Real algebraic varieties

Florent Schaffhauser

Transcript of
Christian Merten (cmerten@mathi.uni-heidelberg.de)

WiSe 2022

Contents

Chapter 1

Algebraic sets

1.1 Polynomial equations

Let k be a field.

Definition 1.1. The *affine space of dimension* n is the set k^n.

Definition 1.2. An *algebraic subset* of k^n is a subset $V \subseteq k^n$ for which there exists a subset $A \subseteq k[x_1, \ldots, x_n]$ such that

$$V = \{x \in k^n \mid \forall P \in A \colon P(x) = 0\}.$$

Notation: $V = \mathcal{V}_{k^n}(A)$.

Remark 1.3. If $A \subseteq k[x_1, \ldots, x_n]$ is a subset and I is the ideal generated by A, then

$$\mathcal{V}(A) = \mathcal{V}(I).$$

Definition 1.4. Let $Z \subseteq k^n$ be a subset. Define the ideal in $k[x_1, \ldots, x_n]$

$$\mathcal{I}(Z) \coloneqq \{P \in k[x_1, \ldots, x_n] \mid \forall x \in Z \colon P(x) = 0\}.$$

Remark 1.5. Since $k[x_1, \ldots, x_n]$ is a Noetherian ring, all ideals are finitely generated. For $I \subseteq k[x_1, \ldots, x_n]$ there exist polynomials $P_1, \ldots, P_m \in k[x_1, \ldots, x_n]$ such that $I = (P_1, \ldots, P_m)$ and

$$\mathcal{V}(I) = \mathcal{V}(P_1, \ldots, P_m) = \mathcal{V}(P_1) \cap \ldots \cap \mathcal{V}(P_m).$$

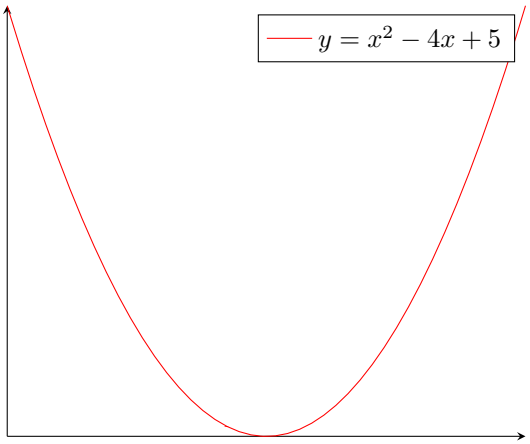


Figure 1.1: parabola

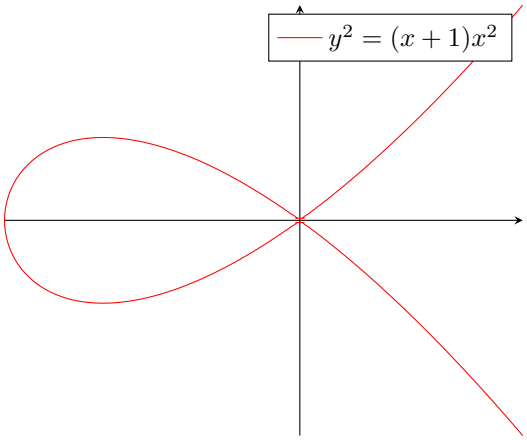


Figure 1.2: nodal cubic

Thus all algebraic subsets of k^n are intersections of hypersurfaces.

Proposition 1.6. *The maps*

$$\mathcal{I}\colon \{\textit{subsets of } k^n\} \longrightarrow \{\textit{ideals in } k[x_1, \ldots, x_n]\}$$

and

$$\mathcal{V}\colon \{\textit{ideals in } k[x_1, \ldots, x_n]\} \longrightarrow \{\textit{subsets of } k^n\}$$

satisfy the following properties

(i) $Z_1 \subseteq Z_2 \implies \mathcal{I}(Z_1) \supseteq \mathcal{I}(Z_2)$

(ii) $I_1 \subseteq I_2 \implies \mathcal{V}(I_1) \supseteq \mathcal{V}(I_2)$

(iii) $\mathcal{I}(Z_1 \cup Z_2) = \mathcal{I}(Z_1) \cap \mathcal{I}(Z_2)$

(iv) $\mathcal{I}(\mathcal{V}(I)) \supseteq I$

(v) $\mathcal{V}(\mathcal{I}(Z)) \supseteq Z$ *with equality if and only if* Z *is an algebraic set.*

Proof. Calculation. □

Lemma 1.7. *Let* $I, J \subseteq k[x_1, \ldots, x_n]$ *be ideals. Then*

$$\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$$

where IJ *is the ideal generated by the products* PQ*, where* $P \in I$ *and* $Q \in J$*.*

Lemma 1.8. *Let* $I_j \in k[x_1, \ldots, x_n]$ *be ideals. Then*

$$\bigcap_{j \in J} \mathcal{V}(I_j) = \mathcal{V}\left(\bigcup_{j \in J} I_j\right).$$

1.2 The Zariski topology

The algebraic subsets of k^n can be used to define a topology on k^n.

Proposition 1.9. *The algebraic subsets of k^n are exactly the closed sets of a topology on k^n.*

Proof. $\emptyset = \mathcal{V}(1)$ and $k^n = \mathcal{V}(0)$. The rest follows from 1.7 and 1.8. □

Definition 1.10. The topology on k^n where the closed sets are exactly the algebraic subsets of k^n, is called the *Zariski topology*.

Lemma 1.11. *(i) Let $Z \subseteq k^n$ be a subset. Then*

$$\overline{Z} = \mathcal{V}(\mathcal{I}(Z)).$$

(ii) Let $Z \subseteq k^n$ be a subset. Then

$$\sqrt{\mathcal{I}(Z)} = \mathcal{I}(Z).$$

(iii) Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then

$$\mathcal{V}(I) = \mathcal{V}(\sqrt{I}).$$

Proof. (i) Let $V = \mathcal{V}(I)$ be a Zariski-closed set such that $Z \subseteq V$. Then $\mathcal{I}(Z) \supseteq \mathcal{I}(V)$. But $\mathcal{I}(V) = \mathcal{I}(\mathcal{V}(I)) \supseteq I$, so $\mathcal{V}(\mathcal{I}(Z)) \subseteq \mathcal{V}(I) = V$. Thus

$$\mathcal{V}(\mathcal{I}(Z)) \subseteq \bigcap_{V \text{ closed}, Z \subseteq V} V = \overline{Z}.$$

Since $\mathcal{V}(I(Z))$ is closed, the claim follows.

□

Corollary 1.12. *For ideals $I, J \subseteq k[x_1, \ldots, x_n]$ we have*

$$\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ) = \mathcal{V}(I \cap J).$$

Proof. $\sqrt{I \cap J} = \sqrt{IJ}$ □

Proposition 1.13. *The Zariski topology turns k^n into a Noetherian topological space: If $(F_n)_{n \in N}$ is a decreasing sequence of closed sets, then $(F_n)_{n \in \mathbb{N}}$ is stationary.*

Proof. Let $V_1 \supseteq V_2 \supseteq \ldots$ be a decreasing sequence of closed sets. Then $\mathcal{I}(V_1) \subseteq \mathcal{I}(V_2) \subseteq \ldots$ is an increasing sequence of ideals in $k[x_1, \ldots, x_n]$. As $k[x_1, \ldots, x_n]$ is Noetherian, this sequence is stationary. Thus there exists $n_0 \in \mathbb{N}$ such that $\forall n \geq n_0$, $\mathcal{I}(V_n) = \mathcal{I}(V_{n_0})$. Therefore,

$$V_n = \mathcal{V}(\mathcal{I}(V_n)) = \mathcal{V}(\mathcal{I}(V_{n_0})) = V_{n_0}$$

for $n \geq n_0$. □

Definition 1.14. Let $P \in k[x_1, \ldots, x_n]$. The subset

$$D_{k^n}(P) \coloneqq k^n \setminus \mathcal{V}(P)$$

is called a *standard* or *principal open set* of k^n.

Remark 1.15. Since a Zariski-closed subset of k^n is an intersection of finitely many $\mathcal{V}(P_i)$, a Zariski-open subset of k^n is a union of finitely many standard open sets. Thus the standard open sets form a basis for the Zariski topology of k^n.

Proposition 1.16. *The affine space k^n is quasi-compact in the Zariski topology.*

Proof. Let $k^n = \bigcup_{i\in J} U_i$ where U_i is open. Since the standard opens form a basis of the Zariski topology, we can assume $U_i = D(P_i)$ with $P_i \in k[x_1, \ldots, x_n]$. Then $\mathcal{V}((P_i)_{i\in I}) = \bigcap_{i\in J} \mathcal{V}(P_i) = \emptyset$. Since $k[x_1, \ldots, x_n]$ is Noetherian, we can choose finitely many generators $P_{i_1}, \ldots, P_{i_m}$ such that $((P_i)_{i\in J}) = (P_{i_1}, \ldots, P_{i_m})$. Thus

$$\bigcap_{j=1}^{m} \mathcal{V}(P_{i_j}) = \mathcal{V}(P_{i_1}, \ldots, P_{i_m}) = \mathcal{V}((P_i)_{i\in J}) = \emptyset.$$

By passing to complements in k^n, we get

$$\bigcup_{j=1}^{m} D(P_{i_j}) = k^n.$$

□

Proposition 1.17. *Let $P \in k[x_1, \ldots, x_n]$ and let $f_P \colon k^n \to k$ be the associated function on k^n. Then f_p is continuous with respect to the Zariski topology on k^n and k.*

Proof. The closed proper subsets of k are finite subsets $F = \{t_1, \ldots, t_s\} \subseteq k$. The pre-image of a singleton $\{t\} \subseteq k$ is

$$f_P^{-1}(\{t\}) = \{x \in k^n \mid P(x) - t = 0\} = \mathcal{V}(P - t)$$

which is a closed subset of k^n. Thus

$$f_P^{-1}(F) = \bigcup_{i=1}^{s} \mathcal{V}(P - t_i)$$

is closed. □

Proposition 1.18. *If k is infinite, $\mathcal{I}(k^n) = \{0\}$.*

Proof. By induction: for $n = 1$, this follows because a non-zero polynomial only has a finite number of roots. Let $n \geq 1$ and $P \in \mathcal{I}(k^n)$. Thus $P(x) = 0\ \forall x \in k^n$. Let

$$P = \sum_{i=0}^{m} P_i(X_1, \ldots, X_{n-1}) X_n^i$$

for $P_i \in k[X_1, \ldots, X_{n-1}]$. Fix some $x_1, \ldots, x_{n-1} \in k$. Then $P(x_1, \ldots, x_{n-1}, y) \in k[y]$ has an infinite number of roots. Thus $P(x_1, \ldots, x_{n-1}, y) = 0$ for all $x_2, \ldots, x_n$ by the case $n = 1$, implying that $P_i(x_1, \ldots, x_{n-1}) = 0$ for all i. Since this holds for all $(x_1, \ldots, x_{n-1}) \in k^{n-1}$, $P_i = 0$ by induction for all i. □

1.3 Regular functions

Lemma 1.19. *If $U \subseteq k^n$ is a Zariski-open set and $f_P \colon k^n \to k$ is a polynomial function such that for $x \in U$, $f_P(x) \neq 0$, then the function $\frac{1}{f_P}$ is continuous on U.*

Proof. For all $t \in k$,

$$\begin{aligned}\left(\frac{1}{f_P}\right)^{-1}(\{t\}) &= \left\{x \in U \mid \frac{1}{f_P(x)} = t\right\} \\ &= \{x \in U \mid t f_P(x) - 1 = 0\} \\ &= \mathcal{V}(t f_P - 1) \cap U\end{aligned}$$

is closed in U. □

Remark 1.20. There can be many continous functions with respect to the Zariski topology. For instance, all bijective maps $f\colon k \to k$ are Zariski-continuous. In algebraic geometry, we will consider only functions which are locally defined by a rational function. We will define them on open subsets of algebrai sets $V \subseteq k^n$, endowed with the topology induced by the Zariski topology of k^n.

Remark 1.21. The open subsets of algebraic sets $V \subseteq k^n$ are exactly the *locally closed subsets* of k^n.

Definition 1.22. Let $X \subseteq k^n$ be a locally closed subset of k^n. A function $f\colon X \to k$ is called *regular at* $x \in X$, if there exist an open subset $x \in U \subseteq X$ and two polynomial functions $P_U, Q_U\colon U \to k$ such that for all $y \in U$, $Q_U(y) \neq 0$ and

$$f(y) = \frac{P_U(y)}{Q_U(y)}.$$

The function $f\colon X \to k$ is called *regular on* X if, for all $x \in X$, f is regular at x.

Example 1.23. A rational fraction $\frac{P}{Q} \in k(T_1, \ldots, T_n)$ defines a regular function on the standard open set $D(Q)$.

Proposition 1.24. *Let $X \subseteq k^n$ be a locally closed subset. If $f\colon X \to k$ is regular, then f is continous.*

Proof. Since continuity is a local property, we may assume $X = \Omega \subseteq k^n$ open and $f = \frac{P}{Q}$ for polynomial functions $P, Q\colon \Omega \to k$ such that $Q(y) \neq 0$. By 1.19 it suffices to prove that if $P, R\colon \Omega \to k$ are continuous, then $PR\colon \Omega \to k$, $z \mapsto P(z)R(z)$ is continuous. Let $t \in k$. Then

$$\begin{aligned}(PR)^{-1}(\{t\}) &= \{z \in \Omega \mid P(z)R(z) - t = 0\} \\ &= \mathcal{V}(PR - t) \cap \Omega\end{aligned}$$

is closed in Ω. □

Remark 1.25. Being a regular function is a local property.

Proposition 1.26. *Let $X \subseteq k^n$ be a locally closed subset of k^n, endowed with the induced topology. The map*

$$\begin{aligned}\mathcal{O}_X\colon \{\textit{open sets of } X\} &\longrightarrow k - \textit{algebras} \\ U &\longmapsto \{\textit{regular functions on } U\}\end{aligned}$$

defines a sheaf of sheaf of k-algebras on X, which is a subsheaf of the sheaf of functions.

Proof. Constants, sums and products of regular functions are regular, thus $\mathcal{O}_X(U)$ is a sub algebra of the k-algebra of functions $U \to k$. Since restricting a function preserves regularity, $\mathcal{O}_X$ is a presheaf. Since being regular is a local property and the presheaf of functions is a sheaf, $\mathcal{O}_X$ is also a sheaf. □

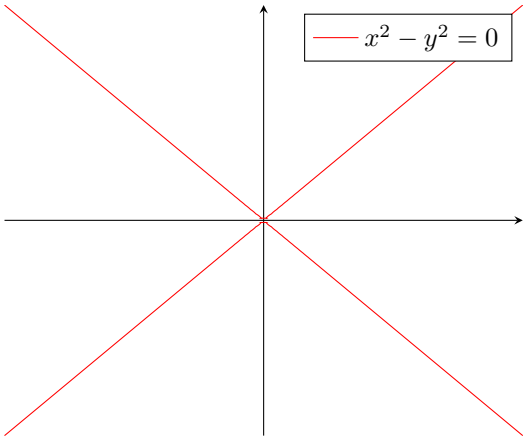


Figure 1.3: Reducible connected algebraic set

1.4 Irreducibility

Definition 1.27. Let X be a topological space. X is

(i) *irreducible* if $X \neq \emptyset$ and X is not the union of two proper closed subets, i.e. for $X = F_1 \cup F_2$ with $F_1, F_2 \subseteq X$ closed, we have $X = F_1$ or $X = F_2$.

(ii) *connected* if X is not the union of two disjoint proper closed subets, i.e. for $X = F_1 \cup F_2$ with $F_1, F_2 \subseteq X$ closed and $F_1 \cap F_2 = \emptyset$, we have $X = F_1$ or $X = F_2$.

A space X which is not irreducible, is called *reducible*.

Lemma 1.28. *If k is infinite, k is irreducible in the Zariski topology.*

Proof. Closed subsets of k are k and finite subsets of k. □

Remark 1.29. If k is finite, k^n is the finite union of its points, which are closed, so k^n is reducible.

Remark 1.30. X irreducible $\implies$ X connected, but the converse is false: Let k be infinite and consider $X = \mathcal{V}_{k^2}(x^2 - y^2)$ (see figure 1.3). Since $x^2 - y^2 = (x - y)(x + y) = 0$ in k if and only if $x = -y$ or $x = y$, we have $X = \mathcal{V}_{k^2}(x - y) \cup \mathcal{V}_{k^2}(x + y)$. Thus X is reducible. But $\mathcal{V}_{k^2}(x - y)$ and $\mathcal{V}_{k^2}(x + y)$ are homeomorphic to k, in particular irreducible and thus connected. Since $\mathcal{V}_{k^2} x - y \cap \mathcal{V}_{k^2}(x + y) \neq \emptyset$, X is connected.

Proposition 1.31. *Let X be a non-empty topological space. The following conditions are equivalent:*

(i) X is irreducible

(ii) If $U_1 \cap U_2 = \emptyset$ with U_1, U_2 open subsets of X, then $U_1 = \emptyset$ or $U_2 = \emptyset$.

(iii) If $U \subseteq X$ is open and non-empty, then U is dense in X.

Proof. Left as an exercise to the reader. □

Proposition 1.32. *Let X be a topological space and $V \subseteq X$. Then V is irreducible if and only if $\overline{V}$ is irreducible.*

Proof. Since $\emptyset$ is closed in X, we have $V = \emptyset \iff \overline{V} = \emptyset$.

($\Rightarrow$) Let $\overline{V} \subseteq Z_1 \cup Z_2$ with $Z_1, Z_2 \subseteq X$ closed. Then $V \subseteq Z_1 \cup Z_2$ and by irreducibility of V we may assume $V \subseteq Z_1$. Since Z_1 is closed, it follows $\overline{V} \subseteq Z_1$.

($\Leftarrow$) Let $V \subseteq Z_1 \cup Z_2$ with $Z_1, Z_2 \subseteq X$ closed. Since $Z_1 \cup Z_2$ is closed, we get $\overline{V} \subseteq Z_1 \cup Z_2$. By irreducibility of $\overline{V}$ we may assume $\overline{V} \subseteq Z_1$, thus $V \subseteq Z_1$. □

Corollary 1.33. *Let X be an irreducible topological space. Then every non-empty open subset $U \subseteq X$ is irreducible.*

Proof. By 1.31, $\overline{U} = X$ and thus irreducible. The claim follows now from 1.32. □

Lemma 1.34 (prime avoidance)**.** *Let $\mathfrak{p}$ be a prime ideal in a commutative ring A. If $I, J \subseteq A$ are ideals such that $IJ \subseteq \mathfrak{p}$, then $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.*

Proof. Assume that $I \not\subset \mathfrak{p}$ and $J \not\subset \mathfrak{p}$. Then there exist $a \in I$, such that $a \notin \mathfrak{p}$ and $b \in J$ such that $b \notin \mathfrak{p}$. But $ab \in IJ \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Contradiction. □

Theorem 1.35. *Let $V \subseteq k^n$ be an algebraic set. Then V is irreducible in the Zariski topology if and only if $\mathcal{I}(V)$ is a prime ideal in $k[T_1, \ldots, T_n]$.*

Proof. ($\Rightarrow$) Since $V \neq \emptyset$, $\mathcal{I}(V) \subsetneq k[T_1, \ldots, T_n]$. Let $P, Q \in k[T_1, \ldots, T_n]$ such that $PQ \in \mathcal{I}(V)$. For $x \in V$, $(PQ)(x) = 0$ in k, hence $P(x) = 0$ or $Q(x) = 0$. Thus $x \in \mathcal{V}(P) \cup \mathcal{V}(Q)$. Therefore $V = (\mathcal{V}(P) \cap V) \cup (\mathcal{V}(Q) \cap V)$ is the union of two closed subsets. Since V is irreducible, we may assume $V = \mathcal{V}(P) \cap V \subseteq \mathcal{V}(P)$, hence $P \in \mathcal{I}(V)$ and $\mathcal{I}(V)$ is prime.

($\Leftarrow$) $V \neq \emptyset$, since $\mathcal{I}(V)$ is a proper ideal. Let $V = V_1 \cup V_2$ with V_1, V_2 closed in V. Then

$$\mathcal{I}(V) = \mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2) \supseteq \mathcal{I}(V_1)\mathcal{I}(V_2).$$

By 1.34, we may assume $\mathcal{I}(V_1) \subseteq \mathcal{I}(V)$. But then

$$V_1 = \mathcal{V}(\mathcal{I}(V_1)) \supseteq \mathcal{V}(\mathcal{I}(V)) = V$$

since V_1 and V are closed. Therefore $V = V_1$ and V is irreducible. □

Corollary 1.36. *If k is infinite, the affine space k^n is irreducible with respect to the Zariski topology.*

Proof. Since k is infinite, $\mathcal{I}(k^n) = (0)$ by 1.18 which is a prime ideal in the integral domain $k[T_1, \ldots, T_n]$. □

Theorem 1.37. *Let $V \subseteq k^n$ be an algebraic set. Then there exists a decomposition*

$$V = V_1 \cup \ldots \cup V_r$$

such that

(i) V_i is a closed irreducible subset of k^n for all i.

(ii) $V_i \not\subset V_j$ for all $i \neq j$.

This decomposition is unique up to permutations.

Definition 1.38. For an algebraic set $V \subseteq k^n$, the V_i's in the decomposition in 1.37 are called the *irreducible components* of V.

Proof of 1.37. Existence: Let A be the set of algebraic sets $V \subseteq k^n$ that admit no finite decomposition into a union of closed irreducible subsets. Assume $A \neq \emptyset$. By noetherianity of k^n, there exists a minimal element $V \in A$. In particular V is not irreducible, so $V = V_1 \cup V_2$ with $V_1, V_2 \subsetneq V$. By minimality of V, $V_1, V_2 \notin A$, thus they admit a finite decomposition into a union of closed irreducible subsets. Since $V = V_1 \cup V_2$, the same holds for V. Contradiction. Removing the $V_i's$ for which $V_i \subseteq V_j$ for some j, we may assume that $V_i \not\subset V_j$ for $i \neq j$.

Uniqueness: Assume that $V = V_1 \cup \ldots \cup V_r$ and $V = W_1 \cup \ldots \cup W_s$ are decompositions that satisfiy (i) and (ii). Then

$$W_1 = W_1 \cap V = (W_1 \cap V_1) \cup \ldots \cup (W_1 \cap V_r).$$

Since W_1 is irreducible and $W_1 \cap V_i$ is closed in W_1, there exists j such that $W_1 = W_1 \cap V_j \subseteq V_j$. Likewise, there exists k such that $V_j \subseteq W_k$. Hence $W_1 \subseteq W_k$, which forces $k = 1$ (because for $k \neq 1$, we have $W_1 \subsetneq W_k$). Thus $W_1 = V_j$ and we can repeat the procedure with $W_2 \cup \ldots \cup W_s = \bigcup_{i \neq j} V_i$. □

Corollary 1.39. *Let $V \subseteq k^n$ be an algebraic set and denote by $V_1, \ldots, V_r$ the irreducible components of V. Let $W \subseteq V$ be an irreducible subset. Then $W \subseteq V_i$ for some i.*

Proof. We have

$$W = W \cap V = \bigcup_{i=1}^{r} \underbrace{W \cap V_i}_{\text{closed in } W}.$$

Since W is irreducible, there exists an i such that $W = W \cap V_i \subseteq V_i$. □

Remark 1.40. (i) The i in 1.39 is not unique in general. Consider

$$V = \{x^2 - y^2 = 0\} = \{x - y = 0\} \cup \{x + y = 0\}.$$

The closed irreducible subset $\{(0,0)\}$ lies in the intersection of the irreducible components of V.

(ii) In view of the corollary 1.39, theorem 1.37 implies that an algebraic set $V \subseteq k^n$ has a unique minimal decomposition into a union of closed irreducible subsets.

Corollary 1.41. *Let $V \subseteq k^n$ be an algebraic set. The irreducible components of V are exactly the maximal closed irreducible subsets of V. In terms of ideals in $k[T_1, \ldots, T_n]$, a closed subset $W \subseteq V$ is an irreducible component of V, if and only if the ideal $\mathcal{I}(W)$ is a prime ideal which is minimal among those containing $\mathcal{I}(V)$.*

Proof. A closed irreducible subset $W \subseteq V$ is contained in an irreducible component $V_j \subseteq V$ by 1.39. If W is maximal, then $W = V_j$.

Conversely, if V_j is an irreducible component of V and $V_j \subseteq W$ for some irreducible and closed subset $W \subseteq V$, again by 1.39 we have $W \subseteq V_i$ for some i, therefore $V_j \subseteq V_i$ which implies $i = j$ and $V_j = W$. □

Proposition 1.42 (Identity theorem for regular functions)**.** *Let $X \subseteq k^n$ be an irreducible algebraic set and let $U \subseteq X$ be open. Let $f, g \in \mathcal{O}_X(U)$ be regular functions on U. If there is a non-empty open set $U' \subseteq U$ such that $f|_{U'} = g|_{U'}$, then $f = g$ on U.*

Proof. The set $Y = \mathcal{V}_U(f - g)$ is closed in U and contains U'. Thus the closure $\overline{U'}^{(U)}$ of U' in U is also contained in Y. By 1.33 U is irreducible, so U' is dense in U. Therefore $Y = U$. □

Example 1.43. If k is infinite and $P \in k[T_1, \ldots, T_n]$ is zero outside an algebraic set $V \subseteq k^n$, then $P = 0$ on k^n.

1.5 Plane algebraic curves

Theorem 1.44. *If $f \in k[x,y]$ is an irreducible polynomial such that $\mathcal{V}(f)$ is infinite, then $\mathcal{I}(\mathcal{V}(f)) = (f)$. In particular, $\mathcal{V}(f)$ is irreducible in this case.*

Remark 1.45. (i) If k is algebraically closed and $n \geq 2$, then for all $f \in k[x_1, \ldots, x_n]$ non-constant, the zero set $\mathcal{V}(f)$ is necessarily infinite.

(ii) The assumption $\mathcal{V}(f)$ infinite is necessary for the conclusion of 1.44 to hold: The polynomial

$$f(x,y) = (x^2-1)^2 + y^2$$

is irreducible because, as a polynomial in y, it is monic and does not have a root in $\mathbb{R}[x]$ (for otherwise there would be a polynomial $P(x) \in \mathbb{R}[x]$ such that $P(x)^2 = -(x^2-1)^2$) and the zero set of f is

$$\mathcal{V}(f) = \{(1,0)\} \cup \{(-1,0)\},$$

which is reducible.

(iii) 1.44 does not hold in this form for hypersurfaces of k^n for $n \geq 3$. For instance, the polynomial

$$f(x,y,z) = x^2y^2 + z^4 \in \mathbb{R}[x,y,z]$$

is irreducible and the hypersurface

$$\mathcal{V}(f) = \{(0,y,0) \colon y \in \mathbb{R}\} \cup \{(x,0,0) \colon x \in \mathbb{R}\}$$

is infinite. However, the function

$$P \colon (x,y,z) \mapsto xy$$

belongs to $\mathcal{I}(\mathcal{V}(f))$ but not to (f). Moreover, $P \in \mathcal{I}(\mathcal{V}(f))$ but neither x nor y are in $\mathcal{I}(\mathcal{V}(f))$, so this ideal is not prime.

(iv) Take $f(x,y) = (x-a)^2 + y^2 \in \mathbb{R}[x,y]$ which is irreducible. Then $\mathcal{V}(f) = \{(a,0)\}$ is irreducible, and $\mathcal{I}(\mathcal{V}(f)) = (x-a, y) \supsetneq (f)$. In particular, (f) is a non-maximal prime ideal.

We need a special case of the famous Bézout theorem, for which we need a result from algebra. For an integral domain R denote by $Q(R)$ its fraction field. If R is a factorial ring then $q \in R[T]$ is called *primitve* if it is non-constant and its coefficients are coprime in R.

Proposition 1.46 (Gauß)**.** *Let R be a factorial ring. Then $R[T]$ is also factorial. A polynomial $q \in R[T]$ is prime in $R[T]$ if and only if*

(i) $q \in R$ and q is prime in R, or

(ii) q is primitve in $R[T]$ and prime in $Q(R)[T]$

Proof. Any algebra textbook. □

Proposition 1.47. *Let R be a factorial ring and $f, g \in R[X]$ coprime. Then f and g are coprime in $Q(R)[X]$.*

Proof. Let $h = \frac{a}{b} \in Q(R)[X]$ be a common irreducible factor of f and g with $a \in R[X]$ and $b \in R \setminus 0$. By Gauß $R[X]$ is factorial, thus we may assume a irreducible. Then

$$\frac{f}{1} = \frac{p_1}{q_1}\frac{a}{b} \text{ and } \frac{g}{1} = \frac{p_2}{q_2}\frac{a}{b}$$

for some $p_1, p_2 \in R[X]$ and $q_1, q_2 \in R \setminus 0$. So $p_1 a = f q_1 b$ and $p_2 a = g q_2 b$. a neither divides q_1, q_2 nor b, for otherwise $a \in R \setminus 0$ by the degree formula for polynomials and h is a unit. Since a divides $f q_1 b$ and $g q_2 b$ and, since $R[X]$ is factorial, a is prime in $R[X]$ and thus $a \mid f$ and $a \mid g$. □

Lemma 1.48 (Special case of Bézout)**.** *Let $f, g \in k[x,y]$ be two polynomials without common factors in $k[x,y]$. Then the set $\mathcal{V}(f) \cap \mathcal{V}(g)$ is finite.*

Proof. Since $k(x)[y]$ is a principal ideal domain, 1.47 implies $(f,g) = k(x)[y]$, hence the existence of $A(x,y), B(x,y), M(x), N(x)$ such that

$$f(x,y)A(x,y) + g(x,y)B(x,y) = \underbrace{M(x)N(x)}_{=:D(x)}$$

with $D(x) \in k[x]$. Since a common zero (x,y) of f and g gives a zero of D, and D has finitely many zeros, there are only finitely many x such that (x,y) is a zero of both f and g. But, for fixed $x \in k$, the polynomial

$$y \mapsto f(x,y) - g(x,y)$$

has only finitely many zeros in k. So $\mathcal{V}(f) \cap \mathcal{V}(g)$ is finite. □

Proof of 1.44. Let $f \in k[x,y]$ be irreducible such that $\mathcal{V}(f) \subseteq k^2$ is infinite. Since $f \in \mathcal{I}(\mathcal{V}(f))$, it suffices to show that $\mathcal{I}(\mathcal{V}(f)) \subseteq (f)$. Let $g \in \mathcal{I}(\mathcal{V}(f))$. Then $\mathcal{V}(f) \subseteq \mathcal{V}(g)$. Thus

$$\mathcal{V}(f) \cap \mathcal{V}(g) = \mathcal{V}(f)$$

which is infinite by assumption. Thus by 1.48, f and g have a common factor. Since f is irreducible, this implies that $f \mid g$, i.e. $g \in (f)$. □

We can use 1.44 to find the irreducible components of a hypersurface $\mathcal{V}(P) \subseteq k^2$.

Corollary 1.49. *Let $P \in k[x,y]$ be non-constant and $P = uP_1^{n_1} \cdots P_r^{n_r}$ be the decomposition into irreducible factors. If each $\mathcal{V}(P_i)$ is infinite, then the algebraic sets $\mathcal{V}(P_i)$ are the irreducible components of $\mathcal{V}(P)$.*

Proof. Note that

$$\mathcal{V}(P) = \mathcal{V}(P_1^{n_1} \cdots P_r^{n_r}) = \mathcal{V}(P_1) \cup \ldots \cup \mathcal{V}(P_r).$$

Since P_i is irreducible and $\mathcal{V}(P_i)$ is infinite for all i, by 1.44 $\mathcal{V}(P_i)$ is irreducible and for $i \neq j$ $\mathcal{V}(P_i) \not\subset \mathcal{V}(P_j)$, for otherwise

$$(P_i) = \mathcal{I}(\mathcal{V}(P_i)) \supset \mathcal{I}(\mathcal{V}(P_j)) = (P_j)$$

which is impossible for distinct irreducible elements P_i, P_j. □

Example 1.50 (Real plane cubics)**.** Let $P(x,y) = y^2 - f(x)$ with $\deg_x f = 3$ in $k[x]$. Since $\deg_y P \geq 1$ and the leading coefficient of P is 1, the polynomial P is primitive in $k[x][y]$. It is reducible in $k(x)[y]$ if and only if there exists $a(x), b(x) \in k(x)$ such that $(y-a)(y-b) = y^2 - f$, i.e. $b = -a$ and $f = a^2$ in $k(x)$, therefore also in $k[x]$. Since $\deg_x f = 3$, this cannot happen. So, P is irreducible by 1.46.

Moreover, when $k = \mathbb{R}$, the cubic polynomial $f(x)$ takes on an infinite number of positive values, so $\mathcal{V}(y^2 - f(x)) = \mathcal{V}(P)$ is infinite. In conclusion, real cubics of the form $y^2 - f(x) = 0$ are irreducible algebraic sets in $\mathbb{R}^2$ by 1.44.

Proposition 1.51. *Let k be an algebraically closed field and let $P \in k[T_1, \ldots, T_n]$ be a non-constant polynomial with $n \geq 2$. Then $\mathcal{V}(P)$ is infinite.*

Proof. Since P is non-constant, we may assume that $\deg_{x_1} P \geq 1$. Write

$$P(T_1, \ldots, T_n) = \sum_{i=1}^{d} g_i(T_2, \ldots, T_n) T_1^i,$$

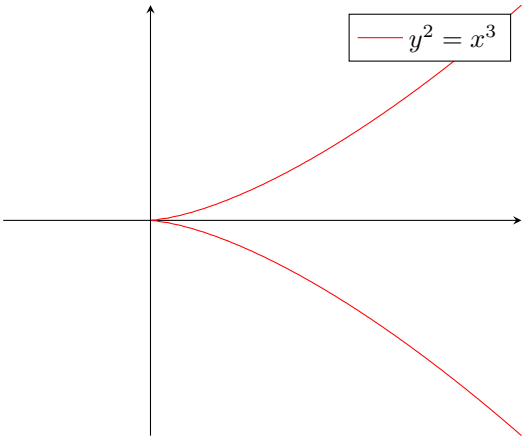


Figure 1.4: the cuspidal cubic

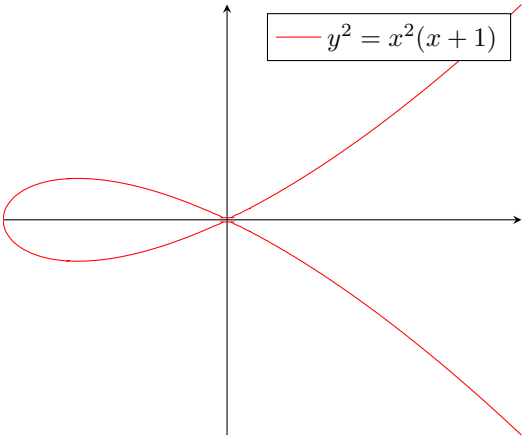


Figure 1.5: the nodal cubic

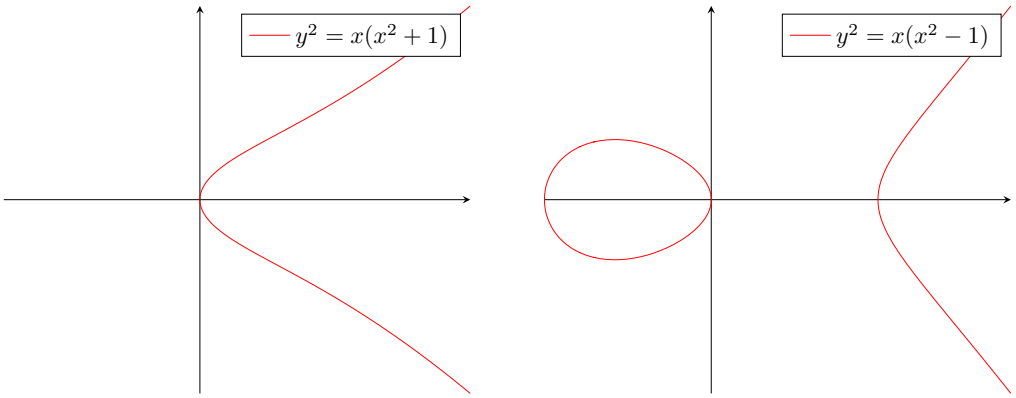


Figure 1.6: the smooth cubics: the second curve demonstrates that the notion of connectedness in the Zariski topologoy of $\mathbb{R}^2$ is very different from the one in the usual topology of $\mathbb{R}^2$.

with $d \geq 1$ and $g_d \neq 0$. Then $D_{k^{n-1}}(g_d)$ is infinite: Since $g_d \neq 0$ and k infinite, it is non-empty. Thus let $(a_2, \ldots, a_n) \in k^{n-1}$ such that $g_d(a) \neq 0$. Then $g_d(ta) = g_d(ta_2, \ldots, ta_n) \in k[t]$ is a non-zero polynomial and thus has only finitely many zeros in k. In particular $D_{k^{n-1}}(g_d)$ is infinite.

For $(a_2, \ldots, a_{n-1}) \in D_{k^{n-1}}(g_d)$, $P(T_1, a_2, \ldots, a_n) \in k[T_1]$ is non-constant and thus has a root a_1 in the algebraically closed field k. Hence $(a_1, \ldots, a_n) \in \mathcal{V}(P)$. □

We finally give a complete classification of irreducible algebraic sets in the affine plane k^2 for an infinite field k.

Proposition 1.52. *Let k be an infinite field. Then the irreducible algebraic subsets of k^2 are:*

(i) the whole affine plane k^2

(ii) single points $\{(a, b)\} \subseteq k^2$

(iii) infinite algebraic sets defined by an irreducible polynomial $f \in k[x, y]$.

Proof. Let $V \subseteq k^2$ be an irreducible algebraic subset of the affine plane. If V is finite, it reduces to a point. So we may assume V infinite. If $\mathcal{I}(V) = (0)$, then $V = k^2$. Otherwise, there is a non-constant polynomial $P \in k[x, y]$ such that P vanishes on V. Since V is irreducible, $\mathcal{I}(V)$ is prime, so it contains an irreducible factor f of P. Let $g \in \mathcal{I}(V)$. Then $V \subseteq \mathcal{V}(f) \cap \mathcal{V}(g)$, but since V is infinite, f and g must have a common factor. By irreducibility of f, it follows $f \mid g$, i.e. $g \in (f)$. Hence $\mathcal{I}(V) = (f)$ and $V = \mathcal{V}(f)$. □

1.6 Prime ideals in $k[x, y]$

Proposition 1.53. *Let A be a principal ideal domain. Let $\mathfrak{p} \subseteq A[X]$ be a prime ideal. Then $\mathfrak{p}$ satisfies exactly one of the following three mutually exclusive possibilities:*

(i) $\mathfrak{p} = (0)$

(ii) $\mathfrak{p} = (f)$, where $f \in A[X]$ is irreducible

(iii) $\mathfrak{p} = (a, q)$, where $a \in A$ is irreducible and $q \in A[X]$ such that its reduction modulo aA is an irreducible element in $A/aA[X]$. In this case, $\mathfrak{p}$ is a maximal ideal.

Proof. Let $\mathfrak{p} \subseteq A[X]$ be a prime ideal. If $\mathfrak{p}$ is principal, then $\mathfrak{p} = (f)$ for some $f \in A[X]$. If $f = 0$, we are done. Otherwise, since $A[X]$ is factorial by Gauß and $\mathfrak{p}$ is prime, f is irreducible.

Let now $\mathfrak{p}$ not be principal. Then there exist $f, g \in \mathfrak{p}$ without common factors in $A[X]$. By 1.47, they also have no common factors in the principal ideal domain $Q(A)[X]$, so $Mf + Ng = 1$ for some $M, N \in Q(A)[X]$. By multiplying with the denominators, we obtain $Pf + Qg = b$ for some $b \in A$ and $P, Q \in A[X]$. So $b \in (f, g) \subseteq \mathfrak{p}$, thus there is an irreducible factor a of b in A such that $a \in \mathfrak{p}$. Moreover, $aA[X] \subsetneq \mathfrak{p}$ since $\mathfrak{p}$ is not principal. Now consider the prime ideal

$$\mathfrak{p}/aA[X] \subset A[X]/aA[X] \simeq (A/aA)[X].$$

Since A is a PID and a is irreducible, A/aA is a field and $(A/aA)[X]$ a PID. So $\mathfrak{p}/aA[X]$ is generated by an irreducible element $\overline{q} \in (A/aA)[X]$ for some $q \in A[X]$. Thus $\mathfrak{p} = (a, q)$. Moreover

$$A[X]/\mathfrak{p} \simeq \left(A/aA\right)[X]/\left(\mathfrak{p}/aA\right)[X] = \left(A/aA\right)[X]/\overline{q}\left(A/aA\right)[X]$$

which is a field since $\left(A/aA\right)[X]$ is a PID. So $\mathfrak{p}$ is maximal in $A[X]$. □

Using 1.53 we can give a simple proof for the classification of maximal ideals of $k[T_1,\dots,T_n]$ when k is algebraically closed and $n=2$.

Corollary 1.54. *If k is algebraically closed, a maximal ideal $\mathfrak{m}$ of $k[x,y]$ is of the form $\mathfrak{m} = (x-a, y-b)$ with $(a,b) \in k^2$. In particular, principal ideals are never maximal.*

Proof. Since $\mathfrak{m}$ is maximal, it is prime and $\mathfrak{m} \neq (0)$. By 1.53, $\mathfrak{m} = (P, f)$ with $P \in k[x]$ irreducible and $f \in k[x,y]$ such that its image $\overline{f}$ in $(k[x]/(P))[y]$ is irreducible or $\mathfrak{m} = (f)$ for $f \in k[x,y]$ irreducible.

(1) $\mathfrak{m} = (P, f)$. Since k is algebraically closed and $P \in k[x]$ is irreducible, $P = x - a$ for some $a \in k$.
$$k[x]/(P) = k[x]/(x-a) \simeq k.$$
Since $\overline{f} \in k[y]$ is also irreducible, $\overline{f} = y - b$ for some $b \in k$.

(2) $\mathfrak{m} = (f)$. Since $k = \overline{k}$, $\mathcal{V}(f)$ is infinite, in particular $\mathcal{V}(f) \neq \emptyset$. Then if $(a,b) \in \mathcal{V}(f)$,
$$(x-a, y-b) = \mathcal{I}(\{(a,b)\}) \supset \mathcal{I}(\mathcal{V}(f)) \supset (f).$$
Since (f) is maximal, it follows that $(f) = (x-a, y-b)$, which is impossible since $x-a$ and $y-b$ habe no common factors in $k[x,y]$.

□

Remark 1.55. The ideal (x^2+1, y) is maximal in $\mathbb{R}[x,y]$ and is not of the form $(x-a, y-b)$ for $(a,b) \in \mathbb{R}^2$. Indeed,
$$\mathbb{R}[x,y]\big/(x^2+1, y) \simeq (\mathbb{R}[y]/y\mathbb{R}[y])\,[x]\big/(x^2+1) \simeq \mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}.$$

Proposition 1.56. *Let k be an algebraically closed field. Then the maps $V \mapsto \mathcal{I}(V)$ and $I \mapsto \mathcal{V}(I)$ induce a bijection*
$$\{\textit{irreducible algebraic subsets of } k^2\} \longleftrightarrow \{\textit{prime ideals in } k[x,y]\}$$
through wich we have correspondences
$$\begin{aligned} \textit{points } (a,b) \in k^2 &\longleftrightarrow \textit{maximal ideals } (x-a, y-b) \textit{ in } k[x,y] \\ \textit{proper, infinite, irreducible algebraic sets} &\longleftrightarrow \textit{prime ideals } (f) \subseteq k[x,y] \textit{ with } f \textit{ irreducible} \\ k^2 &\longleftrightarrow (0). \end{aligned}$$

Proof. Let $V \subseteq k^2$ be an irreducible algebraic set. By 1.52 we can distinguish the following cases:

(i) If $V = k^2$, then $\mathcal{I}(V) = (0)$ since k is infinite and $\mathcal{I}(\mathcal{V}(0)) = (0)$.

(ii) If $V = \{(a,b)\}$, then $\mathcal{I}(V) \supset (x-a, y-b) =: \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\mathcal{I}(V) = \mathfrak{m}$. Since $V = \mathcal{V}(\mathfrak{m})$, this also shows $\mathcal{I}(\mathcal{V}(\mathfrak{m})) = \mathfrak{m}$.

(iii) If $V = \mathcal{V}(f)$ where $f \in k[x,y]$ is irreducible, then by 1.44 $\mathcal{I}(\mathcal{V}(f)) = (f)$.

So, every irreducible algebraic set $V \subseteq k^2$ is of the form $\mathcal{V}(\mathfrak{p})$ for some prime ideal $\mathfrak{p} \subseteq k[x,y]$. Moreover,
$$\mathcal{I}(\mathcal{V}(\mathfrak{p})) = \mathfrak{p}.$$
Let now $\mathfrak{p}$ be a prime ideal in $k[x,y]$. By 1.53 we can dinstiguish the following cases:

(i) $\mathfrak{p} = (0)$: Then $\mathcal{V}(\mathfrak{p}) = k^2$ and since k is infinite, k^2 is irreducible.

(ii) $\mathfrak{p}$ maximal: Then by 1.54, $\mathfrak{p} = (x-a, y-b)$ for some $(a,b) \in k^2$. So $\mathcal{V}(m) = \{(a,b)\}$ is irreducible.

(iii) $\mathfrak{p} = (f)$ with $f \in k[x,y]$ irreducible. Since $k = \overline{k}$, $\mathcal{V}(f)$ is infinite and hence by 1.44 irreducible.

Thus the maps in the proposition are well-defined, mutually inverse and induce the stated correspondences. □

Corollary 1.57. *Assume that k is algebraically closed and let $\mathfrak{p} \subseteq k[x,y]$ be a prime ideal. Then*

$$\mathfrak{p} = \bigcap_{\mathfrak{m} \text{ maximal}, \mathfrak{m} \supset \mathfrak{p}} \mathfrak{m}.$$

Proof. If $\mathfrak{p}$ is maximal, there is nothing to prove. If $\mathfrak{p} = (0)$, $\mathfrak{p}$ is contained in $(x-a, y-b)$ for $(a,b) \in k^2$. Since k is infinite, the intersection of these ideals is (0). Otherwise, by 1.56, $\mathfrak{p} = (f)$ for some $f \in k[x,y]$ irreducible. Then, since $k = \overline{k}$, $\mathcal{V}(f)$ is infinite and with 1.44:

$$\mathfrak{p} = (f) = \mathcal{I}(\mathcal{V}(f)) = \mathcal{I}\left(\bigcup_{(a,b)\in\mathcal{V}(f)} \{(a,b)\}\right) \supset \bigcap_{(a,b)\in\mathcal{V}(f)} \mathcal{I}(\{(a,b)\}) \supset (f) = \mathfrak{p}.$$

By 1.56, the ideals $\mathcal{I}(\{(a,b)\})$ for $(a,b) \in \mathcal{V}(f)$ are exactly the maximal ideals containing $(f) = \mathfrak{p}$. □

Corollary 1.58. *Let $\mathfrak{p} \subseteq k[x,y]$ be a non-principal prime ideal. Then $\mathcal{V}(\mathfrak{p}) \subseteq k^2$ is finite.*

Proof. Since $\mathfrak{p}$ is not principal, there exist $f, g \in \mathfrak{p}$ without common factors. Since $(f,g) \subset \mathfrak{p}$, we have

$$\mathcal{V}(f) \cap \mathcal{V}(g) = \mathcal{V}(f,g) \supset \mathcal{V}(\mathfrak{p})$$

and the left hand side is finite by 1.48. □

1.7 The tangent cone and the Zariski tangent space

1.7.1 The tangent cone at a point

Let $X \subseteq k^n$ be a non-empty Zariski-closed subset.

Let $P \in k[T_1, \ldots, T_n]$ be a polynomial. For all $x \in k^n$, we have a Taylor expansion at x: For all $h \in k^n$:

$$P(x+h) = P(x) + P'(x)h + \frac{1}{2}P''(x)(h,h) + \underbrace{\cdots}_{\text{finite number of terms}}$$
$$= \sum_{d=0}^{\infty} \frac{1}{d!} P^{(d)}(x)(\underbrace{h, \ldots, h}_{d \text{ times}}).$$

Remark 1.59. The term $\frac{1}{d!}P^{(d)}(x)$ is a homogeneous polynomial of degree d in the coordinates of $h = (h_1, \ldots, h_n)$:

$$P^{(d)}(x)(h, \ldots, h) = \sum_{\alpha \in \mathbb{N}_0^n, |\alpha| = d} \frac{d!}{\alpha_1! \cdots \alpha_n!} \frac{\partial^{|\alpha|}}{\partial T_1^{\alpha_1} \cdots \partial T_n^{\alpha_n}} P(x) h_1^{\alpha_1} \cdots h_n^{\alpha_n}.$$

Also, when $x = 0_{k^n}$ and if we write

$$P = P(0) + \sum_{d=1}^{\infty} Q_d$$

with Q_d homogeneous of degree d, then for all $h = (h_1, \dots, h_n) \in k^n$, we have

$$\frac{1}{d!} P^{(d)}(0) \cdot (h, \dots, h) = Q_d(h_1, \dots, h_n).$$

For all $P \in \mathcal{I}(X) \setminus \{0\}$, we denote by P_x^* the *initial term* in the Taylor expansion of P at x, i.e. the term $\frac{1}{d!} P^{(d)}(x) \cdot (h, \dots, h)$ for the smallest $d \geq 1$ such that this is not zero. If $P = 0$, we put $P_x^* := 0$.

Definition 1.60. We set $\mathcal{I}(X)_x^*$ to be the ideal generated by P_x^* for all $P \in \mathcal{I}(X)$.

Remark 1.61. The ideal $\mathcal{I}(X)^*$ is finitely generated. However, if $\mathcal{I}(X) = (P_1, \dots, P_m)$, it is not true in general that $\mathcal{I}(X)_x^* = ((P_1)_x^*, \dots, (P_m)_x^*)$. We may need to add the initial terms at x of some other polynomials of the form $\sum_{k=1}^m P_k Q_k \in \mathcal{I}(X)$.

If $\mathcal{I}(X) = (P)$ is principal though, we have $\mathcal{I}(X)_x^* = (P_x^*)$.

Definition 1.62. The *tangent cone* to X at x is the affine algebraic set

$$\mathcal{C}_x^{(X)} := x + \mathcal{V}_{k^n}(\mathcal{I}(X)_x^*) = \{x + h \colon h \in \mathcal{V}_{k^n}(\mathcal{I}(X)_x^*)\}.$$

Remark 1.63. The algebraic set $\mathcal{C}_x(X)$ is a cone at x: It contains x and for all $x + h \in \mathcal{C}_x(X)$ for some $h \in \mathcal{V}_{k^n}(\mathcal{I}(X)_x^*)$, we have for all $\lambda \in k^\times$, $\lambda h \in \mathcal{V}_{k^n}(\mathcal{I}(X)_x^*)$, i.e. $x + \lambda h \in \mathcal{C}_x(X)$.

Indeed, $P_x^* \in \mathcal{I}(X)_x^*$ is either zero or a homogeneous polynomial of degree $r \geq 1$. Thus for $h \in k^n$ and $\lambda \in k^\times$: $P_x^*(\lambda h) = \lambda^r P_x^*(h)$ which is 0 if and only if $P_x^*(h) = 0$.

Example 1.64. Let k be an infinite field and let $P \in k[x, y]$ be an irreducible polynomial such that $X := \mathcal{V}(P)$ is infinite. Then we know that $\mathcal{I}(X) = (P)$. Then we can determine $\mathcal{C}_X(X)$ by computing the successive derviatives of P at x: In this case $\mathcal{I}(X)_x^* = (P_x^*)$. For convenience wie will mostly consider examples for which $x = 0_{k^2}$.

(i) $P(x, y) = y^2 - x^3$. Then $P_{(0,0)}^* = y^2$, so the tangent cone at $(0, 0)$ is the algebraic set

$$\mathcal{C}_{(0,0)}(X) = \{(x, y) \in k^2 \mid y^2 = 0\}.$$

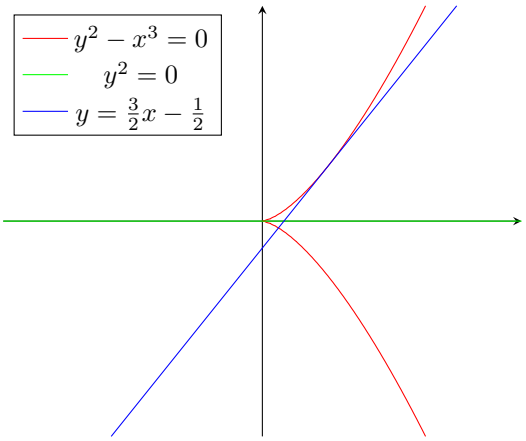


Figure 1.7: The green line is the tangent cone at $(0, 0)$ and the blue line the tangent cone at $(1, 1)$.

Note that $P_{(1,1)}^*(h_1, h_2) = 2h_2 - 3h_1$, so the tangent cone at $(1, 1)$ is

$$\begin{aligned} \mathcal{C}_{(1,1)}(X) &= \{(1 + h_1, 1 + h_2) \mid 2h_2 - 3h_1 = 0\} \\ &= \left\{(x, y) \in k^2 \mid y = \frac{3}{2}x - \frac{1}{2}\right\}. \end{aligned}$$

(ii) $P(x,y) = y^2 - x^2(x+1)$. Then $P^*_{(0,0)} = y^2 - x^2$ so

$$\mathcal{C}_{(0,0)}(X) = \{y^2 - x^2 = 0\}$$

which is a union of two lines.

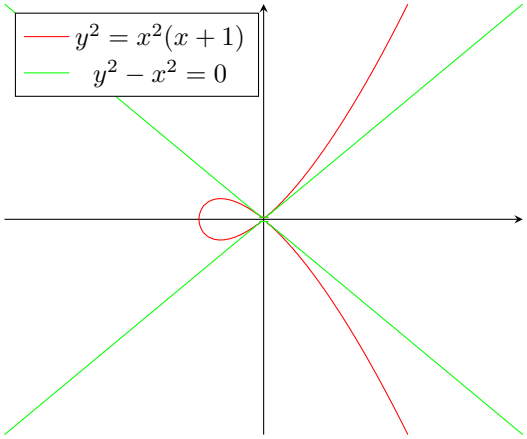


Figure 1.8: The green line is the tangent cone at $(0,0)$.

In contrast, $P^*_{(1,1)}(h_1,h_2) = 2h_2 - 5h_1$ so

$$\mathcal{C}_{(1,1)}(X) = \left\{(x,y) \in k^2 \mid y = \frac{5}{2}x - \frac{3}{2}\right\},$$

which is just one line. Evidently this is related to the origin being a „node“ of the curve of equation $y^2 - x^2(x+1) = 0$.

Remark 1.65. (i) The tangent cone $\mathcal{C}_x(X)$ represents all directions coming out of x along which the initial term P^*_x vanishes, for all $P \in \mathcal{I}(X)$. In that sense, it is the least complicated approximation to X around x, in terms of the degrees of the polynomials involved.

(ii) The notion of tangent cone at a point enables us to define singular points of algebraic sets and even distinguish between the type of singularities: Let $\mathcal{I}(X) = (P)$.

When $\deg(P^*_x) = 1$, the tangent cone to $X \subseteq k^n$ at x is just an affine hyperplane, namely $x + \ker P'(x)$, since $P^*_x = P'(x)$ in this case. The point x is then called *non-singular*.

When $\deg(P^*_x) = 2$, we say that X has a *quadratic singularity* at x. If $X \subseteq k^2$, a quadratic singularity is called a *double point*. In that case, $P^*_x = \frac{1}{2}P''(x)$ is a quadratic form on k^2. If it is non-degenerate, then x is called an *ordinary* double point. For instance, if X is the nodal cubic of equation $y^2 = x^2(x+1)$, then the origin is an ordinary double point (also called a *node*), since $\frac{1}{2}P''(0,0)$ is the quadratic form associated to the symmetric matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. But if X is the cuspidal cubic of equation $y^2 = x^3$, then the origin is *not* an ordinary double point, since $\frac{1}{2}P''(0,0)$ corresponds to $\begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$. Instead, the origin is a *cusp* in the following sense. We can write

$$P(x,y) = l(x,y)^2 + Q_3(x,y) + \dots$$

with $l(x,y) = \alpha x + \beta y$ a linear form in (x,y), and the double point $(0,0)$ is called a cusp if $Q_3(\beta,-\alpha) \neq 0$. This means that

$$t^4 XP(\beta t, -\alpha t)$$

in $k[t]$. And this is indeed what happens for $P(x,y) = y^2 - x^3$, since $l(x,y) = y$ and $Q_3(x,y) = -x^3$.

Remark 1.66. One can define the *multiplicity* of a point $(x,y) \in \mathcal{V}_{k^2}(P)$ as the smallest integer $r \geq 1$ such that $P^{(r)}(x,y) \neq 0$. If $P^{(r)}(x,y) \cdot (h,\ldots,h) = 0 \implies h = 0_{k^2}$, the singularity (x,y) is called *ordinary*. If k is algebraically closed and $(x,y) = (0,0)$, we can write $P^{(r)}(0,0) = \prod_{i=1}^{m}(\alpha_i x + \beta_i y)^{r_i}$, with $r_1 + \ldots + r_m = r$. Then $(0,0)$ is an ordinary singularity of multiplicity r iff $r_i = 1$ for all i. For instance, $(0,0)$ is an ordinary triple point of the trefoil curve $P(x,y) = (x^2+y^2)^2 + 3x^2y - y^3$.

1.7.2 The Zariski tangent space at a point

Let $X \subseteq k^n$ be a Zariski-closed subset and $x \in X$.

The tangent cone is in general not a linear approximation. To remedy this, one can consider the Zariski tangent space to X at a point $x \in X$.

Definition 1.67. The *Zariski tangent space* to X at x is the affine subspace

$$T_x X \coloneqq x + \bigcap_{P \in \mathcal{I}(X)} \ker\, P'(x).$$

Remark 1.68. By translation, $T_x X$ can be canonically identified to the vector space $\bigcap_{P\in\mathcal{I}(X)} \ker\, P'(x)$.

Proposition 1.69. *View the linear forms*

$$P'(x)\colon h \mapsto P'(x) \cdot h$$

as homogeneous polynomials of degree 1 *in the coordinates of* $h \in k^n$ *and denote by*

$$\mathcal{I}(X)_x \coloneqq (P'(x) : P \in \mathcal{I}(X))$$

the ideal generated by these polynomials. Then

$$T_x X = x + \mathcal{V}_{k^n}(\mathcal{I}(X)_x).$$

Proof. It suffices to check that

$$\mathcal{V}_{k^n}(\mathcal{I}(X)_x) = \bigcap_{P \in \mathcal{I}(X)} \ker\, P'(x)$$

which is obvious because the $(P'(x))_{P\in\mathcal{I}(X)}$ generate $\mathcal{I}(X)_x$. □

Corollary 1.70. $T_x X \supseteq \mathcal{C}_x(X)$

Proof. Since $\mathcal{I}(X)_x \subseteq \mathcal{I}(X)^*_x$, one has $\mathcal{V}_{k^n}(\mathcal{I}(X)_x) \supseteq \mathcal{V}_{k^n}(\mathcal{I}(X)^*_x)$. □

Definition 1.71. If $T_x X = \mathcal{C}_x(X)$, the point x is called *non-singular*.

Proposition 1.72. *If* $\mathcal{I}(X) = (P_1,\ldots,P_m)$, *then* $\mathcal{I}(X)_x = (P_1'(x),\ldots,P_m'(x))$

Proof. By definition,

$$(P_1'(x),\ldots,P_m'(x)) \subseteq (P'(x) : P \in \mathcal{I}(X)) = \mathcal{I}(X)_x.$$

But for $P \in \mathcal{I}(X)$, there exist $Q_1,\ldots,Q_m \in k[T_1,\ldots,T_n]$ such that $P = \sum_{i=1}^m Q_i P_i$, so

$$\begin{aligned} P'(x) &= \sum_{i=1}^{m} (Q_i P_i)'(x) \\ &= \sum_{i=1}^{m} (Q_i'(x) \underbrace{P_i(x)}_{=0} + \overbrace{Q_i(x)}^{\in k} P_i'(x)) \end{aligned}$$

since $x \in X$. This proves that $P'(x)$ is in fact a linear combination of the linear forms $(P_i'(x))_{1\leq i\leq m}$. □

Corollary 1.73. *If $\mathcal{I}(X) = (P_1, \ldots, P_m)$, then $T_x X = x + \bigcap_{i=1}^m \ker P_i'(x)$. Moreover, if we write $P = (P_1, \ldots, P_m)$, and view this P as a polynomial map $k^n \to k^m$, then*

$$T_x X = x + ker\ P'(x)$$

with $P'(x)$ the Jacobian of P at x, i.e.

$$P'(x) = \begin{pmatrix} \frac{\partial P_1}{\partial T_1}(x) & \cdots & \frac{\partial P_1}{\partial T_n}(x) \\ \vdots & & \vdots \\ \frac{\partial P_m}{\partial T_1}(x) & \cdots & \frac{\partial P_m}{\partial T_n}(x) \end{pmatrix}.$$

In particular, dim $T_x X = n - \operatorname{rk} P'(x)$.

Example 1.74. (i) $X = \{y^2 - x^3 = 0\} \subseteq k^2$. Then $\mathcal{I}(X) = (y^2 - x^3)$, so,

$$T_{(0,0)} X = (0,0) + \ker \begin{pmatrix} 0 & 0 \end{pmatrix} = k^2.$$

which strictly contains the tangent cone $\{y^2 = 0\}$. In particular, the origin is indeed a singular point of the cuspidal cubic. In general,

$$T_{(x,y)} X = (x,y) + \ker \begin{pmatrix} -3x^2 & 2y \end{pmatrix},$$

which is an affine line if $(x,y) \neq (0,0)$.

(ii) $X = \{y^2 - x^2 - x^3 = 0\} \subseteq k^2$. Then $\mathcal{I}(X) = (y^2 - x^2 - x^3)$, so

$$T_{(0,0)} X = (0,0) + \ker \begin{pmatrix} 0 & 0 \end{pmatrix} = k^2$$

which again strictly contains the tangent cone $\{y = \pm x\}$. In general,

$$T_{(x,y)} X = (x,y) + \ker \begin{pmatrix} -2x & 2y \end{pmatrix},$$

which is an affine line if $(x,y) \neq (0,0)$.

Remark 1.75. The dimension of the Zariski tangent space at x (as an affine subspace of k^n) may vary with x.

Chapter 2

Algebraic varieties

2.1 Spaces with functions

Definition 2.1. Let k be a field. A *space with functions over k* is a pair $(X, \mathcal{O}_x)$ where X is a topological space and $\mathcal{O}_X$ is a subsheaf of the sheaf of k-valued functions, seen as a sheef of k-algebras, and satisfying the following condition:

If $U \subseteq X$ is an open set and $f \in \mathcal{O}_X(U)$, then the set

$$D_U(f) \coloneqq \{x \in U \mid f(x) \neq 0\}$$

is open in U and the function $\frac{1}{f} \colon D_U(f) \to k$, $x \mapsto \frac{1}{f(x)}$ belongs to $\mathcal{O}_X(D_U(f))$.

Remark 2.2. Concretely, it means that there is for each open set $U \subseteq X$ a k-Algebra $\mathcal{O}_X(U)$ of „regular“ functions such that

(i) the restriction of a regular function $f \colon U \to k$ to a sub-open $U' \subseteq U$ is regular on U'.

(ii) if $f \colon U \to k$ is a function and $(U_\alpha)_{\alpha \in A}$ is an open cover of U such that $f|_{U_\alpha}$ is regular on U_α, then f is regular on U.

(iii) if f is regular on U, the set $\{f \neq 0\}$ is open in U and $\frac{1}{f}$ is regular wherever it is defined.

Remark 2.3. If $\{0\}$ is closed in k and $f \colon U \to k$ is continuous, then $D_U(f)$ is open in U. So, this conditions is often automatically met in practice.

Example 2.4. (i) $(X, \mathcal{C}_X)$ a topological space endowed with its sheaf of $\mathbb{R}$-valued (or $\mathbb{C}$-valued) continuous functions, the fields $\mathbb{R}$ and $\mathbb{C}$ being endowed here with their classical topology.

(ii) $(V, \mathcal{O}_V)$ where $V = \mathcal{V}(P_1, \ldots, P_m)$ is an algebraic subset of k^n (endowed with the Zariski topology) and, for all $U \subseteq V$ open,

$$\mathcal{O}_V(U) \coloneqq \left\{ f \colon U \to k \;\middle|\; \begin{array}{l} \forall x \in U \exists x \in U_x \text{ open}, P, Q \in k[x_1, \ldots, x_n] \text{ such that} \\ \text{for } z \in U \cap U_x, Q(z) \neq 0 \text{ and } f(z) = \frac{P(z)}{Q(z)} \end{array} \right\}.$$

(iii) $(M, \mathcal{C}^\infty_M)$ where $M = \varphi^{-1}(0)$ is a non-singular level set of a $\mathcal{C}^\infty$ map $\varphi \colon \Omega \to \mathbb{R}^m$ where $\Omega \subseteq \mathbb{R}^{p+m}$ is an open set (in the usual topology of $\mathbb{R}^{p+m}$) and, for all $U \subseteq M$ open, $\mathcal{C}^\infty_M(U)$ locally smooth maps.

Exercise 2.5. Let $(X, \mathcal{O}_X)$ be a space with functions and let $U \subseteq X$ be an open subset. Define, for all $U' \subseteq U$ open,

$$\mathcal{O}_X|_U(U') \coloneqq \mathcal{O}_X(U').$$

Then $(U, \mathcal{O}_X|_U)$ is a space with functions.

Example 2.6. (i) $(V, \mathcal{O}_V)$ an algebraic subset of k^n, $f\colon V \to k$ a polynomial function, $U \coloneqq D_V(f)$ is open in V and the sheaf of regular functions that we defined on the locally closed subset $D_V(f) = D_{k^n}(f) \cap V$ coincides with the restriction to $D_V(f)$ of the sheaf of regular functions on V.

(ii) $B \subseteq \mathbb{R}^n$ or $\mathbb{C}^n$ an open ball (with respect to the usual topology), equipped with the sheaf of $\mathcal{C}^\infty$ or holomorphic functions.

2.2 Morphisms

Remark 2.7. Note that if $f\colon X \to Y$ is a map and $h\colon U \to k$ is a function defined on a subset $U \subseteq Y$, there is a pullback map f_U^* taking $h\colon U \to k$ to the function $f_U^* \coloneqq h \circ f\colon f^{-1}(U) \to k$. This map is a homomorphism of k-algebras. Moreover given a map $g\colon Y \to Z$ and a subset $V \subseteq Z$ such that $g^{-1}(V) \subseteq U$, we have, for all $h\colon V \to k$,

$$f_U^*(g_V^*(h)) = f_U^*(h \circ g) = (h \circ g) \circ f = h \circ (g \circ f) = (g \circ f)_V^*(h).$$

Definition 2.8. Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be two spaces with functions over a field k. A *morphism of spaces with functions* between $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ is a continuous map $f\colon X \to Y$ such that, for all open set $U \subseteq Y$, the pullback map f_U^* takes a regular function on the open set $U \subseteq Y$ to a regular function on the open set $f^{-1}(U) \subseteq X$.

Remark 2.9. Then, given open sets $U' \subseteq U$ in Y, we have compatible homomorphisms of k-algebras:

In other words, we have a morphism of sheaves on Y $f^*\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$, where by definition $(f_*\mathcal{O}_X)(U) = \mathcal{O}_X(f^{-1}(U))$.

Exercise 2.10. Given $g\colon Y \to Z$, show that $(g \circ f)_*\mathcal{O}_X = g_*(f_*\mathcal{O}_X)$ and that g_* is a functor from sheaves on Y to sheaves on Z.

Remark 2.11. If $f\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ and $g\colon (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ are morphisms, so is the composed map $g \circ f\colon X \to Z$.

Proposition 2.12. *Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be locally closed subsets of an affine space ($X \subseteq k^n, Y \subseteq K^m$) equipped with their respective sheaves of regular functions. Then a map $f\colon X \to Y$ is a morphism of spaces with functions if and only if $f = (f_1, \ldots, f_m)$ with each $f_i\colon X \to k$ a regular function on X.*

Proof. The proof that if each of the f_i's is a regular function, then f is a morphism is similar to point (i) of the previous example: it holds because the pullback of a regular function (in particular, the pullback of a polynomial) by a regular function is a regular function, and because an equation of the form $h(x) = 0$ for h a regular function is locally equivalent to a polynomial equation $P(x) = 0$.

Conversely, if $f\colon X \to Y \subseteq k^m$ is a morphism, then the pullback of the i-th projection $p_i\colon k^m \to k$ is a regular function on X. Since $f^*p_i = f_i$, the proposition is proved. □

Remark 2.13. In the proof of the previous proposition, we used that if the $(f_i\colon X \to k)_{1 \leq i \leq m}$ are regular functions on the locally closed subset $X \subseteq k^n$, then the map

$$\begin{aligned} f\colon X &\to k^m \\ x &\mapsto (f_1(x), \ldots, f_m(x)) \end{aligned}$$

is continuous on X. This is because the pre-image of $f^{-1}(V)$ of an algebraic subset $V = V(P_1, \ldots, P_r) \subseteq k^m$ is the intersection of X with the zero set

$$W = V(P_1 \circ f, \ldots, P_r \circ f) \subseteq k^n$$

which is indeed an algebraic set, because $P_j \circ f$ is a regular function so the equation $P_j \circ f = 0$ is equivalent to a polynomial equation.

Beware, however, that if the $(f_i)_{1 \leq i \leq m}$ are only continuous maps, then W is no longer an algebraic set, so we would need another argument in order to prove the continuity of f. Typically, in general topology, we say that $f\colon X \to k^m$ is continuous because its components $(f_1, \ldots, f_m)$ are continuous. This argument is valid when the topology used on k^m is the product topology of the topologies on k. However, this does not hold in general for the Zariski topology, which is strictly larger than the product topology when k is infinite.

Example 2.14. (i) The projection map

$$\begin{aligned} \mathcal{V}_{k^2}(y - x^2) &\to k \\ (x, y) &\mapsto x \end{aligned}$$

is a morphism of spaces with functions, because it is a regular function on $\mathcal{V}_{k^2}(y - x^2)$. It is actually an isomorphism, whose inverse is the morphism

$$\begin{aligned} k &\to \mathcal{V}(y - x^2) \\ x &\mapsto (x, x^2). \end{aligned}$$

Note that $\mathcal{V}_{k^2}(y - x^2)$ is the graph of the polynomial function $x \mapsto x^2$.

(ii) Let k be an infinite field. The map

$$\begin{aligned} k &\to \mathcal{V}_{k^2}(y^2 - x^3) \\ t &\mapsto (t^2, t^3) \end{aligned}$$

is a morphism and a bijection, but it is not an isomorphism, because its inverse

$$\begin{aligned} \mathcal{V}_{k^2}(y^2 - x^3) &\to k \\ (x, y) &\mapsto \begin{cases} \frac{y}{x} & (x, y) \neq (0, 0) \\ 0 & (x, y) = (0, 0) \end{cases} \end{aligned}$$

is not a regular map (this is where we use that k is infinite).

(iii) Consider the groups $G = \mathrm{GL}(n; k)$, $\mathrm{SL}(n; k)$, $\mathrm{O}(n; k)$, $\mathrm{SO}(n; k)$ etc. as locally closed subsets in k^{n^2} and equip them with their sheaves of regular functions. Then the multiplication $\mu\colon GxG \to G, (g_1, g_2) \mapsto g_1 g_2$ and and inversion $\iota\colon G \to G, g \mapsto g^{-1}$ are morphisms (here $G \times G$ is viewed as a locally closed subset of $k^{n^2} \times k^{n^2} \simeq k^{2n^2}$, equipped with its Zariski topology), since they are given by regular functions in the coefficients of the matrices.

Such groups will later be called *affine algebraic groups*.

2.3 Abstract affine varieties

Recall that an isomorphism of spaces with functions is a morphism $f\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ that admits an inverse morphism.

Remark 2.15. As we have seen, a bijective morphism is not necessarily an isomorphism.

Remark 2.16. Somewhat more formally, one could also define a morphism of spaces with functions (over k) to be a pair (f, φ) such that $f\colon X \to Y$ is a continuous map and $\varphi\colon \mathcal{O}_Y \to f_* \mathcal{O}_X$ is the morphism of sheaves f^*. The question then arises how to define properly the composition $(g, \psi) \circ (f, \varphi)$. The formal answer is $(g \circ f, f_*(\varphi) \circ \psi)$.

Definition 2.17. Let k be a field. An (abstract) *affine variety over* k (also called an affine k-variety) is a space with functions $(X, \mathcal{O}_X)$ over k that is isomorphic to the space with functions $(V, \mathcal{O}_V)$, where V is an algebraic subset of some affine space k^n and $\mathcal{O}_V$ is the sheaf of regular functions on V.

A morphism of affine k-varieties is a morphism of the underlying spaces with functions.

Example 2.18. (i) An algebraic subset $V \subseteq k^n$, endowed with its sheaf of regular functions $\mathcal{O}_V$, is an affine variety.

(ii) It is perhaps not obvious at first, but a standard open set $D_V(f)$, where $f\colon V \to k$ is a regular function on an algebraic set $V \subseteq k^n$, defines an affine variety. Indeed, when equipped with its sheaf of regular functions, $D_V(f) \simeq \mathcal{V}_{k^{n+1}}(tf(x) - 1)$.

Remark 2.19. Let $(X, \mathcal{O}_X)$ be a space with functions. An open subset $U \subseteq X$ defines a space with functions $(U, \mathcal{O}_U)$. If $(U, \mathcal{O}_U)$ is isomorphic to some standard open set $D_V(f)$ of an algebraic set $V \subseteq k^n$, we will call U an *affine open set*.

Then the observation is the following: since an algebraic set $V \subseteq k^n$ is a finite union of standard open sets, every point x in an affine variety X has an affine open neighbourhood.

Less formally, an affine variety X, locally „looks like“ a standard open set $D_V(f) \subseteq k^n$, where $V \subseteq k^n$ is an algebraic set. In particular, open subsets of an affine variety also locally look like standard open sets. In fact, they are finite unions of such sets.

Example 2.20. The algebraic group $\mathrm{GL}(n; k)$ is an affine variety over k.

Remark 2.21. An algebraic set $(V, \mathcal{O}_V)$ is a subset $V \subseteq k^n$ defined by polynomial equations and equipped with its sheaf of regular functions. An affine variety $(X, \mathcal{O}_X)$ is „like an algebraic set“ but without a reference to a particular „embedding“ in affine space. This is similar to having a finitely generated k-Algebra A without specifying a particular isomorphism

$$A \simeq k[X_1, \ldots, X_n]/I.$$

The next example will illustrate precisely this fact.

Example 2.22. Let us now give an abstract example of an affine variety. We consider a finitely generated k-algebra A and define $X \coloneqq \mathrm{Hom}_{k-\mathrm{Alg}}(A, k)$. The idea is to think of X as points on which we can evaluate elements of A, which are thought of as functions on X. For $x \in \mathrm{Hom}_k(A, k)$ and $f \in A$ we set $f(x) \coloneqq x(f) \in k$.

- Topology on X: for all ideal $I \subseteq A$, set

  $$\mathcal{V}_X(I) \coloneqq \{x \in X \mid \forall x \in I\colon f(x) = 0\}.$$

  These subsets of X are the closed sets of a topology on X, which we may call the Zariski topology.

- Regular functions on X: if $U \subseteq X$ is open, a function $h\colon U \to k$ is called regular at $x \in U$ if there it exists an open set $x \in U_x$ and elements $P, Q \in A$ such that for $y \in U_x$, $Q(y) \neq 0$ and $h(y) = \frac{P(y)}{Q(y)}$ in k.

  The function h is called regular on U iff it is regular at $x \in U$. Regular functions then form a sheaf of k-algebras on X.

  Moreover, if $h\colon U \to k$ is regular on X, the set $D_X(h) \coloneqq \{x \in X \mid h(x) \neq 0\}$ is open in X and the function $\frac{1}{h}$ is regular on $D_X(h)$.

So, we have defined a space with functions $(X, \mathcal{O}_X)$, at least whenever $X \neq \emptyset$. We show that X is an affine variety.

Proof. Fix a system of generators of A, i.e.

$$A \simeq k[t_1, \dots, t_n]/I$$

where $k[t_1, \dots, t_n]$ is a polynomial algebra. We denote by $\overline{t_1}, \dots, \overline{t_n}$ the images of $t_1, \dots, t_n$ in A and we define

$$\begin{aligned} \varphi\colon X = \mathrm{Hom}_k(A, k) &\to k^n \\ x &\mapsto (x(\overline{t_1}), \dots, x(\overline{t_n})). \end{aligned}$$

Let $P \in I$ and $x \in X$. Then

$$P(\varphi(x)) = P(x(\overline{t_1}), \dots, x(\overline{t_n})) = x(\overline{P}) = 0.$$

Thus $\varphi(x) \in \mathcal{V}_{k^n}(I)$. Conversely let $a = (a_1, \dots, a_n) \in \mathcal{V}_{k^n}(I)$, then we can define a morphism of k-algebras

$$x_a\colon A \to A/(\overline{t_1} - a_1, \dots, \overline{t_n} - a_n) \simeq k$$

which satisfies $x_a(\overline{t_i}) = a_i$ for all i. So $(a_1, \dots, a_n) = \varphi(x_a) \in \mathrm{im}\ \varphi$.

In particular, we have defined a map

$$\begin{aligned} \psi\colon \mathcal{V}_{k^n}(I) &\to X = \mathrm{Hom}_k(A, k) \\ a &\mapsto x_a \end{aligned}$$

such that $\varphi \circ \psi = \mathrm{Id}_{\mathcal{V}_{k^n}(I)}$. In fact, we also have $\psi \circ \varphi = \mathrm{Id}_X$.

It remains to check that φ and ψ are morphisms of spaces with functions, which follows from the definition of the topology and the notion of regular function on X. □

The elements of $X \coloneqq \mathrm{Hom}_k(A, k)$ are also called the *characters* of the k-algebra A, and this is sometimes denoted by $\hat{A} \coloneqq \mathrm{Hom}_{k-\mathrm{alg}}(A, k)$. Note that $\hat{A}$ is a k-subalgebra of the algebra of all functions $f\colon A \to k$.

The character x_a introduced above and associated to an alemenet $a \in A$ is then denoted by $\hat{a}$ and called the *Gelfand transform* of a. The *Gelfand transformation* is the morphism of k-algebras

$$\begin{aligned} A &\to \hat{A} \\ a &\mapsto \hat{a}. \end{aligned}$$

Exercise 2.23. Let A be a finitely generated k-algebra and let $X = \mathrm{Hom}_{k\text{-alg}}(A, k)$. Show that the map $x \mapsto \ker x$ induces a bijection

$$X \simeq \{\mathfrak{m} \in \mathrm{Spm}\, A \mid A/\mathfrak{m} \simeq k\}.$$

Remark 2.24. Note that we have not assumed A to be reduced and that, if we set $A_{\mathrm{red}} \coloneqq A/\sqrt{(0)}$, then A_{red} is reduced and $\hat{A_{\mathrm{red}}} = \hat{A}$, because a maximal ideal of A necessarily contains $\sqrt{(0)}$ and the quotient field is „the same“.

Remark 2.25. Let $(X, \mathcal{O}_X)$ be an affine variety. One can associate the k-algebra $\mathcal{O}_X(X)$ of globally defined regular functions on X:

$$\mathcal{O}_X(X) = \{f\colon X \to k \mid f \text{ regular on } X\}.$$

Moreover, if $\varphi\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a morphism between two affine varieties, we have a k-algebra homomorphism

$$\begin{aligned} \varphi^*\colon \mathcal{O}_Y(Y) &\to \mathcal{O}_X(X) \\ f &\mapsto f \circ \varphi. \end{aligned}$$

Also, $(\mathrm{id}_X)^* = \mathrm{id}_{\mathcal{O}_X(X)}$ and $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$ whenever $\psi\colon (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ is a morphism of affine varieties. In other words, we have defined a (contravariant) functor k-Aff $\to$ k-Alg.

Proposition 2.26. *Let k be a field. The functor*

$$k\text{-}\mathit{Aff} \to k\text{-}\mathit{Alg}$$
$$(X, \mathcal{O}_X) \mapsto \mathcal{O}_X(X)$$

is fully faithful.

Proof. Since X and Y are affine, we may assume $X = V \subseteq k^n$ and $Y = W \subseteq k^m$. Then $\varphi\colon V \to W$ is given by m regular functions $(\varphi_1, \ldots, \varphi_m)$ on V. On k^m, let us denote by y_i the projection to the i-th factor. Its restriction to W is a regular function

$$y_i|_W\colon W \to k$$

that satisfies $\varphi^*(y_i|_W) = \varphi_i$.

Since for all regular functions $f\colon W \to k$ one has

$$\varphi^* f = f \circ \varphi = f(\varphi_1, \ldots, \varphi_m),$$

we see that the morphism

$$\varphi^*\colon \mathcal{O}_W(W) \to \mathcal{O}_V(V)$$

is entirely determined by the m regular functions $\varphi^*(y_i|_W) = \varphi_i$ on V. In particular, if $\varphi^* = \psi^*$, then $\varphi_i = \varphi^*(y_i|_W) = \psi^*(y_i|_W) = \psi_i$, so $\varphi = \psi$, which proves that $\varphi \mapsto \varphi^*$ is injective.

Surjectivity: Let $h\colon \mathcal{O}_W(W) \to \mathcal{O}_V(V)$ be a morphism of k-algebras. Let

$$\varphi \coloneqq (h(y_1|_W), \ldots, h(y_m|_W))$$

which is a morphism from V to k^m, because its components are regular functions on V. It satisfies $\varphi^*(y_i|_W) = \varphi_i = h(y_i|_W)$, so $\varphi^* = h$.

It remains to show, that $\varphi(V) \subseteq W$. Let $W = \mathcal{V}(P_1, \ldots, P_r)$ with $P_j \in k[Y_1, \ldots, Y_m]$. Then for all $j \in \{1, \ldots, r\}$ and $x \in V$

$$P_j(\varphi(x)) = P_j(h(y_1|_W), \ldots, h(y_m|_W))(x).$$

Since h is a morphism of k-algebras and P_j is a polynomial, we have

$$P_j(h(y_1|_W), \ldots, h(y_m|_W)) = h(P_j(y_1|_W), \ldots, P_j(y_m|_W)).$$

But $P_j \in \mathcal{I}(W)$, so

$$P_j(y_1|_W, \ldots, y_m|_W) = P_j(y_1, \ldots, y_m)|_W = 0,$$

which proves that for $x \in V$, $\varphi(x) \in W$. □

2.4 Geometric Noether normalisation

Consider a plane algebraic curve $\mathcal{C}$, defined by the equation $f(x, y) = 0$. If we fix $x = a$, then the polynomial equation $f(a, y) = 0$ has only finitely many solutions (at most $\deg_y f$). This means that the map

$$\mathcal{C} \coloneqq \mathcal{V}(f) \to k(x, y) \mapsto x$$

has finite fibres. A priori, such a map is not surjective, e.g. for $f(x, y) = xy - 1$. If k is algebraically closed, one can always find such a surjective projection.

Theorem 2.27. *Let k be an algebraically closed field and $f \in k[x_1, \ldots, x_n]$ be a polynomial of degree $d \geq 1$. Then there is a morphism of affine varieties*

$$\pi\colon \mathcal{V}_{k^n}(f) \to k^{n-1}$$

such that:

(i) π *is surjective*

(ii) for $t \in k^{n-1}$*, the fibre* $\pi^{-1}(\{t\}) \subseteq \mathcal{V}(f)$ *consists of at most* d *points.*

Proof. Let $f \in k[x_1, \ldots, x_n]$ be of degree d. We construct a change of variables of the form $(x_i \mapsto x_i + a_i x_n)_{1 \leq i \leq n-1}$ and $x_n \mapsto x_n$, such that the term of degree d of $f(x_1 + a_1 x_n, \ldots, x_{n-1} + a_{n-1} x_n, x_n)$ becomes $c x_n^d$ with $c \in k^\times$. Since

$$f(x_1 + a_1 x_n, \ldots, x_{n-1} + a_{n-1} x_n, x_n) = \sum_{(i_1, \ldots, i_n) \in \mathbb{N}^n} \alpha_{i_1, \ldots, i_n} (x_1 + a_1 x_n)^{i_1} \cdots (x_{n-1} + a_{n-1} x_n)^{i_{n-1}} x_n^{i_n},$$

the coefficient of x_n^d in the above equation is obtained by considering all $(i_1, \ldots, i_n)$ such that $i_1 + \ldots + i_n = d$, and keeping only the term in $x_n^{i_j}$ when expanding $(x_j + a_j x_n)^{i_j}$, so we get

$$\sum_{(i_1, \ldots, i_n) \in \mathbb{N} i_1 + \ldots + i_n = d} \alpha_{i_1, \ldots, i_n} a_1^{i_1} \cdots a_{n-1}^{i_{n-1}},$$

which is equal to $f_d(a_1, \ldots, a_{n-1}, 1)$, where f_d is the (homogeneous) degree d part of f.

Claim: There exist $a_1, \ldots, a_{n-1} \in k$ such that $f_d(a_1, \ldots, a_{n-1}, 1) \neq 0$. Proof of claim by induction: if $n = 1$, $f_d = c x_1^d$ for some $c \neq 0$, so $f_d(1) = c \neq 0$. If $n \geq 2$, we can write

$$f_d(x_1, \ldots, x_n) = \sum_{i=0}^{d} h_i(x_2, \ldots, x_n) x_1^i$$

where $h_i \in k[x_2, \ldots, x_n]$ is homogeneous of degree $d - i$. Since $f_d \neq 0$, there is at least one i_0 such that $h_{i_0} \neq 0$. By induction, we can find $(a_2, \ldots, a_{n-1}) \in k^{n-2}$ such that $h_{i_0}(a_2, \ldots, a_{n-1}, 1) \neq 0$. But then $f(\cdot, a_2, \ldots, a_{n-1}, 1) \in k[x_1]$ is a non zero polynomial, so it has only finitely many roots. As k is infinite, there exists $a_1 \in k$, such that $f(a_1, \ldots, a_{n-1}, 1) \neq 0$.

Then

$$\varphi \colon \begin{cases} x_i \mapsto x_i + a_i x_n & 1 \leq i \leq n-1 \\ x_n \mapsto x_n \end{cases}$$

is a invertible linear transformation $k^n \to k^n$, such that

$$(f \circ \varphi^{-1})(y_1, \ldots, y_n) = c(y_n^d + g_1(y_1, \ldots, y_n) y_n^{d-1} + \ldots + g_d(y_1, \ldots, y_{n-1})$$

for $c \neq 0$. This induces an isomorphism of affine varieties

$$\begin{aligned} \mathcal{V}(f) &\to \mathcal{V}(f \circ \varphi^{-1}) \\ x &\mapsto \varphi(x) \end{aligned}$$

such that

$$\begin{array}{ccc} \mathcal{V}(f) & \xhookrightarrow{\varphi} & k^n = k^{n-1} \times k \\ & \searrow^{\pi} & \downarrow \\ & & k^{n-1} \end{array}$$

defines the morphism π with the desired properties. Indeed: Let $(x_1, \ldots, x_n) \in k^n$ and set $y_i \coloneqq \varphi(x_i)$. Then

$(x_1, \ldots, x_n) \in \mathcal{V}(f)$ iff $x_n = y_n$ is a root of the polynomial

$$t^d + \sum_{j=1}^{d} g_j(y_1, \ldots, y_{n-1}) t^{d-j}.$$

Therefore for all $t = (y_1, \ldots, y_{n-1}) \in k^{n-1}$, $\pi^{-1}(\{t\}) \neq \emptyset$ (because $\overline{k} = k$) and $\pi^{-1}(\{t\})$ has at most d points. $\square$

Definition 2.28. Let $f \in k[x_1, \dots, x_n]$ be a polynomial of degree d. As in the proof of 2.27, ther exists a linear coordinate transformation $\varphi\colon k^n \to k^n$, such that $f \circ \varphi^{-1}(y_1, \dots, y_n) = cy_n^d + \sum_{j=1}^{d} g_j(y_1, \dots, y_{n-1}) y_n^{d-j}$. For a point $x \in \pi^{-1}(y_1, \dots, y_{n-1}) \subseteq \mathcal{V}(f)$, the *multiplicity* of x is the multiplicity of y_n as a root of that polynomial.

A point with multiplicity ≥ 2 are called *ramification point* and its image lies in the *discriminant locus* of π.

With this vocabulary, we can refine the statement of 2.27.

Definition 2.29 (Geometric Noether normalisation)**.** Assume $k = \overline{k}$. If $f \in k[x_1, \dots, x_n]$ is polynomial of degree d, a morphism of affine varieties

$$\pi\colon \mathcal{V}_{k^n}(f) \to k^{n-1}$$

such that

(i) π is surjective

(ii) for $t \in k^{n-1}$, the number of elements in $\pi^{-1}(\{t\})$, counted with their respective multiplicities, is exactly d,

is called a *geometric Noether normalisation.*

Corollary 2.30 (Geometric Noether normalisation for hypersurfaces)**.** *Let k be an algebraically closed field and $f \in k[x_1, \dots, x_n]$ be a polynomial of degree $d \geq 1$. Then there exists a geometric Noether normalisation.*

Example 2.31. Let $f(x, y) = y^2 - x^3 \in \mathbb{C}[x, y]$. Then the map

$$\mathcal{V}_{\mathbb{C}^2}(y^2 - x^3) \to \mathbb{C}(x, y) \qquad\qquad \mapsto y$$

is a geometric Noether normalisation, but $(x, y) \mapsto x$ is not (the fibres of the latter have degree 2, while $\deg f = 3$).

Remark 2.32. In the proof of 2.27, to construct φ and the g_j, we only used that k is infinte. Thus the statement, that for all $f \in k[x_1, \dots, x_n]$ there exists a linear automorphism $\varphi\colon k^n \to k^n$ such that

$$f \circ \varphi^{-1}(y_1, \dots, y_n) = c \left(y_n^d + \sum_{j=1}^{d} g_j(y_1, \dots, y_{n-1}) y_n^{d-j} \right)$$

is valid over k if k is infinite. The resulting map

$$\pi\colon \mathcal{V}_{k^n}(f) \to k^{n-1}$$

still has finite fibres, but it is no longer surjective in general, as the example $f(x, y) = x^2 + y^2 - 1$ shows.

However, it induces a surjective map with finite fibres

$$\hat{\pi}\colon \mathcal{V}_{\overline{k}^n}(f) \to \overline{k}^{n-1}$$

which moreover commutes with the action of $\mathrm{Gal}(\overline{k}/k)$.

Theorem 2.33. *Let k be an infinite field and $\overline{k}$ an algebraic closure of k. Let $f \in k[x_1, \dots, x_n]$ be a polynomial of degree $d \geq 1$. Then there exists a $Gal(\overline{k}/k)$-equivariant geometric Noether normalisation map $\pi\colon \mathcal{V}_{\overline{k}^n}(f) \to \overline{k}^{n-1}$.*

Example 2.34. Let $f(x,y) = y^2 - x^3 \in \mathbb{R}[x,y]$. Then the map

$$\begin{aligned} \pi\colon \mathcal{V}_{\mathbb{C}^2}(y^2 - x^3) &\to \mathbb{C} \\ (x,y) &\mapsto y. \end{aligned}$$

is a geometric Noether normalisation map and it is Galois-invariant:

$$\pi(\overline{(x,y)}) = \pi(\overline{x},\overline{y}) = \overline{y} = \overline{\pi(x,y)}.$$

Exercise 2.35. Show that if $y \in \mathbb{R}$, the group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on $\pi^{-1}(\{y\})$, and that the fixed point set of that action is in bijection with $\{x \in \mathbb{R} \mid y^2 - x^3 = 0\}$.

Next, we want to generalise the results above beyond the case of hypersurfaces.

Theorem 2.36. *Assume k is algebraically closed. Let $V \subseteq k^n$ be an algebraic set. Then there exists a natural number $r \leq n$ and a morphism of algebraic sets*

$$p\colon V \to k^r$$

such that p is surjective and has finite fibres.

Sketch of proof. If $V = k^n$, we take $r = n$ and $p = \mathrm{id}_{k^n}$. Otherwise $V = \mathcal{V}(I)$ with $I \subseteq k[x_1,\ldots,x_n]$ a non-zero ideal. Take $f \in I \setminus \{0\}$. Then there exists a geometric Noether normalisation

$$p_1\colon \mathcal{V}(f) \to k^{n-1}.$$

One can now show that $V_1 \coloneqq p_1(V)$ is an algebraic set in k^{n-1}. Thus there are two cases:

(1) $p_1(V) = k^{n-1}$. Thus $p_1|_V\colon V \to k^{n-1}$ is surjective with finite fibres and we are done.

(2) $p_1(V) \subsetneq k^{n-1}$. In this case $p_1(V) = \mathcal{V}(I_1)$ with $I_1 \subseteq k[x_1,\ldots,x_{n-1}]$ a non-zero ideal. So we can repeat the argument.

After $r \leq n$ steps, the above algorithm terminates, and this happens precisely when $V_r = k^{n-r}$. If we set

$$p \coloneqq p_r \circ \ldots \circ p_1\colon V \to k^{n-r}$$

then p is surjective with finite fibres because $p(V) = V_r = k^{n-r}$ and each p_i has finite fibres. □

Remark 2.37. By the fact used in the proof of 2.36, p is in fact a closed map. Note that when $r = n$, $V = p^{-1}(\{0\})$ is actually finite, in which case $\dim V$ should indeed be 0.

2.5 Gluing spaces with functions

We present a general technique to construct spaces with functions by „patching together“ other spaces with functions „along open subsets“. This will later be used to argue that, in order to define a structure of variety on a topological sapce (or even a set), it suffices to give one atlas.

Theorem 2.38 (Gluing theorem)**.** *Let $(X_i, \mathcal{O}_{X_i})_{i\in I}$ be a family of spaces with functions. For all pair (i,j), assume that the following has been given*

(a) an open subset $X_{ij} \subseteq X_i$

(b) an isomorphism of spaces with functions

$$\varphi_{ji}\colon (X_{ij}, \mathcal{O}_{X_{ij}}) \to (X_{ji}, \mathcal{O}_{X_{ji}})$$

subject to the following compatibility conditions

(1) for all i, $X_{ii} = X_i$ and $\varphi_{ii} = id_{X_i}$

(2) for all pair (i,j), $\varphi_{ij} = \varphi_{ji}^{-1}$

(3) for all triple (i,j,k), $\varphi_{ji}(X_{ik} \cap X_{ij}) = X_{jk} \cap X_{ji}$ and $\varphi_{kj} \circ \varphi_{ji} = \varphi_{ki}$ on $X_{ik} \cap X_{ij}$.

Then there exists a space with functions $(X, \mathcal{O}_X)$ equipped with a family of open sets $(U_i)_{i\in I}$ and isomorphisms of spaces with functions

(A1) $\varphi_i \colon (U_i, \mathcal{O}_X|_{U_i}) \to (X_i, \mathcal{O}_{X_i})$,

such that $\bigcup_{i\in I} U_i = X$ and, for all pair (i,j),

(B2) $\varphi_i(U_i \cap U_j) = X_{ij}$, and

(C3) $\varphi_j \circ \varphi_i^{-1} = \varphi_{ji}$ on X_{ij}.

Such a familiy $(U_i, \varphi_i)_{i\in I}$ is called an atlas for $(X, \mathcal{O}_X)$.

Moreover, if $(Y, \mathcal{O}_Y)$ is a space with functions equipped with an atlas $(V_i, \psi_i)_{i\in I}$ satisfying conditions (A1), (A2) and (A3), then the isomorphisms $\psi_i^{-1} \circ \varphi_i \colon U_i \to V_i$ induce an isomorphism $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$.

Proof. Uniqueness up to canonical isomorphism: Let $(U_i, \varphi_i)_{i\in I}$ and $(V_i, \psi_i)_{i\in I}$ be two atlases modelled on the same gluing data, then for all pair (i,j),

$$\begin{aligned}
\psi_j^{-1} \circ \varphi_j\Big|_{U_i\cap U_j} &= \psi_j^{-1} \circ \underbrace{(\varphi_j \circ \varphi_i^{-1})}_{=\varphi_{ji}} \circ \varphi_i\Big|_{U_i\cap U_j} \\
&= \psi_j^{-1} \circ \underbrace{(\psi_j \circ \psi_i^{-1})}_{=\varphi_{ji}} \circ \varphi_i\Big|_{U_i\cap U_j} \\
&= \psi_i^{-1} \circ \varphi_i\Big|_{U_i\cap U_j}
\end{aligned}$$

so there is a well-defined map

$$\begin{aligned}
f \colon X = \bigcup_{i\in I} U_i &\to \bigcup_{i\in I} V_i = Y \\
(x \in U_i) &\mapsto (\psi_i^{-1} \circ \varphi_i(x) \in V_i)
\end{aligned}$$

which induces an isomorphism of spaces with functions.

Existence: Define $\tilde{X} \coloneqq \bigsqcup_{i\in I} X_i$ and let the topology be the final topology with respect to the canonical maps $(X_i \to \tilde{X})_{i\in I}$. Then define $X \coloneqq \tilde{X}/\sim$ where $(i,x) \sim (j,y)$ in $\tilde{X}$ if $x = \varphi_{ij}(y)$. Conditions (1), (2) and (3) show that $\sim$ is reflexive, symmetric and transitive. We equip X with the quotient topology and denote by

$$p \colon \tilde{X} \to X$$

the canonical continuous projection. Let $U_i \coloneqq p(X_i)$. Since $p^{-1}(U_i) = \bigsqcup_{j\in I} X_{ji}$ is open in $\tilde{X}$, U_i is open in X. Moreover, $\bigcup_{i\in I} U_i = X$, so we have an open covering of X. We put $p_i \coloneqq p|_{X_i}$ and we define a sheaf on X by setting

$$\mathcal{O}_X(U) \coloneqq \{f \colon U \to k \mid \forall i \in I, f \circ p_i \in \mathcal{O}_{X_i}(p_i^{-1}(U))\}$$

for all open sets $U \subseteq X$. This defines a sheaf on X, with respect to which $(X, \mathcal{O}_X)$ is a space with functions. Finally, $p_i \colon X_i \to U_i$ is a homeomorphism and, by construction $\mathcal{O}_{U_i} \simeq (p_i)_* \mathcal{O}_{X_i}$ via pullback by p_i. We have thus constructed a space with functions $(X, \mathcal{O}_X)$, equipped with an open covering $(U_i)_{i\in I}$ and local charts

$$\varphi_i \coloneqq p_i^{-1} \colon (U_i, \mathcal{O}_X|_{U_i}) \xrightarrow{\sim} (X_i, \mathcal{O}_{X_i}).$$

It remains to check that $\varphi_i(U_i \cap U_j) = X_{ij}$ and $\varphi_j \circ \varphi_i^{-1} = \varphi_{ji}$ on X_{ij}, but this follows from the construction of $X = \bigsqcup_{i\in I} X_i/\sim$ and the definition of the φ_i's as $p|_{X_i}^{-1}$. □

Example 2.39. Take $k = \mathbb{R}$ or $\mathbb{C}$ equipped with either the Zariski or the usual topology. Consider the spaces with functions $X_1 = k$, $X_2 = k$ and the open sets $X_{12} = k \setminus \{0\} \subseteq X_1$ and $X_{21} = k \setminus \{0\} \subseteq X_2$. Finally, set

$$\begin{aligned} \varphi_{21} \colon X_{12} &\to X_{21} \\ t &\mapsto \frac{1}{t}. \end{aligned}$$

Since this is an isomorphism of spaces with functions, we can glue X_1 and X_2 along $X_{12} \xrightarrow[\varphi_{21}]{\sim} X_{21}$ and define a space with functions $(X, \mathcal{O}_X)$ with an atlas modelled on (X_1, X_2, φ_{21}). We will now identify this space X with the projective line $k\mathbb{P}^1$. By definition, the latter is the set of 1-dimensional vector subspaces (lines) of k^2:

$$k\mathbb{P}^1 \coloneqq (k^2 \setminus \{0\})/k^\times.$$

Then, we have a covering $U_1 \cup U_2 = k\mathbb{P}^1$, where $U_1 = \{[x_1 : x_2] \mid x_1 \neq 0\}$ and $U_2 = \{[x_1 : x_2] \mid x_2 \neq 0\}$, and we can define charts

$$\begin{aligned} \varphi_1 \colon U_1 &\xrightarrow{\sim} k \\ [x_1 : x_2] &\longmapsto x_2/x_1 \\ [1 : w] &\longmapsfrom w \end{aligned}$$

and $\varphi_2 \colon U_2 \to k$ likewise. Then, on the intersection

$$U_1 \cap U_2 = \{[x_1 : x_2] \mid x_1 \neq 0, x_2 \neq 0\}$$

we have a commutative diagram

$$\begin{array}{ccc} U_1 \cap U_2 & & \\ \downarrow{\scriptstyle \varphi_1} & \searrow^{\varphi_2} & \\ X_1 & \xrightarrow{\varphi_{21}} & X_2 \end{array}$$

with $\varphi_i(U_1 \cap U_2)$ open in X_i. In view of the gluing theorem, we can use this to set up a bijection $k\mathbb{P}^1 \to X$ where $X \coloneqq (X_1 \sqcup X_2)/\sim_{\varphi_{12}}$ and define a topology and a sheaf of regular functions on $k\mathbb{P}^1$ via this identification. Note that this was done without putting a topology on $k\mathbb{P}^1$: the latter is obtained using the bijection $k\mathbb{P}^1 \to X$ constructed above. We now spell out the notion of regular functions thus obtained on $k\mathbb{P}^1$.

Proposition 2.40. *With the identification*

$$k\mathbb{P}^1 = X_1 \sqcup X_2/\sim$$

constructed above, a function $f \colon U \to k$ defined on an open subset $U \subseteq k\mathbb{P}^1$ is an element of $\mathcal{O}_X(U)$ if and only if, for each local chart $\varphi_i \colon U_i \to k$, the function

$$f \circ \varphi_i^{-1} \colon \varphi_i(U_i \cap U) \to k$$

is regular on the open set $\varphi_i(U_i \cap U) \subseteq k$.

Definition 2.41. Let k be a field. An *algebraic k-prevariety* is a space with functions $(X, \mathcal{O}_X)$ such that

(i) X is quasi-compact.

(ii) $(X, \mathcal{O}_X)$ is locally isomorphic to an affine variety.

Remark 2.42. Saying that $(X, \mathcal{O}_X)$ is locally isomorphic to an affine variety means that for $x \in X$, it exists an open neighbourhood $x \in U$ such that $(U, \mathcal{O}_X|_U)$ is isomorphic to an open subset of an affine variety. Since such an open set is a union of principal open sets, which are themselves affine, one can equivalently ask that $(U, \mathcal{O}_U)$ be affine. Thus:

Proposition 2.43. *A space with functions $(X, \mathcal{O}_X)$ is an algebraic prevariety, if and only if there exists a finite open covering*

$$X = U_1 \cup \ldots \cup U_n$$

such that $(U_i, \mathcal{O}_X|_{U_i})$ is an affine variety.

Remark 2.44. As a consequence of the gluing theorem, in order to either construct an algebraic prevariety or put a structure of an algebraic prevariety on a set, it suffices to either define X from certain gluing data $(X_i, X_{ij}, \varphi_{ij})_{(i,j)}$ satisfying appropriate compatibility conditions, or find a covering $(U_i)_{i\in I}$ of a set X and local charts $\varphi_i \colon U_i \to X_i$ such that $X_{ij} = \varphi_i(U_i \cap U_j)$ is open in X_i and $\varphi_j \circ \varphi_i^{-1}$ is an isomorphism of spaces with functions.

In practice, X is sometimes given as a topological space, and $(U_i)_{i\in I}$ is an open covering, with local charts $\varphi_i \colon U_i \to X_i$ that are homeomorphisms. So the condition that X_{ij} be open in X_i is automatic in this case and one just has to check that

$$\varphi_j \circ \varphi_i^{-1} \colon X_{ij} \to X_{ji}$$

induces an isomorphism of spaces with functions. In the present context where X_i and X_j are affine varieties, this means a map

$$X_{ij} \subseteq k^n \to X_{ji} \subseteq k^m$$

between locally closed subsets of k^n and k^m whose components are regular functions.

Example 2.45 (Projective sets)**.** We have already seen that projective spaces $k\mathbb{P}^n$ are algebraic pre-varieties. Let $P \in k[x_0, \ldots, x_n]_d$ be a homogeneous polynomial of degree $d \geq 0$. Although P cannot be evaluated at a point $[x_0 : \ldots : x_n] \in k\mathbb{P}^n$, the condition $P(x_0, \ldots, x_n) = 0$ can be tested, because for $\lambda \in k^x$,

$$P(x_0, \ldots, x_n) = 0 \iff 0 = \lambda^d P(x_0, \ldots, x_n) = P(\lambda x_0, \ldots, \lambda x_n).$$

We use this to define the following *projective sets*

$$\mathcal{V}_{k\mathbb{P}^n}(P_1, \ldots, P_m) = \{[x_0 : \ldots : x_n] \in k\mathbb{P}^n \mid P_i(x_0, \ldots, x_n) = 0 \quad \forall i\}$$

for homogeneous polynomials in $(x_0, \ldots, x_n)$.

We claim that these projective sets are the clsoed sets of a topology on $k\mathbb{P}^n$, called the Zariski topology. A basis for that topology is provided by the principal open sets $D_{k\mathbb{P}^n}(P)$ where P is a homogeneous polynomial. By definition, a regular function on a locally closed subset of $k\mathbb{P}^n$ is locally given by the restriction of a ration fraction of the form

$$\frac{P(x_0, \ldots, x_n)}{Q(x_0, \ldots, x_n)}$$

where P and Q are homogeneous polynomials of the same degree. This defines a sheaf of regular functions on any given locally closed subset X of $k\mathbb{P}^n$.

Proposition 2.46. *A Zariski-closed subset X of $k\mathbb{P}^n$ equipped with its sheaf of regular functions, is an algebraic pre-variety. The same holds for all open subsets $U \subseteq X$.*

Proof. Consider the open covering

$$\begin{aligned} X &= \bigcup_{i=0}^{n} X \cap U_i \\ &= \bigcup_{i=0}^{n} \{[x_0 : \ldots : x_n] \in X \mid x_i \neq 0\}. \end{aligned}$$

Then the restriction to $X \cap U_i$ of the local chart

$$\begin{aligned} \varphi_i \colon U_i &\longrightarrow k^n \\ x = [x_0 : \ldots : x_n] &\longmapsto \underbrace{\left(\frac{x_0}{x_i}, \ldots, \frac{\hat{x_i}}{x_i}, \ldots, \frac{x_n}{x_i} \right)}_{w=(w_0,\ldots,\hat{w_i},\ldots,w_n)} \end{aligned}$$

sends an x such that $P_1(x) = \ldots = P_m(x) = 0$ to a w such that $Q_1(w) = \ldots = Q_m(w) = 0$ where, for all j,

$$\begin{aligned} Q_j(w) &= P_j(w_0, \ldots, w_{i-1}, 1, w_{i+1}, \ldots, w_n) \\ &= P_j(x_0, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \end{aligned}$$

is the dehomogeneisation of P_j. So $\varphi_i(X \cap U_i) = \mathcal{V}_{k^n}(Q_1, \ldots, Q_m) =: X_i$ is an algebraic subset of k^n, in particular an affine variety. It remains to check that $\varphi_i|_{X \cap U_i}$ pulls back regular functions on X_i to regular functions on $X \cap U_i$, and similarly for $(\varphi_i|_{X \cap U_i})^{-1}$. But if f and g are polynomials in $(w_0, \ldots, \hat{w_i}, \ldots, w_n)$,

$$\begin{aligned} \left(\varphi_i^* \frac{f}{g} \right)(x) &= \frac{f(\varphi_i(x))}{g(\varphi_i(x))} \\ &= \frac{f\left(\frac{x_0}{x_i}, \ldots, \frac{\hat{x_i}}{x_i}, \ldots, \frac{x_n}{x_i} \right)}{g\left(\frac{x_0}{x_i}, \ldots, \frac{\hat{x_i}}{x_i}, \ldots, \frac{x_n}{x_i} \right)} \end{aligned}$$

which can be rewritten as a quotient of two homogeneous polynomials of the same degree by multiplying the numerator and denominator by x_i^r with $r \geq \max(\deg(f), \deg(g))$. The computation is similar but easier for $(\varphi_i|_{X \cap U_i})^{-1}$. □

Definition 2.47. A space with functions $(X, \mathcal{O}_X)$ which is isomorphic to a Zariski-closed subset of $k\mathbb{P}^n$ is called a *projective k-variety*.

Lemma 2.48. *The category of affine varieties admits products.*

Proof. Let $(X, \mathcal{O}_X)$, $(Y, \mathcal{O}_Y)$ be affine varieties. Choose embeddings $X \subseteq k^n$ and $Y \subseteq k^p$ for some n and p. Then $X \times Y \subseteq k^{n+p}$ is an affine variety, endowed with two morphisms of affine varieties $\mathrm{pr}_1 \colon X \times Y \to X$ and $\mathrm{pr}_2 \colon X \times Y \to Y$. We will prove that the triple $(X \times Y, \mathrm{pr}_1, \mathrm{pr}_2)$ satisfies the universal property of the product of X and Y.

Let $f_X \colon Z \to X$ and $f_Y \colon Z \to Y$ be morphisms of affine varieties. Then define $f = (f_x, f_y) \colon Z \to X \times Y$. This satisfies $\mathrm{pr}_1 \circ f = f_X$ and $\mathrm{pr}_2 \circ f = f_Y$. If we embed Z into some k^m, the components of f_X and f_Y are regular functions from k^m to k^n and k^p. Thus the components of $f = (f_X, f_Y)$ are regular functions $k^m \to k^{n+p}$, i.e. f is a morphism. □

Theorem 2.49. *The category of algebraic pre-varieties admits products.*

Proof. Let $(X, \mathcal{O}_X), (Y, \mathcal{O}_Y)$ algebraic pre-varieties. Let

$$X = \bigcup_{i=1}^{r} X_i \text{ and } Y = \bigcup_{j=1}^{s} Y_j$$

be affine open covers. Then, as a set,

$$X \times Y = \bigcup_{i,j} X_i \times Y_j.$$

By 2.48, each $X_i \times Y_j$ has a well-defined structure of affine variety. Moreover, if $X_i' \subseteq X_i$ and $Y_j' \subseteq Y_j$ are open sets, then $X_i' \times Y_j'$ is open in $X_i \times Y_j$.

So we can use the identity morphism to glue $X_{i_1} \times Y_{j_1}$ to $X_{i_2} \times Y_{j_2}$ along the common open subset $(X_{i_1} \cap X_{i_2}) \times (Y_{j_1} \cap Y_{j_2})$. This defines an algebraic prevariety P whose underlying set is $X \times Y$. Also, the canonical projections $X_i \times Y_j \to X_i$ and $X_i \times X_j \to X_j$ glue together to give morphisms $p_X \colon X \times Y \to X$ and $p_Y \colon X \times Y \to Y$, which coincide with pr_1 and pr_2.

There only remains to prove the universal property. Let $f_x \colon Z \to X$ and $f_Y \colon Z \to Y$ be morphisms of algebraic prevarieties and set $f = (f_x, f_y) \colon Z \to X \times Y$. In particular, $\mathrm{pr}_1 \circ f = f_X$ and $\mathrm{pr}_2 \circ f = f_Y$ as maps between sets. To prove that f is a morphisms of algebraic prevarieties, it suffices to show that this is locally the case. Z is covered by the open subsets $f_X^{-1}(X_i) \cap f_Y^{-1}(Y_j)$, each of which can be covered by affine open subsets $(W_l^{ij})_{1 \leq l \leq q(i,j)}$. By construction, $f(W_l^{ij}) \subseteq X_i \times Y_j$. So, by the universal property of the affine variety $X_i \times Y_j$, the map $f|_{W_l^{ij}}$ is a morphism of affine varieties. □

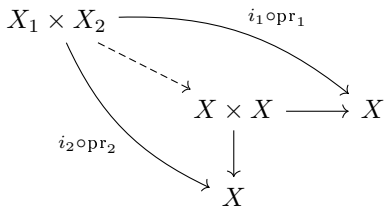
Definition 2.50 (algebraic variety)**.** Let $(X, \mathcal{O}_X)$ be an algebraic pre-variety and $X \times X$ the product in the category of algebraic pre-varieties. If the subset

$$\Delta_X \coloneqq \{(x, y) \in X \times X \mid x = y\}$$

is closed in $X \times X$, then $(X, \mathcal{O}_X)$ is said to be an *algebraic variety*. A morphism of algebraic varieties $f \colon X \to Y$ is a morphism of the underlying pre-varieties.

Example 2.51 (of a non-seperated algebraic prevariety)**.** We glue two copies X_1, X_2 of k along the open subsets $k \setminus \{0\}$ using the isomorphism of spaces with functions $t \mapsto t$. The resulting algebraic prevariety is a „line with two origins", denoted by 0_1 and 0_2. For this prevariety X, the diagonal Δ_X is not closed in $X \times X$.

Indeed, if Δ_X were closed in $X \times X$, then its pre-image in $X_1 \times X_2$ under the morphism $f \colon X_1 \times X_2 \to X \times X$ defined by



where $i_j \colon X_j \hookrightarrow X$ is the canonical inclusion of X_j into $X = (X_1 \sqcup X_2) / \sim$, would be closed in $X_1 \times X_2$. But

$$\begin{aligned} f^{-1}(\Delta_X) &= \{(x_1, x_2) \in X_1 \times X_2 \mid i_1(x_1) = i_2(x_2)\} \\ &= \{(x_1, x_2) \in X_1 \times X_2 \mid x_j \neq 0 \text{ and } x_1 = x_2 \text{ in } k\} \\ &= \{(x, x) \in k \times k \mid x \neq 0\} \subseteq k \times k = X_1 \times X_2 \end{aligned}$$

which is not closed in $X_1 \times X_2$. In fact, $f^{-1}(\Delta_X) = \Delta_k \setminus \{(0,0)\} \subseteq k \times k$.

Corollary 2.52. *Let $(X, \mathcal{O}_X)$, $(Y, \mathcal{O}_Y)$ be algebraic varieties, then the product in the category of algebraic pre-varieties is an algebraic variety. In particular the category of algebraic varieties admits products.*

Proof. $\Delta_{X \times Y} \simeq \Delta_X \times \Delta_Y \subseteq (X \times X) \times (Y \times Y)$. □

Proposition 2.53. *Affine varieties are algebraic varieties.*

Proof. Let X be an affine variety. We choose an embedding $X \subseteq k^n$. Then $\Delta_X = \Delta_{k^n} \cap (X \times X)$. But

$$\Delta_{k^n} = \{(x_i, y_i)_{1 \leq i \leq n} \in k^{2n} \mid x_i - y_i = 0\}$$

is closed in k^{2n}. Therefore, Δ_X is closed in $X \times X$ (note that the prevariety topology of $X \times X$ coincides with its induced topology as a subset of k^{2n} by construction of the product prevariety $X \times X$). □

Exercise 2.54. Let $(X, \mathcal{O}_X)$ be an algebraic pre-variety and let $Y \subseteq X$ be a closed subset. For all open subsets $U \subseteq Y$, we set

$$\mathcal{O}_Y(U) \coloneqq \left\{ h \colon U \to k \mid \forall x \in U \exists x \in \hat{U} \subseteq X \text{ open}, g \in \mathcal{O}_X(\hat{U}) \text{ such that } g|_{\hat{U} \cap U} = h|_{\hat{U} \cap U} \right\}.$$

(a) Show that this defines a sheaf of regular functions on Y and that $(Y, \mathcal{O}_Y)$ is an algebraic prevariety.

(b) Show that the canonical inclusion $i_Y \colon Y \hookrightarrow X$ is a morphism of algebraic prevarieties and that if $f \colon Z \to X$ is a morphism of algebraic prevarieties such that $f(Z) \subseteq Y$, then f induces a morphism $\tilde{f} \colon Y \to Z$ such that $i_Y \circ \tilde{f} = f$.

(c) Show that, if X is an algebraic variety, then Y is also an algebraic variety.

Recall that $k\mathbb{P}^n$ is the projectivisation of the k-vector space k^{n+1}:

$$k\mathbb{P}^n = P(k^{n+1})(k^{n+1} \setminus \{0\})/k^\times.$$

Proposition 2.55 (Segre embedding)**.** *The k-bilinear map*

$$\begin{aligned} k^{n+1} \times k^{m+1} &\longrightarrow k^{n+1} \otimes_k k^{m+1} \simeq k^{(n+1)(m+1)} \\ (x, y) &\longmapsto x \otimes y \end{aligned}$$

induces an isomorphism of algebraic pre-varieties

$$\begin{aligned} P(k^{n+1}) \times P(k^{m+1}) &\xrightarrow{f} \zeta \subseteq P\left(k^{(n+1)(m+1)}\right) = k\mathbb{P}^{nm+n+m} \\ ([x_0 : \ldots : x_n], [y_0 : \ldots : y_m]) &\longmapsto [x_0 y_0 : \ldots x_0 y_m : \ldots : x_n y_0 : \ldots : x_n y_m] \end{aligned}$$

where ζ is a Zariski-closed subset of $k\mathbb{P}^{nm+n+m}$.

Proof. It is clear that f is well-defined. Let us denote by $(z_{ij})_{0 \leq i \leq n, 0 \leq j \leq m}$ the homogeneous coordinates on $k\mathbb{P}^{nm+n+m}$, and call them *Segre coordinates*. Then $f(k\mathbb{P}^n \times k\mathbb{P}^m)$ is contained in the projective variety

$$\begin{aligned} \zeta &= \mathcal{V}\left(\{z_{ij} z_{kl} - z_{kj} z_{il} \mid 0 \leq i, k \leq n, 0 \leq j, l \leq m\}\right) \\ &\subseteq P\left(k^{(n+1)(m+1)}\right) \end{aligned}$$

as can be seen by writing

$$f([x], [y]) = \begin{bmatrix} x_0 y_0 : & \ldots & : x_0 y_m \\ \vdots & & \vdots \\ x_n y_0 : & \ldots & : x_n y_m \end{bmatrix}$$

so that

$$z_{ij} z_{kl} - z_{kj} z_{il} = \begin{vmatrix} x_i y_j & x_i y_l \\ x_k y_j & x_k y_l \end{vmatrix} = 0.$$

The map f is injective because, if $z \coloneqq f([x], [y]) = f([x'], [y'])$ then there exists (i, j) such that $z \in W_{ij} \coloneqq \{z \in k\mathbb{P}^{nm+n+m} \mid z_{ij} \neq 0\}$ so $x_i y_j = x'_i y'_j \neq 0$. In particular $\frac{x_i}{x'_i} = \frac{y'_j}{y_j} = \lambda \neq 0$. Since

$$[x_0 y_0 : \ldots : x_n y_m] = [x'_0 y'_0 : \ldots : x'_n y'_m]$$

means that there exists $\mu \neq 0$ such that, for all (k,l), $x_k y_l = \mu x'_k y'_l$. Taking $k = i$ and $l = j$, we get that $\mu = 1$ and hence, for all k, $x_k y_j = x'_k y'_j$, so $x_k = \frac{y'_j}{y_j} x'_k = \lambda x'_k$. Likewise, for all l, $x_i y_l = x'_i y'_l$, so $y_l = \frac{1}{\lambda} y'_l$. As a consequence $[x_0 : \ldots : x_n] = [x'_0 : \ldots : x'_n]$ and $[y_0 : \ldots : y_m] = [y'_0 : \ldots : y'_m]$, thus proving that f is injective. Note that we have proven that

$$f^{-1}(W_{ij}) = U_i \times V_j$$

where $U_i = \{[x] \in k\mathbb{P}^n \mid x_i \neq 0\}$ and $V_j = \{[y] \in k\mathbb{P}^m \mid y_j \neq 0\}$.

For simplicity, let us assume that $i = j = 0$. The open sets U_0, V_0, W_0 are affine charts, in which f is equivalent to

$$\begin{aligned} k^n \times k^m &\longrightarrow k^{nm+n+m} \\ (u,v) &\longmapsto (v_1, \ldots, v_m, u_1, u_1 v_1, \ldots, u_1 v_m, \ldots, u_n, u_n v_1, \ldots, v_n v_m) \end{aligned}$$

which is clearly regular. In particular $f \mid U_0 \times V_0$ is a morphism of algebraic pre-varieties.

im $f = \zeta$: Let $[z] \in \zeta$. Since the W_{ij} cover $k\mathbb{P}^{nm+n+m}$, we can assume without loss of generality, $z_{00} \neq 0$. Then by definition of ζ, $z_{kl} = \frac{z_{k_0} z_{0l}}{z_{00}}$ for all (k,l). If we set

$$([x_0 : \ldots : x_n], [y_0 : \ldots : y_m]) = \left(\left[1 : \frac{z_{10}}{z_{00}} : \ldots : \frac{z_{n_0}}{z_{00}} \right], \left[1 : \frac{z_{01}}{z_{00}} : \ldots : \frac{z_{0m}}{z_{00}} \right] \right)$$

we have a well defined point $([x],[y]) \in U_0 \times V_0 \subseteq k\mathbb{P}^n \times k\mathbb{P}^m$, which satisfies $f([x],[y]) = [z]$.

Thus $f^{-1} \colon \zeta \to k\mathbb{P}^n \times k\mathbb{P}^m$ is defined and a morphism of algebraic pre-varieties because, in affine charts $W_0 \xrightarrow{f^{-1}|_{W_0}} U_0 \times V_0$ as above, it is the regular map $(u_{ij})_{(i,j)} \mapsto ((u_{i_0})_i, (u_{0j})_j)$. □

Corollary 2.56. *Projective varieties are algebraic varieties.*

Proof. By 2.54 it suffices to show that $k\mathbb{P}^n$ is an algebraic variety. Let $f \colon k\mathbb{P}^n \times k\mathbb{P}^n \to k\mathbb{P}^{n^2+2n}$ be the Segre embedding. For $[x] \in k\mathbb{P}^n$:

$$f([x],[x]) = \begin{bmatrix} x_0x_0 : & \ldots & : x_0x_m \\ \vdots & & \vdots \\ x_nx_0 : & \ldots & : x_nx_m \end{bmatrix}.$$

Thus $f([x],[x])_{ij} = f([x],[x])_{ji}$. Let now $[z] \in \zeta \subseteq k\mathbb{P}^{n^2+2n}$, where ζ is defined in the proof of 2.55, and such that, in Segre coordinates, $z_{ij} = z_{ji}$. Without loss of generality, we can assume $z_{00} = 1$. Set $x_j := z_{0j}$ for $1 \leq j \leq n$. Thus for all (i,j)

$$f([x],[y])_{ij} = x_i x_j = z_{0i} z_{0j} = z_{i0} z_{0j} = z_{ij} z_{00} = z_{ij},$$

i.e.

$$\Delta_{k\mathbb{P}^n} \simeq \{[z] \in \zeta \mid z_{ij} = z_{ji}\}$$

which is a projective and thus closed set of $k\mathbb{P}^n \times k\mathbb{P}^n$. □

2.6 Examples of algebraic varieties

Exercise 2.57. Let $f\colon X \to Y$ be a morphism of algebraic pre-varieties. Assume

(i) Y is a variety.

(ii) There exists an open covering $(Y_i)_{i\in I}$ of Y such that the open subset $f^{-1}(Y_i)$ is a variety.

Show that X is a variety.

Exercise 2.58. Let X be a topological space. Assume that there exists a covering $(X_i)_{i\in I}$ of X by irreducible open subsets such that for all (i,j), $(X_i \cap X_j) \neq \emptyset$. Show that X is irreducible.

2.6.1 Grassmann varieties

Let $0 \leq p \leq n$ be integers. The Grassmannian $\mathrm{Gr}(p,n)$ is the set of p-dimensional linear subspaces of k^n. In order to endow this set with a structure of algebraic prevariety, there are various possibilities:

(i) To a p-dimensional linear subspace $E \subseteq k^n$, we associate the line $\Lambda^p E \subseteq \Lambda^p k^n \simeq k^{\binom{n}{p}}$, which defines a point in the projective space $k\mathbb{P}^{\binom{n}{p}-1}$.

Claim: The map $\mathrm{Gr}(p,n) \to k\mathbb{P}^{\binom{n}{p}-1}$ is an injective map whose image is a Zariski-closed subset of $k\mathbb{P}^{\binom{n}{p}-1}$.

This identifies $\mathrm{Gr}(n,p)$ canonically to a projective variety. In particular one obtains in this way a structure of *algebraic variety* on $\mathrm{Gr}(p,n)$.

(ii) For the second approach, recall that $\mathrm{GL}(n,k)$ acts transitively on $\mathrm{Gr}(p,n)$. But the identification of k^n to $(k^n)^*$ via the canonical basis of k^n enables one to define, for all $E \in \mathrm{Gr}(p,n)$, a canonical complement $E^\perp \in \mathrm{Gr}(n-p,n)$, i.e. an $(n-p)$-dimensional linear subspace such that $E \oplus E^\perp = k^n$.

So the stabiliser of $E \in \mathrm{Gr}(p,n)$ for the action of $\mathrm{GL}(n,k)$ is conjugate to the subgroup

$$\mathrm{P}(p,n) \coloneqq \left\{ g \in \mathrm{GL}(n,k) \;\middle|\; \begin{array}{l} g = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \\ \text{with } A \in \mathrm{GL}(p,k), B \in \mathrm{Mat}(p \times (n-p), k), \\ \text{and } C \in \mathrm{GL}(n-p,k) \end{array} \right\}.$$

This shows that the Grassmannian $\mathrm{Gr}(p,n)$ is a homogeneous space under $\mathrm{GL}(n,k)$ and that

$$\mathrm{Gr}(p,n) \simeq \mathrm{GL}(n,k)/\mathrm{P}(p,n)$$

which is useful if one knows that, given an affine algebraic group G and a closed subgroup H, the homogeneous space G/H is an algebraic variety. We will come back to this later on.

(iii) The third uses the gluing theorem. In particular, it also constructs a standard atlas on $\mathrm{Gr}(p,n)$, like the one we had on $k\mathbb{P}^{n-1} = \mathrm{Gr}(1,n)$. The idea is that, in order to determine a p-dimensional subspace of k^n, it suffices to give a basis of that subspace, which is a family of p vectors in k^n. Geometrically, this means that the subspace in question is seen as the graph of a linear map $A\colon k^p \to k^n$.

Take $E \in \mathrm{Gr}(p,n)$ and let $(v_1,\ldots,v_p)$ be a basis of E over k. Let M be the $(n \times p)$-matrix representing the coordinates of $(v_1,\ldots,v_p)$ in the canonical basis of k^n. Since M has rank p, there exists a $(p \times p)$-submatrix of M with non-zero determinant: We set

$$\begin{aligned} J &\coloneqq \{\text{indices } j_1 < \ldots < j_p \text{ of the rows of that submatrix}\} \\ M_J &\coloneqq \text{the submatrix in question.} \end{aligned}$$

Note that if $M' \in \mathrm{Mat}(n \times p, k)$ corresponds to a basis $(v'_1, \ldots, v'_p)$, there exists a matrix $g \in \mathrm{GL}(p, k)$ such that $M' = Mg$. But then $(M')_J = (Mg)_J = M_J g$, so

$$\det\ (M')_J = \det\ (M_J g) = \det(M_J)\det(g),$$

which is non-zero if and only if $\det(M_J)$ is non-zero. As a consequence, given a subset $J \subseteq \{1, \ldots, n\}$ of cardinal p, there is a well-defined subset

$$G_J \coloneqq \{E \in \mathrm{G}(p, n) \mid \exists M \in \mathrm{Mat}(n \times p, k), E = \mathrm{im}\ M \text{ and } \det(M_J) \neq 0\}.$$

Moreover, if M satisfies the conditions $E = \mathrm{im}\ M$ and $\det(M_J) \neq 0$, then $(MM_J^{-1})_J = I_p$ and $\mathrm{im}(MM_J^{-1}) = \mathrm{im}\ M = E$. In fact, if $E \in G_J$, there is a unique matrix $N \in \mathrm{Mat}(n \times p, k)$, such that $E = \mathrm{im}\ N$ and $N_J = I_p$, for if N_1, N_2 are two such matrices, the columns of N_2 are linear combinations of those of N_1, thus $\exists g \in \mathrm{GL}(p, k)$ such that $N_2 = N_1 g$. But then

$$I_p = (N_2)_J = (N_1 g)_J = (N_1)_J g = g.$$

So, there is a well-defined map

$$\begin{aligned} \hat{\varphi}_J : G_J &\longrightarrow \mathrm{Hom}(k^J, k^n) \\ E &\longmapsto N \text{ such that } E = \mathrm{im}\ N \text{ and } N_J = I_p \end{aligned}$$

whose image can be identified to the subspace $\mathrm{Hom}(k^J, k^{J^c})$, where J^c is the complement of J in $\{1, \ldots, n\}$, via the map $N \mapsto N_{J^c}$. Conversely, a linear map $A \in \mathrm{Hom}(k^J, k^{J^c})$ determines a rank p map $N \in \mathrm{Hom}(k^J, k^n)$ such that $N_J = I_p$ via the formula $N(x) = x + Ax$.

Geometrically, this means that the p-dimensional subspace $\mathrm{im}\ N \subseteq k^n$ is equal to the graph of A. This also means that we can think of G_J as the set

$$\{E \in \mathrm{Gr}(p, n) \mid E \cap k^{J^c} = \{0_{k^n}\}\}.$$

The point is that $\mathrm{im}\ \hat{\varphi}_J = \mathrm{Hom}(k^J, k^{J^c})$ can be canonically identified with the affine space $k^{p(n-p)}$ and that we have a bijection

$$\begin{aligned} \varphi_J : G_J &\xrightarrow{\simeq} \mathrm{Hom}(k^J, k^{J^c}) \simeq k^{p(n-p)} \\ E &\longmapsto A \mid \mathrm{gr}(A) = E \\ \mathrm{gr}(A) &\longmapsfrom A. \end{aligned}$$

Note that the matrix $N \in \mathrm{Mat}(n \times p, k)$ such that $\mathrm{im}\ N = E$ and $N_J = I_p$ is row-equivalent to $\begin{pmatrix} I_p \\ A \end{pmatrix}$ with $A \in \mathrm{Mat}((n-p) \times p, k)$.

Now, if $E \in G_{J_1} \cap G_{J_2}$, then, for all $M \in \mathrm{Mat}(p \times n, k)$ such that $\mathrm{im}\ M = E$, $\hat{\varphi}_{J_1}(E) = MM_{J_1}^{-1}$ and $\hat{\varphi}_{J_2}(E) = MM_{J_2}^{-1}$. So

$$\begin{aligned} \mathrm{im}\ \hat{\varphi}_{J_1} &= \left\{N \in \mathrm{Hom}(k^{J_1}, k^n) \mid N_{J_1} = I_p, \mathrm{im}\ N_{J_1} = E \text{ and } \det(N_{J_2}) \neq 0\right\} \\ &= \{N \in \mathrm{im}\ \hat{\varphi}_{J_1} \mid \det(N_{J_2}) \neq 0\} \end{aligned}$$

which is open in $\mathrm{im}\ \hat{\varphi}_{J_1} \simeq \mathrm{im}\ \varphi_{J_1}$.

Moreover, for all $N \in \mathrm{im}\ \hat{\varphi}_{J_1}$,

$$\hat{\varphi}_{J_2} \circ \hat{\varphi}_{J_1}^{-1}(N) = NN_{J_2}^{-1}$$

and, by Cramer's formulae, this is a regular function on $\mathrm{im}\ \hat{\varphi}_{J_1}$.

We have therefore constructed a covering

$$\mathrm{Gr}(p,n) = \bigcup_{J\subseteq\{1,\dots,n\},\#J=p} G_J$$

of the Grassmannian $\mathrm{Gr}(p,n)$ by subsets G_J that can be identified to the affine variety $k^{p(n-p)}$ via bijective maps $\varphi_J\colon G_j \to k^{p(n-p)}$ such that, for all (J_1,J_2), $\varphi_{J_1}(G_{J_1}\cap G_{J_2})$ is open in $k^{p(n-p)}$ and the map $\varphi_{J_2}\circ\varphi_{J_1}^{-1}\colon \varphi_{J_1}(G_{J_1}\cap G_{J_2}) \to \varphi_{J_2}(G_{J_1}\cap G_{J_2})$ is a morphism of affine varieties. By the gluing theorem, this endows $\mathrm{Gr}(p,n)$ with a structure of algebraic prevariety.

2.6.2 Vector bundles

Definition 2.59. A *vector bundle* is a triple (E,X,π) consisting of two algebraic varieties E and X, and a morphism $\pi\colon E\to X$ such that

(i) for $x\in X$, $\pi^{-1}(\{x\})$ is a k-vector space.

(ii) for $x\in X$, there exists an open neighbourhood U of x and an isomorphism of algebraic varieties

$$\Phi\colon \pi^{-1}(U) \xrightarrow{\simeq} U\times\pi^{-1}(\{x\})$$

such that

(a) $\mathrm{pr}_1\circ\Phi = \pi|_{\pi^{-1}(U)}$ and

(b) for $y\in U$, $\Phi|_{\pi^{-1}(\{y\})}\colon \pi^{-1}(\{y\}) \to \{y\}\times\pi^{-1}(\{x\})$ is an isomorphism of k-vector spaces.

A morphism of vector bundles is a morphism of algebraic varieties $f\colon E_1\to E_2$ such that $\pi_2\circ f = \pi_1$ and f is k-linear in the fibres.

Remark 2.60. In practice, one often proves that a variety E is a vector bundle over X by finding a morphism $\pi\colon E\to X$ and an open covering

$$X = \bigcup_{i\in I} U_i$$

such that $E|_{U_i} \coloneqq \pi^{-1}(U_i)$ is isomorphic to $U_i\times k^{n_i}$ for some integer n_i, in such a way that, on $U_i\cap U_j$, the morphism

$$\Phi_j\circ\Phi_i^{-1}\Big|_{\Phi_i(\pi^{-1}(U_i\cap U_j))} : (U_i\cap U_j)\times k^{n_i} \longrightarrow (U_i\cap U_j)\times k^{n_j}$$

is an isomorphism of algebraic varieties such that the following diagram commutes and $\Phi_j\circ\Phi_i^{-1}$ is linear fibrewise:

$$\begin{array}{ccc} (U_i\cap U_j)\times k^{n_i} & \xrightarrow{\Phi_j\circ\Phi_i^{-1}} & (U_i\cap U_j)\times k^{n_j} \\ & {\scriptstyle \mathrm{pr}_1}\searrow \quad \swarrow{\scriptstyle \mathrm{pr}_1} & \\ & U_i\cap U_j & \end{array} .$$

In particular $k^{n_i}\simeq k^{n_j}$ as k-vector spaces, so $n_i = n_j$ if $U_i\cap U_j\neq\emptyset$, and $\Phi_j\circ\Phi_i^{-1}$ is necessarily of the form

$$(x,v)\longmapsto (x, g_{ji}(x)\cdot v)$$

for some morphism of algebraic varieties

$$g_{ji}\colon U_i \cap U_j \longrightarrow \mathrm{GL}(n,k).$$

These maps $(g_{ij})_{(i,j)\in I\times I}$ then satisfy for $x \in U_i \cap U_j \cap U_l$

$$g_{lj}(x)g_{ji}(x) = g_{li}(x)$$

and for $x \in U_i$, $g_{ii}(x) = \mathrm{I}_n$.

Proposition 2.61. *If $\pi\colon E \to X$ is a morphism of algebraic varieties and X has an open covering $(U_i)_{i\in I}$ over which E admits local trivialisations*

$$\Phi_i\colon E|_{U_i} = \pi^{-1}(U_i) \xrightarrow{\simeq} U_i \times k^n$$

with $pr_1 \circ \Phi_i = \pi|_{\pi^{-1}(U_i)}$ such that the isomorphisms

$$\Phi_j \circ \Phi_i^{-1}\colon (U_i \cap U_j) \times k^n \longrightarrow (U_i \cap U_j) \times k^n$$

are linear in the fibres, then for all $x \in X$, $\pi^{-1}(\{x\})$ has a well-defined structure of k-vector space and the local trivialisations $(\Phi_i)_{i\in I}$ are linear in the fibres. In particular, E is a vector bundle.

Proof. For $x \in U_i$ and $a, b \in \pi^{-1}(\{x\})$, let

$$a + \lambda b \coloneqq \Phi_i^{-1}(x, \mathrm{pr}_2(\Phi_i(a)) + \lambda \mathrm{pr}_2(\Phi_i(b))).$$

By using the linearity in the fibres of $\Phi_j \circ \Phi_i^{-1}$, one verifies that this does not depend on the choice of $i \in I$. □

Remark 2.62. Assume given an algebraic prevariety X obtained by gluing affine varieties $(X_i)_{i\in I}$ along isomorphisms $\varphi_{ji}\colon X_{ij} \xrightarrow{\simeq} X_{ji}$ defined on open subsets $X_{ij} \subseteq X_i$, such that $X_{ii} = X_i$, $\varphi_{ii} = \mathrm{Id}_{X_i}$ and $\varphi_{lj} \circ \varphi_{ji} = \varphi_{li}$ on $X_{ij} \cap X_{il} \subseteq X_i$.

Recall that such an X comes equipped with a canonical map $p\colon \bigsqcup_{i\in I} \to X$ such that $p_i \coloneqq p|_{X_i}\colon X_i \to X$ is an isomorphism onto an affine open subset $U_i \coloneqq p_i(X_i) \subseteq X$ and, if we set $\varphi_i = p_i^{-1}$, we have $\varphi_j \circ \varphi_i^{-1} = \varphi_{ji}$ on $\varphi_i(U_i \cap U_j)$.

Let us now consider the vector bundle $X_i \times k^n$ on each of the affine varieties X_i and assume that an isomorphism of algebraic prevarieties of the form

$$\begin{aligned}\Phi_{ji}\colon X_{ij} \times k^n &\longrightarrow X_{ji} \times k^n\\ (x,v) &\longmapsto (\varphi_{ji}(x), h_{ji}(x)\cdot v)\end{aligned}$$

has been given, where $h_{ij}\colon X_{ij} \to \mathrm{GL}(n,k)$ is a morphism of algebraic varieties, in such a way that the following compatibility conditions are satisfied:

$$\Phi_{ii} = \mathrm{Id}_{X_{ii}\times k^n}$$

and, for all (i,j,l) and all $(x,v) \in (X_{ij} \cap X_{il}) \times k^n$

$$\Phi_{lj} \circ \Phi_{ji}(x,v) = \Phi_{li}(x,v).$$

Then there is associated to this gluing data an algebraic vector bundle $\pi\colon E \to X$, endowed with local trivialisations $\Phi_i\colon E|_{U_i} \xrightarrow{\simeq} U_i \times k^n$, where as earlier $U_i = p(X_i) \subseteq X$, in such a way that, for all (i,j) and all $(\xi, v) \in (U_i \cap U_j) \times k^n$,

$$\Phi_j \circ \Phi_i^{-1}(\xi, v) = (\xi, g_{ji}(\xi)\cdot v)$$

where $g_{ji}(x) = h_{ji}(\varphi_i(\xi)) \in \mathrm{GL}(n,k)$, so $g_{ii} = \mathrm{I}_n$ on U_i, and, for all (i,j,l) and all $\xi \in U_i \cap U_j \cap U_l$,

$$\begin{aligned} g_{lj}(\xi)g_{ji}(\xi) &= h_{lj}(\varphi_j(\xi))h_{ji}(\varphi_i(\xi)) \\ &= h_{lj}(\varphi_{ji}(\varphi_i(\xi)))h_{ji}(\varphi_i(\xi)) \\ &= h_{li}(\varphi_i(\xi)) \\ &= g_{li}(\xi). \end{aligned}$$

Indeed, we can simply set

$$E \coloneqq \left(\bigsqcup_{i \in I} X_i \times k^n \right) / \sim$$

where $(x,v) \sim (\varphi_{ji}(x), h_{ji}(x) \cdot v)$, and, by the gluing theorem, this defines an algebraic prevariety, equipped with a morphism $\pi \colon E \to X$ induced by the first projection $\mathrm{pr}_1 \colon \bigsqcup_{i \in I}(X_i \times k^n) \to \bigsqcup_{i \in I} X_i$. The canonical map $\hat{p} \colon \bigsqcup_{i \in I}(X_i \times k^n) \to E$ makes the following diagram commute

$$\begin{array}{ccc} \bigsqcup_{i \in I}(X_i \times k^n) & \xrightarrow{\hat{p}} & E \\ \downarrow{\scriptstyle \mathrm{pr}_1} & & \downarrow{\scriptstyle \pi} \\ \bigsqcup_{i \in I} X_i & \xrightarrow{p} & X \end{array}$$

and it induces an isomorphism of prevarieties

$$\hat{p}|_{X_i \times k^n} \colon X_i \times k^n \xrightarrow{\simeq} E|_{p(X_i)} = \pi^{-1}(p(X_i))$$

such that $\pi \circ \hat{p}|_{X_i \times k^n} = p|_{X_i} \circ \mathrm{pr}_1$. Since $p|_{X_i}$ is an isomorphism between X_i and the open subset $U_i = p(X_i) \subseteq X$ with inverse φ_i, the isomorphism $\hat{p}|_{X_i \times k^n}$ induces a local trivialisation

$$\begin{aligned} \Phi_i \colon E|_{U_i} &\longrightarrow U_i \times k^n \\ w &\longmapsto (\pi(w), v) \end{aligned}$$

where v is defined as above by $\hat{p}(x,v) = w$. Note that $p(x) = \pi(w)$ in this case, and that $\pi^{-1}(\{\pi(w)\}) \simeq k^n$ via $\Phi|_{\pi^{-1}(\{\pi(w)\})}$. As the isomorphism of algebraic prevarieties

$$\Phi_j \circ \Phi_i^{-1} \colon (U_i \cap U_j) \times k^n \longrightarrow (U_i \cap U_j) \times k^n$$

thus defined is clearly linear fibrewise, we have indeed constructed in this way a vector bundle $\pi \colon E \to X$, at least in the category of algebraic prevarieties.

Note that if the prevariety X obtained via the gluing of the X_i is a variety, then we can show that E is actually a variety (because the product variety $U_i \times k^n$ is separated). The rest of the verifications, in particular the fact that for all $(\xi, v) \in U_i \cap U_j \times k^n$

$$\Phi_j \circ \Phi_i^{-1}(\xi, v) = (\xi, h_{ji}(\varphi_i(\xi)) \cdot v)$$

is left to the reader.

Exercise 2.63. Consider the set

$$E \coloneqq \{(\rho, v) \in k\mathbb{P}^1 \times k\mathbb{P}^2 \mid v \in \rho\}$$

and the canonical map $\pi \colon E \to k\mathbb{P}^1$.

Show that E is a vector bundle on $k\mathbb{P}^1$ and compute its „cocycle of transition functions“ g_{10} on the standard atlas (U_0, U_1) of $k\mathbb{P}^1$ with

$$\begin{aligned} \varphi_{10} \colon k \setminus \{0\} &\longrightarrow k \setminus \{0\} \\ t &\longmapsto \frac{1}{t}. \end{aligned}$$

Chapter 3

Hilbert's Nullstellensatz and applications

3.1 Fields of definition

When k is an algebraically closed field, Hilbert's Nullstellensatz gives us a bijection between algebraic subsets of k^n and radical ideals in $k[T_1, \ldots, T_n]$.

This correspondence induces an anti-equivalence of categories

$$\begin{aligned} \{\text{affine } k\text{-varieties}\} &\longleftrightarrow \{\text{finitely-generated reduced } k\text{-algebras}\} \\ (X, \mathcal{O}_X) &\longmapsto \mathcal{O}_X(X) \\ \hat{A} = \mathrm{Hom}_{k-\mathrm{alg}}(A, k) &\longleftarrow\!\shortmid A. \end{aligned}$$

Lemma 3.1. *Let k be algebraically closed and A a finitely-generated k-Algebra. Then the map*

$$\begin{aligned} \hat{A} = \mathrm{Hom}_{k\text{-}alg}(A, k) &\longrightarrow \mathrm{Spm}\, A \\ \xi &\longmapsto ker\ \xi \end{aligned}$$

is a bijection.

Proof. The map admits an inverse

$$\begin{aligned} \mathrm{Spm}\, A &\longrightarrow \mathrm{Hom}_{k\text{-alg}}(A, k) \\ \mathfrak{m} &\longmapsto (A \to A/\mathfrak{m}). \end{aligned}$$

This is well-defined, since $A/\mathfrak{m}$ is a finite extension of the algebraically closed field k, so $k \simeq A/\mathfrak{m}$. □

Since we have defined a product on the left-hand side of the anti-equivalence, this must correspond to coproduct on the right-hand side. Since the coproduct in the category of commutative k-algebras with unit is given by the tensor product, we have

$$\mathcal{O}_{X\times Y}(X \times Y) \simeq \mathcal{O}_X(X) \otimes_k \mathcal{O}_Y(Y).$$

Corollary 3.2. *Let k be algebraically closed. Then the tensor product of two reduced (resp. integral) finitely-generated k-algebras is reduced (resp. integral).*

Proof. This follows from the anti-equivalence of categories: Reduced since products of affine k-varieties exist and integral since the product of two irreducible affine k-varieties is irreducible. □

Remark 3.3. 3.2 is false in general if $k = \overline{k}$. For instance $\mathbb{C}$ is an integral $\mathbb{R}$-algebra, but

$$\begin{aligned}\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &= \mathbb{R}[x]/(x^2+1) \otimes_{\mathbb{R}} \mathbb{C} \\ &= \mathbb{C}[x]/(x^2+1) \\ &= \mathbb{C}[x]/((x-i)(x+i)) \\ &\overset{(*)}{\simeq} \mathbb{C}[x]/(x-i) \times \mathbb{C}[x]/(x+i) \\ &\simeq \mathbb{C} \times \mathbb{C}\end{aligned}$$

is not integral, where $(*)$ follows from the Chinese remainder theorem.

For a non-reduced example, consider $k = \mathbb{F}_p(t)$ and choose a p-th root $\alpha = t^{\frac{1}{p}}$ in $\overline{\mathbb{F}_p(t)}$. Then $\alpha \notin k$ but $\alpha^n \in k$. If we put $L = k(\alpha)$, then $\alpha \otimes 1 - 1 \otimes \alpha \neq 0$ in $L \otimes_k L$ since the elements $(\alpha^i \otimes \alpha^j)_{0 \leq i,j \leq p-1}$ form a basis of $L \otimes_k L$ as a k-vector space, but

$$(\alpha \otimes 1 - 1 \otimes \alpha)^p = \alpha^p \otimes 1 - 1 \otimes \alpha^p = 1 \otimes \alpha^p - 1 \otimes \alpha^p = 0.$$

We now consider more generally finitely generated reduced k-algebras when k is not necessarily closed.

Example 3.4. Let $A = \mathbb{R}[X]/(x^2+1)$. Since x^2+1 is irreducible in $\mathbb{R}[x]$, it generates a maximal ideal, thus the finitely-generated $\mathbb{R}$-algebra A is a field and in particular reduced. We can equip the topogical space $X \coloneqq \operatorname{Spm} A = \{(0)\}$ with a sheaf of regular functions, defined by $\mathcal{O}_X(\{(0)\}) = A$. In other words, $\operatorname{Spm} A$ is just a point, but equipped with the reduced $\mathbb{R}$-algebra A. It thus differs from the point $\operatorname{Spm} \mathbb{R}$, which is equipped with the reduced $\mathbb{R}$-algebra $\mathbb{R}$, since $\mathbb{R}[x]/(x^2+1) \not\simeq \mathbb{R}$ as $\mathbb{R}$-algebras. Indeed, the $\mathbb{R}$-algebra $\mathbb{R}[x]/(x^2+1)$ is 2 dimensional as a real vector space.

A possesses a non-trivial $\mathbb{R}$-algebra automorphism induced by the automorphism of $\mathbb{R}$-algebras, $P \mapsto P(-x)$ in $\mathbb{R}[x]$. Indeed, $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ as $\mathbb{R}$-algebras, with the previous automorphism corresponding to the complex conjugation $z \mapsto \overline{z}$.

Example 3.5. By analogy with the Zariski topology on maximal spectra of (finitely generated, reduced) $\mathbb{C}$-algebras, we can equip $X = \operatorname{Spm} A$ with a Zariski topology for all (finitely generated reduced) $\mathbb{R}$-algebras A: the closed subsets of this topology are given by

$$\mathcal{V}_X(I) \coloneqq \{\mathfrak{m} \in \operatorname{Spm} A \mid \mathfrak{m} \supset I\}$$

for any ideal $I \subseteq A$. Note that $X = \operatorname{Spm} A$ contains $\hat{A} = \operatorname{Hom}_{k\text{-alg}}(A, k)$ as a subset: the points of $\hat{A}$ correspond to maximal ideals $\mathfrak{m}$ of A with residue field $A/\mathfrak{m} \simeq k$. But when $k \not\simeq \overline{k}$, the set $\operatorname{Spm} A$ is strictly larger than $\hat{A}$: it contains maximal ideals $\mathfrak{m}$ such that $A/\mathfrak{m}$ is a non-trivial finite extension of k. The induced topology on $\hat{A} \subseteq \operatorname{Spm} A$ is the Zariski topologoy of $\hat{A}$ that was introduced earlier.

Let $A = \mathbb{R}[x]$. Maximal ideals in the principal ring $\mathbb{R}[x]$ are generated by a single irreducible polynomial P, which is either of degree 1 or of degree 2 with negative discriminant.

In the first case, $P = x - a$ for some $a \in \mathbb{R}$ and the residue field is $\mathbb{R}[x]/(x-a) \simeq \mathbb{R}$, while, in the second case, $P = x^2 + bx + c$ for $b, c \in \mathbb{R}$ and $b^2 - 4c < 0$ and by choosing a root z_0 of P in $\mathbb{C}$, the map

$$\begin{aligned}\eta_{z_0} \colon \mathbb{R}[x]/(x^2+bx+c) &\longrightarrow \mathbb{C} \\ \overline{P} &\longmapsto P(z_0)\end{aligned}$$

is a field-homomorphism. In particular it is injective. Since $\mathbb{C}$ and $\mathbb{R}[x]/(x^2+bx+c)$ are both degree 2 extensions of $\mathbb{R}$, we have $\mathbb{R}[x]/(x^2+bx+c) \simeq \mathbb{C}$. Note that the other root of x^2+bx+c is $\overline{z_0}$ and that $\eta_{\overline{z_0}} = \sigma \circ \eta_{z_0}$ where σ is complex conjugation on $\mathbb{C}$. So we have to ways to identify $\mathbb{R}[x]/(x^2+bx+c)$ to $\mathbb{C}$ and they are related by the action of $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ on $\mathbb{C}$.

To sum up, the difference between the two possible types of maximal ideals $\mathfrak{m} \subseteq \mathbb{R}[x]$ is the residue field, which is either $\mathbb{R}$ or $\mathbb{C}$. When it is $\mathbb{R}$, we find exactly the points of

$$\begin{aligned}\widehat{\mathbb{R}[x]} &= \mathrm{Hom}_{\mathbb{R}\text{-alg}}(\mathbb{R}[x], \mathbb{R}) \\ &\simeq \{\mathfrak{m} \in \operatorname{Spm} \mathbb{R}[x] \mid \mathbb{R}[x]/\mathfrak{m} \simeq \mathbb{R}\} \\ &\simeq \{(x-a) \colon a \in \mathbb{R}\} \\ &\simeq \mathbb{R}.\end{aligned}$$

And when the residue field is $\mathbb{C}$, we have $\mathfrak{m} = (x^2 + bx + c)$ with $b, c \in \mathbb{R}$ such that $b^2 - 4c < 0$. If we choose z_0 to be the root of $x^2 + bx + c$ with $\mathrm{Im}(z_0) > 0$, we can identify the set of these maximal ideals with the subset

$$H \coloneqq \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}.$$

In other words, the following pictures emerges, where we identify $\operatorname{Spm} \mathbb{R}[x]$ with

$$\hat{H} \coloneqq \{z \in \mathbb{C} \mid \mathrm{Im}(z) \geq 0\}$$

via the map

$$\begin{aligned}\operatorname{Spm} \mathbb{R}[x] &\longrightarrow \hat{H} \\ \mathfrak{m} &\longmapsto \begin{cases} a \in \mathbb{R} & \mathfrak{m} = (x-a) \\ z_0 \in H & \mathfrak{m} = ((x-z_0)(x-\overline{z_0})) \text{ and } \mathrm{Im}(z_0) > 0 \end{cases}\end{aligned}$$

which is indeed bijective. We see that $\operatorname{Spm} \mathbb{R}[x]$ contains a lot more points that $\mathbb{R}$. One could go further and add the ideal (0): This would give the set

$$\mathbb{A}^1_{\mathbb{R}} = \operatorname{Spec} \mathbb{R}[x] = \operatorname{Spm} \mathbb{R}[x] \cup \{(0)\}.$$

Remark 3.6. If A is a k-algebra and $\overline{k}$ is an algebraic closure of k, the group $\mathrm{Aut}_k(\overline{k})$ acts on the $\overline{k}$-algebra $A_{\overline{k}} \coloneqq A \otimes_k \overline{k}$ via $\sigma(a \otimes \lambda) \coloneqq a \otimes \sigma(\lambda)$. Moreover, the map $a \mapsto a \otimes 1$ induces an injective morphism of k-algebras $A \hookrightarrow A \otimes_k \overline{k}$ since the tensor product over fields is left-exact. Its image is contained in the k-subalgebra $\mathrm{Fix}_{\mathrm{Aut}_k(\overline{k})} A_{\overline{k}} \subseteq A_{\overline{k}}$. When k is a perfect field, this inclusion is an equality.

Example 3.7. If $A = \mathbb{R}[x]$, then $A \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}[x]$. The group $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \sigma \rangle$ with $\sigma \colon z \mapsto \overline{z}$, acts naturally on $\mathbb{C}[x]$. This is an action by $\mathbb{R}$-algebra automorphisms. Clearly, $\mathrm{Fix}_{\langle \sigma \rangle} \mathbb{C}[x] = \mathbb{R}[x]$. There is an induced action on $\operatorname{Spm} \mathbb{C}[x]$, defined by

$$\sigma(\mathfrak{m}) = \sigma((x-z)) \coloneqq (x - \sigma(z)) = (x - \overline{z}).$$

When we identify $\operatorname{Spm} \mathbb{C}[x]$ with $\mathbb{C}$ via $(x-z) \mapsto z$, this action is just $z \mapsto \overline{z}$. This „geometric action" induces an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on regular functions on $\mathbb{C}$: to $h \in \mathcal{O}_{\mathbb{C}}(U)$, there is associated a regular function $h \in \mathcal{O}_{\mathbb{C}}(\sigma(U))$, defined for all $x \in \sigma(U)$, by

$$\sigma(h)(z) \coloneqq \sigma \circ h \circ \sigma^{-1}(z) = \overline{h(\overline{z})}.$$

In particular, if $h = P \in \mathcal{O}_{\mathbb{C}}(\mathbb{C}) = \mathbb{C}[x]$, then $P \mapsto \sigma(P)$ coincides with the natural $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ action on $\mathbb{C}[x]$. We will see momentarily that this defines a sheaf of $\mathbb{R}$-algebras on $\operatorname{Spm} \mathbb{R}[x]$. To that end, let us first look more closely at the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ action on $\operatorname{Spm} \mathbb{C}[x]$. Its fixed-point set is

$$\{\mathfrak{m} \in \operatorname{Spm} \mathbb{C}[x] \mid \mathfrak{m} = (x-a), a \in \mathbb{R}\} \simeq \mathbb{R} = \mathrm{Fix}_{z \mapsto \overline{z}}(\mathbb{C}).$$

Moreover, there is a map

$$\begin{aligned}\operatorname{Spm} \mathbb{C}[x] &\longrightarrow \operatorname{Spm} \mathbb{R}[x] \\ \mathfrak{m} &\longmapsto \mathfrak{m} \cap \mathbb{R}[x]\end{aligned}$$

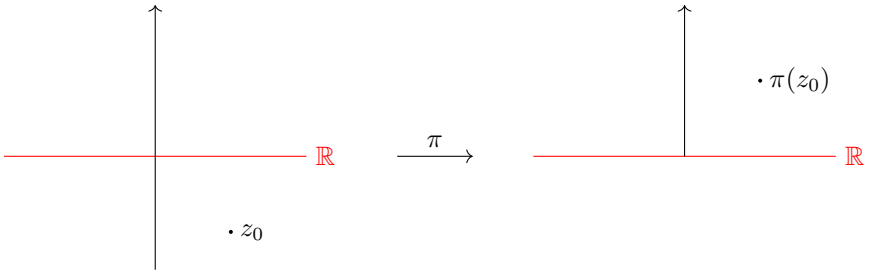


Figure 3.1: The quotient map $\pi\colon \operatorname{Spm}\mathbb{C}[x] \to \operatorname{Spm}\mathbb{R}[x]$ is geometrically a folding.

sending $(x-a)\mathbb{C}[x]$ to $(x-a)\mathbb{R}[x]$ if $a \in \mathbb{R}$, and $(x-z)\mathbb{C}[x]$ to $(x-z)(x-\overline{z})\mathbb{R}[x]$ if $z \in \mathbb{C}\setminus\mathbb{R}$. This map is surjective and induces a bijection

$$(\operatorname{Spm}\mathbb{C}[x])/\operatorname{Gal}(\mathbb{C}/\mathbb{R}) \xrightarrow{\simeq} \operatorname{Spm}\mathbb{R}[x].$$

Geometrically, the quotient map $\pi\colon \operatorname{Spm}\mathbb{C}[x] \to \operatorname{Spm}\mathbb{R}[x]$ is the „folding map“

$$\begin{aligned} \mathbb{C} &\longrightarrow \hat{H} \\ z = u + iv &\longmapsto u + i|v|. \end{aligned}$$

In view of this, it is natural to

(i) put the quotient topology on

$$\operatorname{Spm}\mathbb{R}[x] = (\operatorname{Spm}\mathbb{C}[x]) \,/\, \operatorname{Gal}(\mathbb{C}/\mathbb{R})$$

where $\operatorname{Spm}\mathbb{C}[x] \simeq \mathbb{C}$ is equipped with its topology of algebraic variety.

(ii) define a sheaf of $\mathbb{R}$-algebras on $\operatorname{Spm}\mathbb{R}[x]$ by pushing-forward the structure sheaf on $\operatorname{Spm}\mathbb{C}[x]$ and then taking the $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-invariant subsheaf:

$$\mathcal{O}_{\operatorname{Spm}\mathbb{R}[x]}(U) \coloneqq \mathcal{O}_{\operatorname{Spm}\mathbb{C}[x]}(\pi^{-1}(U))^{\operatorname{Gal}(\mathbb{C}/\mathbb{R})}$$

where $\pi\colon \operatorname{Spm}\mathbb{C}[x] \to \operatorname{Spm}\mathbb{R}[x]$, $\mathfrak{m} \mapsto \mathfrak{m} \cap \mathbb{R}[x]$ is the quotient map, and $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ acts on $\mathcal{O}_{\operatorname{Spm}\mathbb{C}[x]}(\pi^{-1}(U))$ via $h \mapsto \sigma(h) = \sigma \circ h \circ \sigma^{-1}$ (note that the open set $\pi^{-1}(U)$ is $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-invariant).

Observe that

$$\mathcal{O}_{\operatorname{Spm}\mathbb{R}[x]}(\operatorname{Spm}\mathbb{R}[x]) = \mathbb{C}[x]^{\operatorname{Gal}(\mathbb{C}/\mathbb{R})} = \mathbb{R}[x].$$

Also, if $h = \frac{f}{g}$ around $x \in U$, then, around $\sigma(x) \in U$, one has $\sigma(h) = \frac{\sigma(f)}{\sigma(g)}$ and, for all $\lambda \in \mathbb{C}$, $\sigma(\lambda h) = \overline{\lambda}\sigma(h)$.

Remarkably, we will see that we can reconstruct the algebraic $\mathbb{C}$-variety

$$(X_{\mathbb{C}}, \mathcal{O}_{X_{\mathbb{C}}}) \coloneqq (\operatorname{Spm}\mathbb{C}[x], \mathcal{O}_{\operatorname{Spm}\mathbb{C}[x]})$$

from the ringed space

$$(X, \mathcal{O}_X) \coloneqq (\operatorname{Spm}\mathbb{R}[x], \mathcal{O}_{\operatorname{Spm}\mathbb{R}[x]}$$

that we have just constructed.

Chapter 4

Real algebra

4.1 Ordered fields and real fields

Definition 4.1. An *ordered field* is a pair $(k, \leq)$ consisting of a field k and an order relation $\leq$ such that

(i) $\leq$ is a total order: if $x, y \in k$, then $x \leq y$ or $y \leq x$.

(ii) $\leq$ is compatible with addition in k: if $x, y, z \in k$, then $x \leq y$ implies $x + z \leq y + z$.

(iii) $\leq$ is compatible with multiplication in k: if $x, y \in k$, then $0 \leq x$ and $0 \leq y$ implies $0 \leq xy$.

A morphism between two ordered fields $(k, \leq)$ and $(L, \leq)$ is a field homomorphism $\varphi\colon k \to L$ such that $x \leq y$ in k implies $\varphi(x) \leq \varphi(y)$ in L.

Example 4.2. (1) The fields $\mathbb{Q}$ and $\mathbb{R}$, equipped with their usual orderings, are ordered fields.

(2) The field $\mathbb{C}$ can be equipped with a total ordering (the „lexicographic order“) but not with a structure of ordered field.

(3) The field $\mathbb{R}(t)$ of rational fractions with coefficients in $\mathbb{R}$, can be equipped with a structure of ordered field in multiple ways:

Fix an $x \in \mathbb{R}$ and, for all polynomial $P \in \mathbb{R}[t]$, use Taylor expansion at x to write

$$P(t) = a_p(t - x)^p + \text{higher order terms.}$$

with $a_p \neq 0$, then define $P(t) >_{x^+} 0$ if $a_p > 0$, i.e. if the function $t \mapsto P(t)$ is positive on a small interval $(x, x + \varepsilon)$. Set also $\frac{P(t)}{Q(t)} >_{x^+} 0$ if $P(t)Q(t) >_{x^+} 0$, and define $f \leq_{x^+} g$ in $\mathbb{R}(t)$ if either $f = g$ or $g - f >_{x^+} 0$. Equivalently $f \leq_{x^+} g$ in $\mathbb{R}(t)$ if either $f = g$ or $g - f$ is positively-valued on $(x, x + \varepsilon)$ for $\varepsilon > 0$ small enough.

It is clear that this is a total ordering on $\mathbb{R}(t)$, and that this ordering is compatible with addition and multiplication in the sense of the definition of an ordered field. Moreover, the substitution homomorphism $h(t) \mapsto h(t - x)$ induces an isomorphism of ordered fields $(\mathbb{R}(t), \leq_{0^+}) \xrightarrow{\simeq} (\mathbb{R}(t), \leq_{x^+})$, since a function $t \mapsto h(t - x)$ is positively-valued on $(x, x + \varepsilon)$ if and only if the function $t \mapsto h(t)$ is positively valued on $(0, \varepsilon)$.

Note that we can also define orderings on $\mathbb{R}(t)$ by setting $f \leq_{x^-} g$ if either $f = g$ or $g - f$ is positively-valued on $(x - \varepsilon, x)$, for $\varepsilon > 0$ small enough. The substitution homomorphism $h(t) \mapsto h(-t)$ induces an isomorphism of ordered fields $(\mathbb{R}(t), \leq_{0^-}) \xrightarrow{\simeq} (\mathbb{R}(t), \leq_{0^+})$.

Remark 4.3. The ordered field $(\mathbb{R}(t), \leq_{0^+})$ is non-Archimedean: the element t is *infinitely small with respect to any real* $\delta > 0$ in the sense that for all $n \in \mathbb{N}$, $nt < \delta$ (indeed $t \mapsto nt - \delta$ is negatively-valued on $(0, \varepsilon)$ for $\varepsilon > 0$ small enough). Equivalently, $\frac{1}{t}$ is infinitely large with respect to $0 < \delta \in \mathbb{R}$ in the sense that $\frac{1}{t} > n\delta$ for all $n \in \mathbb{N}$.

Proposition 4.4. *Let $(k, \leq)$ be an ordered field and $x, y, z \in k$. Then the following properties hold:*

(a) $x \geq 0$ *or* $-x \geq 0$.

(b) $-1 < 0$ *and* $1 > 0$.

(c) k *is of characteristic* 0.

(d) if $x < y$ *and* $z > 0$, *then* $xz < yz$.

(e) if $x < y$ *and* $z < 0$, *then* $xz > yz$.

(f) $xy \geq 0$ *if and only if* x *and* y *have the same sign.*

(g) $x^2 \geq 0$ *and, if* $x \neq 0$, *then* x *and* $\frac{1}{x}$ *have the same sign.*

(h) if $0 < x \leq y$, *then* $0 < \frac{1}{y} \leq \frac{1}{x}$.

Proof. Elementary verifications. □

It turns out that it is possible to characterise ordered fields without explicitly mentioning the order relation, using cones of positive elements.

Definition 4.5. Let k be a field. A *cone* in k is a subset $P \subseteq k$ such that for all $x, y \in P$ and $z \in k$:

(i) $x + y \in P$

(ii) $xy \in P$

(iii) $z^2 \in P$

A cone $P \subseteq k$ is called a *positive cone* if, additionally, one has:

(iv) $-1 \notin P$

Proposition 4.6. *Let k be a field. Assume that there exists a positive cone $P \subseteq k$. Then:*

(i) $0 \in P$ *and* $1 \in P$.

(ii) k *is of characteristic* 0.

(iii) $P \cap (-P) = \{0\}$

Proof. (i) $0 = 0^2 \in P$ and $1 = 1^2 \in P$ by axiom (iii).

(ii) Since $1 \in P$, by induction and axiom (i), $n \cdot 1 = \underbrace{1 + \ldots + 1}_{n \text{ times}} \in P$ for all $n \in \mathbb{N}$. Assume that there exists $n \in \mathbb{N}$, such that $n \cdot 1 = 0$ in k. Since $1 \neq 0$ in k, it follows $n \geq 2$ so,

$$-1 = 0 - 1 = n \cdot 1 - 1 = (n-1) \cdot 1 \in P,$$

which contradicts axiom (iv).

(iii) Assume that there exists $x \in P \cap (-P) \setminus \{0\}$. In particular $x \neq 0$ and $-x \in P$. So $-x^2 = (-x)x \in P$ by axiom (ii) and $\frac{1}{x^2} = \left(\frac{1}{x}\right)^2 \in P$ by axiom (iii). Again by axiom (ii)

$$-1 = \frac{1}{x^2}(-x^2) \in P$$

which contradicts axiom (iv).

□

Given a positive cone P in a field k, let us set $P^+ = P \setminus \{0\}$ and $P^- = (-P) \setminus \{0\} = -P^+$. Then we have a disjoint union

$$P^- \sqcup \{0\} \sqcup P^+ \subseteq k.$$

Note that P^+ satisfies axioms (i) and (ii) of the definition of a cone, as well as the property that $x \in k \setminus \{0\} \implies x^2 \in P^+$.

We now prove that positive curves can be enlarged, that the resulting notion of maximal positive cone satisfies $P \cup (-P) = k$, and that this defines a structure of ordered field on k by setting $x \leq y$ if and only if $y - x \in P$.

Lemma 4.7. *Assume that P is a positive cone in a field k. If $a \in k \setminus P \cup (-P)$, then the set*

$$P[a] \coloneqq \{x + ay \in k \colon x, y \in P\}$$

is a positive cone in k, satisfying $P \subsetneq P[a]$.

Proof. Let $x, y, x', y' \in P$. Then

$$(x + ay) + (x' + ay') = x + x' + a(y + y') \in P[a]$$

and

$$(x + ay)(x' + ay') = xx' + a^2yy' + a(xy' + x'y) \in P[a].$$

Moreover $z^2 \in P \subseteq P[a]$ for all $z \in k$.

Now assume $-1 = x + ay$ for some $x, y \in P$. If $y = 0$, then $-1 = x \in P$ which is a contradiction. Thus $y \neq 0$ and

$$-a = \frac{1 + x}{y} = \left(\frac{1}{y}\right)^2 y(1 + x) \in P,$$

which contradicts the assumption on a. Finally, we have $P \subseteq P[a]$ and, if $P[a] \subseteq P$ then $a \in P$, again contradicting the assumption on a. So $P \subsetneq P[a]$. □

Proposition 4.8. *Let $\mathcal{P}$ be the set of positive cones of a field k ordered by inclusion. If $\mathcal{P} \neq \emptyset$, then $\mathcal{P}$ admits a maximal element and such an element P satisfies $P \cup (-P) = k$.*

Proof. To obtain a maximal element of $\mathcal{P}$, by Zorn's lemma, it suffices to show, that every chain $(P_i)_{i \in I}$ in $\mathcal{P}$ has an upper bound. We set

$$P = \bigcup_{i \in I} P_i \subseteq k.$$

One verifies immediately that P is a positive cone and an upper bound of the chain $(P_i)_{i \in I}$.

Let P be such a maximal element. If there exists $a \in k \setminus P \cup (-P)$, then by 4.7 $P \subsetneq P[a]$ contradicts the maximality of P. Thus $P \cup (-P) = k$. □

Proposition 4.9. *Let k be a field and denote by*

$$\Sigma k^{[2]} \coloneqq \left\{ y \in k \mid \exists (a_x)_{x \in k} \in \{0, 1\}^{(k)}, y = \sum_{x \in k} a_x x^2 \right\}$$

the set of sums of squares in k. Then $\Sigma k^{[2]}$ is a cone and $-1 \notin \Sigma k^{[2]}$ if and only if for all $x_1, \ldots, x_n \in k$:

$$x_1^2 + \ldots + x_n^2 = 0 \implies x_1 = \ldots = x_n = 0.$$

Proof. One verifies immediately that $\Sigma k^{[2]}$ is a cone in k. If $-1 \in \Sigma k^{[2]}$, then $-1 = x_1^2 + \ldots + x_n^2$ for some $x_i \in k$. Thus

$$0 = \sum_{i=1}^{n} x_i^2 + 1$$

but $1 = 1^2$ and $1 \neq 0$. Conversely let $0 = \sum_{i=1}^{n} x_i^2$ with $x_1 \neq 0$. Then

$$-1 = \frac{1}{x_1^2} \sum_{i=2}^{n} x_i^2 = \sum_{i=2}^{n} \left(\frac{x_i}{x_1} \right)^2 \in \Sigma k^{[2]}.$$

□

Definition 4.10. A field k is called a *real field* if $-1 \notin \Sigma k^{[2]}$, or equivalently if $\sum_{k=1}^{n} x_i^2 = 0$ in k implies $x_k = 0$ for all k.

Corollary 4.11. *Let k be a field. k is real if and only if k contains a positive cone.*

Proof. ($\Rightarrow$): By 4.9 $\Sigma k^{[2]}$ is a positive cone. ($\Leftarrow$): Let P be a positive cone. Since P is closed under addition and for all $z \in k$: $z^2 \in P$, $\Sigma k^{[2]} \subset P$. Since P is positive, $-1 \notin \Sigma k^{[2]}$. □

Proposition 4.12. *Let $(k, \leq)$ be an ordered field. Then the set*

$$P \coloneqq \{x \in k \mid x \geq 0\}$$

is a maximal positive cone in k. In particular, k is a real field. Conversely, if k is a real field and P is a maximal positive cone in k, then the relation $x \leq_P y$ if $y - x \in P$ is an order relation and $(k, \leq_P)$ is an ordered field.

Proof. ($\Rightarrow$): Let $(k, \leq)$ be an ordered field. Then by definition and 4.4, P is a maximal positive cone.

($\Leftarrow$): Let P be a maximal positive cone in k. Since $0 \in P$, we have $x \leq_P x$. Suppose that $x \leq_P y$ and $y \leq_P x$. Then $y - x \in P \cap (-P) = \{0\}$, so $x = y$. Moreover, if $x \leq_P y$ and $y \leq_P z$, then $z - x = (z - y) + (y - x) \in P$. Thus $x \leq_P z$, hence $\leq_P$ is an order relation. Moreover, it is a total order, because if $x, y \in k$, then $y - x \in k = P \cup (-P)$, so either $x \leq_P y$ or $y \leq_P x$.

Finally, this total order on k is compatible with addition and multiplication because $x \leq_P y$ and $z \in k$ implies $(y + z) - (x + z) = y - x \in P$, so $x + z \leq_P y + z$, and $x \geq_P 0$, $y \geq_P 0$ means that $x \in P$ and $y \in P$, so $xy \in P$, hence $xy \geq_P 0$. □

Corollary 4.13. *Let k be a field. Then k admits a structure of ordered field if and only if k is real.*

4.2 Real-closed fields

In this section we study real algebraic extensions of real fields.

Lemma 4.14. *Let k be a real field and $x \in k \setminus \{0\}$. Then x and $-x$ cannot be both sums of squares in k.*

Proof. If $x \in \Sigma k^{[2]}$ and $-x \in \Sigma k^{[2]}$, then

$$1 = \frac{1}{x^2}(-x)x \in \Sigma k^{[2]}$$

contradicting that k is real. □

Proposition 4.15. *Let k be a real field and $a \in k$ such that a is not a square in k. Then the field*

$$k(\sqrt{a}) = k[t]/(t^2 - a)$$

is real if and only if $-a \notin \Sigma k^{[2]}$. In particular, if $\Sigma k^{[2]} \cup (-\Sigma k^{[2]}) \neq k$, then k admits real quadratic extensions.

Proof. Since a is not a square in k, $t^2 - a$ is irreducible in $k[t]$, so $k[t]/(t^2 - a)$ is indeed a field. Denote by $\sqrt{a}$ the class of t in the quotient.

($\Rightarrow$): a is a square in $k(\sqrt{a})$, thus by 4.14 we have $-a \notin \Sigma k(\sqrt{a})^2$. But $\Sigma k^{[2]} \subseteq \Sigma k(\sqrt{a})^{[2]}$, thus $-a \notin \Sigma k(\sqrt{a})^{[2]}$.

($\Leftarrow$): $-1 \in \Sigma k(\sqrt{a})^{[2]}$ if and only if there exist $x_i, y_i \in k$, such that

$$-1 = \sum_{i=1}^{n} (x_i + y_i\sqrt{a})^2 = \sum_{i=1}^{n} (x_i^2 + a y_i^2) + 2\sqrt{a} \sum_{i=1}^{n} x_i y_i.$$

Since $(1, \sqrt{a})$ is a basis of the k-vector space $k(\sqrt{a})$, the previous equality implies

$$-1 = \sum_{i=1}^{n} x_i^2 + a \sum_{i=1}^{n} y_i^2.$$

Since $-1 \notin \Sigma k^{[2]}$, $\sum_{i=1}^{n} y_i^2 \neq 0$, this implies

$$-a = \frac{1 + \sum_{i=1}^{n} x_i^2}{\sum_{i=1}^{n} y_i^2} = \frac{\left(\sum_{i=1}^{n} y_i^2\right)\left(1 + \sum_{i=1}^{n} x_i^2\right)}{\left(\sum_{i=1}^{n} y_i^2\right)^2} \in \Sigma k^{[2]}.$$

□

Simple extensions of odd degree are simpler from the real point of view:

Proposition 4.16. *Let k be a real field and $P \in k[t]$ be an irreducible polynomial of odd degree. Then the field $k[t]/(P)$ is real.*

Proof. Denote by n the degree of P. We proceed by induction on $n \geq 1$. If $n = 1$, then $k[t]/(P) \simeq k$ is real. Since n is odd, we may now assume $n \geq 3$. Let $L \coloneqq k[t]/(P)$. Suppose L is not real. Then there exist polynomials $g_i \in k[t]$, of degree at most $n-1$, such that $-1 = \sum_{i=1}^{m} g_i^2$ in $L = k[t]/(P)$. Since $k \subseteq L$ and k is real, at least one of the g_i is non-constant. By definition of L, there exists $Q \in k[t] \setminus \{0\}$ such that

$$-1 = \sum_{i=1}^{m} g_i^2 + PQ \tag{4.1}$$

in $k[t]$. Since k is real, in $\sum_{i=1}^{m} g_i^2$ no cancellations of the terms of highest degree can occur. Thus $\sum_{i=1}^{m} g_i^2$ is of positive, even degree at most $2n - 2$. By 4.1, it follows that Q is of odd degree at most $n - 2$. In particular, Q has at least one irreducible factor Q_1 of odd degree at most $n - 2$. Since $n \geq 3$, $n - 2 \geq 1$. By induction, $M \coloneqq k[t]/(Q_1)$ is real. But 4.1 implies

$$-1 = \sum_{i=1}^{m} g_i^2$$

in $M = k[t]/(Q_1)$ contradicting the fact that M is real. □

Definition 4.17. A *real-closed* field is a real field that has no proper real algebraic extensions.

Theorem 4.18. *Let k be a field. Then the following conditions are equivalent:*

(i) k is real-closed.

(ii) *k is real and for all $a \in k$, either a or $-a$ is a square in k and every polynomial of odd degree in $k[t]$ has a root in k.*

(iii) *the k-algebra*

$$k[i] := k[t]/(t^2+1)$$

is algebraically closed.

.

Proof. (i)⇒(ii): Let $a \in k$ such that neither a nor $-a$ is a square in k. Then by 4.15 and (i), $\pm a \in \Sigma k^{[2]}$ contradicting 4.14. Let $P \in k[t]$ be a polynomial of odd degree. P has at least one irreducible factor P_1 of odd degree. By 4.16, $k[t]/(P_1)$ is a real extension of k. Since k is real-closed, P_1 must be of degree 1 and thus P has a root in k.

(ii)⇒(iii): Since -1 is not a square in k, the polynomial t^2+1 is irreducible over k. Thus $L := k[t]/(t^2+1)$ is a field. Denote by i the image of t in L and for $x = a+ib \in L = k[i]$, denote by $\overline{x} = a - ib$. This extends to a ring homomorphism $L[t] \to L[t]$. Let $P \in L[t]$ be non-constant. It remains to show, that P has a root in L. We first reduce to the case $P \in k[t]$.

Assume every non-constant polynomial in $k[t]$ has a root in L. Let $P \in L[t]$. Then $P\overline{P} \in k[t]$ has a root $x \in L$, thus either $P(x) = 0$ or $\overline{P}(x) = 0$. In the first case, we are done. In the second case, we have $P(\overline{x}) = \overline{\overline{P}(x)} = \overline{0} = 0$, so $\overline{x}$ is a root of P in L.

Thus we may assume $P \in k[t]$. Write $d = \deg(P) = 2^m n$ with $2 \nmid n$. We proceed by induction on m. If $m = 0$, the result is true by (ii). Now assume $m > 0$. Fix an algebraic closure $\overline{k}$ of k. Since k is real, it is of characteristic 0, thus k is perfect and $\overline{k}/k$ is galois. Let $y_1, \dots, y_d$ be the roots of P in $\overline{k}$. Consider for all $r \in \mathbb{Z}$:

$$F_r := \prod_{1 \le p < q \le d} (t - (y_p + y_q) - r y_p y_q)) \in \overline{k}[t].$$

This polynomial with coefficients in $\overline{k}$ is invariant under permutation of $y_1, \dots, y_d$. Thus its coefficients lie in $\overline{k}^{\mathrm{Gal}(\overline{k}/k)} = k$. Moreover

$$\deg(F_r) = \binom{d}{2} = \frac{d(d-1)}{2} = 2^{m-1} n (2^m - 1).$$

with $n(2^m-1)$ odd. So the induction hypothesis applies and, for all $r \in \mathbb{Z}$, there is a pair $p < q$ in $\{1, \dots, d\}$ such that $(y_p + y_q) + r y_p y_q \in L$. Since $\mathbb{Z}$ is infinite, we can find a pair $p < q$ in $\{1, \dots, d\}$ for which there exists a pair $r \neq r'$ such that

$$\begin{aligned} (y_p + y_q) + r y_p y_q &\in L \\ \text{and } (y_p + y_q) + r' y_p y_q &\in L. \end{aligned}$$

By solving the system, we get $y_p + y_q \in L$ and $y_p y_q \in L$. But y_p, y_q are roots of the quadratic polynomial

$$t^2 - (y_p + y_q)t + y_p y_q \in L[t]$$

and since $i^2 = -1$, the roots of this polynomial lie in $L = k[i]$, by (ii) and the usual formulas

$$t_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

So P indeed has a root in $k[i]$, which finishes the induction.

(iii)⇒(i): Denote again by i the image in the algebraically closed field $k[t]/(t^2+1)$. We first show that $k^{[2]} = \Sigma k^{[2]}$. Let $a, b \in k$. Then $a + ib = (c + id)^2$ in $k[i]$ for some $c, d \in k$. Thus

$$a^2 + b^2 = (a+ib)(a-ib) = (c+id)^2(c-id)^2 = (c^2+d^2)^2.$$

By induction the claim follows. Since t^2+1 is irreducible, $-1 \notin k^{[2]} = \Sigma k^{[2]}$ and k is real.

Let L be a real algebraic extension of k. Since $k[i]$ is algebraically closed and contains k, there exists a k-homomorphism $L \hookrightarrow k[i]$. Since $[k[i] : k] = 2$, either $L = k$ or $L = k[i]$, but $k[i]$ is not real, since $i^2 = -1$ in $k[i]$. So $L = k$ and k is real-closed. □

Corollary 4.19. *A real-closed field k admits a canonical structure of ordered field, in which the cone of positive elements is exactly $k^{[2]}$, the set of squares in k.*

Proof. This was proven in the implication (i)⇒(ii) of 4.18. □

Example 4.20.

- $\mathbb{R}$ is a real-closed field, because $\mathbb{R}[i] = \mathbb{C}$ is algebraically closed.
- The field of real Puiseux series

$$\widehat{\mathbb{R}(t)} := \bigcup_{q>0} \mathbb{R}((t^{\frac{1}{q}})) = \left\{ \sum_{n=m}^{\infty} a_n t^{\frac{n}{q}} : m \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}, a_n \in \mathbb{R} \right\}$$

  is a real closed field because $\widehat{\mathbb{R}(t)}[i] = \widehat{\mathbb{R}[i][t]} = \widehat{\mathbb{C}[t]}$ is the field of complex Puiseux series, which is algebraically closed by the Newton-Puiseux theorem.

Remark 4.21. By 4.18, if k is a real-closed field, then the absolute galois group of k is

$$\mathrm{Gal}(\overline{k}/k) = \mathrm{Gal}(k[i]/k) \simeq \mathbb{Z}/2\mathbb{Z}.$$

The Artin-Schreier theorem shows that if $\overline{k}/k$ is a non-trivial extension of *finite* degree, then k is real-closed.

4.3 Extensions of ordered fields

If a field k admits a structure of ordered field, we will say that k is *orderable*. For an *ordered* field k, an extension L/k is called *oderable* if the field L is orderable such that the induced order on k coincides with the fixed order on k.

Definition 4.22. Let k be a field. A quadratic form $q\colon k^n \to k$ is called *isotropic* if there exists $x \in k \setminus \{0\}$ such that $q(x) = 0$. Otherwise, the quadratic form is called *anisotropic*.

Remark 4.23. Recall that, given a quadratic form q on a finite-dimensional k-vector space E, there always exists a basis of E in which $q(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_r x_r^2$, where $r = \mathrm{rg}(q) \leq n = \dim E$ and $a_1, \ldots, a_r \in k$. The form q is non-degenerate on E if and only if $r = \dim E$.

Example 4.24.

- A field k is real if and only if for all $n \in \mathbb{N}$, the form $x_1^2 + \ldots + x_n^2$ is anisotropic.
- A degenerate quadratic form is isotropic.
- If k is algebraically closed and $n \geq 2$, all quadratic forms on k^n are isotropic.
- If $(k, \leq)$ is an ordered field and $q(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$ with $a_i > 0$ for all i, then q and $-q$ are anisotropic on k^n.

Definition 4.25. Let k be a field and L an extension of k. A quadratic form $q\colon k^n \to k$ induces a quadratic form $q_L\colon L^n \to L$. The form q is called *anisotropic over L* if q_L is anisotropic.

It can be checked that, on an ordered field $(k, \leq)$, a quadratic form q is anisotropic if and only if it is non-degenerate and of constant sign. The interest of this notion for us is given by the following result.

Theorem 4.26. *Let $(k, \leq)$ be an ordered field and L be an extension of k. Then the following conditions are equivalent:*

(i) The extension L/k is orderable.

(ii) For all $n \geq 1$ and all $a = (a_1, \ldots, a_n) \in k^n$ such that $a_i > 0$ for all i, the quadratic form $q(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$ is anisotropic over L (i.e. all positive definite quadratic forms on k are anisotropic over L).

Proof. (i)⇒(ii): Assume that there is an ordering of L that extends the ordering of k and let $n \geq 1$. Let $a = (a_1, \ldots, a_n) \in k^n$ with $a_i > 0$ for all i. Then $a_i > 0$ still holds in L. Since squares are non-negative for all orderings, the sum $a_1x_1^2 + \ldots + a_nx_n^2$ is a sum of positive terms in L. Therefore it can only be 0, if all of its terms are 0. Since $a_i \neq 0$, it follows $x_i = 0$ for all i.

(ii)⇒(i): Define

$$P = \bigcup_{n\geq 1} \left\{ \sum_{i=1}^{n} a_i x_i^2 \colon a_i \in k, a_i > 0, x_i \in L \right\}.$$

The set P is stable by sum and product and contains all squares of L, so it is a cone in L. Suppose $-1 \in P$. Then there exists $n \geq 1$ and $a = (a_1, \ldots, a_n) \in k^n$ with $a_i > 0$ and $x = (x_1, \ldots, x_n) \in L^n$ such that $-1 = \sum_{i=1}^{n} a_i x_i^2$. So

$$a_1x_1^2 + \ldots + a_nx_n^2 + 1 = 0,$$

meaning that the quadratic form $a_1x_1^2 + \ldots + a_nx_n^2 + x_{n+1}^2$ is isotropic on L^{n+1}, contradicting (ii). Thus P is a positive cone containing all positive elements of k. By embedding P in a maximal positive cone, the claim follows. □

Proposition 4.27. *Let $(k, \leq)$ be an ordered field and let $c > 0$ be a positive element in k. Then $k[\sqrt{c}]$ is an orderable extension of k.*

Proof. If c is a square in k, there is nothing to prove. Otherwise, $k[\sqrt{c}]$ is indeed a field. Let $n \geq 1$ and let $a = (a_1, \ldots, a_n) \in k^n$ with $a_i > 0$ for all i. Assume that $x = (x_1, \ldots, x_n) \in k[\sqrt{c}]^n$ satisfies

$$a_1x_1^2 + \ldots + a_nx_n^2 = 0.$$

Since $x_i = u_i + v_i\sqrt{c}$ for some $u_i, v_i \in k$, we can rewrite this equation as

$$\sum_{i=1}^{n} a_i(u_i^2 + cv_i^2) + 2\sum_{i=1}^{n} u_iv_i\sqrt{c} = 0.$$

Since 1 and $\sqrt{c}$ are linearly independent over k, we get $\sum_{i=1}^{n} a_i(u_i^2 + cv_i^2) = 0$, hence $u_i = v_i = 0$ for all i, since all terms in the previous sum are non-negative. So $x_i = 0$ for all i and (ii) of 4.26 is satisfied. □

Proposition 4.28. *Let $(k, \leq)$ be an ordered field and let $P \in k[t]$ be an irreducible polynomial of odd degree. Then the field $L \coloneqq k[t]/(P)$ is an orderable extension of k.*

Proof. Denote by d the degree of P and proceed by induction on $d \geq 1$. If $d = 1$, then $L = k$. Now assume $d \geq 2$. Let $n \geq 1$ and $a_1, \ldots, a_n \in k$ with $a_i > 0$. Denote by q_L the quadratic form

$$q_L(x_1, \ldots, x_n) = a_1x_1^2 + \ldots + a_nx_n^2$$

on L^n. If q_L is isotropic over L, then there exist polynomials $g_1, \ldots, g_n \in k[t]$ with $\deg(g_i) < d$ and $h \in k[t]$ such that

$$q_L(g_1, \ldots, g_n) = hP \tag{4.2}$$

Let g be the greatest common divisor of $g_1, \ldots, g_n$. Since q_L is homogeneous of degree 2, g^2 divides $q_L(g_1, \ldots, g_n)$. Since P is irreducible, g divides h. We may thus assume that $g = 1$. The leading coefficients of the terms on the left hand side of (4.2) are non-negative, thus the sum has even degree $< 2d$. Since the degree of P is odd, h must be of odd degree $< d$. Therefore, h has an irreducible factor $h_1 \in k[t]$ of odd degree. Let α be a root of h_1. By evaluating (4.2) at α, we get

$$q_{k[\alpha]}(g_1(\alpha), \ldots, g_n(\alpha)) = 0$$

in $k[\alpha]$. Since the $gcd(g_1, \ldots, g_n) = 1$ and $k[t]$ is a principal ideal domain, there exist $h_1, \ldots, h_n \in k[t]$ such that

$$h_1g_1 + \ldots + h_ng_n = 1.$$

In particular

$$h_1(\alpha)g_1(\alpha) + \ldots + h_n(\alpha)g_n(\alpha) = 1,$$

so not all $g_i(\alpha)$ are 0 in $k[\alpha]$. Thus $q_{k[\alpha]}$ is isotropic over $k[\alpha] = k[t]/(h_1)$ contradicting the induction hypothesis. □

4.4 Counting real roots

In this section, we will study *Sturm's method* of counting the number of roots of a separable polynomial with coefficients in a real-closed field L.

Lemma 4.29. *Let $(k, \leq)$ be an ordered field and let $P \in k[t]$ be a separable polynomial. Assume that P has a root $a \in k$. Then there exists $\delta > 0$ such that*

(i) for $x \in]a - \delta, a + \delta[$ and $x \neq a$, $P(x) \neq 0$.

(ii) for $x \in]a, a + \delta[$, $P(x)$ and $P'(x)$ have the same sign.

(iii) for $x \in]a - \delta, a[$, $P(x)$ and $P'(x)$ have opposite signs.

(iv) for $x \in]0, \delta[$, $P(a + h)$ and $P(a - h)$ have opposite signs.

Proof. Since P is separable and $P(a) = 0$, it follows that $P'(a) \neq 0$. By continuity of P', there exists $\delta > 0$ such that P' has constant sign on $]a - \delta, a + \delta[$. Suppose $P'(x) > 0$. Since k is real-closed, this implies that P is strictly increasing on this interval. In particular, $P(x) < P(a) = 0$ for $x \in]a - \delta, a[$ and $P(x) > P(a) = 0$ for $x \in]a, a + \delta[$. The case $P'(x) < 0$ is similar which concludes the proof. □

Definition 4.30. Let $(k, \leq)$ be an ordered field. A finite sequence $(P_0, \ldots, P_n)$ of polynomials $P_i \in k[t]$ is called a *Sturm sequence* if it satisfies the following properties:

(i) $P_1 = P_0'$

(ii) for all $x \in k$ and $i \in \{0, \ldots, n\}$, if $P_i(x) = 0$, then $P_{i+1}(x) \neq 0$.

(iii) for all $x \in k$ and all $i \in \{1, \ldots, n-1\}$, if $P_i(x) = 0$ then $P_{i-1}(x)P_{i+1}(x) < 0$.

(iv) $P_n \in k^\times$.

If $P \in k[t]$ is separable and k has characteristic 0, then the greatest common divisor of P and P' is 1. To determine a Bézout relation between P and P', one proceeds by successive Euclidean divisions:

First set $P_0 = P$ and $P_1 = P'$, next define P_2 such that $P_0 = P_1Q_1 - P_2$ and $\deg(P_2) < \deg(P_1)$. Inductively, this defines $P_i = P_{i+1}Q_{i+1} - P_{i+2}$ with $\deg(P_{i+2}) < \deg(P_{i+1})$. This algorithm stops after at most $\deg(P_0)$ steps with $P_{n-1} = P_nQ_n$ and $P_n \neq 0$. Then P_n is a greatest common divisor of $P = P_0$ and $P' = P_1$. Since P and P' are coprime, P_n is a non-zero constant.

Corollary 4.31. *The sequence of polynomials $(P_0, \ldots, P_n)$ is a Sturm sequence. This is called the to P associated Sturm sequence.*

Proof. (i) and (iv) are clear. For (ii) observe that if there exists $x \in k$ and $i \in \{0, \ldots, n\}$ such that $P_i(x) = P_{i+1}(x) = 0$, then $P_j(x) = 0$ for all $j \geq i$ which contradicts $P_n(x) = P_n \neq 0$. Finally for (iii), if $P_i(x) = 0$, then $P_{i-1}(x) = -P_{i+1}(x)$, so $P_{i-1}(x)$ and $P_{i+1}(x)$ have opposite signs. □

Remark 4.32. Let $(k, \leq)$ be an ordered field. For a finite sequence of elements $(a_0, \ldots, a_n)$ in k with $a_0 \neq 0$, the number of *sign changes* in this sequence is the number of pairs (i, j) such that $i < j$, $a_i \neq 0$ and $a_ia_j < 0$ with either $j = i + 1$ or $j > i + 1$ and $a_{i+1} = \ldots = a_{j-1} = 0$.

Theorem 4.33 (Sturm's algorithm)**.** *Let k be a real-closed field equipped with its canonical ordering and let $P \in k[t]$ be a separable polynomial. Let $(P_0, \ldots, P_n)$ be the associated Sturm sequence. For all $a \in k$, we denote by $\nu(a)$ the number of sign changes in the sequence $(P_0(a), \ldots, P_n(a))$. Then, for all pair $a, b \in k$ such that $a < b$ and $P_i(a)P_i(b) \neq 0$ for all i, the number of roots of P in the interval $[a, b]$ is equal to $\nu(a) - \nu(b)$.*

Proof. Let $x_1 < \ldots < x_m$ be the elements of the finite set

$$E = \{x \in]a, b[\mid \exists i \in \{0, \ldots, n\}, P_i(x) = 0\}.$$

There exists a partition of $[a, b]$ in subintervals $[\alpha_j, \alpha_{j+1}]$ where $\alpha_0 = a$, $\alpha_m = b$, and for all $j \in \{0, \ldots, m-1\}$, $\alpha_j \notin E$, $[\alpha_j, \alpha_{j+1}] \cap E = \{x_j\}$. Also

$$\sum_{j=0}^{m-1} (\nu(\alpha_j) - \nu(\alpha_{j+1})) = \nu(\alpha_0) - \nu(\alpha_1) + \nu(\alpha_1) - \ldots - \nu(\alpha_m) = \nu(a) - \nu(b).$$

Thus it suffices to show that for fixed $j \in \{0, \ldots, m-1\}$, the number of roots of P in $[\alpha_j, \alpha_{j+1}]$ is equal to $\nu(\alpha_j) - \nu(\alpha_{j+1})$. By construction, P has at most one root in $[\alpha_j, \alpha_{j+1}]$, at x_j, thus we want to show

$$\nu(\alpha_j) - \nu(\alpha_{j+1}) = \begin{cases} 0 & P(x_j) \neq 0 \\ 1 & P(x_j) = 0 \end{cases}.$$

If $P(x_j) = 0$, then $P(\alpha_j)$ and $P(\alpha_{j+1})$ must have opposite sign. Indeed, by 4.29 $P(x_j + h)P(x_j - h) < 0$ for all $h > 0$ small enough, but P cannot change sign on $[\alpha_j, x_j - h]$ nor on $[x_j + h, \alpha_{j+1}]$, for otherwise the intermediate value theorem would imply the existence of a root $x \neq x_j$ in $[\alpha_j, \alpha_{j+1}]$. So $P(\alpha_j)P(\alpha_{j+1}) < 0$. If $P(\alpha_j) > 0$, then $P(\alpha_{j+1}) < 0$. With $P_1 = P'$ and 4.29, it follows that $P_1(x) < 0$ for x close to x_j. But P_1 cannot change sign in $[\alpha_j, \alpha_{j+1}]$, otherwise its root in that interval would be x_j. Since P is separable and $P_1 = P'$, this is impossible. Thus $P' < 0$ and P is strictly decreasing on $[\alpha_j, \alpha_{j+1}]$. So the sequence of signs in the sequence $(P_0(\alpha_j), P_1(\alpha_j), \ldots, P_n(\alpha_j))$ starts with $(+, -, \ldots)$ while the one at α_{j+1} starts with $(-, -, \ldots)$. Similarly, if $P(\alpha_j) < 0$, then the sequences are $(-, +, \ldots)$ and $(+, +, \ldots)$. In either case, there is one more sign change in the sequence corresponding to α_j, so $\nu(\alpha_j) - \nu(\alpha_{j+1}) = 1$.

Now suppose $P(x_j) \neq 0$. Observe that $P_0(\alpha_j)$ and $P_0(\alpha_{j+1})$ have the same sign, otherwise by the intermediate value theorem and the construction, $P_0(x_j) = 0$. Also a difference between $\nu(\alpha_j)$ and $\nu(\alpha_{j+1})$ only occurs if there exists $i \in \{0, \ldots, n-1\}$ such that $P_i(\alpha_j)P_i(\alpha_{j+1}) < 0$. In this case, again by the intermediate value theorem, we have $P_i(x_j) = 0$. By the definition of a Sturm sequence, we have $P_{i-1}(x_j)P_{i+1}(x_j) < 0$. If $P_{i-1}(x_j) < 0$ then $P_{i-1} < 0$ on $[\alpha_j, \alpha_{j+1}]$, because x_j is the only possible root for P_{i-1} in $[\alpha_j, \alpha_{j+1}]$, so P_{i-1} cannot change sign on that interval. Likewise, P_{i+1} has the same sign on $[\alpha_j, \alpha_{j+1}]$ as it does at x_j. Proceeding similarly when $P_{i-1}(x_j) > 0$, we arrive at the following possibilities for the sign sequences of $P_{i-1}(\alpha_j)P_i(\alpha_j)P_{i+1}(\alpha_j)$ and $P_{i-1}(\alpha_{j+1})P_i(\alpha_{j+1})P_{i+1}(\alpha_{j+1})$:

	$P_i(\alpha_j) < 0$	$P_i(\alpha_j) > 0$
$P_{i-1}(x_j) < 0$	$--+$	$-++$
$P_{i-1}(x_j) > 0$	$+--$	$++-$

(a) Sign sequence at α_j

	$P_i(\alpha_j) < 0$	$P_i(\alpha_j) > 0$
$P_{i-1}(x_j) < 0$	$-++$	$--+$
$P_{i-1}(x_j) > 0$	$++-$	$+--$

(b) Sign sequence at α_{j+1}

Since sign sequences located in cells of the two tables corresponding to the same case have the same number of sign changes, equal to 1, we see that $\nu(\alpha_j) - \nu(\alpha_{j+1}) = 0$. □

We deduce from the previous result, this important result:

Corollary 4.34. *Let $(k, \leq)$ be an ordered field and let L_1, L_2 be real-closed, orderable extensions of k. Let $P \in k[t]$ be an irreducible polynomial over k. Then P has the same number of roots in L_1 as it does in L_2.*

Proof. For a polynomial $Q = c_n t^n + c_{n-1} t^{n-1} + \ldots + c_0 \in k[t]$ with $c_n \neq 0$, the roots of Q in an ordered real-closed extension L of k are bounded by

$$M = 1 + \left|\frac{c_{n-1}}{c_n}\right|_L + \ldots + \left|\frac{c_0}{c_n}\right|_L = 1 + \left|\frac{c_{n-1}}{c_n}\right|_k + \ldots + \left|\frac{c_0}{c_n}\right|_k .$$

Note that M is independent from L. So given $P \in k[t]$ irreducible and the associated Sturm sequence $(P_0, P_1, \ldots, P_n)$, there exists $M \in k$ such that all roots of all P_i's in L are contained in the interval $[-M, M] \subseteq L$. Since $\operatorname{char} k = 0$, P is separable, by 4.33 the number of roots of P in $[-M, M] \subseteq L$ is equal to $\nu(-M) - \nu(M)$. Since $\pm M \in k$, all $P_i \in k[t]$ and the ordering of L extends the one of k, the number of sign changes $\nu(\pm M)$ in the sequences $(P_0(-M), P_1(-M), \ldots, P_n(-M))$ and $(P_0(M), P_1(M), \ldots, P_n(M))$ does not depend on L. □

Remark 4.35. (i) In particular, if $P \in k[t]$ is an arbitrary polynomial, then if P has a root in a real-closed extension L of k, then it has a root in all real-closed extensions of k.

A polynomial with coefficients in an ordered field $(k, \leq)$ might not have roots in any real-closed extensions of k.

(ii) There is a proof of Sturm's algorithm that does not require P to be separable. As a consequence 4.34 holds for all $P \in k[t]$, not only the irreducible ones.

4.5 Real closures

Proposition 4.36. *Let k be a real field. Then there exists a real-closed algebraic orderable extension k^r of k.*

Proof. Let $\overline{k}$ be an algebraic closure of k and E be the set of intermediate extensions $k \subseteq L \subseteq \overline{k}$ such that L is real and algebraic over k. $E \neq \emptyset$ since $k \in E$. Define $L_1 < L_2$ on E if and only if $L_1 \subseteq L_2$ and L_2/L_1 is ordered, i.e. the order relation on L_1 coincides with the on induced by L_2. Then every totally ordered familiy $(E_i)_{i \in I}$ has an upper bound, namely $\bigcup_{i \in I} E_i$. By Zorn, E has a maximal element, which we denote by k^r and which is an algebraic extension of k. Such a k^r is real-closed, because otherwise it would admit a proper real algebraic extension contradicting the maximality of k^r as a real algebraic extension of k. □

Definition 4.37. A real-closed real algebraic extension of a real field k is called a *real closure* of k.

Remark 4.38. By the construction in the proof of 4.36, a real closure of a real field k can be chosen as a subfield k^r of an algebraic closure of $\overline{k}$. Since $k^r[i]$ is algebraically closed and algebraic over k^r, so also over k, it follows $k^r[i] = \overline{k}$.

Proposition 4.39. *Let k be a real field and L be a real-closed extension of k. Let $\overline{k}^L$ be the relative algebraic closure of k in L, i.e.*

$$\overline{k}^L = \{x \in L \mid x \text{ algebraic over } k\}.$$

Then $\overline{k}^L$ is a real closure of k.

Proof. It is immediate that $\overline{k}^L$ is a real algebraic extension of k. Let $x \in \overline{k}^L$. Then x or $-x$ is a square in L, since L is real-closed. Without loss of generality, assume that $x \in L^{[2]}$. Then $t^2 - x \in \overline{k}^L[t]$ has a root in L. Since this root is algebraic over $\overline{k}^L$, hence over k, it belongs to $\overline{k}^L$. Thus x is in fact a square in $\overline{k}^L$. By the same argument every polynomial of odd degree has a root in $\overline{k}^L$. □

Example 4.40. (i) $\overline{\mathbb{Q}}^{\mathbb{R}} = \overline{\mathbb{Q}}^{\mathbb{C}} \cap \mathbb{R}$ is a real closure of $\mathbb{Q}$. In particular, $\overline{\mathbb{Q}}^{\mathbb{C}} = \overline{\mathbb{Q}}^{\mathbb{R}}[i]$ as subfields of $\mathbb{C}$.

(ii) Consider the real field $k = \mathbb{R}(t)$ and the real-closed extension

$$\widehat{\mathbb{R}(t)} = \bigcup_{q>0} \mathbb{R}((t^{1/q})).$$

Then the subfield $\overline{\mathbb{R}(t)}^{\widehat{\mathbb{R}(t)}}$, consisting of all those real Puiseux series that are algebraic over $\mathbb{R}(t)$, is a real closure of $\mathbb{R}(t)$.

The field of real Puiseux series itself is a real closure of the field $\mathbb{R}((t))$ of real formal Laurent series.

Lemma 4.41. *Let L_1, L_2 be real-closed fields and let $\varphi\colon L_1 \to L_2$ be a homomorphism of fields. Then φ is compatible with the canonical orderings of L_1 and L_2.*

Proof. It suffices to prove that $x \geq_{L_1} 0$ implies $\varphi(x) \geq_{L_2} 0$ for all $x \in L_1$. This follows from the fact that in a real-closed field L, for all $x \in L$, $x \geq 0$ if and only if x is a square. □

If k is a real field and k^r is a real closure of k, then k inherits an ordering from k^r. However, different real closures may induce different orderings on k, as the next example shows.

Example 4.42. Let $k = \mathbb{Q}(t)$. This is a real field, since $\mathbb{Q}$ is real. Since π is transcendental over $\mathbb{Q}$, we can embed $\mathbb{Q}(t)$ in $\mathbb{R}$ by sending t to π.

$$i_1\colon \mathbb{Q}(t) \xhookrightarrow{\sim} \mathbb{Q}(\pi) \subseteq \mathbb{R}.$$

Since $\mathbb{R}$ is real-closed, the relative algebraic closure $i_1(\mathbb{Q}(t))^{\mathbb{R}}$ is a real closure of $i_1(\mathbb{Q}(t))$.

We can also embed $\mathbb{Q}(t)$ in the field $\widehat{\mathbb{R}(t)}$ of real Puiseux series via a homomorphism i_2 and then $\overline{i_2(\mathbb{Q}(t))}^{\widehat{\mathbb{R}(t)}}$ is a real closure of $i_2(\mathbb{Q}(t))$. However, the ordering on $\overline{i_1(\mathbb{Q}(t))}^{\mathbb{R}}$ is Archimedean, because it is a subfield of $\mathbb{R}$, while the ordering on $\overline{i_2(\mathbb{Q}(t))}^{\widehat{\mathbb{R}(t)}}$ is not Archimedean (it contains infinitesimal elements, such as t for instance).

The fields $\overline{i_1(\mathbb{Q}(t))}^{\mathbb{R}}$ and $\overline{i_2(\mathbb{Q}(t))}^{\widehat{\mathbb{R}(t)}}$ cannot be isomorphic as fields. Indeed, when two real-closed fields L_1, L_2 are isomorphic as fields, then they are isomorphic as ordered fields, since positivity on a real closed field is defined by the condition of being a square, which is preserved under isomorphisms of fields.

Lemma 4.43. *Let $(k, \leq)$ be an ordered field, L/k an orderable real-closed extension of k and $\varphi\colon k \to L$ a morphism of k-algebras. If E/k is a finite, real extension of k, then φ admits a continuation, i.e. a morphism of k-algebras φ' such that the following diagram commutes:*

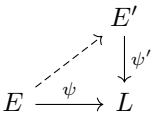
$$\begin{array}{ccc} k & \xrightarrow{\varphi} & L \\ \downarrow & \nearrow_{\varphi'} & \\ E & & \end{array}.$$

Proof. Since k is perfect, E/k is separable. Moreover E/k is finite, thus by the primitive element theorem, $E = k[a]$ for $a \in E$. Let $P \in k[t]$ be the minimal polynomial of a over k. Let E^r be an orderable real-closure of E. Thus E^r is a real-closed extension of k that contains a root of P. By 4.34, P has a root $b \in L$. Now define $\psi\colon k[t] \to L$ by $t \mapsto b$ and $\psi|_k = \varphi$. Since b is a root of P, ψ factors through $E = k[a] = k/(P)$ and gives $\varphi'\colon E \to L$. □

Theorem 4.44. *Let $(k, \leq)$ be an ordered field and k^r be a real closure of k that extends the ordering of k. Let L be a orderable real-closed extension of k. Then there exists a unique homomorphism of k-algebras $k^r \to L$.*

Proof. Uniqueness: Let $\varphi\colon k^r \to L$ be a homomorphism of k-algebras and $a \in k^r$. Since a is algebraic over k, it has a minimal polynomial $P \in k[t]$ over k. Denote by $a_1 \leq \ldots \leq a_n$ the roots of P in k^r. Since the characteristic of k is 0, k is perfect, in particular the irreducible polynomial P is separable and thus $a_1 < \ldots < a_n$. Now there exists a unique $1, \ldots, n$ such that $a = a_j$. By 4.34, the polynomial P also has n distinct roots $b_1 < \ldots < b_n$ in the real-closed field L. Since φ sends roots of P in k^r to roots of P in L, there is a permutation $\sigma \in S_n$ such that $\varphi(a_i) = b_{\sigma(i)}$. By 4.41, φ respects the ordering of the roots and thus $\sigma = \mathrm{id}$ and $\varphi(a) = \varphi(a_j) = b_j$.

Existence: Consider the set $\mathcal{F}$ of all pairs (E, ψ) where $k \subseteq E \subseteq k^r$ is a subextension of k^r/k and $\psi\colon E \to L$ is a homomorphism of k-algebras. Since $(k, k \hookrightarrow L) \in \mathcal{F}$, $\mathcal{F} \neq \emptyset$. Define an inductive ordering on $\mathcal{F}$ by $(E, \psi) \leq (E', \psi)$ if there is a commutative diagram



in the category of k-algebras. Then by Zorn, the set $\mathcal{F}$ admits a maximal element (E, ψ). E is real-closed, otherwise it admits a finite real extension E' of E. In particular $E' \subseteq k^r$. Since L is real-closed, $\psi\colon E \to L$ admits a continuation $\psi'\colon E' \to L$ by 4.43. Thus $(E, \psi) < (E', \psi')$ contradicting the maximality of (E, ψ). Hence E is real-closed and k^r/E is real algebraic, thus $E = k^r$. So ψ is a homomorphism of k-algebras from k^r to L. □

Corollary 4.45. *Let $(k, \leq)$ be an ordered field. If k_1^r and k_2^r are real closures of k whose canonical orderings are compatible with that of k, then there exists a unique isomorphism of k-algebras $k_1^r \xrightarrow{\simeq} k_2^r$.*

Proof. By 4.44 there exist unique homomorphisms of k-algebras $\varphi\colon k_1^r \to k_2^r$ and $\psi\colon k_2^r \to k_1^r$. Then $\psi \circ \varphi$ and $\mathrm{id}_{k_1^r}$ are homomorphisms $k_1^r \to k_1^r$ of k-algebras. By uniqueness in 4.44, $\psi \circ \varphi = \mathrm{id}_{k_1^r}$. Similarly, $\varphi \circ \psi = \mathrm{id}_{k_2^r}$. □

Remark 4.46. Contrary to the situation of algebraic closures of a field k, for ordered fields $(k, \leq)$ there is a well-defined notion of the real closure of k whose canonical ordering is compatible with that of k. As shown by 4.42, it is necessary to fix an ordering of the real field k to get the existence of an isomorphism of fields between two orderable real closures of k.

Corollary 4.47. *Let $(k, \leq)$ be an ordered field and let k^r be the real closure of k. Then k^r has no non-trivial k-automorphism.*

Proof. Take $k_1^r = k_2^r$ in 4.45. □

4.6 The real Nullstellensatz

When k is algebraically closed, Hilbert's Nullstellensatz implies $\mathcal{I}(\mathcal{V}_{k^n}(I)) = \sqrt{I}$ for all ideal $I \subseteq k[T_1, \ldots, T_n]$. In this section we try to compute $\mathcal{I}(\mathcal{V}_{k^n}(I))$ when k is a real-closed field.

Definition 4.48. Let $(k, \leq)$ be an ordered field and let A be a commutative k-algebra with unit. A is called a *real algebra* if it satisfies the following condition: If $\lambda_1, \ldots, \lambda_r > 0$ in k and $a_1, \ldots, a_r \in A$ satisfy

$$\sum_{j=1}^{r} \lambda_j a_j^2 = 0,$$

then $a_j = 0$ for all j. An ideal $I \subseteq A$ is called a *real ideal* if A/I is a real algebra.

Proposition 4.49. *Let $(k, \leq)$ be an ordered field, L/k an orderable extension and $Z \subseteq L^n$ be a subset. Then the ideal $\mathcal{I}_k(Z) \subseteq k[T_1, \ldots, T_n]$ is a real ideal.*

Proof. If $Z = \emptyset$, then $\mathcal{I}_k(Z) = \mathcal{I}_k(\emptyset) = k[T_1, \ldots, T_n]$ is a real ideal. Now assume $Z \neq \emptyset$. In this case, if $P_1, \ldots, P_r \in k[T_1, \ldots, T_n]$ and $\lambda_1, \ldots, \lambda_r > 0$ in k are such that $\sum_{j=1}^r \lambda_j P_j^2 \in \mathcal{I}_k(Z)$, then for all $x \in Z$, $\sum_{j=1}^r \lambda_j P_j^2(x) = 0$ in L. Since L/k is orderable and $\lambda_j > 0$ in k, and thus in L, for all j, this implies that for all j, $P_j(x) = 0$, i.e. $P_j \in \mathcal{I}_k(Z)$. □

Recall that if k is an arbitrary field and $I \subsetneq k[T_1, \ldots, T_n]$ is a proper ideal, then finding a common zero $x \in L^n$ to all polynomials $P \in I$ for some extension L of k is equivalent to finding a homomorphism of k-algebras

$$\varphi\colon k[T_1, \ldots, T_n]/I \longrightarrow L.$$

Indeed, the correspondence is obtained by sending such a φ to $x = (x_1, \ldots, x_n)$ where $x_i = \varphi(T_i \bmod I)$. The basic result should be about giving sufficient conditions for such homomorphisms to exist.

Theorem 4.50 (Real Nullstellensatz I)**.** *Let $(k, \leq)$ be an ordered field and let $k^{(r)}$ be the real closure of k. Let $I \subseteq k[T_1, \ldots, T_n]$ be a proper real ideal. Then there exists a homomorphism of k-algebras*

$$k[T_1, \ldots, T_n]/I \longrightarrow k^{(r)}.$$

In particular, $\mathcal{V}_{k^{(r)}}(I) \neq \emptyset$.

The idea of the proof of 4.50 is the following:

1. Show that there is a real-closed orderable extension L of k for which there exists a homomorpism of k-algebras
$$\varphi_L\colon k[T_1, \ldots, T_n]/I \longrightarrow L.$$
2. Next, show that this implies the existence of a homomorphism of k-algebras
$$\varphi\colon k[T_1, \ldots, T_n]/I \longrightarrow k^{(r)}.$$

Lemma 4.51. *Let k be a real-closed field, A a k-algebra and $\mathfrak{m} \subseteq A$ a maximal ideal. Then $A/\mathfrak{m}$ is real as a k-algebra if and only if it is real as a field.*

Proof. Since k is real-closed, all positive elements in k are squares. Thus $\mathfrak{m}$ is real if and only if for all $a_i \in A$ such that $\sum_{i=1}^r a_i^2 \in \mathfrak{m}$, it follows that $a_i \in \mathfrak{m}$ for $i \in \{1, \ldots, r\}$. Reading this equation in $A/\mathfrak{m}$ gives the result. □

If I in 4.50 was maximal, then we can just take L to be a real closure of the real field $k[T_1, \ldots, T_n]/I$. Note, however, that in order to get an orderable real-closed extension L/k, we would also have to define an ordering of $k[T_1, \ldots, T_n]/I$ extending the one of k.

In any case it is not clear that there exists a maximal ideal $\mathfrak{m} \supset I$ that is real. To remedy the situation, we observe the following:

Lemma 4.52. *Let $(k, \leq)$ be an ordered field, A a k-algebra and $I \subseteq A$ be a real ideal. Then $\sqrt{I} = I$. Moreover if A is noetherian and $\mathfrak{p} \supset I$ is a minimal prime ideal containing I, then $\mathfrak{p}$ is real.*

Proof. For the first part take $a \in \sqrt{I}$. Then there exists a minimal $m \geq 1$ such that $a^m \in I$. If $m = 2l$ then $a^{2l} = (a^l)^2 \in I$. Since I is real, this implies that $a^l \in I$ with $l < m$, contradicting the minimality of m. So $m = 2l + 1$ for some $l \geq 0$. If $l = 0$, we are done. Otherwise if $l \geq 1$, then $\left(a^{l+1}\right)^2 = a^{2l+2} = a(a^{2l+1}) \in I$. Since I is real, this implies that $a^{l+1} \in I$ with $l + 1 < m$, again contradicting the minimality of m.

For the second part, assume that A is noetherian. Then there are finitely many minimal prime ideals and

$$I = \sqrt{I} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$$

where the $\mathfrak{p}_i \supset I$ are the minimal prime ideals containing I. We need to show that every $\mathfrak{p}_i$ is real. To simplify the notation, we show that $\mathfrak{p}_1$ is real. Let $a_1, \ldots, a_m \in A$ such that $a_1^2 + \ldots + a_m^2 \in \mathfrak{p}_1$. Since for all $j \neq 1$, $\mathfrak{p}_1 \not\subset \mathfrak{p}_j$, there exists for all $j > 1$ an element $b_j \in \mathfrak{p}_j \setminus \mathfrak{p}_1$. Set $b = \prod_{j=2}^r b_j$. Then $b \in \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r$ and since $\mathfrak{p}_1$ is prime, $b \notin \mathfrak{p}_1$. But

$$(a_1 b)^2 + \ldots + (a_m b)^2 = (a_1^2 + \ldots + a_m^2) b^2 \in \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r = \sqrt{I} = I.$$

Since I is real, it follows that $a_j b \in I \subseteq \mathfrak{p}_1$. Since $b \notin \mathfrak{p}_1$ and $\mathfrak{p}_1$ is prime, $a_j \in \mathfrak{p}_1$ for all j. □

To complete step 1 in the proof of 4.50, we can choose a minimal prime ideal $\mathfrak{p} \supset I$ and consider its fraction field

$$K = \operatorname{Frac}(k[T_1, \ldots, T_n]/\mathfrak{p}).$$

We need to assure that K/k is a real orderable extension.

Lemma 4.53. *Let $(k, \leq)$ be an ordered field, A be a k-algebra and $\mathfrak{p} \subseteq A$ be a prime ideal. Then the fraction field*

$$K \coloneqq \operatorname{Frac}(A/\mathfrak{p})$$

is a real orderable extension of k if and only if the prime ideal $\mathfrak{p}$ is real.

Proof. ($\Leftarrow$): Let $\mathfrak{p}$ be real and let $a_i, b_i \in A$, $b_i \notin \mathfrak{p}$ and $0 < \lambda_i \in k$ such that

$$\sum_{i=1}^r \lambda_i \left(\frac{a_i}{b_i}\right)^2 = 0 \tag{4.3}$$

This equation implies that

$$\sum_{i=1}^r \lambda_i \left(a_i \prod_{j \neq i} b_j\right)^2 = \prod_{j=1}^r b_j^2 \sum_{i=1}^r \lambda_i \frac{a_i^2}{b_i^2} = 0$$

in $K = \operatorname{Frac}(A/\mathfrak{p})$, so

$$\sum_{i=1}^r \lambda_i \left(a_i \prod_{j \neq i} b_j\right)^2 \in \mathfrak{p}.$$

Since $\mathfrak{p}$ is real, it follows that $a_i \prod_{j \neq i} b_j \in \mathfrak{p}$. Moreover $b_j \notin \mathfrak{p}$ for all j and $\mathfrak{p}$ is prime, so $a_i \in \mathfrak{p}$, thus $\frac{a_i}{b_i} = 0 \in K = \operatorname{Frac}(A/\mathfrak{p})$ for all i. This shows that every positive definite quadratic form over k, is anisotropic over L. By 4.26, the claim follows.

($\Rightarrow$): Assume that $\lambda_i > 0$ in k and $\sum_{i=1}^r \lambda_i a_i^2 \in \mathfrak{p}$ for some $a_i \in A$. Then

$$\sum_{i=1}^r \lambda_i \frac{a_i^2}{1^2} = 0$$

in $K = \operatorname{Frac}(A/\mathfrak{p})$. Since $\lambda_i > 0$ in K, this implies $\frac{a_i}{1} = 0$ in K and therefore $a_i = 0$ in $A/\mathfrak{p}$ for all i. □

Proof of 4.50. Choose a minimal prime ideal $\mathfrak{p}$ containing I and denote by $K = \operatorname{Frac}(k[T_1, \ldots, T_n]/\mathfrak{p})$. By 4.53, we know that K/k is an orderable extension of fields. Let L be the real closure of K. Since L/K and K/k are orderable, it follows that L/k is orderable and we have a canonical morphism of k-algebras $\varphi_L \colon k[T_1, \ldots, T_n]/I \to L$ given by the composition of the canonical morphisms,

$$k[T_1, \ldots, T_n]/I \to k[T_1, \ldots, T_n]/\mathfrak{p} \hookrightarrow \operatorname{Frac}(k[T_1, \ldots, T_n]/\mathfrak{p}) = K \hookrightarrow L.$$

This finishes step one of the strategy outlined above. For step two, let $x_i \coloneqq \varphi_L(T_i)$. These elements generate a sub-extension $k \hookrightarrow k(x_1, \ldots, x_n) \subseteq L$, containing $\operatorname{im} \varphi_L$. Denote by $\overline{k}^L$

the algebraic closure of k in L. Since L is real-closed and L/k is orderable, we know that $\overline{k}^L$ is an orderable real-closure of the ordered field $(k, \leq)$. So by 4.45 there exists a (unique) homomorphism of k-algebras $k^{(r)} \simeq \overline{k}^L$. Thus, to conclude, it suffices to show that there exists a homomorphism of k-algebras $\operatorname{im} \varphi_L \to \overline{k}^L$.

Recall that $\operatorname{im} \varphi_L \subseteq k(x_1, \ldots, x_n)$ and the latter is a real field because it is a subfield of the real field L. In particular, if all x_i are algebraic over k, then $k(x_1, \ldots, x_n) \subseteq \overline{k}^L$ and we are done.

Otherwise, write

$$k(x_1, \ldots, x_n) = k(t_1, \ldots, t_r)[y_1, \ldots, y_s]$$

with each $t_i \in L$ transcendental over k and each $y_j \in L$ algebraic over $k(t_1, \ldots, t_r)$. By construction $r + s = n$ and we may assume that $\varphi_L(T_i) = t_i$ for $1 \leq i \leq r$ and $\varphi_L(T_{r+j}) = y_j$ for $1 \leq j \leq s$. Since k is ordered, $\operatorname{char} k = 0$ so by the primitive element theorem, there exists $y \in L$ algebraic over $k(t_1, \ldots, t_r)$ such that

$$k(t_1, \ldots, t_r)[y_1, \ldots, y_s] = k(t_1, \ldots, t_r)[y] \subseteq L.$$

Denote by $P \in k(t_1, \ldots, t_r)[T]$ the minimal polynomial of y over $k(t_1, \ldots, t_r)$. Then

$$P = T^m + \frac{f_{m-1}}{g_{m-1}} T^{m-1} + \ldots + \frac{f_0}{g_0}$$

for some polyomials $f_i, g_i \in k[t_1, \ldots, t_r]$. Let $h \coloneqq \prod_{0 \leq i \leq m-1} g_i \in k[t_1, \ldots, t_r]$. Then $h \neq 0$ in $k[t_1, \ldots, t_r]$ and y is integral over $k[t_1, \ldots, t_r]\left[\frac{1}{h}\right] \subseteq L$. Since $h \neq 0$ and k is infinite, there are elements $a_1, \ldots, a_r \in k$ such that $h(a_1, \ldots, a_r) \neq 0$, in particular $g_i(a_1, \ldots, a_r) \neq 0$ for all $0 \leq i \leq m-1$. Consider the polynomial

$$P_a = T^m + \frac{f_{m-1}(a_1, \ldots, a_r)}{g_{m-1}(a_1, \ldots, a_r)} T^{m-1} + \ldots + \frac{f_0(a_1, \ldots, a_r)}{g_0(a_1, \ldots, a_r)} \in k[T].$$

Since $P(y) = 0$ in $k(t_1, \ldots, t_r)$, it follows that $P_a(y) = 0$ in k. Thus y is algebraic over k and $y \in \overline{k}^L$.

By the universal properties of $k[t_1, \ldots, t_r]\left[\frac{1}{h}\right]$ and $k[t_1, \ldots, t_r, \frac{1}{h}][T]/(P)$, we can define a morphism of k-algebras

$$k\left[t_1, \ldots, t_r, \frac{1}{h}\right][y] \simeq k\left[t_1, \ldots, t_r, \frac{1}{h}\right][T]/(P) \longrightarrow \overline{k}^L$$

by setting $t_i \mapsto a_i$ for all $1 \leq i \leq r$ and $T \mapsto y$. Since $\operatorname{im} \varphi_L \subseteq k\left[t_1, \ldots, t_r, \frac{1}{h}\right][y]$, this concludes the proof. □

Remark 4.54. We have shown that if $I \subseteq k[T_1, \ldots, T_n]$ is a real ideal and there is a morphism

$$k[T_1, \ldots, T_n]/I \to L$$

where L is a real-closed orderable extension of k, then there is a morphism of k-algebras

$$k[T_1, \ldots, T_n]/I \to \overline{k}^L.$$

We can now deduce from 4.50 the other version of the real Nullstellensatz, starting with a question asked at the beginning of this section.

Theorem 4.55 (Real Nullstellensatz II)**.** *Let $(k, \leq)$ be an ordered field and let $I \subsetneq k[T_1, \ldots, T_n]$ be a proper ideal. Then $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I)) = I$ if and only if I is a real ideal.*

Proof. Let $L := k^{(r)}$ and assume that $I = \mathcal{I}_k(\mathcal{V}_{L^n}(I))$. Then by 4.49 I is a real ideal. Conversely, assume that I is real. We know that $I \subseteq \mathcal{I}_k(\mathcal{V}_{L^n}(I))$ and we want to show that this is an equality. Let $P \in k[T_1, \ldots, T_n] \setminus I$. Then we need to show that $P \notin \mathcal{I}_k(\mathcal{V}_{L^n}(I))$. Write $I = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ with pairwise distinct minimal prime ideals $\mathfrak{p}_i$ containing I. Since $P \notin I$, we may assume that $P \notin \mathfrak{p}_1$. By 4.52, $\mathfrak{p}_1$ is a real ideal. Denote by B the integral domain $k[T_1, \ldots, T_n]/\mathfrak{p}_1$. By 4.53 the fraction field $\mathrm{Frac}(B)$ is an orderable extension of k. Since $P \notin \mathfrak{p}_1$, the element $P_1 = P \bmod \mathfrak{p}_1$ is nonzero in B, so we have inclusions

$$B \subseteq B\left[\frac{1}{P_1}\right] \subseteq \mathrm{Frac}(B).$$

Since $\mathrm{Frac}(B)/k$ is orderable, $B\left[\frac{1}{P_1}\right]$ is a real k-algebra. Moreover B is nonzero and finitely generated over k, since

$$B\left[\frac{1}{P_1}\right] = (k[T_1, \ldots, T_n]/\mathfrak{p}_1)\left[\frac{1}{P_1}\right] \simeq k\left[T_1, \ldots, T_n, 1/P_1\right]/\mathfrak{p}_1\left[1/P_1\right].$$

Thus 4.50 provides a k-algebra homomorphism $\varphi\colon B\left[\frac{1}{P_1}\right] \longrightarrow L$. Pre-composing φ with the canonical morphism

$$k[T_1, \ldots, T_n]/I \longrightarrow k[T_1, \ldots, T_n]/\mathfrak{p}_1$$

induces a morphism $k[T_1, \ldots, T_n] \to L$ sending $(T_1, \ldots, T_n)$ to some $a = (a_1, \ldots, a_n) \in L^n$ and $\frac{1}{P_1}$ to a well-defined element $\frac{1}{P_1(a)}$ in L. So $P(a) = P_1(a) \neq 0$ in L and, since $I \subseteq \mathfrak{p}_1$, we have that $Q(a) = 0$ for all $Q \in I$. So $a \in \mathcal{V}_{L^n}(I)$ and therefore $P \notin \mathcal{I}_k(\mathcal{V}_{L^n}(I))$. □

Corollary 4.56. *Let $(k, \leq)$ be an ordered field and $k^{(r)}$ its real closure. The maps $I \mapsto \mathcal{V}_{k^{(r)}}(I)$ and $Z \mapsto \mathcal{I}_k(Z)$ induce a bijection*

$$\left\{k\text{-algebraic subsets of } \left(k^{(r)}\right)^n\right\} \longleftrightarrow \left\{\text{real ideals of } k[T_1, \ldots, T_n]\right\}.$$

Corollary 4.57. *Let $(k, \leq)$ be an ordered field and $k^{(r)}$ its real closure. For all ideal $I \subsetneq k[T_1, \ldots, T_n]$, we have $\mathcal{V}_{(k^{(r)})^n}(I) \neq \emptyset$ if and only if I is proper and real.*

Proof. If $\mathcal{V}_{(k^{(r)})^n}(I) = \emptyset$ and I real, then by 4.55

$$I = \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I)) = \mathcal{I}_k(\emptyset) = k[T_1, \ldots, T_n].$$

The converse is **??**. □

Remark 4.58. It is also true that real Nullstellensatz II implies real Nullstellensatz I. Indeed, if $I \subsetneq k[T_1, \ldots, T_n]$ is a real proper ideal, by the if-part of 4.57 $\mathcal{V}_{k^{(r)}}(I) \neq \emptyset$. Moreover any $a \in \mathcal{V}_{(k^r)^n}(I) \subseteq k^n$ defines an evaluation morphism of k-algebras

$$\begin{aligned} k[T_1, \ldots, T_n]/I &\longrightarrow k^{(r)} \\ P \bmod I &\longmapsto P(a). \end{aligned}$$

4.7 The real-radical of an ideal

Let $(k, \leq)$ be an ordered field. In this section, we wish to understand $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$ for arbitrary ideal $I \subseteq k[T_1, \ldots, T_n]$.

Proposition 4.59. *Let $(k, \leq)$ be an ordered field and $I \subseteq k[T_1, \ldots, T_n]$ an ideal. Then $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$ is the smallest real ideal containg I.*

Proof. By 4.49, $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$ is real. If J is a real ideal containing I, then by the real Nullstellensatz II (4.55) we have $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I)) \subseteq \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(J)) = J$. □

Let $I \subseteq k[T_1, \ldots, T_n]$ be an ideal. Since $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$ is real, if $Q_0, \ldots, Q_l \in k[T_1, \ldots, T_n]$ satisfy $Q_0^2 + \ldots + Q_l^2 \in \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$, then $Q_j \in \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$ for all j. In particular, $Q_0 \in \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$. Since real ideals are radical, if $Q_0 = P^m$ with $m \geq 1$, then $P \in \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$. In other words, to prove that a given polynomial $P \in k[T_1, \ldots, T_n]$ belongs to $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$, it suffices to show that there is $m \geq 1$ and $Q_1, \ldots, Q_l \in k[T_1, \ldots, T_n]$ such that

$$P^{2m} + Q_1^2 + \ldots + Q_l^2 \in \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I)).$$

This observation motivates the following definition:

Definition 4.60. Let A be a ring and $I \subseteq A$ an ideal. The *real-radical* of I is the set

$$\sqrt[r]{I} := \left\{ P \in A \mid \exists m \geq 1, Q_1, \ldots, Q_l \in A \text{ such that } P^{2m} + Q_1^2 + \ldots + Q_l^2 \in I \right\}.$$

Remark 4.61. (i) Taking $Q_1 = \ldots = Q_l = 0$, we see that $I \subseteq \sqrt[r]{I}$.

(ii) If $(k, \leq)$ is an ordered field and $I \subseteq k[T_1, \ldots, T_n]$ an ideal, then by the observation above, one has $\sqrt[r]{I} \subseteq \mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I))$.

Lemma 4.62. *Let A be a ring and $I \subseteq A$ a real ideal. Then $\sqrt[r]{I} = I$.*

Proof. It suffices to show that $\sqrt[r]{I} \subseteq I$. Suppose that $P \in \sqrt[r]{I}$. Then there exist $m \geq 1$ and $Q_1, \ldots, Q_l$ such that

$$P^{2m} + Q_1^2 + \ldots + Q_l^2 \in I.$$

Since I is real, this implies in particular that $P^m \in I$. By 4.52, I is radical so $P \in I$. □

Proposition 4.63. *Let A be a ring. Then*

$$\sqrt[r]{(0)} = \bigcap_{\mathfrak{p} \subseteq A \text{ prime and real}} \mathfrak{p}.$$

Proof. Let $E := \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ is prime and real}\}$ and let $P^{2m} + Q_1^2 + \ldots + Q_l^2 = 0$ for $P, Q_i \in A$. Since $0 \in \mathfrak{p}$ for all $\mathfrak{p} \in E$, we obtain $P \in \sqrt[r]{\mathfrak{p}} \overset{4.62}{=} \mathfrak{p}$. Conversely, let $s \in A \setminus \sqrt[r]{I}$. We need to show that there exists $\mathfrak{p} \in E$, such that $s \notin \mathfrak{p}$. Consider the set $E_s := \{I \subseteq A \text{ ideal } \mid s \notin \sqrt[r]{I}\}$. The set E_s is non-empty, since $s \notin \sqrt[r]{(0)}$. E_s admits an inductive order defined by inclusion, so by Zorn, there exists a maximal element $J \in E_s$. In particular, $s \notin \sqrt[r]{J}$.

This J is prime, since otherwise there exists $a_1, a_2 \in A \setminus J$ such that $a_1 a_2 \in J$. So $J \subsetneq J + (a_1)$ and $J \subsetneq J + (a_2)$. By maximality of J in E_s, we have $s \in \sqrt[r]{J + (a_1)}$ and $s \in \sqrt[r]{J + (a_2)}$. Hence there exist m_1, m_2 and $(f_i)_{1 \leq i \leq l_1}$ and $(g_j)_{1 \leq j \leq l_2}$ in A such that

$$s^{2m_1} + f_1^2 + \ldots + f_{l_1}^2 = x_1 + a_1 b_1$$

and

$$s^{2m_2} + g_1^2 + \ldots + g_{l_2}^2 = x_2 + a_2 b_2$$

for some $x_1, x_2 \in J$ and $b_1, b_2 \in A$. Multiplying these two equations gives

$$s^{2(m_1+m_2)} + \text{sum of squares} = \underbrace{x_1x_2 + x_1a_2b_2 + x_2a_1b_1 + a_1a_2b_1b_2}_{\in J},$$

so $s \in \sqrt[r]{J}$. Contradiction to $J \in E_s$.

J is real. Otherwise, there are $a_0, \ldots, a_m \in A$ such that $a_0^2 + \ldots + a_m^2 \in J$, but $a_0 \notin J$. This implies $a_0 \in \sqrt[r]{J} \setminus J$. Since $s \notin \sqrt[r]{J}$ by construction of J, we have $J \subsetneq \sqrt[r]{J} \in E_s$ contradicting the maximality of J. □

Corollary 4.64. *Let A be a commutative ring and $I \subseteq A$ an ideal. Then*

$$\sqrt[r]{I} = \bigcap_{\mathfrak{p} \supset I \text{ prime and real in } A} \mathfrak{p}.$$

In particular, $\sqrt[r]{I}$ is a real ideal and it is the smallest real ideal containing I.

Proof. For the first part, one applies 4.63 to A/I. For the second part, observe that $\sqrt[r]{I}$ is real since it is the intersection of real ideals. Secondly, if J is a real ideal containing I, then $\sqrt[r]{I} \subseteq \sqrt[r]{J} \overset{4.62}{=} J$. □

Corollary 4.65 (Real Nullstellensatz III)**.** *Let $(k, \leq)$ be an ordered field, $k^{(r)}$ its real closure and $I \subseteq k[T_1, \ldots, T_n]$ an ideal. Then*

$$\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I)) = \sqrt[r]{I}.$$

Proof. Direct consequence of 4.59 and 4.64. □

Remark 4.66. The real Nullstellensatz III also implies the real Nullstellensatz II. Indeed, if $I \subseteq k[T_1, \ldots, T_n]$ is an ideal, then by 4.65: $\mathcal{I}_k(\mathcal{V}_{(k^{(r)})^n}(I)) = I$ if and only if $\sqrt[r]{I} = I$. The latter holds if and only if I is real.

Remark 4.67. There is another characterisation of the real-radical of an ideal $I \subseteq A$ which is given as follows:

$$\sqrt[r]{I} = \left\{ P \in A \mid \exists m \geq 1, Q_1, \ldots, Q_l \in A, P^m \left(1 + \sum_{i=1}^{l} Q_i^2\right) \in I \right\}.$$