

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	1
1. Krull's principal ideal theorem	3
1.1. Formulation	3
1.2. The nilradical, the Jacobson radical and the Lemma of Nakayama(-Azumaya-Krull)	8
1.3. Regular rings	10
A. Appendix	11
A.1. Introduction to Krull dimension and all that	11
A.2. Localization of rings	14
A.3. "Advanced" Galois Theory: Trace and Norm	15

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 $k[X_1, \dots, X_n]$,
- 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* [2]

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 (Krull's principal ideal theorem). *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

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

(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)

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

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

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

(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 $\text{codim}(A \cap U, U) = \text{codim}(A, X)$ 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 $\lambda \in k[X_1, \dots, X_n]$ vanishing on $Y \setminus X$, but not on all of C . Indeed, $A = Y \setminus X$ and $B = Y \setminus X \cup \overline{C}$ are closed subsets and $A \subsetneq B$. Then we may choose λ such that it vanishes on A but not on all of B , hence not on all of \overline{C} . But then λ can't be identically zero on C since otherwise $\lambda = 0$ on \overline{C} by continuity. Replacing X by $Y \setminus V(\lambda)$ we may then assume X to be affine according to (b).
- (d) Let now X be an affine variety. We saw in Algebra I (cf. [1, Corollary 2.2.2]) that there is a bijection

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

Under this correspondence, A is irreducible iff the corresponding ideal is prime. (*) follows from the special case $X = k^n$, $\mathcal{O}(X) = k[X_1, \dots, X_n] =: R$ 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 $R \rightarrow \mathcal{O}(X)$ (by the Nullstellensatz, cf. [1, Proposition 1.7.1]) has kernel I .

Proof Corollary 1 (using Theorem 11). Let C_1, \dots, 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 $\mathfrak{q} \in \text{Spec } \mathcal{O}(X)$ 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 \mathfrak{p}_i . We conclude that the \mathfrak{p}_i are the minimal prime ideals containing f . By (*) and the principal ideal theorem, $\text{codim}(C_i, X) = \text{ht}(\mathfrak{p}_i) \leq 1$. But $\text{codim}(C_i, X) > 0$ 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 $V(f) = C_1 \cup \dots \cup C_m$ be its decomposition into irreducible components. Since $C_1 \not\subseteq B := C_2 \cup \dots \cup C_m$, 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 $\tilde{X} = X \setminus V(\lambda)$. Denote $\tilde{f} = f|_{\tilde{X}} \in \mathcal{O}(\tilde{X})$, then $V(f) \cap \tilde{X} = V(\tilde{f}) = C_1 \setminus V(\lambda)$ is irreducible and we may replace X and f by their tilded versions \tilde{X} and \tilde{f} .

Step 2. Let R be a factorial domain and $p \in R$ prime. Then $\text{ht}(p) = 1$. Indeed, $\text{ht}(p) > 0$ as $(0) \in \text{Spec } R$ 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 $\lambda_1, \dots, \lambda_n$ such that A is integral over $B = k[\lambda_1, \dots, \lambda_n]$. The latter is factorial, because $B \simeq k[X_1, \dots, X_n]$, the λ_i being algebraically independent. Denote by L and K the quotient fields of A and B and let $\mathfrak{q} = \mathfrak{p} \cap B$, $f_0 = N_{L/K}(f)$. We claim

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

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 $\text{ht}(\mathfrak{q}) = 1$. But $\text{ht}(\mathfrak{p}) \leq \text{ht}(\mathfrak{q})$ holds by the *going-up theorem* (cf. [1, Theorem 7] or [1, Fact 2.6.2] for this particular result), hence $\text{codim}(V(f), X) \leq 1$. 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 $L \hookrightarrow \bar{L}$ (they satisfy the same equation as f). As the elements of \bar{L} which are integral over B form a subring of \bar{L} , all coefficients of the characteristic polynomial $P_{f,L/K}$ (cf. Definition A.3.1) and the minimal polynomial $\text{Min}_{f/K}$ are integral over B by Theorem C(d). But, by definition, these two have their coefficients in K as well, hence $P_{f,L/K}, \text{Min}_{f/K} \in B[T]$. In particular, $f_0 = N_{L/K}(f) \in B$.

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

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

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 \tilde{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

$$q^{mn} = N_{L/K}(q^m) = N_{L/K}(f)N_{L/K}(a) = f_0b \in (f_0)$$

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

Theorem 12 (Krull's height theorem). *Let A be a Noetherian ring, $f_1, \dots, f_r \in A$ and \mathfrak{p} any prime ideal minimal among the prime ideals containing all the f_i . Then $\text{ht}(\mathfrak{p}) \leq r$.*

The following corollary can be derived in the same way as Corollary 1 from Theorem 11.

Corollary 2. *Let X be a quasi-affine variety in k^n , and let $f_1, \dots, f_r \in \mathcal{O}(X)$ and let Z be any irreducible component of $\bigcap_{i=1}^r V(f_i) = V(f_1, \dots, f_r)$. Then $\text{codim}(Z, X) \leq r$.*

The derivation from Corollary 1 by induction on r is significantly easier than the similar inductive derivation of Theorem 12 from Theorem 11 due to the fact that k^n is catenary. We will eventually prove Theorem 12 by Hilbert polynomial arguments.

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

Otherwise, let $V(f_r) = \bigcup_{i=1}^N Y_i$, be the decomposition into irreducible components. Then $Z = \bigcup_{i=1}^N (Z \cap Y_i)$ and, as Z is irreducible, there is an $i \leq N$ such that $Z \subseteq Y_i$ (cf. [1, Proposition 2.1.1]). By Corollary 1, $\text{codim}(Y_i, X) = 1$. Now Z is an irreducible component of $\bigcap_{j=1}^{r-1} V(f_j|_{Y_i})$. Indeed, it is possible to obtain a decomposition of $\bigcap_{j=1}^r V(f_j)$ into irreducible subsets by forming the union over $1 \leq i \leq N$ of the decompositions of $\bigcap_{j=1}^{r-1} V(f_j|_{Y_i})$. Removing the non-maximal elements gives the decomposition of $\bigcap_{j=1}^r V(f_j)$ into irreducible components, which is unique (to be the unique decomposition into irreducible components, it actually suffices, that no component is contained in another, cf. [1, Proposition 2.1.1]). As Z occurs in it, it is not a strict subset of any irreducible component of $\bigcap_{j=1}^{r-1} V(f_j|_{Y_i})$, hence it is an irreducible component of that. Applying the induction assumption we obtain $\text{codim}(Z, Y_i) \leq r - 1$. As X is catenary, we have

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

as claimed. *q.e.d.*

Corollary 3. *If R is any Noetherian ring and $\mathfrak{p} \in \text{Spec } R$, then $\text{ht}(\mathfrak{p}) < \infty$. In particular, any local Noetherian ring is finite-dimensional.*

Remark. The dimension of R (or $\text{Spec } R$) may still be infinite for lack of a finite common bound for the heights of the maximal ideals.

Proposition 1 ([1, Concluding remarks, Proposition 1]). *Let $X \subseteq k^m$ and $Y \subseteq k^n$ be affine algebraic varieties of codimensions a resp. b . Then $X \times Y$ is an affine algebraic variety in k^{m+n} and*

$$\text{codim}(X \times Y, k^{m+n}) = a + b \quad \text{and} \quad \dim(X \times Y) = \dim X + \dim Y .$$

Proof. Let's first prove that $X \times Y$ is an affine algebraic variety (this was done in [1, proof of Proposition 2.2.6] as well). Let $X = V(\mathfrak{p})$, $Y = V(\mathfrak{q})$ with $\mathfrak{p}, \mathfrak{q}$ prime ideals in their respective polynomial rings. Then $X \times Y = V(I)$ where $I \subseteq k[X_1, \dots, X_m, Y_1, \dots, Y_n]$ is the ideal generated by $\{f(X_1, \dots, X_m) \mid f \in \mathfrak{p}\}$ and $\{g(Y_1, \dots, Y_n) \mid g \in \mathfrak{q}\}$. Hence, $X \times Y$ is closed. To prove it's irreducible, let $X \times Y = Z_1 \cup Z_2$ where Z_1, Z_2 are closed. For every $x \in X$ we have $\{x\} \times Y \subseteq Z_1$ or $\{x\} \times Y \subseteq Z_2$, as Y is irreducible and isomorphic to $\{x\} \times Y$. Thus

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

are closed (as every *slice* $(X \times \{y\}) \cap Z_i$ on the right-hand side is closed), hence $X = X_1$ or $X = X_2$ and consequently $X \times Y = Z_1$ or $X \times Y = Z_2$.

Let $X = X_0 \subsetneq \dots \subsetneq X_a = k^m$ and $Y = Y_0 \subsetneq \dots \subsetneq Y_b = k^n$ be chains of irreducible closed subsets, then (using the that $X_i \times Y_j$ is irreducible closed again by the above)

$$X \times Y = X_0 \times Y_0 \subsetneq X_0 \times Y_1 \subsetneq \dots \subsetneq X_0 \times Y_b \subsetneq X_1 \times Y_b \subsetneq \dots \subsetneq X_a \times Y_b = k^{m+n}$$

is a such a chain for $X \times Y$, showing $\text{codim}(X \times Y, k^{m+n}) \geq a + b$.

Denote $\dim X = d$ and $\dim Y = e$. Let $X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_d = X$ and $Y_0 \subsetneq Y_1 \subsetneq \dots \subsetneq Y_e = Y$ be chains of irreducible closed subsets, then

$$X_0 \times Y_0 \subsetneq X_0 \times Y_1 \subsetneq \dots \subsetneq X_0 \times Y_e \subsetneq X_1 \times Y_e \subsetneq \dots \subsetneq X_d \times Y_e = X \times Y$$

is a similar chain. Hence $\dim(X \times Y) \geq d + e$.

Now observe that $a + d = m$, $b + e = n$, and $\dim(X \times Y) + \text{codim}(X \times Y, k^{m+n}) = m + n$, because, by Theorem A, equality occurs in (A.1.2). We conclude

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

showing that the inequalities of the previous two steps are actually equalities. *q.e.d.*

Theorem 13 ([1, Concluding remarks, Corollary 3]). *Let $X, Y \subseteq k^n$ be irreducible and closed, then any irreducible component Z of $X \cap Y$ has codimension*

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

Remark. It follows that the dimension of any irreducible component of $X \cap Y$ is greater then or equal to $\dim X + \dim Y - n$. Note that the assumption *does not* imply $X \cap Y \neq \emptyset$ unless $X = k^n$ or $Y = k^n$ (or, unless one takes the intersection in $\mathbb{P}^n(k)$).

Proof. The intersection $X \cap Y$ is homeomorphic to $(X \times Y) \cap \Delta$ where

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

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

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

and hence

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

proving the assertion. *q.e.d.*

Theorem 14. *Let R be a Noetherian domain.*

- (a) *Every $r \in R \setminus (R^\times \cup \{0\})$ can be written as a product $r = \prod_{i=1}^k r_i$ of irreducible factors r_i .*
- (b) *The following conditions are equivalent:*
 - (α) *The above decomposition is unique up to permutation and multiplicative equivalence of the factors.*
 - (β) *For any irreducible $p \in R$, $(p) = pR$ is a prime ideal.*
 - (γ) *Any $\mathfrak{p} \in \text{Spec } R$ such that $\text{ht}(\mathfrak{p}) = 1$ is principal, i.e. $\mathfrak{p} = (p)$ for some $p \in R$.*

1.2. The nilradical, the Jacobson radical and the Lemma of Nakayama(-Azumaya-Krull)

Proposition 1. *If R is any ring, then*

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

*The ideal $\text{nil}(R)$ is called the **nilradical** of R .*

Proof. If f is nilpotent, i.e. $f^n = 0$ for some n , then $f^n \in \mathfrak{p}$ for all prime ideals \mathfrak{p} , hence also $f \in \mathfrak{p}$ for every prime ideal \mathfrak{p} .

Let $f^n \neq 0$ for all $n \in \mathbb{N}$, then R_f (the localization of R at $f^\mathbb{N} = \{1, f, f^2, \dots\}$) is not the null ring, hence there is a prime ideal $\mathfrak{q} \in \text{Spec}(R_f)$. Its preimage $\mathfrak{p} = \mathfrak{q} \cap R$ is in $\text{Spec}(R)$ and $f \notin \mathfrak{p}$ as f becomes a unit in R_f . *q.e.d.*

Corollary 1. *There is a canonical bijection*

$$\begin{aligned} \{\text{Zariski-closed subsets } A \subseteq \operatorname{Spec} R\} &\xrightarrow{\sim} \{\text{ideals } I \subseteq R \text{ such that } I = \sqrt{I}\} \\ A \subseteq \operatorname{Spec} R &\longmapsto I = \bigcap_{\mathfrak{p} \in A} \mathfrak{p} \\ \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\} = V(I) &\longleftarrow I \end{aligned}$$

in which the irreducible sets correspond to the prime ideals.

Proof. For the first assertion, the only non-trivial part is that going from the right to the left and back again equals the identity. This can be seen from

$$\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}, \quad (1)$$

which follows from applying Proposition `reffprop:nilradicalCapPrimeIdeals` to R/I . The assertion about prime ideals is left as an exercise (and you should have done this on exercise sheet #2!). *q.e.d.*

Proposition 2. *The intersection of the maximal ideals of R , called the **Jacobson-radical**, is*

$$\bigcap_{\mathfrak{m} \in \mathfrak{m}\text{-Spec } R} \mathfrak{m} = \operatorname{rad}(R) = \{r \in R \mid 1 + xr \in R^\times \text{ for all } x \in R\}. \quad (2)$$

Proof. Let $r \in \bigcap_{\mathfrak{m} \in \mathfrak{m}\text{-Spec } R} \mathfrak{m}$ and $x \in R$. If $1 + xr \notin R^\times$ it must be contained in some maximal ideal \mathfrak{m} or R . Since $r \in \mathfrak{m}$ and $1 = 1 + xr - xr \in \mathfrak{m}$, which is a contradiction.

Conversely, let \mathfrak{m} be maximal and $r \notin \mathfrak{m}$. Then $\mathfrak{R}(\mathfrak{m}) = R/\mathfrak{m}$ is a field. Let $-x \bmod \mathfrak{m}$ be inverse to $r \bmod \mathfrak{m}$ (that being non-zero due to $r \notin \mathfrak{m}$) in that field. Then $xr + 1 \in \mathfrak{m}$ and $xr + 1 \notin R^\times$, so r is not an element of the right hand side. *q.e.d.*

Example 1. If R is a local ring and \mathfrak{m} its maximal ideal, then $\operatorname{rad}(R) = \mathfrak{m} = R \setminus R^\times$.

The following is usually known under the name *Nakayama's lemma*. However, Professor Franke rather would like to attribute it to Azumaya and Krull (as Matsumura does in [2]). Making a compromise, it will, from now on, be cited as [NAK].

Proposition 3 (Nakayama's lemma). *Let R be any ring, M a finitely generated R -module such that $\operatorname{rad}(R) \cdot M = M$. Then $M = 0$.*

Proof. Let $m = (m_1, \dots, m_k)^t$ be generators of M . As $M = \operatorname{rad}(R) \cdot M$ there are $\rho_{i,j} \in \operatorname{rad}(R)$ such that $m_i = \sum_{j=1}^k \rho_{i,j} m_j$. In other words $(\operatorname{id}_k - \rho) \cdot m = 0$ where ρ is the matrix formed by the $\rho_{i,j}$. But $\det(\operatorname{id}_k - \rho) \equiv 1 \bmod \operatorname{rad}(R)$ by the Leibniz formula as $\operatorname{rad}(R)$ is an ideal containing the $\rho_{i,j}$. By (2), we conclude $\det(\operatorname{id}_k - \rho) \in R^\times$. Hence, by Cramers rule, $\operatorname{id}_k - \rho$ has an inverse matrix. Therefore $(\operatorname{id}_k - \rho) \cdot m = 0$ implies $m = 0$ and thus $M = 0$. *q.e.d.*

Applying Proposition 3 to M/N , we obtain the following corollary.

Corollary 2. *If M is finitely generated R -module and $N \subseteq M$ any submodule such that $M = N + \operatorname{rad}(R) \cdot M$ then $M = N$ (actually, it suffices M/N to be finitely generated).*

Remark. [NAK] is typically applied to local rings R : If \mathfrak{m} denotes the maximal ideal, then $M = \mathfrak{m} \cdot M + N$ implies $M = N$ if M is finitely generated.

1.3. Regular rings

Proposition 1. *Let R be a Noetherian local ring with maximal ideal \mathfrak{m} and residue field $k = R/\mathfrak{m}$, then $\mathfrak{m}/\mathfrak{m}^2$ is a k -vector space of finite dimension and*

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

Proof. If μ_1, \dots, μ_n generate the ideal \mathfrak{m} , then their images $\bar{\mu}_1, \dots, \bar{\mu}_n$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a k -vector space, proving finite dimensionality.

Conversely, let $\mu_1, \dots, \mu_n \in \mathfrak{m}$ such that their images $\bar{\mu}_1, \dots, \bar{\mu}_n$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a k -vector space. Then $\mathfrak{m} \subseteq \mu_1 R + \dots + \mu_n R + \mathfrak{m}^2$ hence $\mathfrak{m} = \mu_1 R + \dots + \mu_n R$ by Corollary 1.2.2 applied to $M = \mathfrak{m}$, $N = \mu_1 R + \dots + \mu_n R$. By Theorem 12, $\text{ht}(\mathfrak{m}) \leq n$. Thus,

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

finishing the proof. *q.e.d.*

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

(b) For algebraic varieties X , we call X **regular at $x \in X$** if $\mathcal{O}_{X,x}$ is regular. X is called **regular** if it is regular at all $x \in X$.

Remark 1. If R is any Noetherian ring and $\mathfrak{p} \in \text{Spec } R$, then $(\mathfrak{p}R_{\mathfrak{p}})/(\mathfrak{p}R_{\mathfrak{p}})^2 \simeq (\mathfrak{p}/\mathfrak{p}^2)_{\mathfrak{p}}$ and $R_{\mathfrak{p}}$ is regular (or R is regular at \mathfrak{p}) iff $\mathfrak{p}/\mathfrak{p}^2$ has dimension $\text{ht}(\mathfrak{p})$ as a $k(\mathfrak{p})$ -vector space. In particular, R is regular at $\mathfrak{m} \in \mathfrak{m}\text{-Spec } R$ iff $\dim(R_{\mathfrak{m}}) = \text{ht}(\mathfrak{m})$ equals $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. By a result by Serre (which has an easier proof in the classical situation $R = \mathcal{O}_{X,x}$), a regular local ring is regular at all of its prime ideals, i.e. if R is a regular local ring, then so is $R_{\mathfrak{p}}$ for any $\mathfrak{p} \in \text{Spec } R$.

A Noetherian ring R is called *regular* iff $R_{\mathfrak{p}}$ is regular for all $\mathfrak{p} \in \text{Spec } R$ or (equivalently) iff $R_{\mathfrak{m}}$ is regular for any $\mathfrak{m} \in \mathfrak{m}\text{-Spec } R$. These two definitions are equivalent as $R_{\mathfrak{p}} \simeq (R_{\mathfrak{m}})_{\mathfrak{p}}$ if $\mathfrak{p} \in \text{Spec } R$ is prime and \mathfrak{m} a maximal ideal containing \mathfrak{p} . Hence, if $R_{\mathfrak{m}}$ is regular then so is $R_{\mathfrak{p}}$ by Serre's result.

Note that despite Serre's theorem there are Noetherian rings R such that

$$\{\mathfrak{p} \in \text{Spec } R \mid R_{\mathfrak{p}} \text{ is not regular}\}$$

fails to be closed in $\text{Spec } R$.

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 satisfies the following equivalent conditions:

- (a) Every open subset is quasi-compact.
- (b) There is no infinite properly descending chain of closed subsets.
- (c) Every set of closed subsets of X has a \subseteq -minimal element.

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

- (a) If $X = X_1 \cup X_2$ where X_1 and X_2 are closed subsets, then $X = X_1$ or $X = X_2$. Also, $X \neq \emptyset$.
- (b) Any two non-empty open subsets of X have non-empty intersection.
- (c) Every non-empty open subset of X is dense.

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

Proposition 1. (a) *Any subset of a Noetherian topological space is Noetherian with its 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 and closed. We put

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

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

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

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

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

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

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

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

(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 $A \subseteq B \subseteq C \subseteq X$

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

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

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** $\deg \text{tr } L/K$ 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 $f: U \rightarrow k$ 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 $R = k[X_1, \dots, X_n] \rightarrow \mathcal{O}(X)$ 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*

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

Moreover, X is catenary and equality always holds in (2), i.e. $\dim Y + \text{codim}(Y, X) = \dim X$ 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

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

of irreducible closed subsets. To prove $\dim(k^n) \leq n$, and $\dim(X) \leq \deg \operatorname{tr}(K(X)/k)$, one proves $\deg \operatorname{tr}(\mathfrak{K}(\mathfrak{p})/k) > \deg \operatorname{tr}(\mathfrak{K}(\mathfrak{q})/k)$ 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 $X \xrightarrow{(f_1, \dots, f_d)} \mathbb{A}^d(k) = k^d$ (i.e., $\mathcal{O}(X)$ is integral over $k[f_1, \dots, f_d]$ and f_1, \dots, 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 ψ_S has the universal property (on the left) for such ring morphisms:

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

$$\begin{array}{ccc} R & \xrightarrow{\alpha} & A \\ \psi_S \searrow & & \nearrow \exists! \mu \\ & R_S & \end{array}$$

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

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

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

We have an equivalence of categories between the category of R_S -modules and the category of R -modules M on which $M \xrightarrow{s} M$ 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 $M \rightarrow M_S$, which has the universal property (on the left) for all morphisms from M to some R_S -module. It can be constructed as $\{\frac{m}{s} \mid m \in M, s \in S\} / \sim$ 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, \bar{L} an algebraic closure of L . Let $x \in L$. There is a unique monic generator $\text{Min}_{x/K}$ of the ideal $\{P \in K[T] \mid P(x) = 0\}$ in the principal ideal domain $K[T]$. Recall that

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

is called the *degree* and $\text{Min}_{x/K}$ 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** $\text{Tr}_{L/K}(x)$ 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,

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

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

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

where, for M a field, $\text{Tr}_M(f)$ 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

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

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

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

(d) We have

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

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

(e) We have $P_{x,L/K} = \text{Min}_{x/K}^{[L:K(x)]}$. 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 (ℓ_1, \dots, ℓ_k) of L/E and (e_1, \dots, e_m) of E/K and let M be the matrix representation of $E \xrightarrow{x} E$ 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 $L \xrightarrow{x} L$ 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 $P_{x,E/K} = \text{Min}_{x/K}$ since x is a zero of the left hand side by Cayley-Hamilton and $\deg P_{x,E/K} = [E : K] = [K(x) : K] = \deg(x/K) = \deg \text{Min}_{x/K}$ and both polynomials are normed. This shows (e).

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

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

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

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

if $f_{i,j} = 0$ for all $i > j$, as in that case, $\text{Mat}_{\mathcal{B}}(f)$ and hence also $\text{Mat}_{\tilde{\mathcal{B}}}(f)$ are upper triangular (block) matrices. But that's no problem since we can always choose \mathcal{B} in such a way that $\text{Mat}_{\mathcal{B}}(f)$ 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 $\text{char } K = 0$, then $\text{Min}_{x/K}$ is separable. Thus, $d = e$ and $\text{Min}_{x/K} = (T - x_1) \cdots (T - x_e)$ since the zeros of $\text{Min}_{x/K}$ are precisely the possible images of x under the K -linear embeddings $L \hookrightarrow \bar{L}$.

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

Let $y_1, \dots, y_{e'}$ be the zeros of μ in \bar{L} . Then $0 = \text{Min}_{x/K}(x_i) = \mu(x_i^{p^k})$, 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 $x_1^{p^k}, \dots, x_e^{p^k}$ are pairwise different. On the other hand, \bar{L} being algebraically closed, each y_i has a $p^{k^{\text{th}}}$ root $\eta \in \bar{L}$. Then $\text{Min}_{x/K}(\eta) = \mu(y_i) = 0$ and η must be among the x_i . Summarizing, we get $e = e'$ and $x_1^{p^k}, \dots, x_e^{p^k}$ are y_1, \dots, y_e in some order. Since μ factorizes into linear factors,

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

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 ψ_1, \dots, ψ_e be the different K -linear embeddings $K(x) \hookrightarrow \bar{L}$, $\psi_i(x) = x_i$. It is easy to see, that each of the ψ_i has the same number b of extensions to a K -linear embedding $\sigma: L \hookrightarrow \bar{L}$. Then by the previous step the left hand side is

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

Last thing we have to do is part (c). If $\text{char } K = 0$, then $\text{Min}_{x/K}$ is separable and thus $\text{Min}_{x/K} = T - x$ as $e = 1$. Then $x \in K$. By (d), in characteristic $p > 0$, there is a non-negative integer k such that $\text{Min}_{x/K} = (T - x)^{p^k} = T^{p^k} - x^{p^k}$, 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>.
- [2] H. Matsumura and M. Reid. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1989. ISBN: 9780521367646. URL: <http://www.math.unam.mx/javier/Matsumura.pdf>.