# Algebra II

Nicholas Schwab & Ferdinand Wagner

Wintersemester 2017/18

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

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

# Contents

# Introduction

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

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

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

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

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

Professor Franke recommends the following literature:

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

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

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

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

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

# 1. Krull's principal ideal theorem

## 1.1. Formulation

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# A. Appendix

## A.1. Introduction to Krull dimension and all that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Example.** The empty set is a transcendence base of $K/K$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

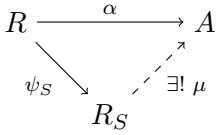
of irreducible closed subsets. To prove $\dim(k^n) \leq n$, and $\dim(X) \leq \deg \mathrm{tr}(K(X)/k)$, one proves $\deg \mathrm{tr}(\mathfrak{K}(\mathfrak{p})/k) > \deg \mathrm{tr}(\mathfrak{K}(\mathfrak{q})/k)$ whenever $A/k$ is an algebra of finite type over $k$, $\mathfrak{q} \supsetneq \mathfrak{p}$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

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

## A.2. Localization of rings

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

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

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

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

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

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

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

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

## A.3. "Advanced" Galois Theory: Trace and Norm

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

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

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

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

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

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

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

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

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

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

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

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

(d) *We have*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Bibliography

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