cap R \subseteq \mathfrak{p}\}$. In particular, it contains the set of all $\mathfrak{q}$ lying over $\mathfrak{p}$. If $\mathfrak{q} = \alpha^{-1}(\mathfrak{r})$ lies over $\mathfrak{p}$, then

$$\rho^{-1}(i^{-1}(\mathfrak{r})) = (\alpha^{-1}(\mathfrak{r})) \cap R = \mathfrak{q} \cap R = \mathfrak{p} = \rho^{-1}(\mathfrak{p}_\mathfrak{p})$$

hence $i^{-1}(\mathfrak{r}) = \mathfrak{p}_\mathfrak{p}$ by the injectivity of $\operatorname{Spec} R_\mathfrak{p} \xrightarrow{\rho^{-1}} \operatorname{Spec} R$.

Because D applies to the integral ring extension $A_\mathfrak{p}/R_\mathfrak{p}$ and $\mathfrak{p}_\mathfrak{p} \in \operatorname{MaxSpec} R_\mathfrak{p}$, $\mathfrak{r}$ is a maximal ideal. There are thus no inclusions between different such $\mathfrak{r}$. Because $\operatorname{Spec} A_\mathfrak{p} \xrightarrow{\alpha^{-1}} \operatorname{Spec} A$ is $\subseteq$-monotonic and injective, there are no inclusions between different $\mathfrak{p} \in \operatorname{Spec} A$ lying over $\mathfrak{p}$.

C Let $\mathfrak{p} \subseteq \tilde{\mathfrak{p}}$ be prime ideals of R and $\mathfrak{q} \in \operatorname{Spec} A$ such that $\mathfrak{q} \cap R = \mathfrak{p}$. By applying A to the ring extension $A/\mathfrak{q}$ of $R/\mathfrak{p}$, there is $\mathfrak{r} \in \operatorname{Spec} A/\mathfrak{q}$ such that $\mathfrak{r} \sqcap R/\mathfrak{p} = \tilde{\mathfrak{p}}/\mathfrak{p}$. The preimage $\tilde{\mathfrak{q}}$ of $\mathfrak{r}$ under $A \to A/\mathfrak{q}$ satisfies $\mathfrak{q} \subseteq \tilde{\mathfrak{q}}$ and $\tilde{\mathfrak{q}} \cap R = \tilde{\mathfrak{p}}$.

□

Remark 2.55.51. The proof of 2.55 does not use Noetherianness, as this is not an assumption.

2.13.2 Application to dimension theory: Proof of $\dim Y = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k})$

This is part of the proof of 2.39.

Proof. Let $B = \mathfrak{k}[X_1, \ldots, X_n]$ and let $X \subseteq Y \subseteq \mathfrak{k}^n$ be irreducible closed subsets of $\mathfrak{k}^n$. We have to show $\operatorname{codim}(X, Y) = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)\backslash\mathfrak{k})$. The inequality

$$\operatorname{codim}(X, Y) \leqslant \operatorname{trdeg}(\mathfrak{K}(Y)\backslash\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)\backslash\mathfrak{k})$$

has been shown in 2.49. In the case of $X = \{0\}$, $Y = \mathfrak{k}^n$, equality holds because the chain of irreducible subsets $\{0\} \subsetneq \{0\} \times \mathfrak{k} \subsetneq \ldots \subsetneq \{0\} \times \mathfrak{k}^n \subsetneq \mathfrak{k}^n$ can be written down explicitly.

We have $Y = V(\mathfrak{p})$ for a unique $\mathfrak{p} \in \operatorname{Spec} B$. Let $A = B/\mathfrak{p}$ be the ring of polynomials on Y. Apply the Noether normaization theorem to A. This yields $(f_i)_{i=1}^d \in A^d$ which are algebraically independent over $\mathfrak{k}$ and such that A is finite over the subalgebra generated by the f_i. Let L be the algebraic closure in $\mathfrak{K}(Y)$ of the subfield of $\mathfrak{K}(Y)$ generated by $\mathfrak{k}$ and the f_i. We have $A \subseteq L$ and since $\mathfrak{K}(Y) = Q(B/\mathfrak{p}) = Q(A)$[7] it follows that $\mathfrak{K}(Y) = L$. Hence $(f_i)_{i=1}^d$ is a transcendence base for $\mathfrak{K}(y)/\mathfrak{k}$ and $d = \operatorname{trdeg} \mathfrak{K}(Y)/\mathfrak{k}$.

$$\begin{aligned} \mathfrak{k}[X_1, \dots, X_d] &\longrightarrow R \\ P &\longmapsto P(f_1, \dots, f_d) \end{aligned}$$

is an isomorphism and in $\mathfrak{k}[X_1, \dots, X_d]$ there is a strictly ascending chain of prime ideals corresponding to $\mathfrak{k}^d \supsetneq \{0\} \times \mathfrak{k}^{d-1} \supsetneq \dots \supsetneq \{0\}$. Thus there is a strictly ascending chain $\{0\} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_d$ of elements of $\operatorname{Spec} R$. Let $\mathfrak{q}_0 = \{0\} \in \operatorname{Spec} A$. If $0 < i \leqslant d$ and a chain $\mathfrak{q}_0 \subsetneq \dots \subsetneq \mathfrak{q}_{i-1}$ in $\operatorname{Spec} A$ with $\mathfrak{q}_j \cap R = \mathfrak{p}_j$ for $0 \leqslant j < i$ has been selected, we may apply going-up (2.55) to A/R to extend this chain by a $\mathfrak{q}_i \in \operatorname{Spec} A$ with $\mathfrak{q}_{i-1} \subseteq \mathfrak{q}_i$ and $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ (thus $\mathfrak{q}_{i-1} \subsetneq \mathfrak{q}_i$ as $\mathfrak{p} - i \neq \mathfrak{p}_{i-1}$). Thus, we have a chain $\mathfrak{q}_0 = \{0\} \subsetneq \dots \subsetneq \mathfrak{q}_d$ in $\operatorname{Spec} A$. Let $\tilde{\mathfrak{q}}_i := \pi_{B,\mathfrak{p}}^{-1}(\mathfrak{q}_i)$, $Y_i := V(\tilde{\mathfrak{q}}_i)$. This is a chain $Y = Y_0 \supsetneq Y_1 \supsetneq \dots \supsetneq Y_d$ of irreducible subsets of $\mathfrak{k}^n$.

Hence $\dim(Y) \geqslant \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k})$.

The general case of $\operatorname{codim}(X, Y) \geqslant \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)\backslash\mathfrak{k})$ is shown in 2.13.8. □

2.13.3 Prime avoidance

Proposition 2.56 (Prime avoidance)**.** Let A be a ring and $I \subseteq A$ a subset which is closed under arbitrary finite sums and non-empty products, for instance, an ideal in A. Let $(\mathfrak{p}_i)_{i=1}^n$ be a finite list of ideals in A of which at most two fail to be prime ideals and such that there is no i with $I \subseteq \mathfrak{p}_i$. Then $I \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$.

Proof. Induction on n. The case of $n < 2$ is trivial. Let $n \geqslant 2$ and the assertion be shown for a list of $n-1$ ideals one wants to avoid. If $n \geqslant 3$ we may, by reordering the $\mathfrak{p}_i$, assume that $\mathfrak{p}_1$ is a prime ideal. By the induction assumption, there is $f_k \in I \backslash \bigcup_{j \neq k} \mathfrak{p}_j$. If there is k with $1 \leqslant k \leqslant n$ and $f_k \notin \mathfrak{p}_k$, then the proof is finished. Otherwise

$$f_1 + \prod_{j=2}^n f_j \in I \backslash \bigcup_{j=1}^n \mathfrak{p}_j.$$

□

2.13.4 The fixed field of the automorphism group of a normal field extension

Recall the definition of a normal field extension in the case of finite field extensions:

[7] by definition

Definition 2.57. A finite field extension L/K is called **normal**, if the following equivalent conditions hold:

A Let $\overline{K}/K$ be an algebraic closure of K. Then any two expansions of Id_K to a ring homomorphism $L \to \overline{K}$ have the same image.

B If $P \in K[T]$ is an irreducible polynomial and P has a zero in L, then P splits into linear factors.

C L is the splitting field of a $P \in K[T]$.

Fact 2.57.52. For an arbitrary algebraic field extension L/K, the following conditions are equivalent:

- L is the union of its subfields which contain K and are finite and normal over K.
- If $P \in K[T]$ is normed, irreducible over K and has a zero in L, then it splits into linear factors in L.
- If $\overline{L}$ is an algebraic closure of L, then all extensions of Id_K to a ring homomorphism $L \to \overline{L}$ have the same image.

Definition 2.58 (Normal field extension)**.** An algebraic field extension[a] L/K is called **normal** if the equivalent conditions from 2.57.52 hold.

[a]not necessarily finite

Definition 2.59. Suppose L/K is an arbitrary field extension. Let $\mathrm{Aut}(L/K)$ be the set of automorphisms of L leaving all elements of (the image in L of) K fixed. Let $G \subseteq \mathrm{Aut}(L/K)$ be a subgroup. Then the **fixed field** is definied as

$$L^G := \{l \in L | \forall g \in G : g(l) = l\}.$$

Proposition 2.60. Let L/K be a normal field extension. If the characteristic of the fields is O, then $L^{\mathrm{Aut}(L/K)} = K$. If the characteristic is $p > 0$, then $L^{\mathrm{Aut}(L/K)} = \{l \in L | \exists n \in \mathbb{N}\ l^{p^n} \in K\}$.

Proof. In both cases $L^G \supseteq$ is easy to see.

If $K \subseteq M \subseteq L$ is an intermediate field, then L is normal over M. If $\sigma \in \mathrm{Aut}(M/K)$, an application of Zorn's lemma to the set of all (N, ϑ) where N is an intermediate field $M \subseteq N \subseteq L$ and $N \xrightarrow{\vartheta} L$ a ring homomorphism such that $\vartheta \restriction_M = \sigma$ shows that σ has an extension to an element of $\mathrm{Aut}(L/K)$. If M is normal over K, it is easily seen to be $\mathrm{Aut}(L/K)$ invariant. Thus L^G is the union of $M^{\mathrm{Aut}(M/K)}$ over all intermediate fields which are finite and normal over K, and it is sufficient to show the proposition for finite normal extensions L/K.

- Characteristic 0: The extension is normal, hence Galois, and the assertion follows from Galois theory.
- Characteristic $p > 0$: Let $l \in L^G$ and $P \in K[T]$ be the minimal polynomial of l over K. We show that $l^{p^n} \in K$ for some $n \in \mathbb{N}$ by induction on $\deg(l/K) := \deg(P)$.

  If $\deg(l/K) = 1$, we have $l \in K$. Otherwise, assume that the assertion has been shown for elements of L^G whose degree over K is smaller than $\deg(l/K)$. Let $\overline{L}$ be an algebraic closure of L and λ a zero of P in $\overline{L}$. If $M = K(l) \subseteq L$, then there is a ring homomorphism $M - \overline{L}$ sending l to λ. This can be extended to a ring homomorphism $L \xrightarrow{\sigma} \overline{L}$. We have $\sigma \in G$ because L/K is normal. Hence $\lambda = \sigma(l) = l$, as $l \in L^G$. Thus l is the only zero of P in $\overline{L}$ and because $\deg P > 1$ it is a multiple zero. It is shown in the Galois theory lecture that this is possible only when $P(T) = Q(T^p)$ for some $Q \in K[T]$. Then $Q(l^p) = 0$ and the induction assumption can be applied to $x = l^p$ showing $x^{p^m} \in K$ hence $l^{p^{m+1}} \in K$ for some $m \in \mathbb{N}$.

□

2.13.5 Integral closure and normal domains

Definition 2.61 (Integral closure, normal domains)**.** Let A be a domain with field of quotients $Q(A)$ and let L be a field extension of $Q(A)$. By 1.9 the set of elements of L integral over A is a subring of L, the **integral closure** of A in L. A is **integrally closed** in L if the integral closure of A in L equals A. A is **normal** if it is integrally closed in $Q(A)$.

Proposition 2.62. Any factorial domain (UFD) is normal.

Proof. Let $x \in Q(A)$ be integral over A. Then there is a normed polynomial $P \in A[T]$ with $P(x) = 0$. In Einführung in die Algebra it was shown that $A[T]$ is a UFD and that the prime elements of $A[T]$ are the elements which are irreducible in $Q(A)[T]$ and for which the gcd of the coefficients is ~ 1. The prime factors of a normed polynomial are all normed up to multiplicative equivalence. We may thus assume P to be irreducible in $Q(A)[T]$. But then $\deg P = 1$ as x is a zero of P in $Q(A)$, hence $P(T) = T - x$ and $x \in A$ as $P \in A[T]$.

Alternative proof[8]: Let $x = \frac{a}{b} \in Q(A)$ be integral over A. Without loss of generality loss of generality $\gcd(a, b) = 1$. Then $x^n + c_{n-1}x^{n-1} + \ldots + c_0 = 0$ for some $c_i \in A$. Multiplication with b^n yields $a^n + c_{n-1}ba^{n-1} + \ldots + c_0b^n = 0$. Thus $b|a^n$. Since $\gcd(a, b) = 1$ it follows that b is a unit, hence $x \in A$. □

[8] http://www.math.lsa.umich.edu/~tfylam/Math221/2.pdf

Remark 2.62.53. It follows from 1.10 and 2.44.42 that the integral closure of A in some field extension L of $Q(A)$ is always normal.

Remark 2.62.54. A finite field extension of $\mathbb{Q}$ is called an **algebraic number field** (ANF). If K is an ANF, let $\mathcal{O}_K$ (the **ring of integers in K**) be the integral closure of $\mathbb{Z}$ in K. One can show that this is a finitely generated (hence free, by results of Einführung in die Algebra) abelian group. We have $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ by the proposiiton.

2.13.6 Action of $\mathrm{Aut}(L/K)$ on prime ideals of a normal ring extension

Theorem 2.63. Let A be a normal domain, L a normal field extension of $K := Q(A)$, B the integral closure of A in L and $\mathfrak{p} \in \operatorname{Spec} A$. Then $G := \mathrm{Aut}(L/K)$ transitively acts on $\{\mathfrak{q} \in \operatorname{Spec} B | \mathfrak{q} \cap A = \mathfrak{p}\}$.

Proof. Let $\mathfrak{q}, \mathfrak{r}$ be prime ideals of B above the given $\mathfrak{p} \in \operatorname{Spec} A$. We must show that there exists $\sigma \in G$ such that $\mathfrak{q} = \sigma(\mathfrak{r})$. This is equivalent to $\mathfrak{q} \subseteq \sigma(\mathfrak{r})$, since the Krull going-up theorem (2.55) applies to the integral ring extension B/A, showing that there are no inclusions between different elements of $\operatorname{Spec} B$ lying above $\mathfrak{p} \in \operatorname{Spec} A$.

If L/K is finite and there is no such σ, then by prime avoidance (2.56) there is $x \in \mathfrak{q} \setminus \bigcup_{\sigma \in G} \sigma(\mathfrak{r})$. As $\mathfrak{r}$ is a prime ideal, $y = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{q} \setminus \mathfrak{r}$.[9] By the characterization of L^G for normal field extensions (2.60), there is a positive integer k with $y^k \in K$. As A is normal, we have $y^k \in K \cap B = A$. Thus

$$y^k \in (A \cap \mathfrak{q}) \setminus (A \cap \mathfrak{r}) = \mathfrak{p} \setminus \mathfrak{p} = \varnothing \lightning .$$

If L/K is not finite, one applies Zorn's lemma to the poset of pairs (M, σ) where M is an intermediate field and $\sigma \in \mathrm{Aut}(M/K)$ such that $\sigma(\mathfrak{r} \cap M) = \mathfrak{q} \cap M$.

□

Remark 2.63.55. The theorem is very important for its own sake. For instance, if K is an ANF which is a Galois extension of $\mathbb{Q}$ it shows that $\mathrm{Gal}(K/\mathbb{Q})$ transitively acts on the set of prime ideals of $\mathcal{O}_K$ over a given prime number p. More generally, if L/K is a Galois extension of ANF then $\mathrm{Gal}(L/K)$ transitively acts on the set of $\mathfrak{q} \in \operatorname{Spec} \mathcal{O}_L$ for which $\mathfrak{q} \cap K$ is a given $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$.

2.13.7 A going-down theorem

[9] $\prod_{\sigma \in G} \sigma(x) = \prod_{\sigma \in G} \sigma^{-1}(x)$

Theorem 2.64 (Going-down for integral extensions of normal domains (Krull))**.** Let B be a domain which is integral over its subring A. If A is a normal domain, then going-down holds for B/A.

Proof. It follows from the assumptions that the field of quotients $Q(B)$ is an algebraic field extension of $Q(A)$. There is an algebraic extension L of $Q(B)$ such that $L/Q(A)$ is normal (for instance an algebraic closure of $Q(B)$). Let C be the integral closure of A in L. Then $B \subseteq C$ and C/B is integral.

$$\begin{array}{ccccc} Q(A) & \hookrightarrow & Q(B) & \hookrightarrow & L := \overline{Q(B)} \\ \uparrow & & \uparrow & & \uparrow \\ A & \hookrightarrow & B & \hookrightarrow & C \end{array}$$

Claim 1. *Going-down holds for C/A.*

Subproof. Let $\mathfrak{p} \subseteq \tilde{\mathfrak{p}}$ be an inclusion of prime ideals of A and $\tilde{\mathfrak{r}} \in \operatorname{Spec} C$ with $\tilde{\mathfrak{r}} \cap A = \tilde{\mathfrak{p}}$. By going-up for integral ring extensions (2.55), $\operatorname{Spec} C \xrightarrow{\cdot \cap A} \operatorname{Spec} A$ is surjective. Thus there is $\mathfrak{r}' \in \operatorname{Spec} C$ such that $\mathfrak{r}' \cap A = \mathfrak{p}$. By going up for C/A there is $\tilde{\mathfrak{r}}' \in \operatorname{Spec} C$ with $\tilde{\mathfrak{r}}' \cap A = \tilde{\mathfrak{p}}, \mathfrak{r}' \subseteq \tilde{\mathfrak{r}}'$. By the theorem about the action of the automorphism group on prime ideals of a normal ring extension (2.63) there exists a $\sigma \in \operatorname{Aut}(L/Q(A))$ with $\sigma(\tilde{\mathfrak{r}}') = \tilde{\mathfrak{r}}$. Then $\mathfrak{r} := \sigma(\mathfrak{r}')$ satisfies $\mathfrak{r} \subseteq \tilde{\mathfrak{r}}$ and $\mathfrak{r} \cap A = \mathfrak{p}$. ■

If $\mathfrak{p} \subseteq \tilde{\mathfrak{p}}$ is an inclusion of elements of $\operatorname{Spec} A$ and $\tilde{\mathfrak{q}} \in \operatorname{Spec} B$ with $\tilde{\mathfrak{p}} \cap A = \tilde{\mathfrak{p}}$, by the surjectivity of $\operatorname{Spec} C \xrightarrow{\cdot \cap B} \operatorname{Spec} B$ (2.55) there is $\tilde{\mathfrak{r}} \in \operatorname{Spec} C$ with $\tilde{\mathfrak{r}} \cap B = \mathfrak{q}$. By going-down for C/A, there is $\mathfrak{r} \in \operatorname{Spec} C$ with $\mathfrak{r} \subseteq \tilde{\mathfrak{r}}$ and $\mathfrak{r} \cap A = \mathfrak{p}$. Then $\mathfrak{q} := \mathfrak{r} \cap B \in \operatorname{Spec} B, \mathfrak{q} \subseteq \tilde{\mathfrak{q}}$ and $\mathfrak{q} \cap A = \mathfrak{p}$. Thus going-down holds for B/A. □

Remark 2.64.56 (Universally Japanese rings)**.** A Noetherian ring A is called universally Japanese if for every $\mathfrak{p} \in \operatorname{Spec} A$ and every finite field extension L of $\mathfrak{k}(\mathfrak{p})$, the integral closure of $A/\mathfrak{p}$ in L is a finitely generated A-module. This notion was coined by Grothendieck because the condition was extensively studied by the Japanese mathematician Nataga Masayoshji. By a hard result of Nagata, algebras of finite type over a universally Japanese ring are universally Japanese. Every field is universally Japanese, as is every PID of characteristic 0. There are, however, examples of Noetherian rings which fail to be universally Japanese.

Example† 2.64.57 (Counterexample to going down)**.** Let $R = \mathfrak{k}[X, Y]$ and $A = \mathfrak{k}[X, Y, \frac{X}{Y}]$. Then going down does not hold for A/R:

For any ideal $Y \in \mathfrak{q} \subseteq A$ we have $X = \frac{X}{Y} \cdot Y \in \mathfrak{q}$. Consider $(Y)_R \subsetneq (X,Y)_R \subseteq \mathfrak{q} \cap R$. As $(X,Y)_R$ is maximal and the preimage of a prime ideal is prime and thus proper, we have $(X,Y)_R = \mathfrak{q} \cap R$. The prime ideal $(\frac{X}{Y}, Y)_A = (\frac{X}{Y}, X, Y)_A$ is lying over $(X,Y)_R$, so going down is violated.

2.13.8 Proof of $\operatorname{codim}(\{y\}, Y) = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k})$

This is part of the proof of 2.39.

Proof. Let $B = \mathfrak{k}[X_1, \ldots, X_n]$ and $X \subseteq Y = V(\mathfrak{p}) \subseteq \mathfrak{k}^n$ irreducible closed subsets of $\mathfrak{k}^n$. We want to show that $\operatorname{codim}(X,Y) = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$. $\leqslant$ was shown in 2.49. $\dim Y \geqslant \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k})$ was shown in 2.13.2 by Applying Noether normalization to $A := B/\mathfrak{p}$, giving us $(f_i)_{i=1}^d \in A^d$ such that the f_i are algebraically independent and A finite over the subalgebra generated by them. We then used going-up to lift a chain of prime ideals corresponding to $\mathfrak{k}^d \supsetneq \{0\} \times \mathfrak{k}^{n-1} \supsetneq \ldots \supsetneq \{0\}$ under $Y \xrightarrow{F=(f_1,\ldots,f_d)} \mathfrak{k}^d$ to a chain of prime ideals in A. This was done left-to-right as going-up was used to make prime ideals larger. In particular, when $\{0\} \in \mathfrak{k}^d$ has several preimages under F, we cannot control to which of them the maximal ideal terminating the lifted chain belongs. Thus, we can show that in the inequality

$$\operatorname{codim}(\{y\}, Y) \leqslant d = \operatorname{trdeg}(\mathfrak{K}(Y)\backslash\mathfrak{k})$$

(see 2.49) equality holds for at least one pint $y \in F^{-1}(\{0\})$ but cannot rule out that there are other $y \in F^{-1}(\{0\})$ for which the inequality becomes strict. However using going-down (2.64) for F, we can use a similar argument, but start lifting of the chain at the right end for the point $y \in Y$ for which we would like to show equality. From this $\operatorname{codim}(X,Y) \geqslant \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$ can be derived similarly to 2.49. Thus

$$\operatorname{codim}(X,Y) = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$$

follows (see 2.67 and 2.69). ☐

Remark 2.64.58. The going-down theorem used to prove this is somewhat more general, as it does not depend on $\mathfrak{k}$ being algebraically closed.

2.14 The height of a prime ideal

In order to complete the proof of 2.13.8 and show $\operatorname{codim}(X,Y) = \operatorname{trdeg}(\mathfrak{K}(Y)/\mathfrak{k}) - \operatorname{trdeg}(\mathfrak{K}(X)/\mathfrak{k})$, we need to localize the $\mathfrak{k}$-algebra with respect to a multiplicative subset and replace the ground field by a larger subfield of that localization which is no longer algebraically closed. To formulate a result which still applies in this context, we need the following:

Definition 2.65 (Height of a prime ideal)**.** Let A be a ring, $\mathfrak{p} \in \operatorname{Spec} A$. We define the **height of the prime ideal $\mathfrak{p}$**, $\operatorname{ht}(\mathfrak{p})$, to be the largest $k \in \mathbb{N}$ such that there is a strictly decreasing sequence $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_k$ of prime ideals of A, or ∞ if there is no finite upper bound on the length of such sequences.

Example 2.66. Let $A = \mathfrak{k}[X_1, \ldots, X_n]$, $X = V(\mathfrak{p})$ for a prime ideal $\mathfrak{p}$. By the correspondence between irreducible subsets of $\mathfrak{k}^n$ and prime ideals in A (2.22), the $\mathfrak{p}_i$ correspond to irreducible subsets $X_i \subseteq \mathfrak{k}^n$ containing X. Thus $\operatorname{ht}(\mathfrak{p}) = \operatorname{codim}(X, \mathfrak{k}^n)$.

Example 2.67. Let $B = \mathfrak{k}[X_1, \ldots, X_n], \mathfrak{q} \in \operatorname{Spec} B$ and let $A := B/\mathfrak{p}$. Let $Y := V(\mathfrak{q}) \subseteq \mathfrak{k}^n$, $\tilde{\mathfrak{p}} := \pi_{B,\mathfrak{q}}^{-1}(\mathfrak{p})$, where $B \xrightarrow{\pi_{B,\mathfrak{p}}} A$ is the projection to the ring of residue classes and let $X = V(\tilde{\mathfrak{p}})$. By 2.44 we have a bijection between the prime ideals $\mathfrak{r} \subseteq \mathfrak{p}$ of A contained in $\mathfrak{p}$ and the prime ideals and the prime ideals $\tilde{\mathfrak{r}} \in \operatorname{Spec} B$ with $\mathfrak{q} \subseteq \tilde{\mathfrak{r}} \subseteq \tilde{\mathfrak{p}}$:

$$\begin{aligned} f : \{\mathfrak{r} \in \operatorname{Spec} A | \mathfrak{r} \subseteq \mathfrak{p}\} &\longrightarrow \{\tilde{\mathfrak{r}} \in \operatorname{Spec} B | \mathfrak{q} \subseteq \tilde{\mathfrak{r}} \subseteq \tilde{\mathfrak{p}}\} \\ \mathfrak{r} &\longmapsto \pi_{B,\mathfrak{q}}^{-1}(\mathfrak{r}) \\ \tilde{\mathfrak{r}}/\mathfrak{q} &\longleftarrow\!\shortmid \tilde{\mathfrak{r}} \end{aligned}$$

By 2.22, the $\tilde{\mathfrak{r}}$ are in canonical bijection with the irreducible subsets Z of Y containing X. Thus, the chains $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \ldots \supsetneq \mathfrak{p}_k$ are in canonical bijection with the chains $X = X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_k \subseteq Y$ of irreducible subsets and $\operatorname{ht}(\mathfrak{p}) = \operatorname{codim}(X, Y)$.

Remark 2.67.59. Let A be an arbitrary ring. One can show that there is a bijection between $\operatorname{Spec} A$ and the set of irreducible subsets $Y \subseteq \operatorname{Spec} A$:

$$\begin{aligned} f : \operatorname{Spec} A &\longrightarrow \{Y \subseteq \operatorname{Spec} A | Y \text{irreducible}\} \\ \mathfrak{p} &\longmapsto V_{\mathbb{S}}(\mathfrak{p}) \\ \bigcup_{\mathfrak{p} \in Y} \mathfrak{p} &\longleftarrow\!\shortmid Y \end{aligned}$$

Thus, the chains $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \ldots \supsetneq \mathfrak{p}_k$ are in canonical bijection with the chains $V(\mathfrak{p}) = X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_k \subseteq \operatorname{Spec} A$ of irreducible subsets, and $\operatorname{ht}(\mathfrak{p}) = \operatorname{codim}(V(\mathfrak{p}), \operatorname{Spec} A)$.

2.14.1 The relation between $\operatorname{ht}(\mathfrak{p})$ and trdeg

We will use the following

Lemma 2.68. Let $\mathfrak{l}$ be an arbitrary field, A a $\mathfrak{l}$-algebra of finite type which is a domain, $K := Q(A)$ the field of quotients and let $(a_i)_{i=1}^n$ be $\mathfrak{l}$-algebraically independent elements of A. Then there exist a natural number $m \geqslant n$ and a transcendence base $(a_i)_{i=1}^m$ for $K/\mathfrak{l}$ with $a_i \in A$ for $1 \leqslant i \leqslant m$.

Proof. The proof is similar to the proof of 2.48. There are a natural number $m \geqslant n$ and elements $(a_i)_{i=n+1}^m \in A^{m-n}$ which generate K in the sense of a matroid used in the definition of trdeg. For instance, one can use generators of the $\mathfrak{l}$-algebra A. We assume m to be minimal and claim that $(a_i)_{i=1}^m$ are $\mathfrak{l}$-algebraically independent. Otherwise there is $j \in \mathbb{N}$, $1 \leqslant j \leqslant m$ such that a_j is algebraic over the subfield of K generated by $\mathfrak{l}$ and the $(a_i)_{i=1}^{j-1}$. We have $j > n$ by the algebraic independence of $(a_i)_{i=1}^n$. Exchanging x_j and x_m, we may assume $j = m$. But then K is algebraic over its subfield generated by $\mathfrak{l}$ and the $(a_i)_{i=1}^{m-1}$, contradicting the minimality of m. □

Theorem 2.69. Let $\mathfrak{l}$ be an arbitrary field, A a $\mathfrak{l}$-algebra of finite type which is a domain, and $\mathfrak{p} \in \operatorname{Spec} A$. Let $K := Q(A)$ be the field of quotients of A. Then

$$\operatorname{ht}(\mathfrak{p}) = \operatorname{trdeg}(K/\mathfrak{l}) - \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p})/\mathfrak{l}).$$

Remark 2.69.60. By example 2.67, theorem 2.39 is a special case of this theorem.

Proof. If $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_k$ is a chain of prime ideals in A, we have $\operatorname{trdeg}(\mathfrak{k}(\mathfrak{p}_i)/\mathfrak{l}) < \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p}_{i+1})/\mathfrak{l})$ by 2.47 ("A first result of dimension theory"). Thus

$$k \leqslant \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p}_k)/\mathfrak{l}) - \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p})/\mathfrak{l}) \leqslant \operatorname{trdeg}(K/\mathfrak{l}) - \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p})/\mathfrak{l}),$$

where the last inequality is another application of 2.47 (using $K = Q(A) = Q(A/\{0\}) = \mathfrak{k}(\{0\})$ and the fact that $\{0\} \subseteq \mathfrak{p}_k$ is a prime ideal). Hence

$$\operatorname{ht}(\mathfrak{p}) \leqslant \operatorname{trdeg}(K/\mathfrak{l}) - \operatorname{trdeg}(\mathfrak{k}(\mathfrak{p})/\mathfrak{l})$$

and it remains to show the opposite inequality.

Claim 1. *For any maximal ideal* $\mathfrak{p} \in \operatorname{MaxSpec} A$

$$\operatorname{ht}(\mathfrak{m}) \geqslant \operatorname{trdeg}(K/\mathfrak{l}).$$

Subproof. By the Noether normalization theorem (1.12), there are $(x_i)_{i=1}^d \in A^d$ which are algebraically independent over $\mathfrak{l}$ such that A is finite over the subalgebra S generated by the x_i. We have $d = \operatorname{trdeg}(K/\mathfrak{l})$ as the x_i form a transcendence base of $K/\mathfrak{l}$.

Claim 1. *We can choose $x_i \in \mathfrak{m}$.*

Subproof. By the Nullstellensatz (2.3), $\mathfrak{k}(\mathfrak{m}) = A/\mathfrak{m}$ is a finite field extension of $\mathfrak{l}$. Hence there exists a normed polynomial $P_i \in \mathfrak{l}[T]$ with $P_i(x_i \mod \mathfrak{m}) = 0$ in $\mathfrak{k}(\mathfrak{m})$. Let $\tilde{x}_i := P_i(x_i) \in \mathfrak{m}$ and $\tilde{S}$ the subalgebra generated by the $\tilde{x}_i$. As $P_i(x_i) - \tilde{x}_i = 0$, x_i is integral over $\tilde{S}$ and so is $S/\tilde{S}$. It follows that $A/\tilde{S}$ is integral, hence finite by 1.10.5. Replacing x_i by $\tilde{x}_i$, we may thus assume that $x_i \in \mathfrak{m}$. ■

The ring homomorphism $\mathrm{ev}_x : R = \mathfrak{l}[X_1, \ldots, X_d] \xrightarrow{P \mapsto P(x_1,\ldots,x_d)} A$ is injective. Because R is a UFD, R is normal (2.62). Thus the going-down theorem (2.64) applies to the integral R-algebra A. For $0 \leqslant i \leqslant d$, let $\mathfrak{p}_i \subseteq R$ be the ideal generated by $(X_j)_{j=i+1}^d$. We have $\mathfrak{m} \sqcap R = \mathfrak{p}_0$ as all $X_i \in \mathfrak{m}$, hence $X_i \in \mathfrak{m} \sqcap R$ and $\mathfrak{p}_0$ is a maximal ideal. By applying going-down and induction on i, there is a chain $\mathfrak{m} = \mathfrak{q}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_d$ of elements of $\operatorname{Spec} A$ such that $\mathfrak{q}_i \sqcap R = \mathfrak{p}_i$. It follows that $\mathrm{ht}(\mathfrak{m}) \geqslant d$. ■

This finishes the proof in the case of $\mathfrak{p} \in \operatorname{MaxSpec} A$.

To reduce the general case to that special case, we proceed as in 2.47: By lemma 2.48 there are $a_1, \ldots, a_n \in A$ whose images in $A/\mathfrak{p}$ form a transcendence base for $\mathfrak{k}(\mathfrak{p})/\mathfrak{l}$. As these images are $\mathfrak{l}$-algebraically independent, the same holds for the a_i themselves.

By lemma 2.68 we can extend $(a_i)_{i=1}^n$ to a transcendence base $(a_i)_{i=1}^m \in A^m$ of $K/\mathfrak{l}$. Let $R \subseteq A$ denote the $\mathfrak{l}$-subalgebra generated by $a_1, \ldots, a_n$ and let $S := R\backslash\{0\}$. Let $A_1 := A_S$ and $\mathfrak{p}_S$ the prime ideal corresponding to $\mathfrak{p}$ under $\operatorname{Spec}(A_1) \cong \{\mathfrak{r} \in \operatorname{Spec} A | \mathfrak{r} \cap S = \varnothing\}$ (2.44). As in 2.44.42, A_1 is a domain with $Q(A_1) \cong K = Q(A)$ and by 2.46 $A_1/\mathfrak{p}_S \cong (A/\mathfrak{p})_{\overline{S}}$, where $\overline{S}$ denotes the image of S in $A/\mathfrak{p}$. As in 2.47, $\mathfrak{k}(\mathfrak{p}_S) \cong \mathfrak{k}(\mathfrak{p})$ is integral over $A_1/\mathfrak{p}_S$. From the fact about integrality and fields (1.10.7), it follows that $A_1/\mathfrak{p}_S$ is a field. Hence $\mathfrak{p}_S \in \operatorname{MaxSpec}(A_1)$ and the special case can be applied to $\mathfrak{p}_S$ and $A_1/\mathfrak{l}_1$, showing that $\mathrm{ht}(\mathfrak{p}_S) \geqslant e = \mathrm{trdeg}(K/\mathfrak{l}_1)$. We have $\mathrm{trdeg}(K/\mathfrak{l}_1) = m - n$, as $(a_i)_{i=n+1}^m$ is a transcendence base for $K/\mathfrak{l}_1$. By the description of $\operatorname{Spec} A_S$ (2.44), a chain $\mathfrak{p}_S = \mathfrak{q}_0 \supsetneq \ldots \supsetneq \mathfrak{p}_e$ of prime ideals in A_S defines a similar chain $\mathfrak{p}_i := \mathfrak{q}_i \sqcap A$ in A with $\mathfrak{p}_0 = \mathfrak{p}$. Thus $\mathrm{ht}(\mathfrak{p}) \geqslant e$. □

Remark 2.69.61. As a consequence of his principal ideal theorem, Krull has shown the finiteness of $\mathrm{ht}(\mathfrak{p})$ for $\mathfrak{p} \in \operatorname{Spec} A$ when A is a Noetherian ring. But $\dim A = \sup_{\mathfrak{p} \in \operatorname{Spec} A} \mathrm{ht}(\mathfrak{p}) = \sup_{\mathfrak{m} \in \operatorname{MaxSpec} A} \mathrm{ht}(\mathfrak{m})$, the Krull dimension of the Noetherian topological space $\operatorname{Spec} A$ may nevertheless be infinite.

Example† 2.69.62 (Noetherian ring with infinite dimension)**.** [a] Let $A =$

$\mathfrak{k}[X_i | i \in \mathbb{N}]$ and $m_1, m_2, \ldots \in \mathbb{N}$ an increasing sequence such that $m_{i+1} - m_i > m_i - m_{i-1}$. Let $\mathfrak{p}_i := (X_{m_i+1}, \ldots, X_{m_{i+1}})$ and $S := A \setminus \bigcup_{i \in \mathbb{N}} \mathfrak{p}_i$. S is multiplicatively closed. A_S is Noetherian but $\operatorname{ht}((\mathfrak{p}_i)_S) = m_{i+1} - m_i$ hence $\dim(A_S) = \infty$.

[a] https://math.stackexchange.com/questions/1109732/noetherian-ring-with-infinite-krull-dimension-nagatas-example

2.15 Dimension of products

Proposition 2.70. Let $X \subseteq \mathfrak{k}^n$ and $Y \subseteq \mathfrak{k}^n$ be irreducible and closed. Then $X \times Y$ is also an irreducible closed subset of $\mathfrak{k}^{m+n}$. Moreover, $\dim(X \times Y) = \dim(X) + \dim(Y)$ and $\operatorname{codim}(X \times Y, \mathfrak{k}^{m+n}) = \operatorname{codim}(X, \mathfrak{k}^m) + \operatorname{codim}(Y, \mathfrak{k}^n)$.

Proof. Let $X = V(\mathfrak{p})$ and $Y = V(\mathfrak{q})$ where $\mathfrak{p} \in \operatorname{Spec} \mathfrak{k}[X_1, \ldots, X_m]$ and $\mathfrak{q} \in \operatorname{Spec} \mathfrak{k}[X_1, \ldots, X_n]$. We denote points of $\mathfrak{k}^{m+n}$ as $x = (x', x'')$ with $x' \in \mathfrak{k}^m, x'' \in \mathfrak{k}^n$. Then $X \times Y$ is the set of zeroes of the ideal in $\mathfrak{k}[X_1, \ldots, X_{m+n}]$ generated by the polynomials $f(x) = \varphi(x')$, with φ running over $\mathfrak{p}$ and $g(x) = \gamma(x'')$ with γ running over $\mathfrak{q}$. Thus $X \times Y$ is closed in $\mathfrak{k}^{m+n}$. We must also show irreducibility. $X \times Y \neq \varnothing$ is obvious.

Assume that $X \times Y = A_1 \cup A_2$, where the $A_i \subseteq \mathfrak{k}^{m+n}$ are closed. For $x' \in \mathfrak{k}^m$, $x' \times Y$ is homeomorphic to the irreducible Y. Thus $X = X_1 \cup X_2$ where $X_i = \{x \in X | \{x\} \times Y \subseteq A_i\}$. Because $X_i = \bigcap_{y \in Y} \{x \in X | (x, y) \in A_i\}$, this is closed. As X is irreducible, there is $i \in \{1; 2\}$ which $X_i = X$. Then $X \times Y = A_i$ confirming the irreducibility of $X \times Y$.

Let $a = \dim X$ and $b = \dim Y$ and $X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_a = X$, $Y_0 \subsetneq Y_1 \subsetneq \ldots \subsetneq Y_b = Y$ be chains of irreducible subsets. By the previous result, $X_0 \times Y_0 \subsetneq X_1 \times Y_0 \subsetneq \ldots \subsetneq X_a \times Y_0 \subsetneq X_a \times Y_1 \subsetneq \ldots \subsetneq X_a \times Y_a = X \times Y$ is a chain of irreducible subsets. Thus $\dim(X \times Y) \geqslant a + b = \dim X + \dim Y$. Similarly one derives

$$\operatorname{codim}(X \times Y, \mathfrak{k}^{m+n}) \geqslant \operatorname{codim}(X, \mathfrak{k}^m) + \operatorname{codim}(Y, \mathfrak{k}^n).$$

By 2.39 we have $\dim(A) + \operatorname{codim}(A, \mathfrak{k}^l) = l$ for irreducible subsets of $\mathfrak{k}^l$. Thus equality must hold in the previous two inequalities. □

2.16 The nil radical

Notation 2.70.63. Let $V_{\mathbb{S}}(I)$ denote the set of $\mathfrak{p} \in \operatorname{Spec} A$ containing I.

Proposition 2.71 (Nil radical)**.** For a ring A, $\bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p} = \sqrt{\{0\}} = \{a \in A | \exists k \in \mathbb{N}\ a^k = 0\} =: \mathfrak{nil}(A)$, the set of nilpotent elements of A. This is called the **nil radical** of A.

Proof. It is clear that elements of $\sqrt{\{0\}}$ must belong to all prime ideals. Conversely, let $a \in A \backslash \sqrt{\{0\}}$. Then $S = a^{\mathbb{N}}$ is a multiplicative subset of A not containing 0. The localisation A_S of A is thus not the null ring. Hence $\operatorname{Spec} A_S \neq \varnothing$. If $\mathfrak{q} \in \operatorname{Spec} A_S$, then by the description of $\operatorname{Spec} A_S$ (Proposition 2.44), $\mathfrak{p} := \mathfrak{q} \sqcap A$ is a prime ideal of A disjoint from S, hence $a \notin \mathfrak{p}$. □

Corollary 2.72. For an ideal I of R, $\sqrt{I} = \bigcap_{\mathfrak{p} \in V_{\mathbb{S}}(I)} \mathfrak{p}$.

Proof. This is obtained by applying the proposition to $A = R/I$ and using the bijection $\operatorname{Spec}(R/I) \cong V(I)$ sending $\mathfrak{p} \in V(I)$ to $\mathfrak{p} := \mathfrak{p}/I$ and $\mathfrak{q} \in \operatorname{Spec}(R/I)$ to its inverse image $\mathfrak{p}$ in R. □

2.16.1 Closed subsets of $\operatorname{Spec} R$

Proposition 2.73. There is a bijection

$$\begin{aligned} f : \{A \subseteq \operatorname{Spec} R | A \text{ closed}\} &\longrightarrow \{I \subseteq R | I \text{ ideal and } I = \sqrt{I}\} \\ A &\longmapsto \bigcap_{\mathfrak{p} \in A} \mathfrak{p} \\ V_{\mathbb{S}}(I) &\longleftarrow I \end{aligned}$$

Under this bijection, the irreducible subsets correspond to the prime ideals and the closed points $\{\mathfrak{m}\}, \mathfrak{m} \in \operatorname{Spec} A$ to the maximal ideals.

Proof. If $A = V_{\mathbb{S}}(I)$, then by 2.72 $\sqrt{I} = \bigcap_{\mathfrak{p} \in A} \mathfrak{p}$. Thus, an ideal with $\sqrt{I} = I$ can be recovered from $V_{\mathbb{S}}(I)$. Since $V_{\mathbb{S}}(J) = V_{\mathbb{S}}(\sqrt{J})$, the map from ideals with $\sqrt{I} = I$ to closed subsets is surjective.

Sine R corresponds to $\varnothing$, the proper ideals correspond to non-empty subsets of $\operatorname{Spec} R$. Assume that $V_{\mathbb{S}}(I) = V_{\mathbb{S}}(J_1) \cup V_{\mathbb{S}}(J_2)$, where the decomposition is proper and the ideals coincide with their radicals. Let $g = f_1 f_2$ with $f_k \in J_k \backslash I$. Since $V_{\mathbb{S}}(g) \supseteq V_{\mathbb{S}}(f_k) \supseteq V_{\mathbb{S}}(I_k)$, $V_{\mathbb{S}}(I) \subseteq V_{\mathbb{S}}(g)$. Hence $g \in \sqrt{I} = I$. As $f_k \notin I$, I fails to be a prime ideal. Conversely, assume that $f_1 f_2 \in I$ while the factors are not in I. Since $I = \sqrt{I}, V_{\mathbb{S}}(f_k) \not\supseteq V_{\mathbb{S}}(I)$. But $V_{\mathbb{S}}(f_1) \cup V_{\mathbb{S}}(f_2) = V_{\mathbb{S}}(f_1 f_2) \supseteq V_{\mathbb{S}}(I)$. The proper decomposition $V_{\mathbb{S}}(I) = (V_{\mathbb{S}}(I) \cap V_{\mathbb{S}}(f_1)) \cup (V_{\mathbb{S}}(I) \cap V_{\mathbb{S}}(f_2))$ now shows that $V_{\mathbb{S}}(I)$ fails to be irreducible. The final assertion is trivial. □

Corollary 2.74. If R is a Noetherian ring, then $\operatorname{Spec} R$ is a Noetherian topological space.

Remark 2.74.64. It is not particularly hard to come up with examples which show that the converse implication does not hold.

Example† 2.74.65. Let $A = \mathfrak{k}[X_n | n \in \mathbb{N}]/I$m where I denotes the ideal generated by $\{X_i^2 | i \in \mathbb{N}\}$. A is not Noetherian, since the ideal J generated by $\{X_i | i \in \mathbb{N}\}$ is not finitely generated. $A/J \cong \mathfrak{k}$, hence J is maximal. As every prime ideal must contain $\mathfrak{nil}(A) \supseteq J$, J is the only prime ideal. Thus $\operatorname{Spec} A$ contains only one element and is hence Noetherian.

Corollary 2.75 (About the smallest prime ideals containing I)**.** If R is Noetherian and $I \subseteq R$ an ideal, then the set $V_{\mathbb{S}}(I) = \{\mathfrak{p} \in \operatorname{Spec} R | I \subseteq \mathfrak{p}\}$ has finitely many $\subseteq$-minimal elements $(\mathfrak{p}_i)_{i=1}^k$ and every element of $V(I)$ contains at least one $\mathfrak{p}_i$. The $V_{\mathbb{S}}(\mathfrak{p}_i)$ are precisely the irreducible components of $V(I)$. Moreover $\bigcap_{i=1}^k \mathfrak{p}_i = \sqrt{I}$ and $k > 0$ if I is a proper ideal.

Proof. If $V_{\mathbb{S}}(I) = \bigcup_{i=1}^k V_{\mathbb{S}}(\mathfrak{p}_i)$ is the decomposition into irreducible components then every $\mathfrak{q} \in V_{\mathbb{S}}(I)$ must belong to at least one $V_{\mathbb{S}}(\mathfrak{p}_i)$, hence $\mathfrak{p}_i \subseteq \mathfrak{q}$. Also $\mathfrak{p}_i \in V_{\mathbb{S}}(\mathfrak{p}_i) \subseteq V_{\mathbb{S}}(I)$. It follows that the sets of $\subseteq$-minimal elements of $V_{\mathbb{S}}(I)$ and of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ coincide. As there are no non-trivial inclusions between the $V_{\mathbb{S}}(\mathfrak{p}_i)$, there are no non-trivial inclusions between the $\mathfrak{p}_i$ and the assertion follows. The final remark is trivial. □

Corollary 2.76. If R is any ring, $\operatorname{ht}(\mathfrak{p}) = \operatorname{codim}(V_{\mathbb{S}}(\mathfrak{p}), \operatorname{Spec} R)$.

2.17 The principal ideal theorem

Krull was able to show:

Theorem 2.77 (Principal ideal theorem / Hauptidealsatz)**.** Let A be a Noetherian ring, $a \in A$ and $\mathfrak{p} \in \operatorname{Spec} A$ a $\subseteq$-minimal element of $V_{\mathbb{S}}(a)$. Then $\operatorname{ht}(\mathfrak{p}) \leqslant 1$.

Proof. Probably not relevant for the exam. □

Remark 2.77.66. Intuitively, the theorem says that by imposing a single equation one ends up in codimension at most 1. This would not be true in real analysis (or real algebraic geometry) as the equation $\sum_{i=1}^n X_i^2 = 0$ shows. By 2.75, if a is a non-unit then a $\mathfrak{p} \in \operatorname{Spec} A$ to which the theorem applies can always be found. Using induction on k, Krull was able to derive:

Theorem 2.78 (Generalized principal ideal theorem)**.** Let A be a Noetherian ring, $(a_i)_{i=1}^k \in A$ and $\mathfrak{p} \in \operatorname{Spec} A$ a $\subseteq$-minimal element of $\bigcap_{i=1}^k V(a_i)$, the set of prime ideals containing all a_i. Then $\operatorname{ht}(\mathfrak{p}) \leqslant k$.

Modern approaches to the principal ideal theorem usually give a direct proof of this more general theorem.

Corollary 2.79. If R is a Noetherian ring and $\mathfrak{p} \in \operatorname{Spec} R$, then $\operatorname{ht}(\mathfrak{p}) < \infty$.

Proof. If $\mathfrak{p}$ is generated by $(f_i)_{i=1}^k$, then $\operatorname{ht}(\mathfrak{p}) \leqslant k$. □

2.17.1 Application to the dimension of intersections

Remark 2.79.67. Let $R = \mathfrak{k}[X_1, \dots, X_n]$ and $I \subseteq R$ an ideal.

If $(\mathfrak{p}_i)_{i=1}^k$ are the smallest prime ideals of R containing I, then $(V_{\mathbb{A}}(\mathfrak{p}_i))_{i=1}^k$ are the irreducible components of $V_{\mathbb{A}}(I)$.

Proof. The $V_{\mathbb{A}}(\mathfrak{p}_i)$ are irreducible, there are no non-trivial inclusions between them and $V_{\mathbb{A}}(I) = V_{\mathbb{A}}(\sqrt{I}) = V_{\mathbb{A}}(\bigcap_{i=1}^k \mathfrak{p}_i) = \bigcup_{i=1}^k V_{\mathbb{A}}(\mathfrak{p}_i)$. □

Corollary 2.80 (of the principal ideal theorem)**.** Let $X \subseteq \mathfrak{k}^n$ be irreducible, $(f_i)_{i=1}^k$ elements of $R = \mathfrak{k}[X_1, \dots, X_n]$ and Y an irreducible component of $A = X \cap \bigcap_{i=1}^k V(f_i)$. Then $\operatorname{codim}(Y, X) \leqslant k$.

Remark 2.80.68. This confirms the naive geometric intuition that by imposing k equations one ends up in codimension at most k.

Proof. If $X = v(\mathfrak{p}), X \cap \bigcap_{i=1}^k V(f_i) = V(I)$ where $I \subseteq R$ is the ideal generated by $\mathfrak{p}$ and the f_i. By 2.79.67, $Y = V(\mathfrak{q})$ where $\mathfrak{q}$ is the smallest prime ideal containing I. Then $\mathfrak{q}/\mathfrak{p}$ is a smallest prime ideal of $R/\mathfrak{p}$ containing all $(f_i \bmod \mathfrak{p})_{i=1}^k$. By the principal ideal theorem (2.77), $\operatorname{ht}(\mathfrak{q}/\mathfrak{p}) \leqslant k$ and the assertion follows from example 2.67. □

Remark 2.80.69. Note that the intersection $X \cap \bigcap_{i=1}^k V(f_i)$ can easily be empty, even when k is much smaller than $\dim X$.

Corollary 2.81. Let A and B be irreducible subsets of $\mathfrak{k}^n$. If C is an irreducible component of $A \cap B$, then $\operatorname{codim}(C, \mathfrak{k}^n) \leqslant \operatorname{codim}(A, \mathfrak{k}^n) + \operatorname{codim}(B, \mathfrak{k}^n)$.

Remark† 2.81.70. Equivalently, $\dim(C) \geqslant \dim(A) + \dim(B) - n$.

Proof. Let $X = A \times B \subseteq \mathfrak{k}^{2n}$, where we use $(X_1, \dots, X_n, Y_1, \dots, Y_n)$ as coordinates of $\mathfrak{k}^{2n}$. Let $\Delta := \{(x_1, \dots, x_n, x_1, \dots, x_n) | x \in \mathfrak{k}^n\}$ be the diagonal in

$\mathfrak{k}^n \times \mathfrak{k}^n$. The projection $\mathfrak{k}^{2n} \to \mathfrak{k}^n$ to the X-coordinates defines a homeomorphism between $(A \times B) \cap \Delta$ and $A \cap B$. Thus, C is homeomorphic to an irreducible component C' of $(A \times B) \cap \Delta$ and

$$\begin{aligned} \operatorname{codim}(C, \mathfrak{k}^n) &= n - \dim(C) \\ &= n - \dim(C') \\ &= n - \dim(A \times B) + \operatorname{codim}(C', A \times B) \\ &\overset{2.80}{\leqslant} 2n - \dim(A \times B) \\ &\overset{2.70}{=} 2n - \dim(A) - \dim(B) \\ &= \operatorname{codim}(A, \mathfrak{k}^n) + \operatorname{codim}(B, \mathfrak{k}^n) \end{aligned}$$

by the general properties of dimension and codimension, 2.80 applied to $(X_i - Y_i)_{i=1}^n$, the result about the dimension of products (2.70) and again the general properties of dimension and codimension. □

Remark 2.81.71. As in 2.80.69, $A \cap B$ can easily be empty, even when A and B have codimension 1 and n is very large.

2.17.2 Application to the property of being a UFD

Proposition 2.82. Let R be a Noetherian domain. Then R is a UFD iff every $\mathfrak{p} \in \operatorname{Spec} R$ with $\operatorname{ht}(\mathfrak{p}) = 1$[a] is a principal ideal.

[a] in other words, every $\subseteq$-minimal element of the set of non-zero prime ideals of R

Proof. Every element of every Noetherian domain can be written as a product of irreducible elements. [10] Thus, R is a UFD iff every irreducible element of R is prime.

Assume that this is the case. Let $\mathfrak{p} \in \operatorname{Spec} R, \operatorname{ht}(\mathfrak{p}) = 1$. Let $p \in \mathfrak{p} \backslash \{0\}$. Replacing p by a prime factor of p, we may assume p to be prime. Thus $\{0\} \subsetneq pR \subseteq \mathfrak{p}$ is a chain of prime ideals and since $\operatorname{ht}(\mathfrak{p}) = 1$ it follows that $\mathfrak{p} = pR$.

Conversely, assume that every $\mathfrak{p} \in \operatorname{Spec} R$ with $\operatorname{ht}(\mathfrak{p}) = 1$ is a principal ideal. Let $f \in R$ be irreducible. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a $\subseteq$-minimal element of $V(f)$. By the principal ideal theorem (2.77), $\operatorname{ht}(\mathfrak{p}) = 1$. Thus $\mathfrak{p} = pR$ for some prime element p. We have $p | f$ since $f \in \mathfrak{p}$. As f is irreducible, p and f are multiplicatively equivalent. Thus f is a prime element. □

2.18 The Jacobson radical

[10] Consider the set of principal ideals rR where r is not a product of irreducible elements.

Proposition 2.83. For a ring A,

$$\bigcap_{\mathfrak{m}\in \operatorname{MaxSpec} A} \mathfrak{m} = \{a \in A | \forall x \in A\ 1 - ax \in A^\times\} =: \operatorname{rad}(A).$$

the **Jacobson radical** of A.

Proof. Suppose $\mathfrak{m} \in \operatorname{MaxSpec} A$ and $a \in A \backslash \mathfrak{m}$. Then $a \mod \mathfrak{m} \neq 0$ and $A/\mathfrak{m}$ is a field. Hence $a \mod \mathfrak{m}$ has an inverse $x \mod \mathfrak{m}$. $1 - ax \in \mathfrak{m}$, hence $1 - ax \notin A^\times$ and a is not al element of the RHS.

Conversely, let $a \in A$ belong to all $\mathfrak{m} \in \operatorname{MaxSpec} A$. If there exists $x \in A$ such that $1 - ax \notin A^\times$ then $(1 - ax)A$ was a proper ideal in A, hence contained in a maximal ideal $\mathfrak{m}$. As $a \in \mathfrak{m}, 1 = (1 - ax) + ax \in \mathfrak{m}$, a contradiction. Hence every element of $\bigcap_{\mathfrak{m}\in \operatorname{MaxSpec} A} \mathfrak{m}$ belongs to the right hand side. □

Example 2.84. If A is a local ring, then $\operatorname{rad}(A) = \mathfrak{m}_A$.

Example 2.85. If A is a PID with infinitely many multiplicative equivalence classes of prime elements (e.g. $\mathbb{Z}$ of $\mathfrak{k}[X]$), then $\operatorname{rad}(A) = \{0\}$: Prime ideals of a PID are maximal. Thus if $x \in \operatorname{rad}(A)$, every prime element divides x. If $x \neq 0$, it follows that x has infinitely many prime divisors. However every PID is a UFD.

Example 2.86. If A is a PID for which $p_1, \ldots, p_n$ is a list of representatives of the multiplicative equivalence classes of prime elements, then $\operatorname{rad}(A) = fA$ where $f = \prod_{i=1}^n p_i$.

3 Projective spaces

Let $\mathfrak{l}$ be any field.

Definition 3.1. For a $\mathfrak{l}$-vector space V, let $\mathbb{P}(V)$ be the set of one-dimensional subspaces of V. Let $\mathbb{P}^n(\mathfrak{l}) := \mathbb{P}(\mathfrak{l}^{n+1})$, the **$n$-dimensional projective space over $\mathfrak{l}$**.

If $\mathfrak{l}$ is kept fixed, we will often write $\mathbb{P}^n$ for $\mathbb{P}^n(\mathfrak{l})$.

When dealing with $\mathbb{P}^n$, the usual convention is to use 0 as the index of the first coordinate.

We denote the one-dimensional subspace generated by $(x_0, \ldots, x_n) \in \mathfrak{k}^{n+1} \backslash \{0\}$ by $[x_0, \ldots, x_n] \in \mathbb{P}^n$. If $x = [x_0, ldots, x_n] \in \mathbb{P}^n$, the $(x_i)_{i=0}^n$ are called **homogeneous coordinates** of x. At least one of the x_i must be $\neq 0$.

Remark 3.1.72. There are points $[1,0],[0,1] \in \mathbb{P}^1$ but there is no point $[0,0] \in \mathbb{P}^1$.

Definition 3.2 (Infinite hyperplane)**.** For $0 \leqslant i \leqslant n$ let $U_i \subseteq \mathbb{P}^n$ denote the set of $[x_0,\ldots,x_n]$ with $x_i \neq 0$. This is a correct definition since two different sets $[x_0,\ldots,x_n]$ and $[\xi_0,\ldots,\xi_n]$ of homogeneous coordinates for the same point $x \in \mathbb{P}^n$ differ by scaling with a $\lambda \in \Bbbk^\times$, $x_i = \lambda\xi_i$. Since not all x_i may be 0, $\mathbb{P}^n = \bigcup_{i=0}^n U_i$. We identify $\mathbb{A}^n = \mathbb{A}^n(\Bbbk) = \Bbbk^n$ with U_0 by identifying $(x_1,\ldots,x_n) \in \mathbb{A}^n$ with $[1,x_1,\ldots,x_n] \in \mathbb{P}^n$. Then $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ where $\infty = [0,1]$. More generally, when $n > 0$ $\mathbb{P}^n \backslash \mathbb{A}^n$ can be identified with $\mathbb{P}^{n-1}$ identifying $[0,x_1,\ldots,x_n] \in \mathbb{P}^n \backslash \mathbb{A}^n$ with $[x_1,\ldots,x_n] \in \mathbb{P}^{n-1}$.

Thus $\mathbb{P}^n$ is $\mathbb{A}^n \cong \Bbbk^n$ with a copy of $\mathbb{P}^{n-1}$ added as an **infinite hyperplane** .

3.0.1 Graded rings and homogeneous ideals

Notation 3.2.73. Let $\mathbb{I} = \mathbb{N}$ or $\mathbb{I} = \mathbb{Z}$.

Definition 3.3. By an **$\mathbb{I}$-graded ring** $A_\bullet$ we understand a ring A with a collection $(A_d)_{d\in\mathbb{I}}$ of subgroups of the additive group $(A,+)$ such that $A_a \cdot A_b \subseteq A_{a+b}$ for $a,b \in \mathbb{I}$ and such that $A = \bigoplus_{d\in\mathbb{I}} A_d$ in the sense that every $r \in A$ has a unique decomposition $r = \sum_{d\in\mathbb{I}} r_d$ with $r_d \in A_d$ and but finitely many $r_d \neq 0$.

We call the r_d the **homogeneous components** of r.

An ideal $I \subseteq A$ is called **homogeneous** if

$$r \in I \implies \forall d \in \mathbb{I}\ r_d \in I_d$$

where $I_d := I \cap A_d$.

By a **graded ring** we understand an $\mathbb{N}$-graded ring. In this case,

$$A_+ := \bigoplus_{d=1}^{\infty} A_d = \{r \in A | r_0 = 0\}$$

is called the **augmentation ideal** of A.

Remark 3.3.74 (Decomposition of 1)**.** If $1 = \sum_{d\in\mathbb{I}} \varepsilon_d$ is the decomposition into homogeneous components, then $\varepsilon_a = 1 \cdot \varepsilon_a = \sum_{b\in\mathbb{I}} \varepsilon_a\varepsilon_b$ with $\varepsilon_a\varepsilon_b \in A_{a+b}$. By the uniqueness of the decomposition into homogeneous components, $\varepsilon_a\varepsilon_0 = \varepsilon_a$ and $b \neq 0 \implies \varepsilon_a\varepsilon_b = 0$. Applying the last equation with $a = 0$ gives $b \neq 0 \implies \varepsilon_b = \varepsilon_0\varepsilon_b = 0$. Thus $1 = \varepsilon_0 \in A_0$.

Remark 3.3.75. The augmentation ideal of a graded ring is a homogeneous ideal.

Proposition 3.4. [a]

- A principal ideal generated by a homogeneous element is homogeneous.
- The operations $\sum, \bigcap, \sqrt{}$ preserve homogeneity.
- An ideal is homogeneous iff it can be generated by a family of homogeneous elements.

[a] This holds for both $\mathbb{Z}$-graded and $\mathbb{N}$-graded rings.

Proof. Most assertions are trivial. We only show that J homogeneous $\implies \sqrt{J}$ homogeneous. Let A be $\mathbb{I}$-graded, $f \in \sqrt{J}$ and $f = \sum_{d \in \mathbb{I}} f_d$ the decomposition. To show that all $f_d \in \sqrt{J}$, we use induction on $N_f := \#\{d \in \mathbb{I} | f_d \neq 0\}$. $N_f = 0$ is trivial. Suppose $N_f > 0$ and $e \in \mathbb{I}$ is maximal with $f_e \neq 0$. For $l \in \mathbb{N}$, the le-th homogeneous component of f^l is f_e^l. Choosing l large enough such that $f^l \in J$ and using the homogeneity of J, we find $f_e \in \sqrt{J}$. As $\sqrt{J}$ is an ideal, $\tilde{f} := f - f_e \in \sqrt{J}$. As $N_{\tilde{f}} = N_f - 1$, the induction assumption may be applied to $\tilde{f}$ and shows $f_d \in \sqrt{J}$ for $d \neq e$. □

Fact 3.4.76. A homogeneous ideal is finitely generated iff it can be generated by finitely many of its homogeneous elements. In particular, this is always the case when A is a Noetherian ring.

3.0.2 The Zariski topology on $\mathbb{P}^n$

Notation 3.4.77. Recall that for $\alpha \in \mathbb{N}^{n+1}$

$$|\alpha| = \sum_{i=0}^{n} \alpha_i \text{ and } x^\alpha = x_0^{\alpha_0} \cdot \ldots \cdot x_n^{\alpha_n}.$$

Definition 3.5 (Homogeneous polynomials)**.** Let R be any ring and

$$f = \sum_{\alpha \in \mathbb{N}^{n+1}} f_\alpha X^\alpha \in R[X_0, \ldots, X_n].$$

We say that f is **homogeneous of degree d** if

$$|\alpha| \neq d \implies f_\alpha = 0.$$

We denote the subset of homogeneous polynomials of degree d by

$$R[X_0, \ldots, X_n]_d \subseteq R[X_0, \ldots, X_n].$$

Remark 3.5.78. This definition gives R the structure of a graded ring.

Definition 3.6 (Zariski topology on $\mathbb{P}^n(\mathfrak{k})$)**.** Let $A = \mathfrak{k}[X_0, \ldots, X_n]$.[a] For $f \in A_d = \mathfrak{k}[X_0, \ldots, X_n]_d$, the validity of the equation $f(x_0, \ldots, x_n) = 0$ does not depend on the choice of homogeneous coordinates, as

$$f(\lambda x_0, \ldots, \lambda x_n) 0 \lambda^d f(x_0, \ldots, x_n).$$

Let $V_{\mathbb{P}}(f) \coloneqq \{x \in \mathbb{P}^n | f(x) = 0\}$.

We call a subset $X \subseteq \mathbb{P}^n$ Zariski-closed if it can be represented as

$$X = \bigcap_{i=1}^{k} V_{\mathbb{P}}(f_i)$$

where the $f_i \in A_{d_i}$ are homogeneous polynomials.

[a] As always, $\mathfrak{k}$ is algebraically closed

Fact 3.6.79. If $X = \bigcap_{i=1}^{k} V_{\mathbb{P}}(f_i) \subseteq \mathbb{P}^n$ is closed, then $Y = X \cap \mathbb{A}^n$ can be identified with the closed subset

$$\{(x_1, \ldots, x_n) \in \mathfrak{k}^n | f_i(1, x_1, \ldots, x_n) = 0, 1 \leqslant i \leqslant k\} \subseteq \mathfrak{k}^n.$$

Conversely, if $Y \subseteq \mathfrak{k}^n$ is closed it has the form

$$\{(x_1, \ldots, x_n) \in \mathfrak{k}^n | g_i(x_1, \ldots, x_n) = 0, 1 \leqslant i \leqslant k\}$$

and can thus be identified with $X \cap \mathbb{A}^n$ where $X := \bigcap_{i=1}^{k} V_{\mathbb{P}}(f_i)$ is given by

$$f_i(X_0, \ldots, X_n) := X_0^{d_i} g_i(X_1/X_0, \ldots, X_n/X_0), d_i \geqslant \deg(g_i).$$

Thus, the Zariski topology on $\mathfrak{k}^n$ can be identified with the topology induced by the Zariski topology on $\mathbb{A}^n = U_0$, and the same holds for U_i with $0 \leqslant i \leqslant n$.

In this sense, the Zariski topology on $\mathbb{P}^n$ can be thought of as gluing the Zariski topologies on the $U_i \cong \mathfrak{k}^n$.

Definition 3.7. Let $I \subseteq A = \mathfrak{k}[X_0, \ldots, X_n]$ be a homogeneous ideal. Let $V_{\mathbb{P}}(I) := \{[x_0, \ldots,_n] \in \mathbb{P}^n | \forall f \in I \ f(x_0, \ldots, x_n) = 0\}$ As I is homogeneous, it is sufficient to impose this condition for the homogeneous elements $f \in I$. Because A is Noetherian, I can finitely generated by homogeneous elements $(f_i)_{i=1}^{k}$ and $V_{\mathbb{P}}(I) = \bigcap_{i=1}^{k} V_{\mathbb{P}}(f_i)$ as in 3.6. Conversely, if the homogeneous f_i are given, then $I = \langle f_1, \ldots, f_k \rangle_A$ is homogeneous.

Remark 3.7.80. Note that $V(A) = V(A_+) = \varnothing$.

Fact 3.7.81. For homogeneous ideals in A and $m \in \mathbb{N}$, we have:

- $V_{\mathbb{P}}(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} V_{\mathbb{P}}(I_\lambda)$.
- $V_{\mathbb{P}}(\bigcap_{k=1}^{m} I_k) = V_{\mathbb{P}}(\prod_{k=1}^{m} I_k) = \bigcup_{k=1}^{m} V_{\mathbb{P}}(I_k)$.
- $V_{\mathbb{P}}(\sqrt{I}) = V_{\mathbb{P}}(I)$.

Fact 3.7.82. If $X = \bigcup_{\lambda \in \Lambda} U_\lambda$ is an open covering of a topological space then X is Noetherian iff there is a finite subcovering and all U_λ are Noetherian.

Proof. By definition, a topological space is Noetherian $\iff$ all open subsets are quasi-compact. □

Corollary 3.8. The Zariski topology on $\mathbb{P}^n$ is indeed a topology. The induced topology on the open set $\mathbb{A}^n = \mathbb{P}^n \backslash V_{\mathbb{P}}(X_0) \cong \mathfrak{k}^n$ is the Zariski topology on $\mathfrak{k}^n$. The same holds for all $U_i = \mathbb{P}^n \backslash V_{\mathbb{P}}(X_i) \cong \mathfrak{k}^n$. Moreover, the topological space $\mathbb{P}^n$ is Noetherian.

3.1 Noetherianness of graded rings

Proposition 3.9. For a graded ring $R_\bullet$, the following conditions are equivalent:

A R is Noetherian.

B Every homogeneous ideal of $R_\bullet$ is finitely generated.

C Every chain $I_0 \subseteq I_1 \subseteq \ldots$ of homogeneous ideals terminates.

D Every set $\mathfrak{M} \neq \varnothing$ of homogeneous ideals has a $\subseteq$-maximal element.

E R_0 is Noetherian and the ideal R_+ is finitely generated.

F R_0 is Noetherian and R/R_0 is of finite type.

Proof. **A** $\implies$ **B,C,D** trivial.

B $\iff$ **C** $\iff$ **D** similar to the proof about Noetherianness.

B $\wedge$ **C** $\implies$ **E** B implies that R_+ is finitely generated. Since $I \oplus R_+$ is homogeneous for any homogeneous ideal $I \subseteq R_0$, C implies the Noetherianness of R_0.

E $\implies$ **F** Let R_+ be generated by $f_i \in R_{d_i}, d_i > 0$ as an ideal.

Claim 1. *The R_0-subalgebra $\tilde{R}$ of R generated by the f_i equals R.*

Subproof. It is sufficient to show that every homogeneous $f \in R_d$ belongs to $\tilde{R}$. We use induction on d. The case of $d = 0$ is trivial. Let $d > 0$ and $R_e \subseteq \tilde{R}$ for all $e < d$. As $f \in R_+$, $f = \sum_{i=1}^k g_i f_i$. Let $f_a = \sum_{i=1}^k g_{i,a-d_i} f_i$, where $g_i = \sum_{b=0}^\infty g_{i,b}$ is the decomposition into homogeneous components. Then $f = \sum_{a=0}^\infty f_a$ is the decomposition of f into homogeneous components, hence $a \neq d \implies f_a = 0$. Thus we may assume $g_i \in R_{d-d_i}$. As $d_i > 0$, the induction assumption may now be applied to g_i, hence $g_i \in \tilde{R}$, hence $f \in \tilde{R}$. ■

F $\implies$ **A** Hilbert's Basissatz (1.3)

□

3.2 The projective form of the Nullstellensatz and the closed subsets of $\mathbb{P}^n$

Let $A = \mathfrak{k}[X_0, \ldots, X_n]$.

Proposition 3.10 (Projective form of the Nullstellensatz)**.** If $I \subseteq A$ is a homogeneous ideal and $f \in A_d$ with $d > 0$, then $V_{\mathbb{P}}(I) \subseteq V_{\mathbb{P}}(f) \iff f \in \sqrt{I}$.

Proof. $\Longleftarrow$ is clear. Let $V_{\mathbb{P}}(I) \subseteq V_{\mathbb{P}}(f)$. If $x = (x_0, \dots, x_n) \in V_{\mathbb{A}}(I)$, then either $x = 0$ in which case $f(x) = 0$ since $d > 0$ or the point $[x_0, \dots, x_n] \in \mathbb{P}^n$ is well-defined and belongs to $V_{\mathbb{P}}(I) \subseteq V_{\mathbb{P}}(f)$, hence $f(x) = 0$. Thus $V_{\mathbb{A}}(I) \subseteq V_{\mathbb{A}}(f)$ and $f \in \sqrt{I}$ be the Nullstellensatz (2.13). □

Definition 3.11. [a] For a graded ring $R_\bullet$, let $\operatorname{Proj}(R_\bullet)$ be the set of $\mathfrak{p} \in \operatorname{Spec} R$ such that $\mathfrak{p}$ is a homogeneous ideal and $\mathfrak{p} \not\supseteq R_+$.

[a] This definition is not too important, the characterization in the following remark suffices.

Remark 3.11.83. As the elements of $A_0 \backslash \{0\}$ are units in A it follows that for every homogeneous ideal I we have $I \subseteq A_+$ or $I = A$. In particular, $\operatorname{Proj}(A_\bullet) = \{\mathfrak{p} \in \operatorname{Spec} A \backslash A_+ | \mathfrak{p} \text{ is homogeneous}\}$.

Proposition 3.12. There is a bijection

$$\begin{aligned} f : \{I \subseteq A_+ | I \text{ homogeneous ideal}, I = \sqrt{I}\} &\longrightarrow \{X \subseteq \mathbb{P}^n | X \text{ closed}\} \\ I &\longmapsto V_{\mathbb{P}}(I) \\ \langle \{f \in A_d | d > 0, X \subseteq V_{\mathbb{P}}(f)\} \rangle &\longleftarrow\!\shortmid X \end{aligned}$$

Under this bijection, the irreducible subsets correspond to the elements of $\operatorname{Proj}(A_\bullet)$.

Proof. From the projective form of the Nullstellensatz it follows that f is injective and that $f^{-1}(V_{\mathbb{P}}(I)) = \sqrt{I} = I$. If $X \subseteq \mathbb{P}^n$ is closed, then $X = V_{\mathbb{P}}(J)$ for some homogeneous ideal $J \subseteq A$. Without loss of generality loss of generality $J = \sqrt{J}$. If $J \nsubseteq A_+$, then $J = A$ (3.11.83), hence $X = V_{\mathbb{P}}(J) = \varnothing = V_{\mathbb{P}}(A_+)$. Thus we may assume $J \subseteq A_+$, and f is surjective.

Suppose $\mathfrak{p} \in \operatorname{Proj}(A_\bullet)$. Then $\mathfrak{p} \neq A_+$ hence $X = V_{\mathbb{P}}(\mathfrak{p}) \neq \varnothing$ by the proven part of the proposition. Assume $X = X_1 \cup X_2$ is a decomposition into proper closed subsets, where $X_k = V_{\mathbb{P}}(I_k)$ for some $I_k \subseteq A_+, I_k = \sqrt{I_k}$. Since X_k is a proper subset of X, there is $f_k \in I_k \backslash \mathfrak{p}$. We have $V_{\mathbb{P}}(f_1 f_2) \supseteq V_{\mathbb{P}}(f_k) \supseteq V_{\mathbb{P}}(I_k)$ hence $V_{\mathbb{P}}(f_1 f_2) \supseteq V_{\mathbb{P}}(I_1) \cup V_{\mathbb{P}}(I_2) = X = V_{\mathbb{P}}(\mathfrak{p})$ and it follows that $f_1 f_2 \in \sqrt{\mathfrak{p}} = \mathfrak{p}$ ↯.

Assume $X = V_{\mathbb{P}}(\mathfrak{p})$ is irreducible, where $\mathfrak{p} = \sqrt{\mathfrak{p}} \in A_+$ is homogeneous. The $\mathfrak{p} \neq A_+$ as $X = \varnothing$ otherwise. Assume that $f_1 f_2 \in \mathfrak{p}$ but $f_i \notin A_{d_i} \backslash \mathfrak{p}$. Then $X \nsubseteq V_{\mathbb{P}}(f_i)$ by the projective Nullstellensatz when $d_i > 0$ and because $V_{\mathbb{P}}(1) = \varnothing$

when $d_i = 0$. Thus $X = (X \cap V_{\mathbb{P}}(f_1)) \cup (X \cap V_{\mathbb{P}}(f_2))$ is a proper decomposition $\lightning$. By lemma 3.14, $\mathfrak{p}$ is a prime ideal. □

Remark 3.12.84. It is important that $I \subseteq A_{+}$, since $V_{\mathbb{P}}(A) = V_{\mathbb{P}}(A_+) = \varnothing$ would be a counterexample.

Corollary 3.13. $\mathbb{P}^n$ is irreducible.

Proof. Apply 3.12 to $\{0\} \in \operatorname{Proj}(A_\bullet)$. □

3.3 Some remarks on homogeneous prime ideals

Lemma 3.14. Let $R_\bullet$ be an $\mathbb{I}$ graded ring ($\mathbb{I} = \mathbb{N}$ or $\mathbb{I} = \mathbb{Z}$). A homogeneous ideal $I \subseteq R$ is a prime ideal iff $1 \notin I$ and for all homogeneous elements $f, g \in R$

$$fg \in I \implies f \in I \vee g \in I.$$

Proof. $\implies$ is trivial. It suffices to show that for arbitrary $f, g \in R$ we have that $fg \in I \implies f \in I \vee g \in I$. Let $f = \sum_{d \in \mathbb{I}} f_d, g = \sum_{d \in \mathbb{I}} g_d$ be the decompositions into homogeneous components. If $f \notin I$ and $g \notin I$ there are $d, e \in I$ with $f_d \in I$, $g_e \in I$, and they may assumed to be maximal with this property. As I is homogeneous and $fg \in I$, we have $(fg)_{d+e} \in I$ but

$$(fg)_{d+e} = f_d g_e + \sum_{\delta=1}^{\infty} (f_{d+\delta} g_{e-\delta} + f_{d-\delta} g_{e+\delta})$$

where $f_d g_e \notin I$ by our assumption on I and all other summands on the right hand side are $\in I$ (as $f_{d+\delta} \in I$ and $g_{e+\delta} \in I$ by the maximality of d and e), a contradiction. □

Remark 3.14.85. If $R_\bullet$ is $\mathbb{N}$-graded and $\mathfrak{p} \in \operatorname{Spec} R_0$, then

$$\mathfrak{p} \oplus R_+ = \{r \in R | r_0 \in \mathfrak{p}\}$$

is a homogeneous prime ideal of R.

$$\begin{aligned} &\{\mathfrak{p} \in \operatorname{Spec} R | \mathfrak{p} \text{ is a homogeneous ideal of } R_\bullet\} \\ = &\operatorname{Proj}(R_\bullet) \sqcup \{\mathfrak{p} \oplus R_+ | \mathfrak{p} \in \operatorname{Spec} R_0\}. \end{aligned}$$

3.4 Dimension of $\mathbb{P}^n$

Proposition 3.15.

- $\mathbb{P}^n$ is catenary.
- $\dim(\mathbb{P}^n) = n$. Moreover, $\operatorname{codim}(\{x\}, \mathbb{P}^n) = n$ for every $x \in \mathbb{P}^n$.
- If $X \subseteq \mathbb{P}^n$ is irreducible and $x \in X$, then

$$\operatorname{codim}(\{x\}, X) = \dim(X) = n - \operatorname{codim}(X, \mathbb{P}^n).$$

- If $X \subseteq Y \subseteq \mathbb{P}^n$ are irreducible subsets, then

$$\operatorname{codim}(X, Y) = \dim(Y) - \dim(X).$$

Proof. Let $X \subseteq \mathbb{P}^n$ be irreducible. If $x \in X$, there is an integer $0 \leqslant i \leqslant n$ and $X \in U_i = \mathbb{P}^n \backslash V_{\mathbb{P}}(X_i)$. Without loss of generality loss of generality $i = 0$. Then $\operatorname{codim}(X, \mathbb{P}^n) = \operatorname{codim}(X \cap \mathbb{A}^n, \mathbb{A}^n)$ by the locality of Krull codimension (2.24). Applying this with $X = \{x\}$ and our results about the affine case gives the second assertion. If Y and Z are also irreducible with $X \subseteq Y \subseteq Z$, then $\operatorname{codim}(X, Y) = \operatorname{codim}(X \cap \mathbb{A}^n, Y \cap \mathbb{A}^n)$, $\operatorname{codim}(X, Z) = \operatorname{codim}(X \cap \mathbb{A}^n, Z \cap \mathbb{A}^n)$ and $\operatorname{codim}(Y, Z) = \operatorname{codim}(Y \cap \mathbb{A}^n, Z \cap \mathbb{A}^n)$. Thus

$$\begin{aligned}\operatorname{codim}(X, Y) + \operatorname{codim}(Y, Z) &= \operatorname{codim}(X \cap \mathbb{A}^n, Y \cap \mathbb{A}^n) \\ &\quad + \operatorname{codim}(Y \cap \mathbb{A}^n, Z \cap \mathbb{A}^n) \\ &= \operatorname{codim}(X \cap \mathbb{A}^n, Z \cap \mathbb{A}^n) \\ &= \operatorname{codim}(X, Z)\end{aligned}$$

because $\mathfrak{k}^n$ is catenary and the first point follows. The remaining assertions can easily be derived from the first two. □

3.5 The cone $C(X)$

Definition 3.16. If $X \subseteq \mathbb{P}^n$ is closed, we define the **affine cone over X**

$$C(X) = \{0\} \cup \{(x_0, \ldots, x_n) \in \mathfrak{k}^{n+1} \backslash \{0\} | [x_0, \ldots, x_n] \in X\}$$

If $X = V_{\mathbb{P}}(I)$ where $I \subseteq A_+ = \mathfrak{k}[X_0, \ldots, X_n]_+$ is homogeneous, then $C(X) = V_{\mathbb{A}}(I)$.

Proposition 3.17.

- $C(X)$ is irreducible iff X is irreducible or $X = \varnothing$.
- If X is irreducible, then

$$\dim(C(X)) = \dim(X) + 1$$

and
$$\operatorname{codim}(C(X), \mathfrak{k}^{n+1}) = \operatorname{codim}(X, \mathbb{P}^n).$$

Proof. The first assertion follows from 3.12 and 2.22 (bijection of irreducible subsets and prime ideals in the projective and affine case).

Let $d = \dim(X)$ and
$$X_0 \subsetneq \ldots \subsetneq X_d = X \subsetneq X_{d+1} \subsetneq \ldots \subsetneq X_n = \mathbb{P}^n$$
be a chain of irreducible subsets of $\mathbb{P}^n$. Then
$$\{0\} \subsetneq C(X_0) \subsetneq \ldots \subsetneq C(X_d) = C(X) \subsetneq \ldots \subsetneq C(X_n) = \mathfrak{k}^{n+1}$$
is a chain of irreducible subsets of $\mathfrak{k}^{n+1}$. Hence $\dim(C(X)) \geqslant 1 + d$ and $\operatorname{codim}(C(X), \mathfrak{k}^{n+1}) \geqslant n - d$. Since
$$\dim(C(X)) + \operatorname{codim}(C(X), \mathfrak{k}^{n+1}) = \dim(\mathfrak{k}^{n+1}) = n + 1,$$
the two inequalities must be equalities. □

3.5.1 Application to hypersurfaces in $\mathbb{P}^n$

Definition 3.18 (Hypersurface)**.** Let $n > 0$. By a **hypersurface** in $\mathbb{P}^n$ or $\mathbb{A}^n$ we understand an irreducible closed subset of codimension 1.

Corollary 3.19. If $P \in A_d$ is a prime element, then $H = V_{\mathbb{P}}(P)$ is a hypersurface in $\mathbb{P}^n$ and every hypersurface H in $\mathbb{P}^n$ can be obtained in this way.

Proof. If $H = V_{\mathbb{P}}(P)$ then $C(H) = V_{\mathbb{A}}(P)$ is a hypersurface in $\mathfrak{k}^{n+1}$ by 2.28. By 3.17, H is irreducible and of codimension 1.

Conversely, let H be a hypersurface in $\mathbb{P}^n$. By 3.17, $C(H)$ is a hypersurface in $\mathfrak{k}^{n+1}$, hence $C(H) = V_{\mathbb{P}}(P)$ for some prime element $P \in A$ (again by 2.28). We have $H = V_{\mathbb{P}}(\mathfrak{p})$ for some $\mathfrak{p} \in \operatorname{Proj}(A)$ and $C(H) = V_{\mathbb{A}}(\mathfrak{p})$. By the bijection between closed subsets of $\mathfrak{k}^{n+1}$ and ideals $I = \sqrt{I} \subseteq A$ (2.14), $\mathfrak{p} = P \cdot A$. Let $P = \sum_{k=0}^{d} P_k$ with $P_d \neq 0$ be the decomposition into homogeneous components. If P_e with $e < d$ was $\neq 0$, it could not be a multiple of P contradicting the homogeneity of $\mathfrak{p} = P \cdot A$. Thus, P is homogeneous of degree d. □

Definition 3.20. A hypersurface $H \subseteq \mathbb{P}^n$ has **degree** d if $H = V_{\mathbb{P}}(P)$, where $P \in A_d$ is an irreducible polynomial.

3.5.2 Application to intersections in $\mathbb{P}^n$ and Bezout's theorem

Corollary 3.21. Let $A \subseteq \mathbb{P}^n$ and $B \subseteq \mathbb{P}^n$ be irreducible subsets of dimensions a and b. If $a + b \geqslant n$, then $A \cap B \neq \varnothing$ and every irreducible component of $A \cap B$ has dimension $\geqslant a + b - n$.

Remark 3.21.86. This shows that $\mathbb{P}^n$ indeed fulfilled the goal of allowing for nicer results of algebraic geometry because "solutions at infinity" to systems of algebraic equations are present in $\mathbb{P}^n$ (see 2.80.69).

Proof. The lower bound on the dimension of irreducible components of $A \cap B$ is easily derived from the similar affine result (corollary of the principal ideal theorem, 2.81).

From the definition of the affine cone it follows that $C(A \cap B) = C(A) \cap C(B)$. We have $\dim(C(A)) = a + 1$ and $\dim(C(B)) = b + 1$ by 3.17. If $A \cap B = \varnothing$, then $C(A) \cap C(B) = \{0\}$ with $\{0\}$ as an irreducible component, contradicting the lower bound $a + b + 1 - n > 0$ for the dimension of irreducible components of $C(A) \cap C(B)$ (again 2.81). □

Remark 3.21.87 (Bezout's theorem)**.** If $A \neq B$ are hypersurfaces of degree a and b in $\mathbb{P}^2$, then $A \cap B$ has ab points counted by (suitably defined) multiplicity.

4 Varieties

4.1 Sheaves

Definition 4.1 (Sheaf)**.** Let X be any topological space.

A **presheaf** $\mathcal{G}$ of sets (or rings, (abelian) groups) on X associates a set (or rings, or (abelian) group) $\mathcal{G}(U)$ to every open subset U of X, and a map (or ring or group homomorphism) $\mathcal{G}(U) \xrightarrow{r_{U,V}} \mathcal{G}(V)$ to every inclusion $V \subseteq U$ of open subsets of X such that $r_{U,W} = r_{V,W} r_{U,V}$ for inclusions $U \subseteq V \subseteq W$ of open subsets.

Elements of $\mathcal{G}(U)$ are often called **sections** of $\mathcal{G}$ on U or **global sections** when $U = X$.

Let $U \subseteq X$ be open and $U = \bigcup_{i \in I} U_i$ an open covering. A family $(f_i)_{i \in I} \in \prod_{i \in I} \mathcal{G}(U_i)$ is called **compatible** if $r_{U_i, U_i \cap U_j}(f_i) = r_{U_j, U_i \cap U_j}(f_j)$ for all $i, j \in I$.

Consider the map

$$\varphi_{U,(U_i)_{i\in I}} : \mathcal{G}(U) \longrightarrow \{(f_i)_{i\in I} \in \prod_{i\in I} \mathcal{G}(U_i) | r_{U_i,U_i\cap U_j}(f_i) = r_{U_j,U_i\cap U_j}(f_j) \text{ for } i,j \in I\}$$
$$f \longmapsto (r_{U,U_i}(f))_{i\in I}$$

A presheaf is called **separated** if $\varphi_{U,(U_i)_{i\in I}}$ is injective for all such U and $(U_i)_{i\in I}$.[a] It satisfies **gluing** if $\varphi_{U,(U_i)_{i\in I}}$ is surjective.

A presheaf is called a **sheaf** if it is separated and satisfies gluing.

The bijectivity of the $\varphi_{U,(U_i)_{i\in I}}$ is called the **sheaf axiom**.

[a] This also called "locality".

Trivial Nonsense† 4.1.88. A presheaf is a contravariant functor $\mathcal{G} : \mathcal{O}(X) \to C$ where $\mathcal{O}(X)$ denotes the category of open subsets of X with inclusions as morphisms and C is the category of sets, rings or (abelian) groups.

Definition 4.2. A subsheaf $\mathcal{G}'$ is defined by subsets (resp. subrings or subgroups) $\mathcal{G}'(U) \subseteq \mathcal{G}(U)$ for all open $U \subseteq X$ such that the sheaf axioms still hold.

Remark 4.2.89. If $\mathcal{G}$ is a sheaf on X and $\Omega \subseteq X$ open, then $\mathcal{G} \restriction_\Omega (U) := \mathcal{G}(U)$ for open $U \subseteq \Omega$ and $r_{U,V}^{(\mathcal{G}\restriction_\Omega)}(f) := r_{U,V}^{(\mathcal{G})}(f)$ is a sheaf of the same kind as $\mathcal{G}$ on Ω.

Remark 4.2.90. The notion of restriction of a sheaf to a closed subset, or of preimages under general continuous maps, can be defined but this is a bit harder.

Notation 4.2.91. It is often convenient to write $f \restriction_V$ instead of $r_{U,V}(f)$.

Remark 4.2.92. Applying the **sheaf axiom** to the empty covering of $U = \varnothing$, one finds that $\mathcal{G}(\varnothing) = \{0\}$.

4.1.1 Examples of sheaves

Example 4.3. Let G be a set and let $\mathfrak{G}(U)$ be the set of arbitrary maps $U \xrightarrow{f} G$. We put $r_{U,V}(f) = f \restriction_V$. It is easy to see that this defines a sheaf. If $\cdot$ is a group operation on G, then $(f \cdot g)(x) := f(x) \cdot g(x)$ defines the structure of a sheaf of group on $\mathfrak{G}$. Similarly, a ring structure on G can be used to define the structure of a sheaf of rings on $\mathfrak{G}$.

Example 4.4. If in the previous example G carries a topology and $\mathcal{G}(U) \subseteq \mathfrak{G}(U)$ is the subset (subring, subgroup) of continuous functions $U \xrightarrow{f} G$, then $\mathcal{G}$ is a subsheaf of $\mathfrak{G}$, called the sheaf of continuous G-valued functions on (open subsets of) X.

Example 4.5. If $X = \mathbb{R}^n$, $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ and $\mathcal{O}(U)$ is the sheaf of $\mathbb{K}$-valued C^∞-functions on U, then $\mathcal{O}$ is a subsheaf of the sheaf (of rings) of $\mathbb{K}$-valued continuous functions on X.

Example 4.6. If $X = \mathbb{C}^n$ and $\mathcal{O}(U)$ the set of holomorphic functions on X, then $\mathcal{O}$ is a subsheaf of the sheaf of $\mathbb{C}$-valued C^∞-functions on X.

4.1.2 The structure sheaf on a closed subset of $\mathfrak{k}^n$

Let $X \subseteq \mathfrak{k}^n$ be open. Let $R = \mathfrak{k}[X_1, \ldots, X_n]$.

Definition 4.7. For open subsets $U \subseteq X$, let $\mathcal{O}_X(U)$ be the set of functions $U \xrightarrow{\varphi} \mathfrak{k}$ such that every $x \in U$ has a neighbourhood V such that there are $f, g \in R$ such that for $y \in V$ we have $g(y) \neq 0$ and $\varphi(y) = \frac{f(y)}{g(y)}$.

Remark 4.7.93. $\mathcal{O}_X$ is a subsheaf (of rings) of the sheaf of $\mathfrak{k}$-valued functions on X. The elements of $\mathcal{O}_X(U)$ are continuous: Let $M \subseteq \mathfrak{k}$ be closed. We must show the closedness of $N := \varphi^{-1}(M)$ in U. For $M = \mathfrak{k}$ this is trivial. Otherwise M is finite and we may assume $M = \{t\}$ for some $t \in \mathfrak{k}$. For $x \in U$, there are open $V_x \subseteq U$ and $f_x, g_x \in R$ such that $\varphi = \frac{f_x}{g_x}$ on V_x. Then $N \cap V_x = V(f_x - t \cdot g_x) \cap V_x)$ is closed in V_x. As the V_x cover U and U is quasi-compact, N is closed in U.

Proposition 4.8. Let $X = V(I)$ where $I = \sqrt{I} \subseteq R$ is an ideal. Let $A = R/I$. Then

$$\begin{aligned} \varphi : A &\longrightarrow \mathcal{O}_X(X) \\ f \mod I &\longmapsto f \restriction_X \end{aligned}$$

is an isomorphism.

Proof. It is easy to see that the map $A \to \mathcal{O}_X(X)$ is well-defined and a ring homomorphism. Its injectivity follows from the Nullstellensatz and $I = \sqrt{I}$ (2.13).

Let $\varphi \in \mathcal{O}_X(X)$. For $x \in X$, there are an open subset $U_x \subseteq X$ and $f_x, g_x \in R$ such that $\varphi = \frac{f_x}{g_x}$ on U_x.

Claim 1. *Without loss of generality loss of generality we can assume $U_x = X \backslash V(g_x)$.*

Subproof. The closed subsets $(X\backslash U_x) \subseteq \mathfrak{k}^n$ has the form $X\backslash U_x = V(J_x)$ for some ideal $J_x \subseteq R$. As $x \notin X\backslash V_x$ there is $h_x \in J_x$ with $h_x(x) \neq 0$. Replacing U_x by $X\backslash V(h_x)$, f_x by $f_x h_x$ and g_x by $g_x h_x$, we may assume $U_x = X\backslash V(g_x)$. ■

Claim 2. *Without loss of generality loss of generality we can assume $V(g_x) \subseteq V(f_x)$.*

Subproof. Replace f_x by $f_x g_x$ and g_x by g_x^2. ■

As X is quasi-compact, there are finitely many points $(x_i)_{i=1}^m$ such that the U_{x_i} cover X. Let $U_i := U_{x_i}, f_i := f_{x_i}, g_i := g_{x_i}$.

As the $U_i = X\backslash V(g_i)$ cover X, $V(I) \cap \bigcap_{i=1}^m V(g_i) = X \cap \bigcap_{i=1}^m V(g_i) = \varnothing$. By the Nullstellensatz (2.2) the ideal of R generated by I and the a_i equals R. There are thus $n \geqslant m \in \mathbb{N}$ and elements $(g_i)_{i=m+1}^n$ of I and $(a_i)_{i=1}^n \in R^n$ such that $1 = \sum_{i=1}^n a_i g_i$. Let for $i > m$ $f_i := 0$, $F = \sum_{i=1}^n a_i f_i = \sum_{i=1}^m a_i f_i \in R$.

Claim 3. *For all $x \in X$ $\quad f_i(x) = \varphi(x) g_i(x)$.*

Subproof. If $x \in V_i$ this follows by our choice of f_i and g_i. If $x \in X\backslash V_i$ or $i > m$ both sides are zero. ■

It follows that

$$\varphi(x) = \varphi(x) \cdot 1 = \varphi(x) \cdot \sum_{i=1}^n a_i(x) g_i(x) = \sum_{i=1}^n a_i(x) f_i(x) = F(x)$$

Hence $\varphi = F \restriction_X$. □

4.1.3 The structure sheaf on closed subsets of $\mathbb{P}^n$

Let $X \subseteq \mathbb{P}^n$ be closed and $R_\bullet = \mathfrak{k}[X_0, \dots, X_n]$ with its usual grading.

Definition 4.9. For open $U \subseteq X$, let $\mathcal{O}_X(U)$ be the set of functions $U \xrightarrow{\varphi} \mathfrak{k}$ such that for every $x \in U$, there are an open subset $W \subseteq U$, a natural number d and $f, g \in R_d$ such that $W \cap V_{\mathbb{P}}(g) = \varnothing$ and $\varphi(y) = \frac{f(y_0, \dots, y_n)}{g(y_0, \dots, y_n)}$ for $y = [y_0, \dots, y_n] \in W$.

Remark 4.9.94. This is a subsheaf of rings of the sheaf of $\mathfrak{k}$-valued functions on X. Under the identification $\mathbb{A}^n = \mathfrak{k}^n$ with $\mathbb{P}^n \backslash V_{\mathbb{P}}(X_0)$, one has $\mathcal{O}_X \upharpoonright_{X \backslash V_{\mathbb{P}}(X_0)} = \mathcal{O}_{X \cap \mathbb{A}^n}$ as subsheaves of the sheaf of $\mathfrak{k}$-valued functions, where the second sheaf is a sheaf on a closed subset of $\mathfrak{k}^n$:

Indeed, if W is as in the definition then $\varphi([1, y_1, \ldots, y_n]) = \frac{f(1,y_1,\ldots,y_n)}{g(1,y_1,\ldots,y_n)}$ for $[1, y_1, \ldots, y_n] \in W$. Conversely if $\varphi([1, y_1, \ldots, y_n]) = \frac{f(y_1,\ldots,y_n)}{g(y_1,\ldots,y_n)}$ on an open subset W of $X \cap \mathbb{A}^n$ then $\varphi([y_0, \ldots, y_n]) = \frac{F(y_0,\ldots,y_n)}{G(y_0,\ldots,y_n)}$ on W where $F(X_0, \ldots, X_n) := X_0^d f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$ and $G(X_0, \ldots, X_n) = X_0^d g(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$ with a sufficiently large $d \in \mathbb{N}$.

Remark 4.9.95. It follows from the previous remark and the similar result in the affine case that the elements of $\mathcal{O}_X(U)$ are continuous on $U \backslash V(X_0)$. Since the situation is symmetric in the homogeneous coordinates, they are continuous on all of U.

The following is somewhat harder than in the affine case:

Proposition 4.10. If X is connected (e.g. irreducible), then the elements of $\mathcal{O}_X(X)$ are constant functions on X.

4.2 The notion of a category

Definition 4.11. A **category** $\mathcal{A}$ consists of:

- A class $\operatorname{Ob}\mathcal{A}$ of **objects of $\mathcal{A}$**.
- For two arbitrary objects $A, B \in \operatorname{Ob}\mathcal{A}$, a **set** $\operatorname{Hom}_{\mathcal{A}}(A, B)$ of **morphisms for A to B in $\mathcal{A}$**.
- A map $\operatorname{Hom}_{\mathcal{A}}(B, C) \times \operatorname{Hom}_{\mathcal{A}}(A, B) \xrightarrow{\circ} \operatorname{Hom}_{\mathcal{A}}(A, C)$, the composition of morphisms, for arbitrary triples (A, B, C) of objects of $\mathcal{A}$.

The following conditions must be satisfied:

A For morphisms $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$.

B For every $A \in \operatorname{Ob}(\mathcal{A})$, there is an $\operatorname{Id}_A \in \operatorname{Hom}_{\mathcal{A}}(A, A)$ such that $\operatorname{Id}_A \circ f = f$ (reps. $g \circ \operatorname{Id}_A = g$) for arbitrary morphisms $B \xrightarrow{f} A$ (reps. $A \xrightarrow{g} C$).

A morphism $X \xrightarrow{f} Y$ is called an **isomorphism (in $\mathcal{A}$)** if there is a morphism $Y \xrightarrow{g} X$ (called the **inverse f^{-1} of f**) such that $g \circ f = \operatorname{Id}_X$ and $f \circ g = \operatorname{Id}_Y$.

Remark 4.11.96.

- The distinction between classes and sets is important here.
- We will usually omit the composition sign $\circ$.
- It is easy to see that Id_A is uniquely determined by the above condition B, and that the inverse f^{-1} of an isomorphism f is uniquely determined.

4.2.1 Examples of categories

Example 4.12.

- The category of sets.
- The category of groups.
- The category of rings.
- If R is a ring, the category of R-modules and the category $\mathbf{Alg}_R$ of R-algebras
- The category of topological spaces.
- The category $\mathrm{Var}_{\mathfrak{k}}$ of varieties over $\mathfrak{k}$ (see 4.17).
- If $\mathcal{A}$ is a category, then the **opposite category** or **dual category** is defined by $\mathrm{Ob}(\mathcal{A}\mathrm{op}) = \mathrm{Ob}(\mathcal{A})$ and $\mathrm{Hom}_{\mathcal{A}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathcal{A}}(Y, X)$.

In most of these cases, isomorphisms in the category were just called 'isomorphism'. The isomorphisms in the category of topological spaces are the homeomophisms.

4.2.2 Subcategories

Definition 4.13 (Subcategories)**.** A **subcategory** of $\mathcal{A}$ is a category $\mathcal{B}$ such that $\mathrm{Ob}(\mathcal{B}) \subseteq \mathrm{Ob}(\mathcal{A})$, such that $\mathrm{Hom}_{\mathcal{B}}(X, Y) \subseteq \mathrm{Hom}_{\mathcal{A}}(X, Y)$ for objects X and Y of $\mathcal{B}$, such that for every object $X \in \mathrm{Ob}(\mathcal{B})$, the identity Id_X of X is the same in $\mathcal{B}$ as in $\mathcal{A}$, and such that for composable morphisms in $\mathcal{B}$, their compositions in $\mathcal{A}$ and $\mathcal{B}$ coincide. We call $\mathcal{B}$ a **full subcategory** of $\mathcal{A}$ if in addition $\mathrm{Hom}_{\mathcal{B}}(X, Y) = \mathrm{Hom}_{\mathcal{A}}(X, Y)$ for arbitrary $X, Y \in \mathrm{Ob}(\mathcal{B})$.

Example 4.14.

- The category of abelian groups is a full subcategory of the category of groups. It can be identified with the category of $\mathbb{Z}$-modules.
- The category of finitely generated R-modules as a full subcategory of the category of R-modules.

- The category of R-algebras of finite type as a full subcategory of $\mathbf{Alg}_R$.
- The category of affine varieties over $\mathfrak{k}$ as a full subcategory of the category of varieties over $\mathfrak{k}$.

4.2.3 Functors and equivalences of categories

Definition 4.15. A **(covariant) functor** (resp. **contravariant functor**) between categories $\mathcal{A} \xrightarrow{F} \mathcal{B}$ is a map $\mathrm{Ob}(\mathcal{A}) \xrightarrow{F} \mathrm{Ob}(\mathcal{B})$ with a family of maps $\mathrm{Hom}_{\mathcal{A}}(X,Y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{B}}(F(X),F(Y))$ (resp. $\mathrm{Hom}_{\mathcal{A}}(X,Y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{B}}(F(Y),F(X))$ in the case of contravariant functors), where X and Y are arbitrary objects of $\mathcal{A}$, such that the following conditions hold:

- $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$.
- For morphisms $X \xrightarrow{f} Y \xrightarrow{g} Z$ in $\mathcal{A}$, we have $F(gf) = F(g)F(f)$ (resp. $F(gf) = F(f)F(g)$).

A functor is called **essentially surjective** if every object of $\mathcal{B}$ is isomorphic to an element of the image of $\mathrm{Ob}(\mathcal{A}) \xrightarrow{F} \mathrm{Ob}(\mathcal{B})$. A functor is called **full** (resp. **faithful**) if it induces surjective (resp. injective) maps between sets of morphisms. It is called an **equivalence of categories** if it is full, faithful and essentially surjective.

Example 4.16.

- There are **forgetful functors** from rings to abelian groups or from abelian groups to sets which drop the multiplicative structure of a ring or the group structure of a group.
- If $\mathfrak{k}$ is any vector space there is a contravariant functor from $\mathfrak{k}$-vector spaces to itself sending V to its dual vector space $V \subseteq$ and $V \xrightarrow{f} W$ to the dual linear map $W^* \xrightarrow{f^*} V^*$. When restricted to the full subcategory of finite-dimensional vector spaces it becomes a contravariant self-equivalence of that category.
- The embedding of a subcategory is a faithful functor. In the case of a full subcategory it is also full.

4.3 The category of varieties

Definition 4.17 (Algebraic variety)**.** An **algebraic variety** or **prevariety** over $\mathfrak{k}$ is a pair $(X, \mathcal{O}_X)$, where X is a topological space and $\mathcal{O}_X$ a subsheaf of the sheaf of $\mathfrak{k}$-valued functions on X such that for every $x \in X$, there are a neighbourhood U_x of x in X, an open subset V_x

of a closed subset Y_x of $\mathfrak{k}^{n_x}$[a] and a homeomorphism $V_x \xrightarrow{\iota_x} U_x$ such that for every open subset $V \subseteq U_x$ and every function $V \xrightarrow{f} \mathfrak{k}$, we have $f \in \mathcal{O}_X(V) \iff \iota_x^*(f) \in \mathcal{O}_{Y_x}(\iota_x^{-1}(V))$.

In this, the **pull-back** $\iota_x^*(f)$ of f is defined by $(\iota_x^*(f))(\xi) := f(\iota_x(\xi))$.

A morphism $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ of varieties is a continuous map $X \xrightarrow{\varphi} Y$ such that for all open $U \subseteq Y$ and $f \in \mathcal{O}_Y(U)$, $\varphi^*(f) \in \mathcal{O}_X(\varphi^{-1}(U))$. An isomorphism is a morphism such that φ is bijective and φ^{-1} also is a morphism of varieties.

[a] By the result of 4.24, it can be assumed that $V_x = Y_x$ without altering the definition.

Example 4.18.
- If $(X, \mathcal{O}_X)$ is a variety and $U \subseteq X$ open, then $(U, \mathcal{O}_X \restriction_U)$ is a variety (called an **open subvariety** of X), and the embedding $U \to X$ is a morphism of varieties.
- If X is a closed subset of $\mathfrak{k}^n$ or $\mathbb{P}^n$, then $(X, \mathcal{O}_X)$ is a variety, where $\mathcal{O}_X$ is the structure sheaf on X (4.7, reps. 4.9). A variety is called **affine** (resp. **projective**) if it is isomorphic to a variety of this form, with X closed in $\mathfrak{k}^n$ (resp. $\mathbb{P}^n$). A variety which is isomorphic to and open subvariety of X is called **quasi-affine** (resp. **quasi-projective**).
- If $X = V(X^2 - Y^3) \subseteq \mathfrak{k}^2$ then $\mathfrak{k} \xrightarrow{t \mapsto (t^3, t^2)} X$ is a morphism which is a homeomorphism of topological spaces but not an isomorphism of varieties.
- The composition of two morphisms $X \to Y \to Z$ of varieties is a morphism of varieties.
- $X \xrightarrow{\mathrm{Id}_X} X$ is a morphism of varieties.

4.3.1 The category of affine varieties

Lemma 4.19. Let X be any $\mathfrak{k}$-variety and $U \subseteq X$ open.

i) All elements of $\mathcal{O}_X(U)$ are continuous.

ii) If $U \subseteq X$ is open, $U \xrightarrow{\lambda} \mathfrak{k}$ any function and every $x \in U$ has a neighbourhood $V_x \subseteq U$ such that $\lambda \restriction_{V_x} \in \mathcal{O}_X(V_x)$, then $\lambda \in \mathcal{O}_X(U)$.

iii) If $\vartheta \in \mathcal{O}_X(U)$ and $\vartheta(x) \neq 0$ for all $x \in U$, then $\vartheta \in \mathcal{O}_X(U)^\times$.

Proof. i) The property is local on U, hence it is sufficient to show it in the quasi-affine case. This was done in 4.7.93.

ii) For the second part, let $\lambda_x := \lambda \restriction_{V_x}$. We have $\lambda_x \restriction_{V_x \cap V_y} = \lambda \restriction_{V_x \cap V_y} = \lambda_y \restriction_{V_x \cap V_y}$. The V_x cover U. By the sheaf axiom for $\mathcal{O}_X$ there is $\ell \in \mathcal{O}_X(U)$ with $\ell \restriction_{V_x} = \lambda_x$. It follows that $\ell = \lambda$.

iii) By the definition of variety, every $x \in U$ has a quasi-affine neighbourhood $V \subseteq U$. We can assume U to be quasi-affine and $X = V(I) \subseteq \mathfrak{k}^n$, as the general assertion follows by an application of ii). If $x \in U$ there are a neighbourhood $x \in W \subseteq U$ and $a, b \in R = \mathfrak{k}[X_1, \dots, X_n]$ such that $\vartheta(y) = \frac{a(y)}{b(y)}$ for $y \in W$, with $b(y) \neq 0$. Then $a(x) \neq 0$ as $\vartheta(x) \neq 0$. Replacing W by $W \backslash V(a)$, we may assume that a has no zeroes on W. Then $\lambda(y) = \frac{b(y)}{a(y)}$ for $y \in W$ has a non-vanishing denominator and $\lambda \in \mathcal{O}_X(U)$. We have $\lambda \cdot \vartheta = 1$, thus $\vartheta \in \mathcal{O}_X(U)^\times$.

□

Proposition 4.20 (About affine varieties)**.**

- Let X, Y be varieties over $\mathfrak{k}$. Then the map

$$\begin{aligned} \varphi : \mathrm{Hom}_{\mathrm{Var}_{\mathfrak{k}}}(X, Y) &\longrightarrow \mathrm{Hom}_{\mathbf{Alg}_{\mathfrak{k}}}(\mathcal{O}_Y(Y), \mathcal{O}_X(X)) \\ (X \xrightarrow{f} Y) &\longmapsto (\mathcal{O}_Y(Y) \xrightarrow{f^*} \mathcal{O}_X(X)) \end{aligned}$$

  is injective when Y is quasi-affine and bijective when Y is affine.

- The contravariant functor

$$\begin{aligned} F : \mathrm{Var}_{\mathfrak{k}} &\longrightarrow \mathbf{Alg}_{\mathfrak{k}} \\ X &\longmapsto \mathcal{O}_X(X) \\ (X \xrightarrow{f} Y) &\longmapsto (\mathcal{O}_X(X) \xrightarrow{f^*} \mathcal{O}_Y(Y)) \end{aligned}$$

  restricts to an equivalence of categories between the category of affine varieties over $\mathfrak{k}$ and the full subcategory $\mathcal{A}$ of $\mathbf{Alg}_{\mathfrak{k}}$, having the $\mathfrak{k}$-algebras A of finite type with $\mathfrak{nil}\, A = \{0\}$ as objects.

Remark 4.20.97. It is clear that $\mathfrak{nil}(\mathcal{O}_X(X)) = \{0\}$ for arbitrary varieties. For general varieties it is however not true that $\mathcal{O}_X(X)$ is a $\mathfrak{k}$-algebra of finite type. There are counterexamples even for quasi-affine X.

If, however, X is affine, we may assume w.l.o.g. that $X = V(I)$ where $I = \sqrt{I} \subseteq R$ is an ideal with $R = \mathfrak{k}[X_1, \dots, X_n]$. Then $\mathcal{O}_X(X) \cong R/I$ (see 4.8) is a $\mathfrak{k}$-algebra of finite type.

Proof. It suffices to investigate φ when Y is an open subset of $V(I) \subseteq \mathfrak{k}^n$, where $I = \sqrt{I} \subseteq R$ is an ideal and $Y = V(I)$ when Y is affine. Let $(f_1, \dots, f_n)$ be the components of $X \xrightarrow{f} Y \subseteq \mathfrak{k}^n$. Let $Y \xrightarrow{\xi_i} \mathfrak{k}$ be the i-th coordinate. By definition $f_i = f^*(\xi_i)$. Thus f is uniquely determined by $\mathcal{O}_Y(Y) \xrightarrow{f^*} \mathcal{O}_X(X)$. Conversely, let $Y = V(I)$ and $\mathcal{O}_Y(Y) \xrightarrow{\varphi} \mathcal{O}_X(X)$ be a morphism of $\mathfrak{k}$-algebras.

Define $f_i := \varphi(\xi_i)$ and consider $X \xrightarrow{f=(f_1,\dots,f_n)} Y \subseteq \mathfrak{k}^n$.

Claim 1. *f has image contained in Y.*

Subproof. For $x \in X, \lambda \in I$ we have $\lambda(f(x)) = (\varphi(\lambda \mod I))(x) = 0$ as φ is a morphism of $\mathfrak{k}$-algebras. Thus $f(x) \in V(I) = Y$. ■

Claim 2. *f is a morphism in* $\mathrm{Var}_{\mathfrak{k}}$

Subproof. For open $\Omega \subseteq Y$, $U = f^{-1}(\Omega) = \{x \in X | \forall \lambda \in J\ (\varphi(\lambda))(x) \neq 0\}$ is open in X, where $Y \backslash \Omega = V(J)$. If $\lambda \in \mathcal{O}_Y(\Omega)$ and $x \in U$, then $f(x)$ has a neighbourhood V such that there are $a, b \in R$ with $\lambda(v) = \frac{a(v)}{b(v)}$ and $b(v) \neq 0$ for all $v \in V$. Let $W := f^{-1}(V)$. Then $\alpha := \varphi(a) \restriction_W \in \mathcal{O}_X(W)$, $\beta := \varphi(b) \restriction_W \in \mathcal{O}_X(W)$. By the second part of 4.19 $\beta \in \mathcal{O}_X(W)^\times$ and $f^*(\lambda) \restriction_W = \frac{\alpha}{\beta} \in \mathcal{O}_X(W)$. The first part of 4.19 shows that $f^*(\lambda) \in \mathcal{O}_X(U)$. ■

By definition of f, we have $f^* = \varphi$. This finished the proof of the first point.

Claim 3. *The functor in the second part maps affine varieties to objects of $\mathcal{A}$ and is essentially surjective.*

Subproof. It follows from the remark that the functor maps affine varieties to objects of $\mathcal{A}$.

If $A \in \mathrm{Ob}(\mathcal{A})$ then $A/\mathfrak{k}$ is of finite type, thus $A \cong R/I$ for some n. Since $\mathfrak{nil}(A) = \{0\}$ we have $I = \sqrt{I}$, as for $x \in \sqrt{I}$, $x \mod I \in \mathfrak{nil}(R/I) \cong \mathfrak{nil}(A) = \{0\}$. Thus $A \cong \mathcal{O}_X(X)$ where $X = V(I)$. ■

Fullness and faithfulness of the functor follow from the first point. □

Remark 4.20.98. Note that giving a contravariant functor $\mathcal{C} \to \mathcal{D}$ is equivalent to giving a functor $\mathcal{C} \to \mathcal{D}\mathrm{op}$. We have thus shown that the category of affine varieties is equivalent to $\mathcal{A}\mathrm{op}$, where $\mathcal{A} \subsetneq \mathbf{Alg}_{\mathfrak{k}}$ is the full subcategory of $\mathfrak{k}$-algebras A of finite type with $\mathfrak{nil}(A) = \{0\}$.

4.3.2 Affine open subsets are a topology base

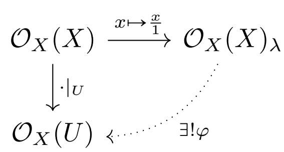
Definition 4.21. A set $\mathcal{B}$ of open subsets of a topological space X is called a **topology base** for X if every open subset of X can be written as a (possibly empty) union of elements of $\mathcal{B}$.

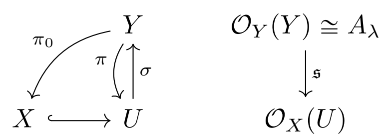
Fact 4.21.99. If X is a set, then $\mathcal{B} \subseteq \mathcal{P}(X)$ is a base for some topology on X iff $X = \bigcup_{U \in \mathcal{B}} U$ and for arbitrary $U, V \in \mathcal{B}$, $U \cap V$ is a union of elements of $\mathcal{B}$.

Definition 4.22. Let X be a variety. An **affine open subset** of X is a subset which is an affine variety.

Proposition 4.23. Let X be an affine variety over $\mathfrak{k}$, $\lambda \in \mathcal{O}_X(X)$ and $U = X \backslash V(\lambda)$. Then U is an affine variety and the morphism $\varphi : \mathcal{O}_X(X)_\lambda \to \mathcal{O}_X(U)$ defined by the restriction $\mathcal{O}_X(X) \xrightarrow{\cdot|_U} \mathcal{O}_X(U)$ and the universal property of the localization is an isomorphism.

Proof. Let X be an affine variety over $\mathfrak{k}$, $\lambda \in \mathcal{O}_X(X)$ and $U = X \backslash V(\lambda)$. The fact that $\lambda \restriction_U \in \mathcal{O}_x(U)^\times$ follows from 4.19. Thus the universal property of the localization $\mathcal{O}_X(X)_\lambda$ can be applied to $\mathcal{O}_X(X) \xrightarrow{\cdot|_U} \mathcal{O}_X(U)$.





For the rest of the proof, we may assume $X = V(I) \subseteq \mathfrak{k}^n$ where $I = \sqrt{I} \subseteq R := \mathfrak{k}[X_1, \ldots, X_n]$ is an ideal. Then $A := \mathcal{O}_X(X) \cong R/I$ and there is $\ell \in R$ such that $\ell \restriction_X = \lambda$. Let $Y = V(J) \subseteq \mathfrak{k}^{n+1}$ where $J \subseteq \mathfrak{k}[Z, X_1, \ldots, X_n]$ is generated by the elements of I and $1 - Z\ell(X_1, \ldots, X_n)$.

Then $\mathcal{O}_Y(Y) \cong \mathfrak{k}[Z, X_1, \ldots, X_n]/J \cong A[Z]/(1 - \lambda Z) \cong A_\lambda$. By the proposition about affine varieties (4.20), the morphism $\mathfrak{s} : \mathcal{O}_Y(Y) \cong A_\lambda \to \mathcal{O}_X(U)$ corresponds to a morphism $U \xrightarrow{\sigma} Y$. We have $\mathfrak{s}(Z \mod J) = \lambda^{-1}$ and $\mathfrak{s}(X_i \mod J) = X_i \mod I$. Thus $\sigma(x) = (\lambda(x)^{-1}, x)$ for $x \in U$. Moreover, the projection $Y \xrightarrow{\pi_0} X$ dropping the Z-coordinate has image contained in U, as for $(z, x) \in Y$ the equation

$$1 = z\lambda(x)$$

implies $\lambda(x) \neq 0$. It thus defines a morphism $Y \xrightarrow{\pi} U$ and by the description of σ it follows that $\sigma\pi = \mathrm{Id}_U$. Similarly it follows that $\sigma\pi = \mathrm{Id}_Y$. Thus, σ and π are inverse to each other. □

Corollary 4.24. The affine open subsets of a variety X are a topology base on X.

Proof. Let $X = V(I) \subseteq \mathfrak{k}^n$ with $I = \sqrt{I}$. If $U \subseteq X$ is open then $X \backslash U = V(J)$ with $J \supseteq I$ and $U = \bigcup_{f \in J}(X \backslash V(f))$. Thus U is a union of affine open subsets. The same then holds for arbitrary quasi-affine varieties.

Let X be any variety, $U \subseteq X$ open and $x \in U$. By the definition of variety, x has a neighbourhood V_x which is quasi-affine, and replacing V_x by $U \cap V_x$ which is also quasi-affine we may assume $V_x \subseteq U$. V_x is a union of its affine open subsets. Because U is the union of the V_x, U as well is a union of affine open subsets. □

4.4 Stalks of sheaves

Definition 4.25 (Stalk)**.** Let $\mathcal{G}$ be a presheaf of sets on the topological space X, and let $x \in X$. The **stalk** (**Halm**) of $\mathcal{G}$ at x is the set of equivalence classes of pairs (U, γ), where U is an open neighbourhood of x and $\gamma \in \mathcal{G}(U)$ and the equivalence relation $\sim$ is defined as follows: $(U, \gamma) \sim (V, \delta)$ iff there exists an open neighbourhood $W \subseteq U \cap V$ of x such that $\gamma \restriction_W = \delta \restriction_W$.

If $\mathcal{G}$ is a presheaf of groups, one can define a groups structure on $\mathcal{G}_x$ by

$$((U,\gamma)/\sim) \cdot ((V,\delta)/\sim) = (U \cap V, \gamma \restriction_{U \cap V} \cdot \delta \restriction_{U \cap V})/\sim .$$

If $\mathcal{G}$ is a presheaf of rings, one can similarly define a ring structure on $\mathcal{G}_x$.

If U is an open neighbourhood of $x \in X$, then we have a map (resp. homomorphism)

$$\begin{aligned} \cdot_x : \mathcal{G}(U) &\longrightarrow \mathcal{G}_x \\ \gamma &\longmapsto \gamma_x := (U,\gamma)/\sim \end{aligned}$$

Fact 4.25.100. Let $\gamma, \delta \in \mathcal{G}(U)$. If $\mathcal{G}$ is a sheaf[a] and if for all $x \in U$, we have $\gamma_x = \delta_x$, then $\gamma = \delta$.

In the case of a sheaf, the image of the injective map $\mathcal{G}(U) \xrightarrow{\gamma \mapsto (\gamma_x)_{x \in U}} \prod_{x \in U} \mathcal{G}_x$ is the set of all $(g_x)_{x \in U} \in \prod_{x \in U} \mathcal{G}_x$ satisfying the following **coherence condition**: For every $x \in U$, there are an open neighbourhood $W_x \subseteq U$ of x and $g^{(x)} \in \mathcal{G}(W_x)$ with $g^{(x)}_y = g_y$ for all $y \in W_x$.

[a] or, more generally, a separated presheaf

Proof. Because of $\gamma_x = \delta_x$, there is $x \in W_x \subseteq U$ open such that $\gamma \restriction_{W_x} = \delta \restriction_{W_x}$. As the W_x cover U, $\gamma = \delta$ by the sheaf axiom. □

Definition 4.26. Let $\mathcal{G}$ be a sheaf of functions. Then γ_x is called the

germ of the function γ at x. The **value at x** of $g = (U, \gamma)/\sim \in \mathcal{G}_x$ defined as $g(x) := \gamma(x)$, which is independent of the choice of the representative γ.

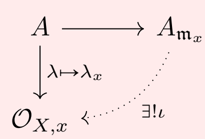
Remark 4.26.101. If $\mathcal{G}$ is a sheaf of C^∞-functions (resp. holomorphic functions), then $\mathcal{G}_x$ is called the ring of germs of C^∞-functions (resp. of holomorphic functions) at x.

4.4.1 The local ring of an affine variety

Definition 4.27. If X is a variety, the stalk $\mathcal{O}_{X,x}$ of the structure sheaf at x is called the **local ring** of X at x. This is indeed a local ring, with maximal ideal $\mathfrak{m}_x = \{f \in \mathcal{O}_{X,x} | f(x) = 0\}$.

Proof. By 2.51 it suffices to show that $\mathfrak{m}_x$ is a proper ideal, which is trivial, and that the elements of $\mathcal{O}_{X,x} \backslash \mathfrak{m}_x$ are units in $\mathcal{O}_{X,x}$. Let $g = (U, \gamma)/\sim \in \mathcal{O}_{X,x}$ and $g(x) \neq 0$. γ is Zariski continuous (first point of 4.19). Thus $V(\gamma)$ is closed. By replacing U by $U \backslash V(\gamma)$ we may assume that γ vanishes nowhere on U. By the third point of 4.19 we have $\gamma \in \mathcal{O}_X(U)^\times$. $(\gamma^{-1})_x$ is an inverse to g. □

Proposition 4.28. Let $X = V_{\mathbb{A}}(I) \subseteq \mathfrak{k}^n$ be equipped with its usual structure sheaf, where $I = \sqrt{I} \subseteq R = \mathfrak{k}[X_1, \ldots, X_n]$. Let $x \in X$ and $A = \mathcal{O}_X(X) \cong R/I$. $\{P \in R | P(x) = 0\} =: \mathfrak{n}_x \subseteq R$ is maximal, $I \subseteq \mathfrak{n}_x$ and $\mathfrak{m}_x := \mathfrak{n}_x / I$ is the maximal ideal of elements of A vanishing at x. If $\lambda \in A \backslash \mathfrak{m}_x$, we have $\lambda_x \in \mathcal{O}_{X,x}^\times$, where λ_x denotes the image under $A \cong \mathcal{O}_X(X) \to \mathcal{O}_{X,x}$. By the universal property of the localization, there exists a unique ring homomorphism $A_{\mathfrak{m}_x} \xrightarrow{\iota} \mathcal{O}_{X,x}$ such that



commutes.

The morphism $A_{\mathfrak{m}_x} \xrightarrow{\iota} \mathcal{O}_{X,x}$ is an isomorphism.

Proof. To show surjectivity, let $\ell = (U, \lambda)/\sim \in \mathcal{O}_{X,x}$, where U is an open neighbourhood of x in X. We have $X \backslash U = V(J)$ where $J \subseteq A$ is an ideal. As $x \in U$ there is $f \in J$ with $f(x) \neq 0$. Replacing U by $X \backslash V(f)$ we may assume $U = X \backslash V(f)$. By 4.23, $\mathcal{O}_X(U) \cong A_f$, and $\lambda = f^{-n}\vartheta$ for some $n \in \mathbb{N}$ and $\vartheta \in A$. Then $\ell = \iota(f^{-n}\vartheta)$ where the last fraction is taken in $A_{\mathfrak{m}_x}$.

Let $\lambda = \frac{\vartheta}{g} \in A_{\mathfrak{m}_x}$ with $\iota(\lambda) = 0$. It is easy to see that $\iota(\lambda) = (X \backslash V(g), \frac{\vartheta}{g})/\sim$. Thus there is an open neighbourhood U of x in $X \backslash V(g)$ such that ϑ vanishes on U. Similar as before there is $h \in A$ with $h(x) \neq 0$ and $W = X \backslash V(h) \subseteq U$.

By the isomorphism $\mathcal{O}_X(W) \cong A_h$, there is $n \in \mathbb{N}$ with $h^n\vartheta = 0$ in A. Since $h \notin \mathfrak{m}_x$, h is a unit and the image of ϑ in $A_{\mathfrak{m}_x}$ vanishes, implying $\lambda = 0$. □

4.4.2 Intersection multiplicities and Bezout's theorem

Definition 4.29. Let $R = \mathfrak{k}[X_0, X_1, X_2]$ equipped with its usual grading and let $x \in \mathbb{P}^2$. Let $G \in R_g, H \in R_h$ be homogeneous polynomials with $x \in V(G) \cap V(h)$. Let $\ell \in R_1$ such that $\ell(x) \neq 0$. Then $x \in U = \mathbb{P}^2 \backslash V(\ell)$ and the rational functions $\gamma = \ell^{-g}G, \eta = \ell^{-h}H$ are elements of $\mathcal{O}_{\mathbb{P}^2}(U)$. Let $I_x(G, H) \subseteq \mathcal{O}_{\mathbb{P}^2,x}$ denote the ideal generated by γ_x and η_x.

The dimension $\dim_{\mathfrak{k}}(\mathcal{O}_{X,x}/I_x(G, H)) =: i_x(G, H)$ is called the **intersection multiplicity** of G and H at x.

Remark 4.29.102. If $\tilde{\ell} \in R_1$ also satisfies $\tilde{\ell}(x) \neq 0$, then the image of $\tilde{\ell}/\ell$ under $\mathcal{O}_{\mathbb{P}^2}(U) \to \mathcal{O}_{\mathbb{P}^2,x}$ is a unit, showing that the image of $\tilde{\gamma} = \tilde{\ell}^{-g}G$ in $\mathcal{O}_{\mathbb{P}^2,x}$ is multiplicatively equivalent to γ_x, and similarly for η_x. Thus $I_x(G, H)$ does not depend on the choice of $\ell \in R_1$ with $\ell(x) \neq 0$.

Theorem 4.30 (Bezout's theorem)**.** In the above situation, assume that $V(H)$ and $V(G)$ intersect properly in the sense that $V(G) \cap V(H) \subseteq \mathbb{P}^2$ has no irreducible component of dimension $\geqslant 1$. Then

$$\sum_{x \in V(G) \cap V(H)} i_x(G, H) = gh.$$

Thus, $V(G) \cap V(H)$ has gh elements counted by multiplicity.

Index