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, $I \subseteq k[X_1, \dots, X_n]$ an ideal, ℓ a field extension of k. Call $x \in \ell^n$ a *zero* of I iff $f(x_1, \dots, x_n) = 0$ 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:*

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

(ii) *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 $n \geq N$.*

(iii) *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 $m, n \in M$

$$\begin{aligned} r \cdot (s \cdot m) &= (r \cdot s) \cdot m & \qquad (r + s) \cdot m &= r \cdot m + s \cdot m \\ 1 \cdot m &= m & r \cdot (m + n) &= r \cdot m + r \cdot n \ . \end{aligned}$$

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*

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

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.*

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

$$\begin{tikzcd} L \arrow[r, hook] \arrow[d, "\pi_{L/(N\cap L)}"'] & N+L \arrow[d, "\pi_{(N+L)/N}"] \\ L/(N \cap L) \arrow[r, dashed, "\sim"] & (N+L)/N \end{tikzcd}$$

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

$$\begin{tikzcd} M \arrow[r, "\pi_{M/L}"] \arrow[d, "\pi_{M/N}"'] & M/L \arrow[d, "\pi_{(M/L)/(N/L)}"] \\ M/N \arrow[r, dashed, "\sim"] & (M/L)/(N/L) \end{tikzcd}$$

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 $m_1, \dots, m_k \in M$, then the *submodule generated by* $\{m_1, \dots, m_k\}$ *is*

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

As was the case for Definition 1.1.1, this can be generalized to infinitely many generators. M is *finitely generated* iff there are $m_1, \dots, m_k \in M$ 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.

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

(ii) *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. $(a) \to (b)$ 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 $N_\ell = N_\infty$.

$(b) \to (c)$ 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 $\mathfrak{M}$.

$(c) \to (a)$ 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 $R \to M/N$ 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

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

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 $r \cdot a := \alpha(r) \cdot a$. 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 $R \to A \to B$.*

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

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

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

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

Proof. (i) Trivial.

(ii) 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 $b = \sum_{i=1}^m \sum_{j=1}^n r_{i,j} \beta_{i,j}$.

(iii) 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.

(iv) 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 $a_1, \dots, a_m$ generate A as an R-algebra and let $\alpha_1, \dots, \alpha_n$ 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 $\mathfrak{B} \subseteq B$ 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. Let $\mathfrak{A} \subseteq A$ be the $\mathfrak{B}$-submodule generated by $\alpha_1, \dots, \alpha_n$. It is a subring containing the a_i by $(*)$ and is an R-algebra because $\mathfrak{B}$ is. Then $\mathfrak{A} = A$ and A is finite over $\mathfrak{B}$. Since $\mathfrak{B}$ is Noetherian, $B \subseteq A$ is a $\mathfrak{B}$-subalgebra, and B is finitely generated as $\mathfrak{B}$-module ($\mathfrak{B}$ being Noetherian), B is of finite type over $\mathfrak{B}$ (Proposition 1(i)) and thus also over R (Proposition 1(iii)). *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 $a_0, \dots, a_{n-1} \in A$. 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. (i) *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 $b_1, \dots, b_n$ 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.*

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

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

(iv) *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. (i) Let $b_1, \dots, b_n$ 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 $C = A[b_1, \dots, b_n]$ is generated by all $b_1^{k_1} \cdots b_n^{k_n}$ where $0 \le k_i < d_i$, hence it is finite over A. The first assertion of (i) 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 $\gamma_1, \dots, \gamma_n$. 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: $M^n = p_0 + p_1 M + \dots + p_{n-1}M^{n-1}$ for suitable $p_0, \dots, p_{n-1} \in A$. Since b^j in C can be expressed by M^j (in the sense that

$$\begin{tikzcd}
(a_1, \dots, a_n) \arrow[d, mapsto] & A^n \arrow[r, "M^j\cdot"] \arrow[d, two heads, "\gamma"'] & A^n \arrow[d, two heads, "\gamma"] & (a_1, \dots, a_n) \arrow[d, mapsto] \\
\sum a_i\gamma_i & C \arrow[r, "\cdot b^j"] & C & \sum a_i\gamma_i
\end{tikzcd}$$

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

(ii) 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.

(iii) Let, more generally, B/A be integral and $c \in C$ integral over B. It satisfies an equation $c^d = \beta_0 + \beta_1 c + \dots + \beta_{d-1}c^{d-1}$ with $\beta_i \in B$. By (i), 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 (i) 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(ii), hence c is integral over A by (i).

(iv) Suppose that B is a field and let $a \in A\backslash\{0\}$. Since B/A is integral, we can find $\alpha_0, \dots, \alpha_{n-1} \in A$ 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

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

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

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

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

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

Proof. Since A is of finite type over k, we can choose $a_1,\dots,a_n$ such that A is integral over $k[a_1,\dots,a_n]$ (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 $x_1,\dots,x_n \in A$ such that A is integral over $k[x_1,\dots,x_n]$ 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

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

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 $k[x_1,\dots,x_n] = k[y_1,\dots,y_n]$. The idea is to choose the d_i such that y_1 is integral over $k[y_2,\dots,y_n]$. Then A is integral over $k[y_2,\dots,y_n]$, 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

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

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

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

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

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

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

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(iv), $K[y_1, \ldots, y_n]$ 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 $\mathfrak{m} \subset R := k[X_1, \ldots, X_n]$*

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

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 $\mathfrak{m}$-$\mathrm{Spec}(R)$, 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 $\mathrm{Spec}\, R$, 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 $I = \langle\prod_{i=1}^{m}(X - \xi_i)^{a_i}\rangle_{k[X]}$ 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

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

which is anti-monotonic (i.e. 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. $(a) \to (b)$ Otherwise, select $M_1 \in \mathfrak{X}$, $M_2 \subsetneq M_1$, if M_1 is not yet minimal and so on.

$(b) \to (c)$ 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 $\mathfrak{X} = \{\bigcap_{\lambda\in F} M_\lambda \mid |F| < \infty\}$. 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 $U = \bigcup_{\lambda\in F}(T \setminus M_\lambda)$.

$(c) \to (b)$ Otherwise, $U = T \setminus M_\infty$ with $M_\infty = \bigcap_{i=1}^{\infty} M_i$ the 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 $M_1 \supsetneq M_2 \supsetneq \dots$ of closed subsets would yield an infinite ascending chain of ideals by applying the correspondence of 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 $\{Y_1, \dots, Y_k\}$ 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

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

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

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

$$A \longmapsto M = A \cap V$$

$$\overline{M} \longleftarrow M$$

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 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 $\operatorname{Spec}(R)$ with R Noetherian, $\operatorname{codim}(A,B)$ 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 $\operatorname{Spec}(R)$ is infinite-dimensional (relatively easy), there are closed points of differing codimensions (quite easy) and $\operatorname{Spec}(R)$ 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 $\operatorname{codim}(X, k^n) > 1$, 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

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

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

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

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 $\mathcal{O} = \mathcal{O}_Z : U \mapsto \mathcal{O}(U)$ the *structure sheaf* of Z.

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

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

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

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

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

(b) The map

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

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

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

are polynomials and $q^{-1}(A) = \Omega \cap V(h_1, \dots, h_\ell)$, 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 $p_i, q_i \in k[X_1, \dots, X_n]$ 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

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

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 $\dim(X) = \deg\operatorname{tr}(K/k)$ and equality always occurs in equation (2.2.1).*

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* $\deg\operatorname{tr}(K/k)$ 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 13th 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.*