Algebra I

Nicholas Schwab

Sommersemester 2017

Contents

1. The Hilbert Basis- and Nullstellensatz

1.1. Noetherian Rings

Definition 1. Let R be a ring, and $f_1, \dots, f_n \in R$, then the *ideal generated by the* f_i is

$$(f_1, \dots, f_n)_R = \left\{ \sum \lambda_i f_i \;\middle|\; \lambda_i \in R \right\} = \bigcap_{f_1,\dots,f_n \in I \text{ ideal}} I \, .$$

The f_i are called a *basis* or *generators* of I.

Remark 1. If I is not necessarily finite,

$$(f_i \mid i \in I)_R = \left\{ \sum_{i \in I} \lambda_i f_i \;\middle|\; \lambda_i = 0 \text{ for all but finitely many } i \right\} = \bigcap_{(f_i)_{i \in I} \subseteq I} I \ .$$

Definition 2. Let k be a field, $I \subseteq k[X_1, \ldots, X_n]$ an ideal, ℓ a field extension of k. Call $x \in \ell^n$ a *zero* of I iff $f(x_1, \ldots, x_n) = 0$ for all $f \in I$.

Remark 2. An element x is a common zero of the $f_i \in k[X_1, \ldots, X_n]$ iff it is a zero of the ideal generated by the f_i.

Proposition 1. *For a ring R the following conditions are equivalent:*

(a) *Every ideal has a finite set of generators (i.e. is finitely generated).*

(b) *Every ascending chain $I_0 \subseteq I_1 \subseteq \ldots$ of ideals in R terminates after finitely many steps, i.e. there is some $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.*

(c) *Every non-empty set $\mathfrak{M}$ of ideals in R has an $\subseteq$-maximal element I.*

Definition 3. A ring with these properties is called *Noetherian*.

Example 1. Fields and principal ideal domains are Noetherian.

Theorem 1 (Hilbert's Basissatz)**.** *If R is Noetherian, so is $R[X_1, \ldots, X_n]$.*

Corollary 1 (of the Basissatz)**.** *Every polynomial system of equations in finitely many variables over a field has finite subsystem with the same set of solutions.*

Theorem 2 (Hilbert's Nullstellensatz)**.** *Let k be a algebraically closed field and I be a proper ideal of $k[X_1, \ldots, X_n]$. Then I has a zero $x \in k^n$.*

Both Hilbert's Nullstellensatz and Hilbert's Basissatz will be proved later on.

1.2. Modules over rings

Definition 1. An R-Module (where R is a ring) is an abelian group $(M, +)$ with an operation

$$\cdot : R \times M \longrightarrow M \ , \quad (r, m) \longmapsto r \cdot m$$

such that for all $r, s \in R$ and $m, n \in M$

$$r \cdot (s \cdot m) = (r \cdot s) \cdot m \qquad (r + s) \cdot m = r \cdot m + s \cdot m$$
$$1 \cdot m = m \qquad r \cdot (m + n) = r \cdot m + r \cdot n \ .$$

A *morphism* of R-Modules is a map $M \xrightarrow{f} N$ which is a homomorphism of abelian groups compatible with $\cdot$. A *submodule* of M is a subgroup $X \subseteq M$ of $(M, +)$ such that $R \cdot X \subseteq X$.

Example 1. The R-submodules of R are the ideals in R.

Proposition 1. *If $N \subseteq M$ is a R-submodule of the R-module M the quotient group M/N has a unique structure of an R-submodule such that the projection $M \xrightarrow{\pi} M/N$ is a morphism of R-modules, and for arbitrary R-modules T the map*

$$\begin{aligned} \mathrm{Hom}_R(M/N, T) &\longrightarrow \{\tau \in \mathrm{Hom}_R(M,T) \mid \tau|_N = 0\} \\ t &\longmapsto \tau = t \circ \pi \end{aligned}$$

is bijective, where t is surjective iff τ is and t is injective iff $\ker(\tau)$ equals N.

Corollary 1. *Let $N, L \subseteq M$ be submodules of some R-Module M.*

(a) *There is a unique isomorphism $L/(N \cap L) \xrightarrow{\sim} (N+L)/N$ such that the following diagram commutes:*

$$\begin{array}{ccc} L & \hookrightarrow & N+L \\ {\scriptstyle \pi_{L/(N\cap L)}}\downarrow & & \downarrow{\scriptstyle \pi_{(N+L)/N}} \\ L/(N\cap L) & \overset{\sim}{\dashrightarrow} & (N+L)/N \end{array}$$

(b) *If further $L \subseteq N$, there is a unique isomorphism $M/N \xrightarrow{\sim} (M/L)/(N/L)$ such that the following diagram commutes:*

$$\begin{array}{ccc} M & \xrightarrow{\pi_{M/L}} & M/L \\ {\scriptstyle \pi_{M/N}}\downarrow & & \downarrow{\scriptstyle \pi_{(M/L)/(N/L)}} \\ M/N & \overset{\sim}{\dashrightarrow} & (M/L)/(N/L) \end{array}$$

Definition 2. If M and N are R-modules, $M \oplus N = M \times N$ equipped with component-by-component addition and scalar multiplication. This can be generalized to finitely many summands.

Example 2. $R^n = \{(r_i)_{i=1}^n \mid r_i \in R\}$ is an R-module.

Definition 3. If M is an R-module and $m_1, \ldots, m_k \in M$, then the *submodule generated by* $\{m_1, \ldots, m_k\}$ *is*

$$\langle m_1, \ldots, m_k \rangle_R = Rm_1 + \ldots + Rm_k = \left\{ \sum r_i \cdot m_i \;\middle|\; r_i \in R \right\} = \bigcap_{m_1,\ldots,m_k \in X \text{ submodule}} X \,.$$

As was the case for Definition 1.1.1, this can be generalized to infinitely many generators. M is *finitely generated* iff there are $m_1, \ldots, m_k \in M$ such that the submodules of M generated by the m_i equals M.

Proposition 2. *Consider an exact sequence*

$$0 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 0$$

of R-modules.

(a) *If M is finitely generated, then so is L.*

(b) *If N and L are finitely generated, then so is M.*

Corollary 2. *$M \oplus N$ is finitely generated iff M and N are.*

Proposition 3. *Let M be an R-module. The following properties are equivalent:*

(a) *Every submodule $N \subseteq M$ of M is finitely generated.*

(b) *Every ascending sequence $N_0 \subseteq N_1 \subseteq \ldots$ of submodules of N terminates.*

(c) *Every non-empty set $\mathfrak{M}$ of R-submodules of M has a $\subseteq$-maximal element.*

Proof. (a) $\rightarrow$ (b) Let $N_\infty = \bigcup_{i=0}^{\infty} N_i$, then this is a submodule, hence finitely generated by a). Let $n_1, \ldots, n_k$ generate N_∞. Choose ℓ_i such that $n_i \in N_{\ell_i}$ and let $\ell = \max_{i \leq k} \ell_i$, then $N_\ell = N_\infty$.

(b) $\rightarrow$ (c) From (b) we conclude, that in the $\subseteq$-ordered set $\mathfrak{M}$ every ascending chain has an upper bound in $\mathfrak{M}$, namely the ideal, that terminates the chain. Therefore by Zorn's Lemma there is $\subseteq$-maximal element in $\mathfrak{M}$.

(c) $\rightarrow$ (a) Let $\mathfrak{M}$ be the set of finitely generated submodules of N. Since $\{0\} \subseteq N$ is a module, this set is not empty. Therefore there is a $\subseteq$-maximal submodule P in $\mathfrak{M}$ generated by $p_1, \ldots, p_n$. Therefore there is no $f \in N \setminus P$ such that $\langle p_1, \ldots, p_n, f \rangle_R$ is a submodule of N since this would be a superset of P. Hence we have $N = P$ is finitely generated.

q.e.d.

Definition 4. A module over a ring R is *Noetherian* iff the equivalent conditions above are fulfilled.

Remark 1. Sub- and quotient modules of Noetherian rings are Noetherian. If N is a submodule of M and if N and M/N are Noetherian, then M is Noetherian.

Proof. The first assertion follows easily from Proposition 2 and the characterization of *Noetherian modules* by Proposition 3(a). For the second assertion let N and M/N be Noetherian and $X \subseteq M$ be a submodule. Since both $(X \cap N) \subseteq N$ and $X/(X \cap N) \simeq (X + N)/N \subseteq M/N$ are finitely generated as submodules of N, M/N respectively, we obtain the exact sequence

$$0 \longrightarrow X \cap N \longrightarrow X \longrightarrow X/(X \cap N) \longrightarrow 0 \,,$$

proving that X is finitely generated by Proposition 2. *q.e.d.*

Remark 2. Any Noetherian module is finitely generated.

Proposition 4. *Let R be a Noetherian ring. Then any finitely generated R-module is Noetherian.*

Proof. We proceed by induction on the number of generators of M. The case of only one generator is immediate. Now let $M = Rm_1 + \ldots + Rm_k$ and any Ry -module with less than k generators be Noetherian. In particular, $N = Rm_1 + \ldots + Rm_{k-1}$ is Noetherian. The map $R \rightarrow M/N$ sending $r \in R$ to $rm_k + N$ is surjective, hence M/N is isomorphic to some quotient of R and thus Noetherian by Remark 1. Then, again by Remark 1, M is Noetherian. *q.e.d.*

Definition 5. For a module M over a ring R, define

$$\mathrm{Ann}(M) = \{r \in R \mid r \cdot M = \{0\}\} = \{r \in R \mid r \cdot m = 0 \ \forall m \in M\} \,.$$

It is called the *annihilator* or *annulator* of M.

Proposition 5. *A module M over a ring R is Noetherian iff it is finitely generated and $R/\operatorname{Ann}(M)$ is a Noetherian ring.*

1.3. Proof of the Hilbert basis theorem

Proof. Let R be a Noetherian ring and $I \subseteq R[T]$ be an ideal. Let $R[T]_{\leq n}$ be the set of polynomials over R of degree smaller or equal to n. This is isomorphic to R^{n+1} ($1, \ldots, T^n$ being free generators) as R-modules, thus Noetherian (Proposition 1.2.4) which implies that $I_{\leq n} = I \cap R[T]_{\leq n}$ is a finitely generated R-module. Let I_n be the set of all $a_n \in R$, such that $a_0 + a_1 T + \ldots + a_n T^n \in I$ for some $a_0, \ldots, a_{n-1} \in R\}$. This is an ideal ($R$-submodule) of R, being the image of $I_{\leq n} \to R$ sending $a_0 + a_+ \ldots + a_n T^n \in I_{\leq n}$ to a_n. We have $I_n \subseteq I_{n+1}$ as $T \cdot I_{\leq n} \subseteq I_{\leq n+1}$. As R is Noetherian, this chain terminates at some $N \in \mathbb{N}$ with $I_n = I_N$ for $n \geq N$. Let $f_1, \ldots, f_k$ be generators of $I_{\leq N}$ as an R-module. We claim that they generate I as an $R[T]$-module. Since they generate $I_{\leq N}$ as an R-module, their N-th coefficients $f_N^{(i)}$, where $i \leq k$, generate $I_n = I_N$, for $n \geq N$, as an R-module.

We show by induction on n, that any $g \in I_{\leq n}$ belongs to $(f_1, \ldots, f_k)_{R[T]}$, thus establishing $I = (f_1, \ldots, f_k)_{R[T]}$. For $n \leq k$ we have $g \in I_{\leq N}$ and the assertion is obvious. Let $n > N$ let the assertion be valid for all $h \in I_{\leq n-1}$. Let $g = \sum_{i=1}^{n} g_i T^i$, $g_n = \sum_{i=1}^{k} \gamma_i f_N^{(i)}$ and $h = g - \sum_{i=1}^{k} \gamma_i T^{n-N} f_i$, then $h \in I_{\leq n-1}$ as the coefficient of T^n cancels. Thus, $h = \sum_{i=1}^{k} \rho_i f_i$ with $\rho_i \in R[T]$ by the induction assumption and

$$g = \sum_{i=1}^{k} (\gamma_i T^{n-k} + \rho_i) f_i \in (f_1, \ldots, f_k)_{R[T]}$$

as claimed. This shows that I is finitely $R[T]$-generated, hence $R[T]$ is Noetherian. *q.e.d.*

Corollary 1. *If R is a Noetherian ring, so is $R[X_1, \ldots, X_n]$ for all $n \in \mathbb{N}$.*

1.4. Finiteness properties of R-algebras

Definition 1. Let R be a ring. An *R-algebra* is a ring A (commutative, with 1) together with a ring homomorphism $R \xrightarrow{\alpha} A$. Then A becomes an R-module via $r \cdot a \coloneqq \alpha(r) \cdot a$. We call A *finite over R* (or *finite as an R-algebra*) if it is finitely generated as an R-module. We call A of *finite type over R* if it is finitely generated as an R-algebra in the sense that there are $f_1, \ldots, f_k \in A$, $k \in \mathbb{N}$, such that any R-subalgebra $B \subseteq A$ (i.e. any subring $B \subseteq A$ which is also a R-submodule, or, equivalently, a subring containing the image of α) containing the f_i must equal A.

Remark 1. If A is an R-algebra and $f_1, \ldots, f_k \in A$, the following subsets of A coincide:

- $\left\{ \sum_{\alpha \in \mathbb{N}_0^k} r_\alpha f_1^{\alpha_1} \cdot \ldots \cdot f_k^{\alpha_k} \;\middle|\; r_\alpha \in R, r_\alpha \neq 0 \text{ only for finitely many } \alpha \right\}$
- The image of the ring homomorphism $R[X_1, \ldots, X_k] \to A$ sending $p \in R[X_1, \ldots, X_k]$ to $p(f_1, \ldots, f_k)$.

- The intersection of all R-subalgebras of A containing the f_i.

Thus, an R-algebra A is of finite type iff it is isomorphic to a quotient of $R[X_1, \ldots, X_k]$ by some ideal I for finite k.

Remark 2. (a) Obviously, if $f_1, \ldots, f_i \in A$ generate A as an R-module, they generate it as an R-algebra. Thus any finite R-algebra is of finite type. On the other side, when $R \neq \{0\}$ and and $n > 0$, $R[X_1, \ldots, X_n]$ is an R-algebra of finite type that is not finitely generated as an R-module.

(b) Obviously, if L/K is a field extension then L is a finite K-algebra iff the field extension is finite. The fact that this still holds if L is a K-algebra of finite type turns out to be essentially equivalent to the Nullstellensatz.

Proposition 1. *Let R be a ring, A an R-algebra. Any A-algebra B becomes an R-algebra via the composition $R \to A \to B$.*

(a) *If A is finite over R, it is of finite type over R.*

(b) *(transitivity of finiteness) If B is finite over A and A finite over R, then B is finite over R.*

(c) *If B over A and A over R are of finite type, then B is of finite type over R.*

(d) *An algebra of finite type over a Noetherian ring is a Noetherian ring.*

Proof. (a) Trivial.

(b) If $b_1, \ldots, b_m$ generate B as an A-module and $a_1, \ldots, a_n$ generate A as an R-module, the $\beta_{i,j} = a_j \cdot b_i$ generate B as an R-module: Indeed, let $b \in B$, then $b = \sum_{i=1}^m \alpha_i b_i$ (with $\alpha_i \in A$) and each α_i can be written as $\alpha_i = \sum_{j=1}^n r_{i,j} a_j$. Then $b = \sum_{i=1}^m \sum_{j=1}^n r_{i,j} \beta_{i,j}$.

(c) By Remark 1, we obtain surjective homomorphisms $A[Y_1, \ldots, Y_m] \xrightarrow{\beta} B$ (as A-algebras, hence also as R-algebras) and $R[X_1, \ldots, X_n] \xrightarrow{\alpha} A$ (as R-algebras). Lifting the latter to a surjective homomorphism $R[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \to A[Y_1, \ldots, Y_m]$ and composing them provides us with a surjective homomorphism

$$R[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \longrightarrow B \ ,$$

proving that B is of finite type over R. In particular, if $b_1, \ldots, b_m$ generate B as an A-algebra and $a_1, \ldots, a_n$ generate A as an R-algebra, then B is generated by $a_1, \ldots, a_n, b_1, \ldots, b_m$ as an R-algebra.

(d) Note that the quotient of a Noetherian ring by an ideal stays Noetherian: The preimage of an infinitely ascending chain of ideals of the quotient ring would be an infinitely ascending chain of ideals of the original ring. Now if $a_1, \ldots, a_m \in A$ generate A as an R-algebra, then

$$\begin{aligned} R[X_1, \ldots, X_m] &\longrightarrow A \\ p &\longmapsto p(a_1, \ldots, a_m) \end{aligned}$$

is surjective and A is isomorphic to a quotient of $R[X_1, \ldots, X_m]$, which by the Basissatz is Noetherian if R is.

q.e.d.

Proposition 2 (Artin-Tate)**.** *Let R be a Noetherian ring, A an R-algebra of finite type and $B \subseteq A$ an R-subalgebra such that A is finite over B. Then B is an R-algebra of finite type.*

Proof. Let $a_1, \ldots, a_m$ generate A as an R-algebra and let $\alpha_1, \ldots, \alpha_n$ generate it as a B-module. We have expressions

$$a_i = \sum_{j=1}^{n} b_{i,j}\alpha_j \quad \text{and} \quad \alpha_k \cdot \alpha_k = \sum_{j=1}^{n} \beta_{j,k,l}\alpha_j \ . \tag{$*$}$$

Let $\widetilde{B} \subseteq B$ be the R-algebra generated by the $b_{i,j}$ and the $\beta_{j,k,l}$. It is of finite type over R thus Noetherian by Proposition 1(d). Let $\widetilde{A} \subseteq A$ be the $\widetilde{B}$-submodule generated by $\alpha_1, \ldots, \alpha_n$. Note that by $(*)$, $\widetilde{A}$ is a subring and contains the a_i, hence $\widetilde{A}$ is an R-algebra because $\widetilde{B}$ is. Then $\widetilde{A} = A$ and A is finite over $\widetilde{B}$, hence so is it's $\widetilde{B}$-submodule $B \subseteq A$ ($\widetilde{B}$ being Noetherian). Therefore B is of finite type over $\widetilde{B}$ (Proposition 1(a)) and thus also over R (Proposition 1(c)). *q.e.d.*

Proposition 3 (Eakin-Nagata)**.** *Let A be a Noetherian ring and $B \subseteq A$ be a subring such that A is finite over B. Then B is Noetherian.*

Remark 3. See Matsumura, CRT, for Eakin-Nagata.

1.5. The notion of integrity and the Noether Normalization Theorem

Remark of the author: It's called integrity not entireness ...

Definition 1. Let $A \subseteq B$ be a ring extension. We call $b \in B$ *integral* over A if it satisfies an equation

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$$

with $a_0, \ldots, a_{n-1} \in A$. We call B over A *integral*, if every element of B is integral.

Remark 1. It is not really necessary to assume $A \to B$ to be injective.

Proposition 1. (a) *An element $b \in B$ is integral over A iff there is an intermediate ring $A \subseteq C \subseteq B$ containing b which is finite over A. If $b_1, \ldots, b_n$ are finitely many integral elements of B, there is an A-subalgebra $A \subseteq C \subseteq B$ containing all b_i which is finite over A.*

(b) *The elements of B which are integral over A form a subring of B, the* integral closure *of A in B.*

(c) *If C/B and B/A are integral, so is C/A.*

(d) *Let B/A be integral (where it is essential that A is a subring of B). If B is a field, then so is A.*

Proof. (*a*) Let $b_1, \ldots, b_n$ be integral over A. Each b_i satisfies an equation

$$b_j^{d_i} = \sum_{i=0}^{d_i-1} a_{i,j} b_j^i \quad \text{where } a_{i,j} \in A \, .$$

Then the subring $C = A[b_1, \ldots, b_n]$ is generated by all $b_1^{k_1} \cdots b_n^{k_n}$ where $0 \leq k_i < d_i$, hence it is finite over A. The first assertion of (a) follows as a special case.

For the other direction let $C \subseteq B$ be an A-subalgebra which is finitely generated as an A-module, say, by $\gamma_1, \ldots, \gamma_n$. Let $b \in C$ and choose $m_{i,j} \in A$ such that

$$b\gamma_j = \sum_{i=1}^{n} m_{i,j} \gamma_j \, .$$

The matrix $M = (m_{i,j})_{i,j=1}^n$ satisfies its own characteristic equation by Cayley-Hamilton theorem: $M^n = p_0 + p_1 M + \ldots + p_{n-1} M^{n-1}$ for suitable $p_0, \ldots, p_{n-1} \in A$. Since b^j in C can be expressed by M^j (in the sense that

$$\begin{array}{ccccc} (a_1, \ldots, a_n) & & A^n & \xrightarrow{M^j \cdot} & A^n \\ \big\downarrow & & \gamma \big\downarrow & & \big\downarrow \gamma \\ \sum a_i \gamma_i & & C & \xrightarrow{\cdot b^j} & C \end{array} \qquad (a_1, \ldots, a_n) \big\downarrow \; \sum a_i \gamma_i$$

commutes) it follows, that $b^n \cdot c = p_0 c + p_1 bc + \ldots + p_{n-1} b^{n-1} c$ (first for $c = \gamma_i$, then all $c \in C$). Taking $c = 1$ shows that b is indeed integral over A.

(*b*) If C is as in A and contains b_1, b_2, then it contains $b_1 \pm b_2$ and $b_1 \cdot b_2$, showing that these are integral over A.

(*c*) Let, more generally, B/A be integral and $c \in C$ integral over B. It satisfies an equation $c^d = \beta_0 + \beta_1 c + \ldots + \beta_{d-1} c^{d-1}$ with $\beta_i \in B$. By (a), there is an A-subalgebra $\mathfrak{B} \subseteq B$ which is finite over A and contains the β_i. Then c is integral over $\mathfrak{B}$, hence by (a) there is a $\mathfrak{B}$-subalgebra $\mathfrak{C} \subseteq C$ containing c and finite over $\mathfrak{B}$. Now $\mathfrak{C}/A$ is finite by Proposition 1.4.1(b), hence c is integral over A by (a).

(*d*) Suppose that B is a field and let $a \in A \setminus \{0\}$. Since B/A is integral, we can find $\alpha_0, \ldots, \alpha_{n-1} \in A$ such that

$$\left(a^{-1}\right)^n + \sum_{i=0}^{n-1} \alpha_i \cdot \left(a^{-1}\right)^i = 0 \, .$$

But then

$$a^{-1} = a^{n-1} \left(a^{-1}\right)^n = -\sum_{i=0}^{n-1} \alpha_i \cdot a^{n-1} \in A \, .$$

So every element of $A \setminus \{0\}$ is an unit and A a field.

q.e.d.

Remark 2. Cayley-Hamilton (similar to other determinant identities) can be derived from the case of algebraically closed fields by embedding integer domains into the algebraic closures of their quotient fields. Fir arbitrary rings R (possibly with zero divisors) one may consider the surjective ring homomorphism

$$\begin{aligned} \mathbb{Z}[X_r : r \in R] &\longrightarrow R \\ X_r &\longmapsto r \end{aligned}$$

and then reduce to the case of integer domains which was done above.

Corollary 1. *A ring extension is finite iff it is integral and of finite type.*

Remark 3. Algebraic independence over k means that

$$\sum_{\alpha \in \mathbb{N}_0^n} \lambda_{\alpha_1,\ldots,\alpha_n} a_1^{\alpha_1} \cdot \ldots \cdot a_n^{\alpha_n} = 0$$

implies that each $\lambda_{\alpha_1,\ldots,\alpha_n} = 0$. Equivalently, the ring homomorphism

$$\begin{aligned} k[X_1, \ldots, X_n] &\longrightarrow k[a_1, \ldots, a_n] \\ X_i &\longmapsto a_i \end{aligned}$$

is injective, hence $k[X_1, \ldots, X_n] \simeq k[a_1, \ldots, a_n]$ as k-algebras.

Theorem 3 (Noether Normalization Theorem)**.** *Let k be a field, A a k-algebra of finite type over k. Then there are over k algebraically independent $a_1, \ldots, a_n \in A$ such that $A/k[a_1, \ldots, a_n]$ is integral.*

Proof. Since A is of finite type over k, we can choose $a_1, \ldots, a_n$ such that A is integral over $k[a_1, \ldots, a_n]$ (e.g. choose the a_i as generators of A as a k-algebra). We may choose a minimal n such that this is possible. We claim

> Let $x_1, \ldots, x_n \in A$ such that A is integral over $k[x_1, \ldots, x_n]$ and n is minimal having this property that such x_i exist. Then the x_i are algebraically independent over k.

We write $x^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$ for short. Suppose that

$$\sum_{\alpha \in \mathbb{N}_0^n} \lambda_\alpha \cdot x^\alpha = 0 \tag{$*$}$$

where

$$S \coloneqq \{\alpha \in \mathbb{N}_0^n \mid \lambda_\alpha \neq 0\}$$

is finite but not empty. Let $y_1 = x_1$ and $y_k = x_k + y_1^{d_k}$ (the d_i will be chosen later on). Since the x_i can be recovered from the y_i, we have $k[x_1, \ldots, x_n] = k[y_1, \ldots, y_n]$. The idea is to choose the d_i such that y_1 is integral over $k[y_2, \ldots, y_n]$. Then A is integral over $k[y_2, \ldots, y_n]$, contradicting the minimality of n.

Let $\omega_d(\alpha) = \alpha_1 + \sum_{i=2}^n d_i \cdot \alpha_i$. The summands can be expressed as

$$\lambda_\alpha x^\alpha = \lambda_\alpha y_1^{\alpha_1} \cdot \prod_{i=2}^n \left(y_i - y_1^{d_i}\right)^{\alpha_i} = \pm \lambda_\alpha y_1^{\omega_d(\alpha)} + \sum_{j=0}^{\omega_d(\alpha)-1} Q_{\alpha,j}(y_2, \ldots, y_n) y_1^j$$

if all d_k are positive. Here $Q_{\alpha,j}$ denotes some polynomial.

If $d_2, \ldots, d_n$ can be chosen in such a way that $\omega_d : S \to \mathbb{N}$ has a unique maximum $\alpha^* \in S$, the relation $(*)$ becomes

$$0 = \lambda_{\alpha^*} y_1^{\omega_d(\alpha^*)} + \sum_{j=0}^{\omega_d(\alpha^*)-1} Q_j(y_2, \ldots, y_n) y_1^j ,$$

proving that y_1 is integral over $k[y_2, \ldots, y_n]$.

To obtain this, $d_2, \ldots, d_n$ can be chosen in several ways. For example, take

$$A = \max \{l \in \mathbb{N} \mid \text{ there is } \alpha \in S \text{ such that } l = \alpha_i \text{ for some } i\}$$

and chose $d_i = (A+1)^{i-1}$. Then ω_d is injective since the $(A+1)$-adic representation of an integer is unique. *q.e.d.*

1.6. Proof of the Nullstellensatz and some consequences

Theorem 4. *Let L/K be a field extension such that L is a K-algebra of finite type. Then L/K is finite.*

Proof. By Noether's Normalization Theorem (Theorem 3) there are $y_1, \ldots, y_n \in L$ algebraically independent over K such that L is integral over $K[y_1, \ldots, y_n]$. By Proposition 1.5.1(d), $K[y_1, \ldots, y_n]$ is a field. But as $y_1, \ldots, y_n$ are algebraically independent, $K[y_1, \ldots, y_n]$ is isomorphic to the polynomial ring $K[X_1, \ldots, X_n]$, which is only a field for $n = 0$. Thus L/K is integral (i.e. algebraic) and since the extension is finitely generated it must be finite. *q.e.d.*

Remark 1. When K is uncountable and $\lambda \in L$ non-algebraic over K, the subfield $K(\lambda)$ is isomorphic to $K(X)$, the field of rational functions over K, which has uncountable dimension as a K-vector space as the $\frac{1}{X-\gamma}$, $\gamma \in K$, are linearly independent. But the dimension (as a K-vector space) of a K-algebra must be countable, as there are only countable many monomials in finitely many elements.

Corollary 1. *Let k be a field and let $\mathfrak{m} \subseteq k[X_1, \ldots, X_n]$ a maximal ideal, then it's residue field $k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite field extension of k.*

Proof. Indeed, it is generated by $X_1 + \mathfrak{m}, \ldots, X_n + \mathfrak{m}$ and thus finite over k. *q.e.d.*

Remark 2. In particular, it L/K is algebraic and $L = K$ if L is algebraically closed.

Remark 3.

- A ring R is a *domain* if $0 \neq 1$ and from $a \cdot b = 0$ follows $a = 0$ or $b = 0$.
- A field is a domain in which every $x \neq 0$ is invertible.
- An ideal $\mathfrak{p} \subseteq R$ is a *prime ideal*, iff $1 \notin \mathfrak{p}$ and $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. This is equivalent to $R/\mathfrak{p}$ being a domain.

  It is *maximal* if $\mathfrak{p} \subsetneq R$ and there is not ideal I with $\mathfrak{p} \subsetneq I \subsetneq R$. This is equivalent to $R/\mathfrak{p}$ being a field.

- An element $p \in R$ of a domain is called *prime* if $p \neq 0$ and $p \cdot R$ is a prime ideal.

  It is called *irreducible* if $p \notin R^\times$ and $p = ab$ implies $a \in R^\times$ or $b \in R^\times$.

Theorem 4a (Hilbert's Nullstellensatz)**.** *If $I \subsetneq k[X_1, \ldots, X_n]$ is a proper ideal in the polynomial ring over a field, it has a zero in l^n where l/k is some finite field extension. In particular, when k is algebraically closed, it has a zero in k^n.*

Proof. Let $\mathfrak{m} \supseteq I$ be a maximal ideal of $R = k[X_1, \ldots, X_n]$ and $l = R/\mathfrak{m}$. It is finite because of Corollary 1. Let $x_i \in l$ be the image of $X_i \in R$ under $R \longrightarrow R/\mathfrak{m}$. Then $(x_1, \ldots, x_n)$ is a zero of I in l^n. *q.e.d.*

Proposition 1. *If k is algebraically closed, there is a bijection between k^n and maximal ideals $\mathfrak{m} \subset R \coloneqq k[X_1, \ldots, X_n]$*

$$\begin{aligned} x \in k^n &\longmapsto \mathfrak{m}_x = \{f \in R \mid f(x) = 0\} \\ \text{the only zero of } \mathfrak{m} &\longmapsfrom \mathfrak{m} \end{aligned}$$

Proof. Obviously, $\mathfrak{m}_x$ is an ideal and

$$\begin{aligned} R/\mathfrak{m}_x &\longrightarrow k \\ (f \mod \mathfrak{m}_x) &\longmapsto f(x) \end{aligned}$$

is an isomorphism. Thus $R/\mathfrak{m}_x$ is a field and $\mathfrak{m}_x$ is a maximal ideal. Moreover x is the only zero of $\mathfrak{m}_x$: If ξ is a different zero (say $\xi_i \neq x_i$), then $f(\xi) \neq 0$ for $f(X) = X_i - x_i$.

Let $\mathfrak{m}$ be any maximal ideal and x a zero of $\mathfrak{m}$, then $\mathfrak{m} \subseteq \mathfrak{m}_x$, hence $\mathfrak{m} = \mathfrak{m}_x$ by its maximality. By the previous remark x is the only zero of $\mathfrak{m}$. *q.e.d.*

Remark 4. (*a*) If $k \neq \overline{k}$, the bijection is between $\mathrm{Aut}(\overline{k}/k)$-orbits on $\overline{k}^n$ and maximal ideals in $R = k[X_1, \ldots, X_n]$. If k has no separable extensions (i.e., k is *separably closed*, $k = k^{\mathrm{sep}}$), then the bijection is between $\overline{k}^n$ and $\mathfrak{m}$-Spec(R), the set of maximal ideals of R.

(*b*) For arbitrary R, Grothendieck takes arbitrary prime ideals (which the lecturer thinks was also proposed by Krull, who, however, was a *n00b* compared to Grothendieck) and turns Spec R, the set of prime ideals of R, into a geometric object.

1.7. Some operations on ideals

Definition 1. For $k = \overline{k}$ and $I \subseteq R = k[X_1, \ldots, X_n]$ we denote the of zeros of I by $V(I)$ called the *variety* of I. If $I = (f_1, \ldots, f_k)_R$ we write $V(f_1, \ldots, f_k)$ for $V(I)$.

Remark 1. By definition, $I \supseteq J$ implies $V(I) \subseteq V(J)$.

Definition 2. For ideals I, J of R let $I + J = \{f + g \mid f \in I, g \in J\}$. Here, R may be any ring.

Remark 2. For $R = k[X_1, \ldots, X_n]$ we have $V(I + J) = V(I) \cap V(J)$.

Definition 3. We can sum arbitrary many ideals $I_\lambda \in R$:

$$\sum_{\lambda\in\Lambda} I_\lambda = \left\{ \sum_{\lambda\in\Lambda} i_\lambda \;\middle|\; i_\lambda \neq 0 \text{ only for finitely many } \lambda \right\} .$$

Remark 3. If $R = k[X_1, \ldots, X_n]$ then

$$V\left(\sum_{\lambda\in\Lambda} I_\lambda\right) = \bigcap_{\lambda\in\Lambda} V(I_\lambda) .$$

Definition 4. For any ideals $I, J \subseteq R$ of some ring R, their *product* is defined as

$$I \cdot J = \left\{ \sum_{k=1}^{n} f_k \cdot g_k \;\middle|\; f_k \in I, g_k \in J \right\} .$$

Remark 4. If $R = k[X_1, \ldots, X_n]$ then $V(I \cdot J) = V(I \cap J) = V(I) \cup V(J)$.

Proof. By Remark 1

$$V(I \cdot J) \supseteq V(I \cap J) \supseteq V(I) .$$

Thus

$$V(I) \cap V(J) \subseteq V(I \cap J) \subseteq V(I \cdot J)$$

and the latter is $\subseteq V(I) \cup V(J)$, implying equality. Indeed, let $x \in k^n \setminus (V(I) \cup V(J))$. Then there are are $f \in I$, $g \in J$ with $f(x) \neq 0$ and $g(x) \neq 0$. Then $f \cdot g \in (I \cdot J)$ and $(f \cdot g)(x) \neq 0$. *q.e.d.*

Remark 5. For infinite intersections the inclusion

$$\bigcup_{\lambda\in\Lambda} V(I_\lambda) \subseteq V\left(\bigcap_{\lambda\in\Lambda} I_\lambda\right)$$

may be proper.

Definition 5. If $I \subset R$ is an ideal of the ring R, it's *radical* is the ideal

$$\sqrt{I} = \{f \in R \mid f^n \in I \text{ for some } n \in \mathbb{N}\} = \{f \in R \mid \text{the image of } f \text{ in } R/I \text{ is nilpotent } \} .$$

Remark. (*a*) The set $\sqrt{\{0\}}$ of the nilpotent elements of R is called the *nil-radical* of R.

(*b*) If $f \in \sqrt{I}$, $g \in \sqrt{I}$ then $f^k \in I$ and $g^l \in I$ for $k, l \in \mathbb{N}$ then

$$(f+g)^{k+l} = \sum_{i+j=k+l} \binom{k+l}{i} f^i \cdot g^j \in I ,$$

from which it can be easily deduced that $\sqrt{I}$ is indeed an ideal again.

(*c*) $\sqrt{\sqrt{I}} = \sqrt{I}$

Proposition 1. *If k is algebraically closed and I an ideal in $R = k[X_1, \ldots, X_n]$ then $\sqrt{I} = \{f \in R \mid f(x) = 0$ for all $x \in V(I)\}$.*

Proof. Is is clear that an element of $\sqrt{I}$ must vanish at all zeros of I. Conversely, let f vanish on $V(I)$. Consider the ideal $J \subseteq S = k[X_1, \ldots, X_n, T]$ generated by the elements of I and by

$$g(X_1, \ldots, X_n, T) = 1 - T \cdot f(X_1, \ldots, X_n) \, .$$

If $(x,t) = (x_1, \ldots, x_n, t)$ was a zero of J, x would be a zero of I, thus $f(x) = 0$, thus $g(x,t) = 1 - t \cdot f(x) = 1 \neq 0$, a contradiction. By the Nullstellensatz $J = S$, hence there is an expression

$$1 = \left(\sum_{i=1}^{K} h_i(X_i T) \cdot \varphi_i(X) \right) + \gamma(X,T) \cdot g(X,T)$$

where $\gamma, h_i \in S$ and $\varphi_i \in I$. Taking $T = f(X)^{-1}$ one has $g(X, f(X)^{-1}) = 0$ and obtains the identity

$$1 = \sum_{i=1}^{K} h_i(X, f(X)^{-1}) \varphi_i(X)$$

in $k(X_1, \ldots, X_n)$. Let T^α be the largest power of T occurring in any monomial of any h_i. Multiplying the previous equation by $f(X)^\alpha$ we obtain

$$f(X)^\alpha = \sum_{i=1}^{K} \left(h_i \left(X, f(X)^{-1} \right) f(X)^\alpha \right) \varphi_i(X) = \sum_{i=1}^{K} n_i(X) \cdot \varphi_i(X)$$

where $n_i(X) = h_i \left(X, f(X)^{-1} \right) f(x)^\alpha = \sum_{j=0}^{\alpha} h_{i,j}(X) f(X)^{\alpha - j}$ in R, thus $f^\alpha \in I$. *q.e.d.*

Remark. Taking $f = 1$ one obtains Theorem 2.

Remark 6. We have the following rather obvious relations between these operations on ideals

$$J \cdot \sum_{\lambda \in \Lambda} I_\lambda = \sum_{\lambda \in \Lambda} J \cdot I_\lambda \tag{1}$$

$$\sqrt{I \cap J} = \sqrt{I \cdot J} = \sqrt{I} \cdot \sqrt{J} \tag{2}$$

For infinite Λ we have $\sqrt{\bigcap_{\lambda \in \Lambda} I_\lambda} \subseteq \bigcap_{\lambda \in \Lambda} \sqrt{I_\lambda}$ but equality may fail (e.g. $R = K[T]$, $\Lambda = \mathbb{N}$, $I_\lambda = T^\lambda \cdot R$). Moreover we have the inclusions

$$\sqrt{I + J} \supseteq \sqrt{I} + \sqrt{J} \tag{3}$$

$$(I + J) \cap K \supseteq I \cap K + J \cap K \tag{4}$$

2. Quasi-affine algebraic varieties and their dimension

2.1. The Zariski topology on k^n

Let k be an algebraically closed field.

Definition 1. A subset M of k^n is *Zariski-closed* iff it can be written as $M = V(I)$ where $I \subseteq k[X_1, \ldots, X_n]$ is some ideal.

Example 1. Consider X a metric space and $I \subseteq C(X)$ an ideal in the ring of continues functions on X. Then the set of zeroes $V(I) = \{x \in X \mid f(x) = 0 \text{ for all } f \in I\} = \bigcap_{f \in I} V(f)$ is an closed subset and any closed subset $M \subseteq X$ is $V(f)$ with $f(x) = d_X(x, M) = \inf\{d_X(x, m) \mid m \in M\}$.

Example 2. Let $n = 1$. Any ideal $I \subseteq k[X]$ is principal $I = \left(\prod_{i=1}^{m}(X - \xi_i)^{a_i}\right)_{k[X]}$ and $V(I) = \{\xi_1, \ldots, \xi_n\}$ unless $I = 0$, $V(I) = k$. Thus the Zariski-closed subsets of k are k and the finite subsets and the open subsets are $\emptyset$ and the cofinite subsets (i.e. the subsets U with $k \setminus U$ being finite). In particular the intersection of two non-empty open subsets is in turn non-empty.

Example 3. Let $n = 2$. We will see at the end of this chapter that the Zariski-closed subsets of k^2, besides k^2, are the subsets of the form $C \cup F$ where $C = \left\{x \in k^2 \;\middle|\; P(x) = 0\right\}$ (for some $P \in k[X_1, X_2] \setminus \{0\}$, C is a *curve*) and $F \subseteq k^2$ is finite.

Remark 1. By the results of subsection 1.7, there is a bijection

$$\begin{aligned} \{\text{Zariski-closed subsets of } k^n\} &\xrightarrow{\sim} \left\{\text{ideals } I \subseteq R = k[X_1, \ldots, X_n] \text{ such that } I = \sqrt{I}\right\} \\ M = V(I) &\longleftarrow\!\shortmid I \\ M &\longmapsto I = \{f \in R \mid M \subseteq V(f)\} \end{aligned}$$

which is anti-monotonic (in the sense that from $I \subseteq J$ follows $V(I) \supseteq V(J)$) and it sends $\bigcap_{\lambda \in \Lambda} M_\lambda$ to $\sqrt{\sum_{\lambda \in \Lambda} I_\lambda}$ and $M_1 \cup M_2$ to $I_1 \cap I_2$. In particular, the Zariski-closed subsets are indeed the closed subsets for some topology on k^n.

Remark. A *topology* τ on a set T is a set of subsets of T (the *open* subsets of T) containing $\emptyset$ and T and with the property, that the union of arbitrarily many open subsets and the intersection of finitely many open subsets is in turn open. The complements of the open subsets are called *closed*. The union of finitely many and the intersection of arbitrarily many closed subsets is closed. The topological space (T, τ) may or may not have the following separation properties for which the following is required for arbitrary $x \neq y \in T$.

T0 There is an open subset U with $x \in U$, $y \notin U$ or $x \notin U$, $y \in U$.

T1 There is an open subset U with $x \in U$, $y \notin U$.

T2 (Hausdorff) There are open subsets $U, V \in \tau$ with $U \cap V = \emptyset$ and $x \in U$, $y \in V$.

T is called *quasi-compact* if every open covering of T has a finite sub-covering. It is *compact* if it is quasi-compact and Hausdorff. The *induced topology* on a subset $X \subseteq T$ is $\{X \cap U \mid U \in \tau\}$. A subset X of T is dense if it intersects any non-empty open subset. A map $T \longrightarrow S$ is *continuous* if the following equivalent properties hold:

(a) The preimage of any open subset of S is open in T.

(b) The preimage of any closed subset of S is closed in T.

T is *connected* if the following equivalent properties hold:

(a) If $U \subseteq T$ is both open and closed, then $U = \emptyset$ or $U = T$.

(b) If $T = U \cup V$ with $U, V \in \tau$ and $U \cap V = \emptyset$ then $U = \emptyset$ and $U = T$ or $U = T$ and $V = \emptyset$.

(c) If $T \xrightarrow{f} \mathbb{R}$ is continuous and the real numbers $a < b$ are in $f(T)$, then $[a, b]$ is contained in $f(T)$.

Definition 2. A topological space T is *Noetherian* if it satisfies the following equivalent properties:

(a) There is no infinite properly descending sequence of closed subsets $T \supseteq M_0 \supsetneq M_1 \supsetneq \ldots$.

(b) Any set $\mathfrak{X} \neq \emptyset$ of closed subsets of T contains a $\subseteq$-minimal element.

(c) Any open subset of T is quasi-compact.

Proof. (a) $\rightarrow$ (b) Otherwise, select $M_1 \in \mathfrak{X}$, $M_2 \subsetneq M_1$, if M_1 is not yet minimal and so on.

(b) $\rightarrow$ (c) Let $U \subseteq T$ be open, $U = \bigcup_{\lambda \in \Lambda}(T \setminus M_\lambda)$ with M_λ closed, $M_\lambda \supseteq T \setminus U$. Consider $\mathfrak{X} = \left\{\bigcap_{\lambda \in F} M_\lambda \;\middle|\; |F| < \infty\right\}$. It has a minimal element N which equals $T \setminus U$. because every $u \in U$ is not in M_λ for some λ and $N \cap M_\lambda \subsetneq M_\lambda$ contradicting minimality. If $N = \bigcap_{\lambda \in F} M_\lambda$ then $U = \bigcup_{\lambda \in F}(T \setminus M_\lambda)$.

(c) $\rightarrow$ (b) Otherwise, $U = T \setminus M_\infty$ with $M_\infty = \bigcap_{i=1}^{\infty} M_i$ is covered by the $T \setminus M_i$ without finite sub-covering.

q.e.d.

Corollary 1 (to Remark 1)**.** *The space k^n with the Zariski topology is a Noetherian topological space, as an infinite descending chain $M_1 \supsetneq M_2 \supsetneq \ldots$ of closed subsets would yield an infinite ascending chain of ideals by applying the correspondence from Remark 1.*

Definition 3. A non-empty topological space X is called *irreducible*, if the following equivalent conditions hold:

(a) If $X = A \cup B$ where A and B are closed subsets of X, then $X = A$ or $X = B$.

(b) Two arbitrary non-empty open subsets of X have non-empty intersection.

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

A closed subset of X is called irreducible if it is irreducible as a topological subspace.

Remark 2 (a.k.a. Remark 4)**.** For the sake of simplicity "irreducible subset of X" will be used as as a substitute of "irreducible closed subset of X".

Proposition 1 (a.k.a. Proposition 2)**.** *In a Noetherian topological space X, any closed subset Y is Noetherian and can be expressed as a finite union $Y = \bigcup_{i=1}^{k} Y_i$ of irreducible subsets Y_i where $Y_i \subseteq Y_j$ implies $i = j$. Moreover the Y_i are unique up to permutation of their order and $\{Y_1, \ldots, Y_k\}$ can be characterized as:*

- *The set of irreducible closed subsets of Y containing a non-empty open subset of Y.*
- *The set of $\subseteq$-maximal irreducible subsets of Y.*

The $(Y_i)_{i=1}^k$ *are called the* irreducible components *of* Y*.*

Proof. The first assertion, Y being Noetherian, is trivial. For the existence of a finite decomposition into irreducible subsets, let $\mathfrak{X}$ be the set of closed subsets $Y \subseteq X$ without such a representation. As X is Noetherian $\mathfrak{X}$ has $\subseteq$-minimal element Y. We have $Y \neq \emptyset$, because $\emptyset$ can be written as the empty subset and it is not irreducible because it would be the union $\{Y\}$ of irreducible subsets otherwise. Thus $Y = Y_1 \cup Y_2$ with $Y_1 \subsetneq Y$ and $Y_2 \subsetneq Y$. By the induction assumption ($Y \in \mathfrak{X}$ being minimal) Y_1 and Y_2 can be written as finite unions of irreducible subsets of X. Hence Y is a finite union of irreducible subsets, a contradiction. Let $Y = \bigcup_{i=1}^k Y_i$ where Y_i is irreducible and k is minimal. If $Y_i \subseteq Y_j$ and $i \neq j$, then Y_i could be removed from the list and k would not be minimal. Thus all our claims in the existence assumption are satisfied.

Generally let $Y = \bigcup_{i=1}^k Y_i$, Y_i irreducible and $Y_i \not\subseteq Y_j$ for $i \neq j$. Then $Y_i \not\subseteq \bigcup_{j=1, j\neq i}^k Y_j$ because Y_i is irreducible. Now let A be any irreducible subset of Y containing a non-empty subset U of Y. If $U \cap Y_i \neq \emptyset$ then U is dense in Y_i as Y_i is irreducible. As $A \supseteq U$ and A is closed $A \supseteq Y_i = U$. Hence $A = Y_i$ otherwise we had a non-trivial composition of A with

$$A = Y_i \cup \left(\bigcup_{j=1, j\neq i}^{k} A \cap Y_j \right) .$$

Hence $\{Y_i \mid 1 \leq i \leq k\}$ contains all irreducible subsets containing a non-empty open subset of Y. Conversely, $U_i = Y \setminus \bigcup_{j=1, j\neq i}^k Y_j$, then U_i is open in Y and non-empty since Y_i is no subset of the subtracted union and $U_i \subseteq Y_i$. Thus Y_i is an irreducible subset of Y which contains a non-empty open subset. This establishes uniqueness and the first characterization. The second characterization is left as an exercise. *q.e.d.*

Example 4. (a) Every point is irreducible.

(b) Every irreducible topological space is connected.

(c) $k \times \{0\} \cup \{0\} \times k \subseteq k^2$ turns out to be Zariski-closed ($= V(XY)$) and connected (as we will see) but *not* irreducible, as it is $V(XY) = V(X) \cup V(Y)$.

Proposition 2 (a.k.a. Proposition 3)**.** *Let* I *be an ideal in* $R = k[X_1, \ldots, X_n]$ *then* $V(I)$ *is irreducible iff* $\sqrt{I}$ *is a prime ideal.*

Proof. Without loss of generality we may assume $\sqrt{I} = I$ as ($\sqrt{\sqrt{I}} = \sqrt{I}$ and $V(\sqrt{I}) = V(I)$). If $Y = V(I)$ is irreducible, then $Y \neq \emptyset$, hence $1 \neq I$. If $f, g \in R$ and $fg \in I$, then $Y \subseteq V(fg) = V(f) \cup V(g)$ and

$$Y = (Y \cap V(f)) \cup (Y \cap V(g))$$

where the two members are closed. As Y is irreducible, at least one member equals Y, corresponding to $Y \subseteq V(f)$ or $Y \subseteq V(g)$ which, by the Nullstellensatz as Proposition 1.7.1 implies $f \in I$ or $g \in I$. Hence I is a prime ideal.

Let I be a prime ideal. Then $I \subsetneq R$ hence $Y = V(I)$ is not empty by the Nullstellensatz. Assume $Y = Y_1 \cup Y_2$ a proper decomposition. In particular $Y_1 \not\subseteq Y_2$ and $Y_1 \not\supseteq Y_2$. Let $J_k \subseteq R$ be the ideal of polynomials vanishing on Y_k. Then $J_1 \not\subseteq J_2$ and $J_1 \not\supseteq J_2$ by Remark 1. Let $f \in J_1 \setminus J_2$ and $g \in J_2 \setminus J_1$, then f_1 vanishes on Y_1 but not on Y_2 and g vanishes on Y_2 but not on Y_1, $fg \in I$ (by

Proposition 1.7.1, as it vanishes on Y and $I = \sqrt{I}$) but $f \notin I$ as it does not vanish identically on Y_2 and $g \notin I$ as it does not vanish on Y_1. So I is not prime. *q.e.d.*

Remark. In $R = k[X, Y]$, $X \cdot R$ and $Y \cdot R$ are prime ideals because e.g. $R/Y \cdot R \simeq k[X]$ which is a domain. Hence $k \times \{0\}$ and $\{0\} \times k$ are indeed irreducible as was claimed in example 4. In particular, they are connected and since they have a non-empty intersection, their union is connected as well.

Example 5. We have $k^n = V(\{0\})$ is irreducible as R is a domain, hence $\{0\} \subseteq R$ is prime.

Corollary 2. *If $f \in R = k[X_1, \ldots, X_n]$ is an irreducible polynomial, then $V(f)$ is an irreducible closed subset of k^n, R being a unique factorization domain.*

Definition 4. Let M be an irreducible subset of the Noetherian topological space X. The *codimension* $\operatorname{codim}(M, X)$ of M in X is the (possible infinite) supremum of the set of integers k such that there is a strictly ascending chain $M = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_k \subseteq X$ of irreducible subsets of X. The *dimension* of X is the (possibly infinite) supremum of the codimensions of all irreducible subsets of X.

Remark. This notion of dimension seems to go back to W. Krull.

Remark 3 (a.k.a. Remark 5)**.** (*a*) Let X be Noetherian and $A \supseteq B \supseteq C$ are irreducible, then

$$\begin{array}{c} \operatorname{codim}(C, B) + \operatorname{codim}(B, A) \leq \operatorname{codim}(C, A) \\ \dim(A) + \operatorname{codim}(A, X) \leq \dim(X) \end{array} . \tag{1}$$

(*b*) Let Y be irreducible and $U \subseteq X$ open such that $Y \cap U \neq \emptyset$. Then there is a bijection

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{irreducible subsets } A \text{ of } X \\ \text{such that } A \supseteq Y \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{irreducible subsets } M \text{ of } U \\ \text{such that } M \supseteq U \cap Y \end{array} \right\} \\ A & \longmapsto & M = A \cap U \\ \overline{M} & \longmapsfrom & M \end{array}$$

(which is merely a tedious calculation similar to problem 4 on exercise sheet #6). This implies the *locality of codimension*:

$$\operatorname{codim}(Y, X) = \operatorname{codim}(Y \cap U, U) \, . \tag{2}$$

(*c*) A noetherian topological space is called *catenary* if, for arbitrary $X \supseteq A \supseteq B \supseteq C$ equality holds in the first line of (1).

Theorem 5. *For $X = k^n$ with the Zariski-topology, $\dim(X) = n$ and equality occurs in (1). In particular, X is catenary.*

Remark 4 (a.k.a. Remark 5)**.** Obviously $\operatorname{codim}(\{0\}^n, k^n) \geq n$ because of the chain $\{0\}^n \subsetneq k \times \{0\}^{n-1} \subsetneq k^2 \times \{0\}^{n-2} \subsetneq \ldots \subsetneq k^{n-1} \times \{0\} \subsetneq k^n$. The subsets here are irreducible because they are homeomorphic to k^i which is irreducible by Proposition 2 as $k[X_1, \ldots, X_i]$ is a domain (i.e. $\{0\}$ is prime). Similarly, $\operatorname{codim}(\{x\}, X) \geq n$ for any $x \in X = k^n$.

Remark. (*a*) Even the finiteness of $\dim(k^n)$ is not trivial.

(*b*) In topology, the fact that no open subset $U \subseteq \mathbb{R}^n$, $U \neq \emptyset$ is homeomorphic to any open $V \subseteq \mathbb{R}^k$ for $k \neq n$ is not trivial. Among the first proofs are by Brouwer and Lebesgue (Pflastersatz, Lebesgue covering theorem)

(*c*) For $\mathrm{Spec}(R)$ with R Noetherian, $\mathrm{codim}(A, B)$ is finite for irreducible $A \subseteq B$ (quite hard, probably Krull (even though Krull was a *n00b* compared to Grothendieck)) but there are examples where $\mathrm{Spec}(R)$ is infinite-dimensional (relatively easy), there are closed points of differing codimensions (quite easy) and $\mathrm{Spec}(R)$ may fail to be catenary (very hard, Nagata) but the R encountered "in free nature" are catenary.

Lemma 1. *Let R be a factorial domain. If $\mathfrak{p} \subseteq R$ is a non-zero prime ideal, then $\mathfrak{p}$ contains a prime element.*

Proof. Let $f \in \mathfrak{p} \setminus \{0\}$ and $f = \prod_{i=1}^{n} p_i$ (note $n \neq 0$ as $f \notin R^\times$, as $\mathfrak{p}$ is prime) be it's decomposition into prime factors, then one of the p_i must be in $\mathfrak{p}$, since $\mathfrak{p}$ is prime. *q.e.d.*

Proposition 3 (a.k.a. Proposition 4, formerly known as Proposition 1, srsly get your shit together)**.** *Let $p \in R = k[X_1, \ldots, X_n]$ be an irreducible polynomial. Then $V(p)$ (irreducible by Corollary 2) is of codimension 1 in k^n and all subsets of k^n with codimension 1 can be obtained in this way.*

Proof. Let p be as required, then $\mathfrak{p} = p \cdot R$ is prime. If $X = V(\mathfrak{p})$ had codimension 0, it would equal k^n (which is irreducible by Proposition 2 and $\mathfrak{p} = 0$ and $p = 0$, a contradiction. If $\mathrm{codim}(X, k^n) > 1$, there is a irreducible subset $Y = V(\mathfrak{q})$ between X and k^n where $\mathfrak{q}$ may be assumed prime (Remark 1 and Proposition 2) and $\mathfrak{q} \subsetneq \mathfrak{p}$ by Remark 1. We have $\mathfrak{q} \neq \{0\}$ because $Y = k^n$ otherwise. Let $f \in \mathfrak{q} \setminus \{0\}$, then $p|f$ Let $f = \prod_{i=1}^{m} q_i$ be the prime factor decomposition of f in R, where m may be assumed minimal. Then p is proportional to one of the q_i and if $p \in \mathfrak{q}$ then q_i could be removed from the factors, $f = g \cdot p$, and $g \in \mathfrak{q}$ can be factored with $m - 1$ prime factors, in contradiction to the minimality of m. Thus $p \in \mathfrak{q}$ and $p \cdot R \subseteq \mathfrak{q} \subseteq \mathfrak{p} = p \cdot R$, a contradiction to $\mathfrak{q} \subsetneq \mathfrak{p}$. Thus, the codimension is 1 in this case (a special case of Krull's principal ideal theorem).

On the other hand, let $V(\mathfrak{p})$ be irreducible and of codimension 1. By Proposition 2 we may assume $\mathfrak{p} \subseteq R$ to be a prime ideal. If $p \in \mathfrak{p}$ is a prime, then $V(\mathfrak{p}) \subseteq V(p) \subsetneq k^n$, proving that $V(\mathfrak{p}) = V(p)$. *q.e.d.*

Remark (on Example 3)**.** If Theorem 5 is assumed, $\dim(k^2) = 2$ and the irreducible subsets are of codimension 2 (points), of codimension 1 ($V(f)$ for irreducible f), and 0 (k^2).

2.2. Quasi-affine algebraic varieties

Let the algebraically closed field k be fixed.

Definition 1. An *affine algebraic variety* is (for our purposes) an irreducible (Zariski-closed) subset $Z \subseteq k^n$, for some n. A *quasi-affine algebraic variety* is a non-empty Zariski-open subset of an affine algebraic variety.

Remark 1. A closed subset of a Noetherian space is Noetherian, as is any open subset thereof, affine and quasi-affine varieties are Noetherian.

Definition 2. Let $Z \subseteq k^n$ be a quasi-affine algebraic variety and $f : Z \to k$ a k-valued function

on it. We call f *regular at* x if there is a neighbourhood $U \subseteq Z$ of x and polynomials $p, q \in k[X_1, \ldots, X_n]$ such that $V(q) \cap U = \emptyset$ and such that $f(y) = \frac{p(y)}{q(y)}$ for all $y \in U$. We call f *regular* on Z if it is regular at every point of Z. Denote the ring of regular functions by $\mathcal{O}(Z)$ and put $\mathcal{O}(\emptyset) = \{\text{empty function}\}$.

The association $Z \to \mathcal{O}(Z)$ is part of the structure of a *sheaf*.

Definition 3. Let X be a topological space. A *sheaf* $\mathcal{G}$ (of sets, (abelian) groups or rings) on X associates:

- To each open subset $U \subseteq X$ an object $\mathcal{G}(U)$.
- To each inclusion $V \subseteq U$ of open subsets for X, a morphism

$$\begin{aligned} \mathcal{G}(U) &\longrightarrow \mathcal{G}(V) \\ f &\longmapsto f|_V \end{aligned}$$

(note that $f|_V$ is just notation and does not necessarily mean the restriction to V) such that the following conditions hold:

(α) $f|_U = f$ when $f \in \mathcal{G}(U)$

(β) $(f|_V)|_W = f|_W$ for $f \in \mathcal{G}(U)$ and inclusions $W \subseteq V \subseteq U$ of open subsets.

(γ) If $U = \bigcup_{\lambda \in \Lambda} U_\lambda$ is a covering of an open subset $U \subseteq X$ by open subsets $U_\lambda \subseteq U$, then the map

$$\begin{aligned} \mathcal{G}(U) &\longrightarrow \left\{ (f_\lambda) \in \prod_{\lambda \in \Lambda} \mathcal{G}(U_\lambda) \;\middle|\; f_\lambda|_{U_\lambda \cap U_\vartheta} = f_\vartheta|_{U_\lambda \cap U_\vartheta} \text{ for } \lambda, \vartheta \in \Lambda \right\} \qquad (*) \\ f &\longmapsto (f|_{U_\lambda})_{\lambda \in \Lambda} \end{aligned}$$

is bijective.

Remark. (a) If only (α) and (β) are satisfied, then $\mathcal{G}$ is called a *presheaf*. If in addition $(*)$ is injective it is called a *separated presheaf*.

(b) If $f_\lambda = f|_{U_\lambda}$ then $f_\lambda|_{U_\lambda \cap U_\vartheta} = f|_{U_\lambda}|_{U_\vartheta} = f|_{U_\lambda \cap U_\vartheta} = f|_{U_\vartheta}|_{U_\lambda} = f_\vartheta|_{U_\lambda \cap U_\vartheta}$ by β. Hence $(*)$ is well-defined and only bijectivity may be violated for some presheaves.

(c) Condition (γ) is called the *sheaf axiom* and has interesting consequences if $\Lambda = \emptyset$ (hence $U = \emptyset$). Then the product on the right-hand side of $(*)$ is the empty product (containing just one element), the condition

$$\forall \lambda, \vartheta \in \Lambda \colon f_\lambda|_{U_\lambda \cap U_\vartheta} = f_\vartheta|_{U_\lambda \cap U_\vartheta}$$

is trivially satisfied and it follows that $\mathcal{G}(\emptyset)$ is the object with just one element (i.e. the trivial group, the zero ring etc.).

(*d*) If R is an object and $\mathcal{G}(U) = \{\text{functions } U \to R\}$ and $f|_U$ is the ordinary restriction then $\mathcal{G}$ is a sheaf of these objects, where the group/ring operations on $\mathcal{G}(U)$ are defined pointwise:

$$(f * g)(x) = f(x) * g(x)$$

where $*$ is $+$ or $\cdot$.

(*e*) If R has a topology such that the group/ring operations are continuous (as maps $R \times R \to R$, $R \times R$ carrying the product topology) then $C^0(U) \subseteq \mathcal{G}(U)$, the subset of continuous functions, form a subsheaf. The same happens with C^∞ functions if $R = \mathbb{R}$ or $R = \mathbb{C}$ and $X = \mathbb{R}^n$ (or a C^∞-manifold) or with holomorphic functions if $R = \mathbb{C}$ and $X = \mathbb{C}^n$ (or a holomorphic manifold).

(*f*) It is clear from Definition 2 that $U \mapsto \mathcal{O}(U)$ defines a sheaf of rings on a quasi-affine algebraic variety.

(*g*) The elements of $\mathcal{G}(U)$ are called *sections* of $\mathcal{G}$ on U

Example 1. (*a*) If $f \in k[X_1, \ldots, X_n]$ then $f|_Z \in \mathcal{O}(Z)$ (put $U = Z$, $p = f$ and $q = 1$ in Definition 2).

(*b*) If $f \in \mathcal{O}(Z)$ and $V(f) = \{z \in Z \mid f(z) = 0\}$ is empty, then $\frac{1}{f} \in \mathcal{O}(Z)$.

(*c*) We call $\mathcal{O} = \mathcal{O}_Z \colon U \mapsto \mathcal{O}(U)$ the *structure sheaf* of Z.

Proposition 1. *Let $z \in Z$. If $f_1, \ldots, f_m$ are functions $Z \to k$ which are regular at $z \in Z$ then*

$$\begin{aligned} Z &\longrightarrow k^m \\ \zeta &\longmapsto (f_1(\zeta), \ldots, f_m(\zeta)) \end{aligned}$$

is Zariski-continuous on some neighbourhood of z.

Proof. This will follow easily from the fact that the following classes of maps are Zariski-continuous:

(*a*) $f \colon Z \to k^m$ where $f = (f_1, \ldots, f_m)$ with $f_i \in S = k[X_1, \ldots, X_n]$. Indeed, if $A \subseteq k^m$ is Zariski-closed, then $A = V(I)$ with the ideal $I \subseteq R$ being generated by $I = (g_1, \ldots, g_\ell)_R$, where $R = k[X_1, \ldots, X_m]$. Then

$$f^{-1}(A) = V\big(g_1(f(-)), \ldots, g_\ell(f(-))\big) \,,$$

where $g_i(f(-) = g_i\big(f_1(X_1, \ldots, X_n), \ldots, f_m(X_1, \ldots, X_n)\big) \in S$.

(*b*) The map

$$\begin{aligned} \Omega = k^m \times (k^\times)^m &\xrightarrow{q} k^m \\ (x_1, \ldots, x_m, y_1, \ldots, y_m) &\longmapsto \left(\frac{x_1}{y_1}, \ldots, \frac{x_m}{y_m}\right) \end{aligned}$$

is continuous. Indeed, let $A \subseteq k^m$, $A = V(g_1, \ldots, g_\ell)$ be Zariski-closed. If N is the maximum total degree of the g_i, then $h_1, \ldots, h_\ell$ defined by

$$h_i(X_1, \ldots, X_m, Y_1, \ldots, Y_m) = (Y_1 \cdots Y_m)^N g_i\left(\frac{X_1}{Y_1}, \ldots, \frac{X_m}{Y_m}\right) \in k[X_1, \ldots, X_m, Y_1, \ldots, Y_m]$$

are polynomials and $q^{-1}(A) = \Omega \cap V(h_1, \ldots, h_\ell)$, as the factor $(Y_1 \cdots Y_m)^N$ vanishes nowhere on Ω.

If now f is as in the formulation above, then there are $p_i, q_i \in k[X_1, \ldots, X_n]$ such that in some neighbourhood $U \ni z$ in Z none of the q_i has zeros and $f_i = \frac{p_i}{q_i}$. Then $f|_U$ is equal to the composition of continuous maps

$$U \xrightarrow{(p_1,\ldots,p_m,q_1,\ldots,q_m)} k^m \times (k^\times)^m \xrightarrow{q} k^m$$

and thus continuous itself. *q.e.d.*

Corollary 1. *If $f \in \mathcal{O}(Z)$ then $V(f) = \{z \in Z \mid f(z) = 0\}$ is a closed subset of Z.*

Proof. By Proposition 1, $Z \xrightarrow{f} k$ is continuous. Since $\{0\} \subseteq k$ is Zariski-closed, so is it's preimage $V(f)$. *q.e.d.*

Theorem 6. *If X is a quasi-affine algebraic variety, K the quotient field of $\mathcal{O}(X)$ (the field of rational functions on X) then* $\dim(X) = \deg \mathrm{tr}(K/k)$ *and equality always occurs in equation (2.1.1).*

Remark. (*a*) If K/k is a field extension, then there is a subset $B \subseteq K$ (a *transcendence base*) which is algebraically independent over k and such that K is algebraic over the subfield generated by B and k. The cardinality of B only depends on K/k and is called *transcendence degree* $\deg \mathrm{tr}(K/k)$ of K/k.

(*b*) If $\emptyset \neq U \subseteq X$ is open, then $\mathcal{O}(X) \to \mathcal{O}(U), f \mapsto f|_U$ is an injective homomorphism (by Corollary 1 and irreducibility of X) which can be seen to induce an isomorphism of quotient fields $K(X) \xrightarrow{\sim} K(U)$.

(*c*) If $X = k^n$, then $\mathcal{O}(X) = k[X_1, \ldots, X_n]$ by the following Proposition 2 and $K = k(X_1, \ldots, X_n)$ for which $\{X_1, \ldots, X_n\}$ is a transcendence base over k. Thus, Theorem 5 is a special case of Theorem 6.

Proposition 2. *If $\mathfrak{p} \subseteq R = k[X_1, \ldots, X_n]$ is a prime ideal and $X = V(\mathfrak{p})$, then*

$$\begin{aligned} R/\mathfrak{p} &\longrightarrow \mathcal{O}(X) \\ f \mod \mathfrak{p} &\longmapsto f|_X \end{aligned}$$

is an isomorphism.

Remark. (*a*) The subset $X \subseteq k^n$ occurring here are precisely the affine algebraic varieties in k^n.

(*b*) In particular, the ring extension $\mathcal{O}(X)/k$ is of finite type for such X.

(*c*) If X is a quasi-affine algebraic variety, $\mathcal{O}(X)/k$ may fail to be of finite type (see Nagata (the Lord of the Rings), *Lectures on Hilberts 13^{th} problem*).

Proof of Proposition 2.. Injectivity is quite obvious. To prove surjectivity, let $f \in \mathcal{O}(X)$. By Definition 2, for any $\xi \in X$ there are an open neighbourhood $U_\xi \ni \xi$ in X and $p_\xi, q_\xi \in R$ such that $V(q_\xi) \cap U_\xi = \emptyset$ and $f = \frac{p_\xi}{q_\xi}$ on U_ξ. Recall that any open subset of X is dense, X being irreducible. For any $\xi, \eta \in X$ we therefore have $\frac{p_\xi}{q_\xi} = \frac{p_\eta}{q_\eta}$, hence $p_\xi q_\eta = p_\eta q_\xi$ on the (open and thus) dense subset

$U_\xi \cap U_\eta \subseteq X$, But then we must have

$$p_\xi q_\eta = p_\eta q_\xi \quad (\text{on } X)\ , \tag{$*$}$$

because $V(p_\xi q_\eta - p_\eta q_\xi)$ is closed and dense in X.

If U_ξ is open, the set $X \setminus U_\xi$ is closed in X, hence also in k^n and so it admits a representation $X \setminus U_\xi = V(I_\xi)$ for a suitable ideal $I_\xi \subseteq R$. Then $\xi \notin V(I_\xi)$, hence there is $r_\xi \in I_\xi$ such that $r_\xi(\xi) \neq 0$. Then $W_\xi = X \setminus V(r_\xi) \subseteq U_\xi$. Replacing U_ξ by W_ξ and p_ξ by $r_\xi p_\xi$ and q_ξ by $r_\xi q_\xi$ we still have $f = \frac{p_\xi}{q_\xi}$ on U_ξ, hence (∗), but additionally we obtained the condition $U_\xi = X \setminus V(q_\xi)$. Since the $U_\xi = X \setminus V(q_\xi)$ cover X, which is quasi-compact, we have finitely many $\xi_1, \ldots, \xi_N$ such that $X \setminus V(q_i)$ cover X (where we set $p_i = p_{\xi_i}, q_i = q_{\xi_i}$ for brevity). Let $\mathfrak{p} = (q_{N+1}, \ldots, q_\ell)_R$ and let $p_{N+1} = \ldots = p_\ell = 0$. Then $\bigcap_{i=1}^{\ell} V(q_i) = \emptyset$ in k^m, hence there are $a_1, \ldots, a_\ell \in R$ such that

$$\sum_{i=1}^{\ell} a_i q_i = 1 \quad \text{in } R = k[X_1, \ldots, X_m] \tag{$\#$}$$

by Hilbert's Nullstellensatz. Put $\varphi = \sum_{i=1}^{\ell} a_i p_i \in R$. We claim that $\varphi|_X = f$. Indeed, we have

$$p_i q_j = p_j q_i \quad (\text{on } X) \text{ for all } i, j \leq \ell \tag{\$}$$

If $i, j \leq N$, this is just (∗) and otherwise both sides vanish. Now, if $x \in X$ there is some $j \leq N$ such that $x \in U_{\xi_j}$, hence $f(x) = \frac{p_j(x)}{q_j(x)}$ and therefore

$$\begin{aligned} q_j(x) f(x) = p_j(x) &\overset{(\#)}{=} q_j(x) \sum_{i=1}^{\ell} p_j(x)\big(a_i(x) p_i(x)\big) \overset{(\$)}{=} \sum_{i=1}^{\ell} p_i(x) q_j(x) a_i(x) = q_j(x) \sum_{i=1}^{\ell} p_i(x) a_i(x) \\ &= q_j(x)\varphi(x)\ , \end{aligned}$$

which yields $f(x) = \varphi(x)$ since $q_j(x) \neq 0$. *q.e.d.*

Corollary 2. *In the situation of Proposition, we have a bijection between the closed subsets of X and the ideals I of $\mathcal{O}(X)$ such that $I = \sqrt{I}$*

$$\begin{aligned} \{\textit{closed subsets of } X\} &\xrightarrow{\sim} \left\{\textit{ideals } I \subseteq \mathcal{O}(X) \textit{ such that } I = \sqrt{I}\right\} \\ A \subseteq X &\longmapsto \{f \in \mathcal{O}(X) \mid f|_A = 0\} \\ V(I) &\longmapsto\!\shortmid\ I \end{aligned}$$

By this correspondence, the irreducible subsets correspond to the prime ideals and the points correspond to the maximal ideals.

Proof. It is known from subsection 2.1 that we have a correspondence between the closed subsets of k^n and the ideals $J \subseteq R = k[X_1, \ldots, X_n]$ such that $J = \sqrt{J}$

$$\begin{aligned} \{\text{Zariski-closed subsets of } k^n\} &\xrightarrow{\sim} \left\{\text{ideals } J \subseteq R = k[X_1, \ldots, X_n] \text{ such that } J = \sqrt{J}\right\} \\ A \subseteq X &\longmapsto \{f \in R \mid f|_A = 0\} \\ V(J) &\longmapsto\!\shortmid\ J \end{aligned} \tag{$*$}$$

with the stated behaviour for points/irreducible subsets and maximal/prime ideals. We show that in (∗),

$$A \subseteq X \Longleftrightarrow J \supseteq \mathfrak{p} \tag{$+$}$$

Then the bijection between the ideals I in $R/\mathfrak{p}$ and the ideals J in R such that $J \supseteq \mathfrak{p}$

$$\begin{aligned} \{\text{ideals } I \subseteq R/\mathfrak{p}\} &\xrightarrow{\sim} \{\text{ideals } J \subseteq R \text{ such that } J \supseteq \mathfrak{p}\} \\ I &\longmapsto \text{preimage of } I \text{ under } R \to R/\mathfrak{p} \\ J/\mathfrak{p} &\longmapsto J \end{aligned}$$

(which maps maximal ideals, prime ideals, and ideals coinciding with their radicals on both sides to each other) composed with (∗) gives the desired bijection. By one of the versions of the Nullstellensatz (i.e. (∗) with $J = \mathfrak{p}$ and $A = X$) we have $\mathfrak{p} = \{f \in R \mid f|_X = 0\}$ such that $J \supseteq \mathfrak{p}$ implies $V(J) \subseteq V(\mathfrak{p}) = X$ and vice versa, which shows (+). *q.e.d.*

Fact 1. Let X be a quasi-affine algebraic variety in k^n. The open subsets of the form $X \setminus V(f)$ with $f \in \mathcal{O}(X)$ form a base of the topology on X.

Proof. We have $X \subseteq \overline{X}$ where $\overline{X} \in k^n$ is irreducible. Let $U \subseteq X$ and $x \in U$, then we must find $f \in \mathcal{O}(X)$ such that $f(x) \neq 0$ and $X \setminus V(f) \subseteq U$. If suffices to find $f \in \mathcal{O}(\overline{X})$ such that $f(x) \neq 0$ and such that $\overline{X} \setminus V(f) \subseteq U$. By Corollary 2 applied to $\overline{X}$ such f exists because otherwise $x \in V\left(\left\{f \in \mathcal{O}(\overline{X}) \;\middle|\; f|_{\overline{X}\setminus U} = 0\right\}\right) = \overline{X} \setminus U$. *q.e.d.*

Definition 4. Let $X \subseteq k^m$ and $Y \subseteq k^n$ be quasi-affine varieties. A *morphism* $X \xrightarrow{f} Y$ is a continuous map such that the following equivalent conditions hold:

(a) $f = (f_1, \ldots, f_n)$ where $f_i \in \mathcal{O}_X(X)$.

(b) If $U \subseteq Y$ is open and $\varphi \in \mathcal{O}_Y(U)$ then $f^*\varphi(x) \coloneqq \varphi(f(x))$ defines an element of $\mathcal{O}_X(f^{-1}(U))$.

Proof. (b) → (a) We have $f_i(x) = X_i(f(x))$ where $Y \xrightarrow{X_i} k$ is the i^{th} coordinate.

(a) → (b) Let $x \in f^{-1}(U)$. By definition of $\mathcal{O}_Y(U)$ there are $p, q \in k[X_1, \ldots, X_n] =: S$ and a neighbourhood V of $f(x)$ such that q does not vanish on V and $\varphi(y) = \frac{p(y)}{q(y)}$ on V. We have $\varphi(f(\xi)) = \frac{p(f(\xi))}{q(f(\xi))}$ on $f^{-1}(V)$. By (a), we have a neighbourhood W of x in X and $a_i, b_i \in k[X_1, \ldots, X_m] =: R$ such that $f_i(\xi) = \frac{a_i(\xi)}{b_i(\xi)}$ on W. Replacing W by $W \cap f_i^{-1}(V)$ and replacing the b_i by a common denominator and changing a_i accordingly, we may assume that $W \subseteq f^{-1}(V)$ and $b_1 = \ldots = b_n = b$. Then we have, for $\xi \in W$

$$\varphi(f(\xi)) = \frac{p\left(\frac{a_1}{b}(\xi), \ldots, \frac{a_n}{b}(\xi)\right)}{q\left(\frac{a_1}{b}(\xi), \ldots, \frac{a_n}{b}(\xi)\right)} = \frac{b(\xi)^N p\left(\frac{a_1}{b}(\xi), \ldots, \frac{a_n}{b}(\xi)\right)}{b(\xi)^N q\left(\frac{a_1}{b}(\xi), \ldots, \frac{a_n}{b}(\xi)\right)}$$

and both parts of the fractions on the right hand side are in R if N is large enough (i.e. $N \geq \max(\deg p, \deg q)$)

q.e.d.

Remark 2. (a) $f \in \mathcal{O}(X)$ if and only if $X \xrightarrow{f} k$ is a morphism in this sense.

(b) Using characterization (b) of morphisms, it is clear, that the composition of morphisms is a morphism and that id_x is a morphism $X \longrightarrow X$. Quasi-affine varieties in some k^n with morphisms as in Definition 4 and the ordinary composition of maps therefore form a category.

Definition. A *category* is a triple $\mathcal{A} = (O, M, s, t, \circ)$ consisting of the five elements:

1. A class of objects $O = \mathrm{Ob}(\mathcal{A})$.
2. A class M of morphisms.
3. Maps $O \xleftarrow{s} M \xrightarrow{t} O$ where we put $\mathrm{Hom}_{\mathcal{A}}(X, Y)$ for $\{a \in M \mid s(a) = X, t(a) = Y\}$.
4. $$\begin{aligned} \circ : \{(a, b) \in M \times M \mid t(a) = s(b)\} &\longrightarrow M \\ (a, b) &\longmapsto b \circ a \end{aligned}$$

with the following conditions:

(a) $c \circ (b \circ a) = (c \circ b) \circ a$

(b) For every object $X \in O$, there is a unique $\mathrm{id}_X \in \mathrm{Hom}_{\mathfrak{A}}(X, X)$ such that $f \circ \mathrm{id}_X = f$ and $\mathrm{id}_X \circ g = g$ for morphisms $X \xrightarrow{f} T$, $S \xrightarrow{g} X$.

Example 1. (a) (abelian) groups, group homomorphisms.

(b) k-vector spaces, their linear maps.

(c) R-modules, morphisms of R-modules.

(d) Sets, maps between sets.

(e) rings, ring homomorphisms.

(f) affine or quasi-affine varieties.

(g) k-algebras or k-algebras of finite type, with k-linear ring homomorphisms as morphisms.

Remark. (a) It is normally assumed, that $\mathrm{Hom}_{\mathcal{A}}(X, Y)$ form a set.

(b) If the class of objects and morphisms are sets, the category is called *small*.

Proposition 3. *For affine algebraic varieties $M \subseteq k^m$ and $N \subseteq k^n$ we have a bijection*

$$\begin{aligned} \mathrm{Hom}(M, N) = \left\{ \textit{Morphisms } M \xrightarrow{f} N \right\} &\xrightarrow{\sim} \left\{ \begin{array}{c} \textit{Morphisms of } k\textit{-algebras} \\ \mathcal{O}(N) \xrightarrow{\varphi} \mathcal{O}(M) \end{array} \right\} \\ f &\longmapsto \varphi = f^* \quad \textit{where } f^*\lambda(x) = \lambda(f(x)) \ \forall x \in M \\ f_\varphi = (\varphi(Y_1), \ldots, \varphi(Y_n)) &\longmapsfrom \varphi \ , \end{aligned}$$

where $N \xrightarrow{Y_k} k, (\nu_1, \ldots, \nu_n) \mapsto \nu_k$ denotes the projection onto the k^{th} coordinate.

Remark. Actually the condition on M may be relaxed to M being quasi-affine (as the proof will show). If N is quasi-affine, the map $\longrightarrow$ is still well-defined, but may fail to be bijective (cf. Example 0 below).

Proof. It is obvious from Definition 4(b) that $\to$ is well-defined. To show that $\leftarrow$ is well-defined as well, it is sufficient (by Definition 4(a)) to check that $f_\varphi(M) \subseteq k^n$ is in fact a subset of N. To prove this, let $N = V(\mathfrak{q})$ for some prime ideal $\mathfrak{q} \in \operatorname{Spec} S$ (with $S = k[Y_1, \dots, Y_n]$). If $g \in \mathfrak{q}$ and $x \in M$, then

$$g\big(f_\varphi(x)\big) = g\big(\varphi(Y_1)(x), \dots, \varphi(Y_n)(x)\big) = \varphi\big(g(Y_1, \dots, Y_n)\big)(x) = 0$$

as $g(Y_1, \dots, Y_n) = 0$ in $\mathcal{O}(N)$ by Proposition 2. Thus, $f_\varphi(x) \in V(\mathfrak{q}) = N$, as claimed. It remains to show that these maps are indeed inverse to each other. We have

$$f_{f^*}(x) = \big(f^*Y_1(x), \dots, f^*Y_n(x)\big) = (f_1(x), \dots, f_n(x)) = f(x)\ .$$

Thus, $f_{f^*} = f$. Conversely,

$$f^*_\varphi Y_i(x) = i^{\text{th}} \text{ coordinate of } f_\varphi(x) = \varphi(Y_i)(x)\ ,$$

hence $f^*_\varphi Y_i = \varphi(Y_i)$. Since the Y_i generate $\mathcal{O}(N)$ as a k-algebra (by Proposition 2), we have $f^*_\varphi = \varphi$ on $\mathcal{O}(N)$. *q.e.d.*

Remark. (*a*) Note that $\mathcal{O}(X)$ is a domain when X is (quasi-)affine.

(*b*) The proposition may be restated (in category theoretical manner) by claiming that

$$\begin{gathered}\{\text{affine algebraic varieties over } k\} \xrightarrow{\sim} \{k\text{-algebras of finite type which are domains}\} \\ X \longmapsto \mathcal{O}(X) \\ \Big(X \xrightarrow{f} Y\Big) \longmapsto \Big(\mathcal{O}(Y) \xrightarrow{f^*} \mathcal{O}(X)\Big)\end{gathered}$$

is a (contravariant) *equivalence of categories*.

(*c*) **Lots of stuff about categories:** Let $\mathcal{A}$ be some category, $X, Y \in \operatorname{Ob}(\mathcal{A})$ be objects of $\mathcal{A}$ and $X \xrightarrow{f} Y$ a morphism in $\mathcal{A}$. We say that f is an *isomorphism* in $\mathcal{A}$ if there is a morphism $g \in \operatorname{Hom}_\mathcal{A}(Y, X)$ which is both left- and right-inverse (i.e. $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$).

A *covariant functor* $F\colon \mathcal{A} \to \mathcal{B}$ between categories consists of a map associating an object $F(X) \in \operatorname{Ob}(\mathcal{B})$ to each $X \in \operatorname{Ob}(\mathcal{A})$ and, for objects $X, Y \in \operatorname{Ob}(\mathcal{A})$, a map $\operatorname{Hom}_\mathcal{A}(X, Y) \xrightarrow{F} \operatorname{Hom}_\mathcal{B}(F(X), F(Y))$ such that $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ and $F(\alpha \circ \beta) = F(\alpha) \circ F(\beta)$ for composable morphisms $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$. For a *contravariant functor*, one instead requires that F maps $\operatorname{Hom}_\mathcal{A}(X, Y) \xrightarrow{F} \operatorname{Hom}_\mathcal{B}(F(Y), F(X))$, $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ and $F(\alpha \circ \beta) = F(\beta) \circ F(\alpha)$.

Let $\mathcal{A}^{\mathrm{op}}$ (the *dual* or *opposite* category) be $\mathcal{A}$ with every morphism reversed, i.e. $\operatorname{Ob}(\mathcal{A}^{\mathrm{op}}) = \operatorname{Ob}(\mathcal{A})$ and $\operatorname{Hom}_{\mathcal{A}^{\mathrm{op}}}(X, Y) = \operatorname{Hom}_\mathcal{A}(Y, X)$ for all $X, Y \in \operatorname{Ob}(\mathcal{A})$ and the composition $\alpha \circ \beta$ in $\mathcal{A}^{\mathrm{op}}$ is given by $\beta \circ \alpha$ in $\mathcal{A}$ (with $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ in $\mathcal{A}$, hence $Z \xrightarrow{\beta} Y \xrightarrow{\alpha} X$ in $\mathcal{A}^{\mathrm{op}}$). Then, obviously, each covariant functor $\mathcal{A} \to \mathcal{B}$ corresponds to a covariant functor $\mathcal{A}^{\mathrm{op}} \to \mathcal{B}^{\mathrm{op}}$ and a contravariant functor $\mathcal{A}^{\mathrm{op}} \to \mathcal{B}$. Together with $(\mathcal{A}^{\mathrm{op}})^{\mathrm{op}} = \mathcal{A}$, the reader will easily find two sets of each four similar correspondences.

A (co- or contravariant) functor $F\colon \mathcal{A} \to \mathcal{B}$ is an *equivalence of categories* if it induces bijections $\operatorname{Hom}_\mathcal{A}(X, Y) \xrightarrow{\sim} \operatorname{Hom}_\mathcal{B}(F(X), F(Y))$ resp. $\operatorname{Hom}_\mathcal{B}(F(Y), F(X))$ and if every object $Y \in \operatorname{Ob}(\mathcal{B})$ is $\mathcal{B}$-isomorphic to $F(X)$ for some $X \in \operatorname{Ob}(\mathcal{A})$.

A *functormorphism* (or *natural transformation*) between functors $F, G\colon \mathcal{A} \to \mathcal{B}$ (both co- or both contravariant) is a map φ associating a morphism $F(X) \xrightarrow{\varphi_X} G(X)$ to each $X \in \mathrm{Ob}(\mathcal{A})$ such that for any morphism $X \xrightarrow{\alpha} Y$ in $\mathcal{A}$ the diagram

$$\begin{array}{ccc} F(X) & \xrightarrow{F(\alpha)} & F(Y) \\ {\scriptstyle\varphi_X}\downarrow & & \downarrow{\scriptstyle\varphi_Y} \\ G(X) & \xrightarrow{G(\alpha)} & G(Y) \end{array}$$

(if F, G are covariant)

resp.

$$\begin{array}{ccc} F(Y) & \xrightarrow{F(\alpha)} & F(X) \\ {\scriptstyle\varphi_Y}\downarrow & & \downarrow{\scriptstyle\varphi_X} \\ G(Y) & \xrightarrow{G(\alpha)} & G(X) \end{array}$$

(if F, G are contravariant)

commutes. If $F \xrightarrow{\varphi} G \xrightarrow{\psi} H$ are functormorphisms, then so is $F \xrightarrow{\psi\circ\varphi} H$ defined by $(\psi\circ\varphi)_X = \psi_X \circ \varphi_X$. Obviously, there is a functormorphism $F \xrightarrow{\mathrm{id}_F} F$ given by $(\mathrm{id}_F)_X = \mathrm{id}_F(X)$. We thus have a *category* of co- resp. contravariant functors $\mathcal{A} \xrightarrow{F} \mathcal{B}$ between given categories $\mathcal{A}, \mathcal{B}$.

(*d*) Let $F\colon \mathcal{A} \to \mathcal{B}$ be co- or contravariant functor. We call F faithful (respectively fully faithful) if for objects X, Y of $\mathcal{A}$ the map $\mathrm{Hom}_{\mathcal{A}}(X, Y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{B}}(FX, FY)$ (respectively $\mathrm{Hom}_{\mathcal{A}}(X, y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{B}}(FY, FX)$ if F is contravariant) is injective (if F is to be faithful) or bijective (if F is to be fully faithful). It is *essentially surjective* if every object M of $\mathcal{B}$ is isomorphic to $F(X)$ for some $X \in \mathcal{A}$. F is an equivalence of categories, if it is fully faithful and essentially surjective.

(*e*) Assuming the Axiom of choice, a functor $\mathcal{A} \xrightarrow{F} \mathcal{B}$ is an equivalence of categories iff there is an inverse functor $\mathcal{B} \xrightarrow{G} \mathcal{A}$ (contravariant iff F is) such that there are functormorphisms $FG \simeq \mathrm{id}_{\mathcal{B}}$ and $GF \simeq \mathrm{id}_{\mathcal{A}}$. To construct G, chose for any object M of $\mathcal{B}$ an object X_M of $\mathcal{A}$ with an isomorphism $j_M\colon F(X_M) \xrightarrow{\sim} X$. Put $G(M) = X_M$ and $G(M \xrightarrow{\mu} N)$ is determined by the commutativity of

$$\begin{array}{ccc} F(G(M)) & \xrightarrow{F(G(\mu))} & F(G(N)) \\ {\scriptstyle\wr}\downarrow{\scriptstyle j_M} & & \downarrow{\scriptstyle\wr j_N} \\ M & \xrightarrow{\mu} & N \end{array}$$

Corollary 3. *The contravariant functor $X \xmapsto{F} \mathcal{O}(X)$ from the categoriy of affine algebraic varieties over k to the category of k-algebras of finite type which are domains is an equivalence of categories.*

Proof. By Proposition 3 it is fully faithful. To demonstrate essential surjectivity, let A be a k-algebra of finite type which is a domain. As it is of finite type, there is a surjective ring homomorphism $R = k[X_1, \ldots, X_n] \xrightarrow{\varphi} A$, for some finite n. If $\mathfrak{p} = \ker(\varphi)$ then $A \simeq R/\mathfrak{p}$ and the fact, that A is a domain implies, that $\mathfrak{p} \in \mathrm{Spec}(R)$. By Proposition 2, $\mathcal{O}(X) \simeq R/\mathfrak{p} \simeq A$ where $X = V(\mathfrak{p})$ is an affine algebraic variety in k^n, establishing essential surjectivity. *q.e.d.*

Fact. If $\mathcal{A} \xrightarrow{F} \mathcal{B}$ is an equivalence of categories (or even fully faithful) and $X \xrightarrow{\varphi} Y$ a morphism in $\mathcal{A}$, then φ is an isomorphism in $\mathcal{A}$ iff $F(\varphi)$ is isomorphism in $\mathcal{B}$. Indeed, if $F(Y) \xrightarrow{g} F(X)$ is inverse to $f = F(\varphi)$ then $g = F(\gamma)$ for a unique $Y \xrightarrow{\gamma} X$ as F is fully faithful. Using that F is fully faithful, one easily checks, that γ and φ are inverse.

Corollary 4. *If X and Y are affine algebraic varieties (or isomorphic to affine ones) and $X \xrightarrow{f} Y$ is a morphism such that $\mathcal{O}(Y) \xrightarrow{f^*} \mathcal{O}(X)$ is an isomorphism, then f is one.*

Proposition 4. *Let $X = V(\mathfrak{p}) \subseteq k^n$ be an affine algebraic variety in k^n and $f \in \mathcal{O}(X)$. Then the quasi affine variety $X \setminus V(f)$ is isomorphic to an affine one, namely to $V(\mathfrak{q}) \subseteq k^{n+1}$ where $\mathfrak{q} \subseteq S = k[X_1, \ldots, X_{n+1}]$ is generated by the elements of $\mathfrak{p}$ (viewed as elements of S which do not depend on X_{n+1}) and*

$$g = 1 - X_{n+1}\widetilde{f}(X_1, \ldots, X_n) \,,$$

where $\widetilde{f} \in R = k[X_1, \ldots, X_n + 1]$ is any preimage of f under $R \to R/\mathfrak{p} \simeq \mathcal{O}(X)$.

Proof. Obviously, $\mathfrak{q}$ is an ideal in S (which can (and will) be shown to be prime, but we don't need this right now) which is independent of the choice of $\widetilde{f}$. We have maps

$$\begin{aligned} V(\mathfrak{q}) &\longrightarrow X \setminus V(f) \\ (x_1, \ldots, x_{n+1}) &\overset{\pi}{\longmapsto} (x_1, \ldots, x_n) \\ \left(x_1, \ldots, x_n, \frac{1}{f(x_1, \ldots, x_n)}\right) &\overset{\iota}{\longmapsto} (x_1, \ldots, x_n) \end{aligned} \tag{$*$}$$

It is easily seen form the definition of $\mathcal{O}$ that $\frac{1}{f} \in \mathcal{O}(X \setminus V(f))$. Hence, ι is continuous, as well as π (obviously). By definition of $\mathfrak{q}$, one easily obtains that π and ι are in fact inverse to each other. Thus, $V(\mathfrak{q})$ is homeomorphic to $X \setminus V(f)$. Since the latter is irreducible (as an open and thus dense subset of the irreducible X), so is $V(\mathfrak{q})$, hence it is an affine algebraic variety and the maps in ($*$) are morphisms of algebraic varieties, which are inverse to each other. *q.e.d.*

Remark. By Fact 1 it follows that the *affine open subsets* (open subsets which are isomorphic to affine algebraic varieties) form a base of the topology of any quasi-affine algebraic varieties.

Corollary 5. *Let X be quasi-affine and $x \in X$, then there is a neighbourhood U of x which is isomorphic to an affine algebraic variety.*

Remark 3 (or maybe 2, who knows? But sparrows are butterflies, so who cares?)**.** If $n \geq 2$ then $k[X_1, \ldots, X_n] \xrightarrow{\sim} \mathcal{O}(k^n \setminus \{0\})$. Hence the inclusion $k^n \setminus \{0\} \to k^n$ induces an isomorphism $\mathcal{O}(k^n) \xrightarrow{\sim} \mathcal{O}(k^n \setminus \{0\})$. But $k^n \setminus \{0\} \to k^n$ cannot be isomorphic. As k^n is affine, by Corollary 4 $k^n \setminus \{0\}$ mus fail to be affine. The proof of our claim about $\mathcal{O}(k^n \setminus \{0\})$ follows from

Proposition 5. *If $Z \subseteq k^n$ is Zariski-closed, then any element f of $\mathcal{O}(k^n \setminus Z)$ has the form $f = \frac{p}{q}$ where p, q are elements of $R = k[X_1, \ldots, X_n]$ where $V(q) \cap (k^n \setminus Z) = \emptyset$.*

Proof. The proof given in the lecture was quite messy, so we decided to do the technical details somewhat differently.

Let $\Omega = k^n \setminus Z$. By definition of $\mathcal{O}(\Omega)$, there is a non-empty open subset $U \subseteq \Omega$ such that $f = \frac{p}{q}$ on U, where $p, q \in R$ are polynomials such that $V(q) \cap U = \emptyset$. Let

$$\frac{p}{q} = u \prod_{(\pi) \in \operatorname{Spec} R} \pi^{\nu_\pi}$$

be the prime factorization of $\frac{p}{q}$ in the unique factorization domain R with $u \in R^\times$ a unit and $\nu_\pi \in \mathbb{Z}$. Let

$$p_0 = u \prod_{\substack{(\pi)\in \operatorname{Spec} R \\ \nu_\pi \geq 1}} \pi^{\nu_\pi} \quad \text{and} \quad q_0 = \prod_{\substack{(\pi)\in \operatorname{Spec} R \\ \nu_\pi \leq -1}} \pi^{-\nu_\pi} \ .$$

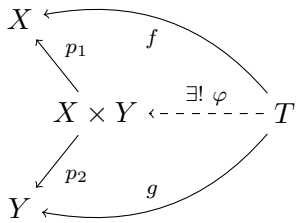
Then $f = \frac{p_0}{q_0}$ and for any polynomials $p, q \in R$ such that $\frac{p}{q} = \frac{p_0}{q_0}$ (as an identity in the quotient field $k(X_1, \ldots, X_n)$ of R) there must be some $\lambda \in R$ with $p = \lambda p_0, q = \lambda q_0$.

Now let $x \in \Omega$. We find an open neighbourhood $x \in V \subseteq \Omega$ and polynomials $p, q \in R$ such that $f = \frac{p}{q}$ on V and $V(q) \cap V = \emptyset$. Since any two non-empty Zariski-open subsets of k^n intersect, we have $pq_0 = p_0 q$ on the open and thus Zariski-dense subset $U \cap V \subseteq k^n$ (recall that $k^n = V(\{0\})$ is irreducible since $\{0\} \subseteq R$ is prime). As polynomials are continuous, we get $pq_0 = p_0 q$ on all of k^n and hence, by Hilbert's Nullstellensatz, as an identity in R. Now since $q_0 \mid q$ and $V(q) \cap V = \emptyset$ we also have $V(q_0) \cap V = \emptyset$. Therefore, $f = \frac{p_0}{q_0}$ on V, proving the assertion. *q.e.d.*

Proposition 6. *Let $X \subseteq k^m$ and $Y \subseteq k^n$ be quasi-affine algebraic varieties. Then $X \times Y \subseteq k^{m+n}$ is quasi-affine and, together with the two projections $X \xleftarrow{p_1} X \times Y \xrightarrow{p_2} Y$, $x \leftarrow\!\shortmid (x, y) \mapsto\!\shortmid y$, satisfies the universal property of the* product *of X and Y in the category of quasi-affine algebraic varieties over k. That is,*

$$\begin{aligned} \operatorname{Hom}(T, X \times Y) &\longrightarrow \operatorname{Hom}(T, X) \times \operatorname{Hom}(T, Y) \\ f &\longmapsto (p_1 f, p_2 f) \end{aligned}$$

is bijective for any object T of that category. Equivalently, if $T \xrightarrow{f} X$ and $T \xrightarrow{g} Y$ are morphisms, then there is precisely one morphism $T \xrightarrow{\varphi} X \times Y$ such that the following diagram commutes



Moreover, if X and Y are affine then so is $X \times Y$ and the canonical linear map

$$\begin{aligned} \mathcal{O}(X) \otimes \mathcal{O}(Y) &\longrightarrow \mathcal{O}(X \times Y) \\ f \otimes g &\longmapsto h(x, y) = f(x) g(y) \ , \end{aligned}$$

is an isomorphism.

Remark. (a) Arbitrary products in any category $\mathcal{A}$ must satisfy

$$\operatorname{Hom}_{\mathcal{A}}\left(T, \prod_{\lambda\in\Lambda} X_\lambda\right) \xrightarrow{\sim} \prod_{\lambda\in\Lambda} \operatorname{Hom}_{\mathcal{A}}(T, X_\lambda)$$

for any T, where $P = \prod_{\lambda\in\Lambda} X_\lambda$ is equipped with morphisms $P \to X_\lambda$. This universal properties uniquely determines P if it exists. The empty product is the *final object*, characterized

up to unique isomorphism by the requirement that $\mathrm{Hom}_{\mathcal{A}}(T, F)$ has for every object T of $\mathcal{A}$ precisely one element. In the categories of sets, abelian groups, R-modules, rings the products are given by the usual (possibly infinite) product set, together with the product structures and the projections to each factor. The empty product in the category of varieties is the one-point variety.

(*b*) A *coproduct* or *dual product* $\coprod_{\lambda\in\Lambda} X_\lambda$ in $\mathcal{A}$ is an object of $\mathcal{A}$ together with the morphisms $X_\lambda \xrightarrow{i_\lambda} \coprod_{\lambda\in\Lambda} X_\lambda$ such that the universal property is fulfilled, i.e.

$$\begin{aligned}\mathrm{Hom}_{\mathcal{A}}\left(\coprod_{\lambda\in\Lambda}, T\right) &\xrightarrow{\sim} \prod_{\lambda\in\Lambda} \mathrm{Hom}_{\mathcal{A}}(X_\lambda, T)\\ f &\longmapsto (fi_\lambda)_{\lambda\in\Lambda}\end{aligned}$$

is bijective.

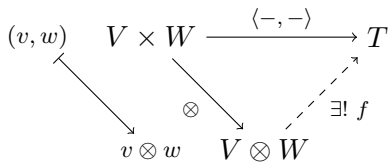
In particular, empty coproducts are *initial* objects I characterized by $|\mathrm{Hom}_{\mathcal{A}}(I, T)| = 1$ for any object T. In the category of sets, groups, abelian groups, R-modules, rings the initial objects are $\emptyset$, $\{0\}$, $\{0\}$, $\{0\}$, $\mathbb{Z}$ and $X \amalg Y$ is the disjoint union of X and Y, (complicated), $X \times Y$, $X \times Y$, $X \otimes_{\mathbb{Z}} Y$. If Λ is arbitrary and for abelian groups or R-modules,

$$\coprod_{\lambda\in\Lambda} = \left\{ (x_\lambda) \in \prod_{\lambda\in\Lambda} X_\lambda \;\middle|\; x_\lambda = 0 \text{ for all but finitely many } \lambda \right\} .$$

(*c*) The tensor product $V \otimes_k W$, together with $V \times W \xrightarrow{\otimes} V \otimes W$, $(v, w) \mapsto v \otimes w$ (which must be k-bilinear) is characterized by the universal property

$$\begin{aligned}\mathrm{Hom}_k(V \otimes W, T) &\longrightarrow \mathrm{Bil}_k(V \times W, T)\\ (V \otimes W \xrightarrow{f} T) &\longmapsto B(v, w) \coloneqq f(v \otimes w) ,\end{aligned}$$

$\mathrm{Bil}_k(V \times W, T)$ denoting the set of k-bilinear maps $V \times W \to T$. Equivalently, for every k-bilinear map $V \times W \xrightarrow{\langle -,-\rangle} T$ there is precisely one linear map $V \otimes W \xrightarrow{f} T$ such that the following diagram commutes



Proof of Proposition 6. Let X and Y be affine $X = V(\mathfrak{p})$, $Y = V(\mathfrak{q})$. Then $X \times Y = V(I)$ where I is the ideal generated by $\{(x, y) \mapsto f(x) \mid f \in \mathfrak{p}\}$ and $\{(x, y) \mapsto g(y) \mid g \in \mathfrak{q}\}$. Thus, $X \times Y$ is closed. Let $X \times Y = A \cup B$ with A and B closed in $X \times Y$. Then for each $y \in Y$ we have $X = A_y \cup B_y$ where $A_y = \{x \in X \mid (x, y) \in A\}$ and $B_y = \{x \in X \mid (x, y) \in B\}$ are easily seen to be closed. As X is irreducible, this implies that for each $y \in Y$ the condition $A_y = X$ or $B_y = X$ are satisfied. Thus, $Y = \widetilde{A} \cup \widetilde{B}$ where $\widetilde{A} = \{y \in A_y \mid A_y = X\}$ and $\widetilde{B} = \{y \in Y \mid B_y = x\}$ turn out to be closed, e.g. $\widetilde{A} = \bigcap_{x\in X} A^{(x)}$ with $A^{(x)} = \{y \in Y \mid (x, y) \in S\}$. Thus, $Y = \widetilde{A}$ or $Y = \widetilde{B}$ and $X \times Y = A$ or $X \times Y = B$, proving that $X \times Y$ is irreducible.

If X and Y are quasi-affine then $X \subseteq \overline{X}$ and $Y \subseteq \overline{Y}$ with $\overline{X}, \overline{Y}$ affine. Then $X \times Y$ is open in $\overline{X} \times \overline{Y}$ (since both $(\overline{X} \setminus X) \times \overline{Y}$ and $\overline{X} \times (\overline{Y} \setminus Y)$ are closed, similar to $X \times Y$ in the affine case), thus quasi affine. If T is any quasi-affine variety and $X \xleftarrow{f} T \xrightarrow{g} Y$ then, by Definition 4, $f = (f_1, \ldots, f_m)$ and $g = (g_1, \ldots, g_n)$ with $g_j, f_i \in \mathcal{O}(T)$ and $T \xrightarrow{(f,g)} X \times Y$, $(f, g) = (f_1, \ldots, f_m, g_1, \ldots, g_n)$ is a uniquely determined morphism of quasi-affine varieties whose projections to the two factors are f and g.

It remains to prove that $\mathcal{O}(X) \otimes_k \mathcal{O}(Y) \xrightarrow{\sim} \mathcal{O}(X \times Y)$. This morphism is surjective because, by Proposition 2, the target space is generated by monomials $x_1^{\alpha_1} \cdots x_m^{\alpha_m} y_1^{\beta_1} \cdots y_n^{\beta_n}$ in (x, y) and such a monomial is the image of $x^\alpha \otimes_k y^\beta$. Assume that $h \in \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$ is in the kernel. There are finite-dimensional subspaces $V \subseteq \mathcal{O}(X)$ and $W \subseteq \mathcal{O}(Y)$ such that $h \in V \otimes_k W$. Let $(f_i)_{i=1}^a$ and $(g_j)_{j=1}^b$ be bases of V and W, then $h = \sum_{i=1}^a \sum_{j=1}^b c_{i,j} f_i \otimes_k g_j$. That h is in the kernel of $\mathcal{O}(X) \otimes_k \mathcal{O}(Y) \xrightarrow{\sim} \mathcal{O}(X \times Y)$ is equivalent to

$$\sum_{i=1}^{a} \sum_{j=1}^{b} c_{i,j} f_i(x) g_j(y) = \sum_{j=1}^{b} \left(\sum_{i=1}^{a} c_{i,j} f_i(x) \right) g_j(y) = 0 \quad \text{for all } x \in X \text{ and } y \in Y \,.$$

As the $(g_j)_{j=1}^b$ are k-linearly independent in $\mathcal{O}(Y)$ is follows that $\sum_{i=1}^a c_{i,j} f_i(x) = 0$ for all $x \in X$ and $j \leq b$. The f_i being k-linearly independent in $\mathcal{O}(X)$, this implies $c_{i,j} = 0$ for $i \leq a$ and $j \leq b$ and therefore $h = 0$. *q.e.d.*

Definition 5. Let X be a quasi-affine algebraic variety, $x \in X$. A *germ* (German: *Keim*) at x of a regular function on $X \times Y$ is an equivalence class of pairs (f, U) where U is an open neighbourhood of x and $f \in \mathcal{O}(U)$ and where $(f, U) \sim (g, V)$ if $f|_W = g|_W$ for some open neighbourhood $W \subseteq U \cap V$ of x in X. The set of such germs is denoted by $\mathcal{O}_{X,x}$ (the *local ring* or *stalk* (German: *Keim*) of X at x) and it is a ring with ring operations

$$\big[(f, U)/_\sim\big] \circ \big[(g, V)/_\sim\big] = \big[(f|_{U \cap V} \circ g|_{U \cap V}, U \cap V)\big]/_\sim$$

for $\circ \in \{+, \cdot\}$.

Remark 4. (*a*) If $U \subseteq X$ open and $x \in U$ then $\mathcal{O}_{U,x} \xrightarrow{\sim} \mathcal{O}_{X,x}$ with $(f, W)/_\sim \mapsto (f, W)/_\sim$

(*b*) Every $\varphi \in \mathcal{O}_{X,x}$ has a unique value $\varphi(x)$ at x defined by $\varphi(x) = f(x)$ where $\varphi = (f, U)/_\sim$.

(*c*) In our situation, X is irreducible and $V(f|_{U \cap V} - g|_{U \cap V})$ is closed in the irreducible space $U \cap V$ in which any non-empty open subset W is dense. Hence, $(f, U) \sim (g, V)$ iff $f|_{U \cap V} = g|_{U \cap V}$.

(*d*) We have a ring homomorphism $\mathcal{O}_{X,x} \to k$, $\psi \mapsto \psi(x)$ of evaluation at x defined by $\psi(x) = f(x)$ when $\psi = (f, U)/_\sim$.

Definition 6. A *local ring* is a ring R satisfying the following equivalent conditions:

(*a*) The non-units of R form an ideal.

(*b*) The non-units of R form an maximal ideal.

(*c*) The set m-Spec(R) of maximal ideals of R has precisely one element.

Remark 5. (*a*) In particular the ring $\{0\}$ is not a local ring as it has no maximal ideals and no non-units.

(*b*) Recall the definitions: an ideal $\mathfrak{p}$ is prime iff $R/\mathfrak{p}$ is a domain which is equivalent to $1 \notin \mathfrak{p}$ and from $ab \in \mathfrak{p}$ follows $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. An ideal $\mathfrak{m}$ is maximal iff $R/\mathfrak{m}$ is a field, or equivalently, $1 \notin \mathfrak{m}$ and from $\mathfrak{m} \subseteq I \subseteq R$ it follows that $I = R$ or $I = \mathfrak{m}$.

(*c*) In $\mathcal{O}_{X,x}$, the ideal $\mathfrak{m}_x$ is maximal since $\mathcal{O}_{X,x}/\mathfrak{m}_x \xrightarrow{\sim} k$, $(\psi \mod x) \mapsto \psi(x)$ is an isomorphism. Let $\psi = (f, U)/_\sim \in \mathcal{O}_{X,x} \setminus \mathfrak{m}_x$, then $f(x) = \psi(x) \neq 0$ hence $V = U \setminus V(f)$ is an open neighbourhood of x. Let $h = \frac{1}{f}$ and $\eta = (h, V)$, then $\eta \cdot \psi = 1$. Hence, $\mathfrak{m}_x$ is the set of non-units in $\mathcal{O}_{X,x}$.

(*d*) *Proof of equivalence.* $(b) \to (a)$ is trivial.

$(a) \to (b)$ Let $\mathfrak{m}$ be the set of non-units. If $\mathfrak{m} \subseteq I \subseteq R$ and $I \neq R$, then all elements of I must be non-units, hence $\mathfrak{m} = I$. Also $1 \notin \mathfrak{m}$, so $\mathfrak{m}$ is maximal.

$(a) \to (c)$ Retaining the previous notation, any ideal $I \subsetneq R$ must not contain any unit, hence $I \subseteq \mathfrak{m}$ and $\mathfrak{m}$ is the only maximal ideal.

$(c) \to (a)$ (assuming that any ideal $I \subsetneq R$ is contained in some maximal ideal, which is implied by the axiom of choice) Let $\mathfrak{m}$ be the only maximal ideal. Then all elements of $\mathfrak{m}$ are non-units and for any non-unit $f \in R$, $fR \subsetneq R$ must be contained in some maximal ideal, hence $f \in \mathfrak{m}$. *q.e.d.*

Example 2. (*a*) The ring $\mathcal{O}_{X,x}$ is local.

(*b*) Any field is a local ring.

2.3. Localization of rings. The Spectrum of a ring.

Definition 1. We define the *spectrum* $\operatorname{Spec} R$ as the set of prime ideals of R and $\mathfrak{m}\text{-}\operatorname{Spec} R$ as the set of maximal ideals of R. We equip $\operatorname{Spec} R$ with the Zariski-Topology in which the closed sets are precisely the sets $V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq I\}$ where $I \subseteq R$ is any ideal.

Fact 1. Just like in the k^n-setting we have the following properties:

(*a*) $V(\sqrt{I}) = V(I)$

(*b*) $V\big(\sum_{\lambda\in\Lambda} I_\lambda\big) = \bigcap_{\lambda\in\Lambda} V(I_\lambda)$

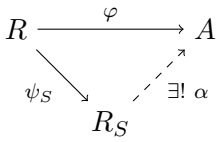
(*c*) $V(I \cdot J) = V(I \cap J) = V(I) \cup V(J)$

Definition 2. A subset $S \subseteq R$ is *multiplicative* if $1 \in S$ and $fg \in S$ for all $f, g \in S$.

Proposition 1. *Let R be a ring, $S \subseteq R$ a multiplicative subset, then there are a ring R_S (the* localization of R with respect to S*) with a ring homomorphism $R \xrightarrow{\psi=\psi_S} R_S$ such that the following properties hold:*

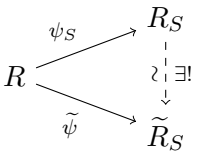
(a) $\psi_S(S) \subseteq R_S^\times$.

(b) *ψ_S has the universal property for ring homomorphisms with (a): If $R \xrightarrow{\varphi} A$ is any ring homomorphism with $\varphi(S) \subseteq A^\times$ then there is unique ring homomorphism $R_S \xrightarrow{\alpha} A$ such that*



commutes.

The properties (a) and (b) characterize R_S uniquely up to unique isomorphism: If $R \xrightarrow{\widetilde{\psi}} \widetilde{R}_S$ also satisfies (a) and (b), then there is a unique ring isomorphism $R_S \xrightarrow{\sim} \widetilde{R}_S$ such that



commutes.

Proof. Uniqueness: If $\widetilde{\psi}$ has the same universal property (up), then by the (up) of ψ there is a unique ring homomorphism $R_S \xrightarrow{i} \widetilde{R}_S$ such that $\widetilde{\psi} = i\psi$ and by the (up) of $\widetilde{\psi}$ there is a unique $\widetilde{R}_S \xrightarrow{j} R_S$ such that $\psi = j\widetilde{\psi}$. By the uniqueness part of the (up) of ψ and $\widetilde{\psi}$ any ring endomorphism a of R_S respectively b of $\widetilde{R}_S$ satisfying $a\psi = \psi$ respectively $b\widetilde{\psi} = \widetilde{\psi}$ must equal id_{R_S} respectively $\mathrm{id}_{\widetilde{R}_S}$. As $a = ji$ and $b = ij$ have these properties, it follows that i and j are inverse to each other, hence isomorphisms.

Construction of R_S: We take $R_S = (R \times S)/_\sim$ where $(r, s) \sim (\rho, \sigma)$ if there is a $t \in S$ such that $t\sigma r = ts\rho$. The proof that this is an equivalence relation which is respected by the ring operations is not hard but tedious and therefore will be left as an exercise to the reader. Remark that $\frac{r}{s}$ often denotes the equivalence class of (r, s). Then $\psi\colon R \to R_S$, $\psi(r) = \frac{r}{1}$ is a ring homomorphism satisfying

(a) as $\frac{1}{s} \in R_S$ is inverse to $\psi(s) = \frac{s}{1}$.

(b) If $R \xrightarrow{\varphi} A$ is as in (b) and $R_S \xrightarrow{\alpha} A$ is such that $\varphi = \alpha\psi$ then $\alpha\left(\frac{r}{s}\right) = \frac{\varphi(r)}{\varphi(s)}$ as $\varphi(s) \in A^\times$ and $\alpha\left(\frac{r}{s}\right)\varphi(s) = \alpha\left(\frac{r}{s}\right)\alpha(\psi(s)) = \alpha\left(\frac{r}{s} \cdot \frac{r}{1}\right) = \alpha\left(\frac{r}{1}\right) = \alpha(\psi(r)) = \varphi(r)$. Hence, α in (b) is unique. Conversely, $\alpha\left(\frac{r}{s}\right) := \frac{\varphi(r)}{\varphi(s)}$ is easily seen to be independent of the choice of representatives. Moreover, α is easily seen to be a ring homomorphism and $\alpha(\psi(r)) = \alpha\left(\frac{r}{1}\right) = \frac{\varphi(r)}{\varphi(1)} = \varphi(r)$.

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

Remark. When $S = f^{\mathbb{N}} = \{f^n \mid n \in \mathbb{N}\}$ the localization R_S is denoted R_f.

Fact 2. If R is a domain and $0 \notin S$ then $R_S = \left\{ \frac{r}{s} \in K \;\middle|\; r \in R, s \in S \right\}$ where K is the quotient field of R.

Example 1. If R is a domain, $S = R \setminus \{0\}$ is multiplicative subset and $R_S = K$ is the quotient field. If R is arbitrary, S the set of non-zero divisors is multiplicative and $R \xrightarrow{\psi_T} R_T$ is injective iff $T \subseteq S$.

Fact 3. Let $S \subseteq T$ be multiplicative subsets and $\widetilde{T}$ the image of T in R_S. Then there is a unique isomorphism $R_T \xrightarrow{\sim} (R_S)_{\widetilde{T}}$ such that the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\quad\psi_S\quad} & R_S \\ {\scriptstyle\psi_T}\downarrow & & \downarrow{\scriptstyle\psi_{\widetilde{T}}} \\ R_T & \xrightarrow[\exists!]{\sim} & (R_S)_{\widetilde{T}} \end{array}$$

Remark. We have $\psi_{\widetilde{T}}(\psi_S(T)) = \psi_{\widetilde{T}}(\widetilde{T}) \subseteq (R_S^\times)_{\widetilde{T}}$, hence the existence and uniqueness of the dotted ring morphism in the diagram.

Proof. By the universal properties (considering ring homomorphisms)

$$\begin{aligned} \operatorname{Hom}((R_S)_{\widetilde{T}}, A) &= \left\{ \alpha \in \operatorname{Hom}(R_S, A) \;\middle|\; \alpha(\widetilde{T}) \subseteq A^\times \right\} \\ &\simeq \left\{ \beta \in \operatorname{Hom}(R, A) \;\middle|\; \beta(S) \subseteq A^\times \text{ and } \alpha(\widetilde{T}) \subseteq A^\times \text{ for } \alpha = \beta\psi_S \right\} \\ &\simeq \left\{ \beta \in \operatorname{Hom}(R, A) \;\middle|\; \beta(T) \subseteq A^\times \right\} \\ &= \operatorname{Hom}(R_T, A) \end{aligned}$$

q.e.d.

Remark 1. $R \xrightarrow{\psi_S} R_S$ is injective iff S contains no zero-divisors. If $r \in R$, $s \in S$ and $sr = 0$, then $\psi_S(r) = 0$ as $\frac{r}{1} = \frac{0}{1}$ in R_S and vice versa. Thus, $\ker(R \xrightarrow{\psi_S} R_S) = \{r \in R \mid \exists s \in S \colon rs = 0\}$.

By the ring homomorphism $R \xrightarrow{\psi_S} R_S$, every R_S-module becomes an R-module (and R_S becomes an R-algebra).

Proposition 2. (*a*) *This functor from R_S-modules to R-modules is fully faithful and its essential image is the full subcategory of R-modules on which the elements of S act bijectively.*

(*b*) *If M is an R-module, there are an R-module M_S on which S acts bijectively and a morphism $M \xrightarrow{\varphi_S} M_S$ which has the following universal property determining is uniquely up to unique isomorphism. If N is some R-module on which S acts bijectively then any morphism $M \xrightarrow{\alpha} N$ uniquely determines a morphism $M_S \xrightarrow{\nu} N$ such that*

$$\begin{array}{ccc} M & \xrightarrow{\quad\alpha\quad} & N \\ & {\scriptstyle\varphi_S}\searrow \quad \nearrow{\scriptstyle\exists!\ \nu} & \\ & M_S & \end{array}$$

(c) *If $M \longrightarrow N$ is a morphism of R-modules, there is a unique morphism $M_S \longrightarrow N_S$ of R-modules such that*

$$\begin{array}{ccc} M & \longrightarrow & N \\ \downarrow & & \downarrow \\ M_S & \dashrightarrow & N_S \end{array}$$

commutes, making $(-)_S$ into a functor between R-modules and R_S-modules.

(d) *If $M \xrightarrow{\alpha} N$ is injective then $M_S \xrightarrow{\alpha_S} N_S$ is injective. We obtain a surjective map from the R-submodules of N to the R_S-submodules of N_S which maps M to the image of M_S in N_S. This becomes bijective when restricted to the R-submodules $M \subseteq N$ which S-saturated in the sense that $m \in N$, $s \in S$, $sm \in M$ implies $m \in M$. The inverse map sends an R_S-submodule $X \subseteq N_S$ to its preimage $\varphi_S^{-1}(X)$ under $N \xrightarrow{\varphi_S} N_S$.*

(e) *If $M \subseteq N$ is a submodule, then there is a unique morphism*

$$(N/M)_S \xrightarrow{\sim} N_S/(\textit{image of } M_S \textit{ in } N_S)$$

such that

$$\begin{array}{ccc} N & \longrightarrow & N/M \\ \downarrow & & \downarrow \\ N_S & & (N/M)_S \\ \downarrow & \overset{\exists!}{\overset{\sim}{\nearrow}} & \\ N_S/(\textit{image of } M_S) & & \end{array}$$

commutes.

Remark. Recall $\mathcal{A} \xrightarrow{F} \mathcal{B}$ faithful (fully faithful) if $\mathrm{Hom}_{\mathcal{A}}(X,Y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{B}}(F(X),F(Y))$ is injective (bijective). The essential image is the set (or class?) of all objects of $\mathcal{B}$ isomorphic to FX for some object X of $\mathcal{A}$. $\mathcal{C}$ is a subcategory of $\mathcal{B}$ iff the class of objects of $\mathcal{C}$ is a subclass of the class of objects of $\mathcal{B}$, $\mathrm{Hom}_{\mathcal{C}}(X,Y) \subseteq \mathrm{Hom}_{\mathcal{B}}(X,Y)$ for all objects X, Y of $\mathcal{C}$ respecting compositions of morphisms and such that every id_X in $\mathcal{C}$ is in $\mathrm{Hom}_{\mathcal{B}}(X,X)$. Then, there is an inclusion functor $\mathcal{C} \longrightarrow \mathcal{B}$ given by identities on objects and morphisms which is faithful. It is fully faithful iff $\mathrm{Hom}_{\mathcal{C}}(X,Y) = \mathrm{Hom}_{B}(X,Y)$ for all objects X, Y of $\mathcal{C}$. In this case, $\mathcal{C}$ is said to be a *full subcategory* of $\mathcal{B}$. For instance, finite dimensional k-vector spaces with linear maps between them form a full subcategory of all k-vector spaces.

We may say that functors $\mathcal{A} \xrightarrow{L} \mathcal{B}$ and $\mathcal{A} \xleftarrow{R} \mathcal{B}$ form an adjoint functor pair, with L being left adjoint to R and R right adjoint to L, if we are given canonical bijections

$$\mathrm{Hom}_{\mathcal{A}}(X, RY) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{B}}(LX, Y).$$

In our example $\mathcal{B}$ are the R_S-modules, $\mathcal{A}$ the R-modules, R the functor from Proposition 2(a) and $L : M \mapsto M_S$.

Other examples:

- $\mathcal{B}$: R-modules, $\mathcal{A}$: Set, R: forgetful functor, $L(X)$ the free module generated by X
- $\mathcal{B}$: groups, $\mathcal{A}$: Set, R: forgetful functor, $L(X)$ the free group generated by X
- $\mathcal{B}$: compact spaces, $\mathcal{A}$: Set, R: forgetful functor, $L(X)$ the Stone-Čech compactification of X

Proof of Proposition 2. (a) The fact that all modules in the image, and thus in the effective image, have S acting bijectively is trivial. If S act bijectively on M, we let $s^{-1} : M \longrightarrow M$ denote the inverse of $M \xrightarrow{s\cdot} M$ and define the structure of an R_S-module by $\frac{r}{s} \cdot m = s^{-1}(r \cdot m)$. If $\frac{r}{s} = \frac{\rho}{\sigma}$ in R_S, there is $t \in S$ such that $t\sigma r = ts\rho$ and $s^{-1}r \cdot m = (ts\sigma)^{-1}\sigma t r \cdot m = (ts\sigma)^{-1}st\rho \cdot m = \sigma^{-1}\rho \cdot m$. It is easy to see that this is OK ...

Similar for full faithfulness: If $M \xrightarrow{\alpha} N$ is any morphism of R-modules, with S acting bijectively on M and N, then $\alpha(s^{-1}m) = s^{-1}\alpha(m)$ and $\alpha(\frac{r}{s}) = \frac{r}{s}\alpha(m)$ for the R_S-module-structure defined before. which is the only one reproducing the original R-module structure ... (many tedious details left out).

(b) Similar to Proposition 1, we define $M_S = (M \times S)/_\sim$ where $(m, s) \sim (\mu, \sigma)$ if there is a $t \in S$ such that $t\sigma m = ts\mu$. Again, write $\frac{m}{s}$ for the equivalence class $(m, s)/_\sim$, and define the module operations in the obvious way, i.e.

$$r \cdot \frac{m}{s} = \frac{r \cdot m}{s} \quad \text{and} \quad \frac{m}{s} + \frac{\mu}{\sigma} = \frac{\sigma m + s\mu}{s\sigma} \quad \text{for all } m, \mu \in M,\ s, \sigma \in S\ .$$

It's easy (but tedious) to check, that M_S indeed has the desired properties.

(c) Easy.

(d) We just prove the injectivity of α_S. If $\alpha_S(\frac{m}{s}) = 0$ then $\frac{\alpha(m)}{s} = 0$ in N_S hence, there is $t \in S$ such that $\alpha(tm) = t\alpha(m) = 0$. But alpha is injective, hence $\alpha(tm) = 0$ implies $tm = 0$ hence $\frac{m}{s} = 0$ in M_S.

(e) Playing around with the definitions, one may check that

$$N_S/(\text{image of } M_S) = \{(n, s)\}_{m\in M, s\in S}/_\sim\ ,$$

where $(n, s) \sim (\nu, \sigma)$ for $n, \nu \in N,\ s, \sigma \in S$ iff there are $t \in S$ and $m \in M$ such that $ts\nu = t\sigma n + m$. On the other hand

$$(N/M)_S = \{(\overline{n}, s)\}/_\sim\ ,$$

such that $(\overline{n}, s) = (\overline{\nu}, s)$ iff there is a $t \in S$ such that $t\sigma n = ts\nu$ in N/M, i.e. $ts\nu = t\sigma n + m$ for some $m \in M$. The conclusion is easily deduced.

q.e.d.

Corollary 1. *Let $S \subseteq R$ be a multiplicative subset of a ring R.*

(a) *The localization of R as an R-module with respect to S is isomorphic to R_S, the localization as a ring.*

(*b*) *If M is a Noetherian R-module, M_S is a Noetherian R_S-Module.*

(*c*) *If R is a Noetherian ring, then so is R_S.*

(*d*) *Every ideal I of R_S has the form $I = J \cdot R_S$ where J is an ideal in R and we have a bijection*

$$\left\{ \begin{array}{c} \text{ideals } J \subseteq R \text{ which are } S\text{-saturated, i.e.} \\ (sr \in J \Rightarrow r \in J)\ \forall s \in S,\, r \in R \end{array} \right\} \xrightarrow{\sim} \{\text{ideals } I \subseteq R_S\}$$

$$J \longmapsto J \cdot R_S = \text{image of } J_S \text{ in } R_S$$
$$= \{\rho\psi_S(j) \mid \rho \in R_S,\, j \in J\}$$
$$\psi_S^{-1}(I) \longmapsto I\ .$$

(*e*) *Under this correspondence, we have*

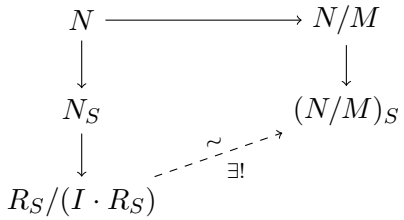
$$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\} \xrightarrow{\sim} \operatorname{Spec}(R_S)$$
$$\mathfrak{p} \longmapsto \mathfrak{q} = \mathfrak{p} \cdot R_S$$
$$\mathfrak{p} = \mathfrak{q} \sqcap R = \psi_S^{-1}(\mathfrak{q}) \longmapsto \mathfrak{q}$$

and this is a (Zariski-)homeomorphism if the l.h.s. is equipped with the induced subspace topology.

(*f*) *In the situation of (d), if $I \subseteq R$ is any ideal and $\widetilde{S}$ denotes the image of S in R/I, we have a unique isomorphism*

$$R_S/(I \cdot R_S) \xrightarrow{\sim} (R/I)_{\widetilde{S}}$$

such that the following diagram commutes



Proof. (*a*) Follows from our explicit construction of M_S and R_S.

(*b*) Denote $M \xrightarrow{\varphi_S} M_S$ the map to the localization. If $N_1 \subsetneq N_2 \subsetneq \ldots$ is a properly ascending chain of submodules in M_S, then so is $\varphi_S^{-1}(N_1) \subsetneq \varphi_S^{-1}(N_2) \subsetneq \ldots$ in M, but M is Noetherian.

(*c*) Special case of (b).

(*d*) This is the special case $M = R$ of the correspondence recapitulated at the beginning. The equality $J \cdot R_S \simeq$ (image of J_S in R_S) follows from

$$J \cdot R_S = \{\psi_S(j) \cdot \rho \mid \rho \in R_S, j \in J\} = \left\{ \frac{j}{1} \cdot \frac{r}{s} \in R_S \;\middle|\; j \in J, r \in R, s \in S \right\}$$
$$= \left\{ \frac{j'}{s} \;\middle|\; j' \in J, s \in S \right\} = \left\{ \text{image of } \frac{j'}{s} \in J_S \text{ in } R_S \;\middle|\; j' \in J, s \in S \right\}$$

(*e*) The bijection follows from (d) if the following facts are shown:

(α) $\mathfrak{p} \in \operatorname{Spec} R$ is S-saturated iff $\mathfrak{p} \cap S = \emptyset$. If $s \cdot 1 = s \in S \cap \mathfrak{p}$, then $\mathfrak{p}$ is not S-saturated as $1 \notin \mathfrak{p}$. If $\mathfrak{p} \cap S = \emptyset$ and $r \in R$, $s \in S$ and $r \cdot s \in \mathfrak{p}$, then $r \in \mathfrak{p}$ as $s \notin \mathfrak{p}$.

(β) If $\mathfrak{q} \in \operatorname{Spec}(R_S)$ then $\mathfrak{q} \sqcap R \in \operatorname{Spec} R$. If $A \xrightarrow{f} B$ is a ring homomorphism and $\mathfrak{q} \in \operatorname{Spec} B$, then $\mathfrak{p} = f^{-1}(\mathfrak{q}) \in \operatorname{Spec} A$. Indeed, we have $1 \notin \mathfrak{p}$ since $f(1) = 1 \notin \mathfrak{q}$. Moreover, if $ab \in \mathfrak{p}$ then $f(a)f(b) = f(ab) \in \mathfrak{q}$, hence $f(a) \in \mathfrak{q}$ (and $a \in \mathfrak{p}$) or $f(b) \in \mathfrak{q}$ (and $b \in \mathfrak{q}$). Applying ths to $R \longrightarrow R_S$ gives the assertion.

(γ) If $\mathfrak{p} \in \operatorname{Spec} R$ and $\mathfrak{p} \cap S = \emptyset$ then $\mathfrak{p} \cdot R_S \in \operatorname{Spec} R_S$. We have $R_S/\mathfrak{p} \cdot R_S \simeq (R/\mathfrak{p})_{\widetilde{S}}$ by (f), where $\widetilde{S}$ is the image of S in $R/\mathfrak{p}$. We have $0 \notin \widetilde{S}$ as $S \cap \mathfrak{p} = \emptyset$. But $R/\mathfrak{p}$ is a domain and by Fact 2, $(R/\mathfrak{p})_{\widetilde{S}}$ is a subring of the field of quotients of $R/\mathfrak{p}$, hence a domain.

The homeomorphism follows form the fact that any closed subset of $\operatorname{Spec}(R_S)$ has the form $V(I)$ and $I = J \cdot R_S$ for an ideal J in R. The preimage of $V(I) \subseteq \operatorname{Spec}(R_S)$ under the studied bijection is easily seen to be $\{\mathfrak{p} \in V(J) \mid \mathfrak{p} \cap S = \emptyset\}$, thus closed in the induced subspace topology, and all Zariski-closed subsets of $\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\}$ can be obtained in this way.

(*f*) This follows from the assertion about quotient modules in Proposition 2 or by a pushing universal properties around:

$$\begin{aligned}
\operatorname{Hom}(R_S/(J \cdot R_S), A) &\simeq \{f \in \operatorname{Hom}(R_S, A) \mid f(j) = 0 \ \forall j \in J \cdot R_S\} \\
&= \left\{ f \in \operatorname{Hom}(R_S, A) \;\middle|\; (J \xrightarrow{\psi_S} R_S \xrightarrow{f} A) = 0 \right\} \\
&\simeq \left\{ g = (f\psi_S) \in \operatorname{Hom}(R, A) \;\middle|\; g(S) \subseteq A^\times \text{ and } g|_J = 0 \right\} \\
&\simeq \left\{ \gamma \in \operatorname{Hom}(R/J, A) \;\middle|\; \gamma(\widetilde{S}) \subseteq A^\times \right\} \\
&\simeq \operatorname{Hom}((R/J)_{\widetilde{S}}, A)
\end{aligned}$$

where $g = \gamma \circ \pi$ with $R \xrightarrow{\pi} R/J$ denoting the projection to R/J.

q.e.d.

Remark. The constructed isomorphism maps

$$\frac{r}{s} \mod J \cdot R_S \longmapsto \frac{r \mod J}{s \mod J} .$$

Corollary 2. *If R is a Noetherian ring, then R_S is Noetherian.*

Proof. This is just Corollary 1. We got it, ok? *q.e.d.*

Corollary 3. $\operatorname{Spec} R_f \simeq \operatorname{Spec}(R) \setminus V(f)$ *(a homeomorphism), and open subsets of this form form a topology base of* $\operatorname{Spec} R$.

Proof. Indeed as $\mathfrak{p}$ is prime, $f^N \notin \mathfrak{p}$ for some $N \in \mathbb{N}$ is equivalent to $f \notin \mathfrak{p}$ which in turn is equivalent to $\mathfrak{p} \notin V(f)$.

Suppose that $U \ni \mathfrak{p}$ is an open neighbourhood of $\mathfrak{p}$, i.e. $U = \operatorname{Spec} R \setminus V(I)$ for some ideal $I \subseteq R$ such that $\mathfrak{p} \not\supseteq I$. Then there must be some $f \in I \setminus \mathfrak{p}$, hence $\mathfrak{p} \in \operatorname{Spec} R \setminus V(f) \subseteq U$. *q.e.d.*

Example 2. $R_f \simeq R[T]/(1 - T \cdot f)$.

Proof. Indeed, we have $Tf = 1$ in $A = R[T]/(1 - Tf)$, hence the image of f in A is in $A^\times$. If $R \xrightarrow{\beta} B$ is a ring homomorphism with $\beta(f) \in B^\times$, there is unique ring homomorphism $R[T] \xrightarrow{\gamma} B$ extending β and such that $\gamma(T) = \beta(f)^{-1}$. This annihilates $(1 - Tf)$, hence comes from a ring homomorphism

$$R[T]/(1 - Tf) \xrightarrow{\delta} B \,.$$

On the other side, for any such δ the homomorphism

$$\gamma \colon R[T] \longrightarrow R[T]/(1 - Tf) \xrightarrow{\delta} B$$

such that $\gamma|_R = \beta$ must send $1 - T \cdot f$ to 0, hence $\gamma(T) \cdot \gamma(f) = 1$ and $\gamma(T) = \beta(f)^{-1}$, hence δ is unique. *q.e.d.*

By comparison with Proposition 2.2.4, we obtain a special case of

Proposition 3. *Let X be a quasi-affine algebraic variety over an algebraically closed field k and $f \in \mathcal{O}(X)\setminus\{0\}$, then the unique ring homomorphism $\iota : \mathcal{O}(X)_f \xrightarrow{\sim} \mathcal{O}(X\setminus V(f))$ is an isomorphism.*

Proof. If X is affine, this follows from Proposition 2.2.4 and Example 2. We won't have to consider the quasi-affine case and the proof is omitted. *q.e.d.*

Remark. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then $S = R\setminus\mathfrak{p}$ is a multiplicative subset, and the image of S in $A = R/\mathfrak{p}$ is $A \setminus \{0\}$, hence $R_S/\mathfrak{p} \cdot R_S \simeq A_{\widetilde{S}}$ is the quotient field of $R/\mathfrak{p}$. Then $\mathfrak{m} = \mathfrak{p} \cdot R_S$ is a maximal ideal of R_S. In fact, if $\rho \in R_S \setminus \mathfrak{m}$ then $\rho = \frac{r}{s}$ with $s \in S = R \setminus \mathfrak{p}$, $r \in R \setminus \mathfrak{p}$ (as $\rho \in \mathfrak{p} \cdot R_S$ otherwise), hence $r \in S$ and $\frac{r}{s}$ is a unit (with inverse $\frac{s}{r}$) in R_S. It follows that R_S is a local ring with maximal ideal $\mathfrak{m}$. One puts $R_\mathfrak{p} \coloneqq R_S$ in this situation.

Remark. If $X \subseteq k^n$ affine and $x \in X$ corresponds to $\mathfrak{m} \in \mathfrak{m}\text{-Spec}(\mathcal{O}(X))$ (which, by Corollary 2.2.2, makes sense) then $\mathcal{O}(X)_\mathfrak{m} \simeq \mathcal{O}_{X,x}$.

Definition 3. Let $\mathfrak{p} \subseteq R$ be prime, $S = R \setminus \mathfrak{p}$, $R_\mathfrak{p} \coloneqq R_S$ is the localization of R at $\mathfrak{p}$. This a local ring with maximal ideal $\mathfrak{p} \cdot R_\mathfrak{p}$, for any $I \supsetneq \mathfrak{p} \cdot R_\mathfrak{p}$ must be given as $J \cdot R_\mathfrak{p}$ where $J \supsetneq \mathfrak{p}$, hence $J \cap S \neq \emptyset$ hence $J \cdot R_\mathfrak{p} = R_\mathfrak{p}$ since $1 = \frac{s}{s} \in J \cdot R_\mathfrak{p}$ with $s \in J \cap S$.

Proposition 4. *Let k be algebraically closed and X an affine algebraic variety in some k^n. Let $x \in X$ correspond to the maximal $\mathfrak{m}_x \subseteq \mathcal{O}(X)$, i.e. $\mathfrak{m}_x = \{f \in \mathcal{O}(X) \mid f(x) = 0\}$. Then the canonical morphism*

$$\mathcal{O}(X)_{\mathfrak{m}_x} \xrightarrow{\varphi} \mathcal{O}_{X,x}$$

(extending $\mathcal{O}(X) \to \mathcal{O}_{X,x}$ by the universal property of localization) is an isomorphism.

Proof. Suppose that $\frac{f}{s} \in \mathcal{O}(X)_{\mathfrak{m}_x}$ is in the kernel $\ker\varphi$, where $f, s \in \mathcal{O}(X)$, $s \notin \mathfrak{m}_x$. Then $s(x) \neq 0$, therefore the image of $\frac{f}{s}$ under φ is $\left(\frac{f|_U}{s|_U}, U\right)/\sim$ where U is any open neighbourhood of x where s

has no zeros. Hence, φ maps $\frac{f}{s}$ to 0 iff $f|_U = 0$ for sufficiently small U. As X is irreducible, U is dense and $f|_U = 0$ implies $f = 0$. Thus, φ is injective.

Let $\gamma \in \mathcal{O}_{X,x}$ then $\gamma = (g, U)/_\sim$ where U is an open neighbourhood of x and $g \in \mathcal{O}(U)$. By definition of $\mathcal{O}(U)$ it is possible to replace U by some smaller open neighbourhood U of x such that $g = \frac{f}{s}$ on U, where f and s are polynomials and $V(s) \cap U = \emptyset$. Then f and s define elements $\mathcal{O}(X)$ and $s \notin \mathfrak{m}_x$ and the image of $\frac{f}{s}$ in $\mathcal{O}_{X,x}$ is γ. Hence, φ is surjective. *q.e.d.*

Proposition 5. *Let $\mathfrak{p} \in \operatorname{Spec} R$, then $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is isomorphic to the quotient field of the domain $R/\mathfrak{p}$.*

Proof. From Corollary 1 we obtain that the prime ideals of R_S correspond to the S-saturated prime ideals of R. Applying this to $S = R \setminus \mathfrak{p}$, the image of S in $R/\mathfrak{p}$ is $(R/\mathfrak{p}) \setminus \{0\}$ and $(R/\mathfrak{p})_{(R/\mathfrak{p})\setminus\{0\}}$ is the quotient field of $R/\mathfrak{p}$. *q.e.d.*

2.4. Proof of $\dim(k^n) = n$

Proposition 1. *Let k be a field (not necessarily algebraically closed), A a k-algebra of finite type, and $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} A$ prime ideals such that $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$. Then*

$$\deg \operatorname{tr}(\mathfrak{K}(\mathfrak{p}_1)/k) > \deg \operatorname{tr}(\mathfrak{K}(\mathfrak{p}_2)/k) \ ,$$

where $\mathfrak{K}(\mathfrak{p})$ denotes the Quotient field of $R/\mathfrak{p}$ (see Proposition 2.3.5)

Lemma 1. *This holds when $\mathfrak{p}_2$ is a maximal ideal.*

Proof. In this case, $A/\mathfrak{p}_2$ is a finite field extension of k by the Hilbert Nullstellensatz (Theorem 4), hence $\deg \operatorname{tr}(\mathfrak{K}(\mathfrak{p}_2)/k) = 0$ and must show that $\deg \operatorname{tr}(\mathfrak{K}(\mathfrak{p}_1)/k) > 0$. Assume not, then $\mathfrak{K}(\mathfrak{p}_2)/k$ is algebraic. Since A is finitely generated as a k-algebra, so is $A/\mathfrak{p}_1$ and its quotient field is finitely generated as a field extension of k, hence finite if it is algebraic. In particular, $\mathfrak{K}(\mathfrak{p}_1)$ is a finite dimensional k-vector space, and the k-vector subspace $A/\mathfrak{p}_1 \subseteq \mathfrak{K}(\mathfrak{p}_1)$ must be finite-dimensional as well. Since $A/\mathfrak{p}_1$ is a domain, it is a field and $\mathfrak{p}_1$ must be maximal, contradicting $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$. *q.e.d.*

Lemma 2. *If $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ and the multiplicative subset $S \subsetneq A$ is disjoint from $\mathfrak{p}_2$, then $\mathfrak{p}_1 R_S \subsetneq \mathfrak{p}_2 R_S$ and these are prime ideals in R_S.*

Proof. Corollary 2.3.1 *q.e.d.*

Proof of Proposition 1. Pick an n-tuple $B = (b_1, \ldots, b_n)$ of elements of A whose images in $\mathfrak{K}(\mathfrak{p}_2)$ form a transcendence base of $\mathfrak{K}(\mathfrak{p}_2)/k$. To do so, choose the b_i to be representatives of a maximal k-algebraically independent subset of $A/\mathfrak{p}_2$. Then all elements of $A/\mathfrak{p}_2$ are algebraic over $k(b_1, \ldots, b_n)$. But the $k(b_1, \ldots, b_n)$-algebraic elements of $\mathfrak{K}(\mathfrak{p}_2)$ form a subfield, hence $\mathfrak{K}(\mathfrak{p}_2)/k(b_1, \ldots, b_n)$ is algebraic.

Let $S = \{f(b_1, \ldots, b_n) \mid f \in k[X_1, \ldots, X_n] \setminus \{0\}\}$. This is a multiplicative subset of A which is disjoint from $\mathfrak{p}_2$ by the k-algebraic independence of the images of the b_i in $\mathfrak{K}(\mathfrak{p}_2)$. Let $\widetilde{A} = A_S$, $\widetilde{\mathfrak{p}}_i = \mathfrak{p}_i \widetilde{A}$, then $\widetilde{\mathfrak{p}}_1 \subsetneq \widetilde{\mathfrak{p}}_2$ by Lemma 2. Let $R = k[X_1, \ldots, X_n]$, then A becomes an R-algebra by sending X_i to b_i and S is the image of $R \setminus \{0\}$. Hence, $\widetilde{A} = A_S$ becomes an algebra over

$R_{R\setminus\{0\}} = \widetilde{k}$, the quotient field of R. Since $\frac{1}{s} \in \widetilde{k}$ for $s \in S$, the images in $\widetilde{A}$ of any generators $a_1, \ldots, a_\ell$ of A as a k-algebra generate $\widetilde{A}$ as a $\widetilde{k}$-algebra. Also, $\mathfrak{K}(\mathfrak{p}_i) \xrightarrow{\sim} \mathfrak{K}\left(\widetilde{\mathfrak{p}}_i\right)$ because the elements of S are already units in $\mathfrak{K}(\mathfrak{p}_i)$. Since the images of the elements of B form a transcendence base for $\mathfrak{K}(\mathfrak{p}_2)/k$, $\mathfrak{K}(\mathfrak{p}_2)$ is algebraic over $\widetilde{k}$. Since $\widetilde{A}$ is a $\widetilde{k}$-algebra of finite type, $\mathfrak{K}(\mathfrak{p}_2) \simeq \mathfrak{K}\left(\widetilde{\mathfrak{p}}_2\right)$ is a finite $\widetilde{k}$-extension (it is finitely generated and algebraic) and $\widetilde{A}/\widetilde{\mathfrak{p}}_2 \subseteq \mathfrak{K}(\widetilde{\mathfrak{p}}_2)$ is a finite dimensional $\widetilde{k}$-algebra, i.e. a finite dimensional $\widetilde{k}$-vector subspace of $\mathfrak{K}(\widetilde{\mathfrak{p}}_2)$, hence a field and $\widetilde{\mathfrak{p}}_2$ is maximal. By Lemma 1, $\mathfrak{K}(\mathfrak{p}_1) \simeq \mathfrak{K}\left(\widetilde{\mathfrak{p}}_1\right)$ is not algebraic over $\widetilde{k}$. Since the image of B in $\mathfrak{K}(\mathfrak{p}_1)$ is k-algebraically independent but does not form a transcendence base (they generate $\widetilde{k}$ together with k), we have $\deg\operatorname{tr}(\mathfrak{K}(\mathfrak{p}_1)/k) > n = \#B = \deg\operatorname{tr}(\mathfrak{K}(\mathfrak{p}_2)/k)$. *q.e.d.*

Corollary 1. *If X is an affine algebraic variety in some k^n (with k an algebraically closed field) and $K(X)$ it's ring of rational functions (i.e. the quotient field of $\mathcal{O}(X)$), then*

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

Proof. By Corollary 2.2.2 there is an antimonotonic bijection between closed subsets of X and ideals $I \subseteq \mathcal{O}(X)$ coinciding with their radicals $\sqrt{I}$, with irreducibles corresponding to prime ideals. If $Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_d = X$ is a chain of irreducible subsets terminating at X and $\mathfrak{p}_i = \{f \in \mathcal{O}(X) \mid f|_{Z_i} = 0\}$ denotes the corresponding prime ideals, then $(0) = \mathfrak{p}_d \subsetneq \ldots \subsetneq \mathfrak{p}_0$. By Proposition 1,

$$\deg\operatorname{tr}\left(K(X)/k\right) = \deg\operatorname{tr}\left(\mathfrak{K}(\mathfrak{p}_d)/k\right) > \deg\operatorname{tr}\left(\mathfrak{K}(\mathfrak{p}_{d-1})/k\right) > \ldots > \deg\operatorname{tr}\left(\mathfrak{K}(\mathfrak{p}_0)/k\right) \geq 0 \ ,$$

hence $\deg\operatorname{tr}(K(X)/k) \geq d$. *q.e.d.*

Corollary 2. $\dim(k^n) = n$.

Proof. The fact that $\dim(k^n) \geq n$ follows from $k^n \supsetneq k^{n-1} \times \{0\} \supsetneq \ldots \supseteq k \times \{0\}^{n-1} \supsetneq \{0\}^n$ being irreducible subsets (Remark 2.1.4). Putting $X = k^n$ we have $\mathcal{O}(X) = k[X_1, \ldots, X_n]$ by Proposition 2.2.2, hence $K(X) = k(X_1, \ldots, X_n)$ has transcendence degree n over k and $\deg\operatorname{tr}(K(X)/k) \leq n$ by Corollary 1. *q.e.d.*

Corollary 3. *Let X be a quasi-affine algebraic variety in k^n and $K(X)$ the quotient field of $\mathcal{O}(X)$. Then* $\dim(X) \leqslant \deg\operatorname{tr}(K(X)/k)$.

Remark. If algebraic varietes in general are defined as on the exercise sheet, one has to define (for irreducible X)

$$K(X) = \{(f, U)\}/_\sim \quad \text{where } U \subseteq X \text{ open}, \ f \in \mathcal{O}(U) \ ,$$

and we set $(f, U) \sim (g, U)$ iff $f|_{U\cap V} = g|_{U\cap V}$ (This can be weakened to $f|_W = g|_W$ on an open subset $W \subseteq U \cap V$. If $f - g$ vanishes on the open and thus dense subset $W \subseteq U \cap V$, it must vanish on all of $U \cap V$ since f and g are continuous.), which turns out to be an equivalence relation. Then (it can be shown that) $\dim(X) = \deg\operatorname{tr}(K(X)/k)$ and $\operatorname{codim}(Z, X) = \dim(X) - \dim(Z)$ for any irreducible $Z \subseteq X$.

Proof of Corollary 3.. Let $X \subseteq \overline{X} \subseteq k^n$. The closure $\overline{X}$ of X is irreducible, hence so is X and

there is a bijection

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

(somewhere on an exercise sheet (on #6, that is)), hence $\dim(X) \leq \dim(\overline{X})$. We want to show that $K(X) \simeq K(\overline{X})$. To do so, we use the fact that there is some $f \in \mathcal{O}(\overline{X}) \setminus \{0\}$ such that $W := \overline{X} \setminus V(f) \subseteq X$ (by Fact 2.2.1, the open subsets $\overline{X} \setminus \{0\}$, $f \in \mathcal{O}(\overline{X})$ form a topology base of $\overline{X}$). Since W is dense in X and $\overline{X}$, we may identify $\mathcal{O}(X)$ and $\mathcal{O}(\overline{X})$ with subrings B and A of $\mathcal{O}(W)$, where $A \subseteq B \subseteq \mathcal{O}(W)$. By Proposition 2.3.3 we have $\mathcal{O}(W) = A_f$, hence A and $\mathcal{O}(W)$ have the same quotient fields. But then the quotient field of B must coincide with $K(\overline{X}) = K(W)$ as well. *q.e.d.*

Remark. In particular, we proved that if X is affine in k^n and $U \subseteq X$ is open and nonempty, then $K(X) \simeq K(U)$.

We would like to prove the opposite inequality to Corollary 1. Our strategy will be to use the Noether normalization theorem. There are $f_1, \ldots, f_d \in \mathcal{O}(X)$ algebraically independent over k, such that $\mathcal{O}(X)$ is integral (and finitely generated, hence finite) over $k[f_1, \ldots, f_d]$. Then

$$X \xrightarrow{(f_1,\ldots,f_d)} k^d$$

is a *finite morphism* in the terminology of modern algebraic topology and one would hope to lift the chain

$$\{0\}^d \subsetneq k \times \{0\}^{d-1} \subsetneq k^2 \times \{0\}^{d-2} \subsetneq \ldots \subsetneq k^d$$

of irreducible subsets of k^d to a chain of irreducible subsets of X of the same length, which would establish equality in Corollary 1. At this point, the going-up and going down theorem of Krull (who certainly was a *n00b* compared to Grothendieck) and Cohen/Seidenberg are our friends and will be proved in the next section.

2.5. Lifting of prime ideals to integral extension rings

Definition 1. Let $A \xrightarrow{f} B$ be a ring homomorphism.

(*a*) We say that *going-up* holds for f if for arbitrary prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ of A and every prime ideal $\widetilde{\mathfrak{p}}$ of B lying *above* $\mathfrak{p}$ (in the sense that $\mathfrak{p} \sqcap A = f^{-1}(\widetilde{\mathfrak{p}})$ equals $\mathfrak{p}$), there is a prime ideal $\widetilde{\mathfrak{q}} \supseteq \widetilde{\mathfrak{p}}$ of B which is above $\mathfrak{q}$ (in the sense that $\mathfrak{q} = f^{-1}(\widetilde{\mathfrak{q}})$).

(*b*) We say that f satisfies *going-down* if for all prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ of A and $\widetilde{\mathfrak{q}} \in \operatorname{Spec} B$ above $\mathfrak{q}$, there exists a prime ideal $\widetilde{\mathfrak{p}} \subseteq \mathfrak{q}$ above $\mathfrak{p}$.

Fact 1. Let $X \xrightarrow{f} Y$ be a morphism of affine algebraic varieties. Let $U \subseteq Y$ be open. In Definition 2.2.4 we constructed a ring homomorphism

$$\begin{aligned} f^* \colon \mathcal{O}_Y(U) &\longrightarrow \mathcal{O}_X(f^{-1}U) \\ \lambda &\longmapsto \lambda \circ f \ . \end{aligned}$$

If $x \in X$, $y = f(x)$ we have a ring homomorphism (also denoted f^*) $\mathcal{O}_{Y,y} \xrightarrow{f^*} \mathcal{O}_{X,x}$ sending $(\lambda, W)/_\sim$ to $(f^*\lambda, f^{-1}W)/_\sim$ (where $W \subseteq Y$ is an open neighbourhood of y and $\lambda \in \mathcal{O}_Y(W)$).

(*a*) The preimage of $\mathfrak{m}_{X,x} \subseteq \mathcal{O}_{X,x}$ under f^* is $(f^*)^{-1}\mathfrak{m}_{X,x} = \mathfrak{m}_{Y,y}$ (where $\mathfrak{m}_{X,x}$, $\mathfrak{m}_{Y,y}$ denote the maximal ideals of the stalks $\mathcal{O}_{X,x}$ and $\mathcal{O}_{Y,y}$).

(*b*) If $I \subseteq \mathcal{O}_X(X)$ is an ideal, then $V((f^*)^{-1}I) = \overline{f(V(I))}$ (the closure with respect to the Zariski topology on Y). If $V(I)$ is irreducible in X then so is $f(V(I))$ in Y and the diagram (of sets)

$$\begin{array}{ccccc}
 & & K \longmapsto \widetilde{\mathfrak{p}} = \{f \in B \mid f|_K = 0\} & & \\
 & & K = V\left(\widetilde{\mathfrak{p}}\right) \longmapsfrom \widetilde{\mathfrak{p}} & & \\
 & \left\{ \begin{array}{c} \text{irreducible subsets} \\ K \subseteq X \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{prime ideals} \\ \widetilde{\mathfrak{p}} \subseteq \mathcal{O}(X) = B \end{array} \right\} & \\
K \big\downarrow & \big\downarrow & & \big\downarrow & \widetilde{\mathfrak{p}} \big\downarrow \\
L = \overline{f(K)} & \left\{ \begin{array}{c} \text{irreducible subsets} \\ L \subseteq Y \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{prime ideals} \\ \mathfrak{p} \subseteq \mathcal{O}(Y) = A \end{array} \right\} & \mathfrak{p} = (f^*)^{-1}(\widetilde{\mathfrak{p}}) \\
 & & L \longmapsto \mathfrak{p} = \{f \in A \mid f|_L = 0\} & & \\
 & & L = V(\mathfrak{p}) \longmapsfrom \mathfrak{p} & &
\end{array}$$

commutes, the horizontal bijections coming from Corollary 2.2.2.

(*c*) If going-up holds for f, then f is a closed map (i.e. the image of a closed subset of X is closed in Y).

Proof. (*a*) trivial since $f^*g \in \mathfrak{m}_{X,x} \Leftrightarrow f^*g(x) = 0 \Leftrightarrow g(y) = g(f(x)) = 0 \Leftrightarrow g \in \mathfrak{m}_{Y,y}$.

(*b*) Assume $I = \sqrt{I}$ without loss of generality. Let $X \subseteq k^m$, $Y \subseteq k^n$. Since $\mathcal{O}_X(X)$ and $\mathcal{O}_Y(Y)$ are quotients of the ring of polynomials over k in m respectively n variables (by Proposition 2.2.2) and by the definition of the Zariski-topology and well-known facts about vanishing sets,

$$\begin{aligned}
\overline{f(V(I))} &= \bigcap_{A \supseteq f(V(I)) \text{ closed}} A = \bigcap_{\substack{J \subseteq \mathcal{O}_Y(Y) \text{ an ideal} \\ V(J) \supseteq f(V(I))}} V(J) = V\left(\sum_{\substack{J \subseteq \mathcal{O}_Y(Y) \text{ an ideal} \\ V(J) \supseteq f(V(I))}} J \right) \\
&= V\Big(\left\{ \lambda \in \mathcal{O}_Y(Y) \;\middle|\; \lambda|_{f(V(I))} = 0 \right\} \Big) = V\Big(\left\{ \lambda \in \mathcal{O}_Y(Y) \;\middle|\; f^*\lambda|_{V(I)} = 0 \right\} \Big) \\
&= (f^*)^{-1}\left(\sqrt{I}\right) = (f^*)^{-1}(I)
\end{aligned}$$

by our assumptions. If $V(I)$ is irreducible, I is a prime ideal (by our additional assumption $I = \sqrt{I}$) and so is $(f^*)^{-1}(I)$ (preimages of prime ideals are always prime). Thus $\overline{f(V(I))} = V((f^*)^{-1}I)$ is irreducible.

(*c*) Since X is Noetherian it is sufficient to show the closedness of $f(Z)$ where $Z \subseteq X$ is irreducible (cf. Proposition 2.1.1). Thus, let $I = \widetilde{\mathfrak{p}}$ be prime, $Z = V(\widetilde{\mathfrak{p}})$. Let $\mathfrak{p} = (f^*)^{-1}\widetilde{\mathfrak{p}} \subseteq \mathcal{O}_Y(Y)$ be the prime ideal below $\widetilde{\mathfrak{p}}$. We will show that $f(Z) = V(\mathfrak{p})$.

If $y \in Y$ belongs to $\overline{f(Z)} = V(\mathfrak{p})$ (they are equal due to (b)), then the maximal ideal $\mathfrak{q} = \{f \in \mathcal{O}_Y(Y) \mid f(y) = 0\}$ contains $\mathfrak{p}$. By our going-up assumption there is a prime ideal $\widetilde{\mathfrak{q}} \supseteq \widetilde{\mathfrak{p}}$ of $\mathcal{O}_X(X)$ such that $(f^*)^{-1}\widetilde{\mathfrak{q}} = \mathfrak{q}$. Let $\mathfrak{m} \supseteq \widetilde{\mathfrak{q}}$ be a maximal ideal, then $(f^*)^{-1}\mathfrak{m} \supseteq (f^*)^{-1}\widetilde{\mathfrak{q}} = \mathfrak{q}$ and equality holds as $\mathfrak{q}$ is already maximal. The maximal ideal $\mathfrak{m} \subseteq \mathcal{O}_X(X)$ corresponds to a point $x \in X$. From $\widetilde{\mathfrak{p}} \subseteq \widetilde{\mathfrak{q}} \subseteq \mathfrak{m}$ it follows, that $V(\mathfrak{m}) = \{x\} \subseteq V(\widetilde{\mathfrak{p}})$, that is, $x \in V(\widetilde{\mathfrak{p}})$. We have $f(x) = y$ because $V(\mathfrak{q}) = \{y\}$ but $f(x) \in V(\mathfrak{q})$ as $\overline{f(x)} = V\big((f^*)^{-1}\mathfrak{m}\big) = V(\mathfrak{q})$ by (b). Hence, y has a preimage $x \in V(\widetilde{\mathfrak{p}}) = Z$ and $f(Z) = V(\mathfrak{p})$ is closed, as was claimed.

q.e.d.

Professor Franke does not [know] to what extent the following is due to the n00b Krull or to Cohen/Seidenberg.

Theorem 7. *Let $A \subseteq B$ be an integral ring extension.*

(*a*) *Any $\mathfrak{p} \in \operatorname{Spec} A$ is of the form $\mathfrak{q} \cap A$ where $\mathfrak{q} \in \operatorname{Spec} B$.*

(*b*) *For any $\mathfrak{p} \in \operatorname{Spec} A$, there are no proper inclusions between the $\mathfrak{q} \in \operatorname{Spec} B$ with $\mathfrak{q} \cap A = \mathfrak{p}$.*

(*c*) *Going-up holds for the inclusion $A \hookrightarrow B$.*

(*d*) *A prime ideal $\mathfrak{q} \in \operatorname{Spec} B$ is maximal iff $\mathfrak{p} = \mathfrak{q} \cap A$ is maximal.*

Proof. (*d*) $S = B/\mathfrak{q}$ is an integral extension of $R = B/\mathfrak{p}$ and the assertion follows form the fact that in an integral ring extension of domains, either both or none of them are fields (cf. Proposition 1.5.1(d)).

(*a*) + (*b*) Let $\mathfrak{p} \in \operatorname{Spec} A$ be arbitrary. Then $S = A \setminus \mathfrak{p}$ is a multiplicative subset not only of A, but also of B, and we put $B_\mathfrak{p} = B_S$. Then $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ (indeed, if

$$b^m = \sum_{i=0}^{m-1} a_i b^i \ , \ a_i \in A \ , \quad \text{then} \quad \left(\frac{b}{s}\right)^m = \sum_{i=0}^{m-1} \frac{a_i}{s^{m-i}} \left(\frac{b}{s}\right)^i$$

for alle $s \in S$, hence $\frac{b}{s}$ is integral over $A_\mathfrak{p}$). We thus have

$$\begin{array}{ccc} A & \xrightarrow{\alpha_\mathfrak{p}} & A_\mathfrak{p} \\ \cap\!| & & \cap\!| \\ B & \xrightarrow[\beta_\mathfrak{p}]{} & B_\mathfrak{p} \end{array}$$

the vertical inclusions being integral ring extensions. By (a) there is $\mathfrak{r} \in \operatorname{Spec}(B_\mathfrak{p})$ such that $\mathfrak{r} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ and, putting $\mathfrak{q} = \beta_\mathfrak{p}^{-1}(\mathfrak{r}) \in \operatorname{Spec} B$ we have $\mathfrak{q} \cap A = \beta_\mathfrak{p}^{-1}(\mathfrak{r}) \cap A = \alpha_\mathfrak{p}^{-1}(\mathfrak{r} \cap A_\mathfrak{p}) = \alpha_\mathfrak{p}^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$. This implies (a).

If $\mathfrak{q} \subsetneq \mathfrak{q}'$ are prime ideals of B such that $\mathfrak{q} \cap A = \mathfrak{p} = \mathfrak{q}' \cap A$, then $\mathfrak{q}B_\mathfrak{p} \subsetneq \mathfrak{q}'B_\mathfrak{p}$. This inclusion is proper, since $\mathfrak{q}$ and $\mathfrak{q}'$ are disjoint from S and we have a bijection between $\operatorname{Spec} B_\mathfrak{p}$ and $\{\mathfrak{q} \in \operatorname{Spec} B \mid \mathfrak{q} \cap S = \emptyset\}$. But $\mathfrak{q}B_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ as $\mathfrak{q} \cap A = \mathfrak{p}$ and $\mathfrak{p}A_\mathfrak{p}$ is already maximal. Thus $\mathfrak{q}B_\mathfrak{p}$ is maximal by (d), a contradiction to $\mathfrak{q}B_\mathfrak{p} \subsetneq \mathfrak{q}'B_\mathfrak{p}$.

(c) Let $\mathfrak{p} \subseteq \mathfrak{q} \subseteq A$ be a chain of prime ideals in A and let $\widetilde{\mathfrak{p}} \in \operatorname{Spec} B$ be above $\mathfrak{p}$. Replacing $A \subseteq B$ by $\widetilde{A} = A/\mathfrak{p} \subseteq B/\widetilde{\mathfrak{p}} = \widetilde{B}$, it suffices to find $\mathfrak{r} \in \operatorname{Spec} \widetilde{B}$ such that $\mathfrak{r} \cap \widetilde{A} = \mathfrak{q}/\mathfrak{p}$ (as the preimage $\widetilde{\mathfrak{q}}$ of $\mathfrak{r}$ under $B \to B/\widetilde{\mathfrak{p}}$ will have the desired property). As $\widetilde{A} \subseteq \widetilde{B}$ still is an integral ring extension, the existence of $\mathfrak{r}$ follows from the proven assertion (a).

q.e.d.

Proof out of the blue of $\dim(X) = \deg \operatorname{tr}(K(X)/k)$*, for* X *affine.* By Noether Normalization (Theorem 3) there are $f_1, \ldots, f_d \in \mathcal{O}(X)$ algebraically independent over k, such that the ring extension $\mathcal{O}(X)/k[f_1, \ldots, f_d]$ is integral. Thus $\deg \operatorname{tr}(K(X)/k) = d$ as the f form a transcendence base. By Theorem 7(c), going-up holds for $k[X_1, \ldots, X_d] \subseteq \mathcal{O}(X)$. The chain

$$\mathfrak{p}_0 = \{0\} \subsetneq \mathfrak{p}_1 = (X_1) \subsetneq \mathfrak{p}_2 = (X_1, X_2) \subsetneq \ldots \subsetneq \mathfrak{p}_d = (X_1, \ldots, X_d) \qquad (*)$$

of prime ideals in $A = k[X_1, \ldots, X_d]$ may be lifted to a chain

$$\mathfrak{q}_0 = \{0\} \subsetneq \mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \ldots \subsetneq \mathfrak{q}_d \subsetneq B = \mathcal{O}(X)$$

of prime ideals of B by applying going-up successively to $\mathfrak{q}_i$ over $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$. Corresponding to this strictly increasing chain of prime ideals in B we have a strictly decreasing chain of irreducible subsets $V(\mathfrak{q}_i) \subsetneq X$ of length d, establishing $\dim(X) \geq d$. *q.e.d.*

Problem with this proof If equality is to hold in $\dim Z + \operatorname{codim}(Z, X) \leq \dim X$ we must have (with $Z = \{x\}$) $\operatorname{codim}(x, X) = d$ for any point $x \in X$. Let $\mathfrak{m} = \mathfrak{m}_x$ and $\mathfrak{n} = \mathfrak{m}_x \cap A$ its preimage A, then $\mathfrak{n}$ is a maximal ideal (Theorem 7) hence $\mathfrak{n} = (X_1 - \xi_1, \ldots, X_d - \xi_d)_A$ and without loss of generality we may assume that the ξ_i are 0. Then we are in the situation from $(*)$ but $\mathfrak{q}_d = \mathfrak{m}$ is given and the descending chain has to be found, which requires going-down.

The situation for proving going-down in this situation is as follows: Let $K = K(X)$. Assume first that $K/k(X_1, \ldots, X_d)$ is Galois and $B = \mathcal{O}(X)$ is $G = \operatorname{Gal}\big(K/k(X_1, \ldots, X_d)\big)$-invariant and that for any $\mathfrak{p} \in \operatorname{Spec} A$ the group G acts transitively upon the prime ideals of B lying above $\mathfrak{p}$ (i.e. if $\mathfrak{q}|\mathfrak{p}$ is a prime ideal above $\mathfrak{p}$ and $\sigma \in G$, then $\sigma\mathfrak{q}$ is a prime ideal of B lying above $\mathfrak{p}$; conversely, each prime ideal $\mathfrak{q}'|\mathfrak{p}$ of B can be obtained as $\mathfrak{q}' = \sigma\mathfrak{q}$ for a suitable $\sigma \in G$), then the maximal length of a chain in $(*)$ ending on $\mathfrak{p}_d$ does not depend on the choice of $\mathfrak{p}_d$ lying above $(X_1, \ldots, X_d)_A$. Since for at least one such $\mathfrak{p}_d$ this length is d, by the above construction, the same holds for the others.

In general, the field extension is not Galois and even if it is, B may not be G-invariant. but this problem can be fixed by chosing L/K such that L/A is normal, denoting the integral closure of A in L by $\widetilde{B}$, chosing a prime ideal $\widetilde{\mathfrak{m}}$ of $\widetilde{B}$ such that $\widetilde{\mathfrak{m}} \cap B = \mathfrak{m}$. Then $\operatorname{Aut}\big(L/k(X_1, \ldots, X_n)\big)$ acts transitively upon the prime ideals of $\widetilde{B}$ lying above a given prime ideal of A. One can use this to find $\{0\} \subsetneq \widetilde{\mathfrak{p}}_1 \subsetneq \ldots \subsetneq \widetilde{\mathfrak{p}}_d = \widetilde{\mathfrak{m}}$ in $\widetilde{B}$ as needed, then puts $\mathfrak{p}_i = B \cap \widetilde{\mathfrak{p}}_i$.

Theorem 8. *Let* A *be a domain which is normal, i.e. integrally closed in its field of quotients* K*.*

(a) *Let* L/K *be a finite normal field extension,* $B \subseteq L$ *the integral closure of* A *in* L*, and* $G = \operatorname{Aut}(L/K)$*. For any* $\mathfrak{p} \in \operatorname{Spec} A$*,* G *transitively acts upon* $\{\mathfrak{q} \in \operatorname{Spec} B \mid \mathfrak{q} \cap A = \mathfrak{p}\}$*.*

(b) *The same holds when* L/K *is algebraic and normal but not necessarily finite.*

We need two preparations.

Lemma 1. *Let $I \subseteq A$ be an ideal in a ring A and let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be finitely many ideals such that I is not contained in any of the $\mathfrak{p}_i$. If at most two of the ideals $\mathfrak{p}_i$ fail to be prime, there is $f \in I \setminus \bigcup_{i=1}^n \mathfrak{p}_i$.*

Proof. Induction on n. If $n \leq 1$ the assertion is trivial. Let $n \leq 2$ and the assertion be true for fewer than n ideals $\mathfrak{p}_i$. If $n > 2$, we may (permuting the the $\mathfrak{p}_i$) assume that $\mathfrak{p}_1$ is prime. By the induction assumption, there is

$$f_i \in I \setminus \bigcup_{\substack{j=1 \\ i \neq j}}^{n} \mathfrak{p}_i \quad \text{for } i = 1, \dots, n\,.$$

If we also have $f_i \notin \mathfrak{p}_i$ for some i, this f_i will do the job. Otherwise, $f = f_1 + \prod_{i=2}^n f_i$ has the desired properties. Indeed, we have $f \notin \mathfrak{p}_i$ for $2 \leq i \leq n$ because for such i the second summand is in $\mathfrak{p}_i$ but f_1 is not. If $n = 2$, that is, $f = f_1 + f_2$, the same argument applies to $\mathfrak{p}_1$. If $n > 2$, remember that we took $\mathfrak{p}_1$ to be prime. We then have $f \notin \mathfrak{p}_1$ because $f_1 \in \mathfrak{p}_1$ but the factors in $\prod_{i=2}^n f_i$ are not in $\mathfrak{p}_1$. *q.e.d.*

Lemma 2. *Let L/K be a normal extension, $G = \mathrm{Aut}(L/K)$, and $\ell \in L$ be fixed under G. If $\operatorname{char} K = p$ then $\ell \in K$ when $p = 0$ and ℓ^{p^k} for some $k \in \mathbb{N}_0$ when $p > 0$.*

First proof. If $p = 0$, the field extension is Galois and $K = L^G$ as claimed.

Assume L/K is finite. Induction on the degree $d = \deg(\ell/K)$ of the minimal polynomial of ℓ. If $d = 1$, then $\ell \in K$, If $d > 1$ and the minimal polynomial f has a zero $\varphi \neq \ell$ in an algebraic closure $\overline{L}$ of L, there is a morphism ϑ from $K(\ell)$ to $\overline{L}$ extending id_K with $\vartheta(\ell) = \varphi$. It is possible to extend $K(\ell) \xrightarrow{\vartheta} \overline{K}$ to $L \xrightarrow{\sigma} \overline{L}$ and $\sigma(L) \subseteq L$ as L/K is normal. But $\sigma(\ell) = \vartheta(\ell) = \varphi \neq f$ contradicting $f \in L^G$.

If $d > 1$ and ℓ is the only zero of f in $\overline{L}$, then ℓ is a zero of multiplicity bigger than 1 of f and $f' = 0$. Hence $f = g(X^p)$ for some $g \in K[X]$. Then $\deg g = \frac{d}{p} < d$, $\varphi = \ell^p$ is a zero of g and the induction assumption can be applied. There is $k \in \mathbb{N}_0$ such that $\varphi^{p^k} \in K$. Then $\ell^{p^{k+1}} = \varphi^{p^k} \in K$. *q.e.d.*

Second proof. We would like to present a somewhat more natural (and less messy) proof. Replacing L with a finite normal extension containing ℓ we may assume that L/K is finite. It's easy to see that $G = \mathrm{Aut}(L/K)$ still fixes ℓ, as each $\sigma \in G$ can be extended to an automorphism of the original field extension. If $\operatorname{char} K = 0$, then L/K is Galois and $\ell \in L^G = K$.

Now let $\operatorname{char} K = p > 0$ and $f \in K[X]$ the minimal polynomial of ℓ. Then there is an integer $k \in \mathbb{N}_0$ and a *separable* polynomial $f_0 \in K[X]$ such that $f = f_0\big(X^{p^k}\big)$ (Indeed, if f is not separable, then each monomial of f must be a power of X^p. Now iterate.). Consider normal closure N of $K\big(\ell^{p^k}\big)$. N/K is Galois and ℓ^{p^k} is fixed by G (as ℓ is), hence also by $\mathrm{Gal}(N/K)$ and we obtain $\ell^{p^k} \in K$, as claimed. *q.e.d.*

Proof of Theorem 8. (*a*) Assume that for some $\mathfrak{p} \in \operatorname{Spec} A$ there are prime ideals $\mathfrak{q}, \widetilde{\mathfrak{q}} \in \operatorname{Spec} B$ above $\mathfrak{p}$, that is, $\mathfrak{q} \cap A = \mathfrak{p} = \widetilde{\mathfrak{q}} \cap A$, such that there is no $\sigma \in G = \mathrm{Aut}(L/K)$ with $\sigma(\mathfrak{q}) = \widetilde{\mathfrak{q}}$. Let $\mathfrak{q}_1 = \mathfrak{q}, \mathfrak{q}_2, \dots, \mathfrak{q}_d$ be the images of $\mathfrak{q}$ under G. By Theorem 7(b) we have $\widetilde{\mathfrak{q}} \subsetneq \mathfrak{q}_i$. By Lemma 1, there is an $f \in \mathfrak{q} \setminus \bigcup_{i=1}^d \mathfrak{q}_i$. Let $\varphi = \prod_{\sigma \in G} \sigma(f)$. We have $\varphi \in \widetilde{\mathfrak{q}}$ but $\varphi \notin \mathfrak{q}$ because otherwise one factor $\sigma(f)$ would have to be in $\mathfrak{q}$, but $\sigma^{-1}(\mathfrak{q})$ is among the $\mathfrak{q}_i$, hence $f \notin \sigma^{-1}(\mathfrak{q})$. Also, $\varphi \in L^G$, as applying $\vartheta \in G$ only permutes the factors. By Lemma 2, $\varphi^k \in K$ for some positive integer $k \in \mathbb{N}$. Since φ^k is integral over A (f is, and hence are it's

conjugates $\sigma(f)$) and A is integrally closed in K, this implies $\varphi^k \in A$. Also $\varphi^k \in \widetilde{\mathfrak{q}} \setminus \mathfrak{q}$, as φ already has this property. But $\widetilde{\mathfrak{q}} \cap A = \mathfrak{p} = \mathfrak{q} \cap A$, contradiction.

(*b*) Let $\mathfrak{p} \in \operatorname{Spec} A$ and let $\mathfrak{q}, \widetilde{\mathfrak{q}} \in \operatorname{Spec} B$ such that $\mathfrak{q} \cap A = \widetilde{\mathfrak{q}} \cap A = \mathfrak{p}$. Let

$$\mathfrak{M} = \left\{ (M, \sigma) \;\middle|\; \begin{array}{c} M \text{ is an intermediate field } K \subseteq M \subseteq L \\ \sigma \in \operatorname{Aut}(M/K) \text{ such that } \sigma\left(\mathfrak{q} \cap M\right) = \widetilde{\mathfrak{q}} \cap M \end{array} \right\}.$$

Introduce a partial order $\preceq$ on $\mathfrak{M}$ via $(M, \sigma) \preceq (\widetilde{M}, \widetilde{\sigma})$ iff $M \subseteq \widetilde{M}$ and $\widetilde{\sigma}|_M = \sigma$. Then $\mathfrak{M} \neq \emptyset$ as $(K, \mathrm{id}) \in \mathfrak{M}$ (where we need that A is normal, hence $B \cap K = A$). If $\mathcal{L} \subseteq \mathfrak{M}$ is non-empty $\preceq$-linearly ordered chain, then $\mathcal{L}$ is dominated by $(M, \sigma) \in \mathfrak{M}$ where $M = \bigcup_{(N,\vartheta)\in\mathcal{L}} N$ and $\sigma = \bigcap_{(N,\vartheta)\in\mathcal{L})} \vartheta$. By Zorns Lemma, $\mathfrak{M}$ thus has a $\preceq$-maximal element (M, σ). If $M = L$ the assertion is proved.

Otherwise, let $x \in L \setminus M$. As L/K is normal, L contains all zeroes $x_1 = x, x_2, \ldots, x_d$ of the minimal polynomial of x in $\overline{L}$. Let $N = M(x_1, \ldots, x_d)$ be the subfield generated by M and the x_i. Then N/M is normal, being a splitting field. Let $\eta \in \operatorname{Aut}(N/K)$ be some extension of $\sigma \in \operatorname{Aut}(M/K)$ to N. Let $\widetilde{A} = B \cap M$, $\widetilde{B} = B \cap N$, and $\widetilde{\mathfrak{p}} = \mathfrak{q} \cap M = \mathfrak{q} \cap \widetilde{A} = \eta^{-1}\left(\widetilde{\mathfrak{q}} \cap M\right) = \eta^{-1}\left(\widetilde{\mathfrak{q}} \cap \widetilde{A}\right)$. Now consider $\mathfrak{q}_1 = \mathfrak{q} \cap \widetilde{B}$, $\mathfrak{q}_2 = \eta - 1\left(\widetilde{\mathfrak{q}} \cap \widetilde{B}\right)$. These are prime ideals of $\widetilde{B}$ lying above $\widetilde{\mathfrak{p}}$. By part (a) there is an automorphism ζ of N/M such that $\zeta(\mathfrak{q}_1) = \mathfrak{q}_2$. Let $\vartheta = \eta\zeta \in \operatorname{Aut}(N/K)$, then $\vartheta(\mathfrak{q} \cap N) = \vartheta(\mathfrak{q}_1) = \eta(\mathfrak{q}_2) = \widetilde{\mathfrak{q}} \cap N$ and $(M, \sigma) \prec (N, \vartheta)$, contradiction!

q.e.d.

Remark. (*a*) It is actually sufficient to assume that A is integrally closed in K and B is a $\operatorname{Aut}(L/K)$-invariant subset of the integral closure of A in L.

(*b*) This result is also important in algebraic number theory where $A = \mathcal{O}_K$, $B = \mathcal{O}_L$ are the rings of integers in their respective fields.

(*c*) If L/K is infinite algebraic, $\operatorname{Aut}(L/K)$ is equipped with the *Krull topology* (not to be confused with *Grothendieck topologies*, a different and – of course – far more powerful concept), in which $X \subseteq \operatorname{Aut}(L/K)$ is a neighbourhood of $\sigma \in \operatorname{Aut}(L/K)$ iff there is an intermediate field $K \subseteq M \subseteq L$ such that $X \supseteq \{\vartheta \in \operatorname{Aut}(L/K) \mid \vartheta|_M = \sigma|_M\}$ and M/K is finite. When L/K is normal and separable over K (that is, an infinite Galois extension) this is equivalent to saying that $\sigma \operatorname{Gal}(L/M) \subseteq X$ for some finite Galois subextension M/K, i.e. the sets $\sigma \operatorname{Gal}(L/M)$, where M/K is a finite Galois subextension, form a neighbourhood system of σ, and there is a bijection

$$\begin{array}{ccc} \{\text{closed subgroups } H \subseteq \operatorname{Gal}(L/K)\} & \xrightarrow{\sim} & \{\text{intermediate fields } M \subseteq L\} \\ H & \longmapsto & M = L^H \\ H = \operatorname{Gal}(L/M) & \longmapsto & M \end{array}$$

where M/K is finite iff H is open iff H has finite index in $\operatorname{Gal}(L/K)$ and M/K is normal iff H is a normal divisor in which case $\operatorname{Gal}(M/K) \simeq \operatorname{Gal}(L/K)/H$.

Theorem 9. *Let $A \subseteq B$ be an integral ring extension where A and B are domains and A is integrally closed in its field of quotients K. Then going-down holds for B/A.*

Proof. Let L/K be a normal field extension containing the field of quotients M of B (e.g. L can be taken to be an algebraic closure of M, or the union of the splitting fields of the K-irreducible polynomials with a zero in M). Let $\widetilde{B}$ be the integral closure of A in L. Let $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals of A and $\widetilde{\mathfrak{q}} \in \operatorname{Spec} B$ such that $\widetilde{\mathfrak{q}} \cap A = \mathfrak{q}$. It is possible to apply Theorem 7 to $\widetilde{B}/A$ and $\widetilde{B}/B$ and Theorem 8 to $\widetilde{B}/A$. By Theorem 7 there is $\mathfrak{q}_2 \in \operatorname{Spec} \widetilde{B}$ such that $\mathfrak{q}_2 \cap B = \widetilde{\mathfrak{q}}$. By Theorem 7 for $\widetilde{B}/A$ there is $\mathfrak{p}_1 \in \operatorname{Spec} \widetilde{B}$ such that $\mathfrak{p}_1 \cap A = \mathfrak{p}$ and (going-up for $\widetilde{B}/A$ there is $\mathfrak{q}_1 \in \operatorname{Spec} \widetilde{B}$ such that $\mathfrak{q}_1 \supseteq \mathfrak{p}_1$ and $\mathfrak{q}_1 \cap A = \mathfrak{p}$. By Theorem 8 there is $\sigma \in \operatorname{Aut}(L/K)$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Let $\widetilde{\mathfrak{p}} = (\sigma(\mathfrak{p}_1)) \cap B$, then $\widetilde{\mathfrak{p}} \cap A = \sigma(\mathfrak{p}_1) \cap A = \mathfrak{p}_1 \cap A = \mathfrak{p}$ and $\widetilde{\mathfrak{p}} \subseteq \sigma(\mathfrak{q}_1) \cap B = \mathfrak{q}_2 \cap B = \widetilde{\mathfrak{q}}$. *q.e.d.*

2.6. Proof of Theorems 5 and 6

Definition 1. Let A be a ring, $\mathfrak{p} \in \operatorname{Spec} A$, then the *height* of $\mathfrak{p}$

$$\operatorname{ht}(\mathfrak{p}) = \sup \{\ell \mid \text{there is a chain of prime ideals } \mathfrak{p}_\ell \subsetneq \mathfrak{p}_{\ell-1} \subsetneq \ldots \subsetneq \mathfrak{p}_0 = \mathfrak{p} \text{ in } A\} \ .$$

If $\mathfrak{q} \subseteq \mathfrak{p}$ is another prime ideal then

$$\operatorname{ht}(\mathfrak{p}/\mathfrak{q}) = \sup \{\ell \mid \text{there is a chain of prime ideals } \mathfrak{q} = \mathfrak{p}_\ell \subsetneq \mathfrak{p}_{\ell-1} \subsetneq \ldots \subsetneq \mathfrak{p}_0 = \mathfrak{p} \text{ in } A\} \ .$$

Furthermore we have, let

$$\dim R = \sup \{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec} R\} = \dim \operatorname{Spec} R \ .$$

Remark 1. (*a*) Obviously, $\operatorname{ht}(\mathfrak{p}/\mathfrak{q})$ coincides with the height of $\mathfrak{p}/\mathfrak{q} \in \operatorname{Spec}(R/\mathfrak{q})$.

(*b*) By the correspondence between the irreducible subsets of $\operatorname{Spec} A$ and the prime ideals of A, we have $\operatorname{ht}(\mathfrak{p}) = \operatorname{codim}(V(\mathfrak{p}), \operatorname{Spec} A)$ and $\operatorname{ht}(\mathfrak{p}/\mathfrak{q}) = \operatorname{codim}(V(\mathfrak{p}), V(\mathfrak{q}))$.

(*c*) By a theorem of Krull, $\operatorname{ht}(\mathfrak{p})$ is finite when A is Noetherian, but nevertheless $\dim(A) = \sup \{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec} A\}$ may be infinite, even when A is Noetherian.

(*d*) Obviously, we have the following inequalities for prime ideals $\mathfrak{r} \subseteq \mathfrak{q} \subseteq \mathfrak{p} \subseteq A$

$$\begin{aligned} \operatorname{ht}(\mathfrak{q}/\mathfrak{r}) + \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) &\leq \operatorname{ht}(\mathfrak{p}/\mathfrak{r}) \\ \operatorname{ht}(\mathfrak{q}) + \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) &\leq \operatorname{ht}(\mathfrak{p}) \ . \end{aligned} \tag{$*$}$$

One would like to have equality here this may fail, even when A is Noetherian. A Noetherian ring is called *catenary* if, for arbitrary prime ideals $\mathfrak{q} \subseteq \mathfrak{p}$ of A, equality holds on the first line. Examples for non-catenary Noetherian rings exist but are hard to construct.

Fact 1. Obviously, $\dim R = \operatorname{ht}(\mathfrak{m})$ when R is local with maximal ideal $\mathfrak{m}$. If $S \subseteq R$ is multiplicative, we have a bijection $\operatorname{Spec} R_S \simeq \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\}$. In particular,

$$\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p} R_S) \quad \text{and (for } S = R \setminus \mathfrak{p}) \quad \operatorname{ht}(\mathfrak{p}) = \dim(R_\mathfrak{p}) \ .$$

Remark 2. If X is an affine variety, $R = \mathcal{O}_X(X)$, $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R$ prime ideals corresponding to irreducible subsets A and B, then $\operatorname{ht}(\mathfrak{p}) = \operatorname{codim}(A, X)$, $\operatorname{ht}(\mathfrak{q}) = \operatorname{codim}(B, X)$, $\operatorname{ht}(\mathfrak{p}/\mathfrak{q}) = \operatorname{codim}(A, B)$ and $\dim R = \dim X$ by the one-to-one correspondence between irreducible subsets of X and $\operatorname{Spec} R$.

Fact 2. Let $B \supseteq A$ be an integral ring extension. Then $\dim B = \dim A$, and $\mathrm{ht}(\mathfrak{q} \cap A) \geq \mathrm{ht}(\mathfrak{q})$ for every $\mathfrak{q} \in \operatorname{Spec} B$. If going-down holds for B/A, the last inequality becomes an equality.

Proof. If $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_\ell$ is a strictly increasing chain of prime ideals in B, $\mathfrak{q}_0 \cap A \subsetneq \ldots \subsetneq \mathfrak{q}_\ell \cap A$ is such a chain in A, the inclusions being proper by Theorem 7(b). Thus $\dim B \leq \dim A$ and the same argument shows $\mathrm{ht}(\mathfrak{q} \cap A) \geq \mathrm{ht}(\mathfrak{q})$.

If $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_d$ is a strictly increasing chain of prime ideals in A it is possible to find $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_d$ a chain of prime ideals in B by going-up (Theorem 7(c)). Thus, $d \leq \dim B$ and $\dim A \leq \dim B$. If going down holds, any increasing chain of prime ideals of A ending in $\mathfrak{q} \cap A$ can be lifted to a similar chain for B ending in $\mathfrak{q}$, establishing $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{q} \cap A)$. *q.e.d.*

Theorem 10. *If B is a domain which is of finite type over a field k and K denotes the field of quotients of B, then* $\dim B = \deg \mathrm{tr}(K/k)$. *Moreover*

$$\mathrm{ht}(\mathfrak{m}) = \deg \mathrm{tr}(K/k) \tag{1}$$

holds for any maximal ideal $\mathfrak{m}$ of B. If $\mathfrak{p}$ is any prime ideal, then

$$\mathrm{ht}(\mathfrak{p}) = \deg \mathrm{tr}(K/k) - \deg \mathrm{tr}(\mathfrak{K}(\mathfrak{p})/k). \tag{2}$$

In particular, this implies that B is catenary.

Proof. The fact that $\dim B = \deg \mathrm{tr}(K/k)$ will follow trivially from (1) and (2).

Let $\mathfrak{p}_\ell \subsetneq \mathfrak{p}_{\ell-1} \subsetneq \ldots \subsetneq \mathfrak{p}_0 = \mathfrak{m}$ be a chain of prime ideals. By Proposition 2.4.1,

$$0 \leqslant \deg \mathrm{tr}(\mathfrak{K}(\mathfrak{m})/k) < \deg \mathrm{tr}(\mathfrak{K}(\mathfrak{p}_1)/k) < \ldots < \deg \mathrm{tr}(\mathfrak{K}(\mathfrak{p}_\ell)/k) \leqslant \deg \mathrm{tr}(K/k)\ ,$$

hence $\mathrm{ht}(\mathfrak{m}) \leq \deg \mathrm{tr}(K/k)$. For the opposite inequality let $x_1, \ldots, x_n \in B$ be algebraically independent over k such that B is finite over $k[x_1, \ldots, x_n]$. By the Noether Normalization Theorem it is possible to find such elements. Let ξ_i denote the image of x_i in $\mathfrak{K}(\mathfrak{m}) = B/\mathfrak{m}$. As this field is finite over k (Nullstellensatz), there are $P_i \in k[X]$ such that $P_i(\xi_i) = 0$ in $\mathfrak{K}(\mathfrak{m})$. Let $y_i = P_i(x_i)$. The y_i are algebraically independent over k since the x_i are, and each x_i is integral over $A = k[y_1, \ldots, y_n]$ as $P_i(x_i) - y_i = 0$. Thus, B is integral over A since B is integral over $k[x_1, \ldots, x_n]$, the latter being integral over A. Moreover, $P(\xi_i) = 0$ implies $y_i \in \mathfrak{m}$. If $\mathfrak{n} = \mathfrak{m} \cap A$ we thus obtain $\mathfrak{n} = (y_1, \ldots, y_n)_A$, as $\mathfrak{n}$ contains $y_1, \ldots, y_n$ and $(y_1, \ldots, y_n)_A \subseteq A$ is a maximal ideal. We consider the chain of prime ideals $\mathfrak{n} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_n = \{0\}$ with $\mathfrak{p}_i = (y_{i+1}, \ldots, y_n)_A$ in A. This may be lifted to a chain $\mathfrak{m} = \mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \ldots \supsetneq \mathfrak{q}_n$ of prime ideals $\mathfrak{q}_i \in \operatorname{Spec} B$ because A is factorial, hence normal and by Theorem 9, going down holds for B/A. Thus $\mathrm{ht}(\mathfrak{m}) \geq n$. But $\deg \mathrm{tr}(K/k) = n$ as the y_i form (a maximal algebraically independent set and thus) a transcendence base.

For the case of general prime ideals $\mathfrak{p}$ we use reduction to the case just established, similar to the proof of Proposition 2.4.1. Let $x_1, \ldots, x_d \in B$ such that their images ξ_i in $B/\mathfrak{p}$ are algebraically independent and such that $B/\mathfrak{p}$ is finite over $k[\xi_1, \ldots, \xi_d]$. It is possible to find such elements by Noether Normalization. Let $R = k[x_1, \ldots, x_d] \subseteq A$, $S = R \setminus \{0\}$, $\widetilde{B} = B_S$, $\widetilde{k} = R_S = k(x_1, \ldots, x_d)$. Then $\widetilde{B}$ is a domain (being a subring of the quotient field of B) and $\widetilde{B}/\widetilde{k}$ is of finite type. Let $\widetilde{\mathfrak{p}} = \mathfrak{p}\widetilde{B}$. By our description of prime ideals in localizations, there is a one-to-one correspondence between the elements $\mathfrak{q} \subseteq \mathfrak{p}$ of $\operatorname{Spec} B$ (note that $\mathfrak{p}$ is disjoint from S as the ξ_i are algebraically independent) and the prime ideals $\widetilde{\mathfrak{q}} \subseteq \widetilde{\mathfrak{p}}$ of $\widetilde{B}$ via $\mathfrak{q} = \widetilde{\mathfrak{q}} \cap B$ and $\widetilde{\mathfrak{q}} = \mathfrak{q}\widetilde{B}$. Thus $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\widetilde{\mathfrak{p}})$. On the other side, $B/\mathfrak{p}$ is finite over R, hence $\widetilde{B}/\widetilde{\mathfrak{p}}$ is finite-dimensional as a vector space over $\widetilde{k}$,

hence a finite $\widetilde{k}$-extension. Thus $\widetilde{\mathfrak{p}}$ is a maximal ideal and $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\widetilde{\mathfrak{p}}) = \deg \operatorname{tr}(K/\widetilde{k})$ (note that K is the quotient field of $\widetilde{B}$ as well). On the other side, it is possible to extend the (k-algebraically independent) $x_1, \ldots, x_d$ to a maximal k-algebraically independent subset $x_1, \ldots, x_n \in B$, that is, to a transcendence base of K/k. We claim that the $x_{d+1}, \ldots, x_n$ form a transcendence base of K over $\widetilde{k}$. If we believe this for the moment,

$$\operatorname{ht}(\mathfrak{p}) = \deg \operatorname{tr}(K/\widetilde{k}) = n - d = \deg \operatorname{tr}(K/k) - \deg \operatorname{tr}(k(\mathfrak{p})/k)$$

and we are done. To prove the claim, note that all elements of k are algebraic over $k(x_1, \ldots, x_n) = \widetilde{k}(x_{d+1}, \ldots, x_n)$. If $Q \in \widetilde{k}[X_{d+1}, \ldots, X_n]$ such that $Q(x_{d+1}, \ldots, x_n) = 0$, we have $Q = \frac{E}{d}$ where $d \in R = k[x_1, \ldots, x_n]$ is not 0 and $E \in R[X_{d+1}, \ldots, X_n]$. Then $E(x_{d+1}, \ldots, x_n) = 0$ contradicting the k-algebraic independence of $x_1, \ldots, x_n$.

From this, the fact that B is catenary is easily derived. Indeed, let $\mathfrak{q} \subseteq \mathfrak{p}$ be prime ideals. By Remark 1(a), $\operatorname{ht}(\mathfrak{p}/\mathfrak{q})$ coincides with the height of $\mathfrak{p}/\mathfrak{q} \in \operatorname{Spec} R/\mathfrak{q}$. Now $(R/\mathfrak{q})/(\mathfrak{p}/\mathfrak{q}) = R/\mathfrak{p}$ implies $\mathfrak{K}(\mathfrak{p}/\mathfrak{q}) = \mathfrak{K}(\mathfrak{p})$, hence

$$\begin{aligned} \operatorname{ht}(\mathfrak{p}/\mathfrak{q}) &= \deg \operatorname{tr}((\text{quotient field of } R/\mathfrak{p})/k) - \deg \operatorname{tr}(\mathfrak{K}(\mathfrak{p}/\mathfrak{q})/k) \\ &= \deg \operatorname{tr}(\mathfrak{K}(\mathfrak{q})/k) - \deg \operatorname{tr}(\mathfrak{K}(\mathfrak{p})/k) \end{aligned}$$

by (2). From this, (∗) is immediate. *q.e.d.*

Corollary 1. *Let $X \subseteq k^n$ be a quasi-affine algebraic variety over an algebraically closed field k and let K be its field of rational functions, then $\dim X = \deg \operatorname{tr}(K/k)$. For any irreducible subset $Z \subseteq X$ we have $\operatorname{codim}(Z, X) = \dim X - \dim Z$. In particular, Theorems 5 and 6 hold.*

Proof. For affine X, this follows from the geometric interpretation of $\operatorname{ht}(\mathfrak{p})$. The quasi-affine case can be reduced to the affine as in the proof of Corollary 2.4.3.

For the sake of completeness, we give a proof of the quasi-affine case. Let $X \subseteq k^n$ be a quasi-affine variety, $\overline{X}$ it's closure. Let us first prove, that $\dim X = \dim \overline{X}$. Since $\mathcal{O}(X)$ and $\mathcal{O}(\overline{X})$ have the same quotient field K (as was shown in the proof of Proposition 2.4.3), this will establish $\dim X = \deg \operatorname{tr}(K/k)$. As was done in the proof of Corollary 2.4.3, we take $f \in \mathcal{O}(\overline{X})$ such that $W := \overline{X} \setminus V(f) \subseteq X$. Let $A = \mathcal{O}(\overline{X})$, $B = \mathcal{O}(W)$, then $A \subseteq \mathcal{O}(X) \subseteq B$ and $B = A_f$. In particular, $B = A[f^{-1}]$ is of finite type over k since so is A. By Theorem 10, $\dim B = \dim A_f = \deg \operatorname{tr}(K/k) = \dim A$, hence there is a chain $\widetilde{\mathfrak{p}}_0 \supsetneq \widetilde{\mathfrak{p}}_1 \supsetneq \ldots \supsetneq \widetilde{\mathfrak{p}}_n$ of prime ideals in B such that $n = \dim A$. The one-to-one correspondence provided by Corollary 2.3.1 shows that this corresponds to a chain $\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_n$ of prime ideals $\mathfrak{p}_i = \widetilde{\mathfrak{p}}_i \cap A \in \operatorname{Spec} A$ satisfying $f \notin \mathfrak{p}_i$. Then

$$V(\mathfrak{p}_0) \subsetneq V(\mathfrak{p}_1) \subsetneq \ldots \subsetneq V(\mathfrak{p}_n) \subseteq W \subseteq X \ ,$$

hence $\dim X \geq n$. The reverse inequality was shown in Corollary 2.4.3.

If $A \supseteq B \supseteq C$ are irreducible subsets of X, then consider $\overline{A} \supseteq \overline{B} \supseteq \overline{C}$. These guys are irreducible subsets of $\overline{X}$ (cf. the proof of Corollary 2.4.3 or exercise sheet #6), hence equation (2.1.1) reduces to the affine case by the *locality of codimension* (cf. Remark 2.1.3(b), equation (2.1.2)). *q.e.d.*

Concluding remarks

Theorem 11 (Principal ideal theorem, Krull 1928)**.** *Let R be a Noetherian domain, $f \in R \setminus \{0\}$, $\mathfrak{p} \in \operatorname{Spec} R$ a prime ideal which is minimal among all the prime ideals containing f. Then* $\operatorname{ht}(\mathfrak{p}) = 1$.

Corollary 1. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then*

$$\dim R \leq \dim_{\mathfrak{K}(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2) = \textit{minimal number of generators of } \mathfrak{m}\ .$$

Definition 1. R is called regular if equality occurs in the above inequality.

Exercise 1. *Confirm that the local rings of the affine variety k^n are regular.*

The fact that $\dim_{\mathfrak{K}(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2)$ is smaller or equal to the minimal number of generators of $\mathfrak{m}$ is trivial. That $\mathfrak{m}$ can be generated by $\dim_{\mathfrak{K}(\mathfrak{m})}(\mathfrak{m}/\mathfrak{m}^2)$ of its elements follows from the following important lemma.

Lemma 1 (Nakayama(-Azumaya-Krull) Lemma)**.** *Let $(R, \mathfrak{m})$ be a local ring and M be a finitely generated R-module.*

(*a*) *If $M = \mathfrak{m}M$ then $M = 0$.*

(*b*) *If $N \subseteq M$ is any submodule such that $M = \mathfrak{m}M + N$ then $M = N$.*

(*c*) *If $m_1, \ldots, m_n \in M$ are such that their images generate $M/\mathfrak{m}M$ as a $\mathfrak{K}(\mathfrak{m})$-vector space then they generate M as an R-module.*

Proof. (*a*) Let $m_1, \ldots, m_k$ generate M. Denote $(m_1, \ldots, m_k) = m$. Since $M = \mathfrak{m} \cdot M$, there are $\mu_{i,j} \in \mathfrak{m}$ such that $m_j = \sum_{i=1}^{k} \mu_{i,j} m_i$. Thus $(\mathrm{id}_{R^k} - \mu)\, m = 0$ where $\mu = (\mu_{i,j})_{i,j=1}^{k}$ is the matrix formed by the coefficients $\mu_{i,j}$. We have $\det(\mathrm{id} - \mu) \equiv 1 \mod \mathfrak{m}$ as the $\mu_{i,j}$ are in $\mathfrak{m}$. Since $R^\times = R \setminus \mathfrak{m}$ this implies $\det(\mathrm{id} - \mu)$ is invertible, hence so is $\mathrm{id} - \mu$ by Cramer's rule. Hence $m = 0$ and $M = 0$.

(*b*) Apply (a) to M/N.

(*c*) Apply (b) to $N = \langle m_1, \ldots, m_n \rangle_R$ the submodule generated by the m_i.

q.e.d.

Corollary 2. *If $Z \subseteq k^n$ is an irreducible subset then all irreducible components of $k^d \cap Z$ have dimension greater or equal to* $\dim(Z) - (n - d)$ *and* $\operatorname{codim}(k^d \cap Z, k^d) \leq \operatorname{codim}(Z, k^n)$.

Corollary 3. *If $X, Y \subseteq k^n$ are irreducible subsets then all irreducible components of $X \cap Y$ have codimension smaller or equal to* $\operatorname{codim}(X, k^n) + \operatorname{codim}(Y, k^n)$.

Remark 1. (*a*) Of course, the intersections may be empty no matter what the lower bound for the dimensions of their irreducible components is.

(*b*) Corollary 3 is derived from Corollary 2 considering $X \times Y \cap \Delta$ where

$$\Delta = \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \mid x_i = y_i\} \subseteq k^{2n} \ .$$