UNIVERSITÀ DI GENOVA

DIME - Dipartimento di ingegneria meccanica, energetica, gestionale e dei trasporti

PHILOSOPHIAE DOCTOR THESIS

On some Aspects of Polynomial Dynamical Systems

Candidate
Mr. Alessio Del Padrone
DIME
Università di Genova, Italia

Advisor
Prof. Angelo Alessandri
DIME
Università di Genova, Italia

Year 2022

ON SOME ASPECTS OF POLYNOMIAL DYNAMICAL SYSTEMS

Alessio Del Padrone

Alessio Del Padrone

DIME, Università di Genova, Via all'Opera Pia, 15-16145 Genova, Italy, Tel 0103532882, Fax 010317750.

E-mail : delpadrone@dime.unige.it

CONTENTS

INTRODUCTION

The aim of this work is to study exact algebraic criteria local/global observability ([**HK77**], [**Ino77**]) for polynomial dynamical system by means of algebraic geometry and computational commutative algebra in the vein of [**SR76**], [**Son79a**], [**Son79b**], [**Bai80**], [**Bai81**], [**Bar95**], [**Bar99**], [**Nes98**], [**Tib04**], [**KO13**], [**Bar16**].

A key point in this topic is to work with polynomials with *real* coefficients and their *real roots* instead of their *complex roots*, as it is usually the case ([**CLO15**], [**KR00**]). A central concept is then the real radical of an ideal [**BN93**], [**Neu98**], [**LLM$^+$13**], along with the Krivine-Dubois-Risler real nullstellensatz for polynomial rings [**Kri64**], [**Dub70**], [**Ris70**], [**BCR98**]. Underestimating this point leads to incorrect results (see, e.g. [**Bar16**] remark on [**KO13**]).

This thesis is therefore devoted to set the necessary algebraic tools in the right context and level of generality (i.e. *real algebra* and *real algebraic geometry*) for applications to our dynamical systems and to further develop their exploit in this context.

The first two chapters set the algebraic and algebraic geometry preliminaries. The third chapter is devoted to the applications of the previous algebraic concepts to the study of the observability of polynomial dynamical systems. In the last chapter an approach to the construction of Lyapunov funtions to prove stability in estimation problems is presented.

Acknowledgments

I wish to thank Professor Maria Virginia Catalisano for constant support.

During these years I have benefited of the encouragement of Professor Roberto Cianci and Professor Patrizia Bagnerini from the DIME research group in Mathematical simulation.

I also like to thank Elena Ausonio and Dyhia Bouhadjra for constant help and discussion.

I am greatly in debt to my advisor Professor Angelo Alessandri for his patient and constant aid.

NOTATION

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: natural, integer, rational, real and complex numbers.
- A: commutative unitary ring. $A^\times$: its group of units.

CHAPTER 1

ALGEBRA

1.1. Commutative rings, ideals, ring homomorphisms, quotient rings

We recall and fix some terminology from algebra ([**Lan02**]), commutative algebra ([**AM69**], [**Kun85**], [**Sha90**], [**Bos18**]) and real algebra ([**Lam84**], [**BCR98**]) which will be of use in the sequel.

1.1.1. Units, zero divisors, integral domains, fields. — Let $A = (A, +, 0_A; \cdot, 1_A)$ be a commutative unitary ring. An element of $a \in A$ is said to be **invertible**, or a **unit**, in A if there exists a $b \in A$ such that $ab = 1$, and then we write $b = a^{-1}$. The set of all units of A is denoted $A^\times = \mathrm{U}(A) := \{a \in A \mid a \text{ is invertible}\}$, and it forms a group under multiplication of A.
An element of $a \in A \setminus \{0\}$ is said to be a **zero divisor** if there exists a nonzero $b \in A \setminus \{0\}$ such that $ab = 0$. If, moreover $a \neq 0$, then a is said to be a **non-trivial zero divisor** of A. The set of all zero divisors of A is denoted $\mathrm{Zdv}(A)$. Obviously $0_A \in \mathrm{Zdv}(A)$ if and only if $1_A \neq 0_A$ (as often implicitly assumed). The non-zero ring A is said to be a **(integral) domain** if whenever $ab = 0$ then $a = 0$ or $b = 0$, and A is said to be a **field** whenever $a \neq 0$ in A implies there exists $b \in A$ such that $ab = 1$, or equivalently $A^\times = A \setminus \{0\}$.
A field K is said to be an **algebraically closed field** if every univariate polynomial with coefficients in K has a root in K (and therefore splits into a product of powers of linear factors with coefficients in K).

1.1.2. Definition. — Let A be a commutative unitary ring. We denote $A^{(2)}$ the set of all **squares in** A, that is the image of the **square map** $\mathrm{p}_2 \colon A \longrightarrow A, a \mapsto a^2$. The set $A^{(2)}$ contains 0, 1 and is closed under products and inverses (meaning: if a square is invertible then also its inverse is square), but it does not need to be closed under sums in general.

1.1.3. Definition. — The **set of all (finite) sums of squares** of elements of A is denoted

$$\mathrm{SQ}(A) = \Sigma A^{(2)} := \{a_1^2 + \cdots + a_n^2 \mid n \in \mathbb{N}_+,\, a_1, \cdots a_n \in A\}.$$

1.1.4. Remark. — Note that:

$$\Sigma A^{(2)} + \Sigma A^{(2)} \subseteq \Sigma A^{(2)}, \quad \Sigma A^{(2)}\Sigma A^{(2)} \subseteq \Sigma A^{(2)}, \quad (A^\times \cap \Sigma A^{(2)})^{-1} \subseteq \Sigma A^{(2)}, \quad \mathbb{N} \cdot 1_A \in \Sigma A^{(2)},$$

i.e. $\Sigma A^{(2)}$ is closed under addition, multiplication and inversion.

Proof. — Obviously, sums of sums of squares, and therefore linear combinations with non-negative integer coefficients $\sum_{i=1}^t n_i\sigma_i$ (with $n_i \in \mathbb{N}, \sigma_i \in \Sigma A^{(2)}$) of them, as well as products of sums of squares, are sums of squares. If $\sigma \in A^\times \cap \Sigma A^{(2)}$, then $\sigma^{-1} = \sigma \cdot (\sigma^{-1})^2 \in \Sigma A^{(2)}$. Clearly $0_A = 0_A^2$ and $1_A = 1_A^2$ are in $\Sigma A^{(2)}$ as well as, therefore, any iterated sum $n \cdot 1_A$ with $n \in \mathbb{N}$. □

1.1.5. Remark. — If A is a commutative unitary ring such that $2 \in A^\times$ then every element of A is a difference of two square elements.

Proof. — Indeed $a = \frac{1}{4}4a = \frac{1}{4}\left((1+a)^2 - (1-a)^2\right) = \left(\frac{1+a}{2}\right)^2 - \left(\frac{1-a}{2}\right)^2$. □

1.1.6. Remark. — (a) Clearly, every field is a domain.
(b) By definition, if A is domain then its cardinal number $|A| \geq 2$.
(c) If A happens to be a domain with a finite number of elements, or finite dimensional as a K-vector space, over a field K, then A is a field. In both cases, the multiplications maps by non zero elements $\mu_a \colon A \longrightarrow A, x \mapsto ax$ are injective as A is a domain and therefore they are bijective since the finiteness assumption.

1.1.7. Characteristic of a ring. — The **characteristic of** A, denoted $\mathrm{char}(A)$, is defined as the smallest $n \in \mathbb{N}_+$ such that $n \cdot 1_A = 0_A$ in A, if there is such an n, otherwise it's defined to be 0.

1.1.8. Example. — (a) The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, their unitary subrings as any unitary ring containing them, they all have characteristic 0.
(b) The residue class ring $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ has characteristic n for any $n \in \mathbb{N}$, $n \geq 2$.
(c) The finite field with p elements, $\mathbb{F}_p = \mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$, with p a prime integer, the finite field with $q = p^n$ elements, $\mathbb{F}_q$, with $q = p^n$ a power of p, their algebraic closure $\overline{\mathbb{F}_p}$, as well as any unitary ring containing them, all have characteristic p.

1.1.9. Remark (Trivial cases of $-1 \in A^{(2)}$). — Note that if $A = \overline{\mathbb{Q}}$ (the algebraic closure of the field $\mathbb{Q}$), $A = \mathbb{C}$, or $A = L$ any algebraically closed field, or A has positive characteristic then $-1 \in \Sigma A^{(2)}$.

Proof. — In the first two examples: $-1 = i^2$, and in general if A is an algebraically closed field then $-1 = a^2$ with a any root of $X^2+1 \in A[X]$. If A has positive characteristic, say $n \geq 2$, then rearranging the n-terms sum $n \cdot 1_A = \sum_{j=1}^{n} 1_A = 0$ we get $-1_A = \sum_{j=1}^{n-1} 1_A^2 \in \Sigma A^{(2)}$. □

1.1.10. Ring homomorphisms. — Let A and B be two commutative unitary rings. A **(unitary) ring homomorphism** from A to B is a map $f\colon A \longrightarrow B$ such that

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y), \qquad f(1_A) = 1_B$$

1.1.10.1. **Remark**. — (a) The integer $\mathrm{char}(A)$ is also the (unique) non negative generator of the kernel of the (unique) unitary ring homomorphism $\iota_A\colon \mathbb{Z} \longrightarrow A, n \mapsto n{\cdot}1_A$, $\mathrm{Ker}(\iota_A) = (\mathrm{char}(A))$.
(b) The image of this ring homomorphism is called the **prime subring of** A, it coincides with the smallest subring of A and it is isomorphic (as a ring) either to $\mathbb{Z}$ (if $\mathrm{char}(A) = 0$) or to $\mathbb{Z}/n\mathbb{Z}$ (if $n = \mathrm{char}(A) > 0$).
(c) If $A = K$ is a field, $\mathrm{Im}(\iota_A)$ is always contained in the **prime subfield of** K, *i.e.* the smallest subfield of K, and it coincides with it if and only if $p = \mathrm{char}(K) > 0$ is a prime integer (and $\mathrm{Im}(\iota_A) \cong \mathbb{F}_p$ prime subfield of K), else it is isomorphic (as a ring) to $\mathbb{Z}$ (subring of $\mathbb{Q}$ prime field of K).

1.1.11. Ideals and Residue Class Rings. — (a) An **ideal** of A is a (necessarily not empty) subset $I \subseteq A$ which is a subgroup of the additive group $(A, +, 0_A)$ and satisfies $AI := \{ax \mid a \in A,\, x \in I\} \subseteq I$. Note that we then have the following "stability property": $I = A \Leftrightarrow 1 \in I$.
(b) If I is an ideal of A, the relation $a \equiv b \pmod{I} :\Leftrightarrow a - b \in I$, called **congruence modulo** I, is an equivalence relation [1] on A which is coherent with the operations (that's why it is called a "congruence") and the **quotient** set $A/I = \{a + I \mid a \in A\}$ is also a commutative unitary ring wrt to the operations induced by those of A. It is called the **residue class ring** or **quotient**

1. An *equivalence relation on a set* S is a binary relation $\sim$ on S which is *reflexive* ($s \sim s$ for each $s \in S$), *symmetric* ($s_1 \sim s_2 \Leftrightarrow s_2 \sim s_1$) and *transitive* ($s_1 \sim s_2, s_2 \sim s_3 \Rightarrow s_1 \sim s_3$), *i.e.* it is a subset $E_\sim$ of the cartesian square $S^2 = S \times S$ containing the diagonal ($\Delta_S := \{(s,s) \mid s \in S\} \subseteq E_\sim$), symmetric with respect to it ($(a,b) \in E_\sim \Leftrightarrow (b,a) \in E_\sim$) and such that $(s_1,s_2), (s_2,s_3) \in E_\sim \Rightarrow (s_1,s_3) \in E_\sim$. Obviously $s_1 \sim s_2 \Leftrightarrow (s_1,s_2) \in E_\sim$.

ring of A modulo I. Moreover the **quotient map** $A \longrightarrow A/I, a \mapsto \overline{a} = [a]_I = a + I$ is a homomorphism of unitary ring with the usual universal property, see [**Lan02**, p. 89].

1.1.11.1. **Principal ideals and finitely generated ideals.**— (a) If $x \in A$, the smallest ideal of A containing x is the subset $(x) := Ax = \{ax \mid a \in A\}$, the **ideal generated by the element** x; the ideals of the form (x), with $x \in A$ are said **principal ideals** of A. Clearly, x is a unit in A if and only if $(x) = A$.
(b) More generally, if $S \subseteq A$ is any subset of A (even the empty one), the smallest ideal of A containing it is the subset (S) containing all the (finite) linear combinations of elements from S with coefficients in A, the **ideal generated by the subset** S. In case $S = \{x_1, \ldots, x_n\}$ is a finite subset of A then we simply write $(S) = (x_1, \ldots, x_n) = Ax_1 + \cdots + Ax_n := \{a_1x_1 + \cdots + a_nx_n \mid a_1, \cdots, a_n \in A\}$; the ideals of this form are said **finitely generated ideals** of A.
(c) Note that $(\emptyset) = (0) = \{0\}$ is the **zero ideal** of A, while its **unit ideal** is $(1) = A$, hence any non zero A has at least two ideals and it has only these two if and only if it is a field.

1.1.11.2. **Kernels, images**. — (a) The **kernel** and the **image** of a ring homomorphism are defined as usual $\mathrm{Ker}(f) = f^{-1}(0_B) = \{a \in A \mid f(a) = 0_B\}$, and $\mathrm{Im}(f) = f(A) = \{f(a) \in a \in A\}$.
(b) The kernel is always an ideal of A, while the second in usually only a subring of B.

1.1.11.3. **Remark**. — If A happens to be a field, then any unitary homomorphism from A to any non-zero ring B is injective. Indeed the kernel of such a homomorphism is an ideal of A, but as A is a field it has to be either (0) or (1).

1.1.11.4. **Definition**. — (a) If J is an ideal of B then $f^{-1}(J)$ is always an ideal of B, called the **contraction** of J to A, *i.e.* $J^c := f^{-1}(J)$.
(b) On the other hand, if I is an ideal of A and f is surjective, then $f(I)$ is an ideal of B also; but if f is not surjective, then $f(I)$ is not necessarily an ideal of B (despite being a multiplicatively closed subgroup of it). Hence, if I is an ideal of A, we define its **extension** to B as the ideal of B generated by $f(I)$, that is $I^e = f(I)B := (f(I)B)$.

1.1.11.5. **Extension-contraction of ideals**. — Given a ring homomorphism $f\colon A \longrightarrow B$, we have two opposite set maps $\{\text{ideals of } A\} \underset{f}{\overset{f^{-1}}{\rightleftarrows}} \{\text{ideals of } B\}$, $I \mapsto I^e \subseteq B$, $J \mapsto J^c \subseteq A$. They are two order-preversing "enlarging" maps, that is

$$I_1 \subseteq I_2 \text{ in } A \Rightarrow I_1^e \subseteq I_2^e \text{ in } B, \qquad J_1 \subseteq J_2 \text{ in } B \Rightarrow J_1^c \subseteq J_2^c \text{ in } A$$
$$I^{ec} \supseteq I \text{ in } A \qquad J^{ce} \subseteq J \text{ in } B.$$

As a consequence $I^{ece} = I^e$ in B and $J^{cec} = J^c$ in A. Therefore, the above ordered correspondence induces a bijection between **contracted ideals** (from B) of A and **extended ideals** (from A) of B

$$\mathcal{C} := \{I \text{ ideal of } A \mid I^{ec} = I\} \underset{f}{\overset{f^{-1}}{\longleftrightarrow}} \mathcal{E} := \{J \text{ ideal of } B \mid J^{ce} = J\},$$

$$A \supseteq I \mapsto I^e = (f(I)B) \subseteq B \qquad B \supseteq J \mapsto J^c = f^{-1}(J) \subseteq A$$

When f is surjective, for example a canonical quotient ring map $A \longrightarrow A/I$, this gives that ideals of B correspond bijectively to ideals of A containing $\mathrm{Ker}(f)$, in the example of the quotient map the ideal I.

1.1.12. Definition (Algebras). — If R is a commutative unitary ring, a **R-algebra** is a pair (A, η) where $\eta\colon R \longrightarrow A$ is a (unitary) ring homomorphism. The homomorphism is called **structure morphism** of the R-algebra A. If A is a R-algebra and $r \in R$ and $a \in A$ we write ra to mean $\eta(r)a$.

1.1.13. Definition (Homomorphism of R-algebras). — If R is a commutative unitary ring, and (A, η_A) and (B, η_B) are two R-algebras, a **homomorphism of R-algebras**

$$f\colon (A, \eta_A) \longrightarrow (B, \eta_B)$$

is a (unitary) ring homomorphism $f\colon A \longrightarrow B$ such that $f \circ \eta_A = \eta_B$. Hence

$$f(ra) = f(\eta_A(r)a) = f(\eta_A(r))f(a) = \eta_B(r)f(a) = rf(a)$$

for each $r \in R$ and $a \in A$.

1.1.14. Example: algebra of functions. — Let R be any commutative unitary ring, and let S be any set, then $R^S = \prod_{s\in S} R = \mathcal{F}(S, R) := \{\varphi \mid \varphi\colon S \longrightarrow R \text{ function from } S \text{ to } R\}$ is an R algebra under pointwise defined sum and product operations, the R-algebra structure is defined by the "diagonal" ring homomorphism $\eta\colon R \longrightarrow R^S, r \mapsto (r)_{s\in S}$ (the constant function with constant value r). The invertible elements of this algebra are $\mathrm{U}(R^S) = \mathrm{U}(R)^S$. Note that, for each $s \in S$ the function $e_s := (\delta_{s,t})_{t\in S} \in R^S$, with $\delta_{s,t} = 1$ if and only of $t = s$ and $\delta_{s,t} = 0$ otherwise, is an idempotent element of R^S, that is $e_s^2 = e_s$ for each $s \in S$, and $e_s e_t = 0$ for each $s, t \in S$ such that $t \neq s$. Hence R^S is a domain if and only if R is a domain and $|S| = 1$.

1.2. Polynomial rings

1.2.1. Definition (polynomials with coefficients in A). — If A is a commutative unitary ring, the set of all A-valued, finite support, sequences

$$A^{(\mathbb{N})} := \{\alpha = (a_n)_{n\in\mathbb{N}} \mid a_n \in A \text{ for each } n \in \mathbb{N}, \text{ there is } N_\alpha \in \mathbb{N} : a_n = 0_A \text{ for each } n \geq N_\alpha\}$$

endowed with pointwise sum and Cauchy product of sequences ($(\alpha\beta)_n := \sum_{i=0}^{n} \alpha_i\beta_{n-i}$ for each n), so that, if $e_i := (\delta_{ij})_{j\in\mathbb{N}}$, with $\delta_{ij} = 1_A$ if $j = i$ and else 0_A, we have $e_1^n = e_n$ for each $n \in \mathbb{N}$, is a commutative unitary ring with unit $1 = e_0 = (1_A, 0_A, 0_A, 0_A, \dots)$, endowed with a (unitary) ring homomorphism $\iota_A \colon A \longrightarrow A^{(\mathbb{N})},\ a \mapsto (a, 0_A, 0_A, 0_A, \dots)$, and which is generated as an A-algebra by the **indeterminate** $X := e_1 = (0_A, 1_A, 0_A, 0_A, \dots)$, that is

$$A^{(\mathbb{N})} = A[X] = \{a_0 + a_1X + \cdots + a_nX^n \mid a_0, a_1, \dots, a_n \in A,\ n \in \mathbb{N}\}.$$

This ring is called the **ring of (univariate) polynomials with coefficients in** A. The multivariate case is defined by induction $A[X_1, \dots, X_n] := (A[X_1, \dots, X_{n-1}])[X_n]$ for each integer $n \geq 2$. One can also avoid the induction defining directly

$$A[X_1, \dots, X_n] = A^{(\mathbb{N}^n)} =$$

$$\{\alpha = (a_{\boldsymbol{k}})_{\boldsymbol{k}\in\mathbb{N}^n} \mid a_{\boldsymbol{k}} \in A \text{ for each } \boldsymbol{k} \in \mathbb{N}^n \text{ and } a_{\boldsymbol{k}} = 0_A \text{ for all but a finite number of } \boldsymbol{k} \in \mathbb{N}^n\}.$$

If $e_{\boldsymbol{k}} := (\delta_{\boldsymbol{k},\boldsymbol{h}})$, with $\delta_{\boldsymbol{k},\boldsymbol{h}} = 1_A$ if $\boldsymbol{h} = \boldsymbol{k}$ and else 0_A, then $e_{\boldsymbol{k}} = X_1^{k_1} \cdots X_n^{k_n}$ and every element of $A[X_1, \dots, X_n]$ is a finite sum of the form $\sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{\boldsymbol{k}}e_{\boldsymbol{k}} = \sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{\boldsymbol{k}}X_1^{k_1} \cdots X_n^{k_n}$ and the operations are defined as usual (the product is the convolution one). Clearly, the obvious map $A \longrightarrow A[X_1, \dots, X_n]$ makes $A[X_1, \dots, X_n]$ an A-algebra.

1.2.2. Remark: ideal extension from A to $A[X_1, \dots, X_n]$. — If I is an ideal of A, then its extension to $A[X_1, \dots, X_n]$ under the structural map is given by

$$I^e = IA[X_1, \dots, X_n] =: I[X_1, \dots, X_n] = \{p \in A[X_1, \dots, X_n] \mid p \text{ has coefficients in } I\}.$$

The homomorphism of A-algebras

$$A[X_1, \dots, X_n] \longrightarrow (A/I)[X_1, \dots, X_n],\ \sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{\boldsymbol{k}}X_1^{k_1} \cdots X_n^{k_n} \mapsto \sum_{\boldsymbol{k}\in\mathbb{N}^n} \overline{a_{\boldsymbol{k}}}X_1^{k_1} \cdots X_n^{k_n}$$

induces a canonical isomorphism $A[X_1, \dots, X_n]/I[X_1, \dots, X_n] \longrightarrow (A/I)[X_1, \dots, X_n]$. Moreover, for any ideal I of A we have $I^{ec} = (I[X_1, \dots, X_n]) \cap A = I$.

1.2.3. Universal property of polynomial rings. — For every pair of commutative unitary rings A and B, there is a natural bijection

$$\{\text{(unitary) ring homomorphisms } A[X] \longrightarrow B\} \longrightarrow \{\text{(unitary) ring homomorphisms } A \longrightarrow B\} \times B$$

such that: to a (unitary) ring homomorphism $\Lambda\colon A[X] \longrightarrow B$ it corresponds the ordered pair $(\Lambda \circ \iota_A, \Lambda(X))$, and conversely to such a pair (λ, b) it corresponds the (unitary) ring homomorphism $\Lambda\colon A[X] \longrightarrow B$ such that $\Lambda(\sum_{i=i}^{n} a_i X^i) := \sum_{i=i}^{n} \lambda(a_i) b^i \in B$.

Similarly, in the multivariate case we have:

$$\{\text{ring homomorphisms } A[X_1, \ldots, X_n] \longrightarrow B\} \longrightarrow \{\text{ring homomorphisms } A \longrightarrow B\} \times B^n.$$

1.2.4. Adjunction of elements. — If A is a unitary subring of B and $\{b_1, \ldots, b_n\}$ is a subset of B, the smallest subring of B containing A and $\{b_1, \ldots, b_n\}$ is

$$A[b_1, \ldots, b_n] := \{f(b_1, \ldots, b_n) \mid f \in A[X_1, \ldots, X_n]\}.$$

It coincides with the image of the ring homomorphism $A[X_1, \ldots, X_n] \longrightarrow B$, such that $\sum_{i=i}^{n} a_i X^i \mapsto \sum_{i=i}^{n} a_i b^i$. If it happens that this ring is a field we write $A(b_1, \ldots, b_n)$.

1.2.5. Remark (polynomials and polynomial functions). — It is common to identify polynomials and polynomial functions, but actually, for every A-algebra B there is only a (obvious) ring homomorphism $\mathcal{P}F_A^B\colon A[X] \longrightarrow \{\text{functions } \varphi\colon B \longrightarrow B\}$ whose image is the set (A-subalgebra) of (univariate) **polynomial functions on B with coefficients in A** and whose kernel coincides with the set of all polynomials with coefficients from A inducing the zero function on B: $\operatorname{Ker}(\mathcal{P}F_A^B) = \{f \in A[X] \mid f(b) = 0 \text{ for each } b \in B\}$. This kernel can be non trivial. For example, if $A = B$ is a finite ring then $f(X) := \prod_{a \in A}(X - a)$ is a nonzero monic polynomial of degree $|A|$, the cardinality of A, inducing the zero function on B, that is $f \in \operatorname{Ker}(\mathcal{P}F_A^B) \setminus \{0\}$.

1.2.6. Proposition. — *Let K be a finite field. Then K is not algebraically closed.*

Proof. — As K is finite the formula $f(X) := 1 + \prod_{a \in K}(X - a) \in K[X]$ defines a polynomial of degree $|K| \geq 2$ with coefficients in K such that $f(a) = 1$ for each $a \in K$. As f has no roots in K, the field K is not algebraically closed. □

1.3. Noetherian rings

1.3.1. Proposition-Definition. — *Let A be a commutative unitary ring, the following facts are equivalent:*

a) *every ideal of A is finitely generated, that is it has a finite system of generators;*
b) *every ascending chain of ideals of A, $I_1 \subseteq I_2 \subseteq \cdots I_n \subseteq \cdots$, becomes stationary (we say that the Ascending Chain Condition for ideals holds in A);*
c) *every non nonempty set of ideals of A contains a maximal element with respect to inclusion (we say that the maximal condition for ideals holds in A).*
d) *any system of generators of an ideal I contains a finite system of generators of I.*

A is said to be **Noetherian** *if it satisfies the above properties.*

Proof. — See [**Kun85**, Ch. 1, Prop. 2.2]. □

1.3.2. Examples of Noetherian rings. — Every field is such, as well as all rings of polynomials in a finite number of indeterminates with coefficients in a Noetherian ring (Hilbert's Basis Theorem, see [**Kun85**, prop. 2.3] or [**Lan02**, Ch. IV, Thm. 4.1]). Every quotient ring of a Noetherian ring is still such, as well as any finite direct product of Noetherian rings.

1.4. Operations on ideals. Prime and maximal ideals. Minimal primes

1.4.1. Lattice properties of ideals. — The set of all ideals of A is a *complete lattice* with respect to set theoretic inclusion, indeed the **intersection** (of any number) of ideals of A is itself an ideal of A (their "infimum" in the lattice) and the **sum** [2] (of any number) of ideals of A is again an ideal of A (which can be shown to be their "supremum" in the lattice).

1.4.2. Products and powers of ideals. — The **product** IJ of two ideals (or of any *finite* number) I and J is defined as the ideal generated by all the products xy, with one element x from I and one element y from J, hence IJ is the set of all finite sums $\Sigma X_i y_i$ with $X_i \in I$ and $y_i \in J$ foreach i. Note that $IJ \subseteq I \cap J \subseteq I + J$ (where all the inclusions can be strict). In

2. The "sum", $\Sigma_{I \in \mathcal{F}} I = (\bigcup_{I \in \mathcal{F}} I)$, of any (possibly infinite) numbers of ideals of A is the set of all finite sums with summands taken each in one of the ideals of the family; it's not difficult to show that this set is an ideal of A containing all the given ideals and it is the smallest one w.r.t. these two properties. In the finite binary case, we obviously have $I + J = \{x + y \mid x \in I,\, y \in J\}$.

particular, given $n \in \mathbb{N}$, we can consider the **power** I^n of an ideal I (with $I^0 = (1)$ by definition), which, if $n > 0$, is the set of all finite sums with summands which are products of n elements from I.

1.4.3. Prime and maximal ideals. — A proper [3] ideal I of A is said to be **prime** if whenever $xy \in I$, for some $x, y \in A$, then $x \in I$ or $y \in I$. Equivalently, I is prime if and only if whenever $J_1 J_2 \subseteq I$, for some ideals J_1, J_2 of A, then $J_1 \subseteq I$ or $J_2 \subseteq I$. In particular (0) is a prime ideal if and only if A is a domain. It's not difficult to check that *I is prime if and only if the quotient ring A/I is a domain*. The set of all prime ideals of a commutative unitary ring is called its **spectrum** and it is denoted $\mathrm{Spec}(A) := \{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime ideal of } A\}$. A proper ideal I of A is said to be **maximal** if it is such among all proper ideals, that is $I \neq A$ and if J is a proper ideal of A such that $I \subseteq J$ then $I = J$. In particular (0) is a maximal ideal if and only if A is a field. It's not difficult to check that *I is maximal if and only if the quotient ring A/I is a field*. In particular, any maximal ideal is prime (but the converse does not hold). The set of all maximal ideals of a commutative unitary ring is called its **maximal spectrum** and it is denoted $\text{m-Spec}(A) := \{\mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal of } A\}$.

1.4.4. Remark: contraction of primes. — If $f\colon A \longrightarrow B$ is a ring homomorphism and $\mathfrak{P}$ is a prime ideal of B, then its contraction to A, *i.e.* $\mathfrak{P}^c = f^{-1}(\mathfrak{P})$, is always a prime ideal of A. Indeed we have the ring injection into a domain $A/f^{-1}(\mathfrak{P}) \hookrightarrow B/\mathfrak{P}$, $\overline{a} \mapsto \overline{\overline{a}}$. This is not true, in general, for maximal ideals: (0) is a maximal ideal of $\mathbb{Q}$, but its contraction to the subring $\mathbb{Z}$ is a prime non maximal ideal of $\mathbb{Z}$.

1.4.5. Remark: extension of primes from A to $A[X_1, \ldots, X_n]$. — Note that, thanks to 1.2.2, we have an injective map $\mathrm{Spec}(A) \hookrightarrow \mathrm{Spec}(A[X_1, \ldots, X_n])$, $\mathfrak{p} \mapsto \mathfrak{p}[X_1, \ldots, X_n]$. This map is, in general, not surjective: (X) is a prime ideal of $\mathbb{Z}[X]$ which does not come as an extension of a prime ideal of $\mathbb{Z}$. Also: $(2, X)$ is a maximal ideal of $\mathbb{Z}[X]$ which properly contains the (extended) prime ideal $(2)\mathbb{Z}[X]$ of $\mathbb{Z}$, note: $\mathbb{Z}[X]/(2, X) \cong \mathbb{F}_2$, while $\mathbb{Z}[X]/(2)\mathbb{Z}[X] \cong \mathbb{F}_2[X]$.

1.4.6. Minimal primes of an ideal. — By Zorn's Lemma, any proper ideal I in a commutative unitary ring is contained in (at least) a maximal ideal ([**AM69**, Ch. I, Cor. 1.4]). On the other hand, among all prime ideals $\mathfrak{p}$ containing I, a special role is played by those which are

3. An ideal I of A is said to be **proper** if $I \neq (1)$, that is $I \neq A$

minimal for this property: a **minimal prime (divisor)** of I is a prime ideal $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$ and if $I \subseteq \mathfrak{q}$ for a prime ideal $\mathfrak{q}$, then $\mathfrak{p} \subseteq \mathfrak{q}$ ([**AM69**, Ch. I, Ex. 8], [**Kun85**, Ch. I, Prop. 4.9], [**Sha90**, Thm. 3.52]). The set of all minimal primes of I is denoted $\mathrm{Min}(I)$. The minimal prime ideals of the ring A are the minimal primes of its zero ideal, thus $\mathrm{Min}(A) := \mathrm{Min}((0))$.

1.4.7. Remark: minimal primes in Noetherian rings. — If A is Noetherian, then $\mathrm{Min}(I)$ is a finite set for each ideal I of A (see 1.11).

1.5. UFDs, PIDs and Euclidean domains. Algebraic and transcendental elements

We recall the following basic definitions and facts about a commutative unitary ring A.

1.5.1. Definition (Divisibility relation in a ring). — Given two elements $x, y \in A$ we say that x **divides** y, and we write $x \mid y$, if there exists $a \in A$ such that $y = ax$. If x does not divide y we write $x \nmid y$.

1.5.2. Definition (Irreducible and prime elements). — A non-zero element $x \in A$ is said to be **prime** if the ideal (x) it generates is a prime ideal, that is $p \mid ab$, with $a, b \in A$ always implies $p \mid a$ or $p \mid b$, *i.e.* whenever $ab = xc$, with $a, b, c \in A$, then $a = xa'$ for some $a' \in A$, or $b = xb'$ for some $b' \in A$. An element $x \in A$ is said to be **irreducible** if x is not a unit in A and it cannot be expressed as a product of two non-units, *i.e.* $x \notin \{0\} \cup A^\times$ and whenever $x = ab$, with $a, b \in A$, then $a \in A^\times$ or $b \in A^\times$. The element x is said **reducible** if it is not irreducible.

1.5.3. Remark. — By the chosen definitions (according to [**Lan02**, II, §5], [**Coh03**, 10.2], [**Bos18**, 2.4] and [**KR00**, 1.2]), the zero element $x = 0 \in A$ is neither irreducible nor prime (although the ideal (0) is prime if A is a domain); 0, all units $u \in A^\times$ and all products of at least two irreducible elements are reducible. If x is irreducible and u is a unit, then ux is still irreducible. Note that if $x \neq 0$ and (x) is a maximal ideal then x is a prime element.

1.5.4. Example. — (a) If $A = \mathbb{Z}$, then x is an irreducible element if and only if it is a prime element if and only if the ideal (x) is maximal in $\mathbb{Z}$ if and only if $x = \pm p$ for a prime $p \in \mathbb{N}$.
(b) In the polynomial ring $A[X]$ any element of the form $uX + b$ with $u \in A^\times$ and $b \in A$ is an irreducible element (by degree reasons), but these elements are prime if and only if A is an integral domain (because $A[X]/(uX + b) \cong A$).

1.5.5. Proposition. — *Let A be an integral domain, then any prime element is an irreducible element.*

Proof. — See [**Bos18**, 2.4, Oss. 5] or [**Coh03**, 10.2]. □

1.5.6. Remark. — The previous result does not hold if A is not an integral domain. Let for example $A = \mathbb{Z}_6 := \mathbb{Z}/(6)$, where $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$, hence A is not a domain. We have that $(\overline{2})$ is a maximal ideal (as $\mathbb{Z}_6/(\overline{2}) \cong \mathbb{Z}_2$ is a field), hence $\overline{2}$ is a prime element in $\mathbb{Z}_6$. But $\overline{2} = \overline{2} \cdot \overline{4}$ and $\overline{2}$ and $\overline{4}$ are non-units, hence $\overline{2}$ is prime but not irreducible.

1.5.7. Definition (UFD). — The ring A is said to be **factorial**, or a **factorial domain**, or a **unique factorization domain (UFD)** if it is a domain and every non-unit in $A \setminus \{0\}$ has a unique factorization up to order and units, *i.e.* for any $x \in A \setminus (\{0\} \cup A^\times)$ there are $u \in A^\times$ and irreducible elements $x_1, \dots, x_n \in A$ such that $x = ux_1 \cdots x_n$ and any two such factorizations can differ only for the the unit factors and the order of the irreducible factors (but their number and the irreducible factors appearing in the two factorizations are the same).

1.5.8. Remark. — (a) If $A = K$ is a field, then any element is either zero or a unit. Then $K \setminus (\{0\} \cup K^\times) =$ and K is trivially a factorial domain.
(b) If A is a (unitary) subring of a factorial domain B, then A is not necessarily factorial, for example for any domain is a unitary subring of its field of fractions (see 1.8, v).

1.5.9. Proposition. — *Let A be a factorial domain and let $x \in A$, then x is a prime element if and only if x is an irreducible element.*

Proof. — See [**Bos18**, 2.4, Prop. 10] or [**Coh03**, 10.2.1]. □

1.5.10. Proposition. — *If A is a factorial domain with field of fractions*[4] *$K_A = \mathrm{qf}(A)$, and $f \in A[X]$, then f is irreducible in $A[X]$ if and only if f is irreducible as an element of $K_A[X]$.*

1.5.11. Remark. — In the situation above we note that any $F \in K_A[X]$ can be written as $F = \frac{1}{a} f$ with $f \in A[X]$ and $a \in A \setminus \{0\}$, then F is irreducible in $K_A[X]$ if and only if f is irreducible in $A[X]$.

4. See 1.8, v): $K = \mathrm{qf}(A) = \{\frac{u}{v} \mid u, v \in A, v \neq 0\}$ where, since A is a domain, $\frac{u}{v} = \frac{s}{t}$ in $K \Leftrightarrow ut = vs$ in A.

1.5.12. Proposition (Gauß Theroem). — *Let A be a commutative unitary ring. If A is factorial then $A[X]$ is factorial too.*

Proof. — See [**Lan02**, IV, §2, Thm. 2.3], [**Bos18**, 2.7, Prop. 1] or [**KR00**, 1.2.12]. □

1.5.13. Definition (PID). — The ring A is said to be **principal**, or a **principal domain**, or a **principal ideal domain (PID)** if it is a domain and every ideal of A is principal, *i.e.* if I is an ideal of A then $I = (x)$ for some $x \in A$.

1.5.14. Proposition. — *Let A be a principal domain and let $x \in A$ be a non-zero non-unit element. Then the following facts are equivalent:*

i) *x is irreducible.*
ii) *x is prime.*
ii) *(x) is a maximal ideal of $\mathbb{Z}$.*

Proof. — See [**Bos18**, 2.4, Prop. 6]. □

1.5.15. Definition (Euclidean Domain). — The ring A is said to be **Euclidean**, or a **Euclidean domain** if it is a domain and there exists a function $\delta\colon A \setminus \{0\} \longrightarrow \mathbb{N}$ such that for all $x, y \in A \setminus \{0\}$ the following properties hold:

a) If $x \mid y$ then $\delta(x) \leq \delta(y)$.
b) There exist elements $q, r \in A$ such that $y = qx + r$ and either $r = 0$ or $\delta(r) < \delta(y)$.

1.5.16. Example. — The following rings are Euclidean domains: (a) the ring of integers $\mathbb{Z}$ ($\delta = |\cdot|$), (b) the ring of Gaußian integers (subring of the complex plane) $\mathbb{Z}[i] \subseteq \mathbb{C}$ ($\delta = |\cdot|^2$), (c) any univariate polynomial ring $K[X]$ with coefficients in a field K ($\delta = \deg(\cdot)$).

1.5.17. Proposition. — *Let A a commutative unitary ring. If A is a PID then A is a UFD, and if A is a Euclidean domain then A is a PID.*

Proof. — See [**Coh03**, Cor. 10.2.3, Cor. 10.2.4] or [**Bos18**, 2.4, Prop. 2, cor. 11]. □

1.5.18. Remark. — None of the previous implications is an equivalence.

1.5.19. Critical Example. — Let $A = K[X,Y,Z,T]/(XT - YZ) = K[x,y,z,t]$, then A is a domain [5] and $x = \overline{X}$ is an irreducible element which is not prime. The ring A is not factorial.

1.5.20. Proposition. — *Let K be a field and let $f \in K[X]$ such that $\deg(f) = 2$ or 3, then f is irreducible if and only if f has no roots in K*

Proof. — By degree reason, such an f is reducible $\Leftrightarrow$ it has a degree one factor over K. □

1.5.21. Remark: non-zero prime ideals of $K[X]$. — (a) Let K be a field, then $K[X]$ is a Euclidean ring, hence a PID, hence a UFD. Let I be a proper non-zero ideal of $K[X]$ then necessarily $I = (f(X))$ for some $f(X) \in K[X]$ non-constant monic polynomial of positive degree (else $f(X) = 0$ or $f(X)$ is a unit). By 1.5.14 we then know that

$$(f(X)) \text{ is maximal } \Leftrightarrow (f(X)) \text{ is prime } \Leftrightarrow f(X) \text{ is irreducible.}$$

(b) Obviously, any polynomial of degree one of $K[X]$ is irreducible. Moreover K is an algebraically closed field if and only if the only irreducible polynomials of $K[X]$ are those of degree one.
(c) If K is not algebraically closed, the irreducible polynomials of degree two or three are exactly those which do not have a root in K. If $K = \mathbb{R}$ the irreducible polynomials are exactly those of degree one or those of degree two with negative discriminant. If $K = \mathbb{Q}$ there are irreducible polynomials of any degree, indeed $X^n - p$ is irreducible in $\mathbb{Q}[X]$ for any prime $p \in \mathbb{N}$ and any $n \in \mathbb{N}_+$ thanks to Eisenstein's Criterion (cf. for example [**Lan02**, IV,§3, Thm 3.1]).

1.5.22. Definition (Algebraic/Transcendental element). — Let K be a subfield of a field L, and let $a \in L$. We say that a is **algebraic over** K if there exists a non zero polynomial $f(X) \in K[X]$ such that $f(a) = 0$, else we say that a is **transcendental over** K. That is a is algebraic (respectively transcendental) over K if and only if the kernel of the **evaluation morphism** $\mathrm{ev}_a \colon K[X] \longrightarrow L$, $f \mapsto f(a)$ is a non-zero (resp. zero) ideal of the Euclidean domain $K[X]$. In this case its monic generator is called the **minimal polynomial of a over K**, it is the monic polynomial of $K[X]$ of least degree vanishing on a and it is necessarily irreducible.

5. Because $f = XT - YZ$ is irreducible in the factorial domain $K[X,Y,Z,T]$. Indeed f can be thought of as a degree one polynomial $f = aX + b$ in $A[X]$, with $A = K[Y,Z,T]$, factorial domain, $a = T$, $b = -YZ$ and $a \nmid b$ in A. Therefore f is irreducible by degree reason.

1.5.23. Remark: on the simple extension $K[X]/(f)$. — The residue class ring $K[X]/(f)$ is a K-algebra generated, as an algebra, by the element $x = \overline{X} = X + (f)$, the equivalence class of the indeterminate X. Hence, as in 1.2.4, we write $K[X]/(f) = K[x]$. If $f \in K$, then: $f = 0 \Leftrightarrow K[x] \cong K[X]$, while $f \in K \setminus \{0\} \Leftrightarrow K[x] = (0)$ (the zero ring). Assuming $\deg(f) = n > 0$, by performing euclidean division we get that for each polynomial $g \in K[X]$ there are two polynomials $q, r \in K[X]$ such that $g = qf + r$ and $\deg(r) < n$ or $r = 0$. Therefore, the generic element $g(x) \in K[x]$ can always be expressed as

$$g(x) = \overline{g(X)} = \overline{q(X)f(X) + r(X)} = \overline{q(X)f(X)} + \overline{r(X)} = r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$$

for some coefficients $a_0, a_1, \ldots, a_{n-1} \in K$ uniquely determined by $g(x)$. That is $K[x]$ is a K-vector space of dimension $n-1$ with K-basis $1, x, \ldots, x^{n-1}$:

$$K[x] = K \oplus Kx \oplus \cdots \oplus Kx^{n-1}.$$

If $K[x] = L$ is a field, which in turn is equivalent to f being irreducible, then $K[x]$ coincides with its field of fractions $K(x) := \mathrm{qf}(K[x])$ (see 1.8, v)) and we write $K[x] = K(x)$ to mean it. Obviously $x \in L$ is algebraic over K with minimal polynomial $LC(f)^{-1}f$, where $LC(f)$, the **leading coefficient of** f is the coefficient of the highest degree monomial in f.

1.5.24. Example. — (a) Let $L := \mathbb{R}[X]/(X^2+1) = \mathbb{R}[x] = \mathbb{R}(x) = \mathbb{R} \oplus \mathbb{R}x$ with x such that $x^2 = -1$. By the universal property of the quotient ring, a (unitary) ring homomorphism $L \to \mathbb{C}$ is uniquely determined by a (unitary) ring homomorphism $\Theta\colon \mathbb{R}[X] \to \mathbb{C}$ such that $(X^2+1) \subseteq \mathrm{Ker}(\Theta)$, and by the universal property of the polynomial ring, Θ is uniquely determined by the choice of $\Theta(X) \in \mathbb{C}$. Hence we see that, by the constraint $(X^2+1) \subseteq \mathrm{Ker}(\Theta)$, that is $\Theta(X)^2 + 1 = 0$ in $\mathbb{C}$, there are only two such choices: either $\Theta(X) = -i$ or $\Theta(X) = i$. Each one induces a field homomorphism $\theta\colon \mathbb{R}[x] \longrightarrow \mathbb{R}[i] = \mathbb{C}$ where $\theta(x) = -i$ in the former case and $\theta(x) = i$ in the latter case. In particular $\pm i \in \mathbb{C}$ are algebraic over $\mathbb{R}$ with minimal polynomial $X^2 + 1$.
(b) Let $L := \mathbb{Q}[X]/(X^3-2) = \mathbb{Q}[x] = \mathbb{Q}(x)$ with $x = \overline{X}$ such that $x^3 = 2$, and hence as $\mathbb{Q}$-vector space: $\mathbb{Q}(x) = \mathbb{Q} \oplus \mathbb{Q}x \oplus \mathbb{Q}x^2$. For instance, $x^{-1} = \frac{1}{2}x^2 \in \mathbb{Q}[x]$. As $X^3 - 2$ has only one real root, there is only one ring homomorphism $\mathbb{Q}(x) \longrightarrow \mathbb{R}$, the one determined by $x \mapsto \sqrt[3]{2}$, whose image is the smallest subfield of $\mathbb{Q}$ containing $\mathbb{Q}$ and $\sqrt[3]{2}$, that is

$$\mathbb{Q}(x) \cong \bigcap_{\{K \text{ subfield of } \mathbb{R} \,|\, K \supseteq \mathbb{Q} \cup \sqrt[3]{2}\}} K =: \mathbb{Q}(\sqrt[3]{2}).$$

The polynomial $X^3-2 \in \mathbb{Q}[X]$ thought of as an element of $\mathbb{Q}(\sqrt[3]{2})[X]$ splits as $X^3-2 = (X-\sqrt[3]{2})(X^2+\sqrt[3]{2}X+\sqrt[3]{4})$, with $X^2+\sqrt[3]{2}X+\sqrt[3]{4}$ irreducible in $\mathbb{Q}(\sqrt[3]{2})[X]$ (because it is a degree two polynomial with no roots in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$). Instead, there are exactly two homomorphisms from $\mathbb{Q}(x)$ to $\mathbb{C}$ corresponding to the two non-real roots $\sqrt[3]{2}e^{\pm\frac{2}{3}\pi i}$ of X^3-2, that is the two complex conjugate roots of the quadratic real polynomial $X^2+\sqrt[3]{2}X+\sqrt[3]{4}$, each giving rise to a field isomorphism to the corresponding smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and the given non-real root. In particular $\sqrt[3]{2}$, $\sqrt[3]{2}e^{\frac{2}{3}\pi i}$, and $\sqrt[3]{2}e^{-\frac{2}{3}\pi i}$ are algebraic over $\mathbb{Q}$ with minimal polynomial X^3-2. Note that the three fields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2}{3}\pi i})$, and $\mathbb{Q}(\sqrt[3]{2}e^{-\frac{2}{3}\pi i}) = \mathbb{Q}(\sqrt[3]{2}e^{\frac{4}{3}\pi i})$, though all isomorphic to $\mathbb{Q}(x)$ as abstract fields, are three distinct subsets of $\mathbb{C}$. Indeed one can show that $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2}e^{\pm\frac{2}{3}\pi i})$ and $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2}{3}\pi i}) \cap \mathbb{Q}(\sqrt[3]{2}e^{\frac{4}{3}\pi i}) = \mathbb{Q}$.

(c) Let $a \in \mathbb{C}$ be any element which is transcendental over $\mathbb{Q}$, that is $f(a) \neq 0$ for every $f \in \mathbb{Q}[X]$, for example $a = \pi \in \mathbb{R}$, $a = e \in \mathbb{R}$, or $a = i\pi \in \mathbb{C}$. Then the unique unitary ring homomorphism $\mathbb{Q}[X] \longrightarrow \mathbb{C}, X \mapsto a$ is injective and its image is the smallest subring of $\mathbb{C}$ containing both $\mathbb{Q}$ and a, that is $\mathbb{Q}[a]$. Hence $\mathbb{Q}[a] \cong \mathbb{Q}[X]$ and this ring homomorphism induces a field homomorphism of $\mathbb{Q}(X)$, the field of (univariate) rational functions with $\mathbb{Q}$-coefficients, with $\mathbb{Q}(a)$ the smallest subfield of $\mathbb{C}$ (or of $\mathbb{R}$ if $a \in \mathbb{R}$) containing both $\mathbb{Q}$ and a.

(d) Let $K := \mathbb{Q}(X)$ and let Y an indeterminate over K. Then $Y^2 - X \in K[Y]$ is irreducible in $K[Y] = \mathbb{Q}(X)[Y]$. Indeed X is not a square in $\mathbb{Q}(X)$, else there exist $u(X), v(X) \in \mathbb{Q}[X]$, with $v \neq 0$ such that $X = \frac{u^2}{v^2}$ in $\mathbb{Q}(X) = \mathrm{qf}(\mathbb{Q}[X])$. By definition of equality in the field of fraction of a domain, this gives $v(X)^2X = u(X)^2$ in the factorial domain $\mathbb{Q}[X]$. But this is impossible by the uniqueness of the factorization into irreducible elements in $\mathbb{Q}[X]$ because in the left hand side the irreducible factor X appears an odd number of times while it appears an even number of times in the right hand side. Therefore $Y^2 - X$ is irreducible as claimed and the residue class ring $L = K[Y]/(Y^2-X) = K[y] = \mathbb{Q}(X)[y] = \mathbb{Q}(X) \oplus \mathbb{Q}(X)y = \mathbb{Q}(X)(y)$ is a field. A generic element α of this field can be represented in a unique way in the form $\alpha = \frac{u_0}{v_0} + \frac{u_1}{v_1}y$ where $u_i, v_i \in \mathbb{Q}[X]$ are monic polynomials such that and $v_0v_1 \neq 0$ and $\mathrm{MCD}(u_i, v_i) = 1$. Hence we can also write $\alpha = \frac{a_0+a_1y}{A}$ where $a_0, a_1, A \in \mathbb{Q}[X]$ are monic polynomial such that $A \neq 0$ and $\mathrm{MCD}(a_0, a_1, A) = 1$. As $y^2 = X$, we could could abusively write $y = \sqrt{X}$ and consequently $L = \mathbb{Q}(X)(\sqrt{X}) = \mathbb{Q}(\sqrt{X})$, indeed $X = (\sqrt{X})^2 \in \mathbb{Q}(\sqrt{X})$, hence $\mathbb{Q}(X) \subseteq \mathbb{Q}(\sqrt{X})$, though this notation could be misleading sometimes.

(e) As $-X$ is not a square in $\mathbb{Q}(X)$ too (be the same argument above), we can also consider the field $\mathbb{Q}(X)[Y]/(Y^2+X) = \mathbb{Q}(\sqrt{-X})$.

1.6. Nilpotent elements, nilradical, reduced ring

1.6.1. Definition. — An element a of a ring A is **nilpotent** if a power of it vanishes, *i.e.* there exists $n \in \mathbb{N}_+$ such that $a^n = 0$ in A.

1.6.2. Definition. — The set of all nilpotent elements of A is an ideal of A and it is called the **nilradical**, $\mathrm{Nil}(A)$, of A. It coincides with the intersection of all minimal primes of (0): $\mathrm{Nil}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Min}((0))} \mathfrak{p}$ (cf. [**AM69**, Ch. 1]).

1.6.3. Definition. — A is said to be a **reduced** ring if it has no nonzero nilpotent elements, *i.e.* $\mathrm{Nil}(A) = (0)$. The ring $A_{\mathrm{red}} := A/\mathrm{Nil}(A)$ is reduced.

1.6.4. Remark: the nilradical of a polynomial ring. — Let A be any unitary commutative ring, then $\mathrm{Nil}(A[X_1, \ldots, X_n]) = \mathrm{Nil}(A)[X_1, \ldots, X_n]$, that is: any polynomial, in n indeterminates, whose coefficients are nilpotent elements of A, is a nilpotent polynomial, and conversely if a polynomial is nilpotent then its coefficients must all be nilpotent elements in A.

1.6.5. Remark: units of $A[X_1, \ldots, X_n]$. — It follows, considering degrees, that there is a group isomorphism $A[X_1, \ldots, X_n]^\times \cong A^\times \times ((X_1, \ldots, X_n) \cap \mathrm{Nil}(A)[X_1, \ldots, X_n])$. such that $f \mapsto (f(0, \ldots, 0), f(X_1, \ldots, X_n) - f(0, \ldots, 0))$.

1.7. Quotient ideals and saturation

1.7.1. Definition. — The **quotient ideal** of two ideals I and J of A is defined as

$$(I : J) = \{a \in A \mid aJ \subseteq I\}.$$

In case I or J, or both, is a principal ideal (a) with $a \in A$, we simply write $(I : a) := (I : (a))$, $(a : J) := ((a) : J)$ and $(a : b) := ((a) : (b))$.

1.7.2. Remark. — The definition makes sense also when $J = S$ is just any subset of A. In that case, it is easy to show that $(I : S)$ is an ideal of A, as it is when J is an ideal (cf. below).

1.7.3. Remark. — Note that we always have $(I : 1) = (I : A) = I$, $(1 : J) = (A : J) = A$, $(I : 0) = A$, while $(0 : J)$ is the so called **annihilator** of J [6].

6. If A is a domain and $J \neq 0$, then $(0 : J) = (0)$.

1.7.4. Properties of the quotient ideal. —

a) $(I : J)$ *is an ideal of* A*;*

b) $(I : J) = A \Leftrightarrow J \subseteq I$*;*

c) $I \subseteq (I : J)$*;*

d) $(I : J)J \subseteq I$*;*

e) $((I_1 : I_2) : I_3) = (I_1 : I_2I_3) = ((I_1 : I_3) : I_2)$*;*

f) $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$*;*

g) $(I : \Sigma J_i) = \bigcap_i (I : J_i)$*;*

h) $I_1 \subseteq I_2 \Rightarrow (I_1 : J) \subseteq (I_2 : J)$ *and* $J_1 \subseteq J_2 \Rightarrow (I : J_1) \supseteq (I : J_2)$*;*

i) if J *is an ideal and* $\mathfrak{p}$ *is a prime ideal, then* $(\mathfrak{p} : J) = A$ *if* $J \subseteq \mathfrak{p}$ *or* $(\mathfrak{p} : J) = \mathfrak{p}$ *if* $J \nsubseteq \mathfrak{p}$*.*

Proof. — For *a)* to *g)* we refer **[AM69]**.

h) It's straightforward.

i) If $J \subseteq \mathfrak{p}$ then $(\mathfrak{p} : J) = A$ by *a)*. Let $J \nsubseteq \mathfrak{p}$, then there exists $j \in J$ such that $j \notin \mathfrak{p}$. By *b)* $\mathfrak{p} \subseteq (\mathfrak{p} : J)$, let then $a \in (\mathfrak{p} : J)$ that is $aJ \subseteq \mathfrak{p}$. In particular $aj \in \mathfrak{p}$, as $\mathfrak{p}$ is a prime ideal and $j \notin \mathfrak{p}$ it is $a \in \mathfrak{p}$. □

1.7.5. Saturation wrt an ideal. — Let I and J be two ideals of A, then

$$(I : J^n) \subseteq (I : J^{n+1}) \text{ for any } n \in \mathbb{N} \qquad (*)$$

thus $(I : J^\infty) := \bigcup_{n\in\mathbb{N}} (I : J^n) = \{a \in A \mid aJ^n \in I \text{ for some } n \in \mathbb{N}_+\}$ is an ideal of A, which is called the **saturation of** I **with respect to** J. It directly follows by definition that $(I : J^\infty) = A \Leftrightarrow 1 \in (I : J^\infty) \Leftrightarrow J^n \subseteq I$ for some $n \in \mathbb{N}_+$.

1.7.6. Remark (Strictly ascending chain). — We note a special property of the chain $(*)$ defining $(I : J^\infty)$. If $(I : J^N) = (I : J^{N+1})$ for some $N \in \mathbb{N}$ then the chain stays stationary after $(I : J^N)$, that is $(I : J^t) = (I : J^N)$ for all $t \in \mathbb{N}$ such that $t \geq N$.

Proof. — Indeed, the claim follows by induction on $n \geq N$, where $n = N$ is the base case and the inductive step goes as follows: if $n \geq N$ and $(I : J^n) = (I : J^{n+1})$ then $(I : J^{n+1}) = (I : J^{n+2})$, which is true because $(I : J^{n+1}) \subseteq (I : J^{n+2})$ holds in general, while if $a \in (I : J^{n+2})$, that is $aJ^{n+2} \subseteq I$, then, for any choice of $j \in J$ we have $ajJ^{n+1} \subseteq I$, hence $aj \in (I : J^{n+1}) = (I : J^n)$ for all $j \in J$. This means $ajJ^n \subseteq I$ for all $j \in J$, that is $aJ^{n+1} \subseteq I$, and therefore $a \in (I : J^{n+1})$ as required. □

It follows that, if A is a Noetherian ring, then $(I : J^\infty) = (I : J^N)$ for some $N \in \mathbb{N}_+$ and the previous ideals in the chain, $(I : J^n)$ with $n < N$, are strictly increasing from $(I : J)$ to $(I : J^\infty)$ in the nontrivial cases $J \not\subseteq I$ (otherwise $(I : J)$ is already (1)) and $I \subsetneq (I : J)$ (otherwise $(I : J^\infty) = (I : J) = I$).

1.8. Rings of fractions

For the construction of **rings of fractions** of commutative unitary rings A with respect to multiplicative systems S (*i.e.* $S \subseteq A$ such that $1 \in S$ and $S \cdot S \subseteq S$) and their properties, we refer to [**AM69**, Ch. 3], [**Sha90**, Ch. 5], [**KR00**, 3.5.A] and [**Eis95**, Ch. 2]:

$$A_S = S^{-1}A = A[S^{-1}] := (A \times S)/\sim \;\cong\; A[X_s \mid s \in S]/(\{sX_s - 1 \mid s \in S\}) \;\cong\; \varinjlim_{f \in S} A_f.$$

We just point out that

i) If $a, b \in A$ and $s, t \in S$, then $\frac{a}{s} = \frac{b}{t}$ in $A_S \;\Leftrightarrow\; u(ta - sb) = 0$ in A for some $u \in S$. The canonical ring homomorphism $\chi_S \colon A \longrightarrow S^{-1}A$, $a \mapsto \frac{a}{1}$ is *universal* among the unitary ring homomorphisms $f \colon A \longrightarrow B$ such that $f(S) \subseteq B^\times$. In general, it is neither injective nor surjective, though it is a unitary ring epimorphism, also called "essentially surjective", *i.e.* if $u, v \colon S^{-1}A \longrightarrow B$ are two (parallel) unitary ring homomorphisms such that $u \circ \chi_S = v \circ \chi_S$ then $u = v$. The kernel of χ_S is the ideal of A given by $\mathrm{Ker}(\chi_S) = \{a \in A \mid sa = 0 \text{ for some } s \in A\} = \bigcup_{s \in S}(0 : s)$. Note that, in particular, $\mathrm{Ker}(\chi_S) \subseteq \mathrm{Zdv}(A)$ for every multiplicative system S such that $0 \notin S$

ii) We have $A_S = 0$ if and only if S contains a nilpotent element (*i.e.* $s \in S$ such that $s^n = 0$, in A, for some $n \in \mathbb{N}_+$). Hence, in particular, $f \in A$ is nilpotent if and only if the fraction ring $A_f = A\left[\frac{1}{f}\right] = 0$.

iii) We have a completely general commutation relation between taking quotient wrt an ideal I and forming fractions wrt a multiplicative system S: $(A/I)_{\overline{S}} \cong A_S/I_S$.

iv) The canonical ring homomorphism $A \longrightarrow A_S$ induces a correspondence (via extension-contraction described in 1.1.11.5) such that: every ideal of A_S is extended from an ideal of A, if I is an ideal of A then $I^{ec} = \bigcup_{s \in S}(I : s)$ (hence $I^e = (1) \Leftrightarrow I \cap S \neq \emptyset$), $I = I^{ec}$ if and only if no element from S becomes zerodivisor in the quotient ring A/I, prime ideals of A_S bijectively correspond to prime ideals of A avoiding S.

v) For any ring, $\Sigma_0 := A \setminus \mathrm{Zdv}(A)$ is a multiplicative system, and the corresponding ring of fraction is called the **total ring of quotients** of A and it is denoted

$$Q_0(A) := (\Sigma_0)^{-1}A = (A \setminus \mathrm{Zdv}(A))^{-1}A.$$

Note that Σ_0 is the biggest multiplicative system S of A such that $\chi_S \colon A \longrightarrow S^{-1}A$ is injective, and that for any multiplicative system S' such that $S' \subseteq \Sigma_0$, *i.e.* S is "zerodivisor free", we have a unitary ring injection $A_{S'} \hookrightarrow Q_0(A)$. Moreover, if S is such a "zerodivisor free" multiplicative system of A then equality in $S^{-1}A$ take the usual simplified appearance $\frac{a}{s} = \frac{b}{t}$ in $A_S \Leftrightarrow ta = sb$ in A. If A is a domain, then $\Sigma_0 = A \setminus \{0\}$, and we define

$$\mathrm{qf}(A) := Q_0(A) = A_{\Sigma_0} = A[\Sigma_0^{-1}] = (A \setminus \{0\})^{-1}A,$$

which is always a field, called **field of fractions** (or **field of quotients**) of the domain A. For example: if A is a domain, then $\mathrm{qf}(A[X_1, \ldots, X_n]) = K_A(X_1, \ldots, X_n)$ is the **field of rational functions** in n indeterminates with coefficients in the field of fractions $K_A = \mathrm{qf}(A)$ of A.

vi) If $f \in A$ then $S := \{f^n \mid n \in \mathbb{N}\}$ is a multiplicative system of A. We define

$$A_f := A_S = A[f^{-1}] \cong A[X]/(fX - 1).$$

We have: $A_f = (0) \Leftrightarrow f$ is nilpotent.

vii) If $\mathfrak{p}$ is a prime ideal of A, then $S := A \setminus \mathfrak{p}$ is a multiplicative system of A. The **localization** of A at the prime $\mathfrak{p}$ is defined to be the ring of fractions

$$A_{\mathfrak{p}} := A_S = A[(A \setminus \mathfrak{p})^{-1}] = \varinjlim_{f \notin \mathfrak{p}} A_f.$$

The ring $A_{\mathfrak{p}}$ is said to be **local** because $\mathfrak{p}A_{\mathfrak{p}}$ is its only maximal ideal. The quotient ring $\kappa(\mathfrak{p}) := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong (A/\mathfrak{p})_{(\overline{0})} = \mathrm{qf}(A/\mathfrak{p})$ is therefore a field, called the **residue field** of the prime $\mathfrak{p}$, it is isomorphic to the field of fractions of the domain $A/\mathfrak{p}$.

viii) Note that, for a maximal ideal $\mathfrak{m}$ of A we have $\kappa(\mathfrak{m}) \cong A/\mathfrak{m}$ because the quotient is already a field; while, to the other extreme, if $\mathfrak{p}$ is minimal prime of A (*i.e.* $\mathfrak{p} \in \mathrm{Min}((0))$), then $\mathfrak{p}A_{\mathfrak{p}} = \mathrm{Nil}(A_{\mathfrak{p}})$ (because $\mathfrak{p}A_{\mathfrak{p}}$ becomes the only minimal prime of $\frac{0}{1}$ in $A_{\mathfrak{p}}$), and the residue field becomes $\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = (A_{\mathfrak{p}})_{\mathrm{red}} \cong \mathrm{qf}(A/\mathfrak{p})$. In case, moreover, $\mathfrak{p}$ is a minimal prime such that $\mathrm{Nil}(A_{\mathfrak{p}}) = (0)$, then $\kappa(\mathfrak{p}) = A_{\mathfrak{p}}$.

1.9. Radical of an ideal

1.9.1. Definition. — The **radical** of an ideal I is defined as

$$\sqrt{I} := \{a \in A \mid \text{there exists } n \in \mathbb{N}_+ \text{ such that } a^n \in I\}.$$

1.9.2. Remark. — Obviously, the radical of the zero ideal coincides with the set of all nilpotent elements in the ring: $\mathrm{Nil}(A) = \sqrt{(0_A)}$.

1.9.3. Proposition (Radical membership test). — *Let I be an ideal of A, let $A[X]$ be the univariate polynomial ring with coefficients in A and indeterminate X, and let $a \in A$. Then*

$$a \in \sqrt{I} \;\Leftrightarrow\; 1 \in (I,\, aX - 1) \subseteq A[X].$$

Proof. — See, for example, [**KR00**, 3.5.15]. □

1.9.4. Radical ideals. — An ideal I is said to be a **radical ideal** if $I = \sqrt{I}$, the family of all such ideals is closed under intersection (as it follows by f) of 1.9.5 e) and f) below).

1.9.5. Radical properties. —

a) $\sqrt{I}$ *is an ideal of* A*;*
b) $I \subseteq \sqrt{I}$*;*
c) $I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$
d) $\sqrt{\sqrt{I}} = \sqrt{I}$*;*
e) $I = \sqrt{J} \Rightarrow I = \sqrt{I}$*;*
f) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ *and* $\sqrt{I^n} = \sqrt{I}$ *for each* $n \in \mathbb{N}_+$*;*
g) $\sqrt{I} = (1) \Leftrightarrow I = (1)$*;*
h) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$*;*
i) If $\mathfrak{p}$ *is a prime ideal of* A *and* $n \in \mathbb{N}_+$ *then* $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$*;*
j) $\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I,\, \mathfrak{p} \text{ prime}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in Min(I)}$*;*
k) If $\varphi\colon A \longrightarrow B$ *is any (unitary) ring homomorphism and* J *is an ideal of* B*, then*

$$\varphi^{-1}(\sqrt{J}) = \sqrt{\varphi^{-1}(J)};$$

l) If S *is a multiplicative system of* A*, then* $\sqrt{I_S} = (\sqrt{I})_S$ *in the ring of fractions* A_S*;*
m) If A *is Noetherian, then* I *contains a power of its radical;*

n) If I is an ideal of A, then $\sqrt{I} = \pi^{-1}(\sqrt{(\overline{0})})$ where $\pi\colon A \longrightarrow A/I$ is the canonical projection on the quotient ring, i.e. $\sqrt{I} = \pi^{-1}(Nil(A/I))$;

o) If $X_1, \ldots, X_n$ are indeterminates over A and I is an ideal of A, then

$$\sqrt{I[X_1, \ldots, X_n]} = \sqrt{I}A[X_1, \ldots, X_n].$$

p) If K is a field, L is an extension field of K, $X_1, \ldots, X_n$ are indeterminates over K, and I is an ideal of $K[X_1, \ldots, X_n]$, then

$$\sqrt{IL[X_1, \ldots, X_n]} = (\sqrt{I})L[X_1, \ldots, X_n].$$

Proof. — See [**AM69**], [**Eis95**, p. 33], and [**Kun85**, Ch. III, Rules 4.8 c)]. Part *o*) can be easily proven, by induction on n, using the canonical isomorphism $A[X]/IA[X] \cong (A/I)[X]$, together with *n*) and the fact that, if R is any commutative unitary ring and $f \in R[X]$, then f is nilpotent in $R[X]$ if and only if its coefficients are nilpotent in R ([**AM69**, Ch. 1, Ex. 2]). Property *p*) is a well known pleasant arithmetic feature of the radical operation but its full proof is non-trivial, see for example [**KR00**, ??] for a proof in case $L = \overline{K}$ an algebraic closure of K. □

1.9.6. Remark. — We can summarize general properties of operations on ideals with respect to any ring homomorphism, in terms of extension-contraction notation (1.1.11.2), as follows ([**AM69**, Ch. 1, Ex. 1.18]):

$$\begin{array}{cc}
(I_1 + I_2)^e = I_1^e + I_2^e & (J_1 + J_2)^c \supseteq J_1^c + J_2^c \\
(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e & (J_1 \cap J_2)^c = J_1^c \cap J_2^c \\
(I_1 I_2)^e = I_1^e I_2^e & (J_1 J_2)^c \supseteq J_1^c J_2^c \\
(I_1 : I_2)^e \subseteq (I_1^e : I_2^e) & (J_1 : J_2)^c \subseteq (J_1^c : J_2^c) \\
\sqrt{I}^e \subseteq \sqrt{I^e} & \sqrt{J}^c = \sqrt{J^c}
\end{array}$$

1.9.7. Proposition. —

a) if A is a Noetherian ring, $(I : J^\infty) = A \Leftrightarrow J \subseteq \sqrt{I}$;

b) Let I, J be ideals of A, then $\sqrt{(I : J)} \subseteq \sqrt{(I : J^\infty)} \subseteq (\sqrt{I} : J)$ and, if A is a Noetherian ring, $\sqrt{(I : J^\infty)} = (\sqrt{I} : J)$.

c) Let I, J be ideals of A with I a radical ideal, then $(I : J)$ is a radical ideal itself and moreover $(I : J^\infty) = (I : J) = (I : \sqrt{J})$;

Proof. — *a*) It follows from *j*) of *1.9.5* .

b) The first inclusion follows from $(I : J) \subseteq (I : J^\infty)$ and monotony of taking radicals (see above). For the second inclusion, if $a \in \sqrt{(I : J^\infty)}$ there exists $t \in \mathbb{N}_+$ such that $a^t J^k \subseteq I$ for some $k \in \mathbb{N}_+$. Hence, as we can assume t great enough ($t \geq k$) if needed, for any $j \in J$, $(aj)^t = a^t j^t \in a^t J^t \subseteq a^t J^k \subseteq I$, which yields $aJ \subseteq \sqrt{I}$ and eventually $a \in (\sqrt{I} : J)$. Assume now, that A is a Noetherian ring and that $a \in (\sqrt{I} : J)$, hence $aJ \subseteq \sqrt{I}$. As aJ is an ideal of A contained in $\sqrt{I}$, then from *j*) of *1.9.5* a power of it, say $(aJ)^t$ with $t \in \mathbb{N}_+$, is contained in I; in particular $a^t J^t \subseteq I$, therefore $a \in \sqrt{(I : J^\infty)}$.
c) From the above *b*), we have in general that $(I : J) \subseteq \sqrt{(I : J)} \subseteq (\sqrt{I} : J) = (I : J)$ where the last equality holds for I is radical, hence $\sqrt{(I : J)} = (I : J)$ in this case. The first equality in the second statement is then clear $(I : J) \subseteq (I : J^\infty) \subseteq \sqrt{(I : J^\infty)} \subseteq (\sqrt{I} : J) = (I : J) \Rightarrow (I : J^\infty) = (I : J)$. For the second one, as $\sqrt{J} \supseteq J$ we have $(I : \sqrt{J}) \subseteq (I : J)$. Let now $a \in (I : J)$, that is $aJ \subseteq I$. If $b \in \sqrt{J}$ there exists $t \in \mathbb{N}_+$ such that $b^t \in J$, hence $(ab)^t = a^t b^t = a(a^{t-1} b^t) \in aJ \subseteq I$ with I radical, hence $ab \in I$. As this holds true for any $b \in \sqrt{J}$ we get $(I : J) \subseteq (I : \sqrt{J})$, and therefore $(I : J) = (I : \sqrt{J})$. □

1.10. Primary ideals

1.10.1. Proposition-Definition. — *A proper ideal Q of A is said to be* **primary** *if whenever $xy \in Q$, for some $x, y \in A$, then $x \in Q$ or $y \in \sqrt{Q}$. The radical of a primary ideal Q is always a prime ideal and it is minimal for this property.*

Proof. — Indeed, if $xy \in \sqrt{Q}$ then $(xy)^n = x^n y^n \in Q$ for some $n \in \mathbb{N}_+$; if, say, $x \notin \sqrt{Q}$ then $x^n \notin Q$ (for all $n \in \mathbb{N}_+$), but as Q is primary it must then be $y^n \in \sqrt{Q}$, that is $(y^n)^m = y^{nm} \in Q$ for some $m \in \mathbb{N}_+$. Hence $y \in \sqrt{Q}$, and $\sqrt{Q} = \mathfrak{p}$ is a prime ideal. Moreover, as it follows from *1.9.5 i*), if $\mathfrak{q}$ is prime ideal such that $\mathfrak{q} \supseteq Q$ then $\mathfrak{q} \supseteq \mathfrak{p}$. □

We say then that Q is a **$\mathfrak{p}$-primary ideal**, with $\mathfrak{p}$ prime, to mean that $\sqrt{Q} = \mathfrak{p}$.

1.10.2. Remark. — Note that, if A is a Noetherian ring, then any such Q is in between two powers of the prime ideal $\mathfrak{p}$; but this is only a necessary condition, indeed it holds for any ideal having prime radical.

1.10.3. Lattice property. — The family of all $\mathfrak{p}$-primary ideals is stable under finite intersections.

1.10.4. Example. — (a) In $K[X,Y]$, (XY, X^2, Y^3) and (X^3, Y^5) are two different (X,Y)-primary ideals. (b) In $K[\underline{X}]$, the ideals $\mathfrak{p}_i := (X_1, \cdots, X_i)$ are prime and all their positive powers $\mathfrak{p}_i^t$ are $\mathfrak{p}_i$-primary.

1.10.5. Example. — (a) One can show that if $\sqrt{I} = \mathfrak{M}$ is a maximal ideal then I is a $\mathfrak{M}$-primary ideal, and that any ideal J, of a Noetherian ring A, such that $\mathfrak{M}^r \subseteq J \subseteq \mathfrak{M}$, for some positive integer r, is a $\mathfrak{M}$-primary ideal. (b) Note that not even powers of (non maximal) prime ideals are necessarily primary ideals ([**AM69**]), though this is true in Euclidean domains (such as $A = \mathbb{Z}$, $K[X]$ with K a field, ...).

1.10.6. Proposition. — *Let Q, J be ideals of A with Q a $\mathfrak{p}$-primary ideal, then*

a) $(Q : J) = A$ if $J \subseteq Q$ or $(Q : J)$ is a $\mathfrak{p}$-primary ideal if $J \not\subseteq Q$. If, moreover, $J \not\subseteq \mathfrak{p}$, then $(Q : J) = Q$;

b) $(Q : J^\infty) = A$ if $J^k \subseteq Q$ for some $k \in \mathbb{N}_+$ or $(Q : J^\infty)$ is a $\mathfrak{p}$-primary ideal if $J^k \not\subseteq Q$ for every $k \in \mathbb{N}_+$. If, moreover, $J \not\subseteq \mathfrak{p}$, then $(Q : J) = Q$;

c) If A is Noetherian, then $(Q : J^\infty) = A$ if $J \subseteq \mathfrak{p}$ or $(Q : J^\infty) = Q$ if $J \not\subseteq \mathfrak{p}$.

Proof. — If $J \subseteq Q$ then $(Q : J) = A$ by *1.7.4 a)*. Let $J \not\subseteq Q$, then there exists $j \in J$ such that $j \notin Q$, and let $a \in (Q : J)$ that is $aJ \subseteq Q$. In particular $aj \in Q$, which is $\mathfrak{p}$-primary, as $j \notin Q$ then $a \in \mathfrak{p}$; hence $Q \subseteq (Q : J) \subseteq \mathfrak{p} \;\Rightarrow\; \mathfrak{p} = \sqrt{Q} \subseteq \sqrt{(Q : J)} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p} \;\Rightarrow\; \sqrt{(Q : J)} = \mathfrak{p}$. Let us check that $(Q : J)$ is indeed primary: let $xy \in (Q : J)$ and $y \notin \mathfrak{p} = \sqrt{(Q : J)}$, then $xyz = (xz)y \in Q$ for any $z \in J$, as Q is $\mathfrak{p}$-primary, we find $xz \in Q$ for any $z \in J$. Therefore $x \in (Q : J)$ and $(Q : J)$ is a primary ideal. For the last statement: let $j \in J \setminus \mathfrak{p}$ and let $a \in A$ such that $aJ \subset Q$. Then $aj \in Q \setminus \mathfrak{p}$, as Q is $\mathfrak{p}$-primary and $j \notin \mathfrak{p}$ we get $a \in Q$, and hence $(Q : J) = Q$. □

1.11. Primary decomposition

For what follows, refer to [**AM69**], [**Sha90**, Ch. 4], or [**KR00**, Tutorial 43] and [**KR05**, 5.6.B].

1.11.1. Theorem (Primary decomposition in Noetherian rings). — *Let A be a Noetherian ring and let I be an ideal of A. Then:*

i) I has a **primary decomposition**, *that is I is an intersection of finitely many $\mathfrak{p}_i$-primary ideals Q_i, i.e. $I = Q_1 \cap \cdots \cap Q_s$, where: $\mathfrak{p}_i = \sqrt{Q_i}$;*

ii) any decomposition as in i) can be rearranged into a **minimal primary decomposition**, *that is $I = Q_1 \cap \cdots \cap Q_r$, where $\mathfrak{p}_i = \sqrt{Q_i}$, with $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$ and none of the Q_i is redundant, that is $Q_i \not\supseteq \bigcap_{\{j \neq i\}} Q_j$ for any $i = 1, \cdots, r$;*

iii) the number of primary ideals Q_i, the prime ideals $\mathfrak{p}_i$, as well as those primary ideals Q_j whose radical $\mathfrak{p}_j$ belong to the minimal prime ideals of I, of a minimal primary decomposition as in ii) are uniquely determined by the ideal I.

1.11.2. Associated prime ideals of an ideal. — If I is an ideal of A, then its **associated prime** are the radicals of primary ideals of any minimal primary decomposition of I. The set of the associated primes of $I = Q_1 \cap \cdots \cap Q_r$ is denoted $\mathrm{Ass}(I)$ and, if A is a Noetherian ring, it can be shown that ([**AM69**, Ch. 4, Prop. 4.6; Ch. 7, Prop. 7.17])

$$\emptyset \neq \mathrm{Min}(I) \subseteq \mathrm{Ass}(I) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\} = \{\mathfrak{p} \text{ prime } \mid \mathfrak{p} = (I : a) \text{ for some } a \in A\}.$$

Those associated primes which are minimal are called **isolated prime** of I, all the others are called **embedded prime** of I. If I is a radical ideal then it has no embedded primes ([**AM69**, Ch. 4, Ex. 2]).

1.11.3. Example. — Observe that, in $K[X, Y]$, $I := (XY, Y^2)$ has, at least, two distinct minimal primary decompositions: $I = (X, Y^2) \cap (Y)$, and $I = (X, Y)^2 \cap (Y)$. In both cases the associated primes are (X, Y) and (Y), with (Y) isolated prime and (X, Y) embedded (for it is not minimal). Clearly, the (X, Y)-primary "component" is not uniquely determined.

1.11.4. Primary decomposition for principal ideals in UFD. — If A is a **unique factorization domain** (UFD) and $a = u a_1^{n_1} \cdots a_k^{n_k} \in A$ with $u \in A$ invertible and a_i irreducible, then $(a) = (a_1^{n_1} \cdots a_k^{n_k}) = (a_1)^{n_1} \cap \cdots \cap (a_k)^{n_k}$ is a ("the") minimal primary decomposition of (a). Clearly, there cannot be embedded components, all associated primes are minimal.

1.12. Real and Semireal Rings and Ideals.

For what follows see [**Kri64**], [**Coh03**, 8.6, 8.7, 8.8], [**Lan02**, XI, 2], [**BCR98**, Ch. 1], [**BPR06**] as well as [**Lam84**].

Let A be a commutative unitary nonzero ring.

1.12.1. Definition. — (a) The ring A is called **semireal** if $-1 \notin \Sigma A^{(2)}$.
(b) The ring A is called **real** (or **formally real**) if $a_1^2 + \cdots + a_t^2 = 0$, with $a_i \in A$, implies that each $a_i = 0$.

1.12.2. Definition. — Let I be an ideal of A.
(a) The ideal I of A is said to be **semireal** if the quotient ring A/I is semireal, that is -1 is not a sum of squares in A/I.
(b) The ideal I of A is said to be **real** if, for every $a_1, \ldots, a_n \in A$ we have $a_1^2 + \cdots + a_n^2 \in I \Rightarrow a_i \in I$ for each $i = 1, \ldots, n$.

1.12.3. Remark. — If A is a semireal ring, then it has characteristic 0.

Proof. — If A has characteristic $n \in \mathbb{N}$, $n \geq 2$, then $n = 1^2 + \cdots + 1^2 = 0$ (n summands). Therefore $-1 = \sum_{i=1}^{n1} 1^2$ in A. □

1.12.4. Remark. — (a) If A is a field: A is real $\Leftrightarrow$ A is semireal.
(b) It is straightforward to check that: I is a semireal (resp. real) ideal of the A if and only if the quotient ring A/I is semireal (resp. real).
(c) If $\mathfrak{m}$ is a maximal ideal of A: $\mathfrak{m}$ is real $\Leftrightarrow$ $\mathfrak{m}$ is semireal.
(d) The conditions defining reality and semireality are clearly invariant under rings isomorphism.
(e) Clearly real rings are semireal, but the converse is in general not the case. For example $\mathbb{Q}[X]/(X^2)$ and $\mathbb{R}[X_1, \ldots, X_n]/(X_1^2 + \cdots + X_n^2)$, for $n \geq 1$, are semireal but not real. The latter, with $n \geq 2$, being an example of a semireal integral domain which is not a real domain.
(f) If A is semireal, then no square can be equal to -1. Nonetheless, this is only a necessary condition. In $A = \mathbb{Z}/(6)$ no square equals -1 (as one can easily check directly), though A is not semireal: $\overline{1}^2 + \overline{2}^2 + \overline{5}^2 = \overline{0}$, whence $-\overline{1} = \overline{2}^2 + \overline{5}^2$ and therefore A is not a semireal ring. To better understand phenomena of this kind the concept of *level of a ring* (or "Stufe" in German) has been developed (see [**Lam84**]).
(g) Obviously, any subring of a real (respectively semireal) ring is still such.
(h) A cartesian product of two (or any of any, even not finite, cardinal number of) real rings, with coordinate-wise operations, as well as any polynomial ring (in any number of indeterminates) is a real ring.

1.12.5. Proposition. — *Let A and B two unitary commutative rings, and let $f\colon A \longrightarrow B$ a unitary ring homomorphism. then*

a) B semireal $\Rightarrow$ A semireal.

b) If f happens to be injective, B real $\Rightarrow$ A real.

c) If A is real and S is a multiplicative system of A then $S^{-1}A$ real.

Proof. — See [**Lam84**, 2.2]. □

1.12.6. Remark. — In [**Lam84**, Rem. 2.2] the following are proven:

i) A is real if and only if A is reduced and all minimal primes of A are real.

ii) A is real if and only if A can be embedded into a direct product of real fields. Actually we have that $A \hookrightarrow \prod_{\mathfrak{p}\in \mathrm{Min}((0))} \mathrm{qf}(A/\mathfrak{p}) \cong \prod_{\mathfrak{p}\in \mathrm{Min}((0))} \mathrm{qf}(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}) \cong \prod_{\mathfrak{p}\in \mathrm{Min}((0))} A_{\mathfrak{p}}$. If A has only finitely many minimal prime ideals, as it is for any Noetherian ring, then A is a subring of a direct product of finitely many real fields.

iii) A is semireal if and only if one its minimal prime is semireal.

1.12.7. Example. — If A is a real ring (respectively semireal) and S is a nonempty set, then the A-algebra of all functions on S with value in A, with pointwise operations, $A^S = \mathcal{F}(S, A) := \{f \mid f\colon S \longrightarrow A\}$ is a real (respectively semireal) ring.

Proof. — Straightforward verification. Note also that $\mathcal{F}(S, A) = A^S = \prod_{s\in S} A$ is a product of real (respectively semireal) rings. □

1.12.8. Example. — (a) The rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $K[X_1, \ldots, X_n]$ with K a real field, as well as $A[X_1, \ldots, X_n]$ and any $S^{-1}A[X_1, \ldots, X_n]$ with A real, their ring products and subrings of them, as well as the rational function fields in any number of indeterminates $K(\{X_i \mid i \in I\})$ with K semireal/real are such.

(b) Any ring in which the square map p_2 is surjective (as any algebraically closed field is), as well as any positive characteristic ring, is not even semireal.

(c) The complex subfield $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2}{3}\pi i})$ is real, thought it is not a subfield of $\mathbb{R}$. Indeed it is isomorphic (cf. 1.5.24 (b)) to $\mathbb{Q}(\sqrt[3]{2})$, subfield of $\mathbb{R}$, and we noticed that for a ring being real/semireal is preserved under field isomorphisms.

(d) Let K be any field. Then, by 1.5.24 (d), (e) the indeterminate X is neither a square nor the opposite of a square, therefore the two residue class rings $K(\sqrt{\pm X}) := K(X)[Y]/(Y^2 \mp X) =$

$K(X) \oplus K(X)y$, with $y^2 = \pm X$ are fields. If moreover K is a real field, or equivalently $K(X)$ is real, then both fields $K(\sqrt{\pm X})$ are real too. Indeed, assume there exist $\alpha_i = \frac{a_{i0}+a_{i1}y}{A_i}$, with $a_{i0}, a_{i1}, A \in K[X]$ monic polynomials such that $A_i \neq 0$ and $\mathrm{MCD}(a_{i0}, a_{i0}, A_i) = 1$, such that $\alpha_1^2 + \cdots + \alpha_t^2 = 0$ in $K(\sqrt{\pm X})$. Then, clearing the denominators multiplying both sides by $(A_0 \cdots A_t)^2$ we get

$$(b_{10} + b_{11}y)^2 + \cdots + (b_{t0} + b_{t1}y)^2 = 0 \text{ in } K(\sqrt{\pm X}) \text{ where } bij = a_{ij} \prod_{k \neq i} A_k \in K[X].$$

Expanding out and grouping according to the powers of y we get

$$\sum_i b_{i0}^2 \pm X \sum_i b_{i0}^2 + 2\left(\sum_i b_{i0}b_{i1}\right) y = 0 \text{ in } K(\sqrt{\pm X}) \Leftrightarrow \begin{cases} \sum_i b_{i0}^2 \pm X \sum_i b_{i0}^2 = 0 \\ \sum_i b_{i0}b_{i1} = 0 \end{cases} \text{ in } K[X].$$

Since the first equation of the system gives $\sum_i b_{i0}^2 = \mp X \sum_i b_{i0}^2$ in $K[X]$, and K is real, if they are both not zero, as polynomials in X, the left hand side has even degree and the right hand side has odd degree. As $K[X]$ is a domain, we are thus left with $\sum_i b_{i0}^2 = \sum_i b_{i0}^2 = 0$ in $K[X]$, but as $K[X]$ is a real ring this implies $b_{ij} = 0$ for every $i = 1, \ldots, t$ and $j = 0, 1$. Hence we conclude that each α_i has to be zero and therefore $K(\sqrt{\pm X})$ are real fields.

1.13. Ordered Rings and Fields. Real-Closed Fields

We recall the standard definitions and notation about orders and preorders on a set.

1.13.1. Definition. — Let S be a set. (a) A **(partial) preorder** on S is a binary relation $\preceq$ on S which is *reflexive*, that is $s \preceq s$ for every $s \in S$, and *transitive*, that is for every $s_1, s_2, s_3 \in S$ if $s_1 \preceq s_2$ and $s_2 \preceq s_3$ then $s_1 \preceq s_3$. A **total preorder** is a preorder such that for every $s_1, s_2 \in S$ it is $s_1 \preceq s_2$ or $s_2 \preceq s_1$. If $\preceq$ is a preorder on S we write $s_2 \succeq s_1$ to mean $s_1 \preceq s_2$, and $s_1 \prec s_2$ to mean $s_1 \neq s_2$ and $s_1 \preceq s_2$. In particular it is $s \not\prec s$ for every $s \in S$.
A **preordered set** is a pair $(S, \preceq)$, where S is a set and $\preceq$ is a preorder on S. (b) A **(partial) order** on S is a (partial) preorder $\leq$ which is *antisymmetric*, that is for every $s_1, s_2 \in S$ if $s_1 \leq s_2$ and $s_2 \leq s_1$ then $s_1 = s_2$. An order is said to be **total** when it is a total preorder. The meaning of $s_2 \geq s_1$ and $s_1 < s_2$ is as above. For a total order $\leq$ on S we then have the **trichotomy law**: for every $s_1, s_2 \in S$ exactly one of the relations $s_1 < s_2$ or $s_1 = s_2$ or $s_2 > s_1$ holds. A **ordered set** is a pair $(S, \leq)$, where S is a set and $\leq$ is a order on S.

Let A be a commutative unitary ring.

1.13.2. Definition. — A preorder $\preceq$ on A is called a **ring-preorder** on A if:

i) $a_1 \preceq a_2 \Rightarrow a_1 + a_3 \preceq a_2 + a_3$ for every $a_1, a_2, a_3 \in A$.
ii) $a_1 \preceq a_2$ and $0 \preceq a \Rightarrow a_1 a_3 \preceq a_2 a_3$ for every $a_1, a_2, a_3 \in A$.
iii) $0 \preceq a^2$ for each $a \in A$.
iv) $0 \not\preceq -1$.

The **nonnegative cone** T of $(A, \preceq)$ is then defined as $T = T_{\preceq} := \{a \in A \mid a \succeq 0\}$. The set $\mathfrak{t} := T \cap (-T)$ is called the **support** of $\preceq$.

1.13.3. Remark. — (a) The trivial preorder ($a \preceq b$ for every $a, b \in A$, hence it would be $T = A$) does satisfy *i)* – *iii)* but it does not fulfill *iv)*.
(b) Request *iii)* implies $0 \preceq 1$, hence $0, 1 \in T$ and $-1 \notin T$.
(c) For every $a \in A$, it is $a \in -T \Leftrightarrow -a \in T$, hence we have $\{a \in A \mid 0 \preceq a \text{ and } a \preceq 0\} = T \cap (-T) = \mathfrak{t}$. This set, the support of $\preceq$, can be thought of as the set of the elements of A which are (zero or) "$\preceq$-*indistinguishable from* 0". Note that request *iv)* implies $1 \notin \mathfrak{t}$.

A preorder, being a relation on A, is a subset of the cartesian square $A^2 := A \times A$. As it is easier to work with subsets of A instead of subsets of A^2, the above definition is usually rephrased in terms of *nonnegative cones* as follows.

1.13.4. Definition. — A **cone** on A is a subset T of A such that:

i) $T + T \subseteq T$.
ii) $T \cdot T \subseteq T$.
iii) $A^{(2)} \subseteq T$.

In this case we define $a \preceq_T b$: $\Leftrightarrow b - a \in T$. The set $\mathfrak{t} := T \cap (-T)$ is the **support of** T.
The cone T is said to be **proper** if, moreover, it satisfies

iv) $-1 \notin T$.

1.13.5. Remark about terminology. — We are here following the terminology of [**BCR98**, 4.2.1], while [**Lam84**], [**BN93**, 2] and [**Neu98**, 1] use "preorder" instead.

1.13.6. Remark. — "Ring-preorders $\preceq$ on A" and "proper cones T of A" are equivalent concepts. Indeed, if $\preceq$ is a ring-preorder on A then $T_{\preceq}$ is a proper cone of A such that $\preceq_{T_{\preceq}}=\preceq$, and vice-versa if T is a proper cone of A then $\preceq_T$ is a ring-preorder on A such that $T_{\preceq_T} = T$.

1.13.7. Critical Example. — If A is such that $-1 \in \mathbb{N} \cdot 1_A$ (as it is in any finite ring) then $-1 \in \sum A^{(2)}$, and hence A cannot have precones. For example, let $A := \mathbb{Z}/(6)$. Then $-\overline{1} = 5 \cdot \overline{1}$ in A, moreover $A^{(2)} = \{\overline{0}, \overline{1}, \overline{4}, \overline{3}\}$ and $A^{(2)} + A^{(2)} = \{\overline{0}, \overline{1}, \overline{4}, \overline{3}, \overline{2}, \overline{5}\} = \mathbb{Z}/(6)$.

1.13.8. Proposition. — *Let $f\colon A \longrightarrow B$ be a unitary ring homomorphism, and let U be a (proper) cone of B with support $\mathfrak{u}$. Then $f^{-1}(U)$ is a (proper) cone of A with support $f^{-1}(\mathfrak{u})$.*

Proof. — All verifications are straightforward. □

The basic properties a precone may have are summarized and proved in the following proposition.

1.13.9. Proposition. — *Let T be a proper cone of A. Then*

a) A is semireal. In particular $char(A) = 0$ and $\mathbb{Z}$ is a unitary subring of A.

b) $T \cdot \mathfrak{t} \subseteq \mathfrak{t}$, $-T \cdot \mathfrak{t} \subseteq \mathfrak{t}$ and $\mathfrak{t}$ is the biggest additive subgroup of A contained in T.

c) $\sum A^{(2)} \subseteq T$ and $\sum A^{(2)}$ is the smallest proper cone on A (i.e. the sums of squares are **universally non-negative***).*

d) $\sum T \cdot A^{(2)} \subseteq T$.

e) If S is a multiplicative system of A such that $S \cap \mathfrak{t} = \emptyset$, then the subset

$$T_S := \{x \in S^{-1}A \mid x = \frac{a}{s} \text{ for some } a \in A, s \in S \text{ with } sa \in T\}$$

of $S^{-1}A$ is a proper cone on $S^{-1}A$, and its inverse image under the canonical ring homomorphism $\chi_S\colon A \longrightarrow S^{-1}A$ is the proper cone $\chi_S^{-1}(T_S) = \{a \in A \mid s^2a \in T \text{ for some } s \in S\}$.

f) T is a total proper cone if and only if $A = T \cup (-T)$

g) If T is a total proper cone then $(T \cap A^\times)^{-1} \subseteq T$.

h) If $2 \in A^\times$ or T is a total proper cone of A then the support $\mathfrak{t}$ is an ideal of A. In this case, $\overline{T} := \pi(T)$, the image of T in the canonical quotient map $\pi\colon A \longrightarrow \overline{A}$ onto the residue class ring $\overline{A} := A/\mathfrak{t}$, is a proper cone on $\overline{A}$ whose inverse image under π is exactly T, and $\overline{A}$ is a semireal ring.

k) If $A = K$ is a field, then $\mathfrak{t} = (0)$.

i) If T is a total proper cone of A with zero support, S is a multiplicative system of A such that $S \cap \mathrm{Zdv}(A) = \emptyset$ and T_S is the proper cone of $S^{-1}A$ defined in e) above, then $\chi_S^{-1}(T_S) = T$. Moreover, the ring-preorder on $S^{-1}A$ associated to T_S is the unique extension of the ring-preorder of A associated to T.

Proof. — *a)* It follows from the conjunction of *i)*, *iii)* and *iv)*. The last statement is clear.
b) Let $t \in T$ and $z \in T \cap (-T)$, that is $0 \preceq_T z \preceq_T 0$. We need to show $\pm tz \in T \cap (-T)$. From $0 \preceq_T t$ we get $0 \preceq_T tz \preceq_T 0$ hence $tz \in T \cap (-T)$, while from $-t \preceq_T 0$ we get $0 \succeq_T -tz \succeq_T 0$ hence $-tz \in T \cap (-T)$. As for the last statement, we note that, as $0 \in \mathfrak{t}$, it is $\mathfrak{t} \neq \emptyset$. By its very definition $-\mathfrak{t} \subseteq \mathfrak{t}$, if now $t_1, t_2 \in \mathfrak{t}$ then by *i)* it must be $t_1 - t_2 \in \mathfrak{t}$, hence $\mathfrak{t}$ is a subgroup of the additive group of A which is contained in T. On the other hand, if $E \subseteq T$ is a subgroup of the additive group of A then $E = -E \subseteq -T$, hence $E \subseteq \mathfrak{t}$. Therefore $\mathfrak{t}$ is the biggest subgroup of the additive group of A contained in T.
c) From *iii)* and *i)* it follows that $\sum A^{(2)} \subseteq T$. On the other hand, the set $\sum A^{(2)}$ clearly always satisfies *i)* – *iii)*. Therefore $\sum A^{(2)}$ is a proper cone if and only if A is semireal, which is the same as asking that A has at least one proper cone. In particular, in this case, $\sum A^{(2)}$ is the smallest proper cone of A.
d) It follows from *iii)*, *ii* and *i)*.
e) Note that, by definition, for $x \in T_S$ we required just that at least one representative of x is of the form $\frac{a}{s}$ with $sa \in T$. The set T_S clearly satisfies *i)* and *ii)*, and it obviously contains $(S^{-1}A)^{(2)}$, therefore T_S satisfies also *iii)*. Assume, by contradiction, that there exist $a \in A$, $s \in S$ with $sa \in T$ such that $\frac{-1}{1} = \frac{a}{s}$ in $S^{-1}A$, so that $-1 \in T_S$. By definition of equality in the fraction ring $S^{-1}A$ there exist $u \in S$ such that $u(-s - a) = 0$ in A. Hence, multiplying both sides by $us \in S$, it is also $u^2 s(-s - a) = 0$. As S is a multiplicatively closed subset of A and $sa \in T$, we get that $(us)^2 = -u^2 as$ is an element of $S \cap \mathfrak{t} = \emptyset$ (by hypothesis), which is absurd. Therefore T_S satisfies all conditions *i)* – *iv)*, and so it is a proper cone on $S^{-1}A$. For the last statement. Let $a \in A$ such that $\frac{a}{1} \in T_S$, that is $\frac{a}{1} = \frac{a'}{s}$ in $S^{-1}A$ with $s \in S$ and $a' \in A$ such that $sa' \in T$. As before, there exist $u \in S$ such that $u(sa - a') = 0$ in A and so $(us)^2 a = u^2 sa' \in T$ with $(us)^2 \in S^{(2)}$. If, for the converse, $a \in A$ is such that there exists $s \in S$ with $s^2 a \in T$, then $\frac{a}{1} = \frac{s^2 a}{s^2} \in T_S$ indeed $s^2 \cdot s^2 a \in T$ as $s^2 \in T$.
f) The proper cone T of A is total if and only if the ring-preorder $\preceq_T$ is a total preorder relation, hence for any $a \in A$ it is $0 \preceq_T a$ (*i.e.* $a \in T$) or $a \preceq_T 0$, which implies $0 \preceq_T -a$ (*i.e.* $-a \in T$,

hence $a \in -T$). For the converse, let $a, b \in T$ then $a - b \in T$ (*i.e.* $a \succeq_T b$) or $b - a \in -T$ (*i.e.* $b \succeq_T a$).

g) Let $a \in T$ be a unit of A, then $aa^{-1} = 1$. As T is a total proper cone, by *e*) $a^{-1} \in T$ or $a^{-1} \in -T$. In the latter case $-a^{-1} \in T$ and so $-1 = -a^{-1}a \in T$, absurd.

h) If T is a total proper cone then $A = T \cup (-T)$ by *c*), thus the claim follows by *a*). Assume $2 \in A^\times$, then from 1.1.5 any $x \in A$ is a square difference $x = y^2 - z^2$ (for some $y, z \in A$). The claim now follows by *iii*) and *a*). For the second statement of this point, we first note that $\pi^{-1}(\overline{T}) = \pi^{-1}(\pi(T)) = T + \mathfrak{t} = T$ as π is a homomorphism with kernel $\mathfrak{t}$ and T is additively closed by *i*), and now $\overline{T}$ is a proper cone of $\overline{A}$ by straightforward verifications and hence, by part *a*), the ring $\overline{A}$ is semireal.

k) If A is a field, as it must have $\operatorname{char}(A) = 0$ by *a*), then $2 \in A^\times$ and so by the above $\mathfrak{t}$ is an ideal of A. As $-1 \notin \mathfrak{t}$, by *iv*), and A is a field we conclude that $\mathfrak{t} = (0)$.

i) As S does not meet $\operatorname{Zdv}(A)$ we have that $\chi_S \colon A \hookrightarrow S^{-1}A$ is a ring injection in this case. Trivially $T \subseteq \chi_S^{-1}(T_S)$. Let now $a \in \chi_S^{-1}(T_S)$ by *e*) above it is $s^2 a \in T$ for some $s \in S$. As T is total, $A = T \cup (-T)$. If $a \in T$ there is nothing to prove, assume then that $-a \in T$. We have thus $T \ni s^2(-a) = -s^2 a$, whence $s^2 a \in -T$, and therefore $s^2 a \in \mathfrak{t} = (0)$ by hypothesis. As $s^2 a = 0$ and S does not contains zero-divisor, we conclude $a = 0 \in T$. For the last statement, let U be a proper cone of $S^{-1}A$ such that $A \cap U = T$ (using the identification induced by the injection χ_S), we claim that then $U = T_S$. Indeed, if $x \in T_S$, then $x = \frac{a}{s}$ with $a \in A$ and $s \in S$ such that $sa \in T = A \cap U \subseteq U$. Therefore $x = \frac{a}{s} = \frac{as}{s^2} = \left(\frac{1}{s}\right)^2 as \in U$. Coversely, if $U \ni \frac{a}{s} = \frac{as}{s^2}$, then $as = \frac{as}{s^2} \cdot s^2 \in A \cap U = T$, and therefore $\frac{a}{s} \in T_S$. We conclude that $U = T_S$ as claimed. □

1.13.10. Proposition (Lattice properties of proper cones). — *Let $\mathcal{T}$ the family of all proper cones on A, considered as an ordered set with respect to set-inclusion. Then:*

a) *$\mathcal{T}$ is closed under arbitrary intersection, and if $\mathcal{T} \neq \emptyset$ then $\sum A^{(2)} = \bigcap \mathcal{T}$ is its minimum.*

b) *Any chain in $\mathcal{T}$ has an upper bound in $\mathcal{T}$.*

c) *Any proper cone T of A is a subset of a maximal one.*

Proof. — *a*) is clear, the last statement is just a rephrase of part *c*) of 1.13.9.

b) If $(T_\lambda)_{\lambda \in \Lambda}$ is a chain in $\mathcal{T}$, that is a family of proper cones of A, totally ordered by set-inclusion, then their union $\overline{T} := \bigcup_{\lambda \in \Lambda} T_\lambda$ is clearly a proper cone of A containing each element of the chain, hence it is an upper bound in $\mathcal{T}$ for the chain.

c) follows by *b*), applying Zorn's Lemma to the partially ordered, with respect to set-inclusion, subset of all proper cones containing the given one (which is nonempty by hyphothesis). □

We now come to what should be considered the best approximation of an order on a general commutative ring, not necessarily a domain.

1.13.11. Definition. — A **ring-quasi-order** on A is a ring-preorder $\preceq$ on A which moreover satisfies:

v) $\preceq$ is a total preoder.

vi) $\{a \in A \mid 0 \preceq a \text{ and } a \preceq 0\}$ is a prime ideal of A.

We say that the ring-quasi-order $\leq$ is a **ring-order** if moreover $\leq$ is an antisymmetric relation on A, equivalently its support (assumed to be a prime ideal) is reduced to 0, that is $\{a \in A \mid 0 \leq a \leq 0\} = (0)$. This is equivalent to require that $\leq$ is a total order relation on the semireal domain A [7].

1.13.12. Remark. — In the specialized literature (see [**Lam84**]) ring-quasi-orders are simply called "orders" (as well as the corresponding nonnegative cones). To avoid conflict with the general standard notion of order recalled in definition 1.13.1 I slightly modified the terminology here.

1.13.13. Remark. — Request *vi*) is equivalent to ask that if a is $\preceq$-indistinguishable from 0 then any xa ($x \in A$) is such, and if a product is $\preceq$-indistinguishable from 0 then at least one factor of the product is such.

1.13.14. Definition. — A **prime cone** of A is a proper cone $\mathcal{N} \subset A$ satisfying moreover

v) $A = \mathcal{N} \cup (-\mathcal{N})$.

vi) Its support $\mathfrak{n} = \mathcal{N} \cap (-\mathcal{N})$ is a prime ideal of A.

In this case we define $a \preceq_{\mathcal{N}} b$: $\Leftrightarrow b - a \in \mathcal{N}$, which is a ring-order on A. We say that $\mathcal{N}$ is a **strict prime cone** of A if $\mathfrak{n} = (0)$.

1.13.15. Remark about terminology. — Again we follow the terminology of [**BCR98**, 4.3.1], while [**Lam84**] uses "order" instead.

7. As the support $\{a \in A \mid 0 \preceq a \preceq 0\} = (0)$ is required to be a prime ideal, A must be an integral domain.

1.13.16. Remark. — (a) "Ring-quasi-orders $\preceq$ on A" and "prime cones $\mathcal{N}$ of A" are equivalent concepts as in the case of ring-preorders and proper cones. Ring-orders on A corresponds to strict prime cones of A and vice-versa.
(b) If A is field then any prime cone is a strict one by part k) of 1.13.9.
(c) If A has a strict prime cone $\mathcal{N}$, then A is necessarily a domain because in this case $(0) = \mathfrak{n}$ is a prime ideal of A.

1.13.17. Proposition. — *Let $f\colon A \longrightarrow B$ be a unitary ring homomorphism, and let $\mathcal{L}$ be a prime cone of B with support $\mathfrak{l}$. Then $f^{-1}(\mathcal{L})$ is a prime cone of A with support $f^{-1}(\mathfrak{l})$. If B is a domain and $\mathcal{L}$ is a strict prime cone of B, then $f^{-1}(\mathcal{L})$ is a strict prime cone of A if and only if f is injective and A is a domain.*

Proof. — Standard verifications. The ideal $f^{-1}(\mathfrak{l})$ is a prime ideal of A by 1.4.4. □

1.13.18. Proposition (Cone criterion). — *Let T be a proper cone of A. Then T is a prime cone of A if and only if whenever $ab \in -T$ it is $a \in T$ or $b \in T$.*

Proof. — Necessity. Let $a \in A$, then $-a^2 = (-a)a \in -T$. Therefore $a \in -T$ or $a \in T$, that is $A = -T \cup T$. By 1.13.9 h) the support $\mathfrak{t} = T \cap (-T)$ is then an ideal of A. Assume $ab \in \mathfrak{t}$, whence also $-ab \in \mathfrak{t}$, and $a \notin \mathfrak{t}$. If $a \notin T$ then $-a \in T$ by $A = -T \cup T$ and $b \in \mathfrak{t}$ as $a(\pm b) = \pm ab \in \mathfrak{t} \subseteq -T$. If $a \notin -T$ then $-a \notin T$ and $b \in \mathfrak{t}$ as $(-a)(\pm b) = \mp ab \in \mathfrak{t} \subseteq -T$. Thus $\mathfrak{t}$ is a prime ideal of A. Sufficiency. Assume $ab \in -T$, with $a \notin T$ and $b \notin T$. Then $a, b \in -T$ and therefore $ab \in \mathfrak{t}$ prime ideal. Therefore $a \in \mathfrak{t} \subseteq T$ or $b \in \mathfrak{t} \subseteq T$, absurd. □

1.13.19. Proposition. — *Let $\mathcal{N}$ be a prime cone of A, then its support $\mathfrak{n}$ is a real prime ideal of A.*

Proof. — Let $x := a_1^2 + \cdots + a_t^2 \in \mathfrak{n} = \mathcal{N} \cap (-\mathcal{N})$ for some $a_1, \ldots, a_t \in A$. As $\sum A^{(2)} \subseteq \mathcal{N}$, then $x_i := \sum_{j \neq i} a_j^2 \in \mathcal{N}$ and $-x_i \in -\mathcal{N}$ for every $i = 1, \ldots, t$. Hence $a_i^2 = x - x_i = x + (-x_i) \in \mathcal{N} \cap (-\mathcal{N}) = \mathfrak{n}$ for every $i = 1, \ldots, t$. Therefore $a_i \in \mathfrak{n}$ for every $i = 1, \ldots, t$ since $\mathfrak{n}$ is a prime ideal. □

1.13.20. Corollary. — *If A has a strict prime cone, then A is a real domain.*

Proof. — A strict prime cone is a prime cone $\mathcal{N}$ with support $\mathfrak{n} = (0)$, which is therefore a real prime ideal of A. Hence the ring A is a real domain. □

1.13.21. Critical example. — Let R be a real domain, such as $R = \mathbb{Z}$ or $R = K$ a real field, and let $A = R[X]/(X^2) = R[\varepsilon] = R \oplus R\varepsilon$, with $\varepsilon^2 = 0$. Note that A is semireal but not real as $\varepsilon^2 = 0$ but $\varepsilon \neq 0$. For any given $x = u + v\epsilon, y = s + t\epsilon \in A$, with $u, v, s, t \in R$, we define $x = u + v\epsilon \leq y = s + t\epsilon :\Leftrightarrow u < s$, or $u = s$ and $v \leq t$. Then $\leq$ is a total order on A such that $T := \{x \in A \mid x \geq 0\}$ is a proper cone on A with support $\mathfrak{t} = T \cap (-T) = (0)$, as $\leq$ is antisymmetric. But A is not a domain, hence (0) is not a prime ideal. Because of this, despite being a "true" order relation even "well behaved" with respect to the ring operations, $\leq$ is not a ring-order, not even a ring-quasi-order, as in definition 1.13.11. The relation $\leq$ on A is only a ring-preorder, as in definition 1.13.2, and T is a proper cone of A which is not a prime cone. Instead $\mathcal{N} := \{a + b\varepsilon \mid a, b \in \mathbb{Z}, a \geq 0\}$ is a prime cone of A with support the real prime ideal $\mathfrak{n} = \mathcal{N} \cap (-\mathcal{N}) = (\varepsilon)$. By the previous corollary there cannot be strict prime cones of A.

Prime cones and their supports have, to some extent, certain maximality properties (w.r.t. set-inclusion), thought this is especially true in the case of fields.

1.13.22. Proposition. — *Let A be a commutative unitary ring.*

a) If T is a proper cone of A and $x, y \in A$ are such that $xy \in -T$, then at least one of $T + xT$, $T + yT$ is proper cone.

b) Every maximal proper cone (w.r.t. set-inclusion) is a prime cone.

c) Any proper cone T of A is contained in a prime cone.

d) If $\mathcal{N}_1$, $\mathcal{N}_2$ and $\mathcal{N}_3$ are three prime cones of A then

d1) $\mathcal{N}_1 \subseteq \mathcal{N}_2 \Rightarrow \mathfrak{n}_1 \subseteq \mathfrak{n}_2$.

d2) $\mathcal{N}_1 \subseteq \mathcal{N}_2$ and $\mathfrak{n}_1 = \mathfrak{n}_2 \Rightarrow \mathcal{N}_1 = \mathcal{N}_2$.

d3) $\mathcal{N}_1 \subseteq \mathcal{N}_2$ and $\mathcal{N}_1 \subseteq \mathcal{N}_3 \Rightarrow \mathcal{N}_2 \subseteq \mathcal{N}_3$ or $\mathcal{N}_3 \subseteq \mathcal{N}_2$.

In particular, the set of all prime cones containing a given one is totally ordered by inclusion.

e) If $\mathcal{N}$ is a prime cone of A, then $\mathcal{N}$ is maximal as a prime cone if and only if it is maximal as a proper cone.

f) If A is a field, then prime cones are exactly the maximal proper cones.

Proof. — *a*) and *b*) can be found in [**Lam84**, 3.4, 3.6].

c) This follows from *c*) of 1.13.10.

d) The first claim is clear as $\mathcal{N}_1 \subseteq \mathcal{N}_2 \Rightarrow -\mathcal{N}_1 \subseteq -\mathcal{N}_2$.

As for the second one. Let $a \in \mathcal{N}_2$, as $\mathcal{N}_1$ is a cone, $a \in \mathcal{N}_1$ or $a \in -\mathcal{N}_1$. In the former case, there is nothing to prove. In the latter case, $-a \in \mathcal{N}_1 \subseteq \mathcal{N}_2$ implies $a \in \mathcal{N}_2 \cap (-\mathcal{N}_2) = \mathfrak{n}_2 = \mathfrak{n}_1 \subseteq \mathcal{N}_1$, therefore $a \in \mathcal{N}_1$.

Finally, for the third claim. Let, by contradiction, $x_3 \in \mathcal{N}_3 \setminus \mathcal{N}_2$, and $x_2 \in \mathcal{N}_2 \setminus \mathcal{N}_3$, and consider the elements $a := x_3 - x_2$ and $-a = x_2 - x_3$. We note that $a \notin \mathcal{N}_2$, otherwise $x_3 = a + x_2 \in \mathcal{N}_2$ and $-a \notin \mathcal{N}_3$, otherwise $x_2 = -a + x_3 \in \mathcal{N}_3$. As $\mathcal{N}_1 \subseteq \mathcal{N}_2 \cap \mathcal{N}_3$ this means that $a \notin \mathcal{N}_1$ and $-a \notin \mathcal{N}_1$, which is impossible as $\mathcal{N}_1$ is a prime cone.

e) It follows from *b*) and *c*) above.

f) See [**Lam84**]. □

Emil Artin, in it's solution of Hilbert 17th problem, showed in 1927 that a field F can be ordered if and only if F is "semireal" in the sense that -1 is not a sum of squares in F.

1.13.23. Theorem. — *Let K be a field. Then the following facts are equivalent:*

a) *K can be ordered;*

b) *The field K has a prime cone as defined in 1.13.14;*

c) *K is semireal, i.e. $-1 \notin \Sigma K^{(2)}$;*

d) *K is a real field, that is for every $x_1, \ldots, x_n \in K$, $\sum_{i=1}^{n} x_i^2 = 0 \;\Rightarrow\; x_1 = \cdots = x_n = 0$.*

Proof. — The proof can be found in [**BCR98**, Thm. 1.1.8]. □

1.13.24. Theorem. — *Let K be a real field.*

a) *Let $x \in K$. If $x \in \sum K^{(2)}$, then $K(\sqrt{x})$ is real. If $K(\sqrt{x})$ is not real, then $-x \in \sum K^{(2)}$. Hence $K(\sqrt{x})$ or $K(\sqrt{-x})$ is real.*

b) *For any irreducible polynomial of odd degree $f \in K[X]$ and any root α of f, the field extension $K(\alpha)$ is real.*

Proof. — The proof can be found in [**Lan02**, XI, §2, Prop. 2.1]. □

1.13.25. Definition. — A field K is said to be a **real-closed field** if it is real and it has no nontrivial real algebraic extension, *i.e.* if L is an algebraic extension of K either $L = K$ or L is not real.

1.13.26. Example. — The field $\mathbb{Q}$ is not real-closed: $\mathbb{Q}[\sqrt{2}]$ is a non trivial real algebraic extension of it. The field $\mathbb{R}$ is a real-closed field, it's only proper algebraic extension is $\mathbb{C} = \mathbb{R}[i]$, which is not real. No algebraically closed field L can be real-closed, indeed -1 is a square in L for any such L.

1.13.27. Remark: conjugation on $K[i]$. — If K is a field in which -1 is not a square, the polynomial $X^2+1 \in K[X]$ is irreducible and therefore the ring $K[i] := K[X]/(X^2+1)$ is a field. As a K-vector space $K[i] = K \oplus iK$ where $\{1, i\}$ is a K-bases of $K[i]$. As for $\mathbb{C} = \mathbb{R}[i]$, hence $\overline{a+ib} := a - ib$ for every $a + ib \in K[X]$ (with $a, b \in K$) is a well defined K-linear involutive automorphism of the field $K[i]$, *i.e.* $\overline{uz_1 + vz_2} = u\overline{z_1} + v\overline{z_2}$ for every $z_1, z_2 \in K[i]$ and $u, v \in K$, $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ for every $z_1, z_2 \in K[i]$ and $\overline{\overline{z}} = z$ for every $z \in K[i]$ (all verifications are standard). As in the complex case, for any $z = a + ib$, with $a, b \in K$, we can define the following maps $K[i] \longrightarrow K$: $\mathbb{R}(z) := a$, $\Im(z) := b$, $\mathrm{N}(z) = |z|^2 := z\overline{z} = a^2 + b^2$. In particular, as in the complex case: for every polynomial $f \in K[X]$ and every $z \in K[i]$ we have $\overline{f(z)} = f(\overline{z})$ and thus $f(z) = 0 \Leftrightarrow f(\overline{z}) = 0$. Hence by Ruffini Theorem we get that, if $z \in K[i]$ is a root of $f \in K[X]$, then $(X-z)(X-\overline{z}) = X^2 - 2\mathbb{R}(z)X + N(z) \in K[X]$ divides $f(X)$, and $(X-z)(X-\overline{z})$ is reducible in $K[X]$ if and only if $\Im(z) = 0$ (that is $z \in K$), in which case $X^2 - 2\mathbb{R}(z)X + N(z) = (X-z)^2$. Therefore, all the quadratic polynomials of the form $X^2 - 2\mathbb{R}(z)X + N(z) \in K[X]$ are irreducible in the factorial domain $K[X]$ as z varies in $K[i] \setminus K$.

1.13.28. Theorem. — *Let K be a field. Then the following facts are equivalent:*

i) K is real-closed.

ii) Every polynomial of $K[X]$, of odd degree, has a root in K and there is a unique ordering on K whose nonnegative cone is the set of squares of K.

iii) The ring $K[i] := K[X]/(X^2+1)$ is an algebraically closed field (in particular, K is not algebraically closed).

iv) K is an ordered field and it has the "intermediate value property" for polynomials (if $f \in K[X]$ is such that $f(x)f(y) < 0$ for some $x, y \in K$, then $f(z) = 0$ for some $z \in K$ such that $x < z < y$).

v) For each $a \in K \setminus \{0\}$ exactly one of a, $-a$ is a square of K, and every polynomial of odd degree of $K[X]$ has a root in K.

Proof. — A complete proof of the equivalence of *i)* $\Leftrightarrow$ *ii)* $\Leftrightarrow$ *iii)* can be found in [**BCR98**, Thm. 1.2.2]. The equivalences *i)* $\Leftrightarrow$ *v)* and *i)* $\Leftrightarrow$ *iv)* are shown in [**Coh03**, Thm. 8.8.7, Prop. 8.8.9].

Here we just show *iii)* $\Rightarrow$ *i)* giving full details. If $K[i]$ is a field, then X^2+1 is irreducible in $K[X]$, therefore -1 is not a square in K. We claim that as $K[i]$ is algebraically closed then every sum of squares in K is itself a square in K, *i.e.* $K^{(2)} = \sum K^{(2)}$. Let $x, y \in K$, than $x+iy \in K[i]$ has a square root in $K[i]$, that is there are $u, v \in K$ such that $x+iy = (u+iv)^2$. By conjugation $x-iy = (u-iv)^2$, and so $x^2+y^2 = (x+iy)(x-iy) = (u+iv)^2(u-iv)^2 = (u^2+v^2)^2$. Thus, by induction, any finite sum of squares in K is a square in K as claimed. We conclude $-1 \notin \sum K^{(2)}$, and so K is a real field. Let now L be a proper algebraic extension of K, as $K[i]$ is algebraically closed and algebraic over K then there is a K-linear field embedding $L \hookrightarrow K[i]$ extending the inclusion $K \subseteq L$ (cf. **[Lan02**, V, §2, Thm. 2.8] or **[Bos18**, 3.4, Prop. 9]). As by assumption $K \subsetneq L$ and $\dim_K K[i] = 2$, it must be $L \cong K[i]$. Therefore any proper algebraic extension of K is not real, that is K is real-closed. □

1.13.29. Remark. — If $K = \mathbb{F}_3 = \mathbb{Z}/(3) = \{\overline{0}, \overline{1}, \overline{2}\}$ (the field with three elements), then $-\overline{1} = \overline{2}$ is not a square in $\mathbb{F}_3$ and so $X^2+1 \in \mathbb{F}_3[X]$ is irreducible and $\mathbb{F}_3[X]/(X^2+1)$ is a field. Indeed, $\mathbb{F}_3[X]/(X^2+1) \cong \mathbb{F}_9$, the field with 9 elements which is not an algebraically closed field, for any algebraically closed field must be infinite (cf 1.2.6).

1.13.30. Proposition. — *Let K be a real-closed field, then the irreducible polynomials of $K[X]$ are either those of degree one or those of degree two without roots in K.*

Proof. — Let $f \in K[X]$ be any polynomial of degree $d > 0$, hence as $K[i]$ is algebraically closed f splits into a product of d linear factors in $(K[i])[X]$. As f is a polynomial with coefficients in K, taking into account 1.13.27, one can write

$$\begin{aligned} f &= a(X-x_1)\cdots(X-x_r)\cdot(X-z_1)(X-\overline{z_1})\cdots(X-z_s)(X-\overline{z_s}) \\ &= \prod_{i=1}^{r}(X-x_i)\cdot\prod_{j=1}^{s}(X^2-2\mathbb{R}(z_j)X+N(z_j)) \end{aligned}$$

where $a \in K \setminus \{0\}$, $r, s \in \mathbb{N}$, with $r+2s = d$, $x_i \in K$, and $z_j \in K[i] \setminus K$. As the quadratic polynomials $X^2 - 2\mathbb{R}(z)X + N(z)$, with $z \in K[i] \setminus K$, have coefficients in K, this shows that in the factorial domain $K[X]$ there are no irreducible polynomials of degree higher than two. □

The following result, due to E. Artin, shows that for an algebraically closed field L either $L = K[i]$ is the algebraic closure of a real-closed subfield K or L is at "infinitely bigger" than any of its subfields K, because it must be $\dim_K L = \infty$. In particular the latter situation is standard in positive characteristic.

1.13.31. Theorem (E. Artin). — *Let L be an algebraically closed field. If K is a proper subfield of L such that L is a finite dimensional K-vector space, then K is not algebraically closed and $L = K[i]$ with $i \in L \setminus K$ such that $i^2 = -1$. In particular, K is real-closed field.*

Proof. — The proof exploits Galois Theroy, it can be found in [**Bos18**, 6.3, Prop. 2]. □

1.13.32. Example. — Let $A = \mathbb{R}[X]$, then $I = (X^2+1)$ is not a real ideal of A, for $1+X^2 \in I$ but $1 \notin I$ (and indeed the quotient ring $A/I \cong \mathbb{C}$ is not real). As I is a maximal ideal of A, the smallest real ideal of A containing I is $(1) = A$ itself.

1.13.33. Example. — Let $A = \mathbb{Q}[X, Y]$, then $I = (X^2 + Y^2)$ is not a real ideal of A, for $X^2 + Y^2 \in I$ but $X \notin I$ (degree reason). Let J be the smallest real ideal of A containing I, as $X^2+Y^2 \in I \subseteq J$ then necessarily $J \supseteq (X, Y)$. As (X, Y) is a real ideal of A [8], it is the smallest real ideal containing I.

1.13.34. Example. — Let $A = \mathbb{Q}[X]$, then $I = (X^2 - 2)$ is a real ideal of A. Indeed if $f_1(X)^2 + \cdots + f_n(X)^2 \in I$ then $\overline{f_1(X)}^2 + \cdots + \overline{f_n(X)}^2 = 0$ in the quotient ring $\mathbb{Q}[X]/I \cong \mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$, which is a real field because it is a subfield of $\mathbb{R}$. Hence $\overline{f_i(X)} = \overline{0}$ in $\mathbb{Q}[X]/I$ for each i, that is $f_i(X) \in I$ for each i.

1.13.35. Example. — Let $A = \mathbb{Q}[X]$, then $I = (X^2 + 2)$ is not a real ideal of A. Indeed it's residue class ring $\mathbb{Q}[X]/I \cong \mathbb{Q}[\sqrt{2}i] = \mathbb{Q}(\sqrt{2}i)$ (subfield of $\mathbb{C}$) is not a real field because it contains i with $i^2 = -1$, and hence $i^2 + 1 = 0$ is a non trivial sum of squares equal to 0.

1.13.36. Theorem-Definition. — *Let H be a real field. Then there exists an algebraic extension K of H such that K is a real-closed field. Such K is called a* **real closure** *of the real field H.*

Proof. — After having fixed an algebraic closure C of H, consider the ordered set (with respect to set-inclusion) of all real subfields of C containing H (they are necessarily algebraic over H being contained in C). A straightforward application of Zorn's Lemma shows that there is a maximal such subfield K. By the maximality property of K, it is a real-closed field.
For a proof without Zorn's Lemma see [**San91**]. □

8. If $S(X, Y) := f_1(X, Y)^2 + \cdots + f_n(X, Y)^2 \in (X, Y)$, then $S(0, 0) = 0$. As $S(0, 0)$ is a sum of squares in $\mathbb{R}$, it must be $f_i(0, 0) = 0$. Hence $f_i(X, Y) \in (X, Y)$ for every i. Or just take the quotient $K[X, Y]/(X, Y) \cong K$.

1.13.37. Remark. — One can prove that each given order $\leq$ on H gives rise to a real-closure $(K, \leq)$ of H extending the given order on the subfield, and that two such real-closures are H-isomorphic up to an order-preserving field isomorphism. But, in general, two real-closures K_1 and K_2 of H could be non-isomorphic (cf. [**BCR98**, 1.3], [**BN93**, 1]).

1.13.38. Example. — (a) The real closure of $\mathbb{Q}$ is $\mathbb{R}_{\text{alg}} := \{x \in \mathbb{R} \mid x \text{ is algebraic over } \mathbb{Q}\}$.
(b) The (real) subfield $H = \mathbb{Q}(\sqrt{2})$ of $\mathbb{R}$ admits two distinct orders. The first order on H is the one pulled back from $\mathbb{R}$ along the field inclusion $H \hookrightarrow \mathbb{R}$ (hence its non-negative cone is $\mathcal{N}_1 = H \cap \mathbb{R}^{(2)}$), while the second one is induced by the only non-trivial $\mathbb{Q}$-automorphism of H, that is $\tau\colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$, $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, with $a, b \in \mathbb{Q}$ (hence $\mathcal{N}_2 = \tau^{-1}(\mathcal{N}_1)$ is the smallest cone of H containing $H^{(2)}$ and $-\sqrt{2}$).

1.14. Properties of real ideals. The Real radical

1.14.1. Proposition. —

a) Any real ideal I of A is a radical ideal;
b) Any intersection of real ideals is still such;
c) Any product of real ideals is still such;
d) The sum of real ideals is not necessarily still such;
e) Let I, J be ideals of A with I a real ideal, then $(I : J)$ is a real ideal itself and moreover $(I : J^\infty) = (I : J) = (I : \sqrt{J})$;
f) If $\varphi\colon A \longrightarrow B$ is a (unitary) ring homomorphism and J is a real ideal of B, then it's contraction to A wrt φ, $J^c = \varphi^{-1}(J)$, is a real ideal of A;
g) If S is a multiplicative system of A and I is real of A, then then $I_S := IA_S$ is a real ideal of the ring of fractions A_S;
h) If I is real then $I[X] = IA[X]$ is real, whenever X is an indeterminate on A;
i) If I is real, all minimal prime ideals of I are real.

Proof. — *a)* If $a^t \in I$ for some $t \in \mathbb{N}_+$, then $a^{2t} = a^{2t} + 0^2 \in I$ also. As I is real, it follows $a \in I$. Hence I is necessarily radical if it is real.
b) It is straightforward.

c) Let's consider the case of two real ideals I_1, I_2. If a sum of squares $a_1^2+\cdots+a_n^2 \in I_1I_2 \subseteq I_1\cap I_2$, then $a_i \in I_1 \cap I_2 \ \ \forall i = 1, \cdots, n$ and hence $a_i^2 \in I_1I_2 \ \ \forall i = 1, \cdots, n$. The general case follows by induction.

d) Let $A = \mathbb{Z}[T]$ and $I := (T-6)$, $J := (T)$ ideals of A. Note that A is a real ring (subring of $\mathbb{R}[T]$) and that I and J are real ideals of A, indeed the quotient rings $A/I \cong \mathbb{Z}$ and $A/J \cong \mathbb{Z}$ are both real rings. Nonetheless, their sum $I + J = (T-6;T) = (6,T)$ is not a real ideal: $1^2 + 2^2 + 5^2 = 30 = 5 \cdot 6 \in I + J$, but $1 \notin I + J$, hence can't be real (the residue class ring is $A/(I + J) \cong \mathbb{Z}/(6)$). Another example: $A = \mathbb{R}[X, X]$ (a real ring), $I = (Y - X^2)$, $J = (Y)$ real ideals: $A/I \cong \mathbb{R}[X]$ and $A/J \cong \mathbb{R}[Y]$ are real rings. But $I + J = (X^2, Y)$ is a non radical ideal, hence not real by point *a*) above.

e) Let $a_1^2 + \cdots + a_n^2 \in (I : J)$, then $(a_1^2 + \cdots + a_n^2)j \in I$ for every $j \in J$. As I is an ideal, we also have $(a_1j)^2 + \cdots + (a_nj)^2 = (a_1^2 + \cdots + a_n^2)j^2 \in I$ for every $j \in J$. As I is real we get $a_kj \in I$ for every $j \in J$ and every $k = 1, \cdots, n$. Therefore $a_k \in (I : J)$ for every $k = 1, \cdots, n$. The last statement follows from 1.9.7 as I real implies I radical.

f) The quickest argument could be that the canonical ring homomorphism $A/\varphi^{-1}(J) \longrightarrow B/J$ is (tautologically) injective, hence B/J real implies $A/\varphi^{-1}(J)$ real.

g) It follows from the canonical isomorphism $A_S/IA_S \cong (A/I)_{\overline{S}}$ and *c*) of 1.12.5.

h) It follows from the canonical isomorphism $A[X]/I[X] \cong (A/I)[X]$ and the easy observation that a polynomial ring with coefficients in a real ring is itself real.

i) The minimal prime ideals of I in A bijectively correspond under contraction wrt the canonical projection $\pi\colon A \longrightarrow A/I$ to the minimal prime ideals of $(\overline{0})$ in A/I . Hence we conclude by 1.12.6 *i*) and *f*) above. See also [**Lam84**, Lemma 2.9] or, in the Noetherian case, [**BCR98**, Lemma 4.1.5], or [**Neu98**, Lemma 2.3]. □

1.14.2. Proposition-Definition. — *The* **real radical** *of an ideal I of A is defined as*

$$\sqrt[R]{I} := \{a \in A \mid a^{2m} + b_1^2 + \cdots + b_t^2 \in I \text{ for some } m \in \mathbb{N},\, b_1, \cdots b_t \in A\}.$$

It coincides with the smallest real ideal of A containing I and with the intersection of all real prime ideals containing I (or A itself, if there is no real prime ideal containing I).

Proof. — Several proofs are possible [**Lam84**, Thm. 6.5], [**BCR98**, Lemma 4.1.7], [**BN93**, Prop. 1], or [**Neu98**, Cor. 2.4]. The one in [**Lam84**] is, maybe, the most transparent though the less "computational". Here we follow [**BCR98**], but giving full details. From the definition it is clear that if J is a real ideal containing I, then $I \subseteq \sqrt[R]{I} \subseteq J$. Hence, as a set,

$\sqrt[R]{I} \subseteq \widetilde{I} := \bigcap_{I \subseteq J \text{ real}} J \subseteq \bigcap_{I \subseteq \mathfrak{p} \text{ real prime}} \mathfrak{p}$, where $\widetilde{I}$ is obviously the smallest real ideal containing I [9]. Moreover, it follows also that $\sqrt[R]{I}$ is "real as a set". Indeed

$$a_1^2 + \cdots + a_t^2 \in \sqrt[R]{I} \Leftrightarrow (a_1^2 + \cdots + a_t^2)^{2m} + \sigma \in I \text{ for some } m \in \mathbb{N}, \sigma \in \sum A^{(2)},$$

but

$$(a_1^2 + \cdots + a_t^2)^{2m} = \sum_{j=1}^{t} a_j^{4m} + \sum_{i=(i_1,\ldots,i_{2m})} a_{i_1}^2 a_{i_2}^2 \cdots a_{i_{2m}}^2 = \sum_{j=1}^{t} a_j^{4m} + \sum_{i=(i_1,\ldots,i_{2m})} (a_{i_1} a_{i_2} \cdots a_{i_{2m}})^2,$$

where the second sum is over all the non-constant functions $i\colon \{1,\ldots,2m\} \longrightarrow \{1,\ldots,t\}$. Hence, by definition of $\sqrt[R]{I}$, all a_j belong to it. To show that $\sqrt[R]{I}$ is an ideal of A, we start by proving $A\sqrt[R]{I} \subseteq \sqrt[R]{I}$. Let $a \in A$ and $x \in \sqrt[R]{I}$, then there are $m \in \mathbb{N}$ and a sum of squares $\sigma \in \sum A^{(2)}$ such that $x^{2m} + \sigma \in I$. Then, as I is an ideal, $I \ni a^{2m}(x^{2m} + \sigma) = (ax)^{2m} + a^{2m}\sigma$ and $a^{2m}\sigma \in \sum A^{(2)}$. Therefore $xa \in \sqrt[R]{I}$. Then we show $\sqrt[R]{I} + \sqrt[R]{I} \subseteq \sqrt[R]{I}$. Let $a_1, a_2 \in \sqrt[R]{I}$, hence there are $m_1, m_2 \in \mathbb{N}$ and a sum of squares $\sigma_1, \sigma_2 \in \sum A^{(2)}$ such that $a_i^{2m_i} + \sigma_i \in I$ for $i = 1, 2$. To show that $a_1 + a_2 \in \sqrt[R]{I}$, letting for a while $k = m_1 + m_2$, we first notice that

$$(a_1 + a_2)^{2k} + (a_1 - a_2)^{2k} = \sum_{j=0}^{2k} \binom{2k}{j} a_1^{2k-j} a_2^j + \sum_{j=0}^{2k} (-1)^j \binom{2k}{j} a_1^{2k-j} a_2^j = 2\sum_{i=0}^{k} \binom{2k}{2i} a_1^{2k-2i} a_2^{2i},$$

as $k = m_1 + m_2$, and hence $2k - 2i = 2m_1 + 2m_2 - 2i$, we get

$$\begin{aligned}
&(a_1 + a_2)^{2k} + (a_1 - a_2)^{2k} = \\
&\sum_{i=0}^{m_2-1} 2\binom{2k}{2i} a_1^{2k-2i} a_2^{2i} + \sum_{i=m_2}^{m_1+m_2} 2\binom{2k}{2i} a_1^{2k-2i} a_2^{2i} = \\
&\sum_{j=m_1+1}^{m_1+m_2} 2\binom{2k}{2k-2j} a_1^{2j} a_2^{2k-2j} + \sum_{i=m_2}^{m_1+m_2} 2\binom{2k}{2i} a_1^{2k-2i} a_2^{2i} = \\
&a_1^{2m_1} \sum_{j=m_1+1}^{m_1+m_2} 2\binom{2k}{2k-2j} a_1^{2j-2m_1} a_2^{2k-2j} + a_2^{2m_2} \sum_{i=m_2}^{m_1+m_2} 2\binom{2k}{2i} a_1^{2k-2i} a_2^{2i-2m_2} = \\
&a_1^{2m_1} \sum_{j=1}^{m_2} 2\binom{2k}{2k-2j} a_1^{2j} a_2^{2m_2-2j} + a_2^{2m_2} \sum_{i=0}^{m_1} 2\binom{2k}{2i} a_1^{2m_1-2i} a_2^{2i} = \\
&a_1^{2m_1}\sigma_1' + a_2^{2m_2}\sigma_2',
\end{aligned}$$

9. If one proves directly that actually the equality with the intersection of real primes holds, then it comes out "for free" that $\sqrt[R]{I}$ is an ideal, being an intersection of such, and that it is also the smallest real ideal containing I. This is the strategy of [**Lam84**], where it is not shown directly that $\sqrt[R]{I}$ is closed under sum.

where σ_1', σ_2' are sum of squares because the binomial coefficients are nonnegative integers. Therefore

$$I \ni (a_1^{2m_1} + \sigma_1)\sigma_1' + (a_2^{2m_2} + \sigma_2)\sigma_2' = (a_1 + a_2)^{2(m_1+m_2)} + (a_1 - a_2)^{2(m_1+m_2)} + \sigma_1\sigma_1' + \sigma_2\sigma_2',$$

and so $a_1 + a_2 \in \sqrt[R]{I}$ as $(a_1 - a_2)^{2(m_1+m_2)} + \sigma_1\sigma_1' + \sigma_2\sigma_2'$ is a sum of squares. We showed so far that $\sqrt[R]{I}$ is a real ideal containing I, and actually it is the smallest ideal real ideal containing I, hence $\sqrt[R]{I} = \widetilde{I}$. To prove $\sqrt[R]{I} = \bigcap_{I \subseteq \mathfrak{p} \text{ real prime}} \mathfrak{p}$, it remains to show, by contraposition, that $A \setminus \sqrt[R]{I} \subseteq A \setminus \bigcap_{I \subseteq \mathfrak{p} \text{ real prime}} \mathfrak{p}$. Hence what we need to show is that if $a \notin \sqrt[R]{I}$ there exists a real prime $\mathfrak{p} \supseteq I$ such that $a \notin \mathfrak{p}$. To this end, consider the set $\mathfrak{J}$ of all real ideals of A such that $a \notin \sqrt[R]{I}$. Clearly it is not empty, as it contains $\sqrt[R]{I}$ at least, and it is straightforward to show that every linear chain (of real ideals) in it has a supremum (the union of the elements in the chain is again a real ideal not containing a), hence by Zorn Lemma ([**Lan02**, Appendix 2.2], [**Bos18**, 3.4, Lemma 5], [**Sha90**, 3.8], [**AM69**, Footnote to 1.3]), $\mathfrak{J}$ has a maximal element $\mathfrak{p}$. We claim that $\mathfrak{p}$ is a prime ideal (real, obviously as $\mathfrak{p} \in \mathfrak{J}$). Else, there are $x_1 \notin \mathfrak{p}$ and $x_2 \notin \mathfrak{p}$ such that $x_1x_2 \in \mathfrak{p}$. By the maximality property in the definition of $\mathfrak{p}$ then we get $a \in \sqrt[R]{\mathfrak{p} + (x_1)} \cap \sqrt[R]{\mathfrak{p} + (x_2)}$, that is there exist $m_1, m_2 \in \mathbb{N}$ and $\sigma_1, \sigma_2 \in \sum A^{(2)}$ such that $a^{2m_i} + \sigma_i \in \mathfrak{p} + (x_i)$, for $i = 1, 2$. Multiplying these two relations we get $(a^{2m_1} + \sigma_1)(a^{2m_2} + \sigma_2) = a^{2(m_1+m_2)} + \sigma' \in (\mathfrak{p} + (x_1))(\mathfrak{p} + (x_2)) \subseteq \mathfrak{p}$, as $(x_1)(x_2) \subseteq \mathfrak{p}$, and with $\sigma' \in \sum A^{(2)}$. Hence $a \in \sqrt[R]{\mathfrak{p}} = \mathfrak{p}$ (as $\mathfrak{p}$ is real), which is a contradiction. Thus $\mathfrak{p} \ni a$ is prime, and so $\sqrt[R]{I} = \bigcap_{I \subseteq \mathfrak{p} \text{ real prime}} \mathfrak{p}$. □

1.14.3. Remark. — Example *1.13.32* shows that $\sqrt[R]{(1 + X^2)} = (1)$ in $\mathbb{R}[X]$, hence the "stability property" 1.9.5 *g*) does not hold for the real radical: a proper ideal can have non proper real radical, thereby disproving [**Bar16**, Prop. 9.3]

1.14.4. Real radical properties. —

a) *if I is real, then $\sqrt[R]{I} = \sqrt{I} = I$;*
b) *$\sqrt[R]{I}$ is a real ideal of A;*
c) *$\sqrt[R]{I} = \bigcap_{\mathfrak{p} \supseteq I,\ \mathfrak{p} \text{ real prime}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in Min(I) | \mathfrak{p} \text{ real}} \mathfrak{p}$;*
d) *$I \subseteq \sqrt[R]{I}$;*
e) *$I \subseteq J \Rightarrow \sqrt[R]{I} \subseteq \sqrt[R]{J}$*
f) *$\sqrt[R]{\sqrt[R]{I}} = \sqrt[R]{I}$;*
g) *$I = \sqrt[R]{J} \Rightarrow I = \sqrt[R]{I}$;*
h) *$\sqrt[R]{IJ} = \sqrt[R]{I \cap J} = \sqrt[R]{I} \cap \sqrt[R]{J}$ and $\sqrt[R]{I^n} = \sqrt[R]{I}$ for each $n \in \mathbb{N}_+$;*

i) $\sqrt[R]{I} = (1)$ *if and only if there are no real prime ideals containing* I *(cf. Example1.13.32);*

j) $\sqrt[R]{I+J} = \sqrt[R]{\sqrt[R]{I} + \sqrt[R]{J}}$*;*

k) If $\mathfrak{p}$ *is a prime ideal of* A *and* $n \in \mathbb{N}_+$ *then* $\sqrt[R]{\mathfrak{p}^n} = \mathfrak{p}$ *if and only if* $\mathfrak{p}$ *is a real prime;*

l) If $\varphi\colon A \longrightarrow B$ *is a (unitary) ring homomorphism and* J *is an ideal of* B*, then*

$$\sqrt[R]{\varphi^{-1}(J)} \subseteq \varphi^{-1}(\sqrt[R]{J}).$$

Moreover: if φ *is surjective, then* $\sqrt[R]{\varphi^{-1}(J)} = \varphi^{-1}(\sqrt[R]{J})$*;*

m) If S *is a multiplicative system of* A*, then* $\sqrt[R]{I_S} = (\sqrt[R]{I})_S$ *in the ring of fractions* A_S*;*

n) If A *is Noetherian,* I *does not necessarily contain a power of its real radical.*

o) If X *is an indeterminate over* A *and* I *is an ideal of* A*, then* $\sqrt[R]{IA[X]} = \sqrt[R]{I}A[X]$*.*

Proof. — Everithing, but *h)* and *m)*, follows quite as 1.9.5, with slight modifications taking into account the previous results (**??**). See also the following Remark about *l)*.

As for *h)*, from $IJ \subseteq I \cap J$ and $I \cap J \subseteq I$, $I \cap J \subseteq J$, by *e)*, as usual, we have the chain of inclusions $\sqrt[R]{IJ} \subseteq \sqrt[R]{I \cap J} \subseteq \sqrt[R]{I} \cap \sqrt[R]{J}$. Let now $a \in \sqrt[R]{I} \cap \sqrt[R]{J}$, *i.e.* there are $s, t \in \mathbb{N}$ and $\sigma, \tau \in \sum A^{(2)}$ such that $f^{2s} + \sigma \in I$ and $f^{2t} + \tau \in J$. Then

$$IJ \ni (f^{2s} + \sigma)(f^{2t} + \tau) = f^{2(s+t)} + f^{2s}\tau + f^{2t}\sigma + \sigma\tau.$$

Being $f^{2s}\tau + f^{2t}\sigma + \sigma\tau \in \sum A^{(2)}$, the above yields $f \in \sqrt[R]{IJ}$. Therefore $\sqrt[R]{I} \cap \sqrt[R]{J} \subseteq \sqrt[R]{IJ}$ and all the inclusions of the previous chain are equalities.

Let's also give an argument to show *m)* (it is stated without proof in [**Neu98**, Lemma 2.2]). The proof is not difficult, but quite tedious. We start showing that $\sqrt[R]{I_S} \subseteq (\sqrt[R]{I})_S$. Let $a \in S$ and $s \in S$ such that $\frac{a}{s} \in \sqrt[R]{I_S}$, then there exist $m \in \mathbb{N}$, $a_1, \cdots, a_r \in A$, $s_1, \cdots, s_r \in S$, $b \in S$ and $t \in S$ such that

$$\frac{a^{2m}}{s^{2m}} + \sum_{i=1}^{r} \frac{a_i}{s_i^2} = \frac{b}{t} \text{ in } A_S \Leftrightarrow \exists u \in S\colon ut(s_1 \cdots s_r)^2 a^{2m} + ut \sum_{i=1}^{r} a_i'^2 = us^{2m}(s_1 \cdots s_r)^2 b \in I \text{ in } A,$$

where $a_i' := s^m(\prod_{j \neq i} s_j)a_i \in A$. Multiplying both sides by $ut \in S$ we get then that

$$(uts_1 \cdots s_r)^2 a^{2m} + \sum_{i=1}^{r} a_i''^2 = u^2 t s^{2m}(s_1 \cdots s_r)^2 b \in I \text{ in } A$$

where $a_i'' := uta' \in A$ and $uts_1 \cdots s_r =: s' \in S$. Thus, multiplying again by $s'^{2m-2} \in S$ we have

$$(s'a)^{2m} + \sum_{i=1}^{r} (s'^{m-1} a_i'')^2 = s'^{2m-2} u^2 t s^{2m}(s_1 \cdots s_r)^2 b \in I \text{ in } A,$$

and, finally, then $\frac{a}{s} = \frac{as'}{ss'}$ in A_S with $as' \in \sqrt[R]{I}$ and $s' \in S$, by the above. Hence $\frac{a}{s} \in (\sqrt[R]{I})_S$. For the opposite inclusion, let now $a \in \sqrt[R]{I}$, then there exist $m \in \mathbb{N}$, $a_1, \cdots, a_r \in A$ and $b \in I$, such that $a^{2m} + \sum_{i=1}^r a_i^2 = b \in I$. Therefore, for any $s \in S$,

$$\left(\frac{a}{s}\right)^{2m} + \sum_{i=1}^{r} \left(\frac{a_i}{s^m}\right)^2 = \frac{a^{2m} + \sum_{i=1}^r a_i^2}{s^{2m}} = \frac{b}{s^{2m}} \in I_S.$$

n) First example: $I = (X^2 + 1) \subseteq \mathbb{Q}[X]$, then clearly $\sqrt[R]{I} = (1)$ but $1 \notin I$. Second example: $I = (X^3 - Y^3) \subseteq \mathbb{Q}[X, Y]$, then $\sqrt[R]{I} = (X - Y)$ (as we shall see in 2.18.9) but $(X - Y)^k \notin I$ for each $k \in \mathbb{N}$. Indeed I is a radical ideal (as $X^3 - Y^3 = (X - Y)(X^2 + XY + Y^2)$ is a product of two irreducible factors in the unique factorization domain $\mathbb{Q}[X, Y]$) such that $X - Y \notin I$ (by degree reasons).

o) As $\sqrt[R]{I}$ is a real ideal of A, by **??** *h*), $\sqrt[R]{I}A[X]$ is a real ideal of $A[X]$. As it contains $IA[X]$, then $\sqrt[R]{IA[X]} \subseteq \sqrt[R]{I}A[X]$. For the opposite inclusion, note that as $\sqrt[R]{I}A[X]$ is generated by the set of monomials $\{aX^k \mid a \in \sqrt[R]{I}, k \in \mathbb{N}\}$ and $\sqrt[R]{IA[X]}$ is an ideal, it suffices to show that $\sqrt[R]{IA[X]}$ contains those monomials. So, let $a \in A$ such that $a^{2m} + \sigma \in I$ for some $m \in \mathbb{N}$, $\sigma \in \sum A^{(2)}$, and let $k \in \mathbb{N}$. Then $(aX^k)^{2m} + X^{2mk}\sigma = (a^{2m} + \sigma)X^{2mk} \in IA[X]$, with $X^{2mk}\sigma = (X^{mk})^2\sigma \in \sum A[X]^{(2)}$. Hence $\{aX^k \mid a \in \sqrt[R]{I}, k \in \mathbb{N}\} \subseteq \sqrt[R]{IA[X]}$, and we conclude that $\sqrt[R]{IA[X]} \subseteq \sqrt[R]{I}A[X]$. □

1.14.5. Remark. — 1.14.4 *l*) differs from 1.9.5 *k*), as well as the "stability property" of 1.9.5 *g*) vs the "unstability property" 1.14.4 *i*). Indeed, let's consider a slight variation of Example *1.13.32*. Let $\iota\colon \mathbb{R} \longrightarrow \mathbb{R}[X]$ be the natural inclusion (non-surjective ring homomorphism) and let $J := (X^2+1)$ (maximal) ideal of $\mathbb{R}[X]$. We have $\sqrt{J} = J$ (as J is prime), $\sqrt[R]{J} = (1)$ (as computed in *1.13.32*), $\iota^{-1}(\sqrt{J}) = \iota^{-1}(J) = \mathbb{R} \cap J = (0)$, while $\iota^{-1}(\sqrt[R]{J}) = \iota^{-1}(\mathbb{R}[X]) = \mathbb{R}[X] \cap \mathbb{R} = \mathbb{R}$. Hence 1.14.4 *l*) is optimal as stated, though, apparently, less general than 1.9.5 *k*).

1.14.6. Remark. — Let K be any field and let $f = h_1^{m_1} \cdots h_r^{m_r} \in K[X_1, \ldots, X_n] = K[\underline{X}]$, with h_i irreducible polynomials pairwise distinct (recall that $K[\underline{X}]$ is a unique factorization domain). Then, as $K[\underline{X}]$ is a UFD, $I := (f) = \bigcap_{i=1}^r (h_i^{m_i})$ and hence the "diagonal" ring homomorphism $\delta_f\colon K[\underline{X}] \longrightarrow K[\underline{X}]/(h_1^{m_1}) \times \cdots \times K[\underline{X}]/(h_r^{m_r})$, such that $p(\underline{X}) \mapsto \left(\overline{p(\underline{X})}^1, \cdots, \overline{p(\underline{X})}^r\right)$, having $\mathrm{Ker}(\Delta_f) = \bigcap_{i=1}^r (h_i^{m_i}) = (f)$, induces an injective ring homomorphism

$$\Delta_f\colon K[\underline{X}]/(f) \hookrightarrow K[\underline{X}]/(h_1^{m_1}) \times \cdots \times K[\underline{X}]/(h_r^{m_r}), \quad \overline{p(\underline{X})} \mapsto \left(\overline{p(\underline{X})}^1, \cdots, \overline{p(\underline{X})}^r\right).$$

Hence if the product ring $K[\underline{X}]/(h_i^{m_i}) \times \cdots \times K[\underline{X}]/(h_r^{m_r})$ is real, also its "subring" $K[\underline{X}]/(f)$ is such, (f) is then real and $\sqrt[R]{(f)} = (f)$. This construction shows, for example, that any product of distinct linear forms, *i.e.* $m_i = 1$ and $h_i = l_i$ with $\deg l_i = 1$, gives rise to a principal real ideal with generator $f = l_1 \cdots l_r$. For $n = 1$, in which case $K[X]$ is even an Euclidean domain, then the above ring homomorphism is actually an isomorphism $\Delta_f \colon K[X]/(f) \xrightarrow{\cong} K[X]/(h_1^{m_1}) \times \cdots \times K[X]/(h_r^{m_r})$. Hence, as a real ideal is radical, in order to $K[X]/(f)$ to be real it must have no nilpotent elements, hence $m_i = 1$ for each $i = 1, \cdots, r$, and each subring $K[X]/(h_i)$ as to be real. This reduces the question to that of classify irreducible polynomials h of $K[X]$ such that the (prime) ideal (h) is real. We will complete this discussion in the general case towards the end of next chapter, cf. *2.18.6* and *2.18.7*.

1.14.7. Proposition (maximal ideals of $K[X]$ with K real-closed). — *Let K be a real-closed field, and let $f \in K[X]$ be a monic polynomial of positive degree d. Then the following facts hold.*

a) (f) *is maximal if and only if either $d = 1$ or $d = 2$ and f is a sum of non-zero squares.*

b) $\sqrt[R]{(f)} = (R\text{-}sqfree(f))$, *where R-sqfree(f), the* **real square free part** *of f, is the product of the distinct linear factors of f, or 1 if there are no such factors.*

c) (f) *is real if and only if f has d distinct roots all in K.*

d) (f) *is a real maximal ideal if and only if $d = 1$.*

Proof. — *a)* Since K is field, $K[X]$ is a Euclidean domain and so its maximal ideals are principal ideals with an irreducible generator $f \in K[X]$. As K is real-closed, from 1.13.30, f is either linear (degree one) or quadratic with no roots in K (degree two). In the latter case, as we can always write $f = X^2 + 2sX + p = (X + s)^2 + p - s^2$ we get f has no root in K if and only if $p - s^2 > 0$. Indeed, by 1.13.24 either $K(\sqrt{p - s^2})$ is real or $K(\sqrt{s^2 - p})$ is real, but K is real-closed hence either $K(\sqrt{p - s^2}) = K$ or $K(\sqrt{s^2 - p}) = K$, that is either $\sqrt{p - s^2} \in K$ or $\sqrt{s^2 - p} \in K$. In the former case $f = (X + s)^2 + \left(\sqrt{p - s^2}\right)^2$ is a sum squares and $\sqrt{p - s^2} \neq 0$, else f is not irreducible, while in the latter case $f = (X + s)^2 - (\sqrt{s^2 - p})^2 = (X + s + \sqrt{s^2 - p})(X + s - \sqrt{s^2 - p})$ is not irreducible. Therefore if (f) is maximal f has to be as claimed. For the converse, in both cases f is clearly irreducible hence (f) is a maximal ideal of $K[X]$ by 1.5.14 and 1.5.17.

b) We can write

$$f=\prod_{i=1}^{h}(X-x_i)^{\mu_i}\prod_{j=1}^{k}(X-z_j)^{\nu_j}(X-\overline{z_j})^{\nu_j}=\prod_{i=1}^{h}(X-x_i)^{\mu_i}\prod_{j=1}^{k}(X^2-2\mathbb{R}(z_j)X+N(z_j))^{\nu_j}$$

where $h,k,\mu_i,\nu_j\in\mathbb{N}$, with $\sum_{i=1}^{h}\mu_i+2\sum_{j=1}^{k}\nu_j=d$, and $x_i\in K$, $z_j\in K[i]\setminus K$ the distinct roots of f in $K[i]$, hence the quadratic factors, if any, do not have zeros in K and therefore they are sum of non-zero squares of $K[X]$ as above. Then we get an identity of ideals of $K[X]$

$$(f)=\prod_{i=1}^{h}\Big(X-x_i\Big)^{\mu_i}\prod_{j=1}^{k}\left(\Big(X-\mathbb{R}(z_j)\Big)^2+\Big(\sqrt{N(z_j)-\mathbb{R}(z_j)^2}\Big)^2\right)^{\nu_j},$$

and by 1.14.4 *h*), *a*) we find

$$\begin{aligned}\sqrt[R]{(f)}&=\bigcap_{i=1}^{h}\sqrt[R]{(X-x_i)^{\mu_i}}\cap\bigcap_{j=1}^{k}\sqrt[R]{\left(\Big(X-\mathbb{R}(z_j)\Big)^2+\Big(\sqrt{N(z_j)-\mathbb{R}(z_j)^2}\Big)^2\right)^{\nu_j}}\\&=\bigcap_{i=1}^{h}(X-x_i)\cap\bigcap_{j=1}^{k}\sqrt[R]{\left(X-\mathbb{R}(z_j),\ \sqrt{N(z_j)-\mathbb{R}(z_j)^2}\right)}\\&=\left(\prod_{i=1}^{h}(X-x_i)\right)\cap\bigcap_{j=1}^{k}(1)=\big((X-x_1)\cdots(X-x_h)\big)\cap(1)\\&=\big(\text{R-sqfree}(f)\big).\end{aligned}$$

Note that in the above writing we might have $h=0$, *i.e.* f has no roots in K, in which case R-sqfree$(f)=1$, or $k=0$ *i.e.* f has all its roots in K and R-sqfree(f) coincides with its usual squarefree part. *c*) and *d*) follows now as corollaries of *a*) and *b*). □

CHAPTER 2

(AFFINE) ALGEBRAIC GEOMETRY

In this chapter we will give an elementary, yet quite thorough, survey of affine algebraic geometry with major emphasis on the tools we will need for the applications to dynamical systems. Then, we recall and fix some terminology from algebraic geometry. The standard basic references for the subject, such as [**Har77**] or [**Sha13**], are partially of use because we specifically need a careful treatment of algebraic sets over a not algebraically closed field, therefore we will greatly refer to [**Kun85**] and [**BCR98**] among others. Let K and L be two fields, with K subfield of L (hence $K \subseteq L$), and let $\mathbb{A}^n_L := L^n$ be the **n-dimensional affine space over** L and $K[\underline{X}] = K[X_1, \ldots, X_n]$ the ring of multivariate polynomials in n indeterminates $X_1, \ldots, X_n$ with coefficients in the subfield K. The starting point of this kind of geometry is the interplay between the left and right annihilators of the natural pairing $\mathbb{A}^n_L \times K[X_1, \ldots, X_n] \longrightarrow L, \quad (P, f) \mapsto < P, f >= \mathrm{ev}_P := f(P)$, where $\mathrm{Ann}_{K[\underline{X}]}(P) = \{f \in K[\underline{X}] \mid f(P) = 0\} = \mathcal{I}(P) \subseteq K[\underline{X}]$ is the "vanishing ideal" of the point P, and $\mathrm{Ann}_{\mathbb{A}^n_L}(f) = \{P \in \mathbb{A}^n_L \mid f(P) = 0\} = \mathcal{Z}(f) \subseteq \mathbb{A}^n_L$ is the "zero locus" of the polynomial f.

2.1. Affine K-algebraic sets of $\mathbb{A}^n_L$

2.1.1. Definition (zero locus $\mathcal{Z}$). — Given a family of polynomials $T \subseteq K[\underline{X}]$ (the "equations") its set of zeros in $\mathbb{A}^n_L$

$$\mathcal{Z}^L_K(T) := \{P = (a_1, \ldots, a_n) \in \mathbb{A}^n_L \mid f(P) = 0 \quad \forall f \in T\} = \bigcap_{f \in T} \mathcal{Z}^L_K(f) = \bigcap_{f \in T} f^{-1}(0) \subseteq \mathbb{A}^n_L$$

is called an **(affine K-)algebraic subset** of $\mathbb{A}^n_L$, or **(affine) K-algebraic set** in $\mathbb{A}^n_L$ for short. To simplify the notation, in what follows we write $\mathcal{Z} = \mathcal{Z}^L_K$ unless the specification is needed.

2.1.2. Remark. — If $T = \{f_1, \ldots, f_t\}$ then $V = \mathcal{Z}(T) = \{P \in \mathbb{A}^n_L \mid f_1(P) = \cdots = f_t(P) = 0\}$ is nothing but the set of solutions in $\mathbb{A}^n_L$ of the system of polynomial equations $f_1 = \cdots = f_t = 0$.

2.1.3. Beahviour of $\mathcal{Z}^L_K$ under field extensions. — Let $K \subset H \subset L$ a composite of field extensions, then $\mathbb{A}^n_K \subseteq \mathbb{A}^n_H \subseteq \mathbb{A}^n_L$ and $K[\underline{X}] \subseteq H[\underline{X}] \subseteq L[\underline{X}]$. If $T \subseteq K[\underline{X}]$ is a set of polynomial equations, then: $\mathcal{Z}^K_K(T) \subseteq \mathcal{Z}^H_K(T) = \mathcal{Z}^H_H(T) \subseteq \mathcal{Z}^L_K(T) \subseteq \mathcal{Z}^L_K(T) = \mathcal{Z}^L_L(T)$. A key fact in dealing with these kind fo situations in given is the following result.

2.1.4. Proposition. — *Let $K \subseteq L$ be any field extension and I an ideal of $K[\underline{X}]$. Then we have $IL[\underline{X}] \cap K[\underline{X}] = I$. In particular, we have $1 \in IL[\underline{X}]$ if and only if $1 \in I$ (in $K[\underline{X}]$).*

Proof. — See [**KR00**, Prop. 2.6.12]. □

2.1.5. Remark. — It follows immediately that the ideal generated by the family of polynomials T, as well as its radical, have the same set of zeros of the starting set: $\mathcal{Z}(T) = \mathcal{Z}((T)) = \mathcal{Z}(\sqrt{(T)})$, more generally we have: $\mathcal{Z}(T') = \mathcal{Z}(T)$ for any $T' \subseteq K[\underline{X}]$ such that $T \subseteq (T') \subseteq \sqrt{(T)}$. We note therefore that the assignment, from subsets $T \mapsto \mathcal{Z}(T)$ of $K[\underline{X}]$ to subsets of $\mathbb{A}^n_L$, is a highly non injective one.

2.1.6. Remark (finiteness of the number of equations). — In particular, from the remark above, being the ring $K[\underline{X}]$ Noetherian by *Hilbert Basis Theorem* ([**Kun85**, Ch. 1, Prop. 2.3]), it follows that *every K-algebraic set $V = \mathcal{Z}(T) \subseteq \mathbb{A}^n_L$ is the zero locus of a finite number of polynomials* (because (T) is always a finitely generated ideal, even if T is an infinite set of polynomials).

2.1.7. Lattice properties of $\mathcal{Z}$. — Any finite union of K-algebraic sets is a K-algebraic set:

$$\bigcup_{i=1}^{s} \mathcal{Z}(T_i) = \mathcal{Z}(\bigcap_{i=1}^{s}(T_i)) = \mathcal{Z}((T_1)\cdots(T_s)) \text{ (product of ideals)},$$

and any intersection (also infinte ones) of K-algebraic sets is such:

$$\bigcap_i \mathcal{Z}(T_i) = \mathcal{Z}(\bigcup_i T_i) = \mathcal{Z}(\Sigma_i(T_i)) \text{ (sum of ideals)}.$$

2.1.8. $\mathcal{Z}$ is inclusion-reversing. — Obviously we have: $T_1 \subseteq T_2 \subseteq K[\underline{X}] \Rightarrow \mathcal{Z}(T_1) \supseteq \mathcal{Z}(T_2) \subseteq \mathbb{A}^n_L$, hence the mapping $\mathcal{Z}$ form subsets of $K[\underline{X}]$ to subsets of $\mathbb{A}^n_L$ is a reversing order one (weakly decreasing), and *it can be restricted to a decreasing mapping between radical ideals of $K[\underline{X}]$ and K-algebraic sets of $\mathbb{A}^n_L$*. Note that, nonetheless, for $n = 1$, $\mathfrak{M}_1 := (X^2 + 1)$ and $\mathfrak{M}_2 := (X^2 + 2)$ are two maximal (hence radical) ideals of $\mathbb{Q}[X]$ having the same set of $\mathbb{R}$-zeros: $\mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(\mathfrak{M}_1) = \emptyset = \mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(\mathfrak{M}_2)$; this kind of problems can happen any time the (bigger) field L is not algebraically closed.

2.2. Basic examples and constructions

2.2.1. Example: the empty set and the whole space. — We always have: $\emptyset = \mathcal{Z}(1) = \mathcal{Z}(K[\underline{X}])$ and $\mathbb{A}^n_L = \mathcal{Z}(0)$, hence $\emptyset$ and $\mathbb{A}^n_L$ are K-algebraic sets.

2.2.2. Example: K-rational points of $\mathbb{A}^n_L$. — If $P = (a_1, \ldots, a_n) \in \mathbb{A}^n_L$ is a **K-rational point**, that is $a_i \in K$ for each i, then $\{P\} = \mathcal{Z}(X_1 - a_1, \ldots, X_n - a_n)$ is a K-algebraic set. Note that $\mathfrak{m}_P := (X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal of $K[\underline{X}]$ (indeed, the quotient ring $K[\underline{X}]/(X_1 - a_1, \ldots, X_n - a_n) \cong K$, a field). Note also that if $P \in \mathbb{A}^n_L \setminus \mathbb{A}^n_K$ it may happen that $\{P\}$ is not a K-algebraic set in $\mathbb{A}^n_L$ (cf. *2.4.3*).

2.2.3. Example: the diagonal Δ_n of $\mathbb{A}^{2n}_L$. — The zero set of the (prime) ideal $\mathfrak{d}_{\mathfrak{n}} := (X_1 - Y_1, \ldots, X_n - Y_n) \subseteq K[\underline{X}, \underline{Y}] := K[X_1, \ldots, X_n; Y_1, \ldots, Y_n]$ coincides with the *diagonal subspace* of the product $\mathbb{A}^n_L \times \mathbb{A}^n_L \cong \mathbb{A}^{2n}_L$, *i.e.* $\mathcal{Z}(\mathfrak{d}_{\mathfrak{n}}) = \{(\underline{a}, \underline{b}) \in \mathbb{A}^{2n}_L \mid \underline{a} = \underline{b}\} =: \Delta_n$.

2.2.4. Example: K-rational "slices". — For each $\underline{a} \in \mathbb{A}^n_K$, the subspace ("cylinder") $\{\underline{a}\} \times \mathbb{A}^n_L$ is a K-algebraic set in $\mathbb{A}^{n+m}_L$, indeed: $\{\underline{a}\} \times \mathbb{A}^m_L = \mathcal{Z}(X_1 - a_1, \ldots, X_n - a_n)$, where the polynomials $X_1 - a_1, \ldots, X_n - a_n \in K[\underline{X}]$ are thought of as elements of the larger polynomial ring $K[\underline{X}, Y_1, \ldots, Y_m]$. Obviously, $\{\underline{a}\} \times \mathbb{A}^m_L$ is the zero set of the (prime) ideal $\mathfrak{m}_{\underline{a}} K[\underline{Y}]$, extended to $K[\underline{X}, Y_1, \ldots, Y_m]$ from the maximal ideal $\mathfrak{m}_{\underline{a}}$ of $K[\underline{X}]$. Note that if $P \in \mathbb{A}^n_L \setminus \mathbb{A}^n_K$ it may happen that $\{P\} \times \mathbb{A}^m_L$ is not a a K-algebraic set in $\mathbb{A}^{n+m}_L$.

2.2.5. Example: "cylindrical" algebraic sets. — More generally, if $V = Z(f_1, \ldots, f_r)$ is a K-algebraic subset of $\mathbb{A}^n_L$, then its **cylinder** in $\mathbb{A}^{n+m}_L = \mathbb{A}^n_L \times \mathbb{A}^m_L$ is defined by the same

equations (ideal) of V but thought of as functions on the larger space:

$$\mathrm{Cyl}_{\mathbb{A}^m_L}(V) := V \times \mathbb{A}^m_L = \mathcal{Z}(f_1, \ldots, f_r) = \mathcal{Z}((f_1, \ldots, f_r)K[\underline{X}, Y_1, \ldots, Y_m])$$

where the polynomials $f_1, \ldots, f_r \in K[\underline{X}]$ are thought of as elements of $K[\underline{X}, Y_1, \ldots, Y_m]$.

2.2.6. Example: cartesian products of algebraic sets. — If $V = Z(f_1, \ldots, f_r) \subseteq \mathbb{A}^n_L$ and $W = Z(g_1, \ldots, g_s) \subseteq \mathbb{A}^m_L$ we then have for their **cartesian product** in $\mathbb{A}^{n+m}_L = \mathbb{A}^n_L \times \mathbb{A}^m_L$:

$$\begin{aligned} V \times W &= (V \times \mathbb{A}^m_L) \cap (\mathbb{A}^n_L \times W) = \mathcal{Z}(f_1, \ldots, f_r, g_1, \ldots, g_s) \\ &= \mathcal{Z}((f_1(\underline{X}), \ldots, f_r(\underline{X}))K[Y_1, \ldots, Y_m] + (g_1(\underline{Y}), \ldots, g_s(\underline{Y}))K[X_1, \ldots, X_n]). \end{aligned}$$

2.3. Zariski topology on $\mathbb{A}^n_L$ relative to K

As seen in the above examples (cf. *2.2.1*) the family of all K-algebraic sets of $\mathbb{A}^n_L$ contains the empty set and the whole affine space, and from 2.1.7 it is also closed under finite unions and arbitrary intersections. Therefore it is the family of closed subsets for a topology on $\mathbb{A}^n_L$. This topology is known as the **Zarisky topology** on $\mathbb{A}^n_L$ (relative to K), see [**Kun85**, Ch. I, Cor. 2.7].

2.3.1. Distinguished open subsets. — A *basis of open subsets* for this topology is given by the subsets of the form $D_f := \mathbb{A}^n_L \setminus \mathcal{Z}(f)$ where $f \in A_k$, called **distinguished open sets**. Moreover $D_{f_1} \cap D_{f_2} = D_{f_1 f_2}$.

Proof. — Indeed: $\emptyset = D_0$, $\mathbb{A}^n_L = D_1$, if $U = \mathbb{A}^n_L \setminus \mathcal{Z}(T)$, with $T \subseteq K[\underline{X}]$, is a generic open subset of $\mathbb{A}^n_L$ then $U = \mathbb{A}^n_L \setminus \mathcal{Z}(T) = \mathbb{A}^n_L \setminus \bigcap_{f \in T} \mathcal{Z}(f) = \bigcup_{f \in T} \mathbb{A}^n_L \setminus \mathcal{Z}(f) = \bigcup_{f \in T} D_f$. The last assertion is straightforward. □

Note that, if L is an infinite field, none non trivial distinguished open sets can be (set theoretically) a K-algebraic set of $\mathbb{A}^n_L$, indeed it can be shown that they are in this case actually dense subsets of the affine space: $\overline{D_f}^Z = \mathbb{A}^n_L$ (where $\overline{S}^Z$, the "Zariski closure" of S, is the closure of S in the Zariski topology of $\mathbb{A}^n_L$ with respect to K). If $P \in \mathbb{A}^n_K$ a **fundamental system of neighborhoods** for P is given by $\{D_f \mid P \in D_f\} = \{\mathbb{A}^n_L \setminus \mathcal{Z}(f) \mid f \in K[\underline{X}] \text{ and } f(P) = 0\}$.

2.3.2. Noetherianity. — As $K[\underline{X}]$ is a Noetherian ring, it satisfies the Ascending Chain Condition on ideals, and as $\mathcal{Z}_K^L$ is an inclusion-reversing map, then the Zariski topology on $\mathbb{A}_L^n$ satisfies a descending chain condition on closed subsets: if $C_0 \supseteq C_1 \supseteq \cdots \supseteq C_i \supseteq \cdots$, with C_i closed algebraic subsets, then $C_i = C_N \ \forall i \geq N$ for some $N \in \mathbb{N}$. We say that $\mathbb{A}_L^n$, with the Zariski topology, is a **Noetherian topological space** ([**Kun85**, Def. 2.13]).

2.4. Remarks and examples on Zariski topology

2.4.1. Remark: behavior under base field extension. — If $H \subseteq K$ are both subfields of L, then $H[\underline{X}] \subseteq K[\underline{X}]$; and so if $T \subseteq H[\underline{X}]$, then $\mathcal{Z}_H^L(T) = \mathcal{Z}_K^L(T)$. This means that any closed subset of $\mathbb{A}_L^n$ which is Zariski closed relative to H is also Zariski closed relative to K, therefore the second topology is finer than the first one.

2.4.2. Example: Zariski topology on $\mathbb{A}_L^1$ relative to K. — For $n = 1$, every ideal of $K[x]$ is principal (it is indeed an Euclidean domain [**Lan02**,]), and the closed subset of $\mathbb{A}_L^1$ for this topology are exactly $\mathbb{A}_L^1$, $\emptyset$, and those finite subsets C of L such that $C = \mathcal{Z}^L(f)$ for some $f \in K[x]$ (in particular, every element of C must be *algebraic over the subfield* K).
If $L = K$ this simply reduces to $\mathbb{A}_L^1$ and all the finite subsets of L, and hence Zariski topology relative to L itself on $\mathbb{A}_L^1$ is nothing but that cofinite topology (and if L is finite it also coincide with the discrete topology). But if $K \subsetneq L$ not every finite subset of $\mathbb{A}_L^1$ is closed in this topology. In the general case, the Zariski topology on $\mathbb{A}_L^1$, relative to a subfield K of L, is a coarser topology than the cofinite topology on L.

2.4.3. Critical example: if $K \subsetneq L$, Zariski topology can be not even T_1. — Even for $n = 1$ several issues may happen, note indeed that:

a) With $K = \mathbb{R}$ and $L = \mathbb{C}$ we have $\mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(X^2 + 1) = \emptyset$, while $\mathcal{Z}_{\mathbb{R}}^{\mathbb{C}}(X^2 + 1) = \{-i, i\}$ but it can be shown that neither $\{i\}$ nor $\{-i\}$ are, separately, $\mathbb{R}$-algebraic sets of $\mathbb{A}_{\mathbb{C}}^1 = \mathbb{C}$. Indeed, the crucial point, whose proof is elementary, is the following:

$$\{f \in \mathbb{R}[X] \mid f(i) = 0\} = \{f \in \mathbb{R}[X] \mid f(-i) = 0\} = (X^2 + 1) \ \text{ in } \ \mathbb{R}[X].$$

Hence, in general, points can be not always closed for this topology if $K \neq L$, unless they are K-rational.

b) With $K=\mathbb{Q}$, $H=\mathbb{Q}(\sqrt[3]{2})$ and $L=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}e^{i\frac{2}{3}\pi})$ (the last one is the splitting field of the polynomial $x^3-2\in\mathbb{Q}[X]$), we have: $\mathcal{Z}_K^H(X^3-2)=\mathcal{Z}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt[3]{2})}(X^3-2)=\{\sqrt[3]{2}\}\subseteq\mathbb{A}^1_{\mathbb{Q}(\sqrt[3]{2})}$ is a closed subset of $\mathbb{A}^1_{\mathbb{Q}(\sqrt[3]{2})}$; but

$$\mathcal{Z}_K^L(X^3-2)=\mathcal{Z}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}e^{i\frac{2}{3}\pi})}(X^3-2)=\{\sqrt[3]{2},\ \sqrt[3]{2}e^{i\frac{2}{3}\pi},\ \sqrt[3]{2}e^{i\frac{4}{3}\pi}\}\subseteq\mathbb{A}^1_{\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}e^{i\frac{2}{3}\pi})}$$

and none of $\{\sqrt[3]{2}\}$, $\{\sqrt[3]{2}e^{i\frac{2}{3}\pi}\}$, $\{\sqrt[3]{2}e^{i\frac{4}{3}\pi}\}$ is alone in itself a closed subset of $\mathbb{A}^1_L$ in the Zariski topology relative to $\mathbb{Q}$. Also in this case, the crucial point is:

$$\begin{aligned}\{f\in\mathbb{Q}[X]\mid f(\sqrt[3]{2})=0\}&=\{f\in\mathbb{Q}[X]\mid f(\sqrt[3]{2}e^{i\frac{2}{3}\pi})=0\}\\&=\{f\in\mathbb{Q}[X]\mid f(\sqrt[3]{2}e^{i\frac{4}{3}\pi})=0\}=(X^3-2)\ \text{ in }\ \mathbb{Q}[X].\end{aligned}$$

2.4.4. Zariski topology on $\mathbb{A}^n_L$ over a finite field L is discrete. — If $K=L$ is a finite field, it can be shown ([**Kun85**, Ch. I, Sec. 1, Exercise 6]) that the Zariski topology on $\mathbb{A}^n_K=K^n$ (finite set) relative to K is the discrete topology.

2.4.5. Special feature of non algebraically closed fields. — If K is not algebraically closed, as it is for $K=\mathbb{R}$, we also have this peculiar behavior: any K-algebraic set $V\subseteq\mathbb{A}^n_K$ can be written as the zero set of a single polynomial in $K[\underline{X}]$ [1]. For $K=\mathbb{R}$ this is clear: let V be defined by the equations $f_1=\cdots=f_t=0$ with $f_i\in\mathbb{R}[\underline{X}]$, then $V=\mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(f_1^2+\cdots+f_t^2)$ (see also [**Kun85**, Exercise 3, Ch. I.1]). Note, though, that $\mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(X^2+Y^2)=\{(0,0)\}$ is just a point, while $\mathcal{Z}_{\mathbb{R}}^{\mathbb{C}}(X^2+Y^2)$ contains the infinitely many points $(a,\pm ia)\in\mathbb{C}^2$, with $a\in\mathbb{R}$, (union of two complex lines).

2.4.6. Remark: not a Hausdorff topology. — As soon as L is an infinite field, the Zariski topology on $\mathbb{A}^n_L$ relative to K is not a Hausdorff one, this is clear when $n=1$ (cf. 2.4.2 and 2.4.3) because, as Zariski topology (relative to K) on $\mathbb{A}^1_L$ is coarser than cofinite topology, open subsets are then complement of (certain) finite sets and therefore they always have nonempty intersection. As it can be verified that $\mathbb{A}^1_L\cong\mathcal{Z}_K^L(X_1)\subseteq\mathbb{A}^n_L$, with $X_1\in K[\underline{X}]$, is a topological

1. It's clearly enough to show that, if L is not algebraically closed, for each $r\in\mathbb{N}_+$ there exists $\omega_r\in L[\underline{Y}]$ such that $\mathcal{Z}_L^L(\omega_r)$ is reduced to the origin of $\mathbb{A}^r_L$. This can be done as follows: as L is not algebraically closed there is a $p(X)\in L[X]$ such that $p(a)\neq 0$ for all $a\in L$. Let d be the degree of p. Define $\omega_1:=Y_1$, $\omega_2:=Y_2^d p\left(\frac{Y_1}{Y_2}\right)$ be the homogenization of p (then $\mathcal{Z}_L^L(\omega_2(Y_1,Y_2))=\{(0,0)\}$), and set inductively $\omega_{n+1}=\omega_2(\omega_n(Y_1,\cdots,Y_n),Y_n+1)$. Even a more general result holds true: if $K\subseteq H\subseteq\overline{K}$ is a tower of fields, where $\overline{K}$ is an algebraic closure of K and H is not algebraically closed (*i.e.* $H\subsetneq\overline{K}$), then for each $m\in\mathbb{N}_+$ there exists a homogeneus polynomial $p\in K[Y_1,\ldots,Y_m]$ such that $\mathcal{Z}_K^H(p)=\{0_{\mathbb{A}^m_H}\}$ ([**Lak87**, Prop. 5]).

subspace of $\mathbb{A}^n_L$ with respect to the Zariski topology relative to K, then $\mathbb{A}^n_L$ is not a Hausdorff space too. More generally, it can be shown that if K is infinite, any two non empty open subsets of $\mathbb{A}^n_L$ must intersect because, in this case, $\mathbb{A}^n_L$ is an *irreducible* topological space in this topology (see [**Kun85**, Ch. I, Sections 1 and 2]). See also 2.8.4 for another general argument on the non separateness of Zariski topology on $\mathbb{A}^n_L$.

2.4.7. Remark. — After characterizing the *closure operator* of this topology (see *2.12.3*), it's not difficult to show that $\mathbb{A}^n_K$ is a dense subset of $\mathbb{A}^n_L$ (with respect to the Zariski topology on $\mathbb{A}^n_L$ with respect to K) if and only if K is infinite or $K = L$.

2.4.8. Remark: comparison with the Euclidean topology on $\mathbb{R}^n$. — In the case $K = L = \mathbb{R}$, as every polynomial function is continuous with respect to the usual Euclidean topology, every Zarisky closed subset of $\mathbb{A}^n_{\mathbb{R}}$ is also closed in the Euclidean topology. But, though, in this case, Zariski topology has closed points, it is not a Hausdorff topology (as $K = \mathbb{R}$ is infinite), therefore the Zariski topology on $\mathbb{A}^n_{\mathbb{R}} = \mathbb{R}^n$, relative to $\mathbb{R}$, is a much coarser topology than the usual Euclidean one.

2.4.9. Subspace Zariski topology. — Any subset $S \subseteq \mathbb{A}^n_L$ inherits the subspace topology from the Zarisky topology on $\mathbb{A}^n_L$ (relative to K), this is also called Zarisky topology on S (relative to K); its closed subsets are those of the form $S \cap \mathcal{Z}^L_K(I)$ as I varies among the ideals of $K[\underline{X}]$.

2.5. Regular (polynomial) functions on K-algebraic set. The coordinate ring.

In Algebraic Geometry, one regards polynomials of $K[\underline{X}]$ as *functions* on the affine space $\mathbb{A}^n_L$. These clearly form a K-subalgebra of the K-algebra of all functions from $\mathbb{A}^n_L$ to $\mathbb{A}^1_L = L$. Moreover, they can be described just as linear combinations of products of powers ("terms" or "monomials") of coordinates of points of $\mathbb{A}^n_L$. Formally, we can say that their K-subalgebra $K[\mathbb{A}^n_L]$ is generated by the coordinate (functions) of $\mathbb{A}^n_L$.

2.5.1. Definition. — Le S be a subset of $\mathbb{A}^n_L$, and $\varphi\colon S \longrightarrow L$ a L-valued function on S. Then φ is said to be a **K-regular function** (or a **K-polynomial function**) on S if there exists a polynomial $f \in K[X_1, \ldots, X_n]$ such that $\varphi = f_{|S}$ [2].

2.5.2. Definition (Coordinate ring $K[S]_L$). — Let S be a subset of $\mathbb{A}^n_L$, then its **coordinate ring (over K)** is the K-algebra of all K-regular functions on S, $K[S]_L := \{f_{|S} \mid f \in K[\underline{X}]\}$. Hence $K[S]_L = K[X_{1|S}, \ldots, X_{n|S}]$ as a K-subalgebra of the algebra of all functions from S to L. Whenever $L = K$ we simply write $K[S] := K[S]_K$.

2.5.3. Remark: $K[S]_L$ are affine K-algebras. — Coordinate rings are clearly reduced and finitely generated K-algebras, hence they are affine K-algebras.

2.5.4. Definition (Zero locus of a regular function). — Le S be a subset of $\mathbb{A}^n_L$, and $\varphi \in K[S]_L$ a K-regular function on it. Then we define the **zero locus of** φ as $\mathcal{Z}(\varphi) = \mathcal{Z}^L_K(\varphi) := \{P \in S \mid \varphi(P) = 0\}$.

2.5.5. Remark. — Choosing a representative for φ, such as $\varphi = f_{|S}$, with $f \in K[X_1, \ldots, X_n]$, we see that $\mathcal{Z}(\varphi) = \mathcal{Z}(f) \cap S$. Hence $\mathcal{Z}(\varphi)$ is a closed subset of S. And if $g \in K[X_1, \ldots, X_n]$ is another representative for φ, then $f_{|S} = g_{|S} \Rightarrow \mathcal{Z}(f) \cap S = \mathcal{Z}(g) \cap S$. Hence, the set $\mathcal{Z}(\varphi)$ does not depend on the specific representative choosen.

2.5.6. Example: $K[\mathbb{A}^n_L]_L \cong K[\underline{X}]$ if L is infinite. — By definition, $K[\mathbb{A}^n_L]_L = K[X_{1|\mathbb{A}^n_L}, \ldots, X_{n|\mathbb{A}^n_L}]$, where the notation $X_{i|\mathbb{A}^n_L}$ should remember that X_i is thought of as a function on $\mathbb{A}^n_L$ instead of the indeterminate X_i, hence X_i corresponds to the i-th projection $\mathrm{pr}_i\colon \mathbb{A}^n_L \longrightarrow \mathbb{A}^1_L$ and $K[\mathbb{A}^n_L]_L \cong K[X_1, \cdots, X_n]$ as soon as L is infinite [3].

---

2. Note that, though $f \in K[X_1, \ldots, X_n]$, the function $f_{|S}$ may assume values in L which do not belong to K. Examples: $\varphi = X_{1|\mathbb{A}^1_{\mathbb{C}}}\colon \mathbb{A}^1_{\mathbb{C}} = \mathcal{Z}^{\mathbb{C}}_{\mathbb{R}}(0) \longrightarrow \mathbb{C}$, then $\varphi(i) = i \in \mathbb{C} \setminus \mathbb{R}$; or $V = \mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(X_1 - X_2) = \{(a, a) \mid a \in \mathbb{R}\}$, and $\varphi = X_{1|S}$, then $\varphi(\pi, \pi) = \pi \in \mathbb{R} \setminus \mathbb{Q}$.

3. While $K[\mathbb{A}^n_L]_L \cong K[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$ if $L = \mathbb{F}_q$ the finite field with $q = p^k$ elements (p a prime integer).

2.5.7. Example: $K[\emptyset]_L = (0)$. — Quite easily $K[\emptyset]_L = K[\mathcal{Z}(1)]_L = (0)$ is the "zero K-algebra": there is only one function from the empty set to $\mathbb{A}^1_L$, the empty function.
But note that $\mathbb{R}[\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X^2+1)]_{\mathbb{R}} = \mathbb{R}[\emptyset]_{\mathbb{R}} = (0)$, while

$$\mathbb{R}[\mathcal{Z}^{\mathbb{C}}_{\mathbb{R}}(X^2+1)]_{\mathbb{C}} = \mathbb{R}[\mathcal{Z}^{\mathbb{C}}_{\mathbb{R}}(X+i) \cup \mathcal{Z}^{\mathbb{C}}_{\mathbb{R}}(X-i)]_{\mathbb{C}} = \mathbb{R}[\{-i\} \cup \{i\}]_{\mathbb{C}} \cong \mathbb{C} \times \mathbb{C}.$$

2.5.8. Example: $K[P]_L \cong K$ if P is K-rational. — Let P be a K-rational point in $\mathbb{A}^n_L$, then a K-regular function φ on $\{P\} = \mathcal{Z}(\mathfrak{m}_P)$ is uniquely determined by its value $\varphi(P)$, which must be an element of $\mathbb{A}^1_K \subseteq \mathbb{A}^1_L$ because $\varphi = f_{|\{P\}}$ for some $f \in K[\underline{X}]$ and the coordinates of P are in K. Therefore $K[P]_L \cong K$ if P is a K-rational point.

2.5.9. Example. — Let $K = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$, and let $V = \mathcal{Z}(X^2-2) = \{-\sqrt{2}, \sqrt{2}\}$, then

$$K[V]_L = \mathbb{Q}[\{-\sqrt{2}, \sqrt{2}\}]_{\mathbb{Q}(\sqrt{2})} \cong \mathbb{Q}(\sqrt{2}), \quad \text{via } \varphi \mapsto \mathrm{ev}_{\sqrt{2}}(\varphi) = \varphi(\sqrt{2}) \in \mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}),$$

indeed, this is clearly a K-algebra homomorphism which is easily seen to be bijective. The main point is again that $\{f \in \mathbb{Q}[X] \mid f(\sqrt{2}) = 0\} = \{f \in \mathbb{Q}[X] \mid f(-\sqrt{2}) = 0\} = (X^2-2)$ in $\mathbb{Q}[X]$.

If $K = \mathbb{Q}$, $L = \mathbb{Q}[\sqrt[3]{5}] = \mathbb{Q}(\sqrt[3]{5})$, and $V = \mathcal{Z}(X^3-5) = \{\sqrt[3]{5}\}$, then, as above,

$$\mathbb{Q}[\mathcal{Z}(X^3-5)]_{\mathbb{Q}(\sqrt[3]{5})} = \mathbb{Q}[\{\sqrt[3]{5}\}]_{\mathbb{Q}(\sqrt[3]{5})} \cong \mathbb{Q}(\sqrt[3]{5}), \text{ via } \varphi \mapsto \varphi(\sqrt[3]{5}),$$

and also taking $L = \mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{5}e^{i\frac{2}{3}\pi}, \sqrt[3]{5}e^{i\frac{4}{3}\pi})$ (the splitting field over $\mathbb{Q}$ of X^3-5), or even $L = \overline{\mathbb{Q}}$,

$$\mathbb{Q}[\mathcal{Z}(X^3-5)]_L = \mathbb{Q}[\{\sqrt[3]{5}, \sqrt[3]{5}e^{i\frac{2}{3}\pi}, \sqrt[3]{5}e^{i\frac{4}{3}\pi}\}]_{\overline{\mathbb{Q}}} \cong \mathbb{Q}[\sqrt[3]{5}] = \mathbb{Q}(\sqrt[3]{5}), \text{ via } \varphi \mapsto \varphi(\sqrt[3]{5}),$$

again because

$$\begin{aligned}\{f \in \mathbb{Q}[X] \mid f(\sqrt[3]{5}) = 0\} &= \{f \in \mathbb{Q}[X] \mid f(\sqrt[3]{5}e^{i\frac{2}{3}\pi}) = 0\} \\ &= \{f \in \mathbb{Q}[X] \mid f(\sqrt[3]{5}e^{i\frac{4}{3}\pi}) = 0\} = (X^3-5) \text{ in } \mathbb{Q}[X].\end{aligned}$$

2.5.10. Proposition (continuity of the regular functions). — *If $\varphi \in K[S]_L$, then φ is a continuous function with respect to the Zariski topology on $\mathbb{A}^1_L$ (relative to K) and the subspace topology on S induced by the Zariski topology on $\mathbb{A}^n_L$ (relative to K).*

Proof. — Let $\varphi = f_{|S}$ for some polynomial $f \in K[X_1, \cdots, X_n]$, and let $C = \mathcal{Z}(g)$, with $g \in K[Y]$, be any closed subset of $\mathbb{A}^1_L$ (as all ideals in $K[Y]$ are principal we can always assume C be defined by a single equation), then $\varphi^{-1}(\mathcal{Z}(g)) = S \cap (f^{-1}(g^{-1}(0))) = S \cap Z(g \circ f)$, where

$(g \circ f) = g(f(X_1, \cdots, X_n)) \in K[X_1, \cdots, X_n]$, is a closed subset of S in the subspace topology. □

2.5.11. Proposition ($K[S]_L$ and $K[\overline{S}^Z]_L$ are isomorphic). — *Let S be any subset of $\mathbb{A}^n_L$, then, the inclusion map $\iota\colon S \hookrightarrow \overline{S}^Z$, of S in its Zariski closure $\overline{S}^Z$, induces a ring homomorphism of restriction $\iota^*\colon K[\overline{S}^Z]_L \longrightarrow K[S]_L$, $\varphi \mapsto \varphi \circ \iota = \varphi_{|S}$ which is an isomorphism of rings.*

Proof. — We first note that ι^* is well defined. Indeed, if $\varphi = f_{|\overline{S}^Z}$, with $f \in K[X_1, \cdots, X_n]$, is a regular function on $\overline{S}^Z$, then $\iota^*(\varphi) = \varphi \circ \iota = \varphi_{|S} = (f_{|\overline{S}^Z})_{|S} = f_{|S}$ is also a regular function on S. The map is clearly a ring homomorphism (by definition of ring operations in algebras of functions), and it is also trivially surjective: if $\psi = f_{|S}$ for some $f \in K[X_1, \cdots, X_n]$ then $\psi = \iota^*(f_{|\overline{S}^Z})$. Let's verify that ι^* is also injective. Let $\varphi = f_{|\overline{S}^Z} \in \mathrm{Ker}(\iota^*)$ ($f \in K[X_1, \cdots, X_n]$), then $0 = \iota^*(\varphi) = f_{|S} \Rightarrow S \subseteq \mathcal{Z}(f)$, but then, as $\overline{S}^Z$ is the smallest closed subset containing S, it must be $\overline{S}^Z \subseteq \mathcal{Z}(f)$. Therefore $\varphi = f_{|\overline{S}^Z} = 0$ in $K[\overline{S}^Z]_L$, and hence ι^* is injective. □

In light of the above proposition there is no point in considering $K[S]$ with S not closed, hence from now on we will always work with coordinate rings of K-algebraic subsets of affine spaces.

2.5.12. Proposition ($K[V \times W]_L$ and $K[V]_L \otimes_K K[W]_L$). — *Let $K \subseteq L$ be any field extension, and let V be a K-rational subset of $\mathbb{A}^n_L$ and W be a K-rational subset of $\mathbb{A}^m_L$. Then we have a surjective K-bilinear homomorphism $\mu = \mu^L_K\colon K[V]_L \times_K K[W]_L \longrightarrow K[V \times W]_L$ such that $(\alpha, \beta) \mapsto \alpha \cdot \beta$, inducing a surjective homomorphism of K-algebras*

$$\mu^{\otimes} = (\mu^L_K)^{\otimes}\colon K[V]_L \otimes_K K[W]_L \longrightarrow K[V \times W]_L,\ \sum_i \alpha_i \otimes \beta_i \mapsto \sum_i \alpha_i \cdot \beta_i$$

and an isomorphism

$$\overline{\mu^{\otimes}} = \overline{(\mu^L_K)^{\otimes}}\colon (K[V]_L \otimes_K K[W]_L)/\,\mathrm{Ker}(\mu^{\otimes}) \longrightarrow K[V \times W]_L,\ \sum_i \overline{\alpha_i \otimes \beta_i} \mapsto \sum_i \alpha_i \cdot \beta_i$$

Proof. — The verifications needed to define μ and $\mu^{\otimes}$ are all straightforward. The maps μ, and $\mu^{\otimes}$, are surjective because a system of K-algebra generators for $K[V \times W]_L$ is given, from its very definition, by the restrictions $\alpha_i := X_{i|V\times W}$ for $i = 1, \ldots, n$ and $\beta_j := Y_{j|V\times W}$ for $j = 1, \ldots, m$,

of the coordinate functions of $\mathbb{A}_L^{n+m}$, and these are in the image of μ, indeed $\mu(\alpha_i, 1_K) = \alpha_i$ for any i, and $\mu(1_K, \beta_j) = \beta_j$ for any i, as well as any "power product" in them:

$$\alpha_1^{h_1} \cdots {\alpha_n}^{h_n} \cdot \beta_1^{k_1} \cdots {\beta_m}^{k_m} = \mu(\alpha_1^{h_1} \cdots {\alpha_n}^{h_n}, \beta_1^{k_1} \cdots {\beta_m}^{k_m}) \text{ for any } \underline{h} \in \mathbb{N}^n, \underline{k} \in \mathbb{N}^m.$$

Hence $K[V \times W]_L = K[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m] = \mathrm{Im}(\mu) = \mathrm{Im}(\mu^{\otimes})$. The last assertion follows then by the standard universal property of the quotient ring. □

2.5.13. Remark ($(\mu_K^L)^{\otimes}$ can have a non zero kernel). — The previous homomorphism $(\mu_K^L)^{\otimes}$ is not always an isomorphism in the general case ($K \subsetneq L$). For example, as $K[V \times W]_K$ is a reduced algebra, its kernel must clearly contain every nilpotent element of $K[V]_L \otimes_K K[W]_L$. It can fail to be an isomorphism even if L is algebraically closed, as shown in 2.10.8. However, if L is algebraically closed, the nilradical of $K[V]_L \otimes_K K[W]_L$ is the major obstruction to $\mu^{\otimes}$ being an isomorphism, as shown by [**Kun85**, Ch. I, Rules 3.12 *c*)] (see also 2.21.1 *o*)). Let's see in the next corollary that, however, if $K = L$ then the kernel $\mathrm{Ker}(\mu^{\otimes})$ is necessarily trivial, and therfore $\mu^{\otimes}$ is an isomorphism of K-algebras.

2.5.14. Corollary ($K[V \times W]_K$ and $K[V]_K \otimes_K K[W]_K$ are isomorphic). — *Let $L = K$ be any field, and let V be a K-rational subset of $\mathbb{A}_K^n$ and W be a K-rational subset of $\mathbb{A}_K^m$. Then the map $K[V]_K \otimes_K K[W]_K \longrightarrow K[V \times W]_K$, $\sum_i \alpha_i \otimes \beta_i \mapsto \sum_i \alpha_i \cdot \beta_i$ is an isomorphism of K-algebras.*

Proof. — From 2.5.12, we only need to show that, if $L = K$, then $\mu^{\otimes}$ is actually injective. To this end, let's start fixing a K-basis $(\varphi_s \otimes \nu_t)_{s \in \mathcal{S}, t \in \mathcal{T}}$ for $K[V]_K \otimes_K K[W]_K$ taking K-bases $(\varphi_s)_{s \in \mathcal{S}}$ for $K[V]$ and $(\nu_t)_{t \in \mathcal{T}}$ for $K[W]$. Thus, let $\sum_{s,t} c_{s,t} \varphi_s \otimes \nu_t \in \mathrm{Ker}(\mu^{\otimes})$ for some $(c_{s,t})_{s \in \mathcal{S}, t \in \mathcal{T}} \in K^{\mathcal{S} \times \mathcal{T}}$. Then $0 = \mu^{\otimes}(\sum_{s,t} c_{s,t} \varphi_s \otimes \nu_t) = \sum_{s,t} c_{s,t} \varphi_s \nu_t$ in $K[V \times W]_K$, as a function on $V \times W$, which means $\sum_{s,t} c_{s,t} \varphi_s(P) \nu_t(Q) = 0$ for every $P \in V$ and every$Q \in W$. Since this relation can be rewritten as: for every $Q \in W$ it is $\sum_s (\sum_t c_{s,t} \nu_t(Q)) \varphi_s(P) = 0$ for every $P \in V$. Note now that, thanks to the hypothesis $L = K$, the inner sum $\sum_t c_{s,t} \nu_t(Q) \in K$ also, because all the ν_t are K-valued functions by assumption (which is not always the case, as we already remarked, if $K \subsetneq L$, cf. footnote to 2.5.1). Therefore, since the φ_s are K-linearly independent in $K[V]$ it must be $\sum_t c_{s,t} \nu_t(Q) = 0$ for every $Q \in W$, for every $s \in \mathcal{S}$. But $(c_{s,t})_{s \in \mathcal{S}, t \in \mathcal{T}} \in K^{\mathcal{S} \times \mathcal{T}}$ and the ν_t are K-linearly independent in $K[W]$ by assumption, hence for every $s \in \mathcal{S}$ and for every $t \in \mathcal{T}$ it is $c_{s,t} = 0$. That is $\sum_{s,t} c_{s,t} \varphi_s \otimes \nu_t = 0$ in $K[V]_K \otimes_K K[W]_K$ as claimed. □

2.6. Regular maps between K-algebraic sets.

2.6.1. Definition. — Let V be a K-algebraic subset of $\mathbb{A}^n_L$, W a K-algebraic subset of $\mathbb{A}^n_L$ and let $\Phi\colon V \longrightarrow W$ be a map from V to W. Then Φ is said to be a **K-regular map** on V, or a K-morphism, if there exists $F = (f_1, \cdots, f_m) \in K[\underline{X}]^m$ such that $(f_1(P), \cdots, f_m(P)) \in W$ for each $P \in V$ and $\Phi(P) = (f_1(P), \cdots, f_m(P))$ for each $P \in V$.

2.6.2. Remark. — Regular functions on V are the same thing as regular maps from V to $\mathbb{A}^1_L$:

$$K[V]_L = \{K\text{-regular maps } V \longrightarrow \mathbb{A}^1_L\}.$$

2.6.3. Proposition (ring homomorphism induced by a regular map). — *If $\Phi\colon V \longrightarrow W$ is a K-regular map between the K-algebraic sets V and W then Φ induces, controvariantly, a K-algebra homomorphism between the coordinate rings of W and V $\Phi^*\colon K[W]_L \to K[V]_L$, defined by "pulling back" along Φ, i.e. $\psi \mapsto \Phi^*(\psi) := \psi \circ \Phi$, such that*

a) $(\mathrm{Id}_V)^* = \mathrm{Id}_{K[V]}$*;*
b) if $\Upsilon\colon W \to X$ is a second K-regular map, $(\Upsilon \circ \Phi)^* = \Phi^* \circ \Upsilon^*$;
c) $\mathrm{Ker}(\Phi^*) = \{\psi \in K[W]_L \mid \psi_{|\overline{\Phi(V)}^Z} \equiv 0\}$.

Proof. — All verifications for *a)* and *b)* are straightforward.
For *c)*, let $\psi = g_{|W} \in K[W]_L$, with $g \in K[Y_1, \ldots, Y_m]$, such that $0 = \Phi^*(\psi) = \psi \circ \Phi$. This means $\Phi(V) \subseteq W \cap \mathcal{Z}(g)$. But $W \cap \mathcal{Z}(g)$ is a closed subset of W, hence $\overline{\Phi(V)}^Z \subseteq W \cap \mathcal{Z}(g)$. This means that $g_{|\overline{\Phi(V)}^Z} \equiv 0$ identically, hence $\psi_{|\overline{\Phi(V)}^Z} \equiv 0$. This shows the $\subseteq$ inclusion. The converse is trivial: if ψ $K[W]_L$ is such that $\psi_{|\overline{\Phi(V)}^Z} \equiv 0$, then necessarily $\Phi^*(\psi) = \psi \circ \Phi \equiv 0$ on V, hence $\psi \in \mathrm{Ker}(\Phi^*)$. □

2.6.4. Definition. — Let V be a K-algebraic subset of $\mathbb{A}^n_L$, W a K-algebraic subset of $\mathbb{A}^n_L$. We say that V and W are **K-isomorphic**, or **K-polynomially isomorphic** if there exists a pair of opposite K-regular maps $\Phi\colon V \longrightarrow W$ and $\Upsilon\colon W \longrightarrow V$ which are inverse, *i.e.* such that $\Upsilon \circ \Phi = \mathrm{Id}_V$ and $\Phi \circ \Upsilon = \mathrm{Id}_W$. In this case, the K-regular map Φ, as well as Υ, is said to be a **K-regular isomorphism**, or a **K-polynomial isomorphism**.

2.6.5. Remark. — See *2.11.5* for an algebraic characterization of K-polynomial isomorphisms of algebraic sets.

2.6.6. Proposition (regular maps are continuous). — *If $\Phi\colon V \longrightarrow W$ is a K-regular map between the K-algebraic subsets V and W, then Φ is a continuous function with respect to the subspace topology on V induced by the Zariski topology on $\mathbb{A}^n_L$ (relative to K) and the subspace topology on W induced by the Zariski topology on $\mathbb{A}^m_L$ (relative to K).*

Proof. — If $W = \mathcal{Z}(R)$ with $R \subseteq K[Y_1, \ldots, Y_m]$ is a Zariski closed subset of $\mathbb{A}^m_L$ then

$$\Phi^{-1}(W) = \Phi^{-1}(\bigcap_{g\in R} \mathcal{Z}(g)) = \bigcap_{g\in R} (\Phi^{-1}(g^{-1}(0))) = \bigcap_{g\in R} (g\circ\Phi)^{-1}(0) = \bigcap_{g\in R} \mathcal{Z}(g\circ\Phi)$$

as $g \circ \Phi = g(f_1(X_1, \ldots, X_n), \ldots, f_m(X_1, \ldots, X_n)) \in K[X_1, \ldots, X_n]$ for each $g(Y_1, \ldots, Y_m) \in K[Y_1, \ldots, Y_m]$, $\Phi^{-1}(W)$ is a Zariski closed subset of $\mathbb{A}^n_L$. That is $\Phi^{-1}(\mathcal{Z}(R)) = \mathcal{Z}(\Phi^*(R))$ where $\Phi^*\colon K[Y_1, \ldots, Y_m] \longrightarrow K[X_1, \ldots, X_n], g \mapsto g \circ \Phi$ is the map induced by Φ. □

2.6.7. Critical example: regular maps need not to be closed maps. — Let L be an infinite field and let's consider $V := \mathcal{Z}(XY - 1) \subseteq \mathbb{A}^2_L$ (a hyperbola), $W := \mathbb{A}^1_L$, and $\Phi\colon V \longrightarrow W$, $(a, a^{-1}) \mapsto a$. Then $\Phi(V) = \mathbb{A}^1_L \setminus \{0\}$ which is not a K-algebraic subset of W, indeed, being L an infinite field, it can be shown that $\overline{\Phi(V)}^Z = \mathbb{A}^1_L$. Hence, in the Zariski topology, a regular (hence continuous) image of a closed subset need not be closed. Note that in the example given, moreover, Φ is an injective map on V. For a second example: let $\Phi\colon \mathbb{A}^1_{\mathbb{R}} \longrightarrow \mathbb{A}^1_{\mathbb{R}}$, $a \mapsto a^2$, then $\Phi(\mathbb{A}^1_{\mathbb{R}}) = \{a \in \mathbb{R} \mid a \geq 0\}$ is not a $\mathbb{R}$-algebraic subset of the affine line $\mathbb{A}^1_{\mathbb{R}}$. Indeed, as we already know that closed subsets of $\mathbb{A}^1_{\mathbb{R}}$ are either finite or total, it is $\overline{\Phi(\mathbb{A}^1_{\mathbb{R}})}^Z = \mathbb{A}^1_L$.

2.6.8. Definition. — Let V be a K-algebraic subset of $\mathbb{A}^n_L$, W a K-algebraic subset of $\mathbb{A}^n_L$ and let $\Phi\colon V \longrightarrow W$. be a K-regular map from V to W. Then Φ is said to be a **dominant** if $\Phi(V)$ is dense in W, that is $\overline{\Phi(V)}^Z = W$.

2.6.9. Proposition (ring injection induced by a dominant regular map). — *Let $\Phi\colon V \longrightarrow W$ be a K-regular map as above. Then its induced K-algebra homomorphism*

$$\Phi^*\colon K[W]_L \to K[V]_L,\ \psi \mapsto \Phi^*(\psi) := \psi \circ \Phi$$

is injective if and only if Φ is dominant.

Proof. — It follows from 2.6.3, *c*). □

2.6.10. Definition-proposition. — *Let V be a K-algebraic subset of $\mathbb{A}^n_L$, W a K-algebraic subset of $\mathbb{A}^n_L$ and let $\Phi\colon V \longrightarrow W$. be a K-regular map from V to W. Then its* **graph** *is defined as $\Gamma_\Phi := \{(P, \Phi(P)) \mid P \in V\} \subseteq V \times W$. The graph of a regular map is a K-algebraic subset of ($V \times W$ and) $\mathbb{A}^{n+m}_L$ and $\mathrm{Im}(\Phi) = pr_W(\Gamma_\Phi)$.*

Proof. — If $V = \mathcal{Z}(h_1, \ldots, h_r)$ with $h_1, \ldots, h_r \in K[X_1, \ldots, X_n]$, and Φ is induced by $F = (f_1, \cdots, f_m) \in K[\underline{X}]^m$ then

$$\Gamma_\Phi = \mathcal{Z}(h_1(X_1, \ldots, X_n), \ldots, h_r(X_1, \ldots, X_n), y_1 - f_1(X_1, \ldots, X_n), \ldots, y_m - f_m(X_1, \ldots, X_n)).$$

Hence Γ_Φ is a K-algebraic subset of $\mathbb{A}^{n+m}_L$. The last assertion is straightforward. □

2.6.11. Proposition. — *Let $\Phi\colon V \longrightarrow W$. as above. Then the inverse maps*

$$(\mathrm{Id}_V, \Phi)\colon V \longrightarrow \Gamma_\Phi,\ P \mapsto (P, \Phi(P)), \quad pr_V\colon \Gamma_\Phi \longrightarrow V,\ (P, \Phi(P)) \mapsto P$$

are K-regular and induce reciprocal isomorphisms of K-algebras on the coordinate rings

$$K[V]_L \underset{pr_V^*}{\overset{(\mathrm{Id}_V,\Phi)^*}{\rightleftarrows}} K[\Gamma_\Phi]_L.$$

In particular Γ_Φ is always K-isomorphic to V.

Proof. — The first map is K-regular because it is induced by $(X_1, \ldots, X_n, f_1, \ldots, f_m) \in K[X_1, \ldots, X_n]^{n+m}$. The second map is the restriction to Γ_Φ of the first projection $V \times W \longrightarrow V$, hence it is induced by $(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]^n$ and therefore it is K-regular. As $\mathrm{pr}_V \circ (\mathrm{Id}_V, \Phi) = \mathrm{Id}_V$ and $(\mathrm{Id}_V, \Phi) \circ \mathrm{pr}_V = \mathrm{Id}_{\Gamma_\Phi}$, by *2.6.3 a)* and *b)*, it follows that $(\mathrm{Id}_V, \Phi)^*$ and pr_V^* are inverse isomorphims on K-algebras. □

2.6.12. Proposition. — *Let V be a K-algebraic subset of $\mathbb{A}^n_L$, W a K-algebraic subset of $\mathbb{A}^n_L$ and let $P = (\underline{a}) \in V$ a K-algebraic subset of V (and thus of $\mathbb{A}^n_L$). That is P is a K-rational point of V. Then, the subset $P \times W := \{P\} \times W$ is a K-algebraic subset (as in 2.2.4) and it is K-isomorphic to W.*

Proof. — The maps $\Upsilon\colon W \longrightarrow P \times W,\ Q \mapsto (P, Q)$ and $\Phi\colon P \times W \longrightarrow W,\ (P, Q) \mapsto Q$ are obviously, set theoretically, inverse maps, which are also K-regular. Indeed

$$\Upsilon = (a_1, \ldots, a_n, Y_1, \ldots, Y_m)_{|W} \text{ and } \Phi = (Y_1, \ldots, Y_m)_{|W}.$$

Hence they give the required K-regular isomorphism. □

2.6.13. Remark. — The previous result does not hold true if P is not K-rational. Consider, indeed, the following: $K = \mathbb{Q}$, $L = \mathbb{R}$, and $V = W = \mathcal{Z}(X^2 - 2) = \{-\sqrt{2}, \sqrt{2}\}$.
Then $\{\sqrt{2}\} \times W = \{(\sqrt{2}, -\sqrt{2}), (\sqrt{2}, \sqrt{2})\}$ is not even a $\mathbb{Q}$-algebraic subset of $\mathbb{A}^{\mathbb{R}}_2$ because

$$\overline{\{\sqrt{2}\} \times W}^{Z} = V \times W.$$

The crucial point to prove this is that, if $f \in \mathbb{Q}[X_1, Y_1]$ is such that $f(\sqrt{2}, -\sqrt{2}) = (\sqrt{2}, \sqrt{2}) = 0$ then it is also $f(-\sqrt{2}, -\sqrt{2}) = (-\sqrt{2}, \sqrt{2}) = 0$; that is $V \times W \subseteq \mathcal{Z}(f)$ necessarily. The claim will be immediately clear using 2.12.3 and *2.21.1 p*) (or by direct proof). Moreover, it is clear that there is no $\mathbb{Q}$-regular map from W to $\{\sqrt{2}\} \times W$, essentially just because $\sqrt{2} \notin \mathbb{Q}$.

2.7. Irreducible topological spaces, irreducible components

In this section X will usually denote a topological space.

2.7.1. Proposition-Definition. — *A (nonempty) topological space X is said to be* **irreducible** *if the following equivalent condition hold true:*

a) if $X = C_1 \cup C_2$ with C_1, C_2 closed subsets of X, then $X = C_1$ or $X = C_2$;
b) if U_1, U_2 are non empty open subsets of X, then $U_1 \cap U_2 \neq \emptyset$;
c) any nonempty open subset of X is dense.

Proof. — See [**Kun85**, Ch. I, Def. 2.8, Lemma 2.9] and [**Har77**, Pag. 3]. Note that in the former reference the empty set is considered irreducible, but not in the latter, as I prefer do not repeat "nonempty" each time, and also in light of 2.11.2, I follow [**Har77**]. □

2.7.2. Definition. — A subspace S of a topological space X is said to be an **irreducible subspace** of X if S endowed with the subspace topology from X is such.

2.7.3. Remark. — A Hausdorff space is irreducible if and only if it is reduced to a point.

2.7.4. Remark: comparison between irreducibility and connectedness. — Clearly, every irreducible space is connected, while the converse does not hold in general: the union of the axes, $\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(XY) = \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X) \cup \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(Y)$, is connected but is clearly not irreducible.

2.7.5. Proposition. — *Irreducible spaces are stable under continuous images and (finite) cartesian products. That is:*

a) If $f\colon X \longrightarrow Y$ is a continuous map between topological spaces, and Z is an irreducible subspace of X then $f(Z)$ is an irreducible subspace of Y.

b) If X and Y are two irreducible topological spaces, then $X \times Y$ is irreducible wrt the product topology.

Proof. — *a)* Let C_1, C_2 two closed subsets of Y such that $f(Z) \subseteq C_1 \cup C_2$, then $Z \subseteq f^{-1}(f(Z)) \subseteq f^{-1}(C_1) \cup f^{-1}(C_2)$, with $f^{-1}(C_i)$, $i = 1, 2$, closed subsets of X by continuity of f. Since Z is irredducible, it must be $Z \subseteq f^{-1}(C_i)$ for some i. Then $f(Z) \subseteq f(f^{-1}(C_i)) \subseteq C_i$. Hence $f(Z)$ is irreducible.

b) Let C_1, C_2 two closed subsets of $X \times Y$ such that $X \times Y = C_1 \cup C_2$. As, for each $x \in X$ the subspace (with the subspace topology coming from $X \times Y$, which in turn coincides with its own product topology) $x \times Y := \{x\} \times Y$ is clearly homeomorphic to Y (via $y \mapsto (x, y)$, and $(x, y) \mapsto y$) and therefore irreducible $x \times Y$ because Y is such, we have

$$x \times Y = (x \times Y) \cap (X \times Y) = ((x \times Y) \cap C_1) \cup ((x \times Y) \cap C_2),$$

then $x \times X \subset C_1$, or $x \times X \subset C_2$. Let, for $i = 1, 2$, $X_i := \{x \in X \mid x \times Y \subset C_i\} \cong ((X \times y) \cap C_i)$, then clearly $X = X_1 \cup X_2$. We claim that the X_i, for $i = 1, 2$, are closed subsets of X. Indeed, clearly it is $X_i = \cap_{y \in Y} \iota_y^{-1}(C_i)$, where, for each $y \in Y$, $\iota_y\colon X \longrightarrow X \times Y$ is the map $x \mapsto (x, y)$, which is continuous because on sub basic open subsets $U \times Y$ (U open of X) and $X \times V$ (V open of Y)

$$\iota_y^{-1}(U \times Y) = U, \text{ and } \iota_y^{-1}(X \times V) = \begin{cases} X \text{ if } y \in V, \\ \emptyset \text{ if } y \notin V \end{cases}.$$

Hence the X_i is an intersection of closed subsets of X and thus it is closed itself. But now X is irreducible, hence $X = X_1$, in which case $X \times Y = C_1$, or $X = X_2$, in which case $X \times Y = C_2$. We conclude that $X \times Y$ is irreducible too. □

2.7.6. Remark. — Since being irreducible is a property stable under homeomorphisms, it is a topological property.

2.7.7. Remark. — If S is an irreducible subspace of a topological space X, then any $S' \subseteq X$, such that $S \subseteq S' \subseteq \overline{S}^X$ is irreducible too (see [**Kun85**, Ch. I, Cor. 2.10]). Obviously, every $\{x\}$ with $x \in X$, as well as its closure $\overline{\{x\}}^X$, is an irreducible subspace of X.

2.7.8. Definition. — By definition ([**Kun85**, Ch. I, Def. 2.11]), an **irreducible component** of a topological space X is any maximal irreducible subspace of X.

2.7.9. Proposition. — *Let X be any topological space. Then:*

a) any irreducible component of X is closed in X;
b) any irreducible subset of a topological space is contained in an irreducible component;
c) any (nonempty) topological space X is the union of its irreducible components;
d) any Noetherian topological space has only finitely many irreducible components; no such component is contained in the union of the others (the union is not redundant).

Proof. — See [**Kun85**, Ch. I, Props. 2.12, 2.14]. □

2.8. Irreducibility and algebraic sets

We now give the algebraic characterization of irreducibility for K-algebraic sets in terms of their K-algebras of regular functions.

2.8.1. Proposition (Irreducible K-algebraic subsets). — *Let V be a K-algebraic subset of $\mathbb{A}^n_L$, then: V is irreducible if and only if $K[V]_L$ is an integral domain.*

Proof. — Assume V is irreducible, and let $\varphi_1, \varphi_2 \in K[V]_L$ such that $\varphi_1\varphi_2 = 0$. This means $\varphi_1(P)\varphi_2(P) = 0$ for each $P \in V$, in L. Since L is a field, we then have the closed decomposition (*2.5.4* and *2.5.5*): $V = \mathcal{Z}(\varphi_1) \cup \mathcal{Z}(\varphi_2)$. Since V is irreducible, it must be $V = \mathcal{Z}(\varphi_1)$ or $V = \mathcal{Z}(\varphi_2)$. In the former case $\varphi_1 = 0$ and in the latter $\varphi_2 = 0$. Therefore $K[V]$ has no non zero zero divisors, that is it is a domain. Assume now that $K[V]$ is a domain, and let, by contradiction, $V = Z_1 \cup Z_2$ for some proper Zariski closed subsets Z_i of V. Let then $\mathfrak{J}_i := \{\varphi \in K[V] \mid \varphi_{|Z_i} = 0\}$, for $i = 1, 2$. Clearly $\mathfrak{J}_1$, $\mathfrak{J}_2$ are ideals of $K[V]$ and neither $\mathfrak{J}_1$ nor $\mathfrak{J}_2$ is the zero ideal (as both Z_i are proper). But $\mathfrak{J}_1 \cap \mathfrak{J}_2 = (0)$ as $V = Z_1 \cup Z_2$. Then $\mathfrak{J}_1\mathfrak{J}_2 \subseteq \mathfrak{J}_1 \cap \mathfrak{J}_2 = (0)$, and therefore $K[V]$ has non trivial zero divisors. Contradiction. □

2.8.2. Remark. — As we already noticed that $\mathbb{A}^n_L$, with the Zarisky topology on (relative to K), is a Noetherian topological space (as well as any K-algebraic set in it), we can conclude that

any K-algebraic set V of $\mathbb{A}^n_L$ is a finite union of uniquely determined irreducible K-algebraic sets $V_1, \dots, V_s \subseteq V$:

$$V = V_1 \cup \cdots \cup V_s \tag{1}$$

2.8.3. Primary decomposition and $\mathcal{Z}$. — As any ideal I of $K[\underline{X}]$ has a minimal primary decomposition (see *1.11*) we find

$$I = Q_1 \cap \cdots \cap Q_r \;\Rightarrow\; V = \mathcal{Z}(I) = \mathcal{Z}(Q_1) \cup \cdots \cup \mathcal{Z}(Q_r) = \mathcal{Z}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{p}_r) \tag{2}$$

where Q_i are $\mathfrak{p}_i$-primary ideals. Hence, every algebraic set of $\mathbb{A}^N_L$ is, set-theoretically, a finite union of zero loci of prime ideals of $K[\underline{X}]$ (some of them my well be empty or not irreducible if L is not algebraically closed, compare *2.13*). We will compare and relate these two closed decompositions (1) and (2) in what follows (cf. 2.15).

2.8.4. Remark: non hausdorffness and product topology. — As already mentioned (*2.4.6*), the Zariski topology is almost never a Hausdorff one unless L is a finite field, for then it's the discrete topology. From a different perspective, we saw (2.8.2) that every K-algebraic set is a finite union of irreducible ones, and if L is not finite then $\mathbb{A}^n_L$ itself is irreducible, hence any two non empty open sets of $\mathbb{A}^n_L$ must intersect, which is the least "Hausdorff behavior" a topological space can have. On the other hand, we saw (2.2.3) that the diagonal subspace Δ_n of $\mathbb{A}^n_L \times \mathbb{A}^n_L$ is a K-algebraic subset of $\mathbb{A}^{2n}_L$, hence it is closed. From this we draw that the Zariski topology on a cartesian product is not the product of the Zariski topologies of the factors. The key point is that, actually, *the Zariski topology on $\mathbb{A}^{2n}_L$ is strictly finer than the topological product of the Zariski topology on $\mathbb{A}^n_L \times \mathbb{A}^n_L$*. Indeed, every product of two closed Zariski subsets of $\mathbb{A}^n_L$ is Zariski closed in $\mathbb{A}^{2n}_L$, as if $V = \mathcal{Z}(f_1(\underline{X}), \dots, f_r(\underline{X}))$ and $U = \mathcal{Z}(g_1(\underline{X}), \dots, g_s(\underline{X}))$ in $\mathbb{A}^n_L$, then

$$V \times U = (V \times \mathbb{A}^n_L) \cap (\mathbb{A}^n_L \times U) = \mathcal{Z}((f_1(\underline{X}), \dots, f_r(\underline{X}))K[\underline{X}, \underline{Y}] + (g_1(\underline{Y}), \dots, g_s(\underline{Y}))K[\underline{X}, \underline{Y}]) \subseteq \mathbb{A}^{2n}_L,$$

but the diagonal $\Delta_n = \mathcal{Z}(\mathfrak{d}_n)$ is a Zariski closed subset of $\mathbb{A}^n_L$ which is not closed in the product topology because $\mathbb{A}^n_L$ is not a Hausdorff space as soon as L is infinite.

2.8.5. Proposition. — *Let $K \subseteq L$ be any field extension, and let V be a K-rational subset of $\mathbb{A}^n_K$ and W be a K-rational subset of $\mathbb{A}^m_K$. The followings hold true:*

a) If $V \times W$ is irreducible, then V and W are irreducible.

b) If $L = K$ the converse holds: if V and W are irreducible, then $V \times W$ is such (wrt the subspace topology induced by the Zariski topology on $\mathbb{A}^n_L$).

Proof. — *a)* It follows from 2.7.5 *a)* and 2.6.6 since the projections from $V \times W$ to its factors are K-regular maps.
b) As we assumed $L = K$, the very same argument used to prove 2.7.5 *b)* works in this case. Indeed, every point of V or W is K-rational (closed in the Zariski topology), therefore all the "slices" $P \times W$ and $V \times Q$ are K-algebraic subsets (cf. 2.6.12) and all the needed maps required in the proof of 2.7.5 *b)* are actually K-regular, hence the proof can be repeated and works word by word in the context of K-algebraic subsets. □

2.8.6. Critical Example. — The previous result 2.8.5 *b)* does not hold true in general if $K \subsetneq L$. Consider, as in 2.6.13, the following situation: $K = \mathbb{Q}$, $L = \mathbb{R}$, and $V = W = \mathcal{Z}(X^2 - 2) = \{-\sqrt{2}, \sqrt{2}\}$. Then V is irreducible, since $\mathbb{Q}[V]_{\mathbb{R}} \cong \mathbb{Q}[X]/(X^2 - 2) = \mathbb{Q}(\sqrt{2})$ is a domain (actually, even a field), but the product space

$$V \times V = \{(-\sqrt{2}, -\sqrt{2}), (-\sqrt{2}, \sqrt{2}), (\sqrt{2}, -\sqrt{2}), (\sqrt{2}, \sqrt{2})\} = \mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(X_1^2 - 2, X_2^2 - 2).$$

We easily verify then that

$$V \times V = \mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(X_1^2 - X_2^2, X_2^2 - 2) = \mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(X_1 + X_2, X_2^2 - 2) \cup \mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(X_1 - X_2, X_2^2 - 2)$$

is not irreducible in the Zariski topology (relative to $\mathbb{Q}$), on the contrary it is even not connected:

$$V \times V = \{(-\sqrt{2}, \sqrt{2}), (\sqrt{2}, -\sqrt{2})\} \cup \{(-\sqrt{2}, -\sqrt{2}), (\sqrt{2}, \sqrt{2})\}.$$

Its K-algebra of regular functions is $\mathbb{Q}[V \times V]_{\mathbb{R}} \cong \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt{2})$. Of course, in the Zariski topology relative to $\mathbb{R}$, it is $V = \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X + \sqrt{2}) \cup \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X - \sqrt{2})$, hence $V_{\mathbb{R}}$ is no longer irreducible in this (finer) topology everything works as expected from 2.8.5.

2.9. Vanishing ideals in $K[X_1, \ldots, X_n]$

We can also proceed the other way round, that is from subsets of the affine space $\mathbb{A}^n_L = L^n$ to subsets of the polynomial rings $K[\underline{X}]$.

2.9.1. Definition. — Given a subset S of $\mathbb{A}^n_L$, the set of all polynomials vanishing on it

$$\mathcal{I}^L_K(S) := \{f \in K[\underline{X}] \mid f(P) = 0 \ \ \forall P \in S\} = \bigcap_{P\in S} \mathcal{I}^L_K(P) \subseteq K[X_1, \ldots, X_n] = K[\underline{X}]$$

is (obviously) a *radical ideal* of $K[\underline{X}]$ (if $f^n \in \mathcal{I}^L_K(S)$, for some n, then $f \in \mathcal{I}^L_K(S)$) and it is called the **(vanishing K-)ideal** of S. Note that, given a polynomial $f \in K[\underline{X}]$, saying $f \in \mathcal{I}(S)$ is equivalent to say that f, thought of as a function on $\mathbb{A}^n_L$, induces the zero function on S, *i.e.* $f \in \mathcal{I}(S) \ \Leftrightarrow \ f_{|S} \equiv 0$.

2.9.2. Remark. — Note that, for example, if $n = 1$, $K = \mathbb{Q}$, $L = \mathbb{C}$ and $S = \{\pi\}$, then $\mathcal{I}^{\mathbb{C}}_{\mathbb{Q}}(\pi) = \{p(X) \in \mathbb{Q}[X] \mid p(\pi) = 0\} = (0)$ just because $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$.

2.9.3. behavior of $\mathcal{I}^L_K$ under field extensions. — If $H \subseteq K$ are both subfields of L, then $\mathbb{A}^n_K \subseteq \mathbb{A}^n_H \subseteq \mathbb{A}^n_L \subseteq$ and $H[\underline{X}] \subseteq K[\underline{X}]$. We have the following relations:

a) if $S \subseteq \mathbb{A}^n_L$, then $\mathcal{I}^L_K(S) = \mathcal{I}^L_H(S) \cap K[\underline{X}]$ and $\mathcal{I}^L_K(S) \subseteq \mathcal{I}^H_K(S \cap \mathbb{A}^n_H)$;

b) from a different perspective, if V is a K-algebraic set in $\mathbb{A}^n_K$, let $\overline{V} \subseteq \mathbb{A}^n_L$ be its closure in the Zaraski topology of $\mathbb{A}^n_L$ relative to L. Then the vanishing ideal of $\overline{V}$ in $L[\underline{X}]$ is the *extension ideal* of its vanishing ideal in $K[\underline{X}]$, that is $\mathcal{I}^L_L(\overline{V}) = \mathcal{I}^K_K(V)L[\underline{X}]$ ([**Kun85**, Ch. 1, Sec. 2, Ex. 7], [**AM69**, Ch. 1])

2.9.4. Example. — Let $K = \mathbb{Q}$, $H = \mathbb{R}$, $L = \mathbb{R}(i) = \mathbb{C}$ and $f = X^2 + 1 \in \mathbb{Q}[X]$. Then $\mathcal{I}^{\mathbb{C}}_{\mathbb{Q}}(\mathcal{Z}^{\mathbb{C}}_{\mathbb{Q}}(f)) = (X^2 + 1) \subsetneq \mathbb{Q}[X] = \mathcal{I}^{\mathbb{R}}_{\mathbb{Q}}(\mathcal{Z}^{\mathbb{R}}_{\mathbb{Q}}(f))$.

To simplify the notation, in what follows we write $\mathcal{I} = \mathcal{I}^L_K$ unless the specification is needed.

2.9.5. Remark: "stability property" of $\mathcal{I}$. — As, tautologically, $S \subseteq \mathcal{Z}(\mathcal{I}(S))$ for every subset S of $\mathbb{A}^n_L$, then $1 \notin \mathcal{I}(S)$ whenever $S \neq \emptyset$. That is $\mathcal{I}(S)$ is always a proper ideal of $K[\underline{X}]$ for nonempty subsets S.

2.9.6. Lattice properties of $\mathcal{I}$. — For any family of subsets $S_i \subseteq \mathbb{A}^n_L$ we have: $\bigcap_i \mathcal{I}(S_i) = \mathcal{I}\left(\bigcup_i S_i\right)$, while $\mathcal{I}(S_1) + \mathcal{I}(S_2) \subseteq \sqrt{\mathcal{I}(S_1) + \mathcal{I}(S_2)} \subseteq \mathcal{I}(S_1 \cap S_2)$. Note that the sum of two (even radical) ideals is, in general, not necessarily radical. The last inclusion above can well be strict if L is not algebraically closed.

2.9.7. Example. — Let L be an infinite field, and let $S_1 = \mathcal{Z}(Y - X^2)$ (a parabola) and $S_2 = \mathcal{Z}(Y)$ (the X axis). It can be shown that $\mathcal{I}(S_1) = (Y - X^2)$ and $\mathcal{I}(S_2) = (Y)$. Then $J := \mathcal{I}(S_1) + \mathcal{I}(S_2) = (Y - X^2, Y) = (X^2, Y)$ is not a radical ideal, for $X^2 \in J$ but $x \notin J$. Indeed $S_1 \cap S_2 = \{(0,0)\}$, and $\mathcal{I}(S_1 \cap S_2) = (X, Y)$. Hence, $\mathcal{I}(S_1 \cap S_2) = \sqrt{\mathcal{I}(S_1) + \mathcal{I}(S_2)}$ in this case.

2.9.8. $\mathcal{I}$ is inclusion-reversing. — As it happens for $\mathcal{Z}$, also $\mathcal{I}$ is a (weakly) decreasing mapping between subsets of the affine space $\mathbb{A}^n_L$ and subsets of the polynomial ring $K[\underline{X}]$, that is $S_1 \subseteq S_2 \subseteq \mathbb{A}^n_L \;\Rightarrow\; K[\underline{X}] \supseteq \mathcal{I}(S_1) \supseteq \mathcal{I}(S_2)$.

2.10. Basic constructions with $\mathcal{I}$. Nullstellensatz (field theoretic version)

2.10.1. Example. — It's not difficult to see that: $\mathcal{I}(\emptyset) = K[\underline{X}] = (1)$ and, if L has infinitely many elements [4], $\mathcal{I}(\mathbb{A}^n_L) = (0)$ (cf. [**Kun85**, Ch. I, Sec. 1, Prop. 1.3 a)]).

2.10.2. Example: vanishing ideal of K-rational points. — Let $P = (a_1, \ldots, a_n) \in \mathbb{A}^n_L$ be a K-rational point as in 2.2.2, then obviously $1 \notin \mathcal{I}(\{P\})$, because $P \in \mathcal{Z}(\mathcal{I}(\{P\}))$, and on the other hand $X_i - a_i \in \mathcal{I}(\{P\})$ for every $i = 1, \cdots, n$. Hence the whole maximal ideal $\mathfrak{m}_P := (X_1 - a_1, \cdots, X_n - a_n) \subseteq \mathcal{I}(\{P\})$, as $1 \notin \mathcal{I}(\{P\})$ and $\mathfrak{m}_P$ maximal, it must then be $\mathcal{I}(\{P\}) = (X_1 - a_1, \cdots, X_n - a_n) = \mathfrak{m}_P$.

2.10.3. Proposition (field theoretic version of Nullstellensatz). — *If K is a field and $\mathfrak{m}$ a maximal ideal of the polynomial ring $P := K[X_1, \ldots, X_n]$, then $\mathfrak{m} \cap K[X_i] \neq (0)$ for each $i = 1, \ldots, n$. Moreover, the K-algebra $P/\mathfrak{m}$ is a finite dimensional K-vector space and hence $P/\mathfrak{m}$ is an algebraic field extension of K.*

Proof. — A proof, relying on Gröbner bases theory, can be found in [**KR00**, Thm. 2.6.6]. □

4. If $L = \mathbb{F}_q$ is a finite field with $q = p^n$ elements, for some $n \in \mathbb{N}_+$ and p a prime integer, it's not difficult to show that $\mathcal{I}(\mathbb{A}^n_L) = (X_1^q - X_1, \cdots, X_n^q - X_n)$. Over a finite fields, "polynomials" and "polynomial functions" are not the "same thing".

2.10.4. Remark: vanishing ideal of arbitrary points. — If $P = (a_1, \dots, a_n) \in \mathbb{A}^n_L$ is an arbitrary point (not necessarily K-rational), then $\mathcal{I}(P)$ is always a prime ideal of $K[\underline{X}]$ because evaluation homomorphism $\mathrm{ev}_P \colon K[\underline{X}]_L \longrightarrow L, f \mapsto f(P)$ has $\mathrm{Ker}(\mathrm{ev}_P) = \mathcal{I}^L_K(P)$, and it induces an injection of rings $K[\underline{X}]/\mathrm{Ker}(\mathrm{ev}_P) = K[\underline{X}]/\mathcal{I}(P) \hookrightarrow L$; as L is a field, then $K[\underline{X}]/\mathcal{I}(P)$ must be a domain. We therefore have a map $\mathbb{A}^n_L \longrightarrow \{\text{prime ideals of } K[X_1, \dots, X_n]\}$ defined by $P \mapsto \mathcal{I}(P) = \mathrm{Ker}(\mathrm{ev}_P)$, which is in general neither injective nor surjective. None the less, by restriction it induces a bijection $\mathbb{A}^n_K \longrightarrow \{\text{"linear" maximal ideals of } K[X_1, \dots, X_n]\}$, where $(a_1, \dots, a_n) \mapsto (X_1 - a_1, \cdots, X_n - a_n)$. Note that $\mathcal{I}^{\mathbb{C}}_{\mathbb{Q}}((\pi, \pi)) = (X - Y)$, $\mathcal{I}^{\mathbb{C}}_{\mathbb{Q}}((\pi, e)) = (0)$ (!?) [5] and $\mathcal{I}^{\mathbb{C}}_{\mathbb{Q}}((i, \pi)) = (X^2 + 1)$ are prime, not maximal, ideals of $\mathbb{Q}[X, Y]$, while $\mathcal{I}^{\mathbb{C}}_{\mathbb{Q}}((i, \sqrt[3]{-2})) = (X^2 + 1, Y^3 + 2)$ is a maximal ideal ($\mathbb{Q}[x, y]/(X^2 + 1, Y^3 + 2) \cong \mathbb{Q}(i, \sqrt[3]{2})$ subfield of $\mathbb{C}$). As a consequence of the field theoretic version of the Hilbert Nullstellensatz (2.10.3), also known as Zariski's Lemma, the vanishing ideal $\mathcal{I}(P)$ is a maximal ideal of $K[\underline{X}]$ if and only if every coordinate of P is algebraic over K.

Proof. — Indeed, if $P = (a_1, \dots, a_n) \in \mathbb{A}^n_L$ and, say, a_1 is transcendental over K, then $\mathcal{I}(P) \cap K[X_1] \neq (0)$ and therefore $\mathcal{I}(P)$ can't be maximal. This shows that if $\mathcal{I}(P)$ is a maximal of $K[X_1, \dots, X_n]$, then each coordinate of P is algebraic over K.
Conversely, if each $a_i \in L$ is algebraic over K, then $\mathcal{I}(P) \cap K[X_i] = (m_{a_i}(X_i))$ is a non zero, proper, ideal of the Euclidean ring $K[X_i]$ generated by the minimal polynomial of a_i over K. Hence $\mathcal{I}(P) \supseteq (m_{a_1}(X_1), \dots, m_{a_n}(X_n))$ and the quotient ring

$$K[\underline{X}]/\mathcal{I}(P) \cong \frac{K[\underline{X}]/(m_{a_1}(X_1), \dots, m_{a_n}(X_n))}{\mathcal{I}(P)/(m_{a_1}(X_1), \dots, m_{a_n}(X_n))},$$

viewed as a K-vector space, has dimension bounded by the product of the degrees of these minimal polynomials, since $K[\underline{X}]/(m_{a_1}(X_1), \dots, m_{a_n}(X_n)) \cong \bigotimes_{i=1}^n K[X_i]/(m_{a_i}(X_i))$. As $K[\underline{X}]/\mathcal{I}(P)$ is always a domain, as already seen above, it must be a field [6], therefore $\mathcal{I}(P)$ is maximal. □

What just proved can be rephrased as: $\mathcal{I}(P)$ is a maximal ideal of $K[\underline{X}]$ for every $P \in \mathbb{A}^n_L$ if and only if L is an algebraic extension of K. Using Hilbert Nullstellensatz (see 2.14.3) one can show that the initial map $\mathbb{A}^n_L \longrightarrow \{\text{prime ideals of } K[X_1, \dots, X_n]\}$ such that $P \mapsto \mathcal{I}(P) = \mathrm{Ker}(\mathrm{ev}_P)$,

5. At least, *if Schanuel's conjecture* is true ([**Mor96**, III.4])...

6. If D is a K-algebra with finite dimension as a vector space over K and D is also a domain, then it is a field. Indeed, because of the finite dimension, every injective K-linear map is also surjective. Applying this to the multiplication endomorphisms of D, we get that every nonzero element of D has an inverse in D.

is surjective for any $n \in \mathbb{N}_+$ and any subfield K of L such that L is algebraic over K if and only if L is an algebraic closure of K.

Proof. — If L is an algebraic closure of K, then L is algebraic over K and hence the map takes values in the set of maximal ideals of $K[\underline{X}]$. If $\mathfrak{m}$ is a maximal ideal of $K[X_1, \ldots, X_n]$ then, thanks to 2.1.4, its extension $\mathfrak{m}L[X_1, \ldots, X_n]$ is a proper ideal of the Noetherian ring $L[X_1, \ldots, X_n]$. Hence, by Noetherianity, there exists a maximal ideal $\mathfrak{M}$ in $L[X_1, \ldots, X_n]$ such that $\mathfrak{m}L[X_1, \ldots, X_n] \subseteq \mathfrak{M}$. By 2.10.3, and the fact that L is algebraically closed, it is necessarily $\mathfrak{M} = (X_1 - a_1, \ldots, X_n - a_n) = \mathcal{I}_L^L(P)$ for some $P = (a_1, \ldots, a_n) \in \mathbb{A}_L^n$, whence $\mathcal{Z}_K^L(\mathfrak{m}) = \mathcal{Z}_L^L(\mathfrak{m}L[X_1, \ldots, X_n]) \supseteq \mathcal{Z}_L^L(\mathfrak{M}) = \{P\}$ and from Hilbert Nullstellensatz 2.14.3 *d*) (for the second equality) $\mathfrak{m} = \sqrt{\mathfrak{m}} = \mathcal{I}_L^K(\mathcal{Z}_K^L(\mathfrak{m})) \subseteq \mathcal{I}_K^L(P)$. As $\mathfrak{m}$ is maximal and $\mathcal{I}_K^L(P)$ is a proper ideal we conclude $\mathfrak{m} = \mathcal{I}_K^L(P)$ [7]. For the converse, let's assume that the map is well defined and surjective for any $n \in \mathbb{N}_+$ and any subfield K of L such that L is algebraic over K. We can then take $n = 1$ and $K = L$. We will show that if L' is an algebraic extension of L then $L' = L$, whence L is algebraically closed. Let $a' \in L'$, as a' is algebraic over L the ideal $\mathcal{I}_L^{L'}(a')$ is a nonzero prime ideal in $L[X]$, hence it is a maximal ideal (because $L[X]$ is an euclidean domain). By the hypothesis we then have that there exists $a \in L$ such that $\mathcal{I}_L^{L'}(a') = \mathcal{I}_L^L(a) = (X - a)$, then $a' = a \in L$ for each $a' \in L'$, whence $L' = L$ as claimed and L is algebraically closed. □

2.10.5. Example: vanishing ideal of the diagonal $\Delta_n \subset \mathbb{A}_L^n$. — Let $\Delta_n := \{(\underline{a}, \underline{b}) \in \mathbb{A}_L^{2n} \mid \underline{a} = \underline{b}\}$ be the diagonal subspace of $\mathbb{A}_L^n \times \mathbb{A}_L^n \cong \mathbb{A}_L^{2n}$ as in 2.2.3. Its vanishing ideal $\mathcal{I}(\Delta_n)$ clearly contains the prime (non maximal) ideal $\mathfrak{d}_\mathfrak{n} = (Y_1 - X_1, \ldots, Y_n - X_n) \subseteq K[\underline{X}, \underline{Y}]$. Let, on the other hand, f be a polynomial of $K[\underline{X}, \underline{Y}]$ such that $f \in \mathcal{I}(\Delta_n)$. Using a sort of "extended division", we will show that, if L is, at least, infinite then $f \in \mathfrak{d}_\mathfrak{n}$. Therefore, in the end, we have that, whenever L is infinite [8], $\mathcal{I}(\Delta_n) = (Y_1 - X_1, \ldots, Y_n - X_n) = \mathfrak{d}_\mathfrak{n}$ in $K[\underline{X}, \underline{Y}]$.

Proof. — From the above discussion, the inclusion $(Y_1 - X_1, \ldots, Y_n - X_n) \subseteq \mathcal{I}(\Delta_n)$ is clear. For the converse, let $A := K[\underline{X}]$. Given any $f \in K[\underline{X}, \underline{Y}] = A[\underline{Y}]$, by **[KR00**, Prop. 3.6.1.], there are polynomials $g_1, \cdots, g_n \in A$ such that

$$f(\underline{X}, \underline{Y}) = g_1(\underline{X})(Y_1 - X_1) + \cdots + g_n(\underline{X})(Y_n - X_n) + f(g_1(\underline{X}), \ldots, g_n(\underline{X})) \text{ in } A[\underline{Y}].$$

7. Note that this does not mean that $\mathcal{Z}_K^L(\mathfrak{m}) = \mathcal{Z}_K^L(\mathcal{I}_K^L(P)) = \{P\}$, indeed the second equality is false in general: for example, $\mathcal{Z}_\mathbb{R}^\mathbb{C}(\mathcal{I}_\mathbb{R}^\mathbb{C}(i)) = \mathcal{Z}_\mathbb{R}^\mathbb{C}(X^2 + 1) = \{-i, i\}$. The point is that $\mathcal{I}_\mathbb{R}^\mathbb{C}(i) = (X^2 + 1) = \mathcal{I}_\mathbb{R}^\mathbb{C}(-i)$, *i.e.* the map we are studying is not injective (unless $K = L$).

8. If $L = \mathbb{F}_q$ is finite, then $\mathcal{I}(\Delta_n) = \mathfrak{d}_\mathfrak{n} + (X_1^q - X_1, \ldots, X_n^q - X_n, Y_1^q - Y_1, \ldots, Y_n^q - Y_n)$

As by assumption is $f \in \mathcal{I}(\Delta_n)$, then $0 = f(\underline{a}, \underline{a}) = f(g_1(\underline{a}), \dots, g_n(\underline{a}))$ for every $\underline{a}) \in \mathbb{A}^n_L$, hence the remainder polynomial $f(g_1(\underline{X}), \dots, g_n(\underline{X}))$ induces the zero function on the whole affine space $\mathbb{A}^n_L$, that is $f(g_1(\underline{X}), \dots, g_n(\underline{X})) \in \mathcal{I}(\mathbb{A}^n_L) = (0)$ as L is infinite. Therefore we have

$$f(\underline{X}, \underline{Y}) = g_1(\underline{X})(Y_1 - X_1) + \cdots + g_n(\underline{X})(Y_n - X_n) \in \mathfrak{d}_{\mathfrak{n}}.$$

□

2.10.6. Example: vanishing ideal of a "cylinder". — Let $V = Z(f_1, \dots, f_r)$ be a K-algebraic subset of $\mathbb{A}^n_L$, and let $\mathrm{Cyl}_{\mathbb{A}^m_L}(V) = V \times \mathbb{A}^m_L$ be its cylinder (cf. 2.2.5) in $\mathbb{A}^{n+m}_L = \mathbb{A}^n_L \times \mathbb{A}^m_L$. If L is infinite, we have

$$\mathcal{I}(\mathrm{Cyl}_{\mathbb{A}^m_L}(V)) = \mathcal{I}(V \times \mathbb{A}^m_L) = \mathcal{I}(V)K[X_1, \dots, X_n, Y_1, \dots, Y_m] = \mathcal{I}(V)[Y_1, \dots, Y_m].$$

Proof. — For the the inclusion $\mathcal{I}(V)[Y_1, \dots, Y_m] \subseteq \mathcal{I}(V \times \mathbb{A}^m_L)$, let $f \in K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ such that $f \in \mathcal{I}(V)[Y_1, \dots, Y_m]$. We can then write $f = \sum_{\underline{\gamma} \in \mathbb{N}^n} f_{\underline{\gamma}}(\underline{X})\, \underline{Y}^{\underline{\gamma}}$, with $f_{\underline{\gamma}} \in \mathcal{I}(V) \subseteq K[\underline{X}]$. Hence, for each $P = \underline{a} \in V$ and each $Q = \underline{b} \in \mathbb{A}^m_L$ we have $f(P, Q) = \sum_{\underline{\gamma} \in \mathbb{N}^n} f_{\underline{\gamma}}(\underline{a})\, \underline{b}^{\underline{\gamma}} = 0$ because $f_{\underline{\gamma}} \in \mathcal{I}(V)$, hence $f_{|V \times \mathbb{A}^m_L} \equiv 0$ and so $f \in \mathcal{I}(V \times \mathbb{A}^m_L)$.
For the converse inclusion, let again $f \in K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ but assume this time that $f \in \mathcal{I}(V \times \mathbb{A}^m_L)$. As before, we can write $f = \sum_{\underline{\gamma} \in \mathbb{N}^n} f_{\underline{\gamma}}(\underline{X})\, \underline{Y}^{\underline{\gamma}}$ with $f_{\underline{\gamma}} \in K[\underline{X}]$. We have to show that $f \in \mathcal{I}(V \times \mathbb{A}^m_L) \Rightarrow f_{\underline{\gamma}} \in \mathcal{I}(V)$ for each $\underline{\gamma}$. Let $P \in V$, then the polynomial function $f(P, \underline{Y}) = \sum_{\underline{\gamma} \in \mathbb{N}^n} f_{\underline{\gamma}}(P)\, \underline{Y}^{\underline{\gamma}}$ vanishes identically on $\mathbb{A}^m_L$ by hypothesis. As L is infinite, this implies $f_{\underline{\gamma}}(P) = 0$ for each $\underline{\gamma}$. As P is arbitrary in V we conclude $f_{\underline{\gamma}} \in \mathcal{I}(V)$ for each $\underline{\gamma}$, and therefore $f \in \mathcal{I}(V)[Y_1, \dots, Y_m]$. □

2.10.7. Example: vanishing ideal of a cartesian product. — Let V and W as in *2.2.6*, with $I = (f_1, \dots, f_r) \subseteq K[\underline{X}]$, $J = (g_1, \dots, g_s) \subseteq K[\underline{Y}]$ and $IK[\underline{Y}] + JK[\underline{X}] = (f_1, \dots, f_r, g_1, \dots, g_s) \subseteq K[X_1, \dots, X_n, Y_1, \dots, Y_m]$, then

$$\begin{aligned} \mathcal{I}(V \times W) &= \mathcal{I}((V \times \mathbb{A}^m_L) \cap (\mathbb{A}^n_L \times W)) = \mathcal{I}(\mathcal{Z}(IK[\underline{Y}] + JK[\underline{X}])) \\ &\supseteq \sqrt{\mathcal{I}(\mathcal{Z}(I))[\underline{Y}] + \mathcal{I}(\mathcal{Z}(J))[\underline{X}]}. \end{aligned}$$

Moreover, if K is a field of characteristic zero (or more generally, if K is a **perfect field** [9]) then $\sqrt{\mathcal{I}(\mathcal{Z}(I))[\underline{Y}] + \mathcal{I}(\mathcal{Z}(J))[\underline{X}]} = \mathcal{I}(\mathcal{Z}(I))[\underline{Y}] + \mathcal{I}(\mathcal{Z}(J))[\underline{X}]$ (because, in that case, the right hand

9. The concept of a **perfect field** and the behavior of tensor products of algebra over it can be found, for example in [**Bos18**, 3.6; 7.4, Ex. 6]. As every field of characteristic zero is a perfect field, and here we are mainly interested in the case $K = \mathbb{R}$, which has zero characteristic, we do not give details on that.

side is already a radical ideal). We will see in 2.21.1 *o*), *p*) that if L is algebraically closed or real-closed, then $\mathcal{I}_K^L(V \times W) = \mathcal{I}_K^L(\mathcal{Z}(I))[\underline{Y}] + \mathcal{I}_K^L(\mathcal{Z}(J))[\underline{X}]$. But, in the general case, only the inclusion shown above does hold.

2.10.8. Critical example. — Let p is a prime integer, $K = \mathbb{F}_p(T)$ and L be an algebraic closure of $\mathbb{F}_p(T)[U]/(U^p - T) = \mathbb{F}_p(\sqrt[p]{T})$. Then (by Frobenius endomorphism in characteristic p): $V = W = \mathcal{Z}_K^L(X^p - T) = \mathcal{Z}_K^L((X - \sqrt[p]{T})^p) = \{\sqrt[p]{T}\}$ and $V \times W = \{(\sqrt[p]{T}, \sqrt[p]{T})\}$. We also have $\mathcal{I}_K^L(V) = (X_1^p - T)$ and $\mathcal{I}_K^L(W) = (Y_1^p - T)$, essentially because $\sqrt[p]{T} \notin K$. In $K[X_1, Y_1]$ we find $\mathcal{Z}(I)[Y_1] + \mathcal{Z}(J)[X_1] = (X_1^p - T, Y_1^p - T) = (X_1^p - Y_1^p, Y_1^p - T) = ((X_1 - Y_1)^p, Y_1^p - T)$, which is not a radical ideal. Indeed, by Frobenius homomorphism,

$$(X_1 - Y_1)^p = X_1^p - Y_1^p = (X_1^p - T) - (Y_1^p - T) \in (X_1^p - T, Y_1^p - T),$$

but $X_1 - Y_1 \notin (X_1^p - T, Y_1^p - T)$ for degree reason. Therefore, in this case,

$$\mathcal{I}(V \times W) \supsetneq \mathcal{I}_K^L(I)[Y_1] + \mathcal{Z}_I^L(J)[X_1].$$

Actually, it is $\mathcal{I}(V \times W) = (X_1 - Y_1, Y_1^p - T)$, indeed $K[X_1, Y_1]/(X_1 - Y_1, Y_1^p - T) \cong L$ and thus $(X_1 - Y_1, Y_1^p - T)$ is a maximal ideal.

2.11. Vanishing ideals, regular functions and regular maps

2.11.1. Remark: coordinate rings are quotients of polynomial rings. — If S is a subset of $\mathbb{A}_L^n$, the inclusion map $i_S \colon S \hookrightarrow \mathbb{A}_L^n$ induces a restriction homorphism of K-algebras in the opposite direction $\mathrm{res}_S = i_S^* \colon K[\mathbb{A}_L^n]_L \longrightarrow K[S]_L$, $f \mapsto f \circ i_S = f_{|S}$ which is surjective by definition of $K[S]_L$, and whose kernel coincides with the vanishing ideal of the subset S. We therefore have an exact sequence [10] of $K[\mathbb{A}_L^n]_L$-modules, as well as K-vector spaces,

$$0 \longrightarrow \mathcal{I}_K^L(S) \longrightarrow K[\mathbb{A}_L^n]_L \xrightarrow{\mathrm{res}_S} K[S]_L \longrightarrow 0.$$

Hence the K-algebras $K[S]$ are all just quotients of the polynomial ring $K[X_1, \cdots, X_n]$ by a radical ideal. In particular, they are all *affine K-algebras*, that is finitely generated reduced K-algebras: $K[S]_L \cong K[\mathbb{A}_L^n]_L / \operatorname{Ker}(\mathrm{res}_S) \cong K[X_1, \cdots, X_n] / \mathcal{I}_K^L(S)$. It can be proven that, conversely, any affine K-algebra is the coordinate ring of some K-algebraic set (see [**Kun85**, Ch. I, Sec. 3, Rules 3.12 f)]).

10. It just means that, in each point, the image of the incoming map is equal to the kernel of the next one.

2.11.2. Corollary (vanishing ideals of irreducible sets). — *Let V be a K-algebraic subset of $\mathbb{A}^n_L$, then: V is irreducible if and only if $\mathcal{I}^L_K(V)$ is a prime ideal of $K[X_1,\dots,X_n]$.*

Proof. — By previous remark, it is a straightforward reformulation of 2.8.1. □

2.11.3. Proposition (defining equations of regular maps). — *Let $V=\mathcal{Z}(I)\subseteq\mathbb{A}^n_L$ and $W=\mathcal{Z}(J)\subseteq\mathbb{A}^m_L$ two K-algebraic sets. Then, given $F=(f_1,\dots,f_m)\in K[X_1,\dots,X_n]^m$ we have that F induces a K-regular map $\Phi_F\colon V\longrightarrow W$ if and only if $\Phi_F^*(\mathcal{I}(\mathcal{Z}(J)))\subseteq\mathcal{I}(\mathcal{Z}(I))$*

Proof. — It is clear that F induces a K-regular map $\Phi_F\colon\mathbb{A}^n_L\longrightarrow\mathbb{A}^m_L$, such that $(a_1,\dots,a_n)\mapsto(f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n))$. This regular map induces, by restriction, a K-regular map between V and W if and only if $\Phi_F(P)\in W$ for each $P\in V$. Assume now that $\Phi_F^*(\mathcal{I}(\mathcal{Z}(J)))\subseteq\mathcal{I}(\mathcal{Z}(I))$ holds true, and let $g\in\mathcal{I}(\mathcal{Z}(J))$. Then

$$\Phi_F^*(g)=g\circ\Phi_F=g((f_1(X_1,\dots,X_n),\dots,f_m(X_1,\dots,X_n)))\in\mathcal{I}(\mathcal{Z}(I)).$$

For any $P\in V=\mathcal{Z}(I)$ we than have $g(\Phi_F(P))=(g\circ\Phi_F)(P)=0$ for any $g\in\mathcal{I}(\mathcal{Z}(J))$, that is $\Phi_F(P)\in W=\mathcal{Z}(\mathcal{I}(\mathcal{Z}(J)))$. Therefore Φ_F restricts to a K-regular map $V\longrightarrow W$. For the converse, assume that $\Phi_F\colon\mathbb{A}^n_L\longrightarrow\mathbb{A}^m_L$ restricts to a K-regular map $V\longrightarrow W$. Then $\Phi_F(V)\subseteq W$, and taking $\mathcal{I}$ this gives $\mathcal{I}(\Phi_F(\mathcal{Z}(I)))\supseteq\mathcal{I}(\mathcal{Z}(J))$. Let now $g\in\mathcal{I}(\mathcal{Z}(J))$, and consider $\Phi_F^*(g)=g\circ\Phi_F$. Let now P be any point in V, then $\Phi_F^*(g)(P)=(g\circ\Phi_F)(P)=g(\Phi_F(P))=0$, therefore $\Phi_F^*(g)\in\mathcal{I}(\mathcal{Z}(I))$, as claimed. □

2.11.4. Remark. — The previous result means that to define a K-regular map from V to W trough $F=(f_1,\dots,f_m)\in K[X_1,\dots,X_n]^m$ we need *generators for their vanish ideals* (not just sets of defining equations): $\mathcal{I}(V)=(u_1,\dots,u_s)\subseteq K[X_1,\dots,X_n]$, $\mathcal{I}(W)=(v_1,\dots,v_t)\subseteq K[Y_1,\dots,Y_m]$, and we need to check that $v_1(f_1,\dots,f_m),\dots,v_t(f_1,\dots,f_m)\in(u_1,\dots,u_s)$.

2.11.5. Proposition (K-isomorhism). — *If $\Phi\colon V\longrightarrow W$ is a K-regular map from V to W, then Φ is a K-polynomial isomorphism if and only if its induced K-algebras homomorphism $\Phi^*\colon K[W]_L\longrightarrow K[V]_L$ is an isomorphism of K-algebras.*

Proof. — From *2.6.3 b)* and *a)* it is clear that if Φ is a K-regular isomorphism, then Φ^* is an isomorphism of K-algebras (whose inverse is Υ^*).
For the converse, as $K[V]\cong K[X_1,\dots,X_n]/\mathcal{I}(V)$ and $K[W]\cong K[Y_1,\dots,Y_m]/\mathcal{I}(V)$, let Υ be the K-regular map induced by a polynomial representative $G=(g_1,\dots,g_n)\in K[Y_1,\dots,Y_m]^n$

for the inverse of the K-algebra isomorphism Φ^*:

$$\Phi^{*-1}\colon K[V] \cong K[X_1,\dots,X_n]/\mathcal{I}(V) \longrightarrow K[W] \cong K[Y_1,\dots,Y_m]/\mathcal{I}(V).$$

All the necessary verifications are straightforward. □

2.11.6. Proposition (vanishing ideals of images and graphs). — *Let $V = \mathcal{Z}(I) \subseteq \mathbb{A}^n_L$ and $W = \mathcal{Z}(J) \subseteq \mathbb{A}^m_L$ two K-algebraic sets, and let $\Phi\colon V \longrightarrow W$ be a K-regular map induced by $F = (f_1,\dots,f_m) \in K[X_1,\dots,X_n]^m$.*

a) If $S \subseteq V$ then $\mathcal{I}(\Phi(S)) = \Phi^{*-1}(\mathcal{I}(S))$ and $\overline{\Phi(S)}^Z = \mathcal{Z}(\Phi^{*-1}(\mathcal{I}(S)))$ In particular, if $S = \mathcal{Z}(I')$ for some ideal $I' \subseteq K[X_1,\dots,X_n]$ containing I, it is $\overline{\Phi(\mathcal{Z}(I'))}^Z \subseteq \mathcal{Z}(\Phi^{*-1}(I'))$.

b) The vanishing ideal of the graph of Φ is

$$\mathcal{I}(\Gamma_\Phi) = \mathcal{I}(V)K[\underline{X},\underline{Y}] + (y_1 - f_1(X_1,\dots,X_n),\dots,y_m - f_m(X_1,\dots,X_n)) \subseteq K[\underline{X},\underline{Y}],$$

and, for any ideal $I' \subseteq K[X_1,\dots,X_n]$ containing I,

$$\mathcal{I}(\Phi(\mathcal{Z}(I'))) = (\ \mathcal{I}(\mathcal{Z}(I'))K[\underline{X},\underline{Y}] + (y_1 - f_1,\dots,y_m - f_m)\ ) \cap K[\underline{Y}],$$

where $K[\underline{X}] = K[X_1,\dots,X_n]$ and $K[\underline{Y}] = K[Y_1,\dots,Y_m]$.

Proof. — *a)* Let $S \subseteq V$ and $P \in S$, then

$$\mathcal{I}(\Phi(P)) = \mathrm{Ker}(\mathrm{ev}_{\Phi(P)}) = \mathrm{Ker}(\mathrm{ev}_{\mathrm{ev}_P\Phi}) = \mathrm{Ker}(\mathrm{ev}_P \circ \Phi^*) = \Phi^{*-1}(\mathcal{I}(P)).$$

Therefore $\mathcal{I}(\Phi(S)) = \bigcap_{P\in S}\mathcal{I}(\Phi(P)) = \bigcap_{P\in S}\Phi^{*-1}(\mathcal{I}(P)) = \Phi^{*-1}(\bigcap_{P\in S}\mathcal{I}(P)) = \Phi^{*-1}(\mathcal{I}(S))$ and $\overline{\Phi(S)}^Z = \mathcal{Z}(\mathcal{I}(\Phi(S))) = \mathcal{Z}(\Phi^{*-1}(\mathcal{I}(S)))$. In particular

$$\mathcal{I}(\mathcal{Z}(I')) \supseteq I' \ \Rightarrow\ \Phi^{*-1}(\mathcal{I}(\mathcal{Z}(I'))) \supseteq \Phi^{*-1}(I')$$

and so $\overline{\Phi(\mathcal{Z}(I'))}^Z = \mathcal{Z}(\Phi^{*-1}(\mathcal{I}(\mathcal{Z}(I')))) \subseteq \mathcal{Z}(\Phi^{*-1}(I'))$.

b) The inclusion $\mathcal{I}(\Gamma_\Phi) \subseteq \mathcal{I}(V)K[\underline{X},\underline{Y}] + (y_1 - f_1(X_1,\dots,X_n),\dots,y_m - f_m(X_1,\dots,X_n))$ is trivial. Let now $h \in K[\underline{X},\underline{Y}] = (K[\underline{X}])[\underline{Y}]$ be such that $h \in \mathcal{I}(\Gamma_\Phi)$. Thanks to [**KR00**, Prop. 3.6.1] we can write $h = \sum_{i=1}^m h_i(\underline{X},\underline{Y})(y_i - f_i(\underline{X})) + h(f_1(\underline{X}),\dots,f_m(\underline{X}))$. As h vanishes on Γ_Φ we get $P \in V \ \Rightarrow\ 0 = \mathrm{ev}_{(P,\Phi(P))}(h) = \mathrm{ev}_P(h(f_1(\underline{X}),\dots,f_m(\underline{X})))$, therefore

$$h(f_1(\underline{X}),\dots,f_m(\underline{X})) \in \mathcal{I}(V)[\underline{X},\underline{Y}].$$

For the last statement, we have $\Phi(\mathcal{Z}(I')) = \mathrm{pr}_W(\Gamma_{\Phi_{|\mathcal{Z}(I')}})$, hence

$$\mathcal{I}(\Phi(\mathcal{Z}(I'))) = {\mathrm{pr}^*_W}^{-1}(\mathcal{I}(\Gamma_{\Phi_{|\mathcal{Z}(I')}})) = \mathcal{I}(\Gamma_{\Phi_{|\mathcal{Z}(I')}}) \cap K[\underline{Y}]$$

as ${\mathrm{pr}_W^*}^{-1}(T) = T \cap K[\underline{Y}]$ for every $T \subseteq K[\underline{X}, \underline{Y}]$. □

2.12. Galois connection and the closure operator

2.12.1. Proposition. — *The two composite maps $\mathcal{Z} \circ \mathcal{I}$ and $\mathcal{I} \circ \mathcal{Z}$ are "enlarging": for any subset S of $\mathbb{A}_L^n$ we have $S \subseteq \mathcal{Z}(\mathcal{I}(S))$, and for any subset T of $K[\underline{X}]$ we have $T \subseteq \mathcal{I}(\mathcal{Z}(T))$. Moreover $\mathcal{Z}(\mathcal{I}(\mathcal{Z}(T))) = \mathcal{Z}(T)$ for every $T \subseteq K[\underline{X}]$, and $\mathcal{I}(\mathcal{Z}(\mathcal{I}(S))) = \mathcal{I}(S)$ for every $S \subseteq \mathbb{A}_L^n$.*

Proof. — The first statement is clear. For the first equation of the second part, from $I \subseteq \mathcal{I}(\mathcal{Z}(T))$ it follows $\mathcal{Z}(T) \supseteq \mathcal{Z}(\mathcal{I}(\mathcal{Z}(T)))$. On the other hand, let $P \in \mathcal{Z}(T)$ be fixed and let $f \in I := \mathcal{I}(\mathcal{Z}(T))$ a generic element, then $f(P) = 0$ by definition of $\mathcal{I}(\mathcal{Z}(T))$; as this is true for all $f \in \mathcal{I}(\mathcal{Z}(T))$, then $P \in \mathcal{Z}(I) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(T)))$ and this shows $\mathcal{Z}(T) \subseteq \mathcal{Z}(\mathcal{I}(\mathcal{Z}(T)))$. Analogously, for the second, from $S \subseteq \mathcal{Z}(\mathcal{I}(S))$ it follows $\mathcal{I}(S) \supseteq \mathcal{I}(\mathcal{Z}(\mathcal{I}(S)))$. On the other hand, let $f \in \mathcal{I}(S)$ be fixed and let $P \in V := \mathcal{Z}(\mathcal{I}(S))$ a generic element, then $f(P) = 0$ by definition of $\mathcal{Z}(\mathcal{I}(S))$; as this is true for all $P \in \mathcal{Z}(\mathcal{I}(S))$, then $f \in \mathcal{I}(V) = \mathcal{I}(\mathcal{Z}(\mathcal{I}(S)))$ and this shows $\mathcal{I}(S) \subseteq \mathcal{I}(\mathcal{Z}(\mathcal{I}(S)))$. □

This shows that the pair of "opposite" maps $\mathcal{Z}$ and $\mathcal{I}$ forms a *Galois connection* ([**Bor94**, 3.1.6.m], [**Mac98**, IV.5], [**Eis95**, Ex. 1.8]).

2.12.2. Example. — Note also that, for $K = L = \mathbb{R}$ and $n = 1$, it is $\mathcal{I}_{\mathbb{R}}^{\mathbb{R}}(\mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(X^2 + 1)) = \mathcal{I}_{\mathbb{R}}^{\mathbb{R}}(\emptyset) = K[X]$ while $\mathcal{I}_{\mathbb{R}}^{\mathbb{C}}(\mathcal{Z}_{\mathbb{R}}^{\mathbb{C}}(X^2 + 1)) = \mathcal{I}_{\mathbb{R}}^{\mathbb{C}}(\{-i, i\}) = (X^2 + 1)$. This shows that if L is not algebraically closed the composite $\mathcal{I} \circ \mathcal{Z}$ can behave badly. Moreover, $(X^2 + 1)$ is a maximal ideal of $\mathbb{R}[X]$ whose extension to $\mathbb{C}[X]$ is no longer such: $(X^2 + 1)\mathbb{C}[X] = (X + i) \cap (X - i) = (X + i)(X - i)$, and neither $(X + i) \subseteq (X^2 + 1)$ nor $(X + i) \subseteq (X^2 + 1)$, hence $(X^2 + 1)\mathbb{C}[X]$ is not a prime ideal of $\mathbb{C}[X]$.

We already noticed that obviously $S \subseteq \mathcal{Z}(\mathcal{I}(S))$. Actually $\mathcal{Z}(\mathcal{I}(S))$ is the smallest Zariski close subset of $\mathbb{A}_L^n$ containing S, i.e. its *(Zariski) closure*.

2.12.3. Proposition (closure operator). — *For every $S \subseteq \mathbb{A}_L^n$ we have:*

$$\overline{S}^Z = \mathcal{Z}(\mathcal{I}(S)) = \{P \in \mathbb{A}_L^n \mid f(P) = 0 \text{ for every } f \text{ such that } f_{|S} \equiv 0\}.$$

Therefore, the composite map $\mathcal{Z} \circ \mathcal{I}$ from $\mathbb{A}_L^n$ to itself is the **closure operator** *of the Zariski topology on $\mathbb{A}_L^n$ relative to K.*

Proof. — If $\mathcal{Z}(I)$ is a Zariski closed subset containing S, from $S \subseteq \mathcal{Z}(I)$ we get $\mathcal{I}(S) \supseteq \mathcal{I}(\mathcal{Z}(I))$, and hence $\mathcal{Z}(\mathcal{I}(S)) \subseteq \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I))) = \mathcal{Z}(I)$. This shows that any Zariski closed subset containing S contains also the Zariski closed subset $\mathcal{Z}(\mathcal{I}(S))$, hence this last is the (Zariski) closure of S. □

2.12.4. Remark: $\mathcal{I}$ is injective on algebraic set. — In particular, this means that for any K-algebraic set $V \subseteq \mathbb{A}^n_L$ we have $\mathcal{Z}(\mathcal{I}(V)) = V$, and therefore $\mathcal{I}$ is an injective map when restricted to K-algebraic sets of $\mathbb{A}^n_L$.

2.12.5. Remark. — Note that, tautologically, $\mathcal{I}(\overline{S}^Z) = \mathcal{I}(\mathcal{Z}(\mathcal{I}(S))) = \mathcal{I}(S)$ for any $S \subseteq \mathbb{A}^n_L$.

2.12.6. Remark. — If L is infinite, then $\mathbb{A}^n_L$ is irreducible ([**Kun85**, Ch. I, Rules 1.8]), while it's a discrete topological space if L is finite ([**Kun85**, Ch. I, Ex.3, Ex. 6]).

2.13. "Pathologies" over non algebraically closed fields

2.13.1. Example. — The ideal $I := (X^2+1)$ is prime ideal in $\mathbb{R}[X]$ (actually a maximal ideal, as the quotient $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ is a field), but its set of real zeros is empty: $\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X^2+1) = \emptyset$ (which is not considered an irreducible space) and $\mathcal{I}^{\mathbb{R}}_{\mathbb{R}}(\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X^2+1)) = \mathcal{I}^{\mathbb{R}}_{\mathbb{R}}(\emptyset) = \mathbb{R}[X]$ which is not a prime ideal.

2.13.2. Example. — A less basic example could be anything like:

$$\mathfrak{p} := ((X-a)^2(X-b)^2 + Y^2) \subseteq \mathbb{R}[X,Y],$$

with $a \neq b$ in $\mathbb{R}$, which is necessarily a prime ideal because ([**Lan02**, II, 5]) the polynomial $f(X,Y) = (X-a)^2(X-b)^2 + Y^2$ is irreducible in the unique factorization domain $\mathbb{R}[X,Y]$. Else, it would necessarily split as $(Y+u(X))(Y+v(X))$ with $u(X), v(X) \in \mathbb{R}[X]$ of degree one. By comparison, it must be $v(X) = -u(X)$, hence we would have $f(X,Y) = Y^2 - u(X)^2$, which is clearly false as f can only take non negative values, being a sum of squares. On the other hand,

$$\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(\mathfrak{p}) = \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(f(X,Y)) = \{(a,0),\,(b,0)\} = \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X-a,Y) \cup \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X-b,Y) = \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(\mathfrak{m}_{(a,0)}) \cup \mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(\mathfrak{m}_{(b,0)})$$

is not irreducible. One can show that $\mathcal{I}^{\mathbb{R}}_{\mathbb{R}}(\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(\mathfrak{p})) = ((X-a)(X-b), Y) = \mathfrak{m}_{(a,0)} \cap \mathfrak{m}_{(b,0)}$, which is not a prime ideal because $X-a \notin \mathcal{I}^{\mathbb{R}}_{\mathbb{R}}(\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(\mathfrak{p}))$ and $X-b \notin \mathcal{I}^{\mathbb{R}}_{\mathbb{R}}(\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(\mathfrak{p}))$, but $(X-a)(Y-b) \in \mathcal{I}^{\mathbb{R}}_{\mathbb{R}}(\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(\mathfrak{p}))$.

2.13.3. Remark. — These kind of phenomena are less unexpected than one could think. Indeed we already mentioned (cf. footnote to 2.4.5) that if L is not algebraically closed then any algebraic subset of $\mathbb{A}^n_L$, of whatever nature, as a set of points, is the zero locus of a single polynomial from $L[\underline{X}]$, i.e. it is an *hypersurface* (in the classical language of Algebraic Geometry). That is, for every I ideal of $L[\underline{X}]$ there exists a polynomial $f \in L[\underline{X}]$ (not unique, in general) such that $\mathcal{Z}^L_L(I) = \mathcal{Z}^L_L(f)$. Sometimes we can choose f to have special properties, for example being irreducible in $L[\underline{X}]$ (as in the example above), in this case the principal ideal (f) is prime by factoriality of $L[\underline{X}]$. This is a huge source of so called "pathologies" of algebraic geometry done at set-theoretic level on non algebraically closed fields. See also 2.18. This cannot happen if L is algebraically closed (see *2.14.3*).

2.14. Hilbert's Nullstellensatz

2.14.1. The $\mathcal{I}$-$\mathcal{Z}$ correspondence. — If we restrict $\mathcal{I}$ from K-algebraic sets of $\mathbb{A}^n_L$ to radical ideals of $K[\underline{X}]$ we then get a strictly decreasing map. Thus, so far we have two opposite, inclusion-reversing, maps

$$\{K\text{-algebraic subsets of } \mathbb{A}^n_L\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} \{\text{radical ideals of } K[X_1, \dots, X_n]\}$$

such that $\mathcal{I} \circ \mathcal{Z}(I) \supseteq I$ and $\mathcal{Z} \circ \mathcal{I}(V) = V$. In particular, $\mathcal{I}$ (restricted to K-algebraic sets), having a left inverse, is necessarily injective (and $\mathcal{Z}$ is, obviously, surjective onto K-algebraic sets), which means that any K-algebraic set V is always completely identified by its vanishing ideal $\mathcal{I}(V)$.

2.14.2. Remark: $\mathcal{I} \circ \mathcal{Z} \neq \mathrm{Id}$ in general.— We noticed above that $\mathcal{I}^{\mathbb{R}}_{\mathbb{R}}(\mathcal{Z}^{\mathbb{R}}_{\mathbb{R}}(X^2+1)) = \mathbb{R}[X]$, but even if we take $L = K = \mathbb{C}$ yet $\mathcal{I}^{\mathbb{C}}_{\mathbb{C}}(\mathcal{Z}^{\mathbb{C}}_{\mathbb{C}}(X^n)) = \mathcal{I}^{\mathbb{C}}_{\mathbb{C}}(\mathcal{Z}^{\mathbb{C}}_{\mathbb{C}}(X)) = (X) \subseteq \mathbb{C}[X]$ for every $n \in \mathbb{N}_+$, though in the first case the starting ideal ((X^2+1) in $\mathbb{R}[X]$) is even a prime ideal. Hence the first composite usually differ from the identity map. In the first example the issue is due to the fact that $\mathbb{R}$ is not an algebraically closed field, while in the second example the point is that the ideals (X^n), with $n \in \mathbb{N}$, $n \geq 2$, are not radical. It naturally raises the question under which condition, if any, this pair of maps is a bijection. This is the case if L is an *algebraically closed field*, this result is one of the many equivalent forms of the fundamental Hilbert's Nullstellensatz.

2.14.3. Theorem (Hilbert Nullstellensatz). — *Let L be a field, the following facts are equivalent:*

a) The field L is an algebraically closed.

b) For every $n \in \mathbb{N}_+$ the only maximal ideals of $L[X_1, \dots, X_n]$ are those corresponding to L-rational points of $\mathbb{A}^n_L$, i.e. the map

$$P = (a_1, \dots, a_n) \in \mathbb{A}^n_L \mapsto (X_1 - a_1, \dots, X_n - a_n) \in \{\text{maximal ideals of } L[X_1, \dots, X_n]\}$$

is bijective.

c) For every $n \in \mathbb{N}_+$ and every subfield K of L, if I is an ideal of $K[X_1, \dots, X_n]$ then $\mathcal{Z}^L_K(I) = \emptyset \Leftrightarrow 1 \in I$;

d) For every $n \in \mathbb{N}_+$ and every subfield K of L, If J is any ideal of $K[X_1, \dots, X_n]$, then $\mathcal{I}^L_K(\mathcal{Z}^L_K(J)) = \sqrt{J}$;

e) For every $n \in \mathbb{N}_+$ and every subfield K of L, the assignment

$$\mathcal{I}^L_K \colon \{K\text{-algebraic sets of } \mathbb{A}^n_L\} \longrightarrow \{\text{radical ideals of } K[X_1, \dots, X_n]\},\ V \mapsto \mathcal{I}^L_K(V)$$

defines a bijection of the set of all K-algebraic sets $V \subseteq \mathbb{A}^n_L$ onto the set of all ideals I of $K[X_1, \dots, X_n]$ such that $I = \sqrt{I}$, with inverse the map

$$\mathcal{Z}^L_K \colon \{\text{radical ideals of } K[X_1, \dots, X_n]\} \longrightarrow \{K\text{-algebraic sets of } \mathbb{A}^n_L\},\ I \mapsto \mathcal{Z}^L_K(I);$$

in this bijection irreducible algebraic sets correspond to prime ideals, and vice-versa.

Proof. — Everything can be found, though in a less compact form, for example among many others, in [**Kun85**, Ch. 1, Sec. 3] as well as in [**KR00**, 2.6]. I will sketch a path of proof giving the exact references to [**KR00**].

a) $\Rightarrow$ *b*) is [**KR00**, Prop. 2.6.11] (with $I = (0)$).

b) $\Rightarrow$ *c*) is [**KR00**, Thm. 2.6.13] (where in the proof it is used *b*) together with 2.1.4 and the Noetherianity of the polynomial ring).

c) $\Rightarrow$ *d*) is [**KR00**, Thm. 2.6.12] (where *d* is deduced from *c*) by means of the so called "Rabinowitsch trick").

d) $\Rightarrow$ *e*) In the given situation, by 2.12.3 we have $\mathcal{Z} \circ \mathcal{I} = \mathrm{Id}$ on K-algebraic subsets. Thanks to *d*), if I is a radical ideal of $K[X_1, \dots, X_n]$ we get also $\mathcal{I} \circ \mathcal{Z}(I) = \sqrt{I} = I$, that is $\mathcal{I} \circ \mathcal{Z} = \mathrm{Id}$ on radical ideals. Hence the two maps are reciprocal inverse. As an algebraic set V is irreducible if and only if its vanishing ideal $\mathcal{I}(V)$ is prime also the last statement clear.

e) $\Rightarrow$ *a)* To prove that L is algebraically closed we need to show that every univariate polynomial $f(X) \in L[X]$ of positive degree has a root in L, *i.e.* $\mathcal{Z}^L(f) \neq \emptyset$. If, by contradiction, $\mathcal{Z}(f) = \emptyset = \mathcal{Z}(1)$, then thanks to *e)* we get $\sqrt{(f)} = \mathcal{I}(\mathcal{Z}^L(f)) = \mathcal{I}(\emptyset) = (1)$ and so $1 \in (f)$. But this is impossible by degree reasons. □

2.14.4. Corollary. — *Let L be a algebraically closed field, and let I be an ideal of $K[X_1, \ldots, X_n]$ (so that $\mathcal{Z}_K^L(I) \subseteq \mathbb{A}_L^n$ is a K-algebraic set). Then $K[\mathcal{Z}_K^L(I)]_L \cong K[X_1, \ldots, X_n]/\sqrt{I}$.*

Proof. — From Hilbert Nullstellensatz $\mathcal{I}_K^L(\mathcal{Z}_K^L(I)) = \sqrt{I}$, the result follows then by 2.11.1. □

2.14.5. Corollary. — *Let L be a algebraically closed field, and let $V = \mathcal{Z}(I) \subseteq \mathbb{A}_L^n$ and $W = \mathcal{Z}(J) \subseteq \mathbb{A}_L^m$ two K-algebraic sets. Let $\Phi\colon V \longrightarrow W$ be a K-regular map induced by $F = (f_1, \ldots, f_m) \in K[X_1, \ldots, X_n]^m$. Then the vanishing ideal of the graph of Φ is*

$$\mathcal{I}(\Gamma_\Phi) = \sqrt{I}K[\underline{X}, \underline{Y}] + (y_1 - f_1(X_1, \ldots, X_n), \ldots, y_m - f_m(X_1, \ldots, X_n)) \subseteq K[\underline{X}, \underline{Y}],$$

and $\mathcal{I}(\Phi(V)) = (\ \sqrt{I}K[\underline{X}, \underline{Y}] + (y_1 - f_1, \ldots, y_m - f_m)\ ) \cap K[\underline{Y}]$, where $K[\underline{X}] = K[X_1, \ldots, X_n]$ and $K[\underline{Y}] = K[Y_1, \ldots, Y_m]$.

Proof. — It immediately follows from 2.11.6 *b)* as, by Hilbert Nullstellenstz, $\mathcal{I}(V) = \sqrt{I}$. □

2.14.6. Corollary. — *Let L be an algebraically closed field, and let $V = \mathcal{Z}(I) \subseteq \mathbb{A}_L^n$ and $W = \mathcal{Z}(J) \subseteq \mathbb{A}_L^m$ two K-algebraic sets If $\Phi\colon V \longrightarrow W$ is a K-regular map induced by $F = (f_1, \ldots, f_m) \in K[\underline{X}]^m$, then, for any ideal $I' \subseteq K[X_1, \ldots, X_n]$ containing $\sqrt{I}$, we have $\overline{\Phi(\mathcal{Z}(I'))}^Z = \mathcal{Z}(\Phi^{*-1}(I'))$ and*

$$\mathcal{I}(\overline{\Phi(\mathcal{Z}(I'))}^Z) = \mathcal{I}(\Phi(\mathcal{Z}(I'))) = (\sqrt{I'}K[\underline{X}, \underline{Y}] + (y_1 - f_1, \ldots, y_m - f_m)) \cap K[\underline{Y}].$$

Proof. — From 2.11.6 *a)*, with $S = \mathcal{Z}(I')$, Hilbert Nullstellensatz, and *1.9.5 k)*, we have

$$\overline{\Phi(\mathcal{Z}(I'))}^Z = \mathcal{Z}(\Phi^{*-1}(\mathcal{I}(\mathcal{Z}(I')))) = \mathcal{Z}(\Phi^{*-1}(\sqrt{I'})) = \mathcal{Z}\left(\sqrt{\Phi^{*-1}(I')}\right) = \mathcal{Z}(\Phi^{*-1}(I')).$$

The first equality in the second statement is clear (cf. 2.12). Then, by Hilbert Nullstellensatz and 2.11.6 *b)* we get $\mathcal{I}(\Phi(\mathcal{Z}(I'))) = (\ \sqrt{I'}K[\underline{X}, \underline{Y}] + (y_1 - f_1, \ldots, y_m - f_m)\ ) \cap K[\underline{Y}]$ □

2.14.6.1. **Critical example**. — Let $L = \mathbb{R}$, $K = \mathbb{Q}$ and $V = \mathbb{R}^2$, $W = \mathbb{R}$ be $\mathbb{Q}$-algebraic sets. We have a $\mathbb{Q}$-regular dominant map $\mathrm{pr}_1 \colon V \longrightarrow W$, $(a_1, a_2) \mapsto a_1$ which induces the ring injection $\mathrm{pr}_1^* \colon \mathbb{Q}[W] = \mathbb{Q}[Y] \hookrightarrow \mathbb{Q}[V] = \mathbb{Q}[X_1, X_2]$, $f(Y) \mapsto f(X_1)$. Let $I := (X_1, X_2^2 + 1)$ in $\mathbb{Q}[X_1, X_2]$, then $\mathcal{Z}_{\mathbb{Q}}^{\mathbb{R}}(I) = \emptyset \Rightarrow \overline{\mathrm{pr}_1(\mathcal{Z}_{\mathbb{Q}}^{\mathbb{R}}(I))}^{Z} = \emptyset$. On the other hand,

$$\mathrm{pr}_1^{*-1}(I) = \{f(Y) \in \mathbb{Q}[Y] \mid f(X_1) \in I\} = (Y) \Rightarrow \mathcal{Z}_{\mathbb{Q}}^{\mathbb{R}}(\mathrm{pr}_1^{*-1}(I)) = \{0\} \supsetneq \emptyset.$$

Therefore the hypothesis on L in *2.14.6* is essential.

2.15. Irreducible components over an algebraically closed field

If L is algebraically closed, and I is a radical ideal, the two decompositions mentioned in *2.8.2* and *2.8.3* do coincide. That is, if $I = Q_1 \cap \cdots \cap Q_r$ is a minimal primary decomposition of I with Q_i $\mathfrak{p}_i$-primary ideals and $V = \mathcal{Z}_K^L(I) = V_1 \cup \cdots \cup V_s$ is the decomposition of V into irreducible components V_i, then $r = s$ and (up to reordering) $\mathcal{Z}_K^L(\mathfrak{p}_i) = V_i$ for $i = 1, \cdots, r$.
Indeed, starting from $I = Q_1 \cap \cdots \cap Q_r$ and taking its zeros we get

$$V = \mathcal{Z}_K^L(Q_1) \cup \cdots \cup \mathcal{Z}_K^L(Q_r) = \mathcal{Z}_K^L(\mathfrak{p}_1) \cup \cdots \cup \mathcal{Z}_K^L(\mathfrak{p}_r) = V_1 \cup \cdots \cup V_r$$

where, now, all the $V_i = \mathcal{Z}_K^L(\mathfrak{p}_i)$ are irreducible because, thanks to Nullstellensatz, their vanishing ideals are all prime: $\mathcal{I}_K^L(V_i) = \mathcal{I}_K^L(\mathcal{Z}_K^L(\mathfrak{p}_i)) = \sqrt{\mathfrak{p}_i} = \mathfrak{p}_i$. As we started from a minimal primary decomposition we don't have repetitions of V_i and as I is a radical ideal there are no embedded primes, therefore the irreducible V_i are maximal, and hence they are the irreducible components of $V = \mathcal{Z}_K^L(I)$.

2.15.1. Critical Example: I not radical. — If I is not radical the result does not hold. For $I = (XY, Y^2)$ ($\mathcal{Z}(I) = \{Y = 0\}$) a minimal primary decomposition is $I = (X, Y)^2 \cap (Y)$, yielding $\mathcal{Z}(I) = \mathcal{Z}((X, Y)^2) \cup \mathcal{Z}(Y) = \{(0, 0)\} \cup \{(a, 0) \mid a \in K\}$ which is not the decomposition of $V = \mathcal{Z}(I)$ into its irreducible components. Indeed V has only one irreducible component, $\mathcal{Z}(Y)$, while the ideal I has two associated prime, one of which is embedded (the maximal ideal (X, Y)). This is due to the fact that I is not a radical ideal: $Y^2 \in I$ but $Y \notin I$.

2.15.2. Critical Example: L not algebraically closed. — If L is not algebraically closed the result does not hold. Let $L = K = \mathbb{R}$, and $I := ((X^2 - 1)^2 + X^2) \subseteq \mathbb{R}[X, Y]$. It is a

prime ideal of $\mathbb{R}[X,Y]$ because $f(X,Y) := (X^2-1)^2+Y^2$ is an irreducible [11] polynomial in the unique factorization domain $\mathbb{R}[X,Y]$. Being I a prime ideal of $\mathbb{R}[X,Y]$, it coincides with its own minimal primary decomposition, while $\mathcal{Z}(I) = \{(-1,0),(1,0)\} = \mathcal{Z}((X+1,Y)) \cup \mathcal{Z}((X-1,Y))$ has two irreducible components.

2.16. Removing K-algebraic sets

In applications, we can be interested in subsets of $\mathbb{A}^n_L$ which are defined not only by polynomial equations, but rather, by a combination of polynomial equations and polynomial *inequations* (and, over $\mathbb{R}$, also *inequalities*); in other words we are interested in set difference of varieties:

$$\{P \in \mathbb{A}^N_L \mid f_1 = \cdots = f_r = 0 \wedge g_1 \cdots g_s \neq 0\} = \mathcal{Z}(I) \setminus \mathcal{Z}(J) = V \setminus U$$

where $I := (f_1,\ldots,f_r)$, $J := (g_1,\ldots,g_s) \subset K[\underline{X}]$, $V = \mathcal{Z}(I)$ and $U = \mathcal{Z}(J)$.

2.16.1. Remark. — As, for example, $D_f = \mathbb{A}^n_L \setminus \mathcal{Z}(f) = \mathcal{Z}(0) \setminus \mathcal{Z}(f)$ it is clear that this kind of subset, $V \setminus U$, is not a K-algebraic sets of $\mathbb{A}^n_L$ in general (at least set-theoretically), but we can nonetheless consider its *Zariski closure*: $\overline{V \setminus U}^Z = \mathcal{Z}(\mathcal{I}(V \setminus U))$.

Things go smoothly for vanishing ideals, in fact, the following result holds true over any field.

2.16.2. Proposition. — *If V, U are K-algebraic subsets of $\mathbb{A}^n_L$ then $\mathcal{I}(V) : \mathcal{I}(U) = \mathcal{I}(V \setminus U)$.*

Proof. — If $f \in \mathcal{I}(V) : \mathcal{I}(U)$ (that is $f\,\mathcal{I}(U) \subseteq \mathcal{I}(V)$) and $P \in V \setminus U$ (that is $v(P) = 0$ for any $v \in \mathcal{I}(V)$ and there exists $u \in \mathcal{I}(U)$ such that $u(P) \neq 0$), then $(fu)(P) = f(P)u(P) = 0$ because $fu \in \mathcal{I}(V)$, but as $u(P) \neq 0$ it must be $f(P) = 0$. Hence $f \in \mathcal{I}(V \setminus U)$. For the converse: let $f \in \mathcal{I}(V \setminus U)$ and let $u \in \mathcal{I}(U)$, we need to show $fu \in \mathcal{I}(V)$. Consider the obvious decomposition $V = (V \setminus U) \bigcup (V \cap U)$, and let $P \in V$. If $P \in V \setminus U$ then $(fu)(P) = f(P)u(P) = 0$ because $f \in \mathcal{I}(V \setminus U)$, if instead $P \in V \cap U \subseteq U$ then $(fu)(P) = f(P)u(P) = 0$ because $u \in \mathcal{I}(U)$; hence $fu \in \mathcal{I}(V)$. □

11. Indeed, thinking $f(X,Y) \in (\mathbb{R}[X])[Y]$ as a degree two monic polynomial, it should split as $(Y + a(X))(Y + b(X))$ with $a(X), b(X) \in \mathbb{R}[X]$. Expanding out and comparing coefficients of same degree, one get the relations $a(X) + b(X) = 0$ and $a(X)b(X) = (X^2-1)^2$. The last one implies that $a(X)$ and $b(X)$ assume the same sign on each real value, while from the first they must be opposite. Hence we would get $a(X) = b(X) = 0$, which eventually gives a contradiction.

On the other hand, at the level of point sets, things depend on the property of the field extension $K \subseteq L$.

2.16.3. Proposition. — *Let I and J be ideals of $K[\underline{X}]$, then*

a) $\mathcal{Z}(I) \setminus \mathcal{Z}(J) \subseteq \mathcal{Z}((I : J^\infty))$;
b) $\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z \subseteq \mathcal{Z}((I\colon J^\infty))$;
c) if I is a radical ideal then $\mathcal{Z}(I) \setminus \mathcal{Z}(J) \subseteq \mathcal{Z}((I : J))$ and $\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z \subseteq \mathcal{Z}((I\colon J))$.

Proof. — *a)* We actually prove that $\mathcal{Z}(I) \setminus \mathcal{Z}(J) \subseteq \bigcap_{k\in\mathbb{N}_+} \mathcal{Z}((I : J^k)) = \mathcal{Z}((I : J^\infty)) \subseteq \mathcal{Z}(I)$. If $P \in \mathbb{A}^n_L$ is such that $f(P) = 0$ for each $f \in I$ and $g(P) \neq 0$ for some $g \in J$, and if $h \in (I : J^k)$ (i.e. $hJ^k \subseteq I$), as $hg^k \in I$ and $g(P) \neq 0$, we have $0 = (hg^k)(P) = h(P)g(P)^k$ in L then $h(P) = 0$. As this holds true for any $h \in (I : J^k)$ and for any $k \in \mathbb{N}_+$, then $P \in \mathcal{Z}((I : J^\infty))$. The last inclusion follows by the inclusion-reversing property of $\mathcal{Z}$ applied to the $I \subseteq (I : J^\infty)$.
b) It follows from *a)* as $I \subseteq (I\colon J^\infty)$ and $\mathcal{Z}((I\colon J^\infty))$ is Zariski closed.
c) They follow from *a*, *b* and 1.9.7 *c)*, by which $(I\colon J^\infty) = (I : J)$ as I is radical. □

2.16.4. Critical Example: L not algebraically closed. — The inclusion in *b)* of 2.16.3 may be strict. Indeed, taking, as in *2.13.2*, $K = L = \mathbb{R}$, and $I := ((X^2-1)^2+Y^2)$, $J := (X+1)$ ideals in $\mathbb{R}[X, Y]$, in $\mathbb{A}^2_{\mathbb{R}}$ we find: $V = \mathcal{Z}(I) = \{(-1, 0), (1, 0)\}$ and $U = \mathcal{Z}(J) = \{(-1, a) \mid a \in \mathbb{R}\}$, hence $V \setminus U = \{(1, 0)\} = \overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z$. While, being I a prime ideal such that $(X + 1)^t \notin I$ for every $t \in \mathbb{N}$, $(I : J^\infty) = I$, hence $\mathcal{Z}((I : J^\infty)) = V$. This shows that, if L is not algebraically closed, then $\mathcal{Z}((I\colon J^\infty))$ may not be the smallest (Zariski) closed subset containing $\mathcal{Z}(I) \setminus \mathcal{Z}(J)$ (thereby disproving a claim in [**KO13**, Comment to Thm. 2.1]). Again this is a "pathology" of non algebraically closed fields.

2.17. Removing K-algebraic sets: L an algebraically closed field

Everything works smoothly over algebraically fields, thanks to Hilbert Nullstellensatz. A second, more geometric proof (cf. 2.17.2), of the following will be based on the comparison (cf.*2.15*) between minimal primary decomposition and minimal irreducible decomposition over an algebraically closed field.

2.17.1. Proposition. — *If L is algebraically closed, then for any pair of ideals $I, J \subseteq K[\underline{X}]$ we have:*

a) $\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J)) = \sqrt{(I\colon J^\infty)}$;
b) $\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}((I\colon J^\infty))$;
c) if I is a radical ideal then $\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J)) = (I\colon J)$ and $\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}((I\colon J))$.

Proof. — *a)* To show "$\supseteq$", as any vanishing ideal is radical, it's enough to show that we have $(I\colon J^\infty) \subseteq \mathcal{I}(\mathcal{Z}(I)\setminus\mathcal{Z}(J))$, and from *2.16.2* it suffices to show that $f\,\mathcal{I}(\mathcal{Z}(J)) \subseteq \mathcal{I}(\mathcal{Z}(I))$ for each $f \in (I\colon J^\infty)$. So let's assume that $g \in \mathcal{I}(\mathcal{Z}(J))$ and there exists $t \in \mathbb{N}_+$ such that $fJ^t \subseteq I$, we need to show that $fg \in \mathcal{I}(\mathcal{Z}(I))$. By Hilbert's Nullstellensatz $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$, hence there exists $k \in \mathbb{N}_+$ such that $g^k \in J$ and so $fg^{\max\{k,t\}} \in fJ^t \subseteq I \subseteq \mathcal{I}(\mathcal{Z}(I))$ implies $(fg)^{\max\{k,t\}} \in \mathcal{I}(\mathcal{Z}(I))$, but $\mathcal{I}(\mathcal{Z}(I))$ is a radical ideal, therefore $fg \in \mathcal{I}(\mathcal{Z}(I))$; we conclude that $f \in \mathcal{Z}(I) \setminus \mathcal{Z}(J)$. Let's now consider the "$\subseteq$" part. From *2.16.3* we get $\mathcal{Z}(I) \setminus \mathcal{Z}(J) \subseteq \mathcal{Z}(I\colon J^\infty)$, applying $\mathcal{I}$ we thus get $\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J)) \supseteq \mathcal{I}(\mathcal{Z}(I\colon J^\infty)) = \sqrt{(I\colon J^\infty)}$, where the last equality is, again, Hilbert's Nullstellensatz.
b) By *2.12.3* and part *a)* above, we have:

$$\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J))) = \mathcal{Z}(\sqrt{(I\colon J^\infty)}) = \mathcal{Z}((I\colon J^\infty))$$

c) As I is radical, from 1.9.7 *c)* we get $(I\colon J^\infty) = (I : J)$ and $(I : J)$ itself is a radical ideal, hence by *a)* we conclude $\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J)) = \sqrt{(I : J^\infty)} = \sqrt{(I : J)} = (I : J)$. Then, *2.12.3* and the previous identity yield $\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J))) = \mathcal{Z}((I\colon J))$. □

2.17.2. A second proof of *b)***.** — We now give an other proof of 2.17.1 *b)* exploiting primary decomposition. Notice that, once *b)* is established, then *a)* follows just by taking the vanishing ideals and applying the Nullstellensatz, together with the already mentioned trivial fact that $\mathcal{I}(\overline{S}^Z) = \mathcal{I}(S)$.

Proof. — From 2.15, we have $I = Q_1 \cap \cdots \cap Q_r$ (minimal primary decomposition of I with Q_i $\mathfrak{p}_i$-primary ideals) and $V = \mathcal{Z}_K^L(I) = V_1 \cup \cdots \cup V_r$ (minimal irreducible decomposition of V) with $V_i = \mathcal{Z}(Q_i)$ and $\mathcal{I}(V_i) = \sqrt{Q_i} = \mathfrak{p}_\mathfrak{i}$ for every $i = 1, \cdots, r$. Then we find (as the union is finite)

$$\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \overline{\bigcup_{i=r} V_i \setminus \mathcal{Z}(J)}^Z = \bigcup_{i=r} \overline{V_i \setminus \mathcal{Z}(J)}^Z = \bigcup_{i=r} \overline{\mathcal{Z}(Q_i) \setminus \mathcal{Z}(J)}^Z.$$

Hence we start by considering the case $I = Q$ is a $\mathfrak{p}$-primary ideal and $V = \mathcal{Z}(Q)$ is irreducible (we have, by Nullestellensatz $\mathcal{I}(V) = \sqrt{Q} = \mathfrak{p}$). Now $V \setminus \mathcal{Z}(J)$ is a Zariski open subset of V.

But V is irreducible, hence $\overline{V \setminus \mathcal{Z}(J)}^Z = V$ as soon as $V \setminus \mathcal{Z}(J) \neq \emptyset$, which is equivalent to $V \not\subseteq \mathcal{Z}(J)$. Hence

$$\overline{V \setminus \mathcal{Z}(J)}^Z = \begin{cases} \emptyset & \Leftrightarrow \quad V \subseteq \mathcal{Z}(J) \\ V & \Leftrightarrow \quad V \not\subseteq \mathcal{Z}(J) \end{cases}$$

But, by the Nullstellensatz, $\mathcal{Z}(Q) \subseteq \mathcal{Z}(J) \Leftrightarrow \mathcal{I}(\mathcal{Z}(Q)) \supseteq \mathcal{I}(\mathcal{Z}(J)) \Leftrightarrow \mathfrak{p} = \sqrt{Q} \supseteq \sqrt{J} \Leftrightarrow \mathfrak{p} \supseteq J$. Hence, by 1.10.6, $(Q\colon J^\infty) = (1)$, and thus $\overline{V \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}((Q\colon J^\infty))$ if $V \subseteq \mathcal{Z}(J)$. If instead, $\overline{V \setminus \mathcal{Z}(J)}^Z = V$, then $V \not\subseteq \mathcal{Z}(J)$. Again, by the Nullstellensatz, $\mathcal{I}(V) = \mathfrak{p} \not\supseteq \sqrt{J}$, and therefore $\mathfrak{p} \not\supseteq J$. Thus, again by 1.10.6, $(Q\colon J^\infty) = Q$, and therefore $\overline{V \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}((Q\colon J^\infty))$ if $V \not\subseteq \mathcal{Z}(J)$. Now, returning to the general case, we can split the previous decomposition as

$$\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \bigcup_{\{i|V_i \subseteq \mathcal{Z}(J)\}} \overline{\mathcal{Z}(Q_i) \setminus \mathcal{Z}(J)}^Z \cup \bigcup_{\{i|V_i \not\subseteq \mathcal{Z}(J)\}} \overline{\mathcal{Z}(Q_i) \setminus \mathcal{Z}(J)}^Z = \bigcup_{\{i|V_i \not\subseteq \mathcal{Z}(J)\}} V_i.$$

On the other hand

$$\begin{aligned} \mathcal{Z}((\bigcap_{i=1}^r Q_i : J^\infty)) = \mathcal{Z}(\bigcap_{i=1}^r (Q_i : J^\infty)) &= \bigcup_{i=1}^r \mathcal{Z}((Q_i : J^\infty)) \\ &= \bigcup_{\{i|\mathfrak{p}_i \supseteq J\}} \mathcal{Z}((Q_i : J^\infty)) \cup \bigcup_{\{i|\mathfrak{p}_i \not\supseteq J\}} \mathcal{Z}((Q_i : J^\infty)) \\ &= \bigcup_{\{i|\mathfrak{p}_i \not\supseteq J\}} \mathcal{Z}(Q_i). \end{aligned}$$

As, by Nullstellensatz, $V_i \not\subseteq \mathcal{Z}(J) \Leftrightarrow \mathfrak{p}_i \not\supseteq J$, and $\mathcal{Z}(Q_i) = V_i$ for each $i = 1, \cdots, r$, the argument is complete. □

2.17.3. Remark: geometric interpretation of the second proof. — This argument clearly shows that, over an algebraically closed field, the closure of the set difference $V \setminus U$, of two K-algebraic sets V and U, is the union of those irreducible component of V which are not completely contained in U.

2.17.4. Critical Example: L not algebraically closed. — The following example shows that the hypothesis on L is essential, the result in 2.17.1 is, in general, false over non algebraically closed fields. To deal with that case we need a deeper understanding of the composite $\mathcal{I} \circ \mathcal{Z}$ (see 2.18). As in Example *2.13.2*, let $L = K = \mathbb{R}$, $I := (X^2(X-1)^2 + Y^2)$ (prime) ideal of $\mathbb{R}[X, Y]$ and $J := (X - 1)$. The real loci in $\mathbb{A}^2_{\mathbb{R}}$ are $V = \mathcal{Z}^{\mathbb{R}}(I) = \{(0,0), (1,0))\}$, two points, and $U := \mathcal{Z}^{\mathbb{R}}(J) = \{X = 1\}$, a line. Clearly $V \setminus U = \{(0,0)\}$ (Zariski closed), hence $\mathcal{I}^{\mathbb{R}}(\overline{V \setminus U}^Z) = \mathcal{I}^{\mathbb{R}}((0,0)) = (X, Y)$. Let's compute $\sqrt{(I\colon J^\infty)}$ and compare the result with

$\mathcal{I}^{\mathbb{R}}(\overline{V \setminus U}^{Z})$. Note that, as I is prime we have the following two facts: *i*) it is a radical ideal, hence $(I\colon J^{\infty}) = (I\colon J)$ is a radical ideal (see 1.9.7 *c*)) and moreover *ii*) $(I\colon J) = I$ whenever $J \not\subseteq I$ (see 1.7.4 *h*)). As $X - 1 \notin (X^2(X-1)^2 + Y^2)$ we get $\sqrt{(I\colon J^{\infty})} = (I\colon J) = I$, but then $\sqrt{(I\colon J^{\infty})} = I \subsetneq \mathcal{I}^{\mathbb{R}}(\mathcal{Z}^{\mathbb{R}}(I) \setminus \mathcal{Z}^{\mathbb{R}}(J)) = (X, Y)$, contrary to what expected from 2.17.1 *a*). Let's check what happens over $\mathbb{C}$:

$$V^{\mathbb{C}} := \mathcal{Z}^{\mathbb{C}}(I) = \mathcal{Z}^{\mathbb{C}}((X(X-1)+iY)(X(X-1)-iY)) = \mathcal{Z}^{\mathbb{C}}(Y-iX(X-1)) \cup \mathcal{Z}^{\mathbb{C}}(Y+iX(X-1))),$$

decomposes as a union of two (infinite complex) curves meeting in the two real points $\{(0,0), (1,0)\}$, and $U^{\mathbb{C}} := \mathcal{Z}^{\mathbb{C}}(J) = \{X - 1 = 0\} = \{(1, z) \mid z \in \mathbb{C}\}$ is a (complex) line. Clearly, again, $V^{\mathbb{C}} \cap U^{\mathbb{C}} = \{(1,0)\}$, but now $V^{\mathbb{C}} \setminus U^{\mathbb{C}} = V^{\mathbb{C}} \setminus \{(1,0)\}$ is an infinite set which is not even a Zariski closed one. Though, it is clear that $\overline{V^{\mathbb{C}} \setminus U^{\mathbb{C}}}^{Z} = \overline{V^{\mathbb{C}} \setminus \{(1,0)\}}^{Z} = V^{\mathbb{C}}$, which is now coherent with 2.17.1 *a*) and the previous colon computation $\sqrt{(I\colon J^{\infty})} = I$. Indeed

$$\mathcal{I}^{\mathbb{C}}(\overline{V^{\mathbb{C}} \setminus U^{\mathbb{C}}}^{Z}) = \mathcal{I}^{\mathbb{C}}(V^{\mathbb{C}}) = \mathcal{I}^{\mathbb{C}}(\mathcal{Z}^{\mathbb{C}}(I)) = \sqrt{I} = I \quad \text{(as } I \text{ is prime, for last equality).}$$

2.18. Real Nullstellensatz

2.18.1. Proposition. — *Let L be a real field and I an ideal of $K[\underline{X}]$, then*

a) $\mathcal{I}_K^L(\mathcal{Z}_K^L(I))$ *is a real ideal and* $\sqrt[R]{I} \subseteq \mathcal{I}_K^L(\mathcal{Z}_K^L(I))$*;*
b) $\mathcal{Z}_K^L(\sqrt[R]{I}) = \mathcal{Z}_K^L(I)$.

Proof. — *a*) If $f_1^2 + \cdots + f_r^2 \in \mathcal{I}(\mathcal{Z}(I))$ with $f_i \in K[\underline{X}]$, then $f_1^2(P) + \cdots + f_r^2(P) = 0$ for all $P \in \mathcal{Z}(I)$. As L is a real field, it must be $f_i(P) = 0$ for all $i = 1, \cdots, r$, and for all $P \in \mathcal{Z}(I)$. This means $f_i \in \mathcal{I}(\mathcal{Z}(I))$ for all $i = 1, \cdots, r$. Since $I \subseteq \mathcal{I}_K^L(\mathcal{Z}_K^L(I))$ then $\sqrt[R]{I} \subseteq \mathcal{I}_K^L(\mathcal{Z}_K^L(I))$.
b) As $I \subseteq \sqrt[R]{I}$, it is $\mathcal{Z}_K^L(\sqrt[R]{I}) \subseteq \mathcal{Z}_K^L(I)$. On the other hand, let $P \in \mathcal{Z}_K^L(I)$ and $f \in \sqrt[R]{I}$. Since $f^{2m} + \sigma \in I$ for some $m \in \mathbb{N}$ and $\sigma \in \sum K[\underline{X}]^{(2)}$, then $f^{2m}(P) + \sigma(P) = 0$. As $f^{2m}(P)$ is a square and $\sigma(P)$ is a sum of squares, each summand of $f^{2m}(P) + \sigma(P)$ has to be zero, hence $f^{2m}(P) = 0$ and thus $f(P) = 0$. This shows that $\mathcal{Z}_K^L(\sqrt[R]{I}) \supseteq \mathcal{Z}_K^L(I)$ also, and therefore one concludes $\mathcal{Z}_K^L(\sqrt[R]{I}) = \mathcal{Z}_K^L(I)$. □

The references for the following are [**Kri64**], [**Dub70**], [**Ris70**], [**Lam84**, Thm. 6.7], [**BCR98**, Cor. 4.1.8].

2.18.2. Theorem (Real Nullstellensatz (Krivine-Dubois-Risler)). — *Let L be a real field, the following facts are equivalent:*

a) The field L is a real-closed.

b) For every $n \in \mathbb{N}_+$ the only real maximal ideals of $L[X_1, \dots, X_n]$ are those corresponding to L-rational points of $\mathbb{A}^n_L$, i.e. the map $\mathbb{A}^n_L \longrightarrow \{$real maximal ideals of $L[X_1, \dots, X_n]\}$

$$P = (a_1, \dots, a_n) \mapsto (X_1 - a_1, \dots, X_n - a_n) = \mathcal{I}^L_L(P)$$

is bijective.

c) For every $n \in \mathbb{N}_+$ and every subfield K of L, if I is an ideal of $K[X_1, \dots, X_n]$ then $\mathcal{Z}^L_K(I) = \emptyset$ if and only if $(1 + \sum K_{\geq 0} \cdot K[\underline{X}]^{(2)}) \cap I \neq \emptyset$, that is there are $h_1, \dots, h_t \in K[\underline{X}]$ and non-negative elements $\mu_1 \dots, \mu_t \in K_{\geq 0}$ such that $1 + \mu_1 h_1^2 + \cdots + \mu_t h_t^2 \in I$.

d) For every $n \in \mathbb{N}_+$ and every subfield K of L, if $J = (f_1, \dots, f_r)$ is any ideal of $K[X_1, \dots, X_n]$, then

$$f \in \mathcal{I}^L_K(\mathcal{Z}^L_K(J)) \quad \Leftrightarrow \quad f^{2N} + \sum_{j=1}^{t} \mu_j \widetilde{h_j}(X_1, \dots, X_n)^2 = \sum_{i=1}^{r} \widetilde{g_i}(X_1, \dots, X_n) f_i,$$

for suitable $\widetilde{h_j}, \widetilde{g_i} \in K[X_1, \dots, X_n]$ and non-negative elements $\mu_1 \dots, \mu_t \in K_{\geq 0}$.

In particular, if $K = L$ is a real-closed field then $\mathcal{I}^L_L(\mathcal{Z}^L_L(J)) = \sqrt[R]{J}$.

e) For every $n \in \mathbb{N}_+$ the assignment

$$\mathcal{I}^L_L \colon \{K\text{-algebraic sets of } \mathbb{A}^n_L\} \longrightarrow \{\text{real ideals of } L[X_1, \dots, X_n]\},\ V \mapsto \mathcal{I}^L_L(V)$$

defines a bijection of the set of all L-algebraic sets $V \subseteq \mathbb{A}^n_L$ onto the set of all ideals I of $L[X_1, \dots, X_n]$ such that $I = \sqrt[R]{I}$, with inverse the map

$$\mathcal{Z}^L_L \colon \{\text{real ideals of } L[X_1, \dots, X_n]\} \longrightarrow \{L\text{-algebraic sets of } \mathbb{A}^n_L\},\ I \mapsto \mathcal{Z}^L_L(I);$$

in this bijection irreducible algebraic sets correspond to real prime ideals, and vice-versa.

Proof. — The proof will follow the line of the classical Hilbert Nullstellensatz as close as possible, but the real case has some specific subtleties that need to be taken into account, therefore we will give full details at each step.

a) $\Rightarrow$ b) The map $P = (a_1, \dots, a_n) \in \mathbb{A}^n_L \mapsto \mathfrak{m}_P := (X_1 - a_1, \dots, X_n - a_n)$ is well defined because $\mathfrak{m}_P$ is a real maximal ideal of $L[X_1, \dots, X_n]$, indeed the factor ring $L[\underline{X}]/\mathfrak{m}_P \cong L$ is a real field, and we showed in 2.10.2 that $\mathfrak{m}_P = \mathcal{I}^L_L(P)$ for any L-rational point of $\mathbb{A}^n_L$. Moreover, the map is clearly injective. We need to show that it is also surjective, *i.e.* that for every real maximal

ideal $\mathfrak{m}$ of $L[X_1,\dots,X_n]$ there exists a L-rational point $P \in \mathbb{A}^n_L$ such that $\mathfrak{m} = \mathcal{I}(P)$. As $\mathfrak{m}$ is maximal, from the field theoretic version of the Nullstellensatz, 2.10.3, it follows that for each $i = 1,\dots,n$ the contracted ideal $\mathfrak{m} \cap L[X_i]$ is nonzero. As $L[X_i]$ is a Euclidean domain, by 1.4.4 and 1.5.21, the contraction is then a maximal ideal of $L[X_i]$ and by 1.14.1 f) it is also a real ideal, therefore $\mathfrak{m} \cap L[X_i] = (X_i - a_i)$ for some $a_i \in L$ as L is a real-closed field (cf. 1.14.7). Therefore $\mathfrak{m}$ contains $(X_1 - a_1,\dots,X_n - a_n)$, as the latter is itself a maximal ideal we get $\mathfrak{m} = (X_1 - a_1,\dots,X_n - a_n)$ as required.

b) $\Rightarrow$ *a*) By definition 1.13.25, we need to show that if L' is any *real* algebraic extension of L then $L' = L$. Let $\alpha \in L'$ then we have the composite of real algebraic field extensions $L \subseteq L(\alpha) \subseteq L'$. Thus $L(\alpha) \cong L[X]/\operatorname{Ker}(\mathrm{ev}_\alpha)$, as $L(\alpha)$ is a real field we have that $\operatorname{Ker}(\mathrm{ev}_\alpha) = \mathcal{I}_L(\alpha)$ is a maximal ideal of $L[X]$ which is also a real ideal. Hence, by *b*), there exists $a \in L$ such that $\operatorname{Ker}(\mathrm{ev}_\alpha) = (X - a)$. But then $L(\alpha) \cong L[X]/\operatorname{Ker}(\mathrm{ev}_\alpha) \cong L$, and being $L(\alpha)$ a finite dimensional vector space on L, it must be $L = L(\alpha)$, that is $\alpha = a \in L$. Therefore $L' = L$ and L is real-closed.

a) $\Rightarrow$ *c*) Let us fix $n \in \mathbb{N}_+$, a subfield K of L and an ideal $I \subseteq K[\underline{X}]$. Assume that I is not disjoint from the (multiplicative) set $S_K := 1 + \sum K_{\geq 0} \cdot K[\underline{X}]^{(2)}$, hence there are polynomials $h_j \in K[\underline{X}]$ and non-negative coefficients $\mu_j \in K_{\geq 0}$ (for $j = 1,\dots,t$) such that $1 + \sum \mu_j h_j^2 \in I$. We contend that then $\mathcal{Z}^L(I) = \emptyset$, else there is a $P \in \mathcal{Z}^L(I)$ and then $1 + \sum \mu_j h_j^2(P) = 0$ in the real field L, a contradiction. The converse is proved in [**Kri64**, Applications. I. Théorème, p. 311] making use also of Tarski's Theorem ([**Tar48**], [**Col75**], [**Col98**], [**Rob63**]).

c) $\Rightarrow$ *d*) We argue as is the already quoted [**KR00**, Thm. 2.6.12] with suitable modifications. Let $J = (f_1,\dots,f_r)$ be an ideal of $K[X_1,\dots,X_n]$. The necessity part follows easily as L is real. Let then $f \in \mathcal{I}(\mathcal{Z}^L(J))$. If $f = 0$ the claim is trivial, hence assume $f \neq 0$ and consider the new ideal

$$\begin{aligned} J' :&= JK[X_1,\dots,X_n,X_{n+1}] + (X_{n+1}f - 1) \\ &= (f_1(X_1,\dots,X_n),\dots,f_r(X_1,\dots,X_n),X_{n+1}f(X_1,\dots,X_n) - 1) \end{aligned}$$

in the polynomial ring $K[X_1,\dots,X_n,X_{n+1}]$. We claim that $\mathcal{Z}^L(J') = \emptyset$. By contradiction, let $P' = (P, a_{n+1}) \in \mathcal{Z}^L(J')$, with $P \in \mathbb{A}^n_L$ and $a_{n+1} \in L$, then

$$f_i(P) = 0 \text{ for every } i = 1,\dots,r \text{ and } a_{n+1}f(P) = 1.$$

Hence $P \in \mathcal{Z}^L(J)$ and $f(P) \neq 0$, which contradicts $f \in \mathcal{I}(\mathcal{Z}^L(J))$. Therefore $\mathcal{Z}^L(J') = \emptyset$ as claimed, and by *c*) there must be $h_1,\dots,h_t \in K[X_1,\dots,X_{n+1}]$, non-negative elements

$\mu_1 \ldots, \mu_t \in K_{\geq 0}$ and polynomials $g_1, \ldots, g_{r+1} \in K[X_1, \ldots, X_{n+1}]$ such that

$$1 + \sum_{j=1}^{t} \mu_j h_j(X_1, \ldots, X_{n+1})^2 = \sum_{i=1}^{r} g_i(X_1, \ldots, X_{n+1}) f_i + g_{r+1}(X_1, \ldots, X_{n+1})(X_{n+1} f - 1).$$

This relation holds also in the field $K(X_1, \ldots, X_{n+1})$, where it can be evaluated under the substitution $X_{n+1} \mapsto \frac{1}{f}$, yielding

$$1 + \sum_{j=1}^{t} \mu_j h_j \left(X_1, \ldots, X_n, \frac{1}{f} \right)^2 = \sum_{i=1}^{r} g_i \left(X_1, \ldots, X_n, \frac{1}{f} \right) f_i.$$

If $u_j \in \mathbb{N}$, respectively $v_i \in \mathbb{N}$, is the degree of h_j, respectively g_i, with respect to X_{n+1}, and $N := \sum_{j=1}^{t} u_j + \sum_{i=1}^{r} v_i$, then multiplying both sides by f^{2N} we get an identity

$$f^{2N} + \sum_{j=1}^{t} \mu_j \widetilde{h_j}(X_1, \ldots, X_n)^2 = \sum_{i=1}^{r} \widetilde{g_i}(X_1, \ldots, X_n) f_i,$$

with suitable $\widetilde{h_j}, \widetilde{g_i} \in K[X_1, \ldots, X_n]$.

In particular, if $K = L$ is real-closed, then each μ_j is a square in L and hence $f \in \sqrt[K]{J}$.

d) $\Rightarrow$ *e)* In the given situation, by 2.12.3 we have $\mathcal{Z} \circ \mathcal{I} = \mathrm{Id}$ on K-algebraic subsets. Thanks to *d)*, if I is a real ideal of $K[X_1, \ldots, X_n]$ we get also $\mathcal{I} \circ \mathcal{Z}(I) = \sqrt[R]{I} = I$, that is $\mathcal{I} \circ \mathcal{Z} = \mathrm{Id}$ on real ideals. Hence the two maps are reciprocal inverse.

e) $\Rightarrow$ *a)* To show that L is real-closed we will check that it fulfills the conditions of 1.13.28 *v)*.

Let $f \in L[X]$ be an odd degree polynomial, then f has a zero α in a real-closed extension L' of L by 1.13.28. Assume, by contradiction, that $\mathcal{Z}^L(f) = \emptyset$. Then $1 \in \mathcal{I}(\mathcal{Z}^L(f)) = \sqrt[R]{(f)}$ by *e)*. Hence we have an equation $1 + \sum h_i(X)^2 = f(X)g(X)$ with $h_i, g \in L[X]$ which yields $1 + \sum h_i(\alpha)^2 = 0$ in the real field L', which is an absurd.

Let $a \in L \setminus \{0\}$ and assume $\mathcal{Z}^L(X^2 - a) = \emptyset$ and $\mathcal{Z}^L(X^2 + a) = \emptyset$, then $X^2 - a$, $X^2 + a$ are both irreducible in $L[X]$ and by *e)* we have $1 \in \mathcal{I}(\mathcal{Z}^L(X^2 - a)) = \sqrt[R]{(X^2 - a)}$ and $1 \in \mathcal{I}(\mathcal{Z}^L(X^2 + a)) = \sqrt[R]{(X^2 + a)}$. As L is a real field, by 1.13.24 *a)*, for every $a \in L \setminus \{0\}$ we have that at least one of the field extensions $L(\sqrt{a}) \cong L[X]/(X^2 - a)$ or $L(\sqrt{-a}) \cong L[X]/(X^2 - a)$ is real, that is at least one of the ideals $(X^2 - a)$ or $(X^2 + a)$ of $L[X]$ is a real ideal, which in turns is equivalent to $\sqrt[R]{(X^2 - a)} = (X^2 - a)$ or $\sqrt[R]{(X^2 + a)} = (X^2 + a)$. Therefore, for every $a \in L$ it can't be $1 \in \sqrt[R]{(X^2 - a)}$ and $1 \in \sqrt[R]{(X^2 + a)}$, that is a is a square in L or $-a$ is a square in L. Moreover, they can't be both squares: indeed if $a = b^2$ and $-a = c^2$ with $b, c \in L$, then $0 = b^2 + c^2$ in L. As L is real, $b = c = 0$ and then $a = 0$. Therefore, for every $a \in L \setminus \{0\}$ exactly one of a, $-a$ is a square in L. □

2.18.3. Remark. — If L is real closed, then every non-negative element of L is a square, *i.e.* $L_{\geq 0} = L^{(2)}$. Hence $S_L = 1 + \sum L_{\geq 0} \cdot L[\underline{X}]^{(2)} = 1 + \sum L[\underline{X}]^{(2)}$ and so, taking $K = L$, condition c) above simplifies as follows:
For every $n \in \mathbb{N}_+$ and every ideal I of $L[X_1, \ldots, X_n]$ then

$$\mathcal{Z}_K^L(I) = \emptyset \quad \Leftrightarrow \quad (1 + \sum L[\underline{X}]^{(2)}) \cap I \neq \emptyset,$$

that is there are $h_1, \ldots, h_t \in L[\underline{X}]$ such that $1 + h_1^2 + \cdots + h_1^2 \in I$.
If K is not real closed the reference to $K_{\geq 0}$ cannot be omitted.

2.18.4. Example. — (a) Let $I := (X^2 + 1) \in \mathbb{R}[X]$, then $\sqrt[R]{I} = \mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(\emptyset) = \mathbb{R}[X]$ (cf. *1.13.32*).
(b) Let $I := ((X^2-1)^2+Y^2) \in \mathbb{R}[X, Y]$, then $\sqrt[R]{I} = \mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(\{(-1, 0), (1, 0)\}) = (X^2-1, Y)$, which, by the way, shows that $(X^2 - 1, Y)$ is a real ideal (cf. *2.13.2*).

2.18.5. Theorem. — *Let L be a real-closed field. Let I be an ideal of $L[X_1, \ldots, X_n]$, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be its minimal primes. The ideal I is real if and only if I is radical and each $\mathcal{Z}^L(\mathfrak{p}_i)$ has a nonsingular point.*

Proof. — See [**Lam84**, Thm. 6.10] □

2.18.6. Proposition. — *Let L be a real-closed field, K a subfield of L and $f \in K[X_1, \ldots, X_n]$ an irreducible polynomial. Then the following properties are equivalent:*

i) *The principal ideal (f) is real;*
ii) $(f) = \mathcal{I}_K^L(\mathcal{Z}_K^L(f))$;
iii) *The polynomial f has a nonsingular zero in L^n (i.e. there is a $P \in \mathbb{A}_L^n$ such that $f(P) = 0$ but $\frac{\partial f}{\partial X_i}(P) \neq 0$ for some i);*
iv) *The sign of f changes on L^n (i.e. there are $P, Q \in \mathbb{A}_L^n$ such that $f(P)f(Q) < 0$);*
v) $\dim(\mathcal{Z}(f)) = n - 1$.

Proof. — See [**BCR98**, Theorem 4.5.1]. □

2.18.7. Corollary. — *Let L be a real-closed field and $f \in K[X_1, \ldots, X_n]$ be any non-constant polynomial. Then the following properties are equivalent:*

i) *The principal ideal (f) is real;*
ii) $(f) = \mathcal{I}_K^L(\mathcal{Z}_K^L(f))$;
iii) *f is a square-free product of irreducible indefinite (over K) polynomials.*

Proof. — See [**Lam84**, Thm. 6.11], where *f indefinite* is used to mean that it changes sign on K^n. The so called "Changing sign criterion", *i.e.* the equivalence *i)* $\Leftrightarrow$ *iii)*, is a result of Dubois and Efroymson (cf. [**DE70**]). □

2.18.8. Critical Example: f irreducible but not indefinite. — We already saw that $f = Y^2 + (X-a)^2(X-b)^2$, with $a, b \in \mathbb{R}$, although being irreducible, does not generate a real ideal. This is coherent with the previous result, as f clearly violates 2.18.6 *iv)* (and it's not difficult to directly check that, of course, it violates 2.18.6 *iii)* too). It is also straightforward to verify that $\sqrt[R]{(f)} = (Y, (X-a)(X-b))$ if $a \neq b$ and $\sqrt[R]{(f)} = (Y, X-a)$ if $a = b$ (indeed: in the first case $\mathbb{R}[X,Y]/(Y,(X-a)(X-b)) \cong \mathbb{R} \times \mathbb{R}$ is a real ring, as well as in the second case $\mathbb{R}[X,Y]/(Y,(X-a)) \cong \mathbb{R}$).

2.18.9. Critical Example: f indefinite but not irreducible. — We also note that the hypothesis "f irreducible" is a necessary one. To find an example of reducible f satisfying 2.18.6 *iii)*, *iv)* we could start from a product $f = f_1 f_2$ with, at least f_1 not proportional to f_2, and even better $\gcd(f_1, f_2) = 1$, and not both of degree one and/or such that (f_1) and (f_2) are real (in which case we would have: $K[\underline{X}]/(f) \hookrightarrow K[\underline{X}]/(f_1) \times K[\underline{X}]/(f_2)$ real ring). Note that, then, $X^2 - Y^2 = (X+Y)(X-Y)$ cannot do the job. Hence, the easiest first candidate appears to be the reducible polynomial $f = X^3 - Y^3 = (X-Y)(X^2+XY+Y^2) \in \mathbb{R}[X,Y]$. But for the irreducibility request, it satisfies 2.18.6 *iii*, *iv)* and *v)*. We will give two proofs that its real radical is bigger than (f), one is very quick but does not show directly a sum of squares in (f) whose summands' bases do not belong to (f), while the second does exactly that.

Proof. — Since $(X^3 - Y^3) = (X-Y)(X^2+XY+Y^2)$, as ideals of $\mathbb{R}[X,Y]$, from 1.14.4 *h)* we get: $\sqrt[R]{(X^3-Y^3)} = \sqrt[R]{(X-Y)} \cap \sqrt[R]{(X^2+XY+Y^2)} = (X-Y) \cap (X,Y) = (X-Y)$. □

Proof. — To have a chance to find a sum of squares in (f) we have, at least, to find $g \in \mathbb{R}[X,Y]$ such that the product fg has constant non negative sign, hence we can take $g = (X-Y)h$ with

h a sum squares in $\mathbb{R}[X,Y]$. Let's start with the obvious candidate $g = X - Y$ [12]:

$$\begin{aligned}
(X^3-Y^3)(X-Y) &= \underline{X^4+Y^4} - XY^3 - X^3Y \\
&= \underline{(X-Y)^4 + 4X^3Y - 6X^2Y^2 + 4XY^3} - XY^3 - X^3Y \\
&= (X-Y)^4 + 3(\boxed{X^3Y - 2X^2Y^2 + XY^3}) \\
&= (X-Y)^4 + 3(X^3Y + \underline{X^4 - 2X^2Y^2 + Y^4} + XY^3 \underline{-X^4 - Y^4}) \\
&= (X-Y)^4 + 3[\underline{(X^2-Y^2)^2} + X^3Y + XY^3 \underline{-(X-Y)^4 - 4X^3Y + 6X^2Y^2 - 4XY^3}] \\
&= (X-Y)^4 + 3[(X^2-Y^2)^2 - (X-Y)^4 - 3(\boxed{X^3Y - 2X^2Y^2 + XY^3})],
\end{aligned}$$

and we notice that

$$\begin{aligned}
& X^3Y - 2X^2Y^2 + XY^3 = (X^2-Y^2)^2 - (X-Y)^4 - 3(X^3Y - 2X^2Y^2 + XY^3) \\
\Rightarrow\quad & X^3Y - 2X^2Y^2 + XY^3 = \frac{1}{4}[(X^2-Y^2)^2 - (X-Y)^4].
\end{aligned}$$

Hence

$$\begin{aligned}
(X^3-Y^3)(X-Y) &= -2(X-Y)^4 + 3(X^2-Y^2)^2 - \frac{9}{4}[(X^2-Y^2)^2 - (X-Y)^4]] \\
&= \frac{1}{4}(X-Y)^4 + \frac{3}{4}(X^2-Y^2)^2 = \left(\frac{1}{2}(X-Y)^2\right)^2 + \left(\frac{\sqrt{3}}{2}(X^2-Y^2)\right)^2,
\end{aligned}$$

that is $(f) \ni [(X-Y)^2]^2 + [\sqrt{3}(X^2-Y^2)]^2 = 4(X-Y)(X^3-Y^3)$ a sum of squares in (f) whose summands do not have bases belonging to (f). Therefore (f) is not a real ideal, despite f clearly satisfies 2.18.6 *iii*), *iv*) . Moreover, being that $\sqrt[R]{(f)}$ is a real ideal containing (f), it clearly must be $X-Y \in \sqrt[R]{(f)}$. But $(X-Y)$ is a real ideal and $f \in (X-Y)$, hence $\sqrt[R]{(X^3-Y^3)} = (X-Y)$. □

2.19. Irreducible components over a real-closed field

If L is real-closed, and I is a real ideal, the two decompositions mentioned in *2.8.2* and *2.8.3* do coincide. That is, if $I = Q_1 \cap \cdots \cap Q_r$ is a minimal primary decomposition of I with Q_i $\mathfrak{p}_i$-primary ideals and $V = \mathcal{Z}_K^L(I) = V_1 \cup \cdots \cup V_s$ is the decomposition of V into irreducible components V_i, then $r = s$ and (up to reordering) $\mathcal{Z}_K^L(\mathfrak{p}_i) = V_i$ for $i = 1, \cdots, r$ (note moreover

12. Note that f and g are not, separately, symmetric functions of X, Y, but their product is.

that, as I is a real ideal, then each minimal prime $\mathfrak{p}_i = \sqrt{Q_i}$ is now a real prime ideal (cf. 1.12.6 i)). Indeed, starting from $I = Q_1 \cap \cdots \cap Q_r$ and taking its zeros we get

$$V = \mathcal{Z}_K^L(Q_1) \cup \cdots \cup \mathcal{Z}_K^L(Q_r) = \mathcal{Z}_K^L(\mathfrak{p}_1) \cup \cdots \cup \mathcal{Z}_K^L(\mathfrak{p}_r) = V_1 \cup \cdots \cup V_r$$

where, now, all the $V_i = \mathcal{Z}_K^L(\mathfrak{p}_i)$ are irreducible because, thanks to 1.12.6 i) and the Real Nullstellensatz, their vanishing ideals are (real) primes: $\mathcal{I}_K^L(V_i) = \mathcal{I}_K^L(\mathcal{Z}_K^L(\mathfrak{p}_i)) = \sqrt[R]{\mathfrak{p}_i} = \mathfrak{p}_i$. As we started from a minimal primary decomposition we don't have repetitions of V_i and as I is a real ideal (hence also radical) there are no embedded primes, therefore the irreducible V_i are maximal, and hence they are the irreducible components of $V = \mathcal{Z}_K^L(I)$.

2.19.1. Critical Example: I not real. — The two examples given before (cf. 2.15.1 and 2.15.2) show the necessity of the hypothesis also over a real-closed field. Let $L = K = \mathbb{R}$. For $I := (XY, Y^2) \subseteq \mathbb{R}[X, Y]$ (as in 2.15.1) a minimal primary decomposition is $I = (X, Y)^2 \cap (Y)$, yielding $\mathcal{Z}(I) = \mathcal{Z}((X, Y)^2) \cup \mathcal{Z}(Y) = \{(0, 0)\} \cup \{(a, 0) \mid a \in K\}$ which is not the decomposition of $V = \mathcal{Z}(I)$ into its irreducible components. Indeed V has only one irreducible component, $\mathcal{Z}(Y)$, while the ideal I has two associated prime, one of which is embedded (the maximal ideal (X, Y)). This is due to the fact that I is not a real ideal since it is not even a radical ideal: $Y^2 \in I$ but $Y \notin I$. The ideal $I = \mathfrak{p} := ((X^2 - 1)^2 + X^2) \subseteq \mathbb{R}[X, Y]$ (as in 2.15.2) is a prime ideal of $\mathbb{R}[X, Y]$, hence radical at least, but not a real one (as already seen $f(X, Y) = (X^2 - 1)^2 + X^2$ is irreducible, but clearly $\sqrt[R]{(f)} = (X, (X + 1)(X - 1)) \supsetneq (f)$). Being $\mathfrak{p} = (f)$ a prime ideal of $\mathbb{R}[X, Y]$, it coincides with its own minimal primary decomposition, while $\mathcal{Z}(\mathfrak{p}) = \{(-1, 0), (1, 0)\} = \mathcal{Z}((X + 1, Y)) \cup \mathcal{Z}((X - 1, Y))$ has two irreducible components.

2.20. Removing K-algebraic sets: L a real-closed field

Let's now state and prove a real analogous of 2.17.1, which is suitable to deal with the case $L = K = \mathbb{R}$.

2.20.1. Proposition. — *If L is a real-closed field, then for any pair of ideals $I, J \subseteq K[\underline{X}]$ we have:*

a) $\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J)) = \sqrt[R]{(I \colon J^\infty)}$;
b) $\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}((I \colon J^\infty))$;
c) if I is a real ideal then $\mathcal{I}(\mathcal{Z}(I) \setminus \mathcal{Z}(J)) = (I \colon J)$ *and* $\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z = \mathcal{Z}((I \colon J))$.

Proof. — *a*) Let's consider the "$\subseteq$" part. From *2.16.3* we get $\mathcal{Z}(I)\setminus\mathcal{Z}(J)\subseteq\mathcal{Z}(I\colon J^\infty)$, applying $\mathcal{I}$ we thus get $\mathcal{I}(\mathcal{Z}(I)\setminus\mathcal{Z}(J))\supseteq\mathcal{I}(\mathcal{Z}(I\colon J^\infty))=\sqrt{(I\colon J^\infty)}$, where the last equality is Real Nullstellensatz. To show "$\supseteq$", as any vanishing ideal is real by *2.18.1*, it's enough to show that we have $(I\colon J^\infty)\subseteq\mathcal{I}(\mathcal{Z}(I)\setminus\mathcal{Z}(J))$, and from *2.16.2* and *1.14.2* it suffices to show that $f\,\mathcal{I}(\mathcal{Z}(J))\subseteq\mathcal{I}(\mathcal{Z}(I))$ for each $f\in(I\colon J^\infty)$. So let's assume that $P\in\mathcal{Z}(I)$, $g\in\mathcal{I}(\mathcal{Z}(J))$ and there exists $t\in\mathbb{N}_+$ such that $fJ^t\subseteq I$, we need to show that $(fg)(P)=0$. By Real Nullstellensatz $\mathcal{I}(\mathcal{Z}(J))=\sqrt[R]{J}$, hence there exists $k\in\mathbb{N}_+$ and a sum of squares $\sigma\in\sum K[\underline{X}]^2$ such that $g^{2k}+\sigma\in J$ and therefore $f(g^{2k}+\sigma)^t\in fJ^t\subseteq I\subseteq\mathcal{I}(\mathcal{Z}(I))$. By the binomial theorem, and the fact that non negative elements of L are squares, the polynomial $(g^{2k}+\sigma)^t$ is itself a sum of squares, as it is also $f^{2kt}(g^{2k}+\sigma)^t=((fg)^{kt})^2+\sigma'\in\mathcal{I}(\mathcal{Z}(I))$ (with $\sigma'\in\sum K[\underline{X}]^2$). As $\mathcal{I}(\mathcal{Z}(I))$ is a real ideal, and recalling that every real ideal is also radical (see **??**), it follows that $fg\in\mathcal{I}(\mathcal{Z}(I))$.

b) By *2.12.3* and part *a*) above, we have:

$$\overline{\mathcal{Z}(I)\setminus\mathcal{Z}(J)}^{Z}=\mathcal{Z}(\mathcal{I}(\mathcal{Z}(I)\setminus\mathcal{Z}(J)))=\mathcal{Z}(\sqrt[R]{(I\colon J^\infty)})=\mathcal{Z}((I\colon J^\infty)).$$

Note that also the "second proof" (see 2.17.2) of 2.17.1 *b*) can be adapted to this case with slight modifications.

c) By **??** *e*), the analogous of the same proof of 2.17.1 *c*) works.. □

2.21. Summary formulas for the coordinate ring

2.21.1. Proposition. — *The coordinate ring construction verifies the following properties:*

a) $K[S]_L\cong K[X_1,\cdots,X_n]/\mathcal{I}_K^L(S)$ *is an* **affine reduced K-algebra**, *i.e. a finitely generated K-algebra with no nilpotent elements, for every subset S of $\mathbb{A}_L^n$;*

b) $K[S]_L=K[\overline{S}^Z]_L$ *for every subset S of $\mathbb{A}_L^n$;*

c) $K[\mathbb{A}_L^n]_L=K[X_1,\cdots,X_n]$ *whenever L is an infinite field;*

d) $K[\mathbb{A}_L^n]_L=K[X_1,\cdots,X_n]/(X_1^q-X_1,\ldots,X_n^q-X_n)$ *if $L=\mathbb{F}_q$ finite field with $q=p^k$ element (p prime integer);*

e) $K[\emptyset]_L=(0)$ *the zero ring;*

f) *If P is K-rational point of $\mathbb{A}_L^n$, then $K[P]_L\cong K$;*

g) *For every ideal I of $K[X_1,\cdots,X_n]$ we have $K[\mathcal{Z}(I)]_L\cong K[X_1,\cdots,X_n]/\mathcal{I}_K^L(\mathcal{Z}_K^L(I))$.*

h) *If L is algebraically closed then $K[\mathcal{Z}_K^L(I)]_L\cong K[X_1,\cdots,X_n]/\sqrt{I}$, for every ideal I of $K[\underline{X}]$.*

k) *If L is real-closed then $K[\mathcal{Z}_K^L(I)]_L\cong K[X_1,\cdots,X_n]/\sqrt[R]{I}$, for every ideal I of $K[\underline{X}]$.*

i) V *is an irreducible* K*-algebraic set of* $\mathbb{A}^n_L$ *if and only if* $K[V]_L$ *is a domain;*

j) *If* $S_1 \subseteq S_2$ *then* $K[S_1]_L \cong K[S_2]_L/\mathcal{I}_{S_2}(S_1)$ *where* $\mathcal{I}_{S_2}(S_1) := \{f \in K[S_2] \mid f_{|S_1} = 0\}$.

l) *If* P *is a point of* $\mathbb{A}^n_L$ *whose coordinates all are algebraic over* K*, then* $K[P]_L \cong K[\underline{X}]/\mathcal{I}^L_K(P)$ *is a subfield of* L*, also denoted* $K(P)$*, and* $K \subseteq K(P)$ *is a finite extension of fields, i.e.* $\dim_K K(P)$ *is finite;*

m) $K[\Delta_{\mathbb{A}^n_L}]_L = K[\underline{X},\underline{Y}]/\mathfrak{d}_n = K[X_1,\dots,X_n,Y_1,\dots,Y_n]/(X_1-Y_1,\dots,X_n-Y_n)$ *for every field extension* $K \subseteq L$*;*

n) *If* $V = \mathcal{Z}(I) \subseteq \mathbb{A}^n_L$*, then* $K[V \times \mathbb{A}^m_L]_L = K[\underline{X},\underline{Y}]/\mathcal{I}(V \times \mathbb{A}^m_L) = K[\underline{X},\underline{Y}]/\mathcal{I}(V)[\underline{Y}] \cong K[V][Y_1,\dots,Y_m]$ *for every field extension* $K \subseteq L$*;*

o) *If* L *is algebraically closed,* $V = Z(I) \subseteq \mathbb{A}^n_L$ *and* $W = Z(J) \subseteq \mathbb{A}^m_L$ *then* $\mathcal{I}^L_K(V \times W) = \sqrt{I}[\underline{Y}] + \sqrt{J}[\underline{X}]$ *and* $K[V \times W]_L \cong K[\underline{X},\underline{Y}]/(\sqrt{I}[\underline{Y}] + \sqrt{J}[\underline{X}])$*. If, moreover,* K *is a perfect field then* $K[V \times W]_L \cong K[\underline{X},\underline{Y}]/(\sqrt{I}[\underline{Y}] + \sqrt{J}[\underline{X}]) \cong K[V]_L \otimes_K K[W]_L$.

p) *If* L *is real-closed,* $V = Z(I) \subseteq \mathbb{A}^n_L$ *and* $W = Z(J) \subseteq \mathbb{A}^m_L$ *then* $\mathcal{I}^L_K(V \times W) = \sqrt[R]{\sqrt[R]{I}[\underline{Y}] + \sqrt[R]{J}[\underline{X}]}$ *and* $K[V \times W]_L \cong K[\underline{X},\underline{Y}]/(\sqrt[R]{\sqrt[R]{I}[\underline{Y}] + \sqrt[R]{J}[\underline{X}]})$

q) *If* $F\colon V \longrightarrow W$ *is a polynomial map with coefficients in* K *between* K*-algebraic set, then* F *induces a ring homomorphism in the opposite direction* $F^*\colon K[W]_L \longrightarrow K[V]_L, \alpha \mapsto \alpha \circ F$ *such that* $(\mathrm{Id}_V)^* = \mathrm{Id}_{K[V]_L}$ *and* $(G \circ F)^* = F^* \circ G^*$.

r) *If* L *is algebraically closed,* $K \subseteq H \subseteq L$ *is a tower of field extensions, and* V *is a* K*-algebraic set in* $\mathbb{A}^n_L$*, then* $\mathcal{I}^L_H(V) = \sqrt{\mathcal{I}^L_K(V)H[\underline{Y}]}$ *and* $H[V]_L \cong (H \otimes_K K[V]_L)_{red}$*. If, moreover* K *is a perfect field (e.g. if it is finite, or it has characteristic zero, or it is algebraically closed), then* $H[V]_L \cong H \otimes_K K[V]_L$.

s) *If* L *is algebraically closed then* $K[\mathcal{Z}(I) \setminus \mathcal{Z}(J)]_L = K[\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z]_L \cong K[\underline{X}]/\sqrt{(I\colon J^\infty)}$ *for every pairs of ideals* I, J *of* $K[\underline{X}]$*. Moreover, if* I *is radical then* $K[\mathcal{Z}(I) \setminus \mathcal{Z}(J)]_L \cong K[\underline{X}]/(I\colon J)$.

t) *If* L *is real-closed then* $K[\mathcal{Z}(I) \setminus \mathcal{Z}(J)]_L = K[\overline{\mathcal{Z}(I) \setminus \mathcal{Z}(J)}^Z]_L \cong K[\underline{X}]/\sqrt[R]{(I\colon J^\infty)}$ *for every pairs of ideals* I, J *of* $K[\underline{X}]$*. Moreover, if* I *is real then* $K[\mathcal{Z}(I) \setminus \mathcal{Z}(J)]_L \cong K[\underline{X}]/(I\colon J)$.

Proof. — This is essentially a summary, in terms of coordinate rings, of what developed so far. In particular, *g)*, *h)*, *l)*, *o)*, *r)* and *s)* are consequences of Hilbert Nullstellensatz (2.14.3) and hold true if we are dealing with zeros in an algebraically closed field. *s)* follows from 2.17.1. For *o)* and *r)* we used *1.9.5 h) and o)*, see also [**Kun85**, Ch. 1, Rules 3.12].

Instead, *k)*, *p* and *t)* need L to be real-closed (for example $L = \mathbb{R}$) and follows from Dubois-Risler Real Nullstensatz (2.18.2). For *t)* we used 2.20.1.

More specifically, for p): using 2.10.7, Real Nullstellensatz, and *1.14.4 j) and o*) we get

$$\mathcal{I}(\mathcal{Z}(I) \times \mathcal{Z}(J)) = \sqrt[R]{\mathcal{I}(\mathcal{Z}(I))[\underline{Y}] + \mathcal{I}(\mathcal{Z}(J))[\underline{X}]} = \sqrt[R]{\sqrt[R]{I}[\underline{Y}] + \sqrt[R]{J}[\underline{X}]}$$

The result now follows from k).

Similarly, for o), we have the canonical isomorphism

$$K[\underline{X}, \underline{Y}]/(\sqrt{I}[\underline{Y}] + \sqrt{J}[\underline{X}]) \cong (K[\underline{X}]/\sqrt{I}) \otimes_K (K[\underline{Y}]/\sqrt{J}).$$

If K is a perfect field, then the tensor product of two reduced K-algebras is still such ([**Bos18**, 7.3, Ex. 6]), hence $\sqrt{I}[\underline{Y}] + \sqrt{J}[\underline{X}]$ is already a radical ideal and then o) follows from h). For perfect fields we refer to [**Bos18**, 3.6, Def. 3, Oss. 4]. □

CHAPTER 3

DYNAMICAL SYSTEMS

General references for this chapter are [**BR05**], [**CHS10**] [**Kai80**], [**Kha02**], [**Isi95**] and [**Isi99**], [**Nv90**], [**Son79b**], [**Son98**], for control theory and dynamical system theory in the engineering area, and [**Arn92**], [**PS94**], [**PSV84**], [**Tes12**], [**Tur98**], [**War83**] for the mathematical and mathematical physics point of view.

3.1. Generalities on dynamical systems: the unforced case

3.1.1. Definition (dynamical system, state equation). — A **(continuous time) dynamical system** is a system whose state depends on time and it is modeled by one or more ordinary differential equations. In general, we are thus interested in a system of n ordinary differential equations, in normal form, of first order, with initial condition (Cauchy problem) under hypotheses of existence and unicity:

$$\begin{cases} \dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y}) \\ \boldsymbol{y}(t_0) = \boldsymbol{y_0} \end{cases}$$

where $\boldsymbol{f} = (f_1, \ldots, f_n)$ is a vector value function of many real variables, defined (at least) on an open subset Ω of $\mathbb{R}^{n+1}$, often a "cylinder" of the form $\Omega = I \times D$, with $I \subseteq \mathbb{R}$ and D a connected open subset of $\mathbb{R}^n$ ($t_0 \in I$, $\boldsymbol{y_0} \in D$). The equation $\dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y})$ is called the **state equation** of the system.

3.1.2. Definition (linear dynamical system). — We say that the above system is a **linear (dynamical) system** if all components f_i are linear functions, *i.e.* there exists a matrix-valued

function $A = A(t) \in \mathrm{Mat}_n(\mathbb{R})$ such that

$$\boldsymbol{f}(t, \boldsymbol{y}) = A(t)\boldsymbol{y}.$$

3.1.3. Definition (polynomial dynamical system). — We say that the above system is a **polynomial dynamical system** if all components f_i are polynomials with real coefficients, *i.e.* $f_i = f_i(Y_1, \ldots, Y_n) \in \mathbb{R}[Y_1, \ldots, Y_n]$.

3.1.4. Definition (solutions of a dynamical system). — A **solution**, or **integral curve**, of the above system is a (vector value) function

$$\boldsymbol{y} \colon I_{\boldsymbol{y}} \longrightarrow \mathbb{R}^n$$

of one real variable, defined on a interval $I_{\boldsymbol{y}} \subseteq I$ (depending on $\boldsymbol{y}$ in general), such that it is

$$(t, \boldsymbol{y}(t)) \in \Omega \ \text{ and } \ \dot{\boldsymbol{y}}(t) = \boldsymbol{f}(t, \boldsymbol{y}(t)) \ \text{ for each } t \in I_{\boldsymbol{y}}, \quad \text{and } \ \boldsymbol{y}(t_0) = \boldsymbol{y_0}.$$

3.1.5. Definition. — The **graph** of any such solution

$$\Gamma_{\boldsymbol{y}} := \{(t, \boldsymbol{y}(t)) \in \Omega \mid t \in I_{\boldsymbol{y}}\} \subseteq \Omega \subseteq \mathbb{R}^{n+1}$$

is said an **integral curve** of the ordinary differential equation $\dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y})$, while its image

$$\boldsymbol{y}(I_{\boldsymbol{y}}) := \{\boldsymbol{y}(t) \mid t \in I_{\boldsymbol{y}}\} \subseteq \mathbb{R}^n$$

is called **orbit**, or **trajectory**, or **characteristic** of the integral curve (or of the dynamical system).

3.1.6. Definition (equilibrium points). — The constant solutions, if any, corresponding to points $\boldsymbol{y_0} \in D \subseteq \mathbb{R}^n$ such that $\boldsymbol{f}(t, \boldsymbol{y}) = \boldsymbol{0}$ for each $t \in I$, are said **equilibrium points**, or **critical** (or also **singular** or **stationary**) **points** of the system. Any such solution correspond to a **point orbit** of the system.

3.1.7. Remark. — As it is known, the theory of first order normal ordinary differential equations systems includes the case of scalar ordinary differential equations, in normal form, of order $n \in \mathbb{N}_+$:

$$y^{(n)}(t) = f(t, y(t), y'(t), \dots, y^{(n-1)}(t)).$$

Indeed, by the substitutions (change of variables)

$$y_1 := y, \quad y_2 := y' = y_1', \quad \dots, \quad y_n := y^{(n-1)} = y_{n-1}',$$

one gets

$$y^{(n)}(t) = f(t, y(t), y'(t), \dots, y^{(n-1)}(t)) \Leftrightarrow \begin{cases} y_1' = y_2 \\ y_2' = y_3 \\ \vdots \\ y_{n-1}' = y_n \\ y_n' = f(t, y_1, y_2, \dots, y_n) \end{cases}$$

where the system has $\boldsymbol{f}(t, y_1, y_2, \dots, y_n) := (y_2, y_3, \dots, y_n, f(t, y_1, y_2, \dots, y_n))$, that is $f_n = f$ and $f_i = y_{i+1}$ for $i = 1, \dots, n-1$. Obviously $\boldsymbol{f}$ is polynomial if f is such.

The n^{th}-order equation and the system are equivalent in the following sense: any real valued function y which is a solution of the former "gives raise" to a solution $\boldsymbol{y} := (y, y', \dots, y^{(n-1)})$ of the latter by means of the above described change of variables. And, vice versa, any given vector valued function $\boldsymbol{y} := (y_1, y_2, y_3, \dots, y_n)$ which is a solution of the latter identifies a solution $y := y_1$ of the former. In general, however a system of n equations of the first order cannot be tracked back to a single equation of n^{th}- order. The notion of a system is more general.

3.1.8. Typical hypotheses. — As in the present work we are mainly concerned with polynomial dynamical systems, though too conservative to cover all applications ([**BR05**, Preface]), we will generally assume that: $\boldsymbol{f}$ is continuous on Ω, locally Lipschitz continuous in $\boldsymbol{y}$ uniformly wrt t. In this way we have local existence and unicity for the given Cauchy problem or, when $\boldsymbol{f}$ is defined on a "strip" $\Omega = I \times \mathbb{R}^n$ with I a real interval, there continuous and locally Lipschitz continuous in $\boldsymbol{y}$ uniformly wrt t in every strip $[a, b] \times \mathbb{R}^n$ for every $[a, b] \subseteq I$, or having granted the existence and unicity of local solutions that $||\boldsymbol{f}||$ grows sublinearly in $\boldsymbol{y}$ uniformly wrt t, so to have existence and unicity of globally defined solutions on the whole of I. In the aforementioned cases, thanks to Gronwall's Lemma, it holds moreover a Theorem of Kamke ([**PSV84**, Ch. 1,

1.9]) on the continuous and uniformly continuous dependance of the solutions on initial data and any parameters, as well as on the function $\boldsymbol{f}$ itself.

3.1.9. Geometric and cinematic interpretation. — A geometric interpretation of the equation $\dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y})$ is the following: trough the equation, to each point $(t, \boldsymbol{y})$, thought of as an "event" (given by "when" and "where"), it is associated the vector $(1, \dot{\boldsymbol{y}}) = (1, \boldsymbol{y})$, which is tangent to the solution curve at that point. Therefore the equation determines a field of directions in its domain and solve the equation means to find those curves that pass through the points being tangent to their prescribed direction vectors. From a cinematic point of view, $\boldsymbol{y}$ can be thought of as the time-position law of a particle and the vector field $\boldsymbol{f}(t, \boldsymbol{y})$ can be regard as the "wind velocity" at time t and position $\boldsymbol{y}$.

3.2. Autonomous system

3.2.1. Definition (autonomous system). — A dynamical system is said to be **autonomous** if its differential equation is of the form

$$\dot{\boldsymbol{y}} = \boldsymbol{f}(\boldsymbol{y})$$

where the vector valued function $\boldsymbol{f} = \boldsymbol{f}(t, \boldsymbol{y}) = \boldsymbol{f}(\boldsymbol{y})$ is independent on time.

3.2.2. Remark (autonomous linear system). — An autonomous linear system is one of the form

$$\dot{\boldsymbol{y}} = A\boldsymbol{y}$$

for some time-invariant real square matrix $A \in \mathrm{Mat}_n(\mathbb{R})$.

3.2.3. Remark. — This happens quite often in many models of natural laws (at least, sometimes, in first approximation). In this case $\boldsymbol{f} \colon \Omega \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is a **vector field** on $\mathbb{R}^n$, and hence the solutions of the dynamical system can be thought of as its **flow lines**, that is curves in $\mathbb{R}^n$ passing through $\boldsymbol{y}$ with velocity given by $\boldsymbol{f}(\boldsymbol{y})$, for each $\boldsymbol{y} \in \Omega$.

3.2.4. Remark. — Every not autonomous equation $\dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y})$ can always be thought of as an autonomous one by means of the following coordinate change

$$z_0 := t, \quad z_i := y_i \ \text{ for } \ i = 1, \dots, n$$

together with the "extra equation" $\dot{z_0} = 1$, so that

$$\dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y}) \Leftrightarrow \dot{\boldsymbol{z}} = \boldsymbol{f}^*(\boldsymbol{z})$$

where $\boldsymbol{f}^* \colon \Omega \subseteq \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^{n+1}$ is defined by

$$\boldsymbol{f}^*(\boldsymbol{z}) := (1, f_1(z_0, z_1, \dots, _n), \dots, f_n(z_0, z_1, \dots, _n)).$$

Therefore WLOG we can bound our attention to the study of autonomous systems.

3.2.5. Phase space, or state space, and phase curves. — If the equation $\dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y})$ models whatever process or phenomenon, any solution of it represents the evolution of the modelled process or phenomenon as the independent variable t, often regarded ad a time, varies. The vectors $\boldsymbol{y}(t) \in \mathbb{R}^n$ of the corresponding orbit represent as "time" t varies the different "phases" of that process. Hence, in the whole vector space $\mathbb{R}^n$ all "possible states" of a system are represented, and therefore it is called **phase space** or **state space**. Besides, this is in agreement with the cinematic-mechanic interpretation of a system coming from an autonomous equations of the second order $y''(t) = f(y(t), y'(t))$, as in classical mechanics, in which the "phase space" is the space representing both the position and the momentum of a particle. Coherently, if $\boldsymbol{y} = \boldsymbol{y}(t)$ is a solution, then it is also called **phase curve** of the system $\dot{\boldsymbol{y}} = \boldsymbol{f}(t, \boldsymbol{y})$.

3.2.6. Solutions structure for autonomous systems, phase portrait. — The structure of the solutions of an autonomous dynamical system can be understood analyzing their orbits in the connected Ω of the phase space $\mathbb{R}^n$: under the stated hypotheses, Ω is covered by trajectories of the system, necessarily disjoint, which can be classified in the following three classes ([**Tes12**, 6.3]):

a) **Equilibrium points**, corresponding to the *constant solutions* of the state equation. They are given by the zeros of the vector field $\boldsymbol{f}(t, \boldsymbol{y})$.

b) **Cycles**, corresponding to the *non-constant periodic solutions* of the state equation. Their orbits are given simple (*i.e.* with no self-intersections) closed curves inside Ω in the state space.

c) **Open trajectories**, corresponding to the *non-periodic solutions* of the state equation. Their orbits are neither points nor cycles, but non-closed simple curves in Ω. They can approach an equilibrium point or go to infinity. Sometimes, they can also spiral around a closed orbit (limit cycle) form the inside or from the outside of it (in dimension two). In dimension higher than two their behavior can be quite hard to grasp.

Moreover, there are no self-intersecting non closed orbits. The configuration of the system's orbits inside Ω is the **phase portrait** of the autonomous system. Hence it is a geometric representation of the trajectories of the system in the state space.

3.2.7. Lie derivative: the derivative along a trajectory and first integrals. — In the analysis of the solutions structure of a dynamical system are of crucial importance the concepts of **derivative along a trajectory**, or **Lie derivative**, of a scalar field (*i.e.* a function)

$$E\colon \Omega \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}$$

of class C^1 on Ω, and of **first integral**, or **constant of motion** for the system ([**Arn92**, Ch. 2, §2], [**Kha02**, 13.2], [**PS94**, Vol. 2, Ch. 4, Def. 3.2], [**Tes12**, 6.6], [**War83**, 2.24]).

a) The **(Lie) derivative of E along the trajectories** of the system $\dot{\boldsymbol{y}} = \boldsymbol{f}(\boldsymbol{y})$ is defined as

$$L_{\boldsymbol{f}} E(\boldsymbol{y}) = \dot{E}(\boldsymbol{y}) := < \nabla E(\boldsymbol{y}), \boldsymbol{f}(\boldsymbol{y}) >,$$

that is

$$\dot{E}(\boldsymbol{y}) = < \nabla E(\boldsymbol{y}(t)), \boldsymbol{f}(\boldsymbol{y}(t)) > = < \nabla E(\boldsymbol{y}(t)), \dot{\boldsymbol{y}}(t) > = \frac{\mathrm{d}}{\mathrm{d}t} E(\boldsymbol{y}(t))$$

for each $\boldsymbol{y} \in \Omega$.

b) If $\dot{E}(\boldsymbol{y}) = 0$ for each $\boldsymbol{y} \in \Omega$, the field E is said to be a **first integral** (or a **"constant of motion"**) of the system.

3.2.8. Remark. — One finds that E is a first integral of the system if and only if each one of its orbits is entirely contained in a unique fibre (level set) of E or, equivalently, if and only if E is constant on each solution of the system ([**PS94**, Vol. 2, Ch. 4, Prop. 3.4]).

3.2.9. The Lie derivative of a polynomial subset/ideal. — For future use let us note the following construction, given a subset G of the polynomial ring $\mathbb{R}[W_1, \dots, W_n]$, and let $f = (f_1; \dots; f_n) \in \mathbb{R}[W_1, \dots, W_n]^n$ be a polynomial vector field. Then we define the following ideals of $\mathbb{R}[W_1, \dots, W_n]$

$$L_f^0(G) := (G),\ L_f(G) = L_f^1(G) := (G \cup \{L_f p \mid p \in G\}), \dots, L_f^s(G) := (\{L_f^r p \mid r \in \mathbb{N}, r \leq s, p \in G\}), \dots$$

then clearly:

1. each $L_f^s(G)$ is an ideal of $\mathbb{R}[W_1, \dots, W_n]$ (by definition);
2. for any subset G of the polynomial ring $\mathbb{R}[W_1, \dots, W_n]$ we have $L_f^s(G) = L_f^s((G))$;
3. $L_f^1 L_f^s(G) = L^{s+1}(I)$ (by the algebraic properties of Lie derivatives);
4. $(G) \subseteq L_f^1(G) \subseteq \cdots \subseteq L^s(G) \subseteq L^{s+1}(G) \subseteq \cdots$ is an ascending chain of ideals in $\mathbb{R}[W_1, \dots, W_n]$;
5. $L_f^\infty(G) := \bigcup_{s \in \mathbb{N}} L_f^s(G)$ is an ideal of $\mathbb{R}[W_1, \dots, W_n]$ (as it directly follows by the previous point);
6. The chain of ideals stabilizes after the first equality, that is there is a finite $r \in \mathbb{N}$ such that

   $$(G) \subset L_f(G) \subset \cdots \subset L_f^{r-1}(G) \subset L_f^r(G) = L_f^{r+1}(G) = \cdots = L_f^s(G) = \cdots = L_f^\infty(G)$$

   for each $s \in \mathbb{N}$ such that $s \geq r$. This is a straightforward consequence of Hilbert Basis Theorem, the previous definitions and the previous results;
7. By Groebner basis theory (see **[CLO15]**, **[KR00]**) it is then possible, in a finite number of steps, to find a finite number of generators for $L_f^\infty(G) = L_f^r(G)$ given a finite subset G of $\mathbb{R}[W_1, \dots, W_n]$.

3.3. Stability

A central role in the study of dynamical systems, as well as in control theory, is played by the notion of **stability** for a solution (typically an equilibrium point) of an autonomous system. The point is that, when one models a situation, a process, or a problem in a mathematical framework by means of a dynamical system, the relevant "data" are identified: initial or boundary conditions, any parameters, the function $\boldsymbol{f}$ itself, the "algorithm", could be regarded as datum of the problem. Any variation on these data causes a variation in the solution. It is therefore of interest to study the correspondence

$$\text{data} \quad \mapsto \quad \text{solution},$$

from this point of view, also by defining a suitable "continuity" notion (in the vein of Kamke's Theorem, for example). The concept of stability embodies this notion: do small variations on data reflect in small (or, at least, controllable) variations on solutions? The practical interest of this is apparent, for example, if one thinks to any mechanical appliance: there the stability of the appliance becomes insensibility to perturbations of any kind. Kamke's Theorem represents a first result in this direction, but it has a limit in the fact that it holds on bounded time intervals, while the main interest is on long time or standard use. Hence it is necessary to develope suitable tools to ensure control on perturbed solutions on unbounded time. This is what Lyapunov has developed.

3.3.1. Definition (Lyapunov stability). — Given a state equation (autonomous system) $\dot{\boldsymbol{y}} = \boldsymbol{f}(\boldsymbol{y})$ and a solution $\boldsymbol{y} = \boldsymbol{y}(t; 0, \boldsymbol{y}_0)$ of it (corresponding to the initial datum $(0, \boldsymbol{y}_0)$ and assuming $\boldsymbol{y}$ defined on $[0, +\infty[$), we say that ([**Arn92**, Ch. 3, §23], [**Kha02**, 4.1], [**PS94**, Vol. 2, Ch. 4, Def 3.3], [**Tur98**, Ch. 11], [**Tes12**, 6.5]):

a) The solution $\boldsymbol{y}$ is **(Lyapunov) stable** if for each $\varepsilon > 0$ there exists $\delta > 0$ such that for every initial data $\boldsymbol{z}_0$ with $||\boldsymbol{z}_0 - \boldsymbol{y}_0|| < \delta$ the corresponding solution $\boldsymbol{z} = \boldsymbol{z}(t; 0, \boldsymbol{z}_0)$ is defined on $[0, +\infty[$ and satisfies $||\boldsymbol{z}(t) - \boldsymbol{y}(t)|| < \varepsilon$ for each $t \in [0, +\infty[$.

b) The solution $\boldsymbol{y}$ is **(locally) attractive** if there exists $\delta_0 > 0$ such that

$$\lim_{t \longrightarrow +\infty} ||\boldsymbol{z}(t) - \boldsymbol{y}(t)|| = 0$$

for every solution $\boldsymbol{z}$ with $||\boldsymbol{z}(0) - \boldsymbol{y}_0|| < \delta_0$. The solution is **globally attractive** if this holds for every solution $\boldsymbol{z}$.

c) The solution $\boldsymbol{y}$ is **asymptotically stable** if it is stable and attractive.

d) The solution $\boldsymbol{y}$ is **exponentially stable** if there are constants $\alpha, \delta, M > 0$ such that $||\boldsymbol{z}(t; 0, \boldsymbol{z}_0) - \boldsymbol{y}(t)|| < M e^{-\alpha t ||\boldsymbol{z}_0 - \boldsymbol{y}_0||}$ whenever $||\boldsymbol{z}_0 - \boldsymbol{y}_0|| < \delta$ (any exponentially stable solution is stable as well).

e) The solution $\boldsymbol{y}$ is **unstable** if it is not stable. This means, essentially, that there are solutions "starting" however close to $\boldsymbol{y}$ which do not stay definitely close to it.

3.3.2. Stability of equilibrium points. — This notion is clearly crucial in classifying the nature of equilibrium points of the system, *i.e.* of the solutions $\boldsymbol{y}_0$ of the equation $\boldsymbol{f}(\boldsymbol{y}) = \boldsymbol{0}$. Let us check that we can always assume $\boldsymbol{y}_0 = \boldsymbol{0}$. Indeed, if $\boldsymbol{f}(\boldsymbol{y}) = \boldsymbol{0}$, then under the

change of variable $\boldsymbol{z}(t) := \boldsymbol{y}(t) - \boldsymbol{y}_0$ the given state equation is equivalent to $\dot{\boldsymbol{z}} = \boldsymbol{g}(\boldsymbol{z})$ where $\boldsymbol{g}(\boldsymbol{z}) := \boldsymbol{f}(\boldsymbol{z} + \boldsymbol{y}_0)$, and this last has $\mathbf{0}$ as an equilibrium point.

In the analysis of the stability of asymptotically stable equilibrium points the previous terminology is completed as follows.

e) If $\boldsymbol{y}_0$ is an asymptotically stable equilibrium point, its **basin of attraction** is the set of points $\boldsymbol{z}_0 \in \Omega$ such that $\lim_{t \longrightarrow +\infty} ||\boldsymbol{z}(t; 0, \boldsymbol{z}_0) - \boldsymbol{y}_0|| = 0$.

f) A point $\boldsymbol{y}_0$ is said to be **globally asymptotically stable (GAS)** if it is an asymptotically stable equilibrium point and its basin of attraction is the all of Ω.

3.4. Stability analysis: linear case

Stability analysis can be very difficult in general. In the special, but relevant, case of linear systems, as we have an explicit representations of the solutions, the stability analysis of the origin as an equilibrium point can be studied directly. For nonlinear systems we do not have usually an explicit form for the solutions, therefore the stability analysis must be performed in an indirect way, a main tool to this end is the so called "Lyapunov method".

3.4.1. Stability analysis for linear systems. — For an autonomous linear system $\dot{\boldsymbol{y}} = A\boldsymbol{y}$, if the (complex) spectrum of A is

$$\mathrm{sp}_{\mathbb{C}}(A) = \{\lambda_1, \ldots, \lambda_k\}$$

(where the λ_i are the distinct complex eigenvalues of A), then ([**Kai80**, 2.6], [**PS94**, Vol. 2, Ch. 4, Teo. 3.6], [**Tes12**, 3.2, 6.5], [**Tur98**, 11.2]):

a) The origin $\mathbf{0}$ is an asymptotically stable equilibrium point if and only if A is an **Hurwitz matrix**, that is $\mathrm{sp}_{\mathbb{C}}(A) \subset \{z \in \mathbb{C} \mid \mathbb{R}(z) < 0\}$. In this case, its basin of attraction is $\mathbb{R}^n$.

b) The origin $\mathbf{0}$ is a stable equilibrium point, but not asymptotically stable, if and only if $\mathrm{sp}_{\mathbb{C}}(A) \subset \{z \in \mathbb{C} \mid \mathbb{R}(z) \leq 0\}$ and each eigenvalue is a regular [1] one.

c) The origin $\mathbf{0}$ is an unstable equilibrium point in all other cases.

1. An eigenvalue is **regular** if its algebraic multiplicity, as a root of the characteristic polynomial, equals its geometric multiplicity, *i.e.* the dimension of its eigenspace.

3.5. Stability analysis: Lyapunov method

3.5.1. Lyapunov method for stability analysis in general. — To analyze the stability of the origin for a dynamical system can be very difficult in the general case. A. M. Lyapunov devised a method to tackle this task, generalizing a classic Theorem of Langrange-Dirichelt (built upon an observation of Torricelli) giving a sufficient condition for the stability of an equilibrium point: if the potential energy of a conservative mechanical system has a strong local minimum in a given point, the equilibrium of that point is stable ([**Lei10**]).

In Lyapunov generalization of this result the role of the potential energy is played by the so called "Lyapunov function".

3.5.2. Definition (Lyapunov function). — A **Lyapunov function** for the autonomous system $\dot{\boldsymbol{y}} = \boldsymbol{f}(\boldsymbol{y})$ is a scalar field

$$V \colon \mathcal{U} \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}$$

such that the following properties hold true:

a) $\mathbf{0} \in \mathcal{U}$, and $\mathcal{U}$ is an open subset of $\mathbb{R}^n$,
b) $V(\mathbf{0}) = 0$ and $V(\boldsymbol{y}) > 0$ for each $\boldsymbol{y} \in \mathcal{U} \setminus \{\mathbf{0}\}$,
c) V is of class C^1 and $L_{\boldsymbol{f}} V = \dot{V}(\boldsymbol{y}) \leq 0$ for each $\boldsymbol{y} \in \mathcal{U}$.

If, moreover, $\dot{V} < 0$ in $\mathcal{U} \setminus \{\mathbf{0}\}$, then V is said to be a **strict Lyapunov function**.

The main result is the following ([**Kha02**, 4.1, Thm. 4.1, Thm. 4.2], [**PS94**, Vol. 2, Ch. 4, Sec. 3.5, Teo. 3.7, Prop. 3.11, Prop. 3.12], [**Tes12**, 6.6]).

3.5.3. Lyapunov method. — *Given a locally lipschtiz autonomous system $\dot{\boldsymbol{y}} = \boldsymbol{f}(\boldsymbol{y})$ on an open subset $\Omega \subseteq \mathbb{R}^n$, such that $\mathbf{0} \in \Omega$ and $\boldsymbol{f}(\mathbf{0}) = \mathbf{0}$. Then:*

a) If there exists a Lyapunov function V for $\dot{\boldsymbol{y}} = \boldsymbol{f}(\boldsymbol{y})$ defined in an open neighborhood of the origin $\mathbf{0} \in \mathcal{U} \subseteq \Omega$, then $\mathbf{0}$ is a stable point for the system.
b) If there exists such a V as in a) which, moreover, is a strict Lyapunov function, then $\mathbf{0}$ is an asymptotically stable point for the system.
c) If $\Omega = \mathbb{R}^n$, $\mathbf{0}$ is the unique equilibrium point of the system, and there exists a strict Lyapunov function such that V is defined on $\mathbb{R}^n$ and $V(\boldsymbol{y}) \longrightarrow +\infty$ as $||\boldsymbol{y}|| \longrightarrow +\infty$, then $\mathbf{0}$ is a globally asymptotically stable point for the system.
d) If $\Omega = \mathbb{R}^n$, $\mathbf{0}$ is an equilibrium point of the system, there exists a Lyapunov function such that V is defined on $\mathbb{R}^n$, $V(\boldsymbol{y}) \longrightarrow +\infty$ as $||\boldsymbol{y}|| \longrightarrow +\infty$, and $\mathbf{0}$ is the unique invariant

subset[2] *of* $\{\boldsymbol{y} \in \mathbb{R}^n \mid V(\boldsymbol{y}) = 0\}$*, then* $\mathbf{0}$ *is an asymptotically stable point for the system. Moreover, the stability is global if* $\mathbf{0}$ *is the unique equilibrium point of the system.*

3.5.4. Remark. — There is no general strategy for the search of a Lyapunov function, circumstance that bounds the applicability of the method and constitutes the main weakness of this theory.

In general, the search of a Lyapunov function is difficult: sometimes one can take the *total energy of the system* or a *first integral*, if it is positive defined at least in an open neighborhood of the origin. More generally, if the system admits one or more first integrals simultaneously vanishing only at the origin, then the sum of the squares of these integrals is a Lyapunov function for the system.

From an algorithmic point of view the "sum of squares" (SOS) strategy is largely studied and exploited (cf. [**Las10**], [**ABCR20**]). But, on the other end, there are examples of polynomial systems having the origin as a globally asymptotically stable (GAS) equilibrium point not admitting any Lyapunov function of *polynomial* type (cf. [**BR05**, Prop. 5.2] and [**AKP11**]).

It could then be of interest to have a characterization of those polynomial systems for which a polynomial Lyapunov function does exist, in the style of [**BR05**, Prop. 5.3].

3.6. Converse Lyapunov theorems

The conditions given are only sufficient ones. Although it can be proven that they are also necessary in a sense (cf. [**Kha02**, Sec. 4.7], [**Mas49**], [**Mas56**], [**Mas58**], [**Hah67**] and [**BR05**]), these kind of results are more of theoretical interest. A thorough discussion of the problem and a presentation of the known results can be found in [**Hah67**, Ch. VI], where it is also said (cf. [**Hah67**, Ch. VI, n. 47]):

> [...] We also mention that the converse theorems are primarily of theoretical significance. They find no application in the treatment of stability problems in practice, for the converse theorem assumes as known the solution of the practical problem, the stability behavior. Even the constructive procedures of the converse theorems give in general no hint (except in the linear case) as to how a Liapunov function can practically be obtained. It is obvious that knowledge about the existence of a Liapunov function can still occasionally be important [...]

2. A subset $S \subseteq \Omega$ is (positively) invariant if every semiorbit starting in S stays in S as $t \to +\infty$.

An updated discussion on this line of research, as well as several generalizations of the notion of "stability" and its treatment in the time variant case, can be found in [**BR05**].

3.7. Basic examples

3.7.1. Example (Malthus Model, 1798). — It is a proposed model for the growth of an isolated population with infinite resources, where:

- $N(t)$ is the number of member of the population at time t;
- b is the number (rate) of new borns per unit of population per unit time;
- d is the number (rate) of deaths per unit of population per unit time;
- $p = b - d$ represents the "biological potential" of the population;

then

$$\dot{N} = pN.$$

Hence

$$N(t) = N(0)e^{pt}.$$

The constant solution $N(t) = 0$ is an unstable equilibrium point.

This model is quite unrealistic in many cases if by "population" is meant a biological population, it is instead quite accurate if we are dealing with a population of a radioactive element (then $p = -d$ is the radioactive decay count rate).

3.7.2. Example (Logistic Growth Model of Verhulst, 1845). — It is a proposed model for the dinamic of an isolated population with linear competition for resources, where:

- $N(t)$ is the number of member of the population at time t;
- $p = b - d > 0$ is corrected by the term ("interspecific competition") $-\frac{1}{K}N(t)$ (with $K > 0$), linearly decreasing as a function of N;

then

$$\dot{N} = pN\left(1 - \frac{N}{K}\right).$$

The term $-\frac{p}{K}N(t)^2$ mitigates the exponential growth caused by $pN(t)$ and therefore it can be regarded as the model, in this context, of the "social friction", which is assumed be proportional to the number of encounters among individuals (competing for the resources) per unit time.

Solving the differential equation, one finds

$$N(t) = \frac{KN(0)e^{pt}}{K - N(0) + N(0)e^{pt}}.$$

If $N(t) \neq 0$, then $N(t) \longrightarrow K$ as $t \longrightarrow +\infty$, and therefore K is called "carrying capacity of the environment".

The constant solution $N(t) \equiv 0$ is a unstable, while $N(t) \equiv K$ is asymptotically stable with basin of attraction $[0; , +\infty[$

3.7.3. Example (Predator - Prey model of Lotka, 1925 - Volterra, 1924). — This model was independently developed by Lotka (1925), originally in connection with a chemical kinetics problem, and by Volterra (1924), to explain certain consequences of the absence of fishing during the World War I on the marine population of the Adriatic Sea.

- $x(t)$ is the number of predator at time t;
- $y(t)$ is the number of prey at time t;
- A is the relative rate of growth of prey, assumed to be positive and constant in absence of predator, but linearly decreasing, with relative rate $B > 0$, as a function of the number of predator;
- C is the relative rate of growth of predator, assumed to be negative and constant in absence of prey, but linearly increasing, with relative rate $D > 0$, as a function of the number of prey.

Then one finds the time invariant nonlinear system:

$$\begin{cases} \frac{\dot{x}}{x} = A - By \\ \frac{\dot{y}}{y} = -C + Dx \end{cases} \left(\Rightarrow \begin{cases} \dot{x} = (A - By)x \\ \dot{y} = (-C + Dx)y \end{cases} \Leftrightarrow \begin{cases} \dot{x} = Ax - Bxy \\ \dot{y} = -Cy + Dxy \end{cases} \right)$$

It has

$$(x_0, y_0) = \left(\frac{C}{D}, \frac{A}{B}\right),$$

as its only equilibrium point. Taking the difference of the first equation times $(-C + Dx)$ and the second times $(A - By)$ one gets

$$0 = \left(\frac{C}{x} + D\right)\dot{x} - \left(\frac{A}{y} - B\right)\dot{y} = \frac{\mathrm{d}}{\mathrm{d}t}[-C\ln(x) + Dx - A\ln(y) + By],$$

hence

$$E(x, y) := -C\ln(x) + Dx - A\ln(y) + By$$

is a first integral of the system. It is a strictly convex scalar field in the first quadrant ($x > 0, y > 0$), the equilibrium point (X_0, y_0) is its global minimum, and $E \longrightarrow +\infty$ as x or y go to 0^+ or $+\infty$. Therefore, the level sets $\{E = c\}$ with $c > E(x_0, y_0)$, which are the orbits of the system, are regular closed curves "winding" counter clokwise around the equilibrium point (x_0, y_0) (as one deduces by the sign of the second members of the equations of the system) with a period depending on the "level" c. The equilibrium is neutrally stable, that is it is not asymptotical. A "positively defined" first integral for the system is given by:

$$V(x, y) := E(x, y) - E\left(\frac{C}{D}, \frac{A}{B}\right).$$

3.7.4. Example (One Dimensional Dinamic). — Newton's equation of one dimensional dynamics

$$\ddot{y} = \frac{F}{m}$$

where $\ddot{y}$ represents the acceleration of a material point of mass m subject to a net force $\boldsymbol{F} = \boldsymbol{F}(t, y, \dot{y})$, function of time, position and velocity in general, is equivalent to the system of two equations

$$\begin{cases} \dot{y}_1 = y_2 \\ \dot{y}_2 = \frac{F(t, y_1, y_2)}{m} \end{cases} \qquad \text{(hence } \boldsymbol{f}(t, y_1, y_2) = \left(y_2, \tfrac{F(t, y_1, y_2)}{m}\right)\text{)}.$$

It has, among many others, some interesting special cases:

3.7.4.1. **Free Fall Motion (near Earth)**. — The motion of a heavy body acted upon by the force of gravity in the proximity of the surface of a planet:

$$\ddot{y} = -g \qquad \Leftrightarrow \qquad y(t) = y(0) + \dot{y}(0)t - \frac{1}{2}gt^2$$

3.7.4.2. **Harmonic Oscillator**. — The motion of a mass (m) - spring (k) (undamped) system $\left(\omega^2 = \frac{k}{m}\right)$, or of a hanging pendulum (of length ℓ) under small angular displacements $\left(\omega^2 = \frac{g}{\ell}\right)$:

$$\ddot{y} = -\omega^2 y \quad \Leftrightarrow \quad y(t) = y(0)\cos(\omega t) + \frac{\dot{y}(0)}{\omega}\sin(\omega t) = \sqrt{y(0)^2 + \left(\frac{\dot{y}(0)}{\omega}\right)^2}\sin(\omega t + \phi)$$

(where $\tan(\phi) = -\frac{\dot{y}(0)}{y(0)\omega}$)

3.7.4.3. **van der Pol equation**. — It describes the motion of a perturbed harmonic oscillator by a forcing term $\varepsilon(1-y^2)\dot{y}$ ($\varepsilon > 0$):

$$\ddot{y} = -\omega^2 y + \varepsilon(1-y^2)\dot{y}.$$

If $|y| > 1$ (high values of y), the forcing term represents an active resistance (it dissipates energy), while for small values of y ($|y| < 1$) it represents a "negative resistance" (it supplies energy). In this case, the system presents self-sustained oscillations. It can be shown by linearization that the origin is an unstable equilibrium point for it and, by ad hoc method, that it has a limiting cycle.

3.7.5. Example. — Let $\boldsymbol{f}$ be the polynomial vector field on $\mathbb{R}^2$ such that

$$\boldsymbol{f}(X_1, X_2) := (-X_1 + X_1X_2, -X_2).$$

As shown in [**AKP11**] then the dynamical system $\dot{\boldsymbol{x}} = \boldsymbol{f}$ has the origin has a globally asymptotically stable equilibrium point, having $V(X_1, X_2) := \ln(1+X_1^2) + X_2^2$ as a Lyapunov function vanishes at the origin ([**Kha02**],), but it does not admit any polynomial Lyapunov function.

3.8. Observability and an algebraic approach to it for polynomial systems

Let now the dynamic equations be given by

$$\begin{cases} \dot{x} = f(x(t), u(t)),\ x(t_0) = x_0 \\ y = h(x(t)) \end{cases},\ t \geq 0 \tag{3}$$

where $f : \mathbb{R}^n \times \mathbb{R}^p \to \mathbb{R}^n$ and $h : \mathbb{R}^n \to \mathbb{R}^m$ are polynomial functions; $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^p$, and $y(t) \in \mathbb{R}^m$ are the state, input, and measurement vectors, respectively.

Note that the initial state x_0 may be taken in a fixed algebraic subset $V = \mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(p_1, \ldots, p_l)$, with no extra effort, but we will not go trough this possibility here.

The observability of a system is defined as follows ([**HK77**], [**Son79a**], [**Nv90**], [**Isi95**]).

3.8.1. Definition (Observability and distinguishability). — A system is **observable** if the initial state x_0 is uniquely determined by the knowledge of $y(t)$ on a finite time interval. We say that two initial states $x_{0,1}, x_{0,2} \in \mathbb{R}^n$ are **distinguishable** if the corresponding output signals y_1 and y_2 differ. If this property is satisfied by all couples of initial states then the system is observable.

3.8.2. An algebraic criterion for observability. — It is well known that in the algebraic case, as well as in the analytic case, more generally, observability can be characterized by means of iterated Lie derivatives of h along f ([**HK77**],[**Son79a**], [**Bai81**], [**Nv90**], [**Bar95**], [**Bar16**]):

$$h(x),\ L_fh(x) =< \nabla h(x), f(x) >= \sum_{i=1}^{n} f_i(x)\frac{\partial h}{\partial x_i},\ L_f^2h(x) = L_f(L_fh(x)), \dots$$

That is ([**HK77**], [**Son79a**], [**Nv90**], [**Isi95**]), letting

$$\Phi(x) := \begin{pmatrix} h(x) \\ L_fh(x) \\ L_f^2h(x) \\ \vdots \end{pmatrix}$$

be the (infinite dimensional) **observability mapping**, we have

$$x_{0,1} \text{ and } x_{0,2} \text{ are indistinguishable} \quad \Leftrightarrow \quad \Phi(x_{0,1}) = \Phi(x_{0,2}).$$

In our polynomial case this provides an infinite set of *polynomial equations* defining the *locus of indistinguishability* (or "non-observability locus") of the system, which is therefore an $\mathbb{R}$-algebraic set as in the previous chapter, indeed

$$\{(x_1; x_2) \in \mathbb{R}^n \times \mathbb{R}^n \mid \Phi(x_1) = \Phi(x_2)\} = \mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(\mathcal{J})$$

where $\mathcal{J}$ is the ideal of $\mathbb{R}[X_1, \dots, X_n, Z_1, \dots, Z_n]$ generated by the (infinitely many) polynomials

$$h(Z) - h(X),\ L_fh(Z) - L_fh(X),\ L_f^2h(Z) - L_f^2h(X), \dots$$

where $h(Z) - h(X) := h(Z_1, \dots, Z_n) - h(X_1, \dots, X_n), \cdots \in \mathbb{R}[X_1, \dots, X_n, Z_1, \dots, Z_n]$.

Hence, we can say that the system is observable if and only if $\mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(\mathcal{J}) = \Delta_n = \mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(\mathfrak{d}_{\mathfrak{n}})$ (the diagonal of $\mathbb{R}^n \times \mathbb{R}^n$, 2.2.3 and 2.10.5). But, as it always trivially is $\mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(\mathfrak{d}_{\mathfrak{n}}) \subseteq \mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(\mathcal{J})$, then:

$$\text{the system is observable } \Leftrightarrow \mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(\mathcal{J}) \setminus \mathcal{Z}_{\mathbb{R}}^{\mathbb{R}}(\mathfrak{d}_{\mathfrak{n}}) = \emptyset.$$

3.8.3. Remark. — Note that, as quoted in chapter one, by Hilbert Basis Theorem this ideal is generated by a *finite subset* of the previous infinite set of polynomials, but as Hilbert's Theorem does not give us an explicit finite generating set for $\mathcal{J}$, it is relevant to this concern to exploit the construction introduced in 3.2.9.

3.8.4. Algebraic criterion for observability.— From the above, and 2.18.2, we can conclude that the system

$$\left\{ \begin{array}{l} \dot{x} = f(x(t), u(t)),\ x(t_0) = x_0 \\ y = h(x(t)) \end{array} \right. ,\ t \geq 0 \tag{4}$$

is observable if and only if

$$\sqrt[R]{L^{\infty}_{f^{\Delta}}(h^{\Delta})} = \sqrt[R]{\mathfrak{d}_{\mathfrak{n}}},$$

where $h^{\Delta} := h^{\Delta} := h(Z_1, \ldots, Z_n) - h(X_1, \ldots, X_n)$, $f^{\Delta} := \begin{pmatrix} f(Z_1, \ldots, Z_n) \\ f(X_1, \ldots, X_n) \end{pmatrix}$, and $\mathfrak{d}_{\mathfrak{n}} = (Z_1 - X_!, \ldots, Z_n - X_n)$. But, as $\mathbb{R}[X_1, \ldots, X_n, Z_1, \ldots, Z_n]/\mathfrak{d}_{\mathfrak{n}} \cong \mathbb{R}[X_1, \ldots, X_n]$ is a real ring (see 1.12.4), the ideal $\mathfrak{d}_{\mathfrak{n}}$ is a real ideal (as in 1.12.2) and hence $\sqrt[R]{\mathfrak{d}_{\mathfrak{n}}} = \mathfrak{d}_{\mathfrak{n}}$ (by 1.14.4). Therefore, the above system is observable if and only if

$$\sqrt[R]{L^{\infty}_{f^{\Delta}}(h^{\Delta})} = \mathfrak{d}_{\mathfrak{n}}.$$

3.8.5. Remark. — Depending on the difficulty of the computation with polynomials, a slightly different approach can be followed using result from 2.20.1: a major bottle-neck always is the real radical of an ideal.

3.8.6. Example.— Let us consider the system defined by (see [**Bar16**, Example 20.])

$$f = x, \qquad h = x^3,$$

it clearly is an observable system as h is a bijective function. Now

$$f^{\Delta} = \begin{pmatrix} Z \\ X \end{pmatrix}, \qquad h^{\Delta} = Z^3 - X^3$$

then

$$L_{f^{\Delta}}(h^{\Delta}) = 3h^{\Delta} \text{ and therefore } L^{\infty}_{f^{\Delta}}(h^{\Delta}) = (Z^3 - X^3),$$

and we already saw (2.18.9) that $\sqrt[R]{(Z^3 - X^3)} = (Z - X)$.

3.8.7. Example.— Let us consider the system defined by (see [**Bar16**, Example II.5])

$$f = x, \qquad h = x^3,$$

it clearly is an observable system as h is a bijective function. Now

$$f^\Delta = \begin{pmatrix} Z \\ X \end{pmatrix}, \qquad h^\Delta = Z^3 - X^3$$

then

$$L_{f^\Delta}(h^\Delta) = 3h^\Delta \text{ and therefore } L^\infty_{f^\Delta}(h^\Delta) = (Z^3 - X^3),$$

and we already saw (2.18.9) that $\overset{R}{\sqrt{(Z^3 - X^3)}} = (Z - X)$.

CHAPTER 4

ISS LYAPUNOV FUNCTIONS FOR STATE OBSERVERS OF DYNAMIC SYSTEMS USING HAMILTON–JACOBI INEQUALITIES

4.1. Input-to-State Stability for State Observers

Estimation for nonlinear noise-free continuous-time systems is usually accomplished by using observers, which are dynamic systems that aim at tracking the state variables by using only incomplete information on the state. Let the dynamic equations be given by

$$\begin{cases} \dot{x} = f(x,u) \\ y = h(x) \end{cases}, \ t \geq 0 \tag{5}$$

where $f : \mathbb{R}^n \times \mathbb{R}^p \to \mathbb{R}^n$ and $h : \mathbb{R}^n \to \mathbb{R}^m$ are smooth functions; $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^p$, and $y(t) \in \mathbb{R}^m$ are the state, input, and measurement vectors, respectively. A full-order state observer is in general described by the dynamic equation

$$\dot{\hat{x}} = \gamma(\hat{x}, y, u) \ t \geq 0 \tag{6}$$

where $\hat{x}(t) \in \mathbb{R}^n$ is the estimate of $x(t)$ at time t and $\gamma : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}^n$ is a smooth function to be chosen in such a way as to ensure that the estimation error $e := x - \hat{x}$ with dynamics given by

$$\dot{e} = f(x,u) - \gamma(x - e, h(x)) =: F_\gamma(e,x,u) \tag{7}$$

being asymptotically stable to zero. Moreover, usually $m < n$, i.e., roughly speaking, not all of the state variables are accessible. Notice that Label (7) depends in general on the system trajectory and it would always be preferable to ensure the global asymptotic stability to zero fro the estimation error. In line with **[SJT03]**, the interest concerns observers for (5) with globally asymptotically stable estimation error by finding a suitable mapping γ and a smooth Lyapunov

function $(e,x) \mapsto V(e,x)$ such that

$$\alpha_1(|e|) \leq V(e,x) \leq \alpha_2(|e|) \tag{8}$$

$$\nabla_e V \cdot F_\gamma(e,x,u) + \nabla_x V \cdot f(x,u) \leq -\alpha_3(|e|) \tag{9}$$

for all $t \geq 0$, $e \in \mathbb{R}^n$, and $x \in \mathbb{R}^n$, where α_1, α_2 of class $\mathcal{K}_\infty$ and α_3 is continuous positive definite (A continuous function $\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is positive definite if it is null only in zero. Moreover, it is said to belong to class $\mathcal{K}$ if it is strictly increasing. It is said to belong to class $\mathcal{K}_\infty$ if it is of class $\mathcal{K}$ and also $\lim_{r\to+\infty} \alpha(r) = +\infty$. A continuous function $\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to belong to class $\mathcal{KL}$ if, for each fixed s, the mapping $\beta(r,s)$ belongs to class $\mathcal{K}$ with respect to r and, for each fixed r, the mapping $\beta(r,s)$ is decreasing with respect to s and $\lim_{s\to+\infty} \beta(r,s) = 0$.)

If the system is affected by disturbances, the performances deteriorate in such a way as to make the estimation error increase with the growth of the uncertainty. Anyway, it is expected to keep the estimation error asymptotically stable to zero without noise. This combination can be given with mathematical rigor by using the notion of ISS. Thus, in lieu of (5) we focus on

$$\begin{cases} \dot{x} = f(x,u) + g(x)\, w \\ y = h(x) + k(x)\, w \end{cases} \quad t \geq 0 \tag{10}$$

where $w(t) \in \mathbb{R}^p$ is the disturbance; $g : \mathbb{R}^n \to M_{n\times p}(\mathbb{R})$ and $k : \mathbb{R}^n \to M_{m\times p}(\mathbb{R})$ are smooth. Therefore, the dynamics of the estimation error is given by

$$\dot{e} = f(x,u) + g(x)w - \gamma(x-e, h(x) + k(x)w) =: F_\gamma(e,x,u,w) \tag{11}$$

where $F_\gamma(e,x,u,w)$ is used instead of $F_\gamma(e,x,u)$ as in (7) with a little abuse of notation. Based on the aforesaid, we say that the observer (6) is ISS if there exists a function β of class $\mathcal{KL}$ and a function χ of class $\mathcal{K}_\infty$ such that

$$|e(t)| \leq \beta\left(|e(0)|, t\right) + \chi\left(|w|_{\infty(0,t)}\right) \;\; t \geq 0 \tag{12}$$

where $|w|_{\infty(0,t)} := \operatorname*{ess\,sup}_{0\leq\tau\leq t} |w(\tau)|$. The above ISS statement can be equivalently expressed by means of an ISS Lyapunov function **[Son00]**: (12) holds if and only if there exist functions α_1, α_2 of class $\mathcal{K}_\infty$ and α_3, η of class $\mathcal{K}$ such that

$$\alpha_1(|e|) \leq V(e,x) \leq \alpha_2(|e|) \tag{13}$$

$$\nabla_e V \cdot F_\gamma(e,x,u,w) + \nabla_x V \cdot f(x,u) \leq -\alpha_3(|e|) \quad \text{if} \quad |e| \geq \eta(|w|) \tag{14}$$

for all $t \geq 0,\ e \in \mathbb{R}^n,\ w \in \mathbb{R}^q,\ x \in \mathbb{R}^n$, and $u \in \mathbb{R}^p$. The observer problem needs to be more reliably formulated in an ISS framework since a system may admit a Lyapuonv function in a noise-free case, while being not ISS. By contrast, an input-to-state stable system is asymptotically stable to zero if the external input is null. As pointed out in [**SJT03**], small noises can cause the instability of the estimation error and thus an observer with a globally asymptotically stable error may exist in the absence of disturbances, whereas the error dynamics turns out to be not ISS, as shown the following nice example presented in [**SL15**].

4.1.1. Example. — Considering for the system (Example 3, p.50, [**SL15**])

$$\left\{\begin{array}{rcl} \dot{x}_1 &=& -x_1 + 2 \\ \dot{x}_2 &=& x_1 x_3 \\ \dot{x}_2 &=& -x_1 x_2 + u \\ y_1 &=& x_1 + w_1 \\ y_2 &=& x_2 + w_2 \end{array}\right. \tag{15}$$

with $u(t) = \sin(t)$, the observer

$$\left\{\begin{array}{rcl} \dot{\hat{x}}_1 &=& -\hat{x}_1 + 2 + y_1 - \hat{x}_1 \\ \dot{\hat{x}}_2 &=& \hat{x}_1 \hat{x}_3 + y_1(y_2 - \hat{x}_2) \\ \dot{\hat{x}}_3 &=& -\hat{x}_1 \hat{x}_2 + u + y_1(y_2 - \hat{x}_2) \end{array}\right. \tag{16}$$

provides an estimation error that is asymptotically stable to zero if $w_1(t) = w_2(t) = 0$ for all $t \geq 0$. If, instead, we chose $x_1(0) = 1$, $w_1(t) = -x_1(t)$, and $w_2(t) = 0$ for all $t \geq 0$, it follows that

$$\lim_{t \to +\infty} w_1(t) = -2 \qquad \lim_{t \to +\infty} w_2(t) = 0$$

and the state is bounded, but the dynamics of the observer turns out to be with $\hat{x}_1(t) = 1$ for all $t \geq 0$ and

$$\left\{\begin{array}{rcl} \dot{\hat{x}}_2 &=& \hat{x}_3 \\ \dot{\hat{x}}_3 &=& -\hat{x}_2 + \sin(t) \end{array}\right.$$

and hence the second and third observer state variables are divergent, thus showing that ISS for the estimation error does not hold since the estimation error is unbounded with a bounded disturbance.

The above example suggests constructing observers together with an ISS Lyapunov function for the dynamics of the associated estimation error. Toward this end, instead of (14), let us

consider the equivalent inequality

$$\nabla_e V \cdot F_\gamma(e,x,u,w) + \nabla_x V \cdot f(x,u) \leq -\alpha_3(|e|) + \alpha_4(|w|) \tag{17}$$

where α_3, α_4 are of class $\mathcal{K}_\infty$. Once the ISS Lyapunov functions are chosen, one may analyze the effect of attenuation and the disturbances on the estimation error. Thus, using (17), let us consider

$$V(e(t),x(t)) - V(e(t_0),x(t_0)) \leq -\int_{t_0}^{t} \alpha_3(|e(s)|)ds + \int_{t_0}^{t} \alpha_4(|w(s)|)ds \tag{18}$$

for all $t \geq t_0 \geq 0$, which provides an upper bound on $V(e(t),x(t))$ based on the initial conditions and a measure of the "energy" of the noises. If V is a continuously differentiable function, (18) holds if (17) is satisfied. The function V is thus a storage function, while α_3 and α_4 have to be regarded as dissipation and supply rates, respectively. If $w(\cdot)$ and $e(\cdot)$ belong to the L_2 space of functions of time, the link between ISS and the H_∞ approach is easily found **[GSW99]**. Let us now focus on the case with the dynamics of the estimation error affine in the noises.

4.1.2. Theorem. — *Consider the observer (6) for (10) such that*

$$F_\gamma(e,x,u,w) = H_\gamma(e,x,u) + G_\gamma(e,x)w \tag{19}$$

where $H_\gamma : \mathbb{R}^{2n} \to \mathbb{R}^n$ *and* $G_\gamma : \mathbb{R}^{2n}\times \to M_{n\times p}(\mathbb{R})$. *If there exists a continuously differentiable function* $(e,x) \mapsto V(e,x)$ *such that (8) is satisfied for some functions* α_1, α_2 *of class* $\mathcal{K}_\infty$ *and the Hamilton–Jacobi inequality*

$$\nabla_e V \cdot H_\gamma(e,x) + \frac{|\nabla_e V \cdot G_\gamma(e,x) + \nabla_x V \cdot g(x)|^2}{2\mu^2} + \nabla_x V \cdot f(x,u) + \frac{|e|^2}{2} \leq 0 \tag{20}$$

holds for some $\mu > 0$ *and all* $t \geq 0$, $x \in \mathbb{R}^n$, $u \in \mathbb{R}^p$, *and* $e \in \mathbb{R}^n$. *Then,* $V(e,x)$ *is an ISS Lyapunov function and the* L_2 *to* L_2 *dissipative inequality (18) is satisfied with* $\alpha_3(r) = \frac{1}{2}r^2$, $\alpha_4(r) = \frac{\mu^2}{2}r^2$, *i.e.,*

$$V(e(t),x(t)) - V(e(t_0),x(t_0)) \leq -\frac{1}{2}\int_{t_0}^{t} |e(s)|^2 ds + \frac{\mu^2}{2}\int_{t_0}^{t} |w(s)|^2 ds \tag{21}$$

for all $t \geq t_0 \geq 0$ *and thus the observer (6) is ISS.*

Proof. — From (11) and(19), we obtain

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}t}V(e,x) &= \nabla_e V\cdot H_\gamma + (\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g)w + \nabla_x V\cdot f\\
&= \nabla_e V\cdot H_\gamma + \frac{\mu^2}{2}\left(\frac{2\,(\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g)w}{\mu^2}\right) + \nabla_x V\cdot f\\
&= \nabla_e V\cdot H_\gamma + \frac{\mu^2}{2}\Bigg(-|w|^2 + \frac{2\,(\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g)w}{\mu^2} - \frac{|\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g|^2}{\mu^4}\\
&\quad + \frac{|\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g|^2}{\mu^4} + |w|^2\Bigg) + \nabla_x V\cdot f\\
&= \nabla_e V\cdot H_\gamma - \frac{\mu^2}{2}\left|w - \frac{\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g}{\mu^2}\right|^2 + \frac{|\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g|^2}{2\mu^2} + \nabla_x V\cdot f + \frac{\mu^2}{2}|w|^2\\
&\le \nabla_e V\cdot H_\gamma + \frac{|\nabla_e V\cdot G_\gamma + \nabla_x V\cdot g|^2}{2\mu^2} + \nabla_x V\cdot f + \frac{\mu^2}{2}|w|^2\,.
\end{aligned}$$

Using (20), the previous inequality yields

$$\frac{\mathrm{d}}{\mathrm{d}t}V(e,x) \le -\frac{1}{2}|e|^2 + \frac{\mu^2}{2}|w|^2 \tag{22}$$

and hence we can conclude about ISS with (21) as a final result. □

We say that the observer admits an L_2-gain μ w.r.t. w if (21) holds. Clearly, a small gain is preferable since it entails a stronger noise attenuation. In the following, we will analyze how to take care of the Hamilton–Jacobi inequality (20), starting with the following example.

4.1.3. Example. — Let us consider

$$\left\{\begin{array}{rcl}\dot{x}_1 &=& x_1 + \sin(x_2)\,w\\ \dot{x}_2 &=& x_1 - 2\,x_2 + \exp(-x_2)\\ y &=& x_1 + x_2\end{array}\right. \tag{23}$$

and let

$$\left\{\begin{array}{rcl}\dot{\hat{x}}_1 &=& \hat{x}_1 + 2\,(y - \hat{x}_1 - \hat{x}_2)\\ \dot{\hat{x}}_2 &=& \hat{x}_1 - 2\,\hat{x}_2 + \exp(-\hat{x}_2) - (y - \hat{x}_1 - \hat{x}_2)\end{array}\right. \tag{24}$$

be a candidate observer for (23). It is straightforward to obtain

$$\dot{e} = H(e,x) + G(e,x)\,w$$

where

$$H(e,x) = \begin{pmatrix} -e_1 - 2e_2 \\ 2e_1 - e_2 + \exp(-x_2)\,(1-\exp(e_2)) \end{pmatrix}$$
$$G(e,x) = \begin{pmatrix} \sin(x_2) \\ 0 \end{pmatrix}.$$

Let us consider $V(e) = \frac{1}{2}\,e_1^2 + \frac{1}{2}\,e_2^2$ as a candidate ISS Lyapunov function. We have

$$\nabla_e V \cdot H + \frac{(\nabla_e V \cdot G)^2}{2\mu^2} + \frac{|e|^2}{2} = -\frac{1}{2}\,e_1^2 - \frac{1}{2}\,e_2^2 + \exp(-x_2)\,(1-\exp(e_2))\,e_2 + \frac{\sin(x_2)^2}{2\mu^2}\,e_1^2\,. \tag{25}$$

Since $\exp(-x_2)\,(1-\exp(e_2))\,e_2 \leq 0$, $\forall e_2, x_2 \in \mathbb{R}$, and $\sin(x_2)^2 \leq 1$, $\forall x_2 \in \mathbb{R}$, (25) yields

$$\nabla_e V \cdot H + \frac{(\nabla_e V \cdot G)^2}{2\mu^2} + \frac{|e|^2}{2} = -\frac{1}{2}\left(1 - \frac{1}{\mu^2}\right) e_1^2 - \frac{1}{2}\,e_2^2 < 0$$

for $e \neq 0$ if $\mu > 1$. Thus, observer (24) is ISS with an L_2-gain larger than 1.

The next section regards the application of what has been presented so far to observers for a class of polynomial systems.

4.2. State Observers for Polynomial Systems

After choosing a given observer structure, the problem reduces to find an ISS Lyapunov function that satisfies (20). Unfortunately, the satisfaction of conditions like (20) is not easy to be attained, which has motivated the investigation on the weaker notion of practical L_2-gain such as proposed in **[RA02]**. We will address the problem of constructing observers with practical L_2-gain for a class of polynomial systems.

More specifically, instead of (10), let us focus on

$$\begin{cases} \dot{x} = A\,x + f(x) + g(x)\,w \\ y = C\,x + k(x)\,w \end{cases}, \; t \geq 0 \tag{26}$$

where $A \in \mathbb{R}^{n\times n}$, $C \in \mathbb{R}^{m\times n}$, $f(x) \in \mathbb{R}[x]^{n\times n}$, $g(x) \in \mathbb{R}[x]^{n\times p}$, $k(x) \in \mathbb{R}[x]^{m\times p}$, and the pair (A, C) is detectable. To estimate the state, we rely on observers given by

$$\dot{\hat{x}} = A\,\hat{x} + f(\hat{x}) + L(y - C\,\hat{x}),\; t \geq 0 \tag{27}$$

with the gain $L \in \mathbb{R}^{n\times m}$ chosen such that $A - LC$ has eigenvalues with a strictly negative real part. Such a condition can be satisfied owing to the detectability assumption and ensures that the estimation error dynamics

$$\dot{e} = (A - LC)\, e + f(x) - f(\hat{x}) + (g(x) - L\, k(x))\, w \tag{28}$$

is locally asymptotically stable to zero in the absence of noise, i.e., with $w(t) \equiv 0$ for all $t \geq 0$. More specifically, we have

$$\dot{e} = (A - LC)\, e + f(x) - f(x - e)\,.$$

In the noisy setting, for the sake of brevity, let us rewrite (28) as

$$\dot{e} = H(e, x, L) + G(x, L)\, w$$

with

$$H(e, x, L) := (A - LC)\, e + f(x) - f(x - e) \in \mathbb{R}[x, e]^{n\times 1} \qquad G(x, L) := g(x) - L\, k(x) \in \mathbb{R}[x]^{n\times p}\,.$$

Therefore, it is convenient to search for a polynomial ISS Lyapunov function $V(e, x)$ such that (21) holds for some $\mu > 0$. Given a candidate Lyapunov function, we may apply the SOS decomposition of such a function and of the opposite of its time derivative by using a positivity certification, which does not depend on the characteristics of the chosen polynomial since the following holds **[BPT13, Las15]** .

4.2.1. Theorem. — *A polynomial $p(e) \in \mathbb{R}[e]^{2d}$ in $e = (e_1, \ldots, e_n) \in \mathbb{R}^n$ has sum-of-squares decomposition (or is said to be SOS) if and only if there exists a real symmetric and positive semidefinite matrix $P \in \mathbb{R}^{s(d)\times s(d)}$ such that $p(e) = v_d(e)^\top P\, v_d(e)$, where $v_d(e)$ is the vector of all the monomials in the components of $e \in \mathbb{R}^n$ of degree equal to or less than $d \in \mathbb{N}$, i.e.,*

$$v_d(e) := (1, e_1, \ldots, e_n, e_1e_2, \ldots, e_{n-1}e_n, e_n^2, \ldots, e_1^d, \ldots, e_n^d)$$

of dimension

$$s(d) := \left(\begin{smallmatrix} n+d \\ d \end{smallmatrix} \right).$$

Proof. — See (Proposition 2.1, p. 17, **[Las10]**). □

Thus, from now on, we will refer to well-established definitions as follows **[PPPP02]**. A polynomial $p(e) \in \mathbb{R}[e]^{2d}$ is ε-SOS polynomial if $p(e) - \varepsilon \sum_{i=1}^{n} e_i^2 \in \mathbb{R}[e]^{2d}$ with $d \in \mathbb{N}$, $d \geq 1$ is SOS for some "small" tolerance $\varepsilon > 0$. In addition, a polynomial, square matrix $M(x)$ with $M_{ij}(x) \in \mathbb{R}[x]$ for $i, j = 1, \ldots, s(d)$ is said to be an ε-SOS matrix if the bipartite polynomial $p(e, x) := v_d(e)^\top M(x) v_d(e)$ is ε-SOS for all $x \in \mathbb{R}^n$. In this respect, $p(e, x)$ is said to be a bipartite ε-SOS polynomial.

4.2.2. Theorem. — *Consider observer (27) for system (26). If there exist a bipartite ε-SOS $V(e, x)$ and $\mu > 0$ such that*

$$\eta(e,x)^\top \Pi_e^\top H(e,x,L) + \eta(e,x)^\top \Pi_x^\top (Ax + f(x)) + |\eta(e,x)|^2 + \frac{|e|^2}{2} \leq 0 \tag{29}$$

$$\begin{pmatrix} 2I & \Pi_e^\top G(x,L) + \Pi_x^\top g(x) \\ G(x,L)^\top \Pi_e + g(x)^\top \Pi_x & \mu^2 I \end{pmatrix} > 0 \tag{30}$$

for all $x \in \mathbb{R}^n$ and $e \in \mathbb{R}^n$, where $\eta(e, x) \in \mathbb{R}^q$ is the column vector of all the monomials in e and x appearing in $\nabla_e V(e, x)$ and $\nabla_x V(e, x)$ with $\Pi_e, \Pi_x \in \mathbb{R}^{n \times q}$ such that

$$\nabla_e V(e,x) = \Pi_e \, \eta(e,x) \qquad \nabla_x V(e,x) = \Pi_x \, \eta(e,x)\,. \tag{31}$$

Then, observer (27) is ISS with L_2-gain equal to μ.

Proof. — The proof is line with **[Reh15]**. The time derivative of $V(e, x)$ is given by

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}t} V(e,x) &= \nabla_e V(e,x) \cdot H(e,x,L) + \nabla_e V(e,x) \cdot (G(x,L)w) + \nabla_x V(e,x) \cdot (Ax + f(x)) \\ &+ \nabla_x V(e,x) \cdot (g(x)w) \end{aligned}$$

and, using (31), we obtain

$$\frac{\mathrm{d}}{\mathrm{d}t} V(e,x) = \eta(e,x)^\top \Pi_e^\top H(e,x,L) + \eta(e,x)^\top \Pi_x^\top (Ax + f(x)) + \eta(e,x)^\top \left(\Pi_e^\top G(x,L) + \Pi_x^\top g(x) \right) w \tag{32}$$

Using (Lemma 4.2, p. 861 in **[Reh15]**), from (30), it follows that

$$\eta(e,x)^\top \left(\Pi_e^\top G(x,L) + \Pi_x^\top g(x) \right) w \leq \eta(e,x)^\top \eta(e,x) + \frac{\mu^2}{2} w^\top w$$

and, after replacing this upper bound in (32), it follows that (22) (see the proof of Theorem 4.1.2) holds if (29) is satisfied, which allows for concluding. □

Based on the aforesaid, one can proceed with the observer design. Let be $d \in \mathbb{N}$ with $d \geq 1$ and $\varepsilon > 0$, and the problem to solve is the following.

4.2.3. Problem. — Find a bipartite ε-SOS $V(e,x)$, $L \in \mathbb{R}^{n\times m}$, and $\mu \geq 0$ such that (29) and (30) hold and μ is minimized.

Indeed, the available SOS tools do not allow for solving Problem 4.2.3. Thus, we will address the observer design by relying on the so-called practical L_2-gain proposed in [**RA02**]. However, first of all consider the pure linear case by dealing with (26) without $f(x)$ and with $g(x)$ and $k(x)$ being real matrices, as follows:

$$\left\{ \begin{array}{l} \dot{x} = A\,x + D\,w \\ y = C\,x + E\,w \end{array} \right. \quad t \geq 0$$

where the pair (A, C) is detectable, $D \in \mathbb{R}^{n\times p}$, and $E \in \mathbb{R}^{m\times p}$. The observer equation is as follows:

$$\dot{\hat{x}} = A\,\hat{x} + L(y - C\,\hat{x})\ t \geq 0\,.$$

Since the dynamics of the estimation error is

$$\dot{e} = (A - LC)e + (D - LE)w$$

and, after a little algebra and using the Schur complement ([**BBFG94**]), (20) becomes

$$\left(\begin{array}{cc} AP - C^\top Y^\top + PA - YC + \frac{I}{2} & PD - Y\ E \\ (PD - YE)^\top & -\frac{\mu^2}{2} I \end{array} \right) < 0$$

with $P = P^\top \in \mathbb{R}^{n\times n}, P > 0$ and $Y = PL \in \mathbb{R}^{n\times m}$. Since the pair (A, C) is detectable, the above linear matrix inequality (LMI) admits a solution in P and Y, and it follows $L = P^{-1}Y$. Moreover, using popular LMI-based tools [**BBFG94**], it is straightforward to minimize μ^2 exactly since the problem is convex. Thus, one may search for approximate solutions to Problem 4.2.3 for (26) and (27) by relying on the solution obtained by neglecting the nonlinearities, which thus holds only locally. Thus, instead of Problem 4.2.3, let us consider the much simpler LMI problem

$$\min \delta \quad \text{w.r.t.} \quad Y, P > 0, \delta > 0 \tag{33a}$$

$$\left(\begin{array}{cc} AP - C^\top Y^\top + PA - YC + \frac{I}{2} & PD - YE \\ (PD - YE)^\top & -\frac{\delta}{2} I \end{array} \right) < 0\,. \tag{33b}$$

After finding the solution denoted by Y^*, P^*, δ^*, the gain is given by $L^* = (P^*)^{-1}Y^*$, which provides a local L_2-gain $\mu = \sqrt{\delta^*}$ with the Lyapunov function $V(e) = e^\top P^* e$ for (26) and (27). Since it is difficult to ensure a constant L_2-gain over all the operating points, we will rely on the notion of practical L_2-gain proposed in [**RA02**]. Based on the practical L_2-gain, one can

overcome the problem of finding a globally fixed L_2-gain. More specifically, assume that there exists a bipartite ε-SOS function $V(e,x)$ such that

$$\nabla_e V \cdot H(e,x,L^*) + \nabla_x V \cdot (Ax + f(x)) + \frac{|e|^2}{2} < 0 \tag{34}$$

for $e \neq 0$, then

$$\nabla_e V \cdot H(e,x,L^*) + \frac{|\nabla_e V \cdot G(x,L^*) + \nabla_x V \cdot g(x)|^2}{2\mu(e,x)^2} + \nabla_x V \cdot (Ax + f(x)) + \frac{|e|^2}{2} \leq 0 \tag{35}$$

holds if $(e,x) \mapsto \mu(e,x) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ is chosen such that

$$\mu(e,x) \geq \mu(e,x)^* := \frac{|\nabla_e V \cdot G(x,L^*) + \nabla_x V \cdot g(x)|}{\sqrt{-2\nabla_e V \cdot H(e,x,L^*) - 2\nabla_x V \cdot (Ax + f(x)) - |e|^2}} \tag{36}$$

and thus $\mu(e,x)^*$ is referred to as practical L_2-gain. Based on the aforesaid, the problem to solve reduces to the following.

4.2.4. Problem. — Given $L^* \in \mathbb{R}^{n\times m}$ as a solution of (33), find a bipartite ε-SOS $V(e,x)$ such that (34) holds.

The solution of Problem 4.2.4 allows for adopting a more flexible notion of attenuation w.r.t. the noises by using an L_2-gain that may depend on both e and x. Following the same reasoning of the proof of Theorem 4.1.2, instead of (22), we obtain

$$\frac{\mathrm{d}}{\mathrm{d}t} V(e,x) \leq -\frac{1}{2}|e|^2 + \frac{\mu(e,x)^2}{2}|w|^2 \tag{37}$$

from (35) if (34) holds with $\mu(e,x)$ subject to (36). Thus, (37) may be used whenever the L_2-gain cannot be bounded from above in the usual sense such as in Example 4.1.3, for which the lower bound given by 1 holds globally, i.e., for all e, $x \in \mathbb{R}^n$. In practice, the attenuation w.r.t. the disturbances are left to vary in the state space. Moreover, (35) is easier to be satisfied as compared with (34). Indeed, additional constraints can be introduced by constraining the estimation error to belong to suitable compact sets and/or taking into account the boundedness of the state trajectories [**Reh15**]. This allows for facilitating feasibility when solving Problem 4.2.4.

In the next section, we will show numerical results obtained in a simulation case study.

4.3. Numerical Results

In this section, we will show how to apply the proposed approach by exploiting the polynomial structure of the system and observer equations. Thanks to the use of SOS toolbox [**PPPP02**], we will find an ISS polynomial Lyapunov function, which guarantees stability, as illustrated so far. The numerical results are obtained by dealing with the Van der Pol oscillator, which is an interesting example of a polynomial system with a stable limit cycle ([**Kha02**]) and is thus well-suited for the purpose of testing.

Let us consider a system with two coupled Van der Pol oscillators with the first and third state variable as outputs, i.e.,

$$\begin{cases} \dot{x} = A\,x + f(x) + D\ w \\ y = C\,x + Ew \end{cases}$$

where $x \in \mathbb{R}^4$, $w \in \mathbb{R}^4$, $y \in \mathbb{R}^2$,

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 1 \end{pmatrix} \qquad f(x) = \begin{pmatrix} 0 \\ -x_1^2 x_2 \\ 0 \\ -x_3^2 x_4 \end{pmatrix} \qquad D = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad E = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The observer is thus given by

$$\dot{\hat{x}} = A\,\hat{x} + f(\hat{x}) + L(y - C\,\hat{x})$$

with the gain

$$L = \begin{pmatrix} 3.0189 & 0.2703 \\ 3.9558 & 0.6106 \\ 0.2703 & 3.0189 \\ 0.6106 & 3.9558 \end{pmatrix}$$

obtained by solving (33) with Yalmip [**Lf04**]. The solution provides a value of μ equal to 4.6575. Using the SOS toolbox [**PPPP02**], we solved Problem 4.2.4 with $\varepsilon = 10^{-9}$ and additional

constraints $e \in B_r(\sqrt{10})$ and $x \in B_r(10)$, thus obtaining the Lyapunov function

$$
\begin{aligned}
V(e,x) = {} & -1.0962\text{e}{-10}\, e_1 e_2 x_1^2 + 2.0092\text{e}{-11}\, e_1 e_4 x_3^2 + 2.6663\text{e}{-10}\, e_2^2 x_1^2 + 2.6452\text{e}{-12}\, e_2 e_3 x_1^2 \\
& - 4.5329\text{e}{-11}\, e_2 e_4 x_1^2 + 2.2772\text{e}{-11}\, e_2 e_4 x_3^2 + 7.7374\text{e}{-11}\, e_3 e_4 x_3^2 - 2.8571\text{e}{-10}\, e_4^2 x_3^2 + 4.3459\text{e}{-6}\, e_1^2 \\
& - 2.0934\text{e}{-6}\, e_1 e_2 - 1.3632\text{e}{-7}\, e_1 e_3 - 1.6176\text{e}{-7}\, e_1\, e_4 + 8.6434\text{e}{-7}\, e_2^2 - 1.6176\text{e}{-7}\, e_2 e_3 + 3.9843\text{e}{-8}\, e_2 e_4 \\
& + 4.3459\text{e}{-6}\, e_3^2 - 2.0934\text{e}{-6}\, e_3 e_4 + 8.6435\text{e}{-7}\, e_4^2
\end{aligned}
$$

which certifies that this observer is ISS.

BIBLIOGRAPHY

[ABCR20] A. Alessandri, P. Bagnerini, R. Cianci, and R. Revetria, *Modeling and estimation of thermal flows based on transport and balance equations*, Advances in Mathematical Physics **2020** (2020), 1–10.

[AKP11] A. A. Ahmadi, M. Krstic, and P. A. Parrilo, *A globally asymptotically stable polynomial vector field with no polynomial lyapunov function*, 2011 50th IEEE Conference on Decision and Control and European Control Conference, 2011, pp. 7579–7580.

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969)., 1969.

[Arn92] V. I. Arnol'd, *Ordinary differential equations. Transl. from the 3rd Russian ed. by Roger Cooke*, Berlin etc.: Springer-Verlag, 1992.

[Bai80] J. Baillieul, *The geometry of homogeneous polynomial dynamical systems*, Nonlinear Anal., Theory Methods Appl. **4** (1980), 879–900.

[Bai81] ———, *Controllability and observability of polynomial dynamical systems*, Nonlinear Anal., Theory Methods Appl. **5** (1981), 543–552.

[Bar95] Z. Bartosiewicz, *Local observability of nonlinear systems*, Syst. Control Lett. **25** (1995), no. 4, 295–298.

[Bar99] ———, *Real analytic geometry and local observability*, Differential geometry and control. Proceedings of the Summer Research Institute, Boulder, CO, USA, June 29–July 19, 1997, Providence, RI: American Mathematical Society, 1999, pp. 65–72.

[Bar16] ———, *Algebraic criteria of global observability of polynomial systems*, Automatica **69** (2016), 210–213.

[BBFG94] Saxon Boyd, Venkataramanan Balakrishnan, E. Feron, and L. Ghaoui, *Linear matrix inequalities in control theory*, 01 1994, pp. 31 – 34 vol.1.

[BCR98] J. Bochnak, M. Coste, and M.-F. Roy, *Real algebraic geometry. Transl. from the French.*, vol. 36, Berlin: Springer, 1998.

[BN93] E. Becker and R. Neuhaus, *Computation of real radicals of polynomial ideals*, Computational algebraic geometry. Papers from a conference, held in Nice, France, April 21–25, 1992, Boston: Birkhäuser, 1993, pp. 1–20.

[Bor94] F. Borceux, *Handbook of categorical algebra. 1*, Encyclopedia of Mathematics and its Applications, vol. 50, Cambridge University Press, Cambridge, 1994, Basic category theory.

[Bos18] S. Bosch, *Algebra. From the viewpoint of Galois theory. Translation and critical revision of the eighth German edition*, Cham: Birkhäuser, 2018.

[BPR06] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in real algebraic geometry*, vol. 10, Berlin: Springer, 2006.

[BPT13] Grigoriy Blekherman, Pablo A. Parrilo, and Rekha R. Thomas (eds.), *Semidefinite optimization and convex algebraic geometry*, MOS/SIAM Ser. Optim., vol. 13, Philadelphia, PA: Society for Industrial and Applied Mathematics (SIAM), 2013 (English).

[BR05] A. Bacciotti and L. Rosier, *Liapunov functions and stability in control theory*, Berlin: Springer, 2005.

[CHS10] D. Cheng, X. Hu, and T. Shen, *Analysis and design of nonlinear control systems.*, Berlin: Springer; Beijing: Science Press, 2010.

[CLO15] D.A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, Cham: Springer, 2015.

[Coh03] P. M. Cohn, *Basic algebra*, Springer-Verlag London, Ltd., London, 2003, Groups, rings and fields. MR 1935285

[Col75] George E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975), 1975, pp. 134–183. Lecture Notes in Comput. Sci., Vol. 33. MR 0403962

[Col98] G. E. Collins, *Quantifier elimination by cylindrical algebraic decomposition – twenty years of progress*, Quantifier elimination and cylindrical algebraic decomposition. Proceedings of a symposium, Linz, Austria, October 6–8, 1993, Wien: Springer, 1998, pp. 8–23.

[DE70] D. W. Dubois and G. Efroymson, *Algebraic theory of real varieties. I*, Stud. and Essays Presented to Yu-Why Chen on his 60-th Birthday, 107-135 (1970), 1970.

[Dub70] D. W. Dubois, *A nullstellensatz for ordered fields*, Ark. Mat. **8** (1970), 111–114.

[Eis95] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, vol. 150, Berlin: Springer-Verlag, 1995.

[GSW99] Lars Grne, Eduardo Sontag, and Fabian Wirth, *Asymptotic stability equals exponential stability, and iss equals finite energy gain - if you twist your eyes*, Systems Control Letters **38** (1999), 127–134.

[Hah67] W. Hahn, *Stability of motion. Translated by Arne P. Baartz*, vol. 138, Springer, Berlin, 1967.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[HK77] R. Hermann and A. J. Krener, *Nonlinear controllability and observability*, IEEE Trans. Autom. Control **22** (1977), 728–740.

[Ino77] Yujiro Inouye, *On the observability of autonomous nonlinear systems*, J. Math. Anal. Appl. **60** (1977), no. 1, 236–247. MR 444141

[Isi95] A. Isidori, *Nonlinear control systems.*, Berlin: Springer, 1995.

[Isi99] ———, *Nonlinear control systems. II*, London: Springer, 1999.

[Kai80] T. Kailath, *Linear systems*, Prentice Hall, Englewood Cliffs, NJ, 1980.

[Kha02] H. K. Khalil, *Nonlinear systems.*, Upper Saddle River, NJ: Prentice Hall, 2002.

[KO13] Y. Kawano and T. Ohtsuka, *Observability at an initial state for polynomial systems*, Automatica **49** (2013), no. 5, 1126–1136.

[KR00] M. Kreuzer and L. Robbiano, *Computational commutative algebra. I*, Berlin: Springer, 2000.

[KR05] ———, *Computational commutative algebra. II*, Berlin: Springer, 2005.

[Kri64] J.-L. Krivine, *Anneaux préordonnés*, J. Analyse Math. **12** (1964), 307–326. MR 175937

[Kun85] E. Kunz, *Introduction to commutative algebra and algebraic geometry. Transl. from the German by Michael Ackerman. With a preface by David Mumford*, Boston-Basel-Stuttgart: Birkhäuser. X, 238 p. DM 98.00 (1985)., 1985.

[Lak87] D. Laksov, *Radicals and Hilbert Nullstellensatz for not necessarily algebraically closed fields*, Enseign. Math. (2) **33** (1987), 323–338.

[Lam84] T. Y. Lam, *An introduction to real algebra*, Rocky Mt. J. Math. **14** (1984), 767–814.

[Lan02] S. Lang, *Algebra.*, vol. 211, New York, NY: Springer, 2002.

[Las10] J. B. Lasserre, *Moments, positive polynomials and their applications*, vol. 1, London: Imperial College Press, 2010.

[Las15] Jean-Bernard Lasserre, *An introduction to polynomial and semi-algebraic optimization*, 02 2015.

[Lei10] R. I. Leine, *The historical development of classical stability concepts: Lagrange, Poisson and Lyapunov stability*, Nonlinear Dyn. **59** (2010), no. 1-2, 173–182.

[LLM+13] J. B. Lasserre, M. Laurent, B. Mourrain, P. Rostalski, and P. Trébuchet, *Moment matrices, border bases and real radical computation*, J. Symb. Comput. **51** (2013), 63–85.

[Lf04] Johan Lfberg, *Yalmip: A toolbox for modeling and optimization in matlab*, vol. 2004, 01 2004.

[Mac98] S. Mac Lane, *Categories for the working mathematician*, second ed., Graduate Texts in Mathematics, vol. 5, Springer-Verlag, New York, 1998.

[Mas49] J. L. Massera, *On Liapounoff's conditions of stability*, Ann. Math. (2) **50** (1949), 705–721.

[Mas56] ———, *Contributions to stability theory*, Ann. Math. (2) **64** (1956), 182–206.

[Mas58] ———, *Erratum: Contributions to stability theory*, Ann. Math. (2) **68** (1958), 202.

[Mor96] P. Morandi, *Field and Galois theory*, vol. 167, New York, NY: Springer, 1996.

[Nes98] D. Nesić, *A note on observability tests for general polynomial and simple Wiener-Hammerstein systems*, Syst. Control Lett. **35** (1998), no. 4, 219–227.

[Neu98] R. Neuhaus, *Computation of real radicals of polynomial ideals. II*, J. Pure Appl. Algebra **124** (1998), no. 1-3, 261–280.

[Nv90] H. Nijmeijer and A. van der Schaft, *Nonlinear dynamical control systems*, New York etc.: Springer-Verlag, 1990.

[PPPP02] Stephen Prajna, Antonis Papachristodoulou, Pablo Parrilo, and Samani Prajna, *Sum of squares optimization toolbox for matlab*.

[PS94] C. D. Pagani and S. Salsa, *Analisi matematica. Vol. 1-2*, Milano: Ed. Masson, 1994 (Italian).

[PSV84] L. C. Piccinini, G. Stampacchia, and G. Vidossich, *Ordinary differential equations in R^n. Problems and methods. Transl. from the Italian by A. LoBello*, vol. 39, Springer, Cham, 1984.

[RA02] Alain Rapaport and Alessandro Astolfi, *Practical L_2 disturbance attenuation for nonlinear systems*, Automatica **38** (2002), no. 1, 139–145 (English).

[Reh15] Branislav Rehak, *Sum-of-squares based observer design for polynomial systems with a known fixed time delay*, Kybernetika **51** (2015), 856–873.

[Ris70] J.-J. Risler, *Une caractérisation des idéaux des variétés algébriques réelles*, C. R. Acad. Sci., Paris, Sér. A **271** (1970), 1171–1173 (French).

[Rob63] Abraham Robinson, *Introduction to model theory and to the metamathematics of algebra*, North-Holland Publishing Co., Amsterdam, 1963. MR 0153570

[San91] Tomas Sander, *Existence and uniqueness of the real closure of an ordered field without zorn's lemma*, Journal of Pure and Applied Algebra **73** (1991), no. 2, 165–180.

[Sha90] R. Y. Sharp, *Steps in commutative algebra*, vol. 19, Cambridge etc.: Cambridge University Press, 1990.

[Sha13] I. R. Shafarevich, *Basic algebraic geometry 1. Varieties in projective space. Translated from the Russian by M. Reid*, Berlin: Springer, 2013.

[SJT03] Hyungbo Shim, Seo J.H, and A.R. Teel, *Nonlinear observer design via passivation of error dynamics*, Automatica **39** (2003), 885–892.

[SL15] Hyungbo Shim and Daniel Liberzon, *Nonlinear observers robust to measurement disturbances in an iss sense*, IEEE Transactions on Automatic Control **61** (2015), 1–1.

[Son79a] E. D. Sontag, *On the observability of polynomial systems. I: Finite-time problems*, SIAM J. Control Optim. **17** (1979), 139–151.

[Son79b] ———, *Polynomial response maps*, vol. 13, Springer, Cham, 1979.

[Son98] ———, *Mathematical control theory. Deterministic finite dimensional systems.*, vol. 6, New York, NY: Springer, 1998.

[Son00] Eduardo Sontag, *The iss philosophy as a unifying framework for stability-like behavior*, The ISS Philosophy As A Unifying Framework for Stability-like Behavior (2000).

[SR76] E. D. Sontag and Y. Rouchaleau, *On discrete-time polynomial systems*, Nonlinear Anal., Theory Methods Appl. **1** (1976), 55–64.

[Tar48] Alfred Tarski, *A Decision Method for Elementary Algebra and Geometry*, RAND Corporation, Santa Monica, Calif., 1948. MR 0028796

[Tes12] G. Teschl, *Ordinary differential equations and dynamical systems*, vol. 140, Providence, RI: American Mathematical Society (AMS), 2012.

[Tib04] B. Tibken, *Observability of nonlinear systems - an algebraic approach*, 2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601), vol. 5, 2004, pp. 4824–4825 Vol.5.

[Tur98] G. Turchetti, *Dinamica classica dei sistemi fisici*, Zanichelli Editore, S.p.A., Bologna, 1998 (Italian).

[War83] F. W. Warner, *Foundations of differentiable manifolds and Lie groups. Reprint*, vol. 94, Springer, New York, NY, 1983.