REAL ALGEBRA FROM HILBERT'S 17th PROBLEM

José F. Fernando
J. Manuel Gamboa

Preface

We collect in this survey part of the lectures held in Madrid (by both authors) and Pisa (by the first author) in postgraduate courses on Real Algebraic Geometry. It is not easy to present something new concerning this subject, because there is a lot of high qualified material developed by several remarkable researchers in Real Algebra and Real Geometry along the last thirty years. Nevertheless, we have tried to provide a non absolutely standard presentation of several aspects concerning Artin-Lang's Theorem, the Real Nullstellensatz, the Positivstellentsätze and the intrinsic relations among them and with the pair formed by the polynomial Łojasiewicz's inequality and a strong version of Hilbert's 17th Problem for polynomials. Moreover, we approach a soft study of the Zariski and real spectra of a ring, and we apply this to analyze the main properties of the so called polynomial Stone–Čech compactification of $\mathbb{R}^n$.

We have tried to contextualize historically many of the presented results and some other related ones. We are conscious that we have forgotten the important contributions in this area of many relevant mathematicians who have not been recognized in these notes as much as they deserve. Our last purpose is to offend somebody; this is why we would like to apologize in advance for our ignorance and our wrong viewpoint in all the situations in which this happens.

Many members of the group working in Real Algebraic and Analytic Geometry at the UCM in Madrid (current researching contract MTM2011-22435), but specially the first author of these notes, are in debt with the group of Real Algebraic and Analytic Geometry of the Dipartimento di Matematica dell'Università di Pisa. A great part of the postdoctoral training in Real Analytic Geometry of the first author has been performed in the Dipartimento di Matematica di Pisa during the last ten years. He has worked together with Prof. Acquistapace and Prof. Broglia, among other matters, in several fruitful attempts to get a better understanding of the obstructions for a positive solution to Hilbert's 17th Problem in the global analytic case, to provide local-global criteria to have some kind of Positivstellensätze in the global analytic case and, right now, to present a kind of Nullstellensatz involving Łojasiewicz's inequality as was already done by other authors in the past in different contexts. This is why a big amount of his recent research and learning is located in

this department in a close collaboration with his colleges (and of course his friends) Francesca (Prof. Acquistapace) and Fabrizio (Prof. Broglia).

Apart form the extraordinary ambient to perform research in the Dipartimento di Matematica dell'Università di Pisa and all the facilities that he has received to work there from his first postdoctoral stay in 2003, the first author would like to thank the enormous affect that he has always received during the uncountable many researching stays enjoyed there. During the last ten years he enjoyed the opportunity of meeting there a great amount of very nice people (graduate students, predoctoral students, post-doctoral students, professors and other people non related with the mathematical world) who made very pleasant his frequent visits to Pisa.

The second author of these notes is, probably, the unique member of the group of real algebraic geometers working in Madrid who never enjoyed an academical stay in Pisa. However, his contact with the italian school began thirty years ago with the strong encouragement received from Prof. Alberto Tognoli. After that, he took profit of the mathematical knowledge and research resource from other italian real algebraic geometers; among them, Prof. Francesca Acquistapace and Prof. Fabrizio Broglia play an outstanding role. The contact with them in many mathematical meetings and their frequent visits to Madrid constitute a permanent source of personal and mathematical enrichment due to their extreme generosity.

Pisa & Madrid, July 2012

Jose F. Fernando & J.M. Gamboa

Table of Contents

Introduction

David Hilbert proposed in the *International Congress of Mathematicians* held at Paris in 1900, as the seventeenth of his famous list of 23 problems, the following one:

H17. Is it true that every *positive semidefinite* polynomial $f \in \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, that is, satisfying $f(x) \geq 0$ for each point $x \in \mathbb{R}^n$, is a sum of squares of *rational functions,* that is, quotients of polynomials in n variables?

The answer is affirmative, and for $n = 1$ the result is rather elementary; it follows essentially from the fact that $\mathbb{R}[\mathtt{t}]$ is a unique factorization domain whose irreducible elements of degree greater than 1 have the form $a(\mathtt{t} - b)^2 + c^2$, where a, b and c are real numbers and $c \neq 0$. Using this, we prove in Proposition 1.5 (Ch.I) a well known fact: each positive semidefinite univariate polynomial is a sum of two squares of polynomials in $\mathbb{R}[\mathtt{t}]$. On the other hand, Hilbert answered **H17** in the affirmative in [Hi] for $n = 2$, and proved the existence of positive semidefinite polynomials in two variables which are not sum of squares of polynomials in $\mathbb{R}[\mathtt{x}_1, \mathtt{x}_2]$; hence, rational functions are needed. However, Hilbert did not provided any concrete positive semidefinite polynomial which is not a sum of squares of polynomials. The first explicit example was obtained in 1967 by Motzkin, see [Mz], and it will be carefully presented in our initial analysis of Hilbert's 17th Problem.

Artin, see [Ar] and [J, VI], answered affirmatively **H17** for arbitrary n, and indeed he showed that the result holds also if $\mathbb{R}$ is replaced by a field admitting a unique ordering compatible with addition and multiplication. Artin's proof employs several ingredients: an *specialization* argument; Sturm's Theorem [Stu] and the theory of ordered fields introduced by Artin and Schreier in [AS], precisely to solve **H17.** Later on in 1953, Lang revised Artin's proof in [L1], [L2], and he presented a rather similar solution in which the specialization argument is substituted by the theory of *real places.* In 1955, Robinson obtained in [Ro] a completely new solution, using *model theoretical* techniques. In fact he proved what is known as *Artin–Lang's Theorem,* 3.5 (Ch.I), as a consequence of *Quantifier elimination Theorem* for real closed fields discovered by Tarski in 1949, [T].

It is worthwhile mentioning two important facts. First, the ideas and mathemat-

ical tools used in the different solutions of **H17** became crucial to the development of a new branch of mathematics known today as Real Algebra and Real Geometry. Second, the proofs quoted above are not constructive, that is, they do not provide an algorithm to find rational functions $f_1, \ldots, f_m$ such that $f = f_1^2 + \cdots + f_m^2$. There exist constructive approaches to **H17**, but we do not present them in these notes.

Any case, let us mention that Hilbert's solution for polynomials in two variables is constructive. Later in 1940, Habicht obtained in [H] a constructive solution for positive definite homogeneous polynomials, that is, satisfying the inequality $f(x) > 0$ for each point $x \in \mathbb{R}^n \setminus \{0\}$. Twenty years later, the logician Kreisel obtained a constructive solution in [Kr] for arbitrary n, and his student Delzell published in 1984, see [D], a constructive and continuous representation with respect to small perturbations of the coefficients.

Moreover, Delzell's solution provides representations of f as a sum of squares of rational functions $f = f_1^2 + \cdots + f_m^2$ such that the codimension of the set of zeros of a common denominator of $f_1, \ldots, f_m$ is ≥ 3. In particular, each positive semidefinite polynomial $f \in \mathbb{R}[\mathtt{x}_1, \mathtt{x}_2]$ can be written as $f = (g_1^2/g^2) + (g_2^2/g^2)$ with $g, g_1, g_2 \in \mathbb{R}[\mathtt{x}_1, \mathtt{x}_2]$ and $g(x) > 0$ for each point $x \in \mathbb{R}^2$.

Chapter I of these notes is devoted to present Artin's solution of **H17**. To that end the preliminaries concerning the theory of ordered fields are explained in Sections §1 and §2, with special emphasis focused on *real closed fields* and the existence and uniqueness of the *real closure* of an ordered field, which needs *Sturm's Theorem.* The proper solution of **H17** is the content of Section §3; in fact we prove a stronger result, namely, *Artin-Lang's Theorem* 3.5.

In Chapter II we present the Real Algebra built up around Hilbert's 17th Problem. A main goal is to provide several equivalent formulations of Artin-Lang's Theorem in Section §2. This requires to introduce previously, in Section §1, the fundamental notions of *real ring* and *prime cone* of a ring. As a consequence of Artin-Lang's Theorem, we prove in Section §3 the Real Nullstellensatz and the Positivstellensätze; these last provide us a solution of Hilbert's 17th Problem with *controlled denominators,* that we abbreviate $\mathbf{H17_c}$. In the fourth Section of this Chapter we introduce the notions of *real ideal* and *real radical* of an ideal, and we prove Łojasiewicz's polynomial inequality, denoted **Łi**. It must be pointed out that $\mathbf{H17_c}$ + **Łi** imply the Real Nullstellensatz, which is in fact equivalent to the Positivstellensätze, see Exercise 3.11.

Chapter III has a topological flavour. To begin with we study in its first section very general results about the Zariski spectrum of a commutative ring with unity and its subspace of closed points. The real spectrum of a real ring and its subspace of closed points, which are more subtle constructions, are presented in Section §2.

To finish, both spectra are compared in Section §3, where the so called Stone-Cěch polynomial compactification of $\mathbb{R}^n$ is introduced.

1 Analysis of Hilbert's 17th Problem.

This problem concerns the relationship between *positivity,* that is a geometric property, and *sums of squares,* which are algebraic formulae. With independence of the precise meaning of positivity, it seems clear that sums of squares must be *positive elements.* Thus, it seems natural to ask under what assumptions these are the only positive elements of a ring of functions.

A natural question that arises from the statement of **H17** is why one looks for representations of semidefinite polynomials as sums of squares of *rational functions* instead of sums of squares of polynomials. We have already quoted that Hilbert realized in [Hi] the existence of polynomials in two variables which are sums of squares of rational functions but they are not sums of squares of polynomials. As commented before, the first explicit example of a positive semidefinite polynomial in two variables which is not a sum of squares of polynomials is due to Motzkin, see [Mz]. This is the polynomial

$$f(\mathtt{x},\mathtt{y}) := \mathtt{x}^4\mathtt{y}^2 + \mathtt{x}^2\mathtt{y}^4 + 1 - 3\mathtt{x}^2\mathtt{y}^2.$$

In fact, for every point $(x, y) \in \mathbb{R}^2$, the arithmetic and geometric means of the real numbers x^4y^2, x^2y^4 y 1 are, respectively,

$$m_a := (x^4y^2 + x^2y^4 + 1)/3 \quad \& \quad m_g := \sqrt[3]{x^4y^2 \cdot x^2y^4 \cdot 1} = x^2y^2.$$

Since $m_a \geq m_g$, for every $(x, y) \in \mathbb{R}^2$ we have

$$f(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2 = 3(m_a - m_g) \geq 0.$$

However, f is not a sum of squares of polynomials in $\mathbb{R}[\mathtt{x},\mathtt{y}]$.

Proof. Otherwise, there would exist $f_1, \ldots, f_r \in \mathbb{R}[\mathtt{x},\mathtt{y}]$ such that

$$f := \sum_{i=1}^{r} f_i^2. \tag{1.1}$$

Since $\deg(f) = 6$, then $\deg(f_i) \leq 3$ for each $1 \leq i \leq r$. Let us divide $f_i \in \mathbb{R}[\mathtt{y}][\mathtt{x}]$ by the monic polynomial $\mathtt{x}$. Thus, there exist $q_i \in \mathbb{R}[\mathtt{x},\mathtt{y}]$ and $r_i \in \mathbb{R}[\mathtt{y}]$ satisfying $f_i = \mathtt{x}q_i + r_i$ for each $1 \leq i \leq r$, and so $f_i(0,\mathtt{y}) = r_i$. But

$$1 = f(0,\mathtt{y}) = \sum_{i=1}^{r} f_i^2(0,\mathtt{y}) = \sum_{i=1}^{r} r_i^2,$$

and consequently,

$$0 = \deg(1) = \deg\Big(\sum_{i=1}^{r} r_i^2\Big) = 2\max\{\deg(r_i) :\ 1 \le i \le r\},$$

that is, each $r_i \in \mathbb{R}$. Thus, using the equality $f_i = \mathtt{x}q_i + r_i$, and after substituting in (1.1) we obtain

$$\begin{aligned} 1 = f(\mathtt{x},0) = \sum_{i=1}^{r} f_i^2(\mathtt{x},0) = \sum_{i=1}^{r}(\mathtt{x}q_i(\mathtt{x},0) + r_i)^2 = \mathtt{x}^2\sum_{i=1}^{r} q_i^2(\mathtt{x},0) \\ + 2\mathtt{x}\sum_{i=1}^{r} r_i q_i(\mathtt{x},0) + \sum_{i=1}^{r} r_i^2 = \mathtt{x}^2\sum_{i=1}^{r} q_i^2(\mathtt{x},0) + 2\mathtt{x}\sum_{i=1}^{r} r_i q_i(\mathtt{x},0) + 1, \end{aligned}$$

or equivalently,

$$\mathtt{x}\sum_{i=1}^{r} q_i^2(\mathtt{x},0) = -2\sum_{i=1}^{r} r_i q_i(\mathtt{x},0).$$

Suppose there exists some $q_i(\mathtt{x},0) \neq 0$ and set $d := \max\{\deg(q_i(\mathtt{x},0)) : 1 \le i \le r\}$. Then, counting degrees,

$$1 + 2d = \deg\Big(\sum_{i=1}^{r} r_i q_i(\mathtt{x},0)\Big) \le d,$$

a contradiction. Hence $q_i(\mathtt{x},0) = 0$ for $1 \le i \le r$, and so $q_i(\mathtt{x},\mathtt{y}) := \mathtt{y}g_i(\mathtt{x},\mathtt{y})$ for some polynomial $g_i \in \mathbb{R}[\mathtt{x},\mathtt{y}]$. Therefore,

$$f_i(\mathtt{x},\mathtt{y}) = \mathtt{x}q_i(\mathtt{x},\mathtt{y}) + r_i = \mathtt{xy}g_i(\mathtt{x},\mathtt{y}) + r_i \quad \text{for each} \quad 1 \le i \le r.$$

After substituting in (1.1) one gets

$$\begin{aligned} \mathtt{x}^4\mathtt{y}^2 + \mathtt{x}^2\mathtt{y}^4 + 1 - 3\mathtt{x}^2\mathtt{y}^2 = f(\mathtt{x},\mathtt{y}) = \sum_{i=1}^{r} f_i^2(\mathtt{x},\mathtt{y}) = \sum_{i=1}^{r}(\mathtt{xy}g_i + r_i)^2 \\ = \mathtt{x}^2\mathtt{y}^2\Big(\sum_{i=1}^{r} g_i^2\Big) + 2\mathtt{xy}\sum_{i=1}^{r} r_i g_i + 1, \end{aligned}$$

and consequently,

$$\mathtt{x}^2\mathtt{y}^2\Big(\mathtt{x}^2 + \mathtt{y}^2 - 3 - \Big(\sum_{i=1}^{r} g_i^2\Big)\Big) = 2\mathtt{xy}\sum_{i=1}^{r} r_i g_i.$$

After dividing both sides by $\mathtt{xy}$ it follows

$$\mathtt{xy}\Big(\mathtt{x}^2 + \mathtt{y}^2 - 3 - \Big(\sum_{i=1}^{r} g_i^2\Big)\Big) = 2\sum_{i=1}^{r} r_i g_i. \tag{1.2}$$

Nevertheless, for each $1 \leq i \leq r$ we have

$$2 + \deg(g_i) = \deg(\mathtt{x}\mathtt{y}g_i + r_i) = \deg(f_i) \leq 3,$$

that is, $\deg(g_i) \leq 1$, and so the degree of $\sum_{i=1}^{r} r_i g_i$ is ≤ 1. Thus, after comparing degrees in equation (1.2) we obtain

$$\sum_{i=1}^{r} r_i g_i = 0 \quad \& \quad \mathtt{x}^2 + \mathtt{y}^2 - 3 = \sum_{i=1}^{r} g_i^2,$$

but this is impossible because it implies $\sum_{i=1}^{r} g_i^2(0,0) = -3$. □

Remarks 1.1 (1) The statement of **H17** can be made explicit in the precedent example; namely, the polynomial f can be represented as the sum of four squares in the field $\mathbb{R}(\mathtt{x},\mathtt{y})$ of rational functions in two variables as follows:

$$\mathtt{x}^4\mathtt{y}^2 + \mathtt{x}^2\mathtt{y}^4 + 1 - 3\mathtt{x}^2\mathtt{y}^2 = \frac{\mathtt{x}^2\mathtt{y}^2(\mathtt{x}^2+\mathtt{y}^2+1)(\mathtt{x}^2+\mathtt{y}^2-2)^2 + (\mathtt{x}^2-\mathtt{y}^2)^2}{(\mathtt{x}^2+\mathtt{y}^2)^2}.$$

(2) Motzkin's example shows that **H17** statement is the best one for polynomials in $n \geq 2$ variables.

Exercise 1.2 Prove that the polynomials

$$\begin{aligned} f(\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3) &:= \mathtt{x}_1^4\mathtt{x}_2^2 + \mathtt{x}_2^4\mathtt{x}_3^2 + \mathtt{x}_3^4\mathtt{x}_1^2 - 3\mathtt{x}_1^2\mathtt{x}_2^2\mathtt{x}_3^2 \quad \text{and} \\ g(\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3,\mathtt{x}_4) &:= \mathtt{x}_4^4 + \mathtt{x}_1^2\mathtt{x}_2^2 + \mathtt{x}_1^2\mathtt{x}_3^2 + \mathtt{x}_2^2\mathtt{x}_3^2 - 4\mathtt{x}_1\mathtt{x}_2\mathtt{x}_3\mathtt{x}_4 \end{aligned}$$

are positive semidefinite but they are not sums of squares in the rings $\mathbb{R}[\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3]$ and $\mathbb{R}[\mathtt{x}_1,\mathtt{x}_2,\mathtt{x}_3,\mathtt{x}_4]$, respectively.

Exercise 1.3 Consider, for every positive integer m, the homogeneous polynomial of degree m, called *Hurwitz's polynomial,*

$$H_m(\mathtt{x}_1,\ldots,\mathtt{x}_m) := \sum_{j=1}^{m} \mathtt{x}_j^m - m\prod_{j=1}^{m} \mathtt{x}_j.$$

(1) Prove that for every positive integer d the following identity holds:

$$H_{2d}(\mathtt{x}_1,\ldots,\mathtt{x}_{2d}) = H_d(\mathtt{x}_1^2,\ldots,\mathtt{x}_d^2) + H_d(\mathtt{x}_{d+1}^2,\ldots,\mathtt{x}_{2d}^2) + d\Big(\prod_{j=1}^{d}\mathtt{x}_j - \prod_{j=d+1}^{2d}\mathtt{x}_j\Big)^2.$$

(2) Prove that for every positive integer n the polynomial $H_{2^n}(\mathtt{x}_1, \ldots, \mathtt{x}_{2^n})$ is a sum of squares in the polynomial ring $\mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_{2^n}]$.

(3) Let $d_1, \ldots, d_m$ be non-negative integers such that $\sum_{j=1}^m d_j = 2^n$. Prove that

$$g(\mathtt{x}_1, \ldots, \mathtt{x}_m) := \sum_{j=1}^m d_j \mathtt{x}_j^{2^n} - 2^n \prod_{j=1}^m \mathtt{x}_j^{d_j} \in \mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_m]$$

is a sum of squares in the ring $\mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_m]$.

For the sake of completeness, let us see that for univariate polynomials with real coefficients to be positive semidefinite is equivalent to be a sum of two squares of polynomials. First we prove the next auxiliary result, which has its own interest.

Lemma 1.4 *Let A be a commutative ring and let $x_1, \ldots, x_r \in A$ such that each x_i is a sum of two squares in A. Then, $x := x_1 \cdots x_r$ is a sum of two squares in A.*

Proof. The result is obvious for $r = 1$ and we prove it for $r = 2$. Let $a, b, c, d \in A$ such that $x_1 := a^2 + b^2$ and $x_2 := c^2 + d^2$. If A contains a root of $\mathtt{t}^2 + 1$ we denote it by j. Otherwise we consider the ideal $\mathfrak{a}$ generated by $\mathtt{t}^2 + 1$ in $A[\mathtt{t}]$, the quotient $B := A[\mathtt{t}]/(\mathtt{t}^2 + 1)$, that contains A as a subring, and denote $j := \mathtt{t} + \mathfrak{a} \in B$. Any case $j^2 = -1$ and we factorize the product $x_1 x_2$ in B as follows:

$$\begin{aligned} x_1 x_2 &= (a^2 + b^2)(c^2 + d^2) \\ &= (a + bj)(a - bj)(c + dj)(c - dj) \\ &= (a + bj)(c + dj)(a - bj)(c - dj) \\ &= ((ac - bd) + (ad + bc)j)((ac - bd) - (ad + bc)j) \\ &= (ac - bd)^2 + (ad + bc)^2. \end{aligned}$$

Notice that both $(ac - bd), (ad + bc) \in A$, and we get the equality

$$x_1 x_2 = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Suppose by induction that $r \geq 3$ and $y := x_1 \cdots x_{r-1}$ is a sum of two squares in A. Then, by the case just proved, $x = y x_r$ is a sum of two squares too. □

Proposition 1.5 *Each positive semidefinite univariate polynomial $f \in \mathbb{R}[\mathtt{t}]$ is a sum of two squares in $\mathbb{R}[\mathtt{t}]$.*

Proof. We may assume that f is a monic polynomial. Since $\mathbb{R}[\mathtt{t}]$ is a unique factorization domain, $f := f_1^{m_1} \cdots f_s^{m_s}$ where $f_1, \ldots, f_s$ are monic irreducible polynomials in $\mathbb{R}[\mathtt{t}]$. We may assume that $m_1, \ldots, m_r$ are even integers for some $r \leq s$ and $m_{r+1}, \ldots, m_s$ are odd. Let us write

$$m_j := 2k_j \quad \text{for all } j \leq r \quad \& \quad m_j := 2k_j + 1 \quad \text{for all } r+1 \leq j \leq s.$$

Consequently, $g := \prod_{j=1}^{s} f_i^{k_j} \in \mathbb{R}[\mathtt{t}]$ and $f = g^2 f_{r+1} \cdots f_s$. Clearly, if $r = s$ we are done. Suppose that $r < s$ and notice that, $\mathbb{C}$ being algebraically closed, the monic irreducible polynomials in $\mathbb{R}[\mathtt{t}]$ have either the form $\mathtt{t} - b$ with $b \in \mathbb{R}$ or the form $(\mathtt{t}-b)^2 + c^2$ with $b, c \in \mathbb{R}$ and $c \neq 0$. Let us check that $\deg(f_j) = 2$ for $r+1 \leq j \leq s$. Otherwise we may assume that there exists $t \leq s$ such that

$$f_j(\mathtt{t}) := \mathtt{t} - b_j \quad \text{for each } r+1 \leq j \leq t \leq s,$$

and $b_t := \max\{b_j : r+1 \leq j \leq t\}$. Let $\eta \in \mathbb{R}$ such that $g(\eta) \neq 0$, $\eta < b_t$ and $\eta > b_j$ for each $r+1 \leq j \leq t-1$. Then,

$$f_j(\eta) > 0 \quad \text{for each } r+1 \leq j \leq t-1 \quad \& \quad f_t(\eta) < 0.$$

On the other hand, $f_j := (\mathtt{t} - d_j)^2 + e_j^2$ with $e_j \neq 0$ for every $t+1 \leq j \leq s$, and this implies $f_j(\eta) = (\eta - d_j)^2 + e_j^2 > 0$. Therefore,

$$f(\eta) = g^2(\eta) \prod_{j=1}^{t-1} f_j(\eta) \Big(\prod_{j=t+1}^{s} f_j(\eta) \Big) f_t(\eta) < 0,$$

since all factors of the right hand side, except the last one, are positive. This contradicts the assumption that f is positive semidefinite.

Therefore, $f_j(\mathtt{t}) := (\mathtt{t} - d_j)^2 + e_j^2$ for each $r+1 \leq j \leq s$, where $d_j, e_j \in \mathbb{R}$. Hence, by Lemma 1.4, the product $f_{r+1} \cdots f_s = h_1^2 + h_2^2$ for some polynomials $h_1, h_2 \in \mathbb{R}[\mathtt{t}]$. Finally,

$$f = g^2 f_{r+1} \cdots f_s = g^2(h_1^2 + h_2^2) = (gh_1)^2 + (gh_2)^2,$$

as wanted. □

Exercise 1.6 Let A be a commutative ring and let $x, y \in A$ be sums of four squares in A. Prove that xy is a sum of four squares in A. *Hint: Use quaternions.*

Remarks 1.7 (1) We will see in Corollary 1.10 that a field E is orderable if and only if it is *real,* that is, -1 is not a sum of squares in E. It is natural to ask if for *non real* fields each element is a sum of squares.

(2) The answer to the above question is affirmative if $\mathrm{ch}(E) \neq 2$. Indeed, if E is not a real field, there exist $y_1, \ldots, y_s \in E$ such that $-1 = y_1^2 + \cdots + y_s^2$. This implies that each $a \in E$ is a sum of squares in E because the elements $x_1 := (a+1)/2$ and $x_2 := (a-1)/2$ satisfy

$$\begin{aligned} a = ((a+1)/2)^2 + (-1)\cdot((a-1)/2)^2 &= x_1^2 + (y_1^2 + \cdots + y_s^2)x_2^2 \\ &= x_1^2 + (y_1x_2)^2 + \cdots + (y_sx_2)^2. \end{aligned}$$

(3) However, if $\mathrm{ch}(E) = 2$ the field E is not real, because $-1 = 1^2$, but the polynomial $f(\mathtt{t}) := \mathtt{t}^2+\mathtt{t}+1$ is not a sum of squares in the field $E(\mathtt{t})$. Otherwise there would exist polynomials $a_0, a_1, \ldots, a_r \in E[\mathtt{t}] \setminus \{0\}$ such that $f := (a_1/a_0)^2 + \cdots + (a_r/a_0)^2$, that is,

$$a_0^2 f = a_1^2 + \cdots + a_r^2 = (a_1 + \cdots + a_r)^2.$$

Let $g := (a_1 + \cdots + a_r)/a_0 \in E(\mathtt{t})$. Then, $f = g^2$, and so $g \in E(\mathtt{t})$ is a root of the monic polynomial $\mathtt{x}^2 - f \in A[\mathtt{x}]$, where $A := E[\mathtt{t}]$ in an UFD, and so it is integrally closed. Hence $g \in A$ and $f = g^2$. Since

$$2 = \deg(f) = \deg(g^2) = 2\deg(g),$$

it follows that $\deg(g) = 1$ and, f being monic, we may assume that g is monic too. Thus $g(\mathtt{t}) = \mathtt{t} + \varepsilon$ for some $\varepsilon \in E$, and this leads us to a contradiction:

$$\mathtt{t}^2 + \mathtt{t} + 1 = f(\mathtt{t}) = g(\mathtt{t})^2 = (\mathtt{t} + \varepsilon)^2 = \mathtt{t}^2 + 2\varepsilon\mathtt{t} + \varepsilon^2 = \mathtt{t}^2 + \varepsilon^2.$$

(1.8) Artin's idea. Artin's solution to Hilbert's 17th Problem consists, essentially, of three parts:

(1) To define the concept of *ordering* of a real field E and to prove that its *totally positive* elements, that is, those which are positive with respect to all orderings in E are, exactly, the sums of squares in E.

(2) To prove that given an ordered field E, the field $E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ of rational functions admits an ordering that extends the given ordering in E.

(3) To prove that if E is a real field admitting a unique ordering, then a polynomial $f \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ is negative with respect to some ordering in $E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ if and only if $f(x) < 0$ for some point $x \in R^n$, where R is a certain real algebraic extension of E called *a real closure of* E.

In fact these three steps appear in the solutions of **H17** due to Artin, Lang and Robinson quoted before. The only difference between them relies essentially in the way the third step is proved. While the two first proofs use Sturm's Theorem, the third one is based upon the existence of quantifiers elimination in the first-order theory of real closed fields.

CHAPTER I

Artin's solution of Hilbert's 17th Problem

In this chapter we approach Artin's solution of Hilbert's 17th Problem. We begin by introducing some crucial preliminary notions for our purposes.

1 Ordered fields

As one can expect, our first step is the introduction of the notion of ordering in a field (and more generally a cone), compatible with its field operations.

Definitions 1.1 (Cones) Let E be a field and let $P \subset E$ be a subset. Denote

$$E^2 := \{x^2 : x \in E\}.$$

(1) The subset P is a *cone* in E if $P + P \subset P$, $P \cdot P \subset P$ and $E^2 \subset P$.

(2) The cone P is *proper* if $-1 \notin P$.

(3) A proper cone P is an *ordering in* E if $P \cup (-P) = E$, where $-P := \{-x : x \in P\}$.

Definitions and Remarks 1.2 (Real field and ordered field) (1) The subset of elements which are *sums of squares in* E is

$$\Sigma E^2 := \left\{ x \in E : \exists n \in \mathbb{N}, \quad x_1, \ldots, x_n \in E \quad \text{such that} \quad x = \sum_{j=1}^{n} x_j^2 \right\}.$$

Note that ΣE^2 is a cone in E, because given two sums of squares

$$x := \sum_{i=1}^{m} x_i^2 \quad \& \quad y := \sum_{j=1}^{n} y_j^2, \quad \text{where each} \quad x_i, y_j \in E,$$

both $x + y$ and xy are sums of squares in E:

$$x + y = \sum_{i=1}^{m} x_i^2 + \sum_{j=1}^{n} y_j^2 \in \Sigma E^2 \quad \& \quad xy = \sum_{i,j} (x_i y_j)^2 \in \Sigma E^2.$$

(2) The set ΣE^2 is contained in every cone P in E since $E^2 \subset P$ and $P + P \subset P$.

(3) The field E is said to be *real* if $-1 \notin \Sigma E^2$, that is, if ΣE^2 is a proper cone in E. This is equivalent to:

(3.1) *If* $a_1, \ldots, a_r \in E$ *satisfy* $\sum_{i=1}^r a_i^2 = 0$, *then* $a_1 = 0, \ldots, a_r = 0$.

Indeed, suppose that E is a real field and there exist $a_1, \ldots, a_r \in E \setminus \{0\}$ such that $\sum_{i=1}^r a_i^2 = 0$. Then,

$$-1 = \sum_{i=2}^{r} (a_i/a_1)^2 \in \Sigma E^2,$$

a contradiction.

The converse is evident because, if E is not a real field there exist $b_1, \ldots, b_s \in E$ such that $-1 = \sum_{i=1}^s b_i^2$, and so $b_0 = 1 \neq 0$ and $\sum_{j=0}^s b_j^2 = 0$, against the hypothesis.

(4) Every real field has zero characteristic. Otherwise, suppose that $\mathrm{ch}(E) = p > 0$; hence $-1 = 1^2 + \overset{p-1}{\cdots} + 1^2$, which is false because E is a real field.

(5) An *ordered field* is a pair $(E, \leq)$ where E is a field and $\leq$ is a total order relation in E such that, for every $x, y, z \in E$,

$$x + z \leq y + z \quad \text{if } x \leq y \quad \& \quad 0 \leq xy \quad \text{if } 0 \leq x, y.$$

(6) It is said that E is an *orderable field* if there exists an order relation $\leq$ in E such that the pair $(E, \leq)$ is an ordered field.

Proposition 1.3 *Let E be a field.*

(1) *If $\leq$ is an order relation in E such that $(E, \leq)$ is an ordered field, then the subset $P_\leq := \{x \in E : 0 \leq x\}$ is an ordering in E.*

(2) *If $P \subset E$ is an ordering in E, then $(E, \leq_P)$ is an ordered field, where $\leq_P$ is defined by $x \leq_P y$ if $y - x \in P$. We will write also that (E, P) is an* ordered field.

(3) *If P is an ordering in E then $P \cap (-P) = \{0\}$.*

(4) *Let P be an ordering in E and $p_1, \ldots, p_n \in P$ with $\sum_{i=1}^n p_i = 0$. Then, each $p_i = 0$.*

Proof. (1) Let $x, y \in P_\leq$. Then, $0 \leq x$ and $0 \leq y$, thus

$$0 \leq y = 0 + y \leq x + y \quad \& \quad 0 \leq xy, \quad \Longrightarrow \quad P_\leq + P_\leq \subset P_\leq \quad \& \quad P_\leq \cdot P_\leq \subset P_\leq.$$

To see that $P_\leq$ is a cone we must check the inclusion $E^2 \subset P_\leq$. Given $x \in E$, and since $\leq$ is a total order relation, either $0 \leq x$ or $0 \leq -x$. This implies, from $P_\leq \cdot P_\leq \subset P_\leq$, that $x^2 = (-x)^2 \in P_\leq$.

Let us prove that $P_{\leq}$ is a proper cone. Otherwise $-1 \in P_{\leq}$, that is, $0 \leq -1$, and we have just seen that $1 = 1^2 \in P_{\leq}$, or equivalently, $0 \leq 1$. Adding up -1 to both members of this inequality we get $-1 = (-1) + 0 \leq (-1) + 1 = 0$, and so $-1 \leq 0 \leq -1$. Thus $-1 = 0$, and this is false.

Finally, we must check that $P_{\leq} \cup (-P_{\leq}) = E$, which follows straightforwardly from the fact that $\leq$ is a total order relation.

(2) Since $0 = 0^2 \in E^2 \subset P$, each element $x \in E$ satisfies $x - x = 0 \in P$, that is, $x \leq_P x$, and so $\leq_P$ is a reflexive relation. Suppose it is not antisymmetric. Then, there exist distinct elements $x, y \in E$ such that $x \leq_P y$ and $y \leq_P x$, that is, $z = y - x \in P$ and $-z = x - y \in P$. But $P \cdot P \subset P$, and so $-z^2 = z(-z) \in P$. Moreover, $1/z^2 = (1/z)^2 \in E^2 \subset P$, and consequently,

$$-1 = (-z^2) \cdot (1/z^2) \in P \cdot P \subset P.$$

This is false, because P is a proper cone. Moreover, $\leq_P$ is a transitive relation, since given $x \leq_P y \leq_P z$ one has $y - x \in P$ and $z - y \in P$. Hence,

$$z - x = (z - y) + (y - x) \in P + P \subset P,$$

which means $x \leq_P z$.

Moreover, the equality $P \cup (-P) = E$ implies that $\leq_P$ is a total order relation. To finish we just need to check that $\leq_P$ is compatible with the addition and product in E. First, given $x, y \in E$ such that $x \leq_P y$ and $z \in E$, we have

$$(y + z) - (x + z) = y - x \in P \iff x + z \leq_P y + z.$$

Moreover, if $0 \leq_P x$ and $0 \leq_P y$ then $x, y \in P$, and so $xy \in P \cdot P \subset P$, that is, $0 \leq_P xy$.

(3) Suppose there exists a non-zero element $x \in P \cap (-P)$. Then, $x, -x \in P$, which implies $-x^2 = x(-x) \in P \cdot P \subset P$. Thus $-1 = (-x^2)(1/x)^2 \in P \cdot P \subset P$, and this is impossible because P is a proper cone.

(4) We argue by induction on the number n of summands. For $n = 2$, $p_1 + p_2 = 0$, that is, $p_1 = -p_2 \in P \cap (-P) = \{0\}$, and so $p_1 = 0$ and $p_2 = 0$. For the inductive step, suppose that $p_1 + \cdots + p_{n+1} = 0$, where each $p_i \in P$. Then,

$$p_1 + \cdots + p_n = -p_{n+1} \in P \cap (-P) = \{0\},$$

and so $p_{n+1} = 0$ and $p_1 + \cdots + p_n = 0$. By the induction hypothesis the last equality implies that $p_1 = 0, \ldots, p_n = 0$. □

Remarks 1.4 (1) Given two orderings P_1 and P_2 in a field E such that $P_1 \subset P_2$, then $P_1 = P_2$. Otherwise there would exist $a \in P_2 \setminus P_1 \subset E \setminus P_1 \subset (-P_1)$, that is, $-a \in P_1 \subset P_2$. Hence $a \in P_2 \cap (-P_2) = \{0\}$, which is false because $0 \in P_1$.

(2) Given a field extension $K|E$ and an ordering P in K then, $P \cap E$ is an ordering in E. Indeed, let $x, y \in P \cap E$. Then, $x + y, xy \in P \cap E$ because P is an ordering and E is a field. Moreover, $E^2 \subset E$ and $E^2 \subset K^2 \subset P$, which implies $E^2 \subset P \cap E$. This shows that $P \cap E$ is a cone in E, and it is proper since $-1 \notin P$. Finally, $P \cap E$ is an ordering in E, because for each $a \in E \setminus (P \cap E)$ it follows that $a \in K \setminus P$, and so $-a \in E \cap P$.

Exercise 1.5 (1) Let E be a field, (K, P) an ordered field and $\varphi : E \to K$ a field homomorphism. Prove that $Q := \varphi^{-1}(P)$ is an ordering in E.

(2) Find two distinct orderings in the field $E := \mathbb{Q}(\sqrt{2})$.

(3) Find an algebraic number $u \in \mathbb{C} \setminus \mathbb{R}$ over $\mathbb{Q}$ such that the field $\mathbb{Q}(u)$ admits an ordering.

Exercise 1.6 (1) Prove that the field $\mathbb{R}$ of real numbers admits a unique automorphism.

(2) Prove that the field $\mathbb{C}$ of complex numbers admits infinitely many automorphisms.

Exercise 1.7 Let (E, P) be an ordered field. The *absolute value* of $a \in E$ with respect to P is $|a| := \max\{-a, a\}$. Prove that

$$|a + b| \leq |a| + |b| \quad \& \quad |ab| = |a| \cdot |b| \quad \forall\, a, b \in E.$$

Exercise 1.8 (1) Prove that for every $a \in \mathbb{R}$ there exists an ordering in the field $\mathbb{R}(\mathtt{t})$ of rational functions in one variable with respect to which $\mathtt{t} - a$ is positive but $\mathtt{t}$ is smaller than all real numbers larger than a.

(2) Prove that for every $a \in \mathbb{R}$ there exists an ordering in the field $\mathbb{R}(\mathtt{t})$ with respect to which $\mathtt{t} - a$ is negative but $\mathtt{t}$ is larger than all real numbers smaller than a.

(3) Prove the existence of an ordering in $\mathbb{R}(\mathtt{t})$ with respect to which $\mathtt{t}$ is larger than all real numbers.

A basic but fundamental result in the theory of ordered fields states that the notions of real and orderable field coincide. In fact we prove next a slightly stronger result due to Serre, [S], that will be useful in the sequel.

Lemma 1.9 (Serre's Criterion) *Let P be an ordering in the field E and let $K|E$ be a field extension. The following statements are equivalent:*

(1) *There exists an ordering Q in K such that $Q \cap E = P$.*

(2) *For every $p_1, \dots, p_r \in P \setminus \{0\}$ the only solution in K of the equation*

$$p_1 \mathtt{x}_1^2 + \cdots + p_r \mathtt{x}_r^2 = 0$$

is $\mathtt{x}_1 = 0, \dots, \mathtt{x}_r = 0$.

Proof. (1) $\Longrightarrow$ (2). Suppose, by way of contradiction, there exist $p_1, \dots, p_r \in P \setminus \{0\}$ and $x_1, \dots, x_r \in K$ such that $x_1 \neq 0$ and $p_1 x_1^2 + \cdots + p_r x_r^2 = 0$. Each $p_i \in P \subset Q$ and $x_i^2 \in K^2 \subset Q$. Thus, by Proposition 1.3,

$$-p_1 x_1^2 = p_2 x_2^2 + \cdots + p_r x_r^2 \in Q \cap (-Q) = \{0_K\},$$

and this is false because $p_1 \neq 0$ and $x_1 \neq 0$.

(2) $\Longrightarrow$ (1) Let $\mathcal{F}$ be the set of all proper cones of K containing P. It is a non-empty set because

$$Q_0 := \Big\{ \sum_i p_i x_i^2 : \ p_i \in P, \ x_i \in K \Big\} \in \mathcal{F}.$$

Indeed, it is obvious that $Q_0 + Q_0 \subset Q_0$ and $K^2 \subset Q_0$. Also $Q_0 \cdot Q_0 \subset Q_0$ because given

$$u := \sum_{i=1}^{r} p_i x_i^2 \quad \& \quad v := \sum_{j=1}^{s} q_j y_i^2,$$

where $p_i, q_j \in P$ and $x_i, y_j \in K$, its product is

$$uv = \sum_{i,j} p_i q_j (x_i y_j)^2 \in Q_0,$$

since $p_i q_j \in P$ and $x_i y_j \in K$. Henceforth Q_0 is a cone in K and it contains P, because $p = p \cdot 1^2 \in Q_0$ for every $p \in P$. Moreover $-1 \notin Q_0$; otherwise there would exist $p_1, \dots, p_r \in P$ and $x_1, \dots, x_r \in K$ such that if we denote $p_0 := 1 \in P$ and $x_0 := 1 \in K$,

$$-1 = p_1 x_1^2 + \cdots + p_r x_r^2 \quad \Longrightarrow \quad p_0 x_0^2 + p_1 x_1^2 + \cdots + p_r x_r^2 = 0$$

and $x_0 \neq 0$, against the hipothesis.

The set $\mathcal{F}$ ordered by inclusion is inductive, because given a chain $\mathcal{C} \subset \mathcal{F}$ the set $Q_1 := \bigcup_{Q \in \mathcal{C}} Q \in \mathcal{F}$ is an upper bound of $\mathcal{C}$. Indeed, since $Q \subset Q_1$ for every $Q \in \mathcal{C}$, it is enough to prove that $Q_1 \in \mathcal{F}$. Given $q_1, q_2 \in Q_1$ there exists, since $\mathcal{C}$

is a chain, an element $Q_* \in \mathcal{C}$ such that $q_1, q_2 \in Q_*$, and so $q_1 + q_2 \in Q_* \subset Q_1$ and $q_1 q_2 \in Q_* \subset Q_1$. Moreover, $K^2 \subset Q_* \subset Q_1$ and $P \subset Q_* \subset Q_1$ and, finally, $-1 \notin Q_1$ because $-1 \notin Q$ for every $Q \in \mathcal{C}$.

By Zorn's Lemma there exists a maximal element $\widehat{Q} \in \mathcal{F}$, and we will prove that $\widehat{Q}$ is an ordering in K, that is, $K = \widehat{Q} \cup (-\widehat{Q})$, and obviously $\widehat{Q}$ contains P because $\widehat{Q} \in \mathcal{F}$. Thus, let $a \in K \setminus \widehat{Q}$ and consider $\widehat{Q}[-a] := \{x - ay : \ x, y \in \widehat{Q}\}$. Let us prove that $\widehat{Q}[-a] \in \mathcal{F}$. First, given $x_1, x_2, y_1, y_2 \in \widehat{Q}$ consider

$$\zeta_1 := x_1 - ay_1 \in \widehat{Q}[-a] \quad \& \quad \zeta_2 := x_2 - ay_2 \in \widehat{Q}[-a].$$

Then,

$$\zeta_1 + \zeta_2 = (x_1 + x_2) - a(y_1 + y_2) \in \widehat{Q}[-a]$$
$$\& \quad \zeta_1\zeta_2 = (x_1x_2 + a^2y_1y_2) - a(x_1y_2 + x_2y_1) \in \widehat{Q}[-a].$$

This, together with the obvious inclusion $K^2 \subset \widehat{Q} \subset \widehat{Q}[-a]$ implies that this last is a cone in K and, moreover, $P \subset \widehat{Q} \subset \widehat{Q}[-a]$. Even more, $\widehat{Q}[-a]$ is a proper cone because in case $-1 \in \widehat{Q}[-a]$ there exist $x, y \in \widehat{Q}$ such that $-1 = x - ay$, and $y \neq 0$ because $-1 \notin \widehat{Q}$. Therefore,

$$a = (1 + x)/y = (1/y)^2 y(1 + x) \in \widehat{Q},$$

and this is false. Now, $\widehat{Q}$ being a maximal element of $\mathcal{F}$ contained in $\widehat{Q}[-a] \in \mathcal{F}$ it follows that $\widehat{Q} = \widehat{Q}[-a]$, and so $-a \in \widehat{Q}$. Thus, $\widehat{Q}$ is an ordering in K containing P. By Remark 1.4 (2) $\widehat{Q} \cap E$ is an ordering in E, and from the inclusion $P \subset \widehat{Q} \cap E$ and Remark 1.4 (1) the equality $P = \widehat{Q} \cap E$ holds. □

Corollary 1.10 *A field E admits an ordering if and only if E is a real field.*

Proof. Suppose first that E admits an ordering $P \subset E$ but E is not a real field. Then, $-1 \in \Sigma E^2 \subset P$. But $1 = 1^2 \in P$, and so $1 \in P \cap (-P)$, against Proposition 1.3 (3).

Suppose, conversely, that E is a real field. Then, by Remark 1.2 (4), $\mathrm{ch}(E) = 0$, and so E contains the field $\mathbb{Q}$ of rational numbers. Let P denote the usual ordering in $\mathbb{Q}$. We will apply Serre's Criterion 1.9 to show that there exists an ordering Q in E such that $Q \cap \mathbb{Q} = P$. Let $p_1, \ldots, p_r \in P \setminus \{0\}$ and $x_1, \ldots, x_r \in E$ such that $p_1x_1^2 + \cdots + p_rx_r^2 = 0$. Each $p_i := m_i/n = m_in/n^2$ is a positive rational number that can be written as

$$p_i = (1/n)^2(1^2 + \overset{nm_i}{\cdots} + 1^2) = y_{i1}^2 + \cdots + y_{is_i}^2, \quad \text{with} \quad y_{ij} \in \mathbb{Q} \setminus \{0\} \subset E \setminus \{0\}.$$

Consequently,

$$0 = \sum_{i=1}^{r} p_i x_i^2 = \sum_{i=1}^{r} x_i^2 \sum_{j=1}^{s_i} y_{ij}^2 = \sum_{i,j} (x_i y_{ij})^2,$$

and every $x_i y_{ij} \in E$. Since E is a real field, each product $x_i y_{ij} = 0$, and so $x_i = 0$. Hence, by Serre's Criterion, there exists an ordering in E which extends the usual ordering in $\mathbb{Q}$, and we are done. □

Corollary 1.11 Let (E, P) be an ordered field. Then, the field $E_n := E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ of rational functions over E admits an ordering Q such that $E \cap Q = P$.

Proof. We apply Serre's Criterion 1.9 once more. Suppose, by way of contradiction, the existence of $p_1, \ldots, p_r \in P \setminus \{0\}$ and rational functions $f_1, \ldots, f_r \in E_n \setminus \{0\}$ such that $p_1 f_1^2 + \cdots + p_r f_r^2 = 0$. Let us write each $f_i := g_i/h$ for some polynomials $g_1, \ldots, g_r, h \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, where $h \neq 0$. Hence,

$$p_1 g_1^2 + \cdots + p_r g_r^2 = 0.$$

Since $g = g_1 \cdots g_r \neq 0$ and $\mathrm{ch}(E) = 0$ there exists a point $a \in E^n$ such that $g(a) \neq 0$, and so each product $p_i g_i(a) \in P \setminus \{0\}$. Therefore

$$0 = p_1 g_1(a)^2 + \cdots + p_r g_r(a)^2 \in P \setminus \{0\},$$

and this is impossible. □

Exercise 1.12 Let E be a field and let $S \subset E$ be a subset such that $S \cdot S \subset S$. Prove that a given element $a \in E$ is positive in all orderings in E containing S if and only if there exist a positive integer n and $s_1, \ldots, s_n \in S$ and $x_1, \ldots, x_n \in E$ such that

$$a = \sum_{j=1}^{n} s_j x_j^2.$$

Exercise 1.13 Let (K, P) be an ordered field and let $E \subset K$ be a subfield. An element $a \in K$ is said to be *infinitely large* with respect to E if $|x| \leq a$ for every $x \in E$, and it is said that a is *infinitely small* with respect to E if $|a| < |x|$ for every $x \in E \setminus \{0\}$.

(1) Prove that $a \in K \setminus \{0\}$ is infinitely large with respect to E if and only if a^{-1} is infinitely small with respect to E.

(2) Prove that the set

$$V := \{a \in K : \ a \text{ is not infinitely large with respect to } E\}$$

is a *valuation ring* of K, that is, V is a ring and $a^{-1} \in V$ for every $a \in K \setminus V$.

(3) Prove that V is a *local ring,* that is, there exists a unique maximal ideal $\mathfrak{m}$ in V, consisting of all infinitely small elements of K with respect to E.

(4) Prove that the quotient $V/\mathfrak{m}$ is a real field.

Exercise 1.14 Let E be a field and let $V \subset E$ be a *real* valuation ring of E, that is, the residual field $\kappa := V/\mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of V, is a real field. Prove that E is a real field.

Exercise 1.15 Let (E, P) be an ordered field, $\overline{E}$ an algebraic closure of E, $a \in E$ and let $u \in \overline{E}$ be a root of the polynomial $\mathtt{t}^2 - a$.

(1) Prove that if $a \in \Sigma E^2$ then there exists an ordering Q in the field $K := E(u)$ such that $Q \cap E = P$.

(2) Prove that if the field $E(u)$ is not real, then $-a \in \Sigma E^2$.

Exercise 1.16 Let (E, P) be an ordered field and let $K|E$ be a finite field extension of odd degree. Prove that there exists an ordering Q in K such that $Q \cap E = P$.

Exercise 1.17 Let $f \in \mathbb{Q}[\mathtt{t}]$ be an irreducible polynomial. Prove that $\mathbb{Q}[\mathtt{t}]/(f)$ admits an ordering if and only if f has a real root.

Definition 1.18 An element a in a real field E is said to be *totally positive* in E if $a \in P$ for every ordering P in E.

Let us see next that totally positive elements of a real field E are, precisely, those elements in E which are sum of squares in E.

Proposition 1.19 *Let E be a real field and let $\mathcal{F}$ be the set of all orderings in E. Then, $\Sigma E^2 = \bigcap_{P \in \mathcal{F}} P$.*

Proof. An inclusion is evident because $\Sigma E^2 \subset P$ for every ordering P in E. Thus, it is enough to show that given $a \in E \setminus \Sigma E^2$ there exists an ordering Q in E such that $-a \in Q$. Consider the cone

$$P_0 := \Big\{\sigma_1 - a\sigma_2 : \ \sigma_1, \sigma_2 \in \Sigma E^2\Big\}.$$

Let us see that it is a proper cone. If not, $-1 \in P_0$, that is, there exist two sums of squares σ_1, σ_2 such that $-1 = \sigma_1 - a\sigma_2$, and this implies

$$a = (1 + \sigma_1)/\sigma_2 = (1/\sigma_2)^2(1 + \sigma_1)\sigma_2 \in \Sigma E^2,$$

against the hypothesis.

Hence, the family $\mathcal{G}$ consisting of all proper cones in E containing P_0 is non-empty. Given $P_1, P_2 \in \mathcal{G}$ define $P_1 \preceq P_2$ if $P_1 \subset P_2$. The pair $(\mathcal{G}, \preceq)$ is an inductive ordered set since it can be checked straightforwardly that given a chain $\mathcal{C} \subset \mathcal{G}$, the union $\bigcup_{P \in \mathcal{C}} P \in \mathcal{G}$ is an upper bound of $\mathcal{C}$. In this way $\mathcal{G}$ has, by Zorn's Lemma, a maximal element Q, and the same argument used in the proof of (2) $\Longrightarrow$ (1) in Lemma 1.9 shows that $Q \cup (-Q) = E$, that is, Q is an ordering in E. Since $-a = 0 - a \cdot 1 \in P_0 \subset Q$, we are done. □

Remarks 1.20 (1) The last proposition can be read as follows: *If E is a real field and $a \in E \setminus \Sigma E^2$, then a is negative with respect to some ordering in E.*

(2) By Proposition 1.19, if a field E admits a unique ordering then, ΣE^2 is the unique ordering in E. Suppose, conversely, that ΣE^2 is an ordering in E, and let P be an arbitrary ordering in E. Since $\Sigma E^2 \subset P$ it follows from Remark 1.4 (1) that $\Sigma E^2 = P$.

(3) In particular, if $E^2 := \{x^2 : \ x \in E\}$ is an ordering in E, then it is the unique ordering in E. Indeed, it suffices to check that in this case $E^2 = \Sigma E^2$ and apply part (2). The inclusion $E^2 \subset \Sigma E^2$ is evident. On the other hand, each ordering in E contains ΣE^2 and, by the hypothesis, E^2 is one of them.

(4) Let (E, E^2) and (K, P) be ordered fields. Let us show that each field homomorphism $\varphi : E \to K$ is *order preserving,* that is, given $x, y \in E$ with $x \leq_E y$ we have $\varphi(x) \leq_K \varphi(y)$. Indeed, there exists $z \in E$ such that $y - x = z^2$, and so

$$\varphi(y) - \varphi(x) = \varphi(y - x) = \varphi(z^2) = \varphi(z)^2 \in K^2 \subset P$$

or, in other words, $\varphi(x) \leq_K \varphi(y)$.

(5) By part (3) the squares in $\mathbb{R}$ constitute the unique ordering in the field $\mathbb{R}$ of real numbers.

(6) The field $\mathbb{Q}$ of rational numbers admits, by part (2), a unique ordering. To check this we must show that $Q_0 := \Sigma\mathbb{Q}^2$ is an ordering in $\mathbb{Q}$. We already know that it is a proper cone because -1 is not a sum of squares of rational numbers, and so it suffices to see that $Q_0 \cup (-Q_0) = \mathbb{Q}$. To that end it is enough to observe that given $q := m/n$ where $n, m \in \mathbb{Z}$ are positive in the unique ordering in $\mathbb{R}$ then,

$$q = \frac{mn}{n^2} = \left(\frac{1}{n}\right)^2 (1^2 + \overset{mn}{\cdots} + 1^2) \in \Sigma\mathbb{Q}^2.$$

Exercise 1.21 (**Veblen**). Let K be a field such that -1 is not a square in K and the sum of any two non-squares of K is a non-square. Show that K admits a unique ordering.

Exercise 1.22 In his solution to *Waring's Problem* [Hi1], Hilbert proved that for every pair of positive integers d and n there exist a positive integer m and rational functions $f_1, \ldots, f_m \in \mathbb{Q}(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ such that

$$\Big(\sum_{j=1}^{n} \mathtt{x}_j^2\Big)^d = \sum_{i=1}^{m} f_i(\mathtt{x}_1, \ldots, \mathtt{x}_n)^{2d}.$$

Use this fact to prove that given a field E admitting a unique ordering, each positive element in E is a sum of $2k$-powers in E for every positive integer k.

Exercise 1.23 A field E is said to enjoy the *extension property* if each automorphism of the field $E(\mathtt{t})$ of rational functions is the extension of an automorphism of E. Show that E enjoys the extension property if and only if $\sigma(E) \subset E$ for each automorphism σ of $E(\mathtt{t})$.

Exercise 1.24 A real field E is said to be a *pythagorean field* if $\Sigma E^2 = E^2$.

(1) Prove that a field E is pythagorean if and only if whenever a polynomial $f \in E[\mathtt{t}]$ splits in $E[\mathtt{t}]$ as a product of degree one factors, the same holds true for its derivative $f'(\mathtt{t})$.

(2) Prove that every pythagorean field enjoys the extension property.

Exercise 1.25 Let $E|K$ be a field extension and let P be an ordering in E. It is said that (E, P) is an *archimedean extension* of $(K, P \cap K)$ if for every $x \in E$ there exists $y \in K$ such that $|x| <_P y$. If $K = \mathbb{Q}$ we simply say that (E, P) is an *archimedean field.*

(1) Let $E|K$ be an algebraic extension and let P be an ordering in E. Prove that (E, P) is an archimedean extension of $(K, P \cap K)$.

(2) Let E be a field admitting a unique ordering P and suppose that the pair (E, P) is an archimedean field. Prove that E enjoys the extension property. *Hint: Use Exercise* 1.22.

Exercise 1.26 (1) Let E be a real field which admits an ordering P such that $P \subset \mathbb{Q} + E^2$. Prove that E enjoys the extension property.

(2) Let $\mathbb{Q}((\mathtt{t}))$ be the quotient field of the ring of formal series with coefficients in $\mathbb{Q}$. Prove that $\mathbb{Q}((\mathtt{t}))$ enjoys the extension property.

Remark 1.27 The class of fields that enjoy the extension property was introduced in [GR] and [G1], and has been carefully studied by Fernández and Llerena in [FL1], [FL2].

(1.28) Real closed fields. Real closed fields constitute a distinguished class of ordered fields that plays a fundamental role in the solution of **H17**. A real field is *real closed* if it does not admit real algebraic extensions different from the trivial one. The next theorem provides two useful characterizations of real closed fields.

Theorem 1.29 *Let E be a field. The following conditions are equivalent:*

(1) *E is real closed.*

(2) *The subset $E^2 := \{x^2 : \ x \in E\}$ is an ordering in E and every polynomal in $E[\mathtt{t}]$ whose degree is odd has a root in E.*

(3) *The ring $K := E[\mathtt{t}]/(\mathtt{t}^2+1)$ is an algebraically closed field.*

Proof. Let us prove (1) $\Longrightarrow$ (2). To that end let us check first that

$$E \setminus E^2 \subset -\big(\Sigma E^2\big). \tag{1.1}$$

Indeed, let $a \in E \setminus E^2$. Let $\overline{E}$ be an algebraic closure of E, and let $u \in \overline{E}$ be a root of the polynomial $\mathtt{t}^2 - a$. Consequently,

$$E_1 := E[\mathtt{t}]/(\mathtt{t}^2 - a) \cong E(u) := \{x + yu : \ x, y \in E\},$$

is a degree 2 extension of E. Thus $E_1|E$ is a non trivial algebraic extension, and so E_1 is not a real field. Hence $-1 \in \Sigma E_1^2$, that is, there exist $x_1, \ldots, x_r, y_1, \ldots, y_r \in E$ such that

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

Since $\{1, u\}$ is a basis of E_1 as a vector space over E we have

$$-1 = \sum_{i=1}^{r} x_i^2 + a \sum_{i=1}^{r} y_i^2.$$

But, E being a real field, $\rho := \sum_{i=1}^{r} y_i^2 \neq 0$, and $-\rho a = 1 + \sum_{i=1}^{r} x_i^2$. Therefore

$$-a = \Big(1 + \sum_{i=1}^{r} x_i^2\Big)\Big(\sum_{i=1}^{r} y_i^2\Big)\Big(\frac{1}{\rho}\Big)^2 \in \Sigma E^2,$$

and the inclusion (1.1) is proved. Henceforth, $\Sigma E^2 = E^2$. If not there would exist $x \in \Sigma E^2 \setminus E^2$ and, by (1.1), $-x \in \Sigma E^2$. Thus, there exist $y_1, \dots, y_r, z_1, \dots, z_s \in E$ such that

$$y_1^2 + \cdots + y_r^2 = x = -(z_1^2 + \cdots + z_s^2), \quad \text{and so} \quad y_1^2 + \cdots + y_r^2 + z_1^2 + \cdots + z_s^2 = 0.$$

Since E is a real field, we get $y_i = z_j = 0$, and so $x = 0 = 0^2 \in E^2$, which is false.

We are ready to prove that E^2 is an ordering in E. The equality $E^2 = \Sigma E^2$ implies that $E^2 + E^2 \subset E^2$. It is also evident that $E^2 \cdot E^2 \subset E^2$ and, E being a real field, all reduces to check that $E^2 \cup (-E^2) = E$. But given $a \in E \setminus E^2$ we have seen in (1.1) that $-a \in \Sigma E^2 = E^2$.

Let us prove now that each polynomial in $E[\mathtt{t}]$ of odd degree has at least a root in E. Otherwise we choose a polynomial $f \in E[\mathtt{t}]$ whose odd degree $d_0 > 1$ is minimum among the degrees of the polynomials in $E[\mathtt{t}]$ of odd degree having no root in E. This implies, in particular, that f is irreducible in $E[\mathtt{t}]$. Indeed, f factorizes $f := f_1 \cdots f_k$ as a product of irreducible polynomials in $E[\mathtt{t}]$ and at least one of these factors, say f_1, has odd degree. The minimality of the degree of f implies that $f = f_1$ is irreducible in $E[\mathtt{t}]$.

Since $E[\mathtt{t}]$ is a PID and f is irreducible in $E[\mathtt{t}]$, the quotient $E_2 := E[\mathtt{t}]/(f)$ is a field algebraic extension of degree d_0 of E. Since E is real closed and the degree $d_0 := [E_2 : E] > 1$, the field E_2 is not real, that is, $-1 \in \Sigma E_2^2$. The elements of E_2 are equivalence classes $h + (f)$ where the degree of $h \in E[\mathtt{t}]$ is $< d_0$. Hence, there exist polynomials $h_1, \dots, h_r \in E[\mathtt{t}]$ with $\deg(h_i) < d_0$ such that

$$-1 + (f) = -1_{E_2} = \sum_{i=1}^{r} (h_i + (f))^2 = \sum_{i=1}^{r} h_i^2 + (f),$$

that is, there exists $g \in E[\mathtt{t}]$ such that

$$-1 = \sum_{i=1}^{r} h_i^2 + fg. \tag{1.2}$$

Let $e := \max\{\deg(h_1), \dots, \deg(h_r)\} \leq d_0 - 1$. Now, the field E being real, we have

$$\deg(f) + \deg(g) = \deg\left(1 + \sum_{i=1}^{r} h_i^2\right) = 2e.$$

Thus, $\deg(g) = 2e - d_0$ is odd and $\deg(g) \leq 2(d_0 - 1) - d_0 = d_0 - 2$. From the minimality of d_0 we deduce that g has a root $\eta \in E$, and after evaluating both members of equality (1.2) in $\mathtt{t} = \eta$, it follows that

$$-1 = \sum_{i=1}^{r} h_i(\eta)^2 + f(\eta)g(\eta) = \sum_{i=1}^{r} h_i(\eta)^2 \in \Sigma E^2.$$

This is a contradiction because E is a real field.

Let us prove (2) $\Longrightarrow$ (3). Notice that E^2 being an ordering in E, this is a real field, and so -1 is not a sum of squares in E. In particular $-1 \notin E^2$, that is, $\mathtt{t}^2+1$ is an irreducible polynomial in $E[\mathtt{t}]$. Hence, if $\sqrt{-1}$ is a root of $\mathtt{t}^2+1$ in an algebraic closure of E, the quotient $K := E[\sqrt{-1}] \cong E[\mathtt{t}]/(\mathtt{t}^2+1)$ is a field. We must prove that it is algebraically closed, and to that end is suffices to show that:

(1.29.1) *Each polynomial $f \in E[\mathtt{t}]$ with $\deg(f) \geq 1$ has a root in K.*

Indeed, assume for a while that (1.29.1) is true, and let $g \in K[\mathtt{t}]$ be a non-constant polynomial. Let τ be the *conjugation homomorphism* in K, that is, the involution

$$\sigma : K \to K,\ a+b\sqrt{-1} \mapsto a-b\sqrt{-1}.$$

Clearly $E = \mathrm{Fix}(\sigma) := \{z \in K : \sigma(z) = z\}$. Let $\widehat{\sigma}$ be the induced homomorphism

$$\widehat{\sigma} : K[\mathtt{t}] \to K[\mathtt{t}],\ \sum_{j=0}^{d} \alpha_j \mathtt{t}^j \mapsto \sum_{j=0}^{d} \sigma(\alpha_j)\mathtt{t}^j,$$

and let us check that the product $g\widehat{g} \in E[\mathtt{t}]$. Let us write

$$g(\mathtt{t}) := \sum_{j=0}^{d} \alpha_j \mathtt{t}^j \quad \Longrightarrow \quad \widehat{g}(\mathtt{t}) = \sum_{j=0}^{d} \sigma(\alpha_j)\mathtt{t}^j.$$

Thus $g(\mathtt{t})\widehat{g}(\mathtt{t}) = \sum_{j=0}^{e} b_j \mathtt{t}^j$, where $b_j := \sum_{\ell=0}^{j} \alpha_\ell \sigma(\alpha_{j-\ell}) \in E$, and so $f := g\widehat{g} \in E[\mathtt{t}]$, because

$$\sigma(b_j) = \sigma\Big(\sum_{\ell=0}^{j} \alpha_\ell \sigma(\alpha_{j-\ell})\Big) = \sum_{\ell=0}^{j} \sigma(\alpha_\ell)\alpha_{j-\ell} = \sum_{k=0}^{j} \alpha_k \sigma(\alpha_{j-k}) = b_j.$$

Since we assume that (1.29.1) is true, $0 = f(u) = g(u)\widehat{g}(u) = 0$ for some $u \in K$. If $g(u) = 0$ we are done, and if $g(u) \neq 0$ then $\widehat{g}(u) = 0$, which implies

$$0 = \sigma(0) = \sigma(\widehat{g}(u)) = \sigma\Big(\sum_{j=0}^{d} \sigma(\alpha_j)u^j\Big) = \sum_{j=0}^{d} \alpha_j \sigma(u)^j = g(\sigma(u)),$$

and $\sigma(u) \in K$ is a root of g.

Therefore all reduces to check that (1.29.1) holds. We may assume that f is irreducible in $E[\mathtt{t}]$; otherwise we replace f by one of its irreducible factors. Let us denote $d := 2^m n$ with n odd, the degree of f and let us prove, by induction on m, that f has a root in K. For $m = 0$ there is nothing to prove. Suppose the result is true for polynomials whose degree has the form $2^{m-1}n'$ with n' odd. Since $\mathrm{ch}(E) = 0$

and $f \in E[\mathtt{t}]$ is irreducible, the roots of f in an algebraic closure $\overline{E}$ of E are simple, that is, f has d distinct roots $\xi_1, \ldots, \xi_d$ in $\overline{E}$. We must prove that at least one of them belongs to K. Let us consider, for every integer $s \in \mathbb{Z}$, the polynomial

$$g_s(\mathtt{t}) := \prod_{1 \leq i < j \leq d} (\mathtt{t} - \xi_i - \xi_j - s\xi_i\xi_j) \in \overline{E}[\mathtt{t}],$$

which is symmetric with respect to the symbols $\xi_1, \ldots, \xi_d$. By the Fundamental theorem of symmetric polynomials and Cardano's formulae applied to the coefficients of $f \in E[\mathtt{t}]$, it follows that $g_s \in E[\mathtt{t}]$. Moreover,

$$\deg(g_s) = \binom{d}{2} = \frac{d(d-1)}{2} = 2^{m-1}n(2^m n - 1) \quad \& \quad n' := n(2^m n - 1) \quad \text{is odd.}$$

By the induction hypothesis, for each $s \in \mathbb{Z}$ the polynomial g_s has a root in K. Thus, for each $s \in \mathbb{Z}$ there exist $1 \leq i_s < j_s \leq d$ such that $\mu_s := \xi_{i_s} + \xi_{j_s} - s\xi_{i_s}\xi_{j_s} \in K$. Since $\mathbb{Z}$ is an infinite set and $M := \{(i,j) : 1 \leq i < j \leq d\}$ is finite, the map

$$\mathbb{Z} \to M,\ s \mapsto (i_s, j_s)$$

is not injective. Therefore, there exist $r, s \in \mathbb{Z}$ such that $i_s = i_r$, $j_s = j_r$ and $s \neq r$. Hence,

$$\begin{cases} \xi_{i_r} + \xi_{j_r} - r\xi_{i_r}\xi_{j_r} = \mu_r \\ \xi_{i_r} + \xi_{j_r} - s\xi_{i_r}\xi_{j_r} = \mu_s \end{cases}$$

and so, $(s-r)\xi_{i_r}\xi_{j_r} = \mu_r - \mu_s$. Therefore,

$$\omega_2 := \xi_{i_r}\xi_{j_r} = (\mu_r - \mu_s)/(s-r) \in K$$

and also $2\omega_1 := \xi_{i_r} + \xi_{j_r} = \mu_r + r\omega_2 \in K$. Consequently, ξ_{i_r} and ξ_{j_r} are the roots of the polynomial

$$h(\mathtt{t}) := (\mathtt{t} - \xi_{i_r})(\mathtt{t} - \xi_{j_r}) = \mathtt{t}^2 - (\xi_{i_r} + \xi_{j_r})\mathtt{t} + \xi_{i_r}\xi_{j_r} = \mathtt{t}^2 - 2\omega_1\mathtt{t} + \omega_2 \in K[\mathtt{t}],$$

and all reduces to prove that at least one root of h (and so both) belongs to K. These roots are

$$\omega_1 + \sqrt{\omega_1^2 - \omega_2} \quad \& \quad \omega_1 - \sqrt{\omega_1^2 - \omega_2},$$

and so we must check that $\sqrt{\omega_1^2 - \omega_2} \in K = E[\sqrt{-1}]$. Let $\omega_1^2 - \omega_2 := a + b\sqrt{-1} \in K$, where $a, b \in E$; we look for $x, y \in E$ such that

$$a + b\sqrt{-1} = (x + y\sqrt{-1})^2 \iff a = x^2 - y^2 \quad \& \quad b = 2xy.$$

If $b = 0$, and since $a \in E^2 \cup (-E^2)$, either there exists $x \in E$ with $a = x^2$, and we choose $y = 0$ in this case, either there exists $y \in E$ such that $-a = y^2$, and then we

take $x = 0$. On the other hand, if $b \neq 0$, the searched $x, y \in E$ are solutions of the system of equations

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b. \end{cases}$$

From the second equation $y = b/2x$ and, after substituting this value in the first one, we must prove that there exists $x \in E$ such that $x^2 - b^2/4x^2 = a$. Therefore, we have to prove that the polynomial

$$\mathtt{p}(\mathtt{t}) := 4\mathtt{t}^4 - 4a\mathtt{t}^2 - b^2 \in E[\mathtt{t}]$$

has at least a root $x \in E$. We rewrite $\mathtt{p}(\mathtt{t}) = (2\mathtt{t}^2 - a)^2 - (a^2 + b^2)$, and so the root $x \in E$ we are looking for satisfies the equality

$$(2x^2 - a)^2 = (a^2 + b^2) \quad \Longrightarrow \quad 2x^2 = a \pm \sqrt{a^2 + b^2}.$$

We are going to show that there exists $x \in E$ such that $2x^2 = a + \sqrt{a^2 + b^2}$. We proved in Remark 1.20 (3) that, E^2 being an ordering in E, each sum of squares in E is a square, and so there exists $c \in E$ satisfying $c^2 := a^2 + b^2$. Moreover, we may asssume that $c > 0$ and, since

$$(c - a)(c + a) = c^2 - a^2 = b^2 \geq 0,$$

both $c + a$ and $c - a$ have the same sign. In fact, both are positive because its sum $(c + a) + (c - a) = 2c > 0$. Thus $c + a > 0$ and so $(a + c)/2$ is a square in E.

In this way, there exists $x \in E$ such that $x^2 = (a + c)/2 = (a + \sqrt{a^2 + b^2})/2$, as wanted.

To finish we prove that (3) $\Longrightarrow$ (1), and we see first that $\Sigma E^2 = E^2$. To that end it suffices to check that the sum of two squares in E is a square in E. Let $a, b \in E$ and consider the polynomial $f(\mathtt{t}) := \mathtt{t}^2 - (a + b\sqrt{-1}) \in K[\mathtt{t}]$. Since K is algebraically closed there exists $\eta := c + d\sqrt{-1} \in K$, where $c, d \in E$, such that $f(\eta) = 0$. Therefore,

$$a + b\sqrt{-1} = \eta^2 = (c + d\sqrt{-1})^2 \implies a - b\sqrt{-1} = (c - d\sqrt{-1})^2,$$

and we get

$$\begin{aligned} a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1}) &= (c + d\sqrt{-1})^2(c - d\sqrt{-1})^2 \\ &= ((c + d\sqrt{-1})(c - d\sqrt{-1}))^2 = (c^2 + d^2)^2 \in E^2. \end{aligned}$$

This implies that E is a real field. Otherwise $-1 \in \Sigma E^2 = E^2$, and so $\mathtt{t}^2 + 1$ is a reducible polynomial in $E[\mathtt{t}]$, which is false because $K = E[\mathtt{t}]/(\mathtt{t}^2 + 1)$ is a field.

To prove that E is real closed, let $L|E$ be an algebraic extension such that L is a real field. We must prove that $E = L$. Since algebraicity is a transitive property and $L[\sqrt{-1}]|L$ is an algebraic extension, the same holds for $L[\sqrt{-1}]|E$. Thus $L[\sqrt{-1}]|E[\sqrt{-1}]$ is an algebraic extension too and, since $E[\sqrt{-1}]$ is an algebraically closed field, $L[\sqrt{-1}] = E[\sqrt{-1}]$. Thus, for each $x \in L \subset L[\sqrt{-1}]$ there exist $a, b \in E$ satisfying $x := a + b\sqrt{-1}$ and, either $b = 0$ and $x = a \in E$, or $b \neq 0$ which implies that $\sqrt{-1} = (x - a)/b \in L$, that is, $-1 \in L^2 \subset \Sigma L^2$. This is impossible, because L is a real field. □

Remark 1.30 The third condition in the previous Theorem 1.29 is equivalent to: *E is a real field and $E[\sqrt{-1}]$ is an algebraically closed field.*

Exercise 1.31 (1) Let R be a real closed field and let $R_0 \subset R$ be a subfield algebraically closed in R, that is, each $x \in R$ which is algebraic over R_0 belongs to R_0. Prove that R_0 is a real closed field.

(2) Prove that $\mathbb{R}_{\text{alg}} := \{x \in \mathbb{R} : \ x \text{ is algebraic over } \mathbb{Q}\}$ is a real closed field.

Remarks and Examples 1.32 (1) The quotient fields $\mathbb{R}(\{\mathtt{t}^*\})$ and $R((\mathtt{t}^*))$ of the rings of convergent (resp. formal) Puiseux series in one variable with coefficients in $\mathbb{R}$ (resp. a real closed field R) are real closed fields.

(2) Another examples of real closed fields are the following:

(2.1) Let X be a completely regular topological space and let $\mathfrak{m}$ be a maximal ideal of the ring of continuous functions

$$\mathcal{C}(X) := \{f : X \to \mathbb{R} : f \text{ is continuous}\}.$$

Then, the quotient $\mathcal{C}(X)/\mathfrak{m}$ is a real closed field, see [He, Thm. 42].

(2.2) Let $X \subset \mathbb{R}^n$ be a semialgebraic subset and let $\mathfrak{p}$ be a prime ideal of the ring

$$\mathcal{S}(X) := \{f : X \to \mathbb{R} : \ f \text{ is continuous and semialgebraic}\}.$$

The quotient field of the domain $\mathcal{S}(X)/\mathfrak{p}$ is a real closed field, see [G4] and [Sch1].

(3) A classical result says that for every field E there exists an essentially unique algebraic extension $C|E$ such that C is algebraically closed. It is said that C is the *algebraic closure* of E. The analogous result in Real Algebra states that each ordered field $(E, \leq_E)$ admits a unique *real closure,* namely, a real closed field $(R, \leq_R)$ such that $R|E$ is an algebraic extension and the ordering $\leq_R$ extends the given ordering $\leq_E$. The proof of this result lies, essentially, on Sturm's Theorem 2.7, whose proof will be based on Bolzano's Theorem and the Intermediate Value Theorem concerning univariate polynomials with coefficients in a real closed field.

2 Real closure of an ordered field

To get a proof of Sturm's Theorem in the general setting of real closed fields we will use in a crucial way some classical theorems of Analysis concerning polynomials with coefficients in a real closed field.

Theorem 2.1 (Bolzano) *Let R be a real closed field, $f \in R[\mathtt{t}]$ and $a, b \in R$ such that $a < b$ and $f(a)f(b) < 0$. Then, there exists $x \in R$ such that $a < x < b$ and $f(x) = 0$.*

Proof. Since R is real closed, $C := R[\sqrt{-1}]$ is an algebraically closed field. Let us show that for every root $\omega := a + b\sqrt{-1} \in C \setminus R$ of f whose multiplicity is denoted $\beta := \mathrm{mult}_f(\omega)$, its conjugate $\overline{\omega} = a - b\sqrt{-1}$ is also a root of f and $\beta := \mathrm{mult}_f(\overline{\omega})$. Indeed, $f(\mathtt{t}) := (\mathtt{t} - \omega)^\beta \cdot g(\mathtt{t})$ where ω is not a root of $g \in C[\mathtt{t}]$. Let $\widehat{\sigma} : C[\mathtt{t}] \to C[\mathtt{t}]$ be the ring homomorphism induced by conjugation. Then,

$$f = \widehat{\sigma}(f) = (\mathtt{t} - \overline{\omega})^\beta \cdot \widehat{\sigma}(g),$$

which proves that $\overline{\omega}$ is a root of f and $\beta' := \mathrm{mult}_f(\overline{\omega}) \geq \beta$. Thus, there exists $h \in C[\mathtt{t}]$ such that $f(\mathtt{t}) = (\mathtt{t} - \overline{\omega})^{\beta'} h(\mathtt{t})$ and, since $\widehat{\sigma}$ is an involution that fixes f,

$$f = \widehat{\sigma}(f) = (\mathtt{t} - \omega)^{\beta'} \cdot \widehat{\sigma}(h).$$

Therefore $\beta \geq \beta' \geq \beta$. Consequently, the roots of f in $C \setminus R$ may be arranged as

$$\omega_1 := b_1 + \sqrt{-1}c_1,\ \overline{\omega}_1 := b_1 - \sqrt{-1}c_1, \ldots, \omega_s := b_s + \sqrt{-1}c_s,\ \overline{\omega}_s := b_s - \sqrt{-1}c_s,$$

where $b_j, c_j \in R$ with $c_j \neq 0$, and $\mathrm{mult}_f(\omega_j) = \mathrm{mult}_f(\overline{\omega_j}) = \beta_j$ for each $1 \leq j \leq s$. In this way, if $a_1, \ldots, a_r$ are the different roots of f in R, there exists $e \in R$ such that

$$\begin{aligned} f(\mathtt{t}) &= e \prod_{k=1}^{r} (\mathtt{t} - a_k)^{\alpha_k} \prod_{j=1}^{s} (\mathtt{t} - (b_j + \sqrt{-1}c_j))^{\beta_j} (\mathtt{t} - (b_j - \sqrt{-1}c_j))^{\beta_j} \\ &= e \prod_{k=1}^{r} (\mathtt{t} - a_k)^{\alpha_k} \prod_{j=1}^{s} ((\mathtt{t} - b_j)^2 + c_j^2)^{\beta_j}, \end{aligned}$$

where $a_k, b_j, c_j \in R$, $c_j \neq 0$ and each $\alpha_k, \beta_j > 0$. We may assume that $\alpha_k := 2\gamma_k + 1$ for each $1 \leq k \leq \ell \leq r$ and $\alpha_k := 2\gamma_k$ for $k > \ell$, where each γ_k is a nonnegative integer. Therefore $f = gh$, where

$$h(\mathtt{t}) := \prod_{k=1}^{r} (\mathtt{t} - a_k)^{\alpha_k} \prod_{j=1}^{s} ((\mathtt{t} - b_j)^2 + c_j^2)^{\beta_j} = \prod_{k=1}^{r} (\mathtt{t} - a_k)^{2\gamma_k} \prod_{j=1}^{s} ((\mathtt{t} - b_j)^2 + c_j^2)^{\beta_j}$$

is a positive semidefinite polynomial and $g(\mathtt{t}) := e\prod_{k=1}^{\ell}(\mathtt{t}-a_k) \in R[\mathtt{t}]$. We may assume that

$$a_0 = -\infty < a_1 < \cdots < a_\ell < a_{\ell+1} = +\infty.$$

Suppose there exists $0 \leq k \leq \ell$ such that $a_k < a < b < a_{k+1}$. Then $g(a)g(b) > 0$, and so

$$f(a)f(b) = g(a)h(a)g(b)h(b) = g(a)g(b)h(a)h(b) \geq 0,$$

which is false. Hence, there exists $1 \leq k \leq \ell$ with $a < a_k < b$ and $f(a_k) = 0$, and we are done. □

Notations 2.2 Given an ordered field (E, P) and $a, b \in E$ such that $a < b$, the sets

$$(a,b) := \{x \in E : a <_P x <_P b\}, \quad [a,b) := \{x \in E : a \leq_P x <_P b\},$$
$$(a,b] := \{x \in E : a <_P x \leq_P b\}, \quad [a,b] := \{x \in E : a \leq_P x \leq_P b\}.$$

are called *intervals* in E whose endpoints are a and b.

Theorem 2.3 (Intermediate Value Theorem) *Let R be a real closed field, and let $a, b \in R$ with $a < b$. Then, for each polynomial $f \in R[\mathtt{t}]$ there exists $c \in (a,b)$ such that $f(b) - f(a) = f'(c)(b-a)$.*

Proof. Consider the polynomial

$$g(\mathtt{t}) := (f(\mathtt{t}) - f(a))(b-a) - (f(b) - f(a))(\mathtt{t}-a)$$

which satisfies $g(a) = g(b) = 0$. Since

$$g'(\mathtt{t}) = f'(\mathtt{t})(b-a) - (f(b) - f(a)),$$

it is enough to prove the existence of $c \in (a,b)$ such that $g'(c) = 0$.

The set of roots of g in $(a,b]$ is finite and non-empty, because $g(b) = 0$. Thus there exists $a < b_1 \leq b$ such that $g(b_1) = 0$ and g has no root in the interval (a, b_1). Note that $g(a) = g(b_1) = 0$, and so

$$g(\mathtt{t}) = (\mathtt{t}-a)^m(\mathtt{t}-b_1)^n h(\mathtt{t}),$$

where $h \in R[\mathtt{t}]$ satisfies $h(a)h(b_1) \neq 0$ and $m, n \geq 1$. Notice that h has no root in the interval $[a, b_1]$ and so, by Bolzano's Theorem 2.1, $h(a)h(b_1) > 0$. On the other hand,

$$\begin{aligned} g'(\mathtt{t}) = m(\mathtt{t}-a)^{m-1}(\mathtt{t}-b_1)^n h(\mathtt{t}) + n(\mathtt{t}-b_1)^{n-1}(\mathtt{t}-a)^m h(\mathtt{t}) \\ + (\mathtt{t}-a)^m(\mathtt{t}-b_1)^n h'(\mathtt{t}) = (\mathtt{t}-a)^{m-1}(\mathtt{t}-b_1)^{n-1}h_1(\mathtt{t}), \end{aligned}$$

where

$$h_1(\mathtt{t}) := m(\mathtt{t}-b_1)h(\mathtt{t}) + n(\mathtt{t}-a)h(\mathtt{t}) + (\mathtt{t}-a)(\mathtt{t}-b_1)h'(\mathtt{t}).$$

Notice that

$$h_1(a)h_1(b_1) = mn(a-b_1)h(a)(b_1-a)h(b_1) = -mn(b_1-a)^2h(a)h(b_1) < 0.$$

By Bolzano's Theorem, 2.1, there exists $c \in (a,b_1) \subset (a,b)$ with $h_1(c) = 0$, and so $g'(c) = 0$. □

Corollary 2.4 *Let R be a real closed field, $f \in R[\mathtt{t}]$ a polynomial, $a, b \in R$ such that $a < b$ and $J := (a,b) \subset R$. If $f'(x) > 0$ for each $x \in J$ then, f is a strictly increasing function in J, and if $f'(x) < 0$ for each $x \in J$ then f is a strictly decreasing function in J.*

Proof. Let $x, y \in J$ with $x < y$. By Theorem 2.3 there exists a point $z \in (x,y)$ such that $f(y) - f(x) = f'(z)(y-x)$, and so the sign of the quotient $(f(y)-f(x))/(y-x)$ coincides with the sign of the derivative f' of f in J. □

Exercise 2.5 Let (E,P) be an ordered field. Prove that the following statements are equivalent:

(1) For every $a, b \in E$ such that $a <_P b$, and every polynomial $f \in E[\mathtt{t}]$ with the property $f(a)f(b) <_P 0$, there exists $x \in (a,b)$ satisfying $f(x) = 0$.

(2) The field E is real closed.

(3) For every $a, b \in E$ such that $a <_P b$ there exists $x \in [a,b]$ satisfying $f(t) \leq f(x)$ for each $t \in [a,b]$.

Remark 2.6 Exercise 2.5 shows that real closed fields are characterized by the behaviour of polynomials with respect to two basic properties of continuous functions of a real variable: Bolzano's Theorem and the fact that continuous functions attain their maximum on bounded closed intervals. Nevertheless, Brown, Craven and Pelling found in [BCP] a non real closed field satisfying the Intermediate value Theorem for polynomials.

(2.7) Sturm's Theorem. Sturm's algorithm is a basic tool to handle univariate polynomials with coefficients in a real closed field R, that allows us to determine the number of roots in an interval $(a,b) \subset R$ of a polynomial $f \in R[\mathtt{t}]$. To present it we need to introduce some terminology and a couple of auxiliary results.

(1) Given a real field R and a polynomial $f \in R[\mathtt{t}]$, the *Sturm's sequence* for f is the ordered collection of polynomials $(f_0, \ldots, f_k)$ defined as follows:

$$\begin{cases} f_0 := f, \\ f_1 := f', \\ f_{i-2} := f_{i-1}q_i - f_i : \quad f_{i-2}, f_{i-1}, f_i, q_i \in R[\mathtt{t}] \ \& \ \deg(f_i) < \deg(f_{i-1}) \text{ if } 2 \leq i \leq k, \\ f_{k-1} := f_k q_{k+1}, \end{cases}$$

Notice that Sturm's sequence for f is obtained by using Euclides algorithm to calculate the greatest common divisor of f and f' and changing the sign of the remainder of the division in each step. In particular, f_k is a greatest common divisor of f and f' and it divides each polynomial f_i.

(2) On the other hand, given an ordered sequence of non-zero elements $(a_0, \ldots, a_k)$ in R, we denote $v(a_0, \ldots, a_k)$ the number of indices i's such that $a_i a_{i+1} < 0$. If an ordered collection $(a_0, \ldots, a_k)$ contains zero elements we eliminate them keeping the order of the remaining ones; in this way we obtain a new sequence $(b_0, \ldots, b_\ell)$ without zero elements and we define

$$v(a_0, \ldots, a_k) := v(b_0, \ldots, b_\ell).$$

(3) Let $\rho \in R \setminus \{0\}$. Since $(\rho a_i)(\rho a_{i+1}) = \rho^2 a_i a_{i+1}$ we have

$$v(\rho a_0, \ldots, \rho a_k) = v(a_0, \ldots, a_k).$$

(4) Let $(f_0, \ldots, f_k)$ be the Sturm's sequence of a polynomial $f \in R[\mathtt{t}]$ and let $a \in R$ such that $f(a) \neq 0$. Then, we denote

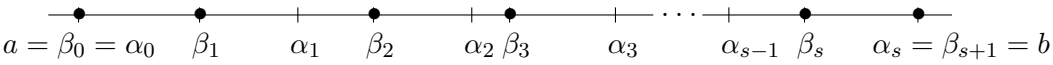
$$v(f; a) := v(f_0(a), \ldots, f_k(a)).$$

Theorem 2.8 (Sturm) *Let R be a real closed field and let $f \in R[\mathtt{t}]$ be a non-zero polynomial. Let $a, b \in R$ such that $a < b$ and $f(a)f(b) \neq 0$. Then, $v(f; a) - v(f; b)$ is the number of roots of f in the interval (a, b).*

Proof. Let $(f_0, f_1, \ldots, f_k)$ be the Sturm's sequence for f. The product $\phi := \prod_{j=0}^{k} f_j$ has a finite number of roots in R, and so there exist $\alpha_1, \ldots, \alpha_{s-1} \in R$ such that

$$a := \alpha_0 < \alpha_1 < \cdots < \alpha_{s-1} < \alpha_s := b,$$

and ϕ has no root in the union $\bigcup_{i=0}^{s-1}(\alpha_i, \alpha_{i+1})$. Let us choose an intermediate point in each interval (α_i, α_{i+1}); for example $\beta_{i+1} := (\alpha_i + \alpha_{i+1})/2$. Denote also $\beta_0 := a$ and $\beta_{s+1} := b$.



In this way, for each interval $[\beta_i, \beta_{i+1}]$ with $0 \leq i \leq s$ the following conditions hold:

(1) The product $\prod_{j=0}^{k} f_j$ has at most one root in this interval, (necessarily such a root is α_i), and it can be a common root of some of the polynomials $f_0, \ldots, f_k$.

(2) If $f_0 = f$ has a root in $[\beta_i, \beta_{i+1}]$ (necessarily such a root is α_i) it belongs to the open subinterval (β_i, β_{i+1}).

A closed interval $[\alpha, \beta]$ satisfying properties (1) y (2) above is called *a fundamental interval* for f. On the other hand, it is evident that

$$v(f; a) - v(f; b) = \sum_{i=0}^{s} (v(f; \beta_i) - v(f; \beta_{i+1})),$$

and the number of roots of f in (a, b) is the number of fundamental intervals (β_i, β_{i+1}) containing a root of f; and in fact exactly one root. Consequently, all reduces to prove that:

(3) Given a fundamental interval $[\alpha, \beta]$ for f the following equality holds:

$$v(f; \alpha) - v(f; \beta) = \begin{cases} 1 & \text{if } f \text{ has a root in the interval } (\alpha, \beta). \\ 0 & \text{otherwise.} \end{cases}$$

We distinguish two cases:

Case 1. *The polynomial f has no root in the fundamental interval $[\alpha, \beta]$.*

First, if no f_i has a root in $[\alpha, \beta]$ then, the sign of each f_i on $[\alpha, \beta]$ is constant, by Bolzano's Theorem, and so $f_i(\alpha) f_i(\beta) > 0$. Hence, $v(f; \alpha) = v(f; \beta)$.

Suppose now that $f_i(\gamma) = 0$ for some $\gamma \in [\alpha, \beta]$ and some $1 \leq i \leq k$. Note that γ is not a root of two consecutive polynomials f_{i_0}, f_{i_0+1}. Otherwise

$$f_{i_0+2}(\gamma) = f_{i_0+1}(\gamma) q_{i_0+1}(\gamma) - f_{i_0}(\gamma) = 0,$$

and continuing the process we deduce that $f_k(\gamma) = 0$. Since f_k divides f it follows that $f(\gamma) = 0$, against our assumption.

Thus, if γ is a root of f_{i_0} then, $f_{i_0-1}(\gamma) \neq 0$ and $f_{i_0+1}(\gamma) \neq 0$. This implies, by Bolzano's Theorem, that the sign of f_{i_0-1} and f_{i_0+1} on the fundamental interval $[\alpha, \beta]$ is constant, because γ is the unique root of the product $\prod_{j=0}^{k} f_j$ in the interval $[\alpha, \beta]$. Moreover,

$$f_{i_0-1}(\gamma) = f_{i_0}(\gamma) q_{i_0}(\gamma) - f_{i_0+1}(\gamma) = -f_{i_0+1}(\gamma),$$

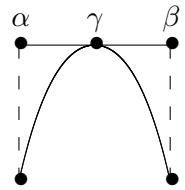
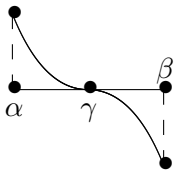
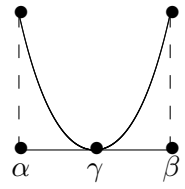
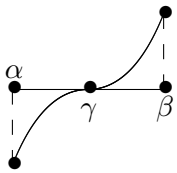
and so the signs of f_{i_0-1} and f_{i_0+1} in the interval $[\alpha,\beta]$ are opposite. Hence, independently of the signs of $f_{i_0}(\alpha)$ and $f_{i_0}(\beta)$, we have

$$v(f_{i_0-1}(\alpha), f_{i_0}(\alpha), f_{i_0+1}(\alpha)) = v(f_{i_0-1}(\beta), f_{i_0}(\beta), f_{i_0+1}(\beta)) = 1.$$

Since the sign on $[\alpha,\beta]$ of those f_k which does not vanish at γ is constant, it follows that $v(f;\alpha) = v(f;\beta)$ in this case.

Caso 2. *Suppose now that f has a root γ in the fundamental interval $[\alpha,\beta]$.*

Notice first that $v(f_0(\alpha), f_1(\alpha)) = 1$ and $v(f_0(\beta), f_1(\beta)) = 0$. To easy the checking of these equalities we draw in a picture below the different possibilities that according to Corollary 2.4 could occur, in terms of the parity of the multiplicity of γ as a root of f.

Even multiplicity		Odd multiplicity	
	$f(\alpha) < 0,\ f'(\alpha) > 0$		$f(\alpha) > 0,\ f'(\alpha) < 0$
	$f(\beta) < 0,\ f'(\beta) < 0$		$f(\beta) < 0,\ f'(\beta) < 0$
	$f(\alpha) > 0,\ f'(\alpha) < 0$		$f(\alpha) < 0,\ f'(\alpha) > 0$
	$f(\beta) > 0,\ f'(\beta) > 0$		$f(\beta) > 0,\ f'(\beta) > 0$

Recall also that $\gamma \in (\alpha,\beta)$. Next let us prove that

$$v(f_1(\alpha), \ldots, f_k(\alpha)) = v(f_1(\beta), \ldots, f_k(\beta)). \tag{2.1}$$

Each quotient $g_i := f_i/f_k \in R[\mathtt{t}]$ is a polynomial for $1 \le i \le k$ since f_k divides f_i. Notice that $g_{i-1} = g_i q_i - g_{i+1}$ for $2 \le i \le k-1$ and $g_k = 1 = \gcd(g_1, g_2)$. Moreover, the unique root of $g_1, \ldots, g_k$ in $[\alpha,\beta]$, if any, is γ; even more, γ is not a root of g_1. Indeed, let ℓ be the multiplicity of γ as a root of $f_0 = f$. Then, it is a root of multiplicity $\ell - 1$ of $f' = f_1$, and so $f_1(\mathtt{t}) := (\mathtt{t}-\gamma)^{\ell-1} h_1(\mathtt{t})$ and $f_k(\mathtt{t}) := (\mathtt{t}-\gamma)^{\ell-1} h_k(\mathtt{t})$ for some polynomials $h_1, h_k \in R[\mathtt{t}]$ with $h_1(\gamma) \neq 0 \neq h_k(\gamma)$. Thus, the quotient $g_1 = h_1/h_k$ does not vanish at γ. Now, arguing as in Case 1 (although $(g_1, \ldots, g_k)$ is not a Sturm's sequence because g_2 is not the derivative of g_1), it follows that

$$v(g_1(\alpha), \ldots, g_k(\alpha)) = v(g_1(\beta), \ldots, g_k(\beta)),$$

since g_1 has no root in (α, β). By 2.7 (3) this implies (2.1) because, for every $1 \leq i \leq k$

$$f_i(\alpha) = g_i(\alpha) f_k(\alpha) \quad \& \quad f_i(\beta) = g_i(\beta) f_k(\beta),$$

and both $f_k(\alpha)$ and $f_k(\beta)$ are not zero. □

Definitions and Remarks 2.9 (1) Sturm's algorithm provides the number of distinct roots of $f \in R[\mathtt{t}]$ in a given interval $I \subset R$. To deduce a procedure to calculate the number of roots of f in R we look for an interval $[-M, M] \subset R$, where M just depends on the coefficients of f, such that all the roots of f in R occur in $[-M, M]$.

(2) Let R be a real closed field and let $f(\mathtt{t}) := a_n \mathtt{t}^n + \cdots + a_1 \mathtt{t} + a_0 \in R[\mathtt{t}]$ be a non-zero polynomial of degree n. Let us denote $M := 1 + \sum_{j=0}^{n-1} |a_j / a_n|$.

(2.1) If $\eta \in R$ is a root of f, then $|\eta| < M$. Indeed we can suppose that $|\eta| \geq 1$ because $M > 1$. Note that

$$a_n \eta^n + \cdots + a_1 \eta + a_0 = f(\eta) = 0,$$

and we divide this equality by $a_n \eta^{n-1}$. We get

$$\eta + (a_{n-1}/a_n) + (a_{n-2}/a_n \eta) + \cdots + (a_0 / a_n \eta^{n-1}) = 0.$$

Since $|\eta| \geq 1$,

$$\begin{aligned} |\eta| = \left|(a_{n-1}/a_n) + (a_{n-2}/a_n \eta) + \cdots + (a_0/a_n \eta^{n-1})\right| \\ \leq |a_{n-1}/a_n| + |a_{n-2}/a_n| + \cdots + |a_0/a_n| < M. \end{aligned}$$

(2.2) Let $(f_0, f_1, \ldots, f_k)$ be the Sturm's sequence of f and let b_i and d_i be, respectively, the leading coefficient and the degree of f_i. Denote

$$v(f; \infty) := v(b_0, b_1, \ldots, b_k) \quad \& \quad v(f; -\infty) := v((-1)^{d_0} b_0, (-1)^{d_1} b_1, \ldots, (-1)^{d_k} b_k).$$

Then, $v(f; -\infty) - v(f; +\infty)$ is the number of roots of f in R. Indeed, by the previous Remark (2.1) and Sturm's Theorem, $v(f; -M) - v(f; M)$ is the number of roots of f in R. Therefore, it is enough to check that

$$v(f; -\infty) = v(f; -M) \quad \& \quad v(f; \infty) = v(f; M).$$

This is so because given a polynomial $f \in R[\mathtt{t}]$ of degree d with leading coefficient b, and $t \in R$ big enough, the sign of $f(t)$ coincides with the sign of b, while the sign of $f(-t)$ is the sign of $b(-1)^d$.

(2.3) A polynomial $a_0 + a_1 \mathtt{t} + \cdots + a_n \mathtt{t}^n \in R[\mathtt{t}]$ of degree n is said to be *hyperbolic* if it has n distinct roots in R. It follows from the precedent Remark (2.2) that

$f \in R[\mathtt{t}]$ is hyperbolic if and only if $d_i = 1 + d_{i-1}$ for each $1 \leq i \leq k$ and the leading coefficients of all the polynomials occurring in the Sturm's sequence for f have the same sign. Thus, if the R-vector space $R_d[\mathtt{t}]$ consisting of those polynomials in $R[\mathtt{t}]$ whose degree is $\leq d$ is identified with R^{d+1} via the map

$$R_d[\mathtt{t}] \to R^{d+1}, \sum_{j=0}^{d} a_j \mathtt{t}^j \mapsto (a_0, \ldots, a_d),$$

the subset $\mathcal{H} \subset R_d[\mathtt{t}]$ consisting of the hyperbolic polynomials is a semialgebraic set, that is, it is a finite union of subsets of R^{d+1} described by conjunctions of polynomial equalities and inequalities, see equality (4.6) in Chapter II.

(3) Let R_1 and R_2 be real closed fields and let $\varphi : R_1 \to R_2$ be a homomorphism. Then, the number of roots in R_1 of a polynomial $f(\mathtt{t}) := \sum_{j=0}^{d} a_j \mathtt{t}^j \in R_1[\mathtt{t}]$ coincides with the number of roots of $f^{\varphi}(\mathtt{t}) := \sum_{j=0}^{d} \varphi(a_j)\mathtt{t}^j \in R_2[\mathtt{t}]$ in R_2. This follows from Sturm's Theorem and Remark 2.9 (2.2) because, by Remark 1.20 (4), the signs of a and $\varphi(a)$ coincide, where a is the leading coefficient of an arbitrary polynomial in the Sturm's sequence for f.

Exercise 2.10 (1) Let $n \geq 2$ be an integer and let a, b be two non-zero real numbers. Calculate the number of real roots of $f(\mathtt{t}) := \mathtt{t}^n + a\mathtt{t} + b$ according to the values of a and b,

(2) Let a, b be two non-zero real numbers. Determine, according to the values of a and b, the number of real roots of $g(\mathtt{t}) := \mathtt{t}^5 - 5a\mathtt{t}^3 + 5a^2\mathtt{t} + 2b$.

Exercise 2.11 Let $a < b$ be real numbers and $g := g_0, g_1, \ldots, g_n \in \mathbb{R}[\mathtt{t}]$ satisfying the following conditions:

(1) For every root $t_0 \in \mathbb{R}$ of g and every small enough real number $\varepsilon > 0$, the product $g(t) \cdot g_1(t) < 0$ for each $t \in (t_0 - \varepsilon, t_0)$ and $g(t) \cdot g_1(t) > 0$ for each $t \in (t_0, t_0 + \varepsilon)$.

(2) For each $0 \leq k \leq n-1$ the polynomials g_k and g_{k+1} do not share any root in R.

(3) If $0 \leq k \leq n-1$ and $g_k(t_0) = 0$ then, $g_{k-1}(t_0)g_{k+1}(t_0) < 0$.

(4) The sign of the polynomial g_n in the open interval (a, b) is constant.

Prove that the number of roots of g in the interval (a, b) coincides with the difference

$$v(g_0(a), \ldots, g_n(a)) - v(g_0(b), \ldots, g_n(b)).$$

Exercise 2.12 (1) How many real roots has the polynomial $f(\mathtt{t}) := \sum_{j=0}^{n} \frac{\mathtt{t}^j}{j!}$?

(2) Let $f \in \mathbb{R}[\mathtt{t}]$ be a polynomial of degree 3 whose complex roots are simple. Calculate the number of real roots of the polynomial $g := 2ff'' - (f')^2$, where f' and f'' denote, respectively, the first and the second derivative of f.

Before proving the existence and uniqueness of the real closure of an ordered field we need two auxiliary lemmata.

Lemma 2.13 (1) *Let P be an ordering in a field E and let $a \in P \setminus E^2$. Let u be a root of the polynomial $\mathtt{t}^2 - a$ in an algebraic closure of E. Then, there exists an ordering Q in the field $K := E(u)$ such that $Q \cap E = P$.*

(2) *Let P be an ordering in a field E and let $b_1, \ldots, b_r \in P$. For each index $1 \leq j \leq r$, let v_j be a root of the polynomial $\mathtt{t}^2 - b_j$ in an algebraic closure of E. Then, the field $K := E(v_1, \ldots, v_r)$ admits an ordering Q such that $Q \cap E = P$.*

Proof. (1) We apply Serre's Criterion, 1.9. Thus, let $p_1, \ldots, p_r \in P \setminus \{0\}$ and $z_1, \ldots, z_r \in K$ such that $p_1 z_1^2 + \cdots + p_r z_r^2 = 0$. Since $\{1, u\}$ is a basis of K as a E-vector space, each $z_i := x_i + y_i u$ for some $x_i, y_i \in E$. Hence,

$$0 = \sum_{i=1}^{r} p_i z_i^2 = \sum_{i=1}^{r} p_i (x_i + y_i u)^2 = \sum_{i=1}^{r} p_i (x_i^2 + a y_i^2) + 2\Big(\sum_{i=1}^{r} p_i x_i y_i \Big) u.$$

Consequently,

$$\sum_{i=1}^{r} p_i x_i^2 + \sum_{i=1}^{r} a p_i y_i^2 = 0$$

and, since $p_i x_i^2 \in P$ and $a p_i y_i^2 \in P$ with $p_i \in P \setminus \{0\}$, it follows from Proposition 1.3 that $p_i x_i^2 = a p_i y_i^2 = 0$, and so $x_i = y_i = 0$, that is, $z_i = 0$ for each $1 \leq i \leq r$.

(2) Let $E_0 := E$ and $E_n := E(v_1, \ldots, v_n)$ for each $1 \leq n \leq r$. After eliminating those $b_i's$ which are squares in E_{i-1} we may assume that

$$E = E_0 \subsetneq E_1 \subsetneq \cdots \subsetneq E_{r-1} \subsetneq E_r = K,$$

where $E_{i+1} = E_i(v_{i+1})$. We argue by induction on r. For $r = 1$ it suffices to apply part (1). Let us suppose the existence of an ordering P_1 in E_{r-1} such that $P_1 \cap E = P$. By part (1) there exists an ordering Q in E_r such that $Q \cap E_{r-1} = P_1$, and so,

$$Q \cap E = Q \cap (E_{r-1} \cap E) = (Q \cap E_{r-1}) \cap E = P_1 \cap E = P;$$

we are done. □

Lemma 2.14 *Let P be an ordering in a field E and fix an algebraic closure $\overline{E}$ of E. Denote $S := \{\sqrt{x} : x \in P\}$ and let $L := E(S) \subset \overline{E}$ be the smallest subfield of $\overline{E}$ containing $E \cup S$. Then, L is a real field and each ordering Q in L satisfies $Q \cap E = P$.*

Proof. We see first that L is a real field. Otherwise there would exist $x_1, \ldots, x_s \in L$ such that $-1 = x_1^2 + \cdots + x_s^2$. Since $T := \{x_i : 1 \leq i \leq s\}$ is a finite set there exist $b_1, \ldots, b_r \in P$ such that $x_1, \ldots, x_s \in K = E(v_1, \ldots, v_r)$, where each $v_j^2 = b_j$. We have just proved in Lemma 2.13 that K is a real field, and so the equality $-1 = x_1^2 + \cdots + x_s^2$ does not hold.

For the second part, let Q be an ordering in L. If $x \in P$, then $x = (\sqrt{x})^2 \in L^2 \subset Q$. Thus $P \subset Q \cap E$ and, by Remark 1.4 (1), $P = Q \cap E$. □

Theorem 2.15 (Real closure: existence & uniqueness) (1) *Let (E, P) be an ordered field. Then, there exists a real closure R of (E, P).*

(2) *Given two real closures R_1 and R_2 of (E, P) there exists a unique E-isomorphism $\phi : R_1 \to R_2$.*

Proof. (1) Let $\overline{E}$ be an algebraic closure of E and let $\mathcal{F}$ be the set consisting of all ordered fields (K, Q_K) such that $E \subset K \subset \overline{E}$ and $P = Q_K \cap E$. Note that $\mathcal{F}$ is non-empty because it contains (E, P). Consider the order relation $\preceq$ defined in $\mathcal{F}$ by $(K_1, Q_1) \preceq (K_2, Q_2)$ if $K_1 \subset K_2$ and $Q_2 \cap K_1 = Q_1$. Notice that $(\mathcal{F}, \preceq)$ is inductive, because given a chain

$$\mathcal{C} := \{(K_i, Q_i) : i \in I\} \subset \mathcal{F}$$

we choose $K := \bigcup_{i \in I} K_i$ and $Q := \bigcup_{i \in I} Q_i$, and we see that $(K, Q) \in \mathcal{F}$ is an upper bound of $\mathcal{C}$. Indeed, it is evident that $E \subset K \subset \overline{E}$ because $E \subset K_i \subset \overline{E}$ for each $i \in I$, and to check that Q is an ordering in K it suffices to repeat the argument used in the proof of Serre's Criterion 1.9. Moreover, each $Q_i \cap E = P$, and so $Q \cap E = P$, which implies that $(K, Q) \in \mathcal{F}$ and it is an upper bound of the chain $\mathcal{C}$ because each $K_i \subset K$ and $Q \cap K_i$ is an ordering in K_i containing Q_i; by Remark 1.4 (1) this implies that $Q \cap K_i = Q_i$.

By Zorn's Lemma, $\mathcal{F}$ has a maximal element (R, Q_R), and we will prove that R is a real closed field. In such a case, since $R|E$ is an algebraic extension because $R \subset \overline{E}$, the field R is a real closure of (E, P).

Let us prove that all real algebraic extensions of R are trivial. By Lemma 2.14, the smallest field $R \subset L \subset \overline{E}$ containing square roots of all elements in Q_R is a real field. Moreover, if Q_L is an ordering in L we have $Q_L \cap R = Q_R$. In particular, $E \subset L \subset \overline{E}$ and

$$Q_L \cap E = Q_L \cap (R \cap E) = (Q_L \cap R) \cap E = Q_R \cap E = P.$$

Therefore, $(L, Q_L) \in \mathcal{F}$ and $(R, Q_R) \preceq (L, Q_L)$. Thus, (R, Q_R) being a maximal element in $\mathcal{F}$, the equality $R = L$ follows. Hence, for every $x \in Q_R$ there exists

$\sqrt{x} \in L = R$, and so $x = (\sqrt{x})^2 \in R^2$, that is, $Q_R \subset R^2$, and consequently $Q_R = R^2$. This implies, by Remark 1.20 (3), that R^2 is the unique ordering in R.

To finish, let $K|R$ be a real algebraic extension; we must see that $K = R$. Note that given an ordering Q_K in K,

$$E \subset R \subset K \subset \overline{E} \quad \text{and} \quad R^2 \subset K^2 \cap R \subset Q_K \cap R.$$

Moreover, R^2 being an ordering in R, we deduce that $Q_K \cap R = R^2$. Consequently,

$$Q_K \cap E = (Q_K \cap R) \cap E = R^2 \cap E = P,$$

that is, the pair $(K, Q_K) \in \mathcal{F}$ and $(R, R^2) \preceq (K, Q_K)$. Since (R, R^2) is a maximal element of $\mathcal{F}$, we deduce that $R = K$. Hence, R admits no proper real algebraic extension, and so R is a real closed field. Consequently, it is a real closure of (E, P).

To approach the uniqueness we prove first the following more general statement, that will be needed in the solution of **H17**:

(2.15.1) *Let R be a real closure of the ordered field (E, P) and let R_1 be a real closed field containing E as a subfield that satisfies $P = R_1^2 \cap E$. Then, there exists a unique E-homomorphism $\psi : R \to R_1$.*

Let $\mathcal{F}$ be the set consisting of all pairs (K, φ), where K is a field extension of E contained in R and $\varphi : K \to R_1$ is an E-homomorphism such that $\varphi(K \cap R^2) \subset R_1^2$. The set $\mathcal{F}$ is non-empty because the pair $(E, \mathtt{j}) \in \mathcal{F}$, where $\mathtt{j} : E \hookrightarrow R_1$ denotes the inclusion map. In fact, $P = E \cap R^2$ because R is a real closure of (E, P), and so

$$\mathtt{j}(E \cap R^2) = \mathtt{j}(P) = P = R_1^2 \cap E \subset R_1^2.$$

Define in $\mathcal{F}$ the order relation $(K_1, \varphi_1) \preceq (K_2, \varphi_2)$ if $K_1 \subset K_2$ and $\varphi_2|_{K_1} = \varphi_1$. Given a chain $\mathcal{C} := \{(K_i, \varphi_i) : i \in I\} \subset \mathcal{F}$ the pair (K, φ), where

$$K := \bigcup_{i \in I} K_i \quad \& \quad \varphi : K \to R_1,\ x \mapsto \varphi_i(x) \quad \text{if } x \in K_i$$

is an upper bound of $\mathcal{C}$ in $\mathcal{F}$. Hence, $(\mathcal{F}, \preceq)$ is an inductive ordered set and, by Zorn's Lemma, there exists a maximal element $(L, \psi) \in \mathcal{F}$. Let us show that $L = R$, and so $\psi : R \to R_1$ is the homomorphism we are looking for. Each $a \in R$ is algebraic over L, because the field extension $R|L$ is algebraic since so is $R|E$. Let us prove that $a \in L$. Consider the irreducible polynomial $f \in L[\mathtt{t}]$ of a over L and let us denote

$$a_1 < \cdots < a_j = a < \cdots < a_r$$

the roots of f in R. According to Remark 2.9 (3), and using the notations introduced there, the number of roots of $f(\mathtt{t}) := \sum_{j=0}^{d} c_j \mathtt{t}^j$ in R coincides with the number of

roots of $f^{\psi}(\mathtt{t}) := \sum_{j=0}^{d} \psi(c_j)\mathtt{t}^j$ in R_1. Let $b_1 < \cdots < b_r$ be the roots of f^{ψ} in R_1 and let $\phi : L(a) \to R_1$ be the unique homomorphism that maps a to $b := b_j$ and satisfies $\phi|_L = \psi$. Let us see that ϕ is order preserving, that is, $\phi(R^2 \cap L(a)) \subset R_1^2$.

Given $y \in R^2 \cap L(a)$, note that $y, a_2 - a_1, \ldots, a_r - a_{r-1} \in R^2$. Let $z, z_2, \ldots, z_r \in R$ such that

$$y = z^2 \quad \& \quad z_i^2 = a_i - a_{i-1} \quad \text{for each index } 2 \leq i \leq r.$$

The field $L_1 := L(a_1, \ldots, a_r, z, z_2, \ldots, z_r)$ is an algebraic extension of $L(a)$, and so it is an algebraic extension of L. By the Primitive Element Theorem, there exists $\theta \in R$ such that $L_1 := L(\theta)$. Let g be the irreducible polynomial of θ over L. Since g has at least one root in R, it follows from Remark 2.9 (3) that the polynomial g^{ψ} has at least one root ρ in R_1. Therefore, there exists a homomorphism $\Psi : L(\theta) \to R_1$ such that $\Psi|_{L(a)} = \phi$ and $\Psi(\theta) = \rho$; in particular $\Psi|_L = \psi$. Notice that for each $2 \leq i \leq r$ we have

$$\Psi(a_i) - \Psi(a_{i-1}) = \Psi(a_i - a_{i-1}) = \Psi(z_i^2) = \Psi(z_i)^2 > 0.$$

Moreover, $f^{\phi} = f^{\psi}$ is the irreducible polynomial of each b_j over $\phi(L)$, and consequently there exists an index $k(i)$ determined by i such that $\Psi(a_i) = b_{k(i)}$. Thus $\Psi(a_i) = b_i$ for each $1 \leq i \leq r$. Then, $\Psi|_{L(a)} = \phi$, and so $\Psi|_L = \psi$. Even more, since $\psi(y) = \Psi(y) = \Psi(z^2) = \Psi(z)^2 > 0$, the homomorphism Ψ is order preserving, and the same holds true for ϕ.

But, (L, ψ) being a maximal element of $\mathcal{F}$ with $(L, \psi) \preceq (L(a), \phi)$, we deduce that $L = L(a)$ or, equivalently, $a \in L$ as we want to prove.

Let us prove the uniqueness of the E-homomorphism $\psi : R \to R_1$. Consider another E-homomorphism $\psi_1 : R \to R_1$ and let $a \in R$. Let f be the irreducible polynomial of a over E. Let $a_1 < \cdots < a_j = a < \cdots < a_r$ the roots of f in R. By Remark 2.9 (3), f^{ψ} has, exactly, r distinct roots in R_1, say $b_1 < \cdots < b_r$. Since both ψ and ψ_1 are order preserving E-homomorphisms,

$$\psi(a) = \psi(a_j) = b_j = \psi_1(a_j) = \psi_1(a),$$

which proves the equality $\psi = \psi_1$, and so (2.15.1) is proved.

(2.15.2) Finally, let R_1 and R_2 be two real closures of (E, P). From (2.15.1), there exists an E-homomorphism $\phi : R_1 \to R_2$, and we must show that it is an isomorphism and it is the unique one. By (2.15.1) there exists also an E-homomorphism $\phi' : R_2 \to R_1$, and so $\phi' \circ \phi : R_1 \to R_1$ and $\phi \circ \phi' : R_2 \to R_2$ are E-homomorphisms. The identity maps $\mathrm{id}_{R_1} : R_1 \to R_1$ and $\mathrm{id}_{R_2} : R_2 \to R_2$ are E-homomorphisms, and the uniqueness part of (2.15.1) implies that $\phi' \circ \phi = \mathrm{id}_{R_1}$ and $\phi \circ \phi' = \mathrm{id}_{R_2}$. This proves that $\phi : R_1 \to R_2$ is an isomorphism, and we see now that it is the unique one. Let $\psi : R_1 \to R_2$ be another E-isomorphism; then $\psi^{-1} \circ \phi : R_1 \to R_1$ and

$\mathrm{id}_{R_1} : R_1 \to R_1$ are E-homomorphisms; using (2.15.1) once more it follows that $\psi^{-1} \circ \phi = \mathrm{id}_{R_1}$, that is, $\phi = \psi$. □

Remarks 2.16 (1) The uniqueness of the real closure R of an ordered field (E, P) is stronger than the one of the algebraic closure of E, because the unique E-automorphism of R is the identity, and this does not happen with the algebraic closure (consider $E = \mathbb{R}$ and the complex conjugation).

(2) If a real field E admits a unique ordering P we say that the real closure of the ordered field (E, P) is *the real closure of* E.

Exercise 2.17 Let (E, P) be an ordered field and let $f \in E[\mathtt{t}]$ be an irreducible polynomial such that $f(a)f(b) < 0$ for some $a, b \in E$. Prove that the quotient $K := E[\mathtt{t}]/(f)$ is a field extension of E which admits an ordering Q such that $Q \cap E = P$.

Exercise 2.18 Let E be a field, P an ordering in $E(\mathtt{t})$ and let R be a real closure of $(E, E \cap P)$. Prove the existence of a unique ordering Q in $R(\mathtt{t})$ with $Q \cap E(\mathtt{t}) = P$.

Exercise 2.19 Let R be a real closed field, $\mathtt{x}_1, \ldots, \mathtt{x}_n$ variables over R and let θ be an algebraic element over the field $R_n := R(\mathtt{x}_1, \ldots, \mathtt{x}_n)$. Let $f \in R[\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{y}]$ be an irreducible polynomial, where $\mathtt{y}$ denotes a single variable over R_n, satisfying $f(\mathtt{x}_1, \ldots, \mathtt{x}_n, \theta) = 0$. Let $a := (a_1, \ldots, a_n) \in R^n$ and $b \in R$ such that $f(a, b) = 0$ and the partial derivative $D_{n+1}f(a, b) \neq 0$. Prove that $K := R_n(\theta)$ is a real field.

Exercise 2.20 Let $u \in \mathbb{C}$ be an algebraic number over $\mathbb{Q}$ and $E := \mathbb{Q}(u)$.

(1) Show that there are as many field homomorphisms $E \to \mathbb{R}_{\mathrm{alg}}$ as orderings in E.

(2) Suppose that $u \neq 0$. Prove that u is a sum of squares in E if and only if $\varphi(u) > 0$ for every field homomorphism $\varphi : E \to \mathbb{R}_{\mathrm{alg}}$.

(3) Find a subfield $E \subset \mathbb{R}_{\mathrm{alg}}$ admitting infinitely many orderings.

Exercise 2.21 (1) Let E be a real field and let E^* be the multiplicative group consisting of non-zero elements in E. Let $E^{*2} := \{x^2 : x \in E^*\}$. Prove that if E^{*2} is a subgroup of E^* of finite index, then E enjoys the extension property, (see Exercise 1.23).

(2) Let R be the real closure of an ordered field (E, P) and let $a_1, \ldots, a_m \in E \setminus E^2$. Prove that the set

$$\mathcal{F} := \{L \text{ is a field} : \ E \subset L \subset R \quad \text{and each } a_i \notin L^2\}$$

admits some maximal element L, and that this field enjoys the extension property.

Remark 2.22 Second part of Exercise 2.21 has been taken from Endler and Viswanathan, [EV], where they analyze a generalization of a construction due to Artin.

3 Solution of Hilbert's 17th Problem

As we announced in the Introduction, we will use the theory of ordered fields studied in the precedent sections to solve Hilbert's 17th Problem. In fact we will prove the following statement, which is a stronger formulation than the one presented in the first section.

Theorem 3.1 (Artin's Theorem) *Let E be a real field admitting a unique ordering. Let R be its real closure and let $f \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$. Then, the following statements are equivalent.*

(1) *The polynomial f is a sum of squares in the field $E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ of rational functions.*

(2) *The polynomial f satisfies $f(x) \geq 0$ for every point $x \in R^n$.*

Indeed (1) $\Longrightarrow$ (2) is almost straightforward. Observe that given a real closed field R whose order relation is denoted $<$, the space R^n is endowed with the topology having the *cubes* $(p - \varepsilon,\ p + \varepsilon)^n$, where $p \in R^n$ and ε is a positive element in R, as a basis of open subsets. This is the so called *order topology* or *Euclidean topology* in R^n. Notice that if $R = \mathbb{R}$ this is the Euclidean topology of $\mathbb{R}^n$.

Let $C := R(\sqrt{-1})$ denote the algebraic closure of R. The topology induced in C^n by the Euclidean topology in R^{2n} via the bijection

$$C^n \to R^{2n},\ (x_1 + \sqrt{-1}y_1, \ldots, x_n + \sqrt{-1}y_n) \mapsto (x_1, \ldots, x_n, y_1, \ldots, y_n)$$

is called the *Euclidean topology* in C^n. If $K = R$ or $K = C$, the polynomial function $f : K^n \to K$ associated to a polynomial $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ is continuous, since it is a sum of products of projections $\pi_i : K^n \to K$, $(x_1, \ldots, x_n) \mapsto x_i$ and constant functions, which are continuous because the Euclidean topology of K^n is obtained as the product topology of the Euclidean topology of K.

Proposition 3.2 (Identity Principle) *Let R be a real closed field and let us denote $C = R(\sqrt{-1})$ its algebraic closure; denote indistinctly $K = R$ or $K = C$. Let $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be a non-zero polynomial. Then,*

$$D_f := \{x \in K^n : f(x) \neq 0\}$$

is a dense subset of K^n in the Euclidean topology.

Proof. Let us denote

$$\mathcal{Z}(f) := \{x \in K^n : \ f(x) = 0\} = K^n \setminus D_f,$$

and we argue by induction on n. For $n = 1$ the set $\mathcal{Z}(f)$ is the set of roots of f in K, and so it is finite. Thus D_f is a dense subset of K. Suppose the result is true for polynomials in $K[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$, and write $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ and

$$f = a_0(\mathtt{x}') + a_1(\mathtt{x}')\mathtt{x}_n + \cdots + a_m(\mathtt{x}')\mathtt{x}_n^m,$$

where each $a_j \in K[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$. Suppose, by way of contradiction, that D_f is not a dense subset of K^n. Then, there exist non-empty open subsets $U_i \subset K$ in the Euclidean topology, for $1 \leq i \leq n$, whose product

$$U := \prod_{i=1}^{n} U_i \subset K^n$$

does not intersect D_f, that is, $U \subset \mathcal{Z}(f)$. For each $x' \in U' := \prod_{i=1}^{n-1} U_i$, the univariate polynomial $f(x', \mathtt{x}_n) \in K[\mathtt{x}_n]$ vanishes identically on the non-empty open subset U_n of K, and so it is the zero polynomial. Thus $a_j(x') = 0$ for $0 \leq j \leq m$ and each $x' \in U'$. Hence $D_{a_j} \cap U' = \varnothing$ and, by induction, $a_j(\mathtt{x}') = 0$, that is, $f = 0$. □

Corollary 3.3 *Given a real closure R of the ordered field (E, P) and a polynomial $f \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ which is a sum of squares in $E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$, then $f(x) \geq 0$ for every point $x \in R^n$.*

Proof. Let $f_1, \ldots, f_r, g \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ such that $g \neq 0$ and $f := \sum_{i=1}^{r} (f_i/g)^2$. Then,

$$D_g = \{x \in R^n : g(x) \neq 0\} \subset \{x \in R^n : f(x) \geq 0\} = C.$$

The set C is a dense subset of R^n because, by the Identity Principle, so is D_g. Moreover, C is a closed subset of R^n because polynomial functions are continuous. Hence $C = R^n$, that is, $f(x) \geq 0$ for every point $x \in R^n$. □

Remarks 3.4 (1) Thus, all we need to prove is (2) $\Longrightarrow$ (1) in Artin's Theorem 3.1. Before that, it should be pointed out that Corollary 2 in page 278 in the classical book *Algebra* [L2] by Lang states a stronger result than Theorem 3.1. Namely, Lang substitutes condition (2): "$f(x) \geq 0$ for every point $x \in R^n$" by

$$(2)' : f(x) \geq 0 \quad \text{for every point } x \in E^n,$$

but this statement is not true in general. Fix in the field $\mathbb{Q}(\mathtt{t})$ of rational functions over $\mathbb{Q}$ in one variable the order that makes $\mathtt{t} > q$ for every $q \in \mathbb{Q}$.

Consider in $E := \mathbb{Q}(\mathtt{t}^2)$ the restriction P of the ordering fixed in $\mathbb{Q}(\mathtt{t})$, and let $f := (\mathtt{x}^2 - \mathtt{t}^2)(\mathtt{x}^2 - 4\mathtt{t}^2) \in E[\mathtt{x}]$. It is easily seen that $f(x) > 0$ for every $x \in E$. However $f(3t/2) < 0$, and so f is not a sum of squares of rational functions in $R(\mathtt{x})$, where R is the real closure of (E, P).

(2) The polynomial used in (1) above is reducible in $E[\mathtt{x}]$, but Dubois proved in [Du] that condition (2)′ above does not imply that f is a sum of squares in $R(\mathtt{x}_1, \ldots, \mathtt{x}_n)$, even for irreducible polynomials $f \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$. To that end consider the unique ordering P_1 in $\mathbb{Q}(\mathtt{t})$ making $\mathtt{t}$ positive but smaller than every positive rational number. Let R be a real closure of $(\mathbb{Q}(\mathtt{t}), P_1)$ and let E be the subfield of R consisting of those elements which can be obtained from $\mathbb{Q}(\mathtt{t})$ by means of a finite sequence of rational operations and radicals. Let $P := R^2 \cap E$ and the polynomial $f(\mathtt{x}) := (\mathtt{x}^3 - \mathtt{t})^2 - \mathtt{t}^3 \in E[\mathtt{x}]$, where $\mathtt{x}$ denotes a variable over $\mathbb{Q}(\mathtt{t})$. Since $f(1)$ and $f(\mathtt{t}^{1/3})$ have opposite signs, f is not a sum of squares in $R(\mathtt{x})$. However, it can be proved that $f(x) \geq 0$ for every $x \in E$.

We will prove a stronger result than Artin's Theorem, called Artin-Lang's theorem, that will be useful in the next chapter.

Theorem 3.5 (Artin-Lang's Theorem) *Let R be the real closure of the ordered field (E, P) and let $E_n := E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ be the field of rational functions with coefficients in E. Let Q_n be an ordering in E_n with $Q_n \cap E = P$, and $f_1, \ldots, f_r \in Q_n \setminus \{0\}$. Then, there exists $x \in R^n$ such that each rational function is defined in x and $f_i(x) > 0$ in R.*

Before proving Artin-Lang's Theorem 3.5 let us see that it implies Artin's Theorem, 3.1. Let E be a field which admits a unique ordering P, and let $f \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be a polynomial which is not a sum of squares in $E_n = E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$. Then there exists, by Proposition 1.19, an ordering Q_n in E_n such that $-f \in Q_n \setminus \{0\}$. Since P is the unique ordering in E we have $Q_n \cap E = P$, and it follows from Artin-Lang's Theorem 3.5 that there exists a point $x \in R^n$ such that f is defined in x and $-f(x) > 0$, against the hypothesis.

Thus, until the end of this section our goal is to prove Artin-Lang's Theorem, 3.5. To that end we introduce now a key notion.

Definition 3.6 Let R be a real closure of the ordered field (E, P) and fix an ordering Q_n in the field $E_n := E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ such that $Q_n \cap E = P$. Let $\{f_1, \ldots, f_r\} \subset E_n[\mathtt{t}]$. We say that a property $\mathcal{P}$ satisfied by these polynomials is *specializable* if there exists

a finite subset $\mathcal{F} := \{\psi_1, \ldots, \psi_\ell\}$ of E_n such that each $\psi_j \in Q_n \setminus \{0\}$ and whenever the rational functions $\psi_1, \ldots, \psi_\ell$ are defined in a point $x \in R^n$ and $\psi_j(x) > 0$ in R for each $1 \leq j \leq \ell$ then, the coefficients of each rational function $f_i(\mathtt{x}, \mathtt{t}) \in E_n[\mathtt{t}]$ are defined in x and the polynomials $f_1(x, \mathtt{t}), \ldots, f_r(x, \mathtt{t}) \in R[\mathtt{t}]$ enjoy property $\mathcal{P}$.

Lemma 3.7 *The property* "a non-zero polynomial $f \in E_n[\mathtt{t}]$ has exactly r roots in a real closure R_n of (E_n, Q_n)" *is specializable.*

Proof. Let us denote $(f_0 = f, f_1 = f', f_2, \ldots, f_k)$ the Sturm's sequence of f. Recall that $f_0 = f,\ f_1 = f',\ f_k = \gcd(f, f')$ and

$$\begin{cases} f_{i-2} = f_{i-1}q_i - f_i, & \text{where} \quad f_{i-1}, f_i, q_i \in E_n[\mathtt{t}], \quad \& \\ \deg(f_i) < \deg(f_{i-1}) & \text{for} \quad 2 \leq i \leq k. \end{cases}$$

Let b_i and d_i denote, respectively, the leading coefficient and the degree of f_i. By Remark 2.9 the number N of roots of f in R_n is given by

$$N := v(b_0, b_1, \ldots, b_k) - v((-1)^{d_0}b_0, (-1)^{d_1}b_1, \ldots, (-1)^{d_k}b_k).$$

For each index $0 \leq j \leq k$, choose $\varepsilon_j, \delta_j \in \{-1, +1\}$ such that the rational functions $\varphi_j := \varepsilon_j b_j$ and $\phi_j := \delta_j(-1)^{d_j}b_j$ are positive with respect to the ordering Q_n in E_n. Let $\psi_1, \ldots, \psi_\ell \in E_n$ be the squares of the non identically zero coefficients of the polynomials $f_0, \ldots, f_k, q_2, \ldots, q_k$. We claim that the finite set

$$\mathcal{F} := \{\varphi_0, \ldots, \varphi_k, \phi_0, \ldots, \phi_k, \psi_1, \ldots, \psi_\ell\}$$

satisfies the conditions that guarantee that the property in the statement is specializable. Indeed, let $x \in R^n$ such that

$$\varphi_0(x), \ldots, \varphi_k(x), \phi_0(x), \ldots, \phi_k(x), \psi_1(x), \ldots, \psi_\ell(x)$$

are positive in the ordering in R.

Observe first that the positivity of the rational functions $\psi_1(x), \ldots, \psi_\ell(x)$ guarantees that $(f_0(x, \mathtt{t}), \ldots, f_k(x, \mathtt{t}))$ is the Sturm's sequence of $f(x, \mathtt{t}) \in R[\mathtt{t}]$, and so

$$N(x) := v(b_0(x), b_1(x), \ldots, b_k(x)) - v((-1)^{d_0}b_0(x), (-1)^{d_1}b_1(x), \ldots, (-1)^{d_k}b_k(x))$$

is the number of roots in R of $f(x, \mathtt{t})$. On the other hand, since $\varphi_0(x), \ldots, \varphi_k(x)$ are positive,

$$v(b_0(x), b_1(x), \ldots, b_k(x)) = v(b_0, b_1, \ldots, b_k),$$

and the positivity of $\phi_0(x), \ldots, \phi_k(x)$ implies that

$$v((-1)^{d_0}b_0(x), (-1)^{d_1}b_1(x), \ldots, (-1)^{d_k}b_k(x)) = v((-1)^{d_0}b_0, (-1)^{d_1}b_1, \ldots, (-1)^{d_k}b_k).$$

Consequently, $N = N(x)$, as wanted. □

Lemma 3.8 *Let $f_1, \dots, f_r \in E_n[\mathtt{t}]$. The property* "each polynomial f_i has some root ρ_i in a real closure R_n of (E_n, Q_n), and such roots satisfy the strict inequalities $\rho_1 < \cdots < \rho_r$", *is specializable.*

Proof. For each index $2 \leq j \leq r$ let $z_j := \sqrt{\rho_j - \rho_{j-1}} \in R_n$. Both ρ_i and z_j are algebraic over E_n, because $R_n|E_n$ is an algebraic field extension. Henceforth, if we denote

$$L_n := E_n(\rho_1, \dots, \rho_r, z_2, \dots, z_r) \subset R_n,$$

the subextension $L_n|K_n$ of $R_n|K_n$ is finite, and so it admits a primitive element θ. Since $z_j \neq 0$ there exists $t_j \in E_n(\theta)$ such that $z_j t_j = 1$.

Let $g \in E_n[\mathtt{t}]$ be the irreducible polynomial of θ over E_n and let $p_i, q_j, m_j \in E_n[\mathtt{t}]$ such that $\rho_i = p_i(\theta)$, $z_j = q_j(\theta)$ and $t_j = m_j(\theta)$. Since

$$f_i(p_i(\theta)) = f_i(\rho_i) = 0, \quad q_j^2(\theta) = z_j^2 = \rho_j - \rho_{j-1} = p_j(\theta) - p_{j-1}(\theta),$$
$$\& \quad q_j(\theta)m_j(\theta) - 1 = z_j t_j - 1 = 0,$$

and g is the irreducible polynomial of θ over E_n, there exist $a_i, b_j, c_j \in E_n[\mathtt{t}]$ such that

$$f_i(p_i) = g a_i, \quad q_j^2 - (p_j - p_{j-1}) = g b_j \quad \& \quad q_j m_j - 1 = g c_j. \tag{3.1}$$

Let $h_1, \dots, h_\ell \in E_n$ be the squares of all non-zero coefficients of the polynomials $g, f_i, p_i, a_i, q_j, b_j, m_j, c_j \in E_n[\mathtt{t}]$. Since $\theta \in R_n$ is a root of g it follows from Lemma 3.7 the existence of positive rational functions $\phi_1, \dots, \phi_s \in E_n$ with respect to the ordering Q_n such that whenever $\phi_1(x), \dots, \phi_s(x) > 0$ for a point $x \in R^n$ then, the polynomial $g(x, \mathtt{t}) \in R_n[\mathtt{t}]$ has a root in R.

We claim that if $x \in R^n$ and $h_1(x), \dots, h_\ell(x), \phi_1(x), \dots, \phi_s(x)$ are positive in R then, each polynomial $f_i(x, \mathtt{t}) \in R_n[\mathtt{t}]$ has a root β_i in R satisfying $\beta_1 < \cdots < \beta_r$. In fact, if

$$h_1(x), \dots, h_\ell(x), \phi_1(x), \dots, \phi_s(x) > 0,$$

all the coefficients of the polynomials

$$g(x, \mathtt{t}), f_i(x, \mathtt{t}), p_i(x, \mathtt{t}), a_i(x, \mathtt{t}), q_j(x, \mathtt{t}), b_j(x, \mathtt{t}), m_j(x, \mathtt{t}), c_j(x, \mathtt{t}) \in R[\mathtt{t}]$$

are well defined, and $g(x, \mathtt{t}) \in R[\mathtt{t}]$ has a root γ in R. Let $\beta_i := p_i(x, \gamma)$ for $1 \leq i \leq r$. Since $g(x, \gamma) = 0$, we deduce from (3.1) that

$$f_i(x, \beta_i) = 0, \quad \beta_j - \beta_{j-1} = q_j(x, \gamma)^2 \quad \& \quad q_j(x, \gamma)m_j(x, \gamma) = 1,$$

and so β_i is a root of $f_i(x, \mathtt{t}) \in R[\mathtt{t}]$ and $\beta_1 < \cdots < \beta_r$, as wanted. □

Proof of Artin-Lang's Theorem. We must prove the existence of a point $x \in R^n$ such that the rational functions $f_1, \ldots, f_r$ are defined in x and $f_1(x), \ldots, f_r(x) > 0$ in the unique ordering of R.

PRELIMINARY PREPARATION. There exist polynomials $p_1, \ldots, p_r, q \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ such that each $f_j := p_j/q = (p_j q)/q^2$, and so, if $x \in R^n$ satisfies $q(x) \neq 0$ then, $f_j(x) > 0$ if and only if $(p_j q)(x) > 0$. Therefore, after substituting f_j by $p_j q$, we may assume from the beginning that the rational functions $f_j \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ are polynomials.

Since $E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ is an UFD each polynomial f_j factorizes $f_j := g_j^2 \prod_{k=1}^{s_j} p_{jk}$ where $g_j, p_{jk} \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ and the polynomials p_{jk} are irreducible and pairwise distinct. Note that since g_j^2 is positive, the sign of f_j in $E_n := E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ is determined by the signs of the factors p_{jk}. Hence, we may assume from the beginning that the rational functions f_j are irreducible polynomials in $E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$.

DEVELOPMENT OF THE PROOF. We are ready to approach the proof of the theorem. We argue by induction on n, and we begin with $n = 1$. Let $\beta_1 < \cdots < \beta_s$ be the roots in R of the irreducible polynomials $f_1, \ldots, f_r \in E[\mathtt{x}_1]$. Let R_1 be a real closure of the ordered field $(E_1, Q_1) := (E(\mathtt{x}_1), Q_1)$. Since the ordering Q_1 in E_1 extends P we have

$$P = Q_1 \cap E = (R_1^2 \cap E_1) \cap E = R_1^2 \cap (E_1 \cap E) = R_1^2 \cap E,$$

and, by (2.15.1), there exists a unique E-homomorphism $R \to R_1$. Since field homomorphisms are injective we may assume that this last is an inclusion, that is, $R \subset R_1$. Notice that $\mathtt{x}_1 \neq \beta_k$ for each $1 \leq k \leq s$, because $\mathtt{x}_1$ is transcendental over E and each β_k is algebraic over E. In this way, if we denote $\beta_0 := -\infty$ and $\beta_{s+1} := +\infty$, there exists an index $0 \leq j_0 \leq s$ such that $\beta_{j_0} < \mathtt{x}_1 < \beta_{j_0+1}$. The algebraic closure of the real closed field R is $R(\sqrt{-1})$, and so each f_k factorizes in $R[\mathtt{x}_1]$ as

$$f_k(\mathtt{x}_1) := a_k(\mathtt{x}_1 - \beta_{k_1}) \cdots (\mathtt{x}_1 - \beta_{k_{t_k}}) \prod_{l=1}^{s_j} F_{kl}(\mathtt{x}_1),$$

where $a_k \in E$, each polynomial $F_{kl}(\mathtt{x}_1)$ has the form $(\mathtt{x}_1 - \gamma)^2 + \delta^2$, and the roots β_{k_ℓ} are pairwise distinct. Consequently, the sign of f_k in (E_1, Q_1), or equivalently in R_1, just depends on the signs of the factors $\mathtt{x}_1 - \beta_{k_\ell}$ in R_1 and the sign of a_k in E. Thus, the sign of f_k just depends on the position of $\mathtt{x}_1$ in R_1 with respect to the roots $\beta_1, \ldots, \beta_s$.

Then, if we choose arbitrarily $x \in (\beta_{j_0}, \beta_{j_0+1}) \subset R$, the sign of $f_j(x)$ in R coincides with the sign of f_j in E_1, for $1 \leq j \leq r$. In particular, if we choose

$$x := \begin{cases} \beta_1 - 1 & \text{if } j_0 = 0, \\ \frac{\beta_{j_0}+\beta_{j_0+1}}{2} & \text{if } 1 \leq j_0 < s, \\ \beta_s + 1 & \text{if } j_0 = s, \end{cases}$$

the first step in the inductive argument is finished.

Suppose the result is true if the number of variables is $n \geq 1$ and let us see that it is also true if the number of variables is $n+1$. The polynomials $f_1, \ldots, f_r$ are irreducible in $E[\mathtt{x}_1, \ldots, \mathtt{x}_n][\mathtt{x}_{n+1}]$. We may assume that f_i is an irreducible polynomial in $E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ for $1 \leq i \leq \ell$ and f_j is an irreducible polynomial in $E_n[\mathtt{x}_{n+1}]$ with $\deg_{\mathtt{x}_{n+1}}(f_j) \geq 1$ for $\ell + 1 \leq i \leq r$, (eventually $\ell = 0$ or $\ell = r$).

Consider in E_n the ordering $Q_n := Q_{n+1} \cap E_n$ and denote, respectively, R_n and R_{n+1} the real closures of (E_n, Q_n) and (E_{n+1}, Q_{n+1}). We may assume by (2.15.1) that $R_n \subset R_{n+1}$.

Let $\rho_1 < \cdots < \rho_s$ be the roots in R_n of the product $f_{\ell+1} \cdots f_r$. Notice that all roots of f_i are simple because f_i is irreducible. Denote $\rho_0 := -\infty$ and $\rho_{s+1} := +\infty$. Since $\mathtt{x}_{n+1}$ is transcendental over E_n and $\rho_1, \ldots, \rho_s$ are algebraic over E there exists an index $0 \leq j_0 \leq s$ such that $\rho_{j_0} < \mathtt{x}_{n+1} < \rho_{j_0+1}$. Analogously to the case $n = 1$ we have:

(1) The signs in (E_{n+1}, Q_{n+1}) of the irreducible polynomials $f_{\ell+1}, \ldots, f_r$ just depend on the signs in (E_n, Q_n) of the respective leading coefficients $g_{\ell+1}, \ldots, g_r$ of these polynomials and the position of $\mathtt{x}_{n+1}$ with respect to the roots $\rho_1, \ldots, \rho_s$.

(2) Choose $\varepsilon_i \in \{-1, +1\}$ such that $\widetilde{g_i} = \varepsilon_i g_i \in Q_n \setminus \{0\}$ for $\ell + 1 \leq i \leq r$.

For each $1 \leq j \leq s$ let us denote $h_j \in \{f_{\ell+1}, \ldots, f_r\}$ such that $h_j(\rho_j) = 0$. Notice that ρ_j determines h_j: this last is the irreducible polynomial of ρ_j over E_n. Let s_i be the number of roots of f_i in R_n for each $\ell + 1 \leq i \leq r$.

By Lemma 3.7 applied to the polynomials $f_{\ell+1}, \ldots, f_r$, and by Lemma 3.8 applied to the family $\{h_1, \ldots, h_s\}$, there exist positive rational functions $\psi_1, \ldots, \psi_m$ in (E_n, Q_n) such that for every point $x \in R^n$ satisfying $\psi_1(x) > 0, \ldots, \psi_m(x) > 0$ in R, the following conditions hold:

(3) Each polynomial $f_i(x, \mathtt{x}_{n+1})$ is well defined and it has s_i roots in R.

(4) If $\beta_1 < \cdots < \beta_s$ are the roots in R of the polynomials $f_i(x, \mathtt{x}_{n+1})$, then β_j is a root of $h_j(x, \mathtt{x}_{n+1})$, since this is one of the polynomials $f_i(x, \mathtt{x}_{n+1})$.

Let $\Delta_{\ell+1}, \ldots, \Delta_r \in E_n$ be the squares of the discriminants of $f_{\ell+1}, \ldots, f_r$. The irreducible polynomials $f_{\ell+1}, \ldots, f_r \in E_n[\mathtt{x}_{n+1}]$ have not multiple roots, and so $\Delta_{\ell+1}, \ldots, \Delta_r$ are strictly positive elements of E_n with respect to the ordering Q_n.

Since the rational functions

$$f_1, \ldots, f_\ell,\ \widetilde{g}_{\ell+1}, \ldots, \widetilde{g}_r,\ h_1, \ldots, h_m,\ \Delta_{\ell+1}, \ldots, \Delta_r \in E_n$$

are positive in (E_n, Q_n) there exists, by the inductive hypothesis, a point $x \in R^n$ such that

$$f_1(x), \ldots, f_\ell(x),\ \widetilde{g}_{\ell+1}(x), \ldots, \widetilde{g}_r(x),\ \psi_1(x), \ldots, \psi_m(x),\ \Delta_{\ell+1}(x), \ldots, \Delta_r(x)$$

are positive in R. In particular, since $\Delta_i(x) > 0$, we deduce:

(5) *For each $\ell + 1 \leq i \leq r$ the polynomial $f_i(x, \mathtt{x}_{n+1}) \in R[\mathtt{x}_{n+1}]$ has no multiple roots.*

Denote $\beta_0 := \beta_1 - 1$ and $\beta_{s+1} := \beta_s + 1$. From (1), (2), (3), (4) and (5) it follows that for every $y \in R$ satisfying $\beta_{j_0} < y < \beta_{j_0+1}$, then $f_j(x, y) > 0$ for each $1 \leq j \leq r$. Note that $f_i(x, y) = f_i(x)$ for $1 \leq i \leq \ell$. Henceforth, choosing

$$y := \begin{cases} \beta_1 - 1 & \text{if } j_0 = 0, \\ \frac{\beta_{j_0} + \beta_{j_0+1}}{2} & \text{if } 1 \leq j_0 < s, \\ \beta_s + 1 & \text{if } j_0 = s, \end{cases}$$

the point $z := (x, y) \in R^{n+1}$ satisfies the requirements. □

Exercise 3.9 (Sign changing criterion) Let (E, P) be an ordered field, R a real closure of (E, P) and let $f \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be an irreducible polynomial. Denote F_n the quotient field of the domain $E[\mathtt{x}_1, \ldots, \mathtt{x}_n]/(f)$. Prove that there exists an ordering Q in F_n such that $Q \cap E = P$ if and only if there exist points $a, b \in R^n$ such that $f(a)f(b) < 0$.

Remark 3.10 The Sign changing criterion is due to Dubois and Efroymson, [DE]. An alternative proof can be obtained from *Knebusch Norm Theorem,* [K].

CHAPTER II

Real Algebra

1 Real rings

In this Chapter we present solutions to two main problems in Real Algebra: the Real Nullstellensatz and the Positivstellensätze. In what follows all rings are commutative with unit, R denotes a real closed field and we shorten $R[\mathtt{x}] := R[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ and $R(\mathtt{x})$ its quotient field.

Real Nullstellensatz. Let $\mathfrak{a} \subset R[\mathtt{x}]$ be an ideal and let $Z \subset R^n$ be a subset. Denote

$$\mathcal{Z}(\mathfrak{a}) := \{x \in R^n : \ f(x) = 0 \quad \forall\, f \in \mathfrak{a}\} \quad \&$$
$$\mathcal{I}(Z) := \{f \in R[\mathtt{x}] : \ f(x) = 0 \quad \forall x \in Z\}.$$

It is straightforward to check that $\mathcal{I}(Z)$ is an ideal of $R[\mathtt{x}]$ and that $\mathfrak{a} \subset \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$. One of our goals is to determine the relationship between the ideals $\mathfrak{a}$ and $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ and, in particular, to decide under what conditions the equality $\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ holds.

Positivstellensätze. Given polynomials $g_1, \ldots, g_r, f \in R[\mathtt{x}]$ one looks for necessary and sufficient conditions to guarantee that $f(x) \geq 0$ for each point x of a basic closed semialgebraic set $S := \{x \in R^n : g_1(x) \geq 0, \ldots, g_r(x) \geq 0\}$. Moreover, we also approach a necessary and sufficient condition for $f|_S$ being strictly positive. Equivalently, if we denote

$$T := \{x \in R^n : f(x) \geq 0\} \quad \& \quad U := \{x \in R^n : f(x) > 0\},$$

one looks for algebraic certificates (that is, equations involving $g_1, \ldots, g_r$ and f) of the inclusions $S \subset T$ and $S \subset U$, that we write using classical notation:

$$\{g_1 \geq 0, \ldots, g_r \geq 0\} \subset \{f \geq 0\} \quad \text{or} \quad \{g_1 \geq 0, \ldots, g_r \geq 0\} \subset \{f > 0\}.$$

Exercise 1.1 Let R be a real closed field and let $\mathfrak{a} \subset R[\mathtt{x}_1, \mathtt{x}_2]$ be the ideal generated by the polynomial $\mathtt{x}_1^4 + (\mathtt{x}_2 - 1)^2(\mathtt{x}_2 - 2)^2$. Determine $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$.

Exercise 1.2 Let R be a real closed field and let $g(\mathtt{x}_1) := \mathtt{x}_1^3 - 1 \in R[\mathtt{x}_1]$. Determine all polynomials $f \in R[\mathtt{x}_1]$ such that $\{g \geq 0\} \subset \{f \geq 0\}$.

Definitions and Remarks 1.3 (Prime cones) (1) The Nullstellensatz and the Positivstellensätze will follow from Artin-Lang's Theorem 3.5, (Ch.I), and some elementary notions and results of Real Algebra. In Chapter I we have studied the set of orderings of a real field, but now we need to generalize such notion to *prime cones in real rings*. Notice that given a prime ideal $\mathfrak{p}$ of a ring A, the domain $A/\mathfrak{p}$ admits a quotient field $\mathrm{qf}(A/\mathfrak{p})$, which can be real or not, and in the first case we can apply the theory developed in Chapter I. This leads us to collect those pairs $\alpha := (\mathfrak{p}, \leq)$, where $\mathfrak{p}$ is a prime ideal of A, such that the quotient $\kappa(\mathfrak{p}) := \mathrm{qf}(A/\mathfrak{p})$ is a real field and $\leq$ is an ordering in $\kappa(\mathfrak{p})$. These pairs are called *prime cones* in A, and $\mathfrak{p}$ is called the *support* of α; we will write $\mathfrak{p} := \mathfrak{p}_\alpha$.

(2) A ring A is said to be *real* if it admits a prime cone.

(3) The notion of prime cone was introduced by Coste and Roy, see [CR], who endowed the set of prime cones of a real ring A with a structure of topological space, called *the real spectrum of* A, see Chapter III. This space is very useful to study the algebraic and topological structure of real algebraic varieties, and it constitutes one of the milestones in the development of Real Algebraic Geometry since 1980.

Prime cones admit equivalent representations that we explain right now.

(1.4) First alternative definition of prime cone. Recall that an ordering in a real field is nothing else but the set of nonnegative elements with respect to an order relation compatible with addition and multiplication. With this idea in mind, let $\alpha := (\mathfrak{p}, \leq)$ be a prime cone in a ring A and let

$$\mathcal{P}_\alpha := \{f \in A : \ f + \mathfrak{p} \geq 0\} = \pi^{-1}(\mathcal{P}_\leq),$$

where $\pi : A \to A/\mathfrak{p}$ is the canonical projection and $\mathcal{P}_\leq$ is the set of nonnegative elements in $A/\mathfrak{p} \subset \kappa(\mathfrak{p})$ with respect to $\leq$. Denote

$$A^2 := \{x^2 : \ x \in A\} \quad \& \quad (-\mathcal{P}_\alpha) := \{-x : \ x \in \mathcal{P}_\alpha\}.$$

Notice that $\mathcal{P}_\alpha/\mathfrak{p} = \mathcal{P}_\leq \cap (A/\mathfrak{p})$, and it is checked straightforwardly that $\mathcal{P}_\alpha$ satisfies the following properties:

(i) $\mathcal{P}_\alpha + \mathcal{P}_\alpha \subset \mathcal{P}_\alpha$, $\mathcal{P}_\alpha \cdot \mathcal{P}_\alpha \subset \mathcal{P}_\alpha$, $A^2 \subset \mathcal{P}_\alpha$.

(ii) $-1 \notin \mathcal{P}_\alpha$.

(iii) $\mathcal{P}_\alpha \cup (-\mathcal{P}_\alpha) = A \quad \& \quad \mathcal{P}_\alpha \cap (-\mathcal{P}_\alpha) = \mathfrak{p}$.

Conversely, it is immediately seen that if $\beta \subset A$ satisfies the above properties, namely,

(i) $\beta + \beta \subset \beta$, $\beta \cdot \beta \subset \beta$, $A^2 \subset \beta$.

(ii) $-1 \notin \beta$.

(iii) $\beta \cup (-\beta) \quad \& \quad \beta \cap (-\beta) := \mathfrak{q}$ is a prime ideal,

and we define in the quotient field $\kappa(\mathfrak{q}) := \mathrm{qf}(A/\mathfrak{q})$ the order relation $\leq_\beta$ as

$$(a+\mathfrak{q})/(b+\mathfrak{q}) \geq_\beta 0 \iff ab+\mathfrak{q} \in \beta/\mathfrak{q} \iff ab \in \beta,$$

the pair $(\mathfrak{q}, \leq_\beta)$ is a prime cone in A with support $\mathfrak{q}$.

Exercise 1.5 Prove that property (iii) above is equivalent to the following property:

Given $a, b \in A$ such that $ab \in \beta$ then, either $a \in \beta$ or $-b \in \beta$.

A subset $\beta \subset A$ satisfying property (i) is said to be a *cone* in A. If it satisfies also condition (ii) it is called a *proper cone,* and we have just said that if conditions (i), (ii) and (iii) are fulfilled then β is a *prime cone.* In what follows ΣA^2 denotes the subset of A consisting of those elements that can be written as a finite sum of squares of elements in A. Note that ΣA^2 is a cone in A, and it is proper if and only if -1 is not a sum of squares in the ring A.

Remarks 1.6 (1) Note that if a cone α in A contains -1 then,

$$(2)^2 a = (a+1)^2 + (-1)(a-1)^2 \in \alpha$$

for each $a \in A$. Thus, if $1/2 \in A$ then $\alpha = A$; this is why it is said that α is not proper.

(2) Note also that the domains A of positive characteristic p admit no proper cone because, given a cone α in A we have

$$-1 = 1 + \overset{p-1}{\cdots} + 1 = 1^2 + \overset{p-1}{\cdots} + 1^2 \in \Sigma A^2 \subset \alpha.$$

(1.7) Second alternative definition of prime cone. (1) Prime cones in a real ring A may be represented as homomorphisms from A to real closed fields. Recall that given a field K and a point $p := (p_1, \ldots, p_n) \in K^n$, the *evaluation at p* is the ring epimorphism $\mathrm{ev}_p : K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to K$, $f \mapsto f(p)$, whose kernel is the maximal ideal

$$\mathfrak{m}_p := \{f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n] : f(p) = 0\} = (\mathtt{x}_1 - p_1, \ldots, \mathtt{x}_n - p_n).$$

We shall see later on that p and $\mathfrak{m}_p$ can be "identified". Moreover,

$$K \cong K[\mathtt{x}_1, \ldots, \mathtt{x}_n]/\ker \mathrm{ev}_p = K[\mathtt{x}_1, \ldots, \mathtt{x}_n]/\mathfrak{m}_p,$$

and ev_p is identified with the canonical projection

$$\pi : K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to K[\mathtt{x}_1, \ldots, \mathtt{x}_n]/\mathfrak{m}_p,\ f \mapsto f + \mathfrak{m}_p.$$

Clearly, $\mathfrak{m}_p$ and ev_p are mutually determined.

(2) In a more abstract setting, given a prime cone α in a ring A let $\kappa_\alpha := \mathrm{qf}(A/\mathfrak{p}_\alpha)$ and R_α be the real closure of the ordered field $(\kappa_\alpha, \leq_\alpha)$. Consider the ring homomorphism

$$\varphi : A \to A/\mathfrak{p}_\alpha \hookrightarrow \kappa_\alpha \hookrightarrow R_\alpha,$$

and notice that $\ker \varphi = \mathfrak{p}_\alpha$ and $\alpha = \varphi^{-1}(R_\alpha^2)$. Hence, the homomorphism φ captures all information concerning α.

In what follows we shall use in each situation the most convenient characterization of prime cone. The apparently different nature of the characterizations above provides us some versatility.

Exercise 1.8 Prove that given a ring A, a real closed field R and a ring homomorphism $\varphi : A \to R$ then, $\alpha := \varphi^{-1}(R^2)$ is a prime cone in A.

Exercise 1.9 Let $f \in \mathbb{R}[\mathtt{x}, \mathtt{y}]$ be an irreducible polynomial whose gradient $\nabla f(p)$ is not zero for some point $p \in \mathbb{R}^2$ such that $f(p) = 0$. Prove that $A := \mathbb{R}[\mathtt{x}, \mathtt{y}]/(f)$ is a real ring.

As commented previously, Artin-Lang's Theorem, 3.5 (Ch.I) is the main tool in the proof of the Real Nullstellensatz and the Positivstellensätze. However we will use a different formulation, due to Robinson [Ro], that will be presented in the next section. Before that, we characterize real rings.

Lemma 1.10 (Characterization of real rings) *Let A be a ring. The following statements are equivalent:*

(1) *The ring A contains a proper cone.*

(2) *The ring A is real.*

(3) *There exist a real closed field R and a ring homomorphism $\varphi : A \to R$.*

(4) $-1 \notin \Sigma A^2$.

Proof. (1) $\Longrightarrow$ (2) The hypothesis says that the set $\mathcal{F}$ of proper cones in A is non-empty, and we order it by inclusion. Let us check that each chain $\mathcal{C}$ in $\mathcal{F}$ has an upper bound β in $\mathcal{F}$. Then, by Zorn's Lemma, $\mathcal{F}$ admits a maximal element γ, and we will show that γ is a prime cone in A.

Indeed, it is evident that the union $\beta := \bigcup_{\alpha \in \mathcal{C}} \alpha$ contains each $\alpha \in \mathcal{C}$; thus, to check that β is an upper bound of $\mathcal{C}$ in $\mathcal{F}$ it is enough to see that $\beta \in \mathcal{F}$. Obviously $-1 \notin \beta$ because $-1 \notin \alpha$ for every $\alpha \in \mathcal{C}$. Moreover, if $\alpha \in \mathcal{C}$ then, $A^2 \subset \alpha \subset \beta$.

Finally, given $a, b \in \beta$ there exist $\alpha_1, \alpha_2 \in \mathcal{C}$ such that $a \in \alpha_1$ and $b \in \alpha_2$. Since $\mathcal{C}$ is a chain we may assume that $\alpha_1 \subset \alpha_2$ and, α_2 being a cone, $a + b, ab \in \alpha_2 \subset \beta$.

Therefore, there exists a maximal element γ in $\mathcal{F}$ and we show now that it is a prime cone in A. We must prove that it satisfies condition (iii) in 1.4 or, equivalently, the condition proposed in Exercise 1.8. Suppose, by way of contradiction, the existence of $a, b \in A$ such that $ab \in \gamma$ but $a \notin \gamma$ and $-b \notin \gamma$. Consider the sets

$$\gamma_1 := \{\sigma_0 + a\sigma_1 : \ \sigma_i \in \gamma\} \quad \& \quad \gamma_2 := \{\eta_0 - b\eta_1 : \ \eta_i \in \gamma\}.$$

Since γ is a cone it follows readily that both γ_1 and γ_2 are also cones in A, and they contain γ strictly because $a \in \gamma_1 \setminus \gamma$ and $-b \in \gamma_2 \setminus \gamma$. Since γ is a maximal element of $\mathcal{F}$ neither γ_1 nor γ_2 are proper cones in A, that is, there exist $\sigma_i, \eta_i \in \gamma$ for $i = 0, 1$, such that

$$-1 = \sigma_0 + a\sigma_1 \quad \& \quad -1 = \eta_0 - b\eta_1.$$

Consequently, $1 + \sigma_0 = -a\sigma_1$ and $1 + \eta_0 = b\eta_1$, and this implies

$$(1 + \sigma_0)(1 + \eta_0) = -ab\sigma_1\eta_1 \quad \Longleftrightarrow \quad -1 = \sigma_0 + \eta_0 + \sigma_0\eta_0 + ab\sigma_1\eta_1 \in \gamma.$$

But this is false because γ is a proper cone in A. This proves that γ is a prime cone in A, and so A is a real ring.

(2) $\Longrightarrow$ (3) This has been proved in 1.7.

(3) $\Longrightarrow$ (4). Suppose that there exist $a_1, \ldots, a_r \in A$ such that $-1 = \sum_{i=1}^{r} a_i^2$. Then,

$$-1 = \varphi(-1) = \sum_{i=1}^{r} \varphi(a_i)^2 \in \Sigma R^2,$$

and this is false because R is a real field.

(4) $\Longrightarrow$ (1) The hypothesis says that $\alpha := \Sigma A^2$ is a proper cone in A. □

Exercise 1.11 Let $f := \sum_{i=1}^{n} \mathbf{x}_i^2$ and $g := 1 + f$. Determine if either $A := \mathbb{R}[\mathbf{x}]/(f)$ or $B := \mathbb{R}[\mathbf{x}]/(g)$ are real rings.

Exercise 1.12 (1) Let A be a ring and let $S \subset A$ be a subset containing 1 such that $0 \in A \setminus S$ and $S \cdot S \subset S$. Suppose that $S + \Sigma A^2 \subset S$ and let $\mathfrak{p}$ be an ideal of A which is maximal among those contained in $A \setminus S$. Prove that $\mathfrak{p}$ is a prime ideal of A and that the quotient field $\kappa(\mathfrak{p})$ of $A/\mathfrak{p}$ is a real field.

(2) Prove that a ring A is real if and only if for every maximal ideal $\mathfrak{m}$ of A the localization $A_{\mathfrak{m}}$ of A at $\mathfrak{m}$ is a real ring.

2 Different formulations of Artin-Lang's Theorem.

We present now several (equivalent) formulations of Artin-Lang's Theorem.

Notations 2.1 As we did in Chapter I, given a field E and variables $\mathtt{x}_1, \ldots, \mathtt{x}_n$ over E, we denote $E_n := E(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ the field of rational functions with coefficients in E and n variables. Moreover, we denote $K^2 := \{x^2 : x \in K\}$ the set of squares of a field K; which is not the product $K \times K$! Among the different formulations of Artin-Lang's Theorem we distinguish the following ones:

(2.2) Artin's formulation. *Let E be a subfield of $\mathbb{R}$, Q an ordering in E_n such that $Q \cap E = \mathbb{R}^2 \cap E$, and let $f_1, \ldots, f_r \in E_n$ be positive with respect to the ordering Q. Then, there exists a point $a \in \mathbb{Q}^n$ such that $f_1, \ldots, f_r$ are defined in a and $f_1(a), \ldots, f_r(a)$ are positive with respect to the ordering $E \cap Q$.*

Since $\mathbb{Q}^n$ is a dense subset of $\mathbb{R}^n$, the precedent statement follows from the next more general formulation, that was already proved in Theorem 3.5, (Ch.I).

(2.3) Generalized Artin's formulation. *Let R be the real closure of an ordered field (E, P) and consider an ordering Q in E_n with $Q \cap E = P$. Let $f_1, \ldots, f_r \in E_n$ be positive with respect to the ordering Q. Then, there exists a point $a \in R^n$ such that $f_1, \ldots, f_r$ are defined in a and $f_1(a), \ldots, f_r(a)$ are positive with respect to the ordering in R.*

(2.4) Lang's formulation. *Let E be a real field and let Q be an ordering in a finitely generated extension $K := E(x_1, \ldots, x_n)$ of E. Let R_E be the real closure of $(E, E \cap Q)$. Then, there exists an E-homomorphism $\varphi : E[x_1, \ldots, x_n] \to R_E$.*

(2.5) Robinson's formulation. *Let R be a real closed field, let A be an R-algebra of finite type, and let R_1 be a real closed field containing R as a subfield such that there exists an R-algebras homomorphism $\psi : A \to R_1$. Then, there exists an R-algebras homomorphism $\varphi : A \to R$.*

Remark 2.6 Last statement (2.5) can be reformulated in terms of prime cones as follows.

$(*)$ *Let R be a real closed field and let $\mathfrak{a}$ be an ideal of $R[\mathtt{x}]$. If $A := R[\mathtt{x}]/\mathfrak{a}$ is a real ring, then there exists a point $p \in \mathcal{Z}(\mathfrak{a})$.*

Proof. Let us see that statement (2.5) implies $(*)$. Since A is a real ring it admits a prime cone $\alpha := (\mathfrak{p}, \leq)$. Denote $\kappa(\mathfrak{p}) := \mathrm{qf}(A/\mathfrak{p})$ and let R_α be the real closure of the

ordered field $(\kappa(\mathfrak{p}), \leq)$. Applying Robinson's formulation (2.5) to the homomorphism

$$\psi : A \to A/\mathfrak{p} \hookrightarrow \kappa(\mathfrak{p}) \hookrightarrow R_\alpha,$$

there exists an R-algebras homomorphism $\varphi : A \to R$. Notice that φ is surjective since $\varphi|_R$ is the identity. In particular $\mathfrak{m} := \ker \varphi$ is a maximal ideal of A because $A/\mathfrak{m} \cong R$. Let $p_i := \varphi(\mathtt{x}_i + \mathfrak{a}) \in R$ for each $1 \leq i \leq n$ and consider the point $p := (p_1, \ldots, p_n) \in R^n$. Since φ is an R-algebras homomorphism, for each $f \in R[\mathtt{x}]$ we have

$$\varphi(f + \mathfrak{a}) = f(\varphi(\mathtt{x}_1 + \mathfrak{a}), \ldots, \varphi(\mathtt{x}_n + \mathfrak{a})) = f(p_1, \ldots, p_n) = f(p).$$

To see this, write $f := \sum_\nu a_\nu \mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n}$ where each $a_\nu \in R$ and $\nu := (\nu_1, \ldots, \nu_n)$. Then,

$$\begin{aligned}\varphi(f + \mathfrak{a}) &= \sum_\nu a_\nu \varphi(\mathtt{x}_1^{\nu_1} + \mathfrak{a}) \cdots \varphi(\mathtt{x}_n^{\nu_n} + \mathfrak{a}) = \sum_\nu a_\nu \varphi(\mathtt{x}_1 + \mathfrak{a})^{\nu_1} \cdots \varphi(\mathtt{x}_n + \mathfrak{a})^{\nu_n} \\ &= \sum_\nu a_\nu p_1^{\nu_1} \cdots p_n^{\nu_n} = f(p_1, \ldots, p_n) = f(p).\end{aligned}$$

Let us check that $p \in \mathcal{Z}(\mathfrak{a})$, that is, $\mathfrak{a} \subset \mathfrak{m}_p$. By the Correspondence Theorem, there exists a maximal ideal $\mathfrak{n}$ of $R[\mathtt{x}]$ such that $\mathfrak{a} \subset \mathfrak{n}$ and $\mathfrak{m} := \mathfrak{n}/\mathfrak{a}$. Now, it suffices to check that $\mathfrak{m}_p \subset \mathfrak{n}$. Once this is proved, the equality $\mathfrak{m}_p = \mathfrak{n}$ holds because $\mathfrak{m}_p$ is maximal, and so $\mathfrak{a} \subset \mathfrak{n} = \mathfrak{m}_p$; hence $p \in \mathcal{Z}(\mathfrak{a})$. Indeed, let $\pi : R[\mathtt{x}] \to A$ be the canonical projection and note that $\mathfrak{n} \subset \pi^{-1}(\pi(\mathfrak{n}))$; moreover, this last is a proper ideal of $R[\mathtt{x}]$ since, otherwise

$$1 + \mathfrak{a} = \pi(1) \in \pi(\mathfrak{n}) = \mathfrak{n}/\mathfrak{a} = \mathfrak{m},$$

which is false. Thus, the maximality of $\mathfrak{n}$ guarantees that $\mathfrak{n} = \pi^{-1}(\pi(\mathfrak{n}))$, and so it is enough to prove that $\mathfrak{m}_p \subset \pi^{-1}(\pi(\mathfrak{n}))$, that is, $\pi(\mathfrak{m}_p) \subset \pi(\mathfrak{n})$. Let $f \in \mathfrak{m}_p$. Then,

$$0 = f(p) = \varphi(f + \mathfrak{a}) = \varphi(\pi(f)) \quad \Longrightarrow \quad \pi(f) \in \ker \varphi = \mathfrak{m} = \mathfrak{n}/\mathfrak{a} = \pi(\mathfrak{n}),$$

and this means, exactly, that $\pi(\mathfrak{m}_p) \subset \pi(\mathfrak{n})$ as wanted.

Conversely, let us prove that condition $(*)$ implies Robinson's formulation (2.5). Let $\psi : A \to R_1$ be an R-algebras homomorphism, where R_1 is a real closed field containing R as a subfield. Notice that A is a real ring, because it admits the prime cone defined by the homomorphism ψ. By the hypothesis, there exists a point $p \in \mathcal{Z}(\mathfrak{a})$. Now, the R-algebras homomorphism we are looking for is defined as $\varphi : A \to R$, $f + \mathfrak{a} \mapsto f(p)$. Note that φ is well defined since given polynomials $f, g \in R[\mathtt{x}]$ such that $f + \mathfrak{a} = g + \mathfrak{a}$ the difference $h := f - g \in \mathfrak{a}$, and so $h(p) = 0$, that is, $f(p) = g(p)$. $\square$

Proof of the equivalence of the precedent formulations. Let us see the equivalence of the precedent statements (2.3), (2.4) and (2.5); in this way we shall use them indistinctly, according to our convenience. To that end we will prove:

$$(2.5) \implies (2.4) \implies (2.3) \implies (2.4) \implies (2.5)$$

(2.5) $\Longrightarrow$ (2.4). Let R_1 be the real closure of the ordered field (K, Q) and consider the inclusions

$$E[x_1, \ldots, x_n] \hookrightarrow K := E(x_1, \ldots, x_n) \hookrightarrow R_1.$$

Let $P := Q \cap E$ and notice that the real closure R_E of the ordered field (E, P) is a subfield of R_1. Therefore the inclusion $\psi : A := R_E[x_1, \ldots, x_n] \hookrightarrow R_1$ is an R_E-algebras homomorphism. By Robinson's formulation there exists an R_E-algebras homomorphism $\varphi_0 : A \to R_E$. Since the inclusion $\mathtt{j} : E[x_1, \ldots, x_n] \hookrightarrow A$ is an E-homomorphism and E is a subfield of R_E, we get an E-homomorphism

$$\varphi := \varphi_0 \circ \mathtt{j} : E[x_1, \ldots, x_n] \hookrightarrow A \to R_E.$$

(2.4) $\Longrightarrow$ (2.3). Let R_n be a real closure of the ordered field (E_n, Q). Since $f_1, \ldots, f_r$ are positive with respect to the ordering Q in E_n, there exist $g_1, \ldots, g_r \in R_n$ such that each $g_j^2 = f_j$. Notice that the ordering $Q_L := R_n^2 \cap L$ in the field

$$L := E(\mathtt{x}_1, \ldots, \mathtt{x}_n)(g_1, \ldots, g_r) = E_n(g_1, \ldots, g_r)$$

satisfies $Q_L \cap E_n = Q$. Since $L|E$ is a finitely generated field extension, it follows from Lang's formulation (2.4) the existence of an E-homomorphism

$$\varphi : E[\mathtt{x}_1, \ldots, \mathtt{x}_n](g_1, \ldots, g_r) \to R_E := R.$$

Denote $a := (\varphi(\mathtt{x}_1), \ldots, \varphi(\mathtt{x}_n)) \in R^n$. Since f is an E-homomorphism, for each $1 \leq i \leq r$ we have

$$f_i(a) = f_i(\varphi(\mathtt{x}_1), \ldots, \varphi(\mathtt{x}_n)) = \varphi(f_i) = \varphi(g_i^2) = \varphi(g_i)^2 > 0.$$

(2.3) $\Longrightarrow$ (2.4). Denote s the transcendence degree of the field extension $K|E$. We may assume without loss of generality that $x_1, \ldots, x_s$ constitute a transcendence basis of this extension and so, see [J, IV], the field extension $K|E(x_1, \ldots, x_s)$ is finite.

In fact, $E(x_1, \ldots, x_s)$ being a field of characteristic zero, there exists an element $y \in K$, with $K := E(x_1, \ldots, x_s, y)$. We can suppose that $x_1, \ldots, x_s$ are variables over E or, more precisely, there exist variables $\mathtt{x}_1, \ldots, \mathtt{x}_s$ over E, an algebraic element z over $E_s := E(\mathtt{x}_1, \ldots, \mathtt{x}_s)$ and an E-isomorphism

$$\psi : K = E(x_1, \ldots, x_s, y) \to E_s(z)$$

such that $\psi(x_i) = \mathtt{x}_i$ for each $1 \leq i \leq s$, and $\psi(y) = z$. Let $g \in E_s[\mathtt{t}]$ be the irreducible polynomial of z over E_s. Then, there exists an E_s-isomorphism

$$\phi : E_s[z] \to E_s[\mathtt{t}]/(g)$$

satisfying $\phi(z) = \mathtt{t} + (g)$. In particular ϕ is an E-isomorphism, and so we replace in the sequel K by the quotient $E_s[\mathtt{t}]/(g)$, and denote also Q the ordering in $E_s[\mathtt{t}]/(g)$ which is the image of the ordering Q in K by the E-isomorphism $\phi \circ \psi$. Let $t_{s+1}, \ldots, t_n$ be the images by ψ of $x_{s+1}, \ldots, x_n$ and let $p_{s+1}, \ldots, p_n \in E_s[\mathtt{t}]$ such that $\phi(t_j) := p_j \bmod (g)$.

Notice that z is a root of g in the real closure R_s of the ordered field $(E_s, E_s \cap Q)$. In particular g has a root in E_s and, by the specialization results in Section §3 of Chapter I, there exists a finite subset $\{h_1, \ldots, h_\ell\} \subset E_s$ such that each h_i is positive with respect to the ordering $E_s \cap Q$ and, for every point $a \in R_E^s$ such that $h_1, \ldots, h_\ell$ are defined in a and $h_1(a), \ldots, h_\ell(a)$ are positive in R_E, then $g(a, \mathtt{t}) \in R_E[\mathtt{t}]$ is a well defined polynomial and it has a root in R_E. Let $h_{\ell+1}, \ldots, h_m \in E_s$ be the squares of the non-zero coefficients of the polynomials $p_{s+1}, \ldots, p_n$.

Since we assume that formulation (2.3) is true, there exists $a := (a_1, \ldots, a_s) \in R_E^s$ such that the rational functions $h_1, \ldots, h_m$ are defined in a and $h_1(a), \ldots, h_m(a)$ are positive in R_E. Hence, there exists a root $b \in R_E$ of the polynomial $g(a, \mathtt{t}) \in R_E[\mathtt{t}]$. The E-homomorphism we are looking for is induced by the assignment

$$\varphi : E[x_1, \ldots, x_n] \to R_E,\ x_i \mapsto \begin{cases} a_i & \text{if } 1 \leq i \leq s, \\ p_i(a, b) & \text{if } s+1 \leq i \leq n. \end{cases}$$

We should check that the assignment above induces in fact an E-homomorphism. For that, we must prove that it preserves the polynomial relations among $x_1, \ldots, x_n$ with coefficients in E. Thus, let $\mathtt{p} \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be such that $\mathtt{p}(x_1, \ldots, x_n) = 0$. We must see that $\mathtt{p}(\varphi(x_1), \ldots, \varphi(x_n)) = 0$. Notice that,

$$\mathtt{p}(\mathtt{x}_1, \ldots, \mathtt{x}_s, p_{s+1}(\mathtt{x}_1, \ldots, \mathtt{x}_s, z), \ldots, p_n(\mathtt{x}_1, \ldots, \mathtt{x}_s, z)) = 0$$

or, equivalently, g divides in $E_s[\mathtt{t}]$ the polynomial

$$\mathtt{p}(\mathtt{x}_1, \ldots, \mathtt{x}_s, p_{s+1}(\mathtt{x}_1, \ldots, \mathtt{x}_s, \mathtt{t}), \ldots, p_n(\mathtt{x}_1, \ldots, \mathtt{x}_s, \mathtt{t})) \in E_s[\mathtt{t}],$$

that is, there exists $h \in E_s[\mathtt{t}]$ such that

$$\mathtt{p}(\mathtt{x}_1, \ldots, \mathtt{x}_s, p_{s+1}(\mathtt{x}_1, \ldots, \mathtt{x}_s, \mathtt{t}), \ldots, p_n(\mathtt{x}_1, \ldots, \mathtt{x}_s, \mathtt{t})) = g(\mathtt{x}_1, \ldots, \mathtt{x}_s, \mathtt{t}) h(\mathtt{x}_1, \ldots, \mathtt{x}_s, \mathtt{t}).$$

After substituting $\mathtt{x}_1 = a_1, \ldots, \mathtt{x}_s = a_s, \mathtt{t} = b$, and since $g(a, b) = 0$, we deduce that

$$\begin{aligned}\mathtt{p}(\varphi(x_1), \ldots, \varphi(x_s), \varphi(x_{s+1}), \ldots, \varphi(x_n)) \\ = \mathtt{p}(a_1, \ldots, a_s, p_{s+1}(a_1, \ldots, a_s, b), \ldots, p_n(a_1, \ldots, a_s, b)) = 0,\end{aligned}$$

which proves that φ is a well defined homomorphism.

(2.4) $\Longrightarrow$ (2.5). We may assume that $A := R[\mathtt{x}]/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal of the polynomial ring $R[\mathtt{x}]$, and let $\mathfrak{q}$ denote the kernel of an R-algebras homomorphism $\psi : A \to R_1$. Let $\mathfrak{p}$ be the unique prime ideal of $R[\mathtt{x}]$ containing $\mathfrak{a}$ such that $\mathfrak{q} := \mathfrak{p}/\mathfrak{a}$. Let $B := R[\mathtt{x}]/\mathfrak{p}$ and denote $K := R(x_1, \ldots, x_n)$ its quotient field, where $x_i \equiv \mathtt{x}_i \bmod \mathfrak{p}$. Consider the epimorphism

$$\pi : A = R[\mathtt{x}]/\mathfrak{a} \to B = R[\mathtt{x}]/\mathfrak{p},\ f + \mathfrak{a} \mapsto f + \mathfrak{p}.$$

Since $\ker \pi = \mathfrak{p}/\mathfrak{a} = \mathfrak{q} = \ker \psi$, there exists an injective R-algebras homomorphism $\phi : B \to R_1$ with $\phi \circ \pi = \psi$, and we denote also $\phi : K \to R_1$ its extension to $K = \mathrm{qf}(B)$. Then, $\phi^{-1}(R_1^2)$ is an ordering in K that necessarily extends the ordering in its subfield $R \subset K$, because R admits a unique ordering. The hypothesis in (2.4) implies the existence of an R-algebras homomorphism $\varphi_0 : B \to R$, and so $\varphi := \varphi_0 \circ \pi$ is the R-homomorphism we are looking for. □

Exercise 2.7 Let E be a real field and let Σ be the set of orderings in E. For every $P \in \Sigma$ let R_P be a real closure of the ordered field (K, P). Let $f \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be a polynomial such that $f(x) \geq 0$ in R_P for every point $x \in R_P^n$. Prove that f is a sum of squares in the field $R_P(\mathtt{x}_1, \ldots, \mathtt{x}_n)$.

3 Real Nullstellensatz and Positivstellensätze

We are in a position to approach the proof of the Real Nullstellensatz and the Positivstellensätze for the polynomial ring $R[\mathtt{x}]$, where R is a real closed field. As far as we know, the first proof of a weak form of the Real Nullstellensatz is due to Krivine, [Kri], but this article passed unnoticed. Five years later Dubois gave in [Du1] a version of the Real Nullstellensatz that involves rational functions, and the statement of Theorem 3.4 is the one proved by Risler in [Ri1]. The Positivstellensätze proved in Theorem 3.7 were proposed by Stengle in [St], although the use of prime cones in its proof goes back to the book of Prestel [P]. Its abstract version proposed in Exercise 3.3 is due to Colliot-Thélène, [CT].

Notation and Exercise 3.1 (1) Let A be a ring and let $g_1, \dots, g_r \in A$. Let us denote

$$\Sigma_A[g_1, \dots, g_r] := \Big\{ \sum_{\nu \in \{0,1\}^r} \sigma_\nu g^\nu : \ \sigma_\nu \in \Sigma A^2, \ g^\nu := g_1^{\nu_1} \cdots g_r^{\nu_r}, \ \nu := (\nu_1, \dots, \nu_r) \Big\}.$$

(2) Prove that $\Sigma_A[g_1, \dots, g_r]$ is the smallest cone in A containing $g_1, \dots, g_r$.

The next result relates algebraic and geometric information and is the key to prove the Real Nullstellensatz and the Positivstellensätze.

Lemma 3.2 *Let R be a real closed field and let $g_1, \dots, g_r, f, h_1, \dots, h_s \in R[\mathtt{x}]$. The following statements are equivalent:*

(1) *The set $T := \{g_1 \geq 0, \dots, g_r \geq 0, \ f \neq 0, \ h_1 = 0, \dots, h_s = 0\}$ is empty.*

(2) *The R-algebra $B := R[\mathtt{x}, \mathtt{z}, \mathtt{y}]/\mathfrak{a}$, where $\mathtt{x} := (\mathtt{x}_1, \dots, \mathtt{x}_n)$, $\mathtt{z} := (\mathtt{z}_1, \dots, \mathtt{z}_r)$ and*

$$\mathfrak{a} := (\mathtt{z}_1^2 - g_1, \dots, \ \mathtt{z}_r^2 - g_r, \ \mathtt{y}f - 1, \ h_1, \dots, h_s) \subset R[\mathtt{x}, \mathtt{z}, \mathtt{y}],$$

is not a real ring.

(3) *There is no prime cone α in $R[\mathtt{x}]$ such that*

$$g_1, \dots, g_r \in \alpha, \quad f \notin \mathfrak{p}_\alpha \quad \& \quad h_1, \dots, h_s \in \mathfrak{p}_\alpha.$$

(4) *There is no R-algebras homomorphism $\varphi : R[\mathtt{x}] \to R_1$, where R_1 is a real closed field containing R as a subfield, such that*

$$\varphi(g_i) \geq 0, \quad \varphi(f) \neq 0 \quad \& \quad \varphi(h_j) = 0 \quad \text{for each } 1 \leq i \leq r \text{ and each } 1 \leq j \leq s. \tag{3.1}$$

(5) *There exist $h \in (h_1, \dots, h_s)R[\mathtt{x}]$, an integer $m \geq 1$ and $a \in \Sigma_{R[\mathtt{x}]}[g_1, \dots, g_r]$ such that $a + f^{2m} + h = 0$.*

Proof. We will prove that

$$(3) \iff (4) \iff (2) \Longrightarrow (5) \Longrightarrow (1) \Longrightarrow (2).$$

The equivalence between (3) and (4) is clear, because the existence of a real closed field R_1 containing R as a subfield and an R-algebras homomorphism $\varphi : R[\mathtt{x}] \to R_1$ satisfying conditions (3.1) is equivalent, by 1.7, to the existence of a prime cone $\alpha := \varphi^{-1}(R_1^2)$ such that $g_1, \dots, g_r \in \alpha$, $f \notin \mathfrak{p}_\alpha$ and $h_1, \dots, h_s \in \mathfrak{p}_\alpha$.

Let us prove that (2) implies (4). Suppose, by way of contradiction, the existence of a real closed field R_1 containing R as a subfield and an R-algebras homomorphism $\varphi : R[\mathtt{x}] \to R_1$, such that

$$\lambda_i := \varphi(g_i) \geq 0, \quad \mu := \varphi(f) \neq 0 \quad \& \quad \varphi(h_j) = 0$$

for each $1 \leq i \leq r$ and each $1 \leq j \leq s$. We will construct an R-algebras homomorphism $\psi : B \to R_1$. In such a case B contains, by 1.7, a prime cone, and this is false because B is not a real ring.

To define the homomorphism ψ it suffices to construct an R-algebras homomorphism $\phi : R[\mathtt{x}, \mathtt{z}, \mathtt{y}] \to R_1$ such that $\mathfrak{a} \subset \ker \phi$, since this implies that ϕ factorizes through the canonical projection

$$\pi : R[\mathtt{x}, \mathtt{z}, \mathtt{y}] \to B = R[\mathtt{x}, \mathtt{z}, \mathtt{y}]/\mathfrak{a},$$

that is, there exists an R-algebras homomorphism $\psi : B \to R_1$ such that $\psi \circ \pi = \phi$. Recall that the R-algebras homomorphism $\phi : R[\mathtt{x}, \mathtt{z}, \mathtt{y}] \to R_1$ is determined by the images of the variables. Each $\lambda_i \geq 0$ in R_1 and so $\lambda_i := \eta_i^2$ for some $\eta_i \in R_1$. Let $\phi : R[\mathtt{x}, \mathtt{z}, \mathtt{y}] \to R_1$ be the R-algebras homomorphism induced by the assignment:

$$\mathtt{x}_k \mapsto \varphi(\mathtt{x}_k), \quad \mathtt{z}_i \mapsto \eta_i \quad \& \quad \mathtt{y} \mapsto 1/\mu.$$

Observe that $\phi|_{R[\mathtt{x}]} = \varphi$, and this implies

$$\phi(h_j) = \varphi(h_j) = 0, \quad \phi(\mathtt{z}_i^2 - g_i) = \eta_i^2 - \lambda_i = 0 \quad \& \quad \phi(\mathtt{y}f - 1) = (1/\mu)\mu - 1 = 0,$$

and consequently $\mathfrak{a} \subset \ker \phi$, which finishes the proof of this implication.

Let us see next that (4) implies (2). Suppose, by way of contradiction, that B is a real ring. By Lemma 1.10 there exist a real closed field R_1 and a ring homomorphism $\psi : B \to R_1$. Note that $\psi|_R : R \to R_1$ is a field homomorphism, hence injective, and so we may assume that R is a subfield of R_1 and ψ is an R-homomorphism. Denote $\mathtt{j} : R[\mathtt{x}] \hookrightarrow R[\mathtt{x}, \mathtt{z}, \mathtt{y}]$ the inclusion map and observe that

$$\varphi := \psi \circ \pi \circ \mathtt{j} : R[\mathtt{x}] \to B \to R_1$$

is an R-algebras homomorphism. Since $\pi(\mathtt{y})\pi(f) - 1 = \pi(\mathtt{y}f - 1) = 0$, because $\mathtt{y}f - 1 \in \mathfrak{a}$, it follows that

$$\varphi(f)\psi(\pi(\mathtt{y})) = \psi(\pi(f))\psi(\pi(\mathtt{y})) = 1 \implies \varphi(f) \neq 0,$$

and, for each $1 \leq i \leq r$ and each $1 \leq j \leq s$,

$$\varphi(g_i) = \psi(\pi(g_i)) = \psi(\pi(\mathtt{z}_i)^2) = \psi(\pi(\mathtt{z}_i))^2 \geq 0 \quad \& \quad \varphi(h_j) = \psi(\pi(h_j)) = 0.$$

This contradicts (4). Therefore, B is not a real ring and this proves (2).

Let us prove, by way of contradiction, that (5) $\Longrightarrow$ (1). Suppose that T is non-empty and there exist $a \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r]$, $m \geq 1$ and $h \in (h_1, \ldots, h_s)R[\mathtt{x}]$ such that $a + f^{2m} + h = 0$. Then, for every point $p \in T$ we have

$$0 = (a + f^{2m} + h)(p) = a(p) + f^{2m}(p) + h(p) = a(p) + f^{2m}(p) > 0$$

because $a(p) \geq 0$ and $f^{2m}(p) > 0$, a contradiction.

Let us prove now that (1) implies (2). If B were a real ring there would exist, by Remark 2.6, a point $(p, q, t) \in \mathcal{Z}(\mathfrak{a})$. This implies

$$g_i(p) = q_i^2 \geq 0, \quad tf(p) = 1 \neq 0 \quad \& \quad h_j(p) = 0,$$

for each $1 \leq i \leq r$ and each $1 \leq j \leq s$, and so $p \in T$, which is false.

To finish, we prove that (2) implies (5). Since B is not a real ring it follows from Lemma 1.10 that $-1 \in \Sigma B^2$. Thus, there exist $S_1, \ldots, S_\ell, P_1, \ldots, P_r$, $Q_1, \ldots, Q_s, C \in R[\mathtt{x}, \mathtt{z}, \mathtt{y}]$ such that

$$-1 = \sum_{k=1}^{\ell} S_k^2 + \sum_{j=1}^{s} Q_j h_j + C(\mathtt{y}f - 1) + \sum_{i=1}^{r} P_i(\mathtt{z}_i^2 - g_i). \tag{3.2}$$

After dividing the polynomials S_k, Q_j, C by $\mathtt{z}_i^2 - g_i$ and changing suitably the polynomials P_i (although for simplicity we keep the same notation), we can suppose that the degree of S_k, Q_j, C with respect to each variable $\mathtt{z}_i$ is ≤ 1. Hence, there exist $s_{k,\nu}, q_{j,\nu}, c_\nu \in R[\mathtt{x}][\mathtt{y}]$ such that, if we denote $\mathtt{z}^\nu := \mathtt{z}_1^{\nu_1} \cdots \mathtt{z}_r^{\nu_r}$, where $\nu := (\nu_1, \ldots, \nu_r)$ and $0 \leq \nu_i \leq 1$, it follows

$$S_k := \sum_{\nu \in \{0,1\}^r} s_{k,\nu}\mathtt{z}^\nu, \quad Q_j := \sum_{\nu \in \{0,1\}^r} q_{j,\nu}\mathtt{z}^\nu \quad \& \quad C := \sum_{\nu \in \{0,1\}^r} c_\nu \mathtt{z}^\nu.$$

After substituting in equality (3.2) we get

$$\begin{aligned} -1 = \sum_{k=1}^{\ell} \Big(\sum_{\nu \in \{0,1\}^r} s_{k,\nu}^2 \mathtt{z}^{2\nu} + 2 \sum_{\substack{\nu,\mu \in \{0,1\}^r, \\ \nu \neq \mu}} s_{k,\nu} s_{k,\mu} \mathtt{z}^{\nu+\mu} \Big) \\ + \sum_{j=1}^{s} Q_j h_j + C(\mathtt{y}f - 1) + \sum_{i=1}^{r} P_i(\mathtt{z}_i^2 - g_i). \end{aligned}$$

Notice that if $\nu, \mu \in \{0,1\}^r$ and $\nu \neq \mu$, then there is no $\tau \in \{0,1\}^r$ such that $\nu + \mu = 2\tau$. Using now that $\mathtt{z}_i^2 - g_i^2 = 0$ in B, there exist $t_\rho \in R[\mathtt{x}, \mathtt{y}]$ with $\rho \in \{0,1\}^r$

and $\rho \neq 0$ such that, after modifying again the $P_i's$ (although for simplicity we keep the same notation), we obtain an expression of the form

$$-1 = \sum_{k=1}^{\ell} \Big(\sum_{\nu \in \{0,1\}^r} s_{k,\nu}^2 g^\nu + \sum_{\substack{\rho \in \{0,1\}^r \\ \rho \neq 0}} t_\rho \mathtt{z}^\rho \Big) + \sum_{j=1}^{s} \Big(\sum_{\nu \in \{0,1\}^r} q_{j,\nu} \mathtt{z}^\nu \Big) h_j$$
$$+ \Big(\sum_{\nu \in \{0,1\}^r} c_\nu \mathtt{z}^\nu \Big) (\mathtt{y}f - 1) + \sum_{i=1}^{r} P_i(\mathtt{z}_i^2 - g_i).$$

Identifying now the coefficients with respect to $\mathtt{z}$ in both sides of the equality we deduce that the new $P_i's$ are identically zero, and so

$$-1 = \sum_{k=1}^{\ell} \Big(\sum_{\nu \in \{0,1\}^r} s_{k,\nu}^2 g^\nu + \sum_{\substack{\rho \in \{0,1\}^r \\ \rho \neq 0}} t_\rho \mathtt{z}^\rho \Big)$$
$$+ \sum_{j=1}^{s} \Big(\sum_{\nu \in \{0,1\}^r} q_{j,\nu} \mathtt{z}^\nu \Big) h_j + \Big(\sum_{\nu \in \{0,1\}^r} c_\nu \mathtt{z}^\nu \Big) (\mathtt{y}f - 1).$$

Moreover, if we compare the independent terms with respect to the variables $\mathtt{z}$, we deduce that

$$-1 = \sum_{k=1}^{\ell} \Big(\sum_{\nu \in \{0,1\}^r} s_{k,\nu}^2 g^\nu \Big) + \sum_{j=1}^{s} q_{j,0} h_j + c_0(\mathtt{y}f - 1).$$

Now we just need to eliminate the term $c_0(\mathtt{y}f - 1)$ in the expression above. To that end we substitute $\mathtt{y} = 1/f$ and we clear the occurring denominator, which is an even power of f. Consequently, there exist $a_{k,\nu}, q_j \in R[\mathtt{x}]$ and an integer $m \geq 1$ such that

$$-f^{2m} = \sum_{\nu \in \{0,1\}^r} \Big(\sum_{k=1}^{\ell} a_{k,\nu}^2 \Big) g^\nu + \sum_{j=1}^{s} q_j h_j \quad \Longrightarrow \sum_{\nu \in \{0,1\}^r} \sigma_\nu g^\nu + f^{2m} + \sum_{j=1}^{s} q_j h_j = 0,$$

where each $\sigma_\nu \in \Sigma R[\mathtt{x}]^2$. Now, let us define

$$a := \sum_{\nu \in \{0,1\}^r} \sigma_\nu g^\nu + f^{2m} \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r] \quad \& \quad h := \sum_{j=1}^{s} q_j h_j \in (h_1, \ldots, h_s),$$

which satisfy $a + f^{2m} + h = 0$, and we are done. □

In a more general setting the next result, whose proof is analogous to the one of the previous Lemma 3.2, holds true.

Exercise 3.3 (Abstract positivstellensatz) Let $g_1, \dots, g_r, f, h_1, \dots, h_s$ be elements of a ring A. Prove that the following statements are equivalent:

(1) *The ring* $B := A[\mathtt{z}, \mathtt{y}]/\mathfrak{a}$, *where* $\mathtt{z} := (\mathtt{z}_1, \dots, \mathtt{z}_r)$, $\mathtt{y}$ *is a single variable and*

$$\mathfrak{a} := (\mathtt{z}_1^2 - g_1, \dots, \mathtt{z}_r^2 - g_r, \mathtt{y}f - 1, h_1, \dots, h_s)$$

is not a real ring.

(2) *There is no prime cone* α *in* A *such that*

$$g_1, \dots, g_r \in \alpha, \quad f \notin \mathfrak{p}_\alpha \quad \& \quad h_1, \dots, h_s \in \mathfrak{p}_\alpha.$$

(3) *There is no real closed field* R *and a homomorphism* $\varphi : A \to R$, *such that*

$$\varphi(f) \neq 0, \quad \varphi(g_i) \geq 0 \quad \& \quad \varphi(h_j) = 0 \tag{3.3}$$

for each $1 \leq i \leq r$ *and each* $1 \leq j \leq s$.

(4) *There exist* $h \in (h_1, \dots, h_s)A$, *an integer* $m \geq 1$ *and* $a \in \Sigma_A[g_1, \dots, g_r]$ *such that* $a + f^{2m} + h = 0$.

We are ready to prove, as a consequence of Lemma 3.2, the Real Nullstellensatz and the Positivstellensätze.

Theorem 3.4 (Real Nullstellensatz) *Let* R *be a real closed field and let* $\mathfrak{a}$ *be an ideal of* $R[\mathtt{x}]$. *Then,*

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \{f \in R[\mathtt{x}] : \ \exists\, \sigma \in \Sigma R[\mathtt{x}]^2 \ \&\ m \geq 1 \text{ such that } f^{2m} + \sigma \in \mathfrak{a}\}.$$

The ideal appearing in the right-hand side of the above equality is known as the *real radical of* $\mathfrak{a}$, and it is denoted $\sqrt[r]{\mathfrak{a}}$. We will study carefully such ideal in the next section.

Proof. We prove first the inclusion $\sqrt[r]{\mathfrak{a}} \subset \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$. Given $f \in \sqrt[r]{\mathfrak{a}}$ there exist a sum of squares $\sigma \in \Sigma R[\mathtt{x}]^2$ and $m \geq 1$ such that $f^{2m} + \sigma \in \mathfrak{a}$. For every point $p \in \mathcal{Z}(\mathfrak{a})$ we have $f^{2m}(p) + \sigma(p) = 0$. Since $f^{2m}(p) \geq 0$ and $\sigma(p) \geq 0$ this implies $f(p) = 0$, that is, $f \in \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$.

Conversely, let $f \in \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ and let $\{h_1, \dots, h_s\} \subset \mathfrak{a}$ be a system of generators of $\mathfrak{a}$. Then, $\{h_1 = 0, \dots, h_s = 0\} \subset \{f = 0\}$, or equivalently, the set

$$\{f \neq 0, \ h_1 = 0, \dots, h_s = 0\} = \varnothing.$$

From Lemma 3.2 there exist $\sigma \in \Sigma R[\mathtt{x}]^2$, $h \in \mathfrak{a} := (h_1, \dots, h_s)R[\mathtt{x}]$ and $m \geq 1$ such that $\sigma + f^{2m} + h = 0$. Thus $f^{2m} + \sigma \in \mathfrak{a}$ and so $f \in \sqrt[r]{\mathfrak{a}}$. □

Exercise 3.5 Let R be a real closed field and let $f \in R[\mathtt{x}]$ be an irreducible polynomial such that $f(a)f(b) < 0$ for some points $a, b \in R^n$. Prove that $\mathcal{I}(\mathcal{Z}(f)) = (f)$.

Exercise 3.6 Prove the equality $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\sqrt[r]{\mathfrak{a}})$ for every ideal $\mathfrak{a}$ of $R[\mathtt{x}]$.

Theorem 3.7 (Positivstellensätze) *Let $f, g_1, \ldots, g_r \in R[\mathtt{x}]$, where R is a real closed field, and denote $S := \{g_1 \geq 0, \ldots, g_r \geq 0\} \subset R^n$. Then,*

(1) *The polynomial f is ≥ 0 on S if and only if there exist $\sigma_1, \sigma_2 \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r]$ and a positive integer m such that $\sigma_1 f = f^{2m} + \sigma_2$.*

(2) *The polynomial f is > 0 on S if and only if there exist $\sigma_1, \sigma_2 \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r]$ such that $\sigma_1 f = 1 + \sigma_2$.*

(3) *The polynomial f vanishes identically on the set S if and only if there exist $\sigma \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r]$ and a positive integer m such that $\sigma + f^{2m} = 0$.*

Proof. (1) Noce that f is positive semidefinite on S if and only if the set

$$\{g_1 \geq 0, \ldots, g_r \geq 0,\ -f \geq 0,\ f \neq 0\} = \varnothing.$$

This last is equivalent, by Lemma 3.2, to the existence of $\sigma \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r, -f]$ and a positive integer m such that $\sigma + f^{2m} = 0$. Notice that $\sigma := \sigma_2 - f\sigma_1$ with $\sigma_i \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r]$, and so $\sigma_1 f = f^{2m} + \sigma_2$.

(2) The polynomial f is positive on S if and only if the set

$$\{g_1 \geq 0, \ldots, g_r \geq 0, -f \geq 0,\ 1 \neq 0\} = \varnothing,$$

which is equivalent, by Lemma 3.2, to the existence of $\sigma \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r, -f]$ and a positive integer m such that $\sigma + 1^{2m} = 0$. Note that $\sigma := \sigma_2 - f\sigma_1$ with $\sigma_i \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r]$, and consequently $\sigma_1 f = 1 + \sigma_2$.

(3) Note that $f|_S \equiv 0$ if and only if $\{g_1 \geq 0, \ldots, g_r \geq 0, f \neq 0\} = \varnothing$. By Lemma 3.2 this is equivalent to the existence of $\sigma \in \Sigma_{R[\mathtt{x}]}[g_1, \ldots, g_r]$ and a positive integer m such that $\sigma + f^{2m} = 0$. □

Exercise 3.8 Let $a, b \in \mathbb{R}$ such that $a \leq b$ and consider the interval $I := [a, b]$. Prove that a polynomial $f \in \mathbb{R}[\mathtt{x}]$ satisfies $f(x) > 0$ for every $x \in I$ if and only if there exist polynomials $p_i \in \mathbb{R}[\mathtt{x}]$, with $1 \leq i \leq 8$, such that

$$(p_1^2 + p_2^2 + (p_3^2 + p_4^2)(b - \mathtt{x})(\mathtt{x} - a))f = 1 + (p_5^2 + p_6^2 + (p_7^2 + p_8^2)(b - \mathtt{x})(\mathtt{x} - a)).$$

Remarks 3.9 (1) Let $f \in R[\mathbf{x}]$ such that $f(x) \geq 0$ for every point $x \in R^n$. By Theorem 3.7 (1) $\sigma_1 f = f^{2m} + \sigma_2$ for some integer $m \geq 1$ and some $\sigma_1, \sigma_2 \in \Sigma R[\mathbf{x}]^2$. In particular,

$$\begin{aligned} \mathcal{Z}(\sigma_1) \subset \mathcal{Z}(\sigma_1) \cup \mathcal{Z}(f) &= \mathcal{Z}(\sigma_1 f) \\ &= \mathcal{Z}(f^{2m} + \sigma_2) = \mathcal{Z}(f^{2m}) \cap \mathcal{Z}(\sigma_2) \subset \mathcal{Z}(f^{2m}) = \mathcal{Z}(f). \end{aligned}$$

Let $\sigma_3 := \sigma_1(f^{2m} + \sigma_2) \in \Sigma R[\mathbf{x}]^2$. Then, $\sigma_1^2 f = \sigma_3$, that is, $f = \sigma_3/\sigma_1^2 \in \Sigma R(\mathbf{x})^2$, and we have represented f as a sum of squares in $R(\mathbf{x})$ with the property that $\mathcal{Z}(f)$ contains the zero-set $\mathcal{Z}(\sigma_1)$ of the denominator σ_1 of this representation.

(2) Let $f \in R[\mathbf{x}]$ be such that $f(x) > 0$ for every point $x \in R^n$. In other words, f is strictly positive on the set $R^n := \{1 \geq 0\}$. From the Positivstellensatz 3.7 (2) there exist $\sigma_1, \sigma_2 \in \Sigma R[\mathbf{x}]^2$ such that $\sigma_1 f = 1 + \sigma_2$. Multiplying both members of this equality by f we get $\sigma_1 f^2 = (1 + \sigma_2) f$, and consequently,

$$(1 + \sigma_1 + \sigma_2) f = \sigma_1 f + (1 + \sigma_2) f = 1 + \sigma_2 + \sigma_1 f^2.$$

Note that $\sigma_3 := \sigma_1 + \sigma_2$ is a sum of squares and $(1+\sigma_3) f = 1+\sigma_2+\sigma_1 f^2$. Multiplying both members by $1 + \sigma_3$ we get

$$(1 + \sigma_3)^2 f = (1 + \sigma_3)(1 + \sigma_2 + \sigma_1 f^2) = 1 + \sigma, \quad \text{where } \sigma_3, \sigma \in \Sigma R[\mathbf{x}]^2.$$

Notation 3.10 (1) In what follows we denote *Solution of Hilbert's 17th Problem with controlled denominators,* and we denote it $\mathbf{H17_c}$, the conjunction of the following two statements, that we have just proved:

(i) If $f \in R[\mathbf{x}]$ and $f(x) \geq 0$ for every point $x \in R^n$, there exists $g \in R[\mathbf{x}]$ with $\mathcal{Z}(g) \subset \mathcal{Z}(f)$ such that $g^2 f \in \Sigma R[\mathbf{x}]^2$.

(ii) If $f \in R[\mathbf{x}]$ and $f(x) > 0$ for every point $x \in R^n$, there exist $\sigma_1, \sigma_2 \in \Sigma R[\mathbf{x}]^2$ such that $(1 + \sigma_1)^2 f = 1 + \sigma_2$.

Exercise 3.11 (1) Prove that the truthfulness of the Real Nullstellensatz implies 2.6 $(*)$ that, as we have just seen, is a reformulation of Artin-Lang's Theorem. Thus the Positivstellensätze, which constitute a logically stronger statement than the Real Nullstellensatz, are consequence of this last result.

(2) Prove that statement 3.7 (1) implies the Real Nullstellensatz. Consequently, the Real Nullstellensatz and the Positivstellensätze are equivalent results.

Hint: Use that given $f, g \in R[\mathbf{x}]$ with $\mathcal{Z}(f) \subset \mathcal{Z}(g)$ then, $\{-f^2 \geq 0\} \subset \{-g^2 \geq 0\}$.

Exercise 3.12 Let $f \in \mathbb{R}[\mathbf{x}]$ be an irreducible polynomial.

(1) Prove that f is reducible in $\mathbb{C}[\mathtt{x}]$ if and only if either f or $-f$ is a sum of two squares of polynomials in $\mathbb{R}[\mathtt{x}]$.

(2) Let $F \in \mathbb{R}[\mathtt{x},\mathtt{y},\mathtt{z}]$ be a positive semidefinite irreducible homogeneous polynomial of degree $d > 0$. Prove that the projective subset

$$\mathcal{Z}_{\text{proj}}(F) := \{(x : y : z) \in \mathbb{P}^2(\mathbb{R}) : \ F(x,y,z) = 0\}$$

is finite with, at most, $\max\left\{d^2/4, \binom{d-1}{2}\right\}$ distinct points.

4 Real radical of an ideal

We have introduced in the proof of Theorem 3.4 the real radical $\sqrt[r]{\mathfrak{a}}$ of each ideal $\mathfrak{a}$ of $R[\mathtt{x}]$, and we have shown that it coincides with the ideal of the zero-set of $\mathfrak{a}$. This construction makes sense for ideals of an arbitrary ring A.

Definitions 4.1 Let $\mathfrak{a}$ be an ideal of a ring A. The *real radical* $\sqrt[r]{\mathfrak{a}}$ of $\mathfrak{a}$ is the subset

$$\sqrt[r]{\mathfrak{a}} := \{f \in A : \ \exists\, \sigma \in \Sigma A^2, \ m \geq 1 \text{ such that } f^{2m} + \sigma \in \mathfrak{a}\}.$$

(2) An ideal $\mathfrak{a}$ of A is *real* if for every $a_1, \ldots, a_r \in A$ such that $a_1^2 + \cdots + a_r^2 \in \mathfrak{a}$ then $a_1, \ldots, a_r \in \mathfrak{a}$.

Exercise 4.2 Is the ideal $\mathfrak{a}$ of $R[\mathtt{x}]$ generated by $f := \sum_{i=1}^n \mathtt{x}_i^2$ a real ideal?

Remarks 4.3 (1) The real radical of an ideal $\mathfrak{a}$ is a real ideal containing $\mathfrak{a}$. This last is obvious, because each $f \in \mathfrak{a}$ satisfies $f^2 + 0^2 = f^2 \in \mathfrak{a}$. For the first part, we check first that $\sqrt[r]{\mathfrak{a}}$ is an ideal. Given $a_1, a_2 \in \sqrt[r]{\mathfrak{a}}$ there exist positive integers m y n and $\sigma_1, \sigma_2 \in \Sigma A^2$ such that $a_1^{2m} + \sigma_1 \in \mathfrak{a}$ and $a_2^{2n} + \sigma_2 \in \mathfrak{a}$. Denote $\ell := m + n$ and observe that

$$(a_1 + a_2)^{2\ell} + (a_1 - a_2)^{2\ell} = \sum_{k=0}^{2\ell} \binom{2\ell}{k} a_1^k a_2^{2\ell-k} + \sum_{k=0}^{2\ell} \binom{2\ell}{k} (-1)^k a_1^k a_2^{2\ell-k}.$$

The summands with odd k in the right-hand side cancel, because they are pairwise equal with different signs. Therefore, if we denote $k = 2j$ for those summands with even k,

$$(a_1 + a_2)^{2\ell} + (a_1 - a_2)^{2\ell} = 2 \sum_{j=0}^{\ell} \binom{2\ell}{2j} a_1^{2j} a_2^{2(\ell-j)} = a_1^{2m}\sigma_3 + a_2^{2n}\sigma_4$$

for some $\sigma_3, \sigma_4 \in \Sigma A^2$ because, for each $0 \leq j \leq \ell$,

$$2j + 2(\ell - j) = 2\ell = 2(m+n) = 2m + 2n,$$

and so either $2j \geq 2m$ or $2(\ell - j) \geq 2n$. Consequently,

$$\begin{aligned}(a_1 + a_2)^{2\ell} + (a_1 - a_2)^{2\ell} + \sigma_1\sigma_3 + \sigma_2\sigma_4 &= a_1^{2m}\sigma_3 + a_2^{2n}\sigma_4 + \sigma_1\sigma_3 + \sigma_2\sigma_4 \\ &= (a_1^{2m} + \sigma_1)\sigma_3 + (a_2^{2n} + \sigma_2)\sigma_4 \in \mathfrak{a},\end{aligned}$$

and this implies that $a_1 + a_2 \in \sqrt[r]{\mathfrak{a}}$.

On the other hand, given $b \in \sqrt[r]{\mathfrak{a}}$ and $a \in A$ there exist a positive integer m and $\sigma \in \Sigma A^2$ such that $b^{2m} + \sigma \in \mathfrak{a}$, and so $(ab)^{2m} + a^{2m}\sigma = a^{2m}(b^{2m} + \sigma) \in \mathfrak{a}$. Thus $ab \in \sqrt[r]{\mathfrak{a}}$.

We have just seen that $\sqrt[r]{\mathfrak{a}}$ is an ideal of A, and we prove now that it is real. Let $a_1, \ldots, a_r \in A$ be such that $\sum_{j=1}^r a_j^2 \in \sqrt[r]{\mathfrak{a}}$. Thus, there exist a positive integer m and $\sigma \in \Sigma A^2$ such that

$$\Big(\sum_{i=1}^r a_i^2\Big)^{2m} + \sigma \in \mathfrak{a}.$$

For each fixed index $1 \leq j \leq r$ this can be rewritten as $a_j^{4m} + \sigma_j \in \mathfrak{a}$ for a sum of squares $\sigma_j \in \Sigma A^2$, and this implies that $a_j \in \sqrt[r]{\mathfrak{a}}$.

(2) Every real ideal $\mathfrak{a}$ of a ring A is a radical ideal. Indeed, let $a \in A$ and let m be a positive integer such that $a^m \in \mathfrak{a}$. Let $r \geq 0$ such that $m \leq 2^r$; then $a^{2^r} \in \mathfrak{a}$ and, $\mathfrak{a}$ being a real ideal, it follows by descending recursion that $a \in \mathfrak{a}$.

(3) A prime ideal $\mathfrak{p}$ of A is the support of some prime cone α in A if and only if $\mathfrak{p}$ is a real ideal. Indeed, let α be a prime cone in A such that $\mathfrak{p} := \mathfrak{p}_\alpha$. Suppose, by way of contradiction, that $\mathfrak{p}$ is not a real ideal. Then, there exist $a_1, \ldots, a_r \in A$ such that $a_1^2 + \cdots + a_r^2 \in \mathfrak{p}$ but $a_1 \notin \mathfrak{p}$. Let us denote $x_i := a_i + \mathfrak{p} \in A/\mathfrak{p}$ and, after dividing by $x_1^2 \neq 0$ in the quotient field $\kappa(\mathfrak{p})$ of $A/\mathfrak{p}$, it follows that

$$-1 = \sum_{j=2}^r (x_j/x_1)^2 \in \Sigma\kappa(\mathfrak{p})^2,$$

which is impossible because $\kappa(\mathfrak{p})$ is a real field.

Conversely, let $\mathfrak{p}$ be a real prime ideal of A. Then, the quotient field $\kappa(\mathfrak{p})$ of $A/\mathfrak{p}$ is a real field. Otherwise there would exist non-zero elements $x_1, \ldots, x_r, y \in A/\mathfrak{p}$ such that

$$-1 = \sum_{j=1}^r (x_j/y)^2 \quad \Longrightarrow \quad y^2 + \sum_{j=1}^r x_j^2 = 0.$$

Let $a_1, \ldots, a_r, b \in A \setminus \mathfrak{p}$ such that $y := b + \mathfrak{p}$ and $x_j := a_j + \mathfrak{p}$ for each $1 \leq j \leq r$. We have

$$b^2 + \sum_{j=1}^{r} a_j^2 \in \mathfrak{p},$$

which contradicts the fact that $\mathfrak{p}$ is a real ideal. Thus, the field $\kappa(\mathfrak{p})$ admits an ordering $\leq$ and $\alpha := \{a \in A : \, a + \mathfrak{p} \geq 0\}$ is a prime cone in A whose support is $\mathfrak{p}$.

(4) Let $\mathfrak{b}$ be a real ideal of A containing an ideal $\mathfrak{a}$. Then, $\sqrt[r]{\mathfrak{a}} \subset \mathfrak{b}$. Indeed, given $f \in \sqrt[r]{\mathfrak{a}}$ there exist nonnegative integers r and $m \geq 1$, and $a_1, \ldots, a_r \in A$ such that

$$(f^m)^2 + \sum_{j=1}^{r} a_j^2 \in \mathfrak{a} \subset \mathfrak{b}.$$

Since $\mathfrak{b}$ is a real ideal, $f^m \in \mathfrak{b}$, and so $f \in \mathfrak{b}$ because, by part (2), $\mathfrak{b}$ is a radical ideal. Consequently, $\sqrt[r]{\mathfrak{a}}$ is the smallest real ideal of A containing the ideal $\mathfrak{a}$.

(5) Let $\mathfrak{a}$ be an ideal of A and let $\mathcal{R}(\mathfrak{a})$ be the collection of all prime real ideals of A containing $\mathfrak{a}$. Then,

$$\sqrt[r]{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in \mathcal{R}(\mathfrak{a})} \mathfrak{p}. \tag{4.1}$$

Indeed, by part (4), $\sqrt[r]{\mathfrak{a}} \subset \mathfrak{p}$ for every $\mathfrak{p} \in \mathcal{R}(\mathfrak{a})$, and this proves an inclusion. Let us prove the converse. Suppose, by way of contradiction, that there exists $f \in A \setminus \sqrt[r]{\mathfrak{a}}$ such that $f \in \mathfrak{p}$ for every ideal $\mathfrak{p} \in \mathcal{R}(\mathfrak{a})$. Therefore, the set $\mathcal{F}$ consisting of those real ideals of A containing $\mathfrak{a}$ but not f is non-empty, because $\sqrt[r]{\mathfrak{a}} \in \mathcal{F}$. It is straightforward to check that $\mathcal{F}$, ordered by inclusion, is an inductive set and so, by Zorn's Lemma, it has a maximal element $\mathfrak{q} \in \mathcal{F}$. Let us prove that $\mathfrak{q}$ is a prime ideal of A and, consequently, $\mathfrak{q} \in \mathcal{R}(\mathfrak{a})$, that is $f \in \mathfrak{q}$, which contradicts the fact that $\mathfrak{q} \in \mathcal{F}$.

Indeed let us suppose, by way of contradiction, the existence of $a, b \in A \setminus \mathfrak{q}$ such that $ab \in \mathfrak{q}$. By Remark 4.3 (1) both $\mathfrak{b}_1 := \sqrt[r]{aA + \mathfrak{q}}$ and $\mathfrak{b}_2 := \sqrt[r]{bA + \mathfrak{q}}$ are real ideals containing $\mathfrak{q}$, and so $\mathfrak{a}$. In fact $\mathfrak{q} \subsetneq \mathfrak{b}_i$ for $i = 1, 2$, because $a \in \mathfrak{b}_1 \setminus \mathfrak{q}$ and $b \in \mathfrak{b}_2 \setminus \mathfrak{q}$. This implies, since $\mathfrak{q}$ is maximal in $\mathcal{F}$, that $f \in \mathfrak{b}_1$ and $f \in \mathfrak{b}_2$, that is, there exist integers $m_1, m_2 \geq 1$, two sums of squares $\sigma_1, \sigma_2 \in \Sigma A^2$ and $c_1, c_2 \in A$ and $g_1, g_2 \in \mathfrak{q}$ such that

$$f^{2m_1} + \sigma_1 = ac_1 + g_1 \quad \& \quad f^{2m_2} + \sigma_2 = bc_2 + g_2.$$

Multiplying the above expressions and writing $m := m_1 + m_2$ we get, using also that $ab \in \mathfrak{q}$, that

$$f^{2m} + \sigma_1 f^{2m_2} + \sigma_2 f^{2m_1} + \sigma_1\sigma_2 = abc_1c_2 + g_1bc_2 + g_2ac_1 + g_1g_2 \in \mathfrak{q}.$$

Since $\sigma := \sigma_1 f^{2m_2} + \sigma_2 f^{2m_1} + \sigma_1\sigma_2 \in \Sigma A^2$ and $f^{2m} + \sigma \in \mathfrak{q}$ it follows that $f \in \mathfrak{q}$, because $\mathfrak{q}$ is a real ideal; a contradiction.

(6) Equality (4.1) is the counterpart in Real Algebra of a classical result in Commutative Algebra, see [AM], that states that the *radical* $\sqrt{\mathfrak{a}}$ of an ideal $\mathfrak{a}$ of a ring A, defined as

$$\sqrt{\mathfrak{a}} := \{f \in A : \ \exists m \geq 1 \quad \text{such that } f^m \in \mathfrak{a}\},$$

coincides with the intersection of those prime ideals of A containing $\mathfrak{a}$.

(7) A ring A is real if and only if it contains a real ideal. Indeed, each real ring A contains a prime cone α, and we have proved in part (3) that its support $\mathfrak{p} := \mathfrak{p}_\alpha$ is a real ideal of A. Conversely, if $\mathfrak{a}$ is a real ideal of A it coincides, by part (4), with its real radical, which by part (5) implies that

$$\mathfrak{a} = \bigcap_{\mathfrak{p} \in \mathcal{R}(\mathfrak{a})} \mathfrak{p},$$

where $\mathcal{R}(\mathfrak{a})$ is the collection of those real prime ideals of A containing $\mathfrak{a}$. In particular this collection is non-empty, and we choose $\mathfrak{p} \in \mathcal{R}(\mathfrak{a})$. Using (3) once more, there exists a prime cone α in A whose support is $\mathfrak{p}$, and this means that A is a real ring.

(8) Let $\mathfrak{a}$ be a real ideal of the polynomial ring $R[\mathbf{x}]$. Then, the solution $\mathbf{H17_c}$ to Hilbert's 17th Problem with controlled denominators implies that $\mathcal{Z}(\mathfrak{a})$ is non-empty. Indeed, $R[\mathbf{x}]$ being noetherian, there exist polynomials $f_1, \ldots, f_m \in \mathfrak{a}$ such that $\mathfrak{a} := (f_1, \ldots, f_m)R[\mathbf{x}]$. Therefore, $f = f_1^2 + \cdots + f_m^2 \in \mathfrak{a}$ and $f(x) \geq 0$ for every point $x \in R^n$, and $\mathcal{Z}(f) = \mathcal{Z}(\mathfrak{a})$. Hence, if $\mathcal{Z}(\mathfrak{a}) = \varnothing$, condition (ii) in $\mathbf{H17_c}$ implies the existence of $\sigma_1, \sigma_2 \in \Sigma R[\mathbf{x}]^2$ such that $1 + \sigma_2 = (1 + \sigma_1)f \in \mathfrak{a}$. Thus, $\mathfrak{a}$ being a real ideal, $1 \in \mathfrak{a}$, which is false.

(9) The Real Nullstellensatz states that $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt[r]{\mathfrak{a}}$ for each ideal $\mathfrak{a}$ of $R[\mathbf{x}]$. This is the counterpart, in the real setting, of the classical Hilbert's Nullstellensatz: if C is an algebraically closed field and $\mathfrak{a}$ is an ideal of $C[\mathbf{x}]$, then $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. We will use this result later on and, among the proofs we know of this classical result, we recommend the one of Arrondo in [A], which just involves Linear Algebra arguments.

Exercise 4.4 Is it true that for every prime ideal $\mathfrak{p}$ of the real ring A its real radical $\sqrt[r]{\mathfrak{p}}$ is a prime ideal too?

Exercise 4.5 Let X be a topological space and let $A := \mathcal{C}(X)$ be the ring of $\mathbb{R}$-valued continuous functions on X.

(1) Let $f, g \in A$ such that $0 \leq f(x) \leq g(x)$ for every $x \in X$. Prove that $f^2 \in gA$.

(2) Prove that every radical ideal of the ring A is a real ideal.

(4.6) Lagrange identity and Cauchy-Schwarz inequality. Our next goal is to represent the real radical of an ideal of $R[\mathtt{x}]$ using *nonnegative* elements, see 4.7, instead of sum of squares. To begin with we recall the classical Cauchy-Schwarz inequality and Lagrange identity. Cauchy-Schwarz inequality states that given an euclidean vector space $(E, \langle\cdot,\cdot\rangle)$, that is, $\langle\cdot,\cdot\rangle$ is a positive definite symmetric bilinear form on the real vector space E, and if we denote

$$\|\cdot\| : E \to \mathbb{R},\ u \mapsto \sqrt{\langle u, u\rangle}$$

the *induced norm,* then

$$\langle x, y\rangle^2 \leq \|x\|^2 \cdot \|y\|^2,$$

or equivalently, $|\langle x, y\rangle| \leq \|x\| \cdot \|y\|$, for every $x, y \in E$. In particular, if $E := \mathbb{R}^n$ is endowed with its usual inner product,

$$(x_1y_1+\cdots+x_ny_n)^2 \leq (x_1^2+\cdots+x_n^2)(y_1^2+\ldots+y_n^2) \quad \forall\,(x_1,\ldots,x_n),\ (y_1,\ldots,y_n) \in \mathbb{R}^n.$$

The above inequality follows at once from the *Lagrange identity:* Given variables $\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{y}_1, \ldots, \mathtt{y}_n$,

$$\Big(\sum_{i=1}^n \mathtt{x}_i^2\Big)\Big(\sum_{j=1}^n \mathtt{y}_j^2\Big) - \Big(\sum_{k=1}^n \mathtt{x}_k\mathtt{y}_k\Big)^2 = \sum_{i,j=1}^n \mathtt{x}_i^2\mathtt{y}_j^2 - \sum_{i,j=1}^n \mathtt{x}_i\mathtt{y}_i\mathtt{x}_j\mathtt{y}_j$$
$$= \sum_{\substack{i,j=1\\ i\neq j}}^n \mathtt{x}_i^2\mathtt{y}_j^2 - 2\sum_{\substack{i,j=1\\ i<j}}^n \mathtt{x}_i\mathtt{y}_i\mathtt{x}_j\mathtt{y}_j = \sum_{\substack{i,j=1\\ i<j}}^n (\mathtt{x}_i\mathtt{y}_j - \mathtt{x}_j\mathtt{y}_i)^2. \qquad \text{(LI)}$$

For an arbitrary ring A and elements $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ we deduce

$$\Big(\sum_{i=1}^n a_i^2\Big)\Big(\sum_{j=1}^n b_j^2\Big) - \Big(\sum_{k=1}^n a_kb_k\Big)^2 = \sum_{\substack{i,j=1\\ i<j}}^n (a_ib_j - a_jb_i)^2, \qquad \text{(CS)}$$

and the right-hand side is a finite sum of squares of elements in A.

Notation and Remark 4.7 (1) Let A be a real field. An element $a \in A$ is said to be *nonnegative,* and in such a case we write $a \geq 0$, if $a \in \alpha$ for every prime cone α in A. Given $a, b \in A$ the expression $a \leq b$ means that $b - a \geq 0$. Even more, the usual rules of calculus with inequalities hold: given $a_1 \leq b_1$ and $a_2 \leq b_2$ for some elements $a_1, a_2, b_1, b_2 \in A$ then,

$$a_1 + a_2 \leq b_1 + b_2 \quad \& \quad (b_1 - a_1)(b_2 - a_2) \geq 0.$$

(2) Notice that $f \geq 0$ if and only if there is no prime cone α in A such that $-f \in \alpha$ and $f \notin \mathfrak{p}_\alpha$. By the Abstract Positivstellensatz 3.3, this is equivalent to the existence of a positive integer m and two sums of squares $\sigma_1, \sigma_2 \in \Sigma A^2$ such that $\sigma_1 f = \sigma_2 + f^{2m}$.

We use the facts above to prove the next result, which allows us to represent the real radical of an ideal in terms of the famous Łojasiewicz's inequality, see 4.12.

Lemma 4.8 *Let $\mathfrak{a}$ be an ideal of the ring A. Then,*

$$\sqrt[r]{\mathfrak{a}} = \{a \in A : \ \exists\, b \in \mathfrak{a} \ \&\ m \geq 1 \text{ such that } b - a^{2m} \geq 0\}. \tag{4.2}$$

Proof. Let $\mathfrak{b}$ denote the set in the right-hand side of the equality (4.2), and let us show that $\sqrt[r]{\mathfrak{a}} = \mathfrak{b}$. First, let $a \in \sqrt[r]{\mathfrak{a}}$; then, there exist $a_1, \ldots, a_r \in A$ and a positive integer m such that

$$b := a^{2m} + \sum_{i=1}^{r} a_i^2 \in \mathfrak{a},$$

and so $a \in \mathfrak{b}$ because $b - a^{2m} \geq 0$ since it is a sum of squares in A.

Conversely, given $a \in \mathfrak{b}$ there exist $b \in \mathfrak{a}$ and a positive integer m such that $b - a^{2m} \geq 0$. Note that there is no prime cone α in A such that $-b + a^{2m} \in \alpha$ and $b - a^{2m} \notin \mathfrak{p}_\alpha$, since the first condition together with the hypothesis $b - a^{2m} \in \alpha$ imply that $b - a^{2m} \in \mathfrak{p}_\alpha$.

It follows from the equivalence between (2) and (4) in the Abstract Positivstellensatz 3.3 that there exist $\sigma_1, \sigma_2 \in \Sigma A^2$ and a positive integer ℓ such that

$$\sigma_1 + (-b + a^{2m})\sigma_2 + (-b + a^{2m})^{2\ell} = 0.$$

Consequently,

$$(-b + a^{2m})^{2\ell} + \sigma_1 + a^{2m}\sigma_2 = b\sigma_2 \in \mathfrak{a},$$

and this implies $-b + a^{2m} \in \sqrt[r]{\mathfrak{a}}$. Since $b \in \mathfrak{a} \subset \sqrt[r]{\mathfrak{a}}$ and this last is a radical ideal, we deduce that $a \in \sqrt[r]{\mathfrak{a}}$, as we want to prove. □

Next we strengthen Lemma 4.8 for finitely generated ideals of a real ring.

Lemma 4.9 *Let A be a real ring, $\mathfrak{a} := (f_1, \ldots, f_r)$ a finitely generated ideal of A and $f := f_1^2 + \cdots + f_r^2$. Then,*

$$\sqrt[r]{\mathfrak{a}} = \Big\{a \in A : \ \exists\, m \geq 1 \quad \& \quad \sigma \in \Sigma A^2 \text{ such that } \sigma f - a^{2m} \geq 0\Big\}.$$

Proof. Indeed, since $f \in \mathfrak{a}$ it follows from the precedent Lemma 4.8 that $\sqrt[r]{\mathfrak{a}}$ contains the set $\mathfrak{b}$ in the right-hand side of the proposed equality. Conversely, let $a \in \sqrt[r]{\mathfrak{a}}$. By Lemma 4.8, there exist $b \in \mathfrak{a}$ and a positive integer ℓ such that $b - a^{2\ell} \geq 0$. Since $b \in \mathfrak{a}$ there exist $g_1, \ldots, g_r \in A$ such that $b := g_1 f_1 + \cdots + g_r f_r$. Let $\sigma := g_1^2 + \cdots + g_r^2 \in \Sigma A^2$. It follows from 4.6 (CS) that $\sigma f - b^2 \in \Sigma A^2$, and this implies $\sigma f - b^2 \geq 0$.

On the other hand $b - a^{2\ell} \geq 0$, and consequently,

$$b + a^{2\ell} = (b - a^{2\ell}) + 2a^{2\ell} \geq 0 \quad \Longrightarrow \quad b^2 - a^{4\ell} = (b + a^{2\ell})(b - a^{2\ell}) \geq 0.$$

In this way, if we denote $m := 2\ell$ we have $b^2 - a^{2m} \geq 0$ and $\sigma f - b^2 \geq 0$. Henceforth,

$$\sigma f - a^{2m} = (\sigma f - b^2) + (b^2 - a^{2m}) \geq 0,$$

as wanted. □

Remark 4.10 For every polynomial $f \in R[\mathbf{x}]$, the algebraic statement $f \geq 0$ *in the ring* $R[\mathbf{x}]$ is equivalent to the geometric statement $f(x) \geq 0$ *for every* $x \in R^n$.

Indeed, we have proved in 3.9 that given $f \in R[\mathbf{x}]$ satisfying $f(x) \geq 0$ for every $x \in R^n$, there exist $\sigma_1, \sigma_2 \in \Sigma R[\mathbf{x}]^2$ and an integer $m \geq 1$ such that $\sigma_1 f = \sigma_2 + f^{2m}$. Thus, by Remark 4.7, $f \geq 0$ in the ring $R[\mathbf{x}]$.

Conversely, if $f \geq 0$ in $R[\mathbf{x}]$ there exist two sums of squares σ_1 and σ_2 in $R[\mathbf{x}]$ such that $\sigma_1 f = \sigma_2 + f^{2m}$, and so $f(x) \geq 0$ for every point $x \in R^n$. Otherwise there would exist $x \in R^n$ such that $f(x) < 0$, and so

$$0 < f(x)^{2m} = \sigma_1(x) f(x) - \sigma_2(x) \leq 0,$$

a contradiction.

As we announced in 4.6, our goal is to obtain an alternative presentation of the real radical of an ideal of the ring $R[\mathbf{x}]$ without involving sums of squares, that are substituted by nonnegative polynomials. Moreover, the next theorem shows that the information about the real radical of an ideal $\mathfrak{a}$ of $R[\mathbf{x}]$ lies in a nonnegative polynomial whose zero-set equals $\mathcal{Z}(\mathfrak{a})$; for example, the sum of the squares of a finite system of generators of $\mathfrak{a}$. The result we want to prove is the following:

Theorem 4.11 *Let* $\mathfrak{a}$ *be an ideal of* $R[\mathbf{x}]$ *and let* $f \in R[\mathbf{x}]$ *be such that* $f(x) \geq 0$ *for each point* $x \in R^n$ *and* $\mathcal{Z}(f) = \mathcal{Z}(\mathfrak{a})$. *Then,*

$$\sqrt[r]{\mathfrak{a}} = \{g \in R[\mathbf{x}] : \ \exists\, m, \ell \geq 1,\ L > 0 : \ Lf(x)(1 + \|x\|^2)^\ell - g^{2m}(x) \geq 0 \ \forall\, x \in R^n\}.$$

The key to prove the precedent theorem is the so called *Łojasiewicz's inequality for polynomials* that we present right now and has its own interest. This inequality was obtained by Łojasiewicz [Ł], who used it in problems of the division of a distribution by a function.

Lemma 4.12 (Polynomial Łojasiewicz's inequality) *Let $f, g \in R[\mathtt{x}]$ be polynomials satisfying $\mathcal{Z}(f) \subset \mathcal{Z}(g)$. Then, there exist positive integers m, ℓ and $L \in R$ such that*

$$g^{2m}(x) \leq L|f(x)|(1 + \|x\|^2)^{\ell} \quad \forall\, x \in R^n.$$

Proof. Let $\mathfrak{a} := (f)$ be the ideal of $R[\mathtt{x}]$ generated by f. Since $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(f) \subset \mathcal{Z}(g)$ it follows from the Real Nullstellensatz 3.4, that $g \in \mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt[r]{\mathfrak{a}}$, and so there exist $h \in R[\mathtt{x}]$, $\sigma \in \Sigma R[\mathtt{x}]^2$ and a positive integer m satisfying $g^{2m} + \sigma = fh$. Consequently, $g^{2m}(x) \leq |f(x)| \cdot |h(x)|$ for every point $x \in R^n$. Thus, it is enough to prove the following:

(4.12.1) *Given a polynomial $h \in R[\mathtt{x}]$ there exist a positive integer ℓ and $L \in R$ such that $|h(x)| \leq L(1 + \|x^2\|)^{\ell}$ for every point $x \in R^n$.*

Indeed, we choose an integer $\ell \geq \deg(h)/2$ and denote $N := \{\nu \in \mathbb{N}^n : |\nu| \leq 2\ell\}$ where, as usual, $|(\nu_1, \ldots, \nu_n)| = \nu_1 + \cdots + \nu_n$. Write $h(\mathtt{x}) := \sum_{\nu \in N} a_\nu \mathtt{x}^\nu$ and denote

$$L_0 := \max\{|a_\nu| : \nu \in N\} \quad \& \quad L := L_0 \cdot \mathrm{card}(N).$$

Then, for every point $x := (x_1, \ldots, x_n) \in R^n$ we have

$$|h(x)| \leq \sum_{\nu \in N} |a_\nu| \cdot |x_1|^{\nu_1} \cdots |x_n|^{\nu_n} \leq \sum_{\nu \in N} |a_\nu| \cdot \|x\|^{\nu_1} \cdots \|x\|^{\nu_n} \leq \sum_{\nu \in N} L_0 \|x\|^{|\nu|}.$$

In particular, if $\|x\| \leq 1$ then $|h(x)| \leq L$, and for every point $x \in R^n$ such that $\|x\| > 1$, we have $|h(x)| \leq L\|x\|^{2\ell}$. In both cases,

$$|h(x)| \leq L(1 + \|x\|^{2\ell}) \leq L(1 + \|x^2\|)^{\ell},$$

and we are done. □

Remark 4.13 Łojasiewicz's inequality 4.12 can be proved without using the Real Nullstellensatz, by means of some basic results on semialgebraic sets.

Next we prove Theorem 4.11.

Proof of Theorem 4.11. Let $g \in \mathbb{R}[\mathtt{x}]$, a positive $L \in R$ and positive integers m, ℓ such that $g^{2m}(x) \leq L|f(x)|(1 + \|x\|^2)^{\ell}$. Then, $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(f) \subset \mathcal{Z}(g)$, and so $g \in \mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt[r]{\mathfrak{a}}$.

Conversely, given $g \in \sqrt[r]{\mathfrak{a}} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ we have $\mathcal{Z}(f) = \mathcal{Z}(\mathfrak{a}) \subset \mathcal{Z}(g)$. By Łojasiewicz's inequality 4.12, there exist positive integers m, ℓ and $L \in R$, necessarily positive, such that $g^{2m}(x) \leq L|f(x)|(1 + \|x\|^2)^{\ell}$ for every point $x \in R^n$. □

Notations and Remarks 4.14 (1) The last result in this section states that the solution to Hilbert's 17th Problem with controlled denominators together with Łojasiewicz's inequality imply the Real Nullstellensatz.

(2) Recall that if K is a field, a subset $Z \subset K^n$ is *algebraic* if there exists an ideal $\mathfrak{a}$ of $K[\mathtt{x}]$ such that $Z := \mathcal{Z}(\mathfrak{a})$. Since $\mathfrak{a}$ is finitely generated, there exist $f_1, \ldots, f_m \in K[\mathtt{x}]$ such that $\mathfrak{a} := (f_1, \ldots, f_m)K[\mathtt{x}]$, and so

$$Z = \{x \in K^n : \ f_1(x) = 0, \ldots, f_m(x) = 0\}.$$

If K is a real closed field, the polynomial $f := \sum_{j=1}^m f_j^2$ satisfies $Z = \mathcal{Z}(f)$.

(3) We will use next, simultaneously, algebraic subsets of R^n and C^n, where R is a real closed field and $C := R[\sqrt{-1}]$ is its algebraic closure. To avoid misunderstandings we associate two polynomial functions to each polynomial $f \in R[\mathtt{x}] \subset C[\mathtt{x}]$, that we denote

$$f : R^n \to R, \ x \mapsto f(x) \quad \& \quad F : C^n \to C, \ z \mapsto f(z),$$

that is, we denote with the capital letter F the unique polynomial function $C^n \to C$ whose restriction to R^n is f. We say that F is the *extension* of f to C^n, and denote

$$\mathcal{Z}(f) := \{x \in R^n : f(x) = 0\} \quad \& \quad \mathcal{Z}_C(F) := \{z \in C^n : F(z) = 0\}.$$

(4) Let us see, by induction on n, that if a polynomial $F \in C[\mathtt{x}]$ vanishes at each point $x \in R^n$, then F is the zero polynomial. This can be seen as some kind of Identity Principle, see Proposition 3.2 (Ch.I), that for $n = 1$ follows from the fact that R is an infinite set, because it contains $\mathbb{Q}$, but the set of roots of a non-zero polynomial is finite. For $n > 1$, let $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ and write

$$F := \sum_{j=0}^{d} a_j(\mathtt{x}')\mathtt{x}_n^j, \quad \text{where each} \quad a_j \in C[\mathtt{x}'].$$

For every point $x' \in R^{n-1}$ the polynomial $F(x', \mathtt{x}_n) \in C[\mathtt{x}_n]$ vanishes identically on R; hence it is the zero polynomial. Thus $a_j(x') = 0$ for each $0 \leq j \leq d$ and every $x' \in R^{n-1}$. The induction hypothesis implies that each $a_j = 0$, and so $F = 0$.

Lemma 4.15 *Let $h, b \in R[\mathtt{x}] \setminus R$ and let $Z \subset C^n$ be an algebraic set such that $Z \not\subset \mathcal{Z}_C(H)$. Then, there exists $\omega \in R^n$ such that, if $b_1(\mathtt{x}) := b(\mathtt{x} + h(\mathtt{x})\omega)$ then, $Z \not\subset \mathcal{Z}_C(B_1)$.*

Proof. Note that if $Z \not\subset \mathcal{Z}_C(B)$ it suffices to choose $\omega = 0$; thus we assume that $Z \subset \mathcal{Z}_C(B)$. Denote $A := B(\mathtt{x} + \mathtt{t}\mathtt{y}) \in C[\mathtt{x}, \mathtt{t}, \mathtt{y}]$, where $\mathtt{t}$ is a single variable and

$\mathtt{y} := (\mathtt{y}_1, \ldots, \mathtt{y}_n)$. Since b is not constant, for each $(x,t) \in C^n \times (C \setminus \{0\})$ the polynomial $A(x,t,\mathtt{y})$ is not constant. On the other hand, $a(\mathtt{x},0,\mathtt{y}) = b(\mathtt{x})$, and so $\mathtt{t}$ divides $a-b$ in $R[\mathtt{x},\mathtt{t},\mathtt{y}]$; in other words, the quotient $g := (a-b)/\mathtt{t} \in R[\mathtt{x},\mathtt{t},\mathtt{y}]$ is a polynomial and we consider its extension $G := (A-B)/\mathtt{t} \in C[\mathtt{x},\mathtt{t},\mathtt{y}]$. In this way,

$$A(\mathtt{x},\mathtt{t},\mathtt{y}) = B(\mathtt{x}+\mathtt{t}\mathtt{y}) = B(\mathtt{x}) + \mathtt{t}G(\mathtt{x},\mathtt{t},\mathtt{y}).$$

For every point $(x,t) \in C^n \times (C \setminus \{0\})$ the polynomial $A(x,t,\mathtt{y}) = B(x) + tG(x,t,\mathtt{y})$ is not constant, and so the same holds for the polynomial $G(x,t,\mathtt{y})$.

Notice that $Z \not\subset \mathcal{Z}_C(H)$ and $Z \subset \mathcal{Z}_C(B)$. Hence there exists $u \in Z$ with $H(u) \neq 0$, but $B(u) = 0$. Therefore

$$A(u,H(u),\mathtt{y}) = B(u) + H(u)G(u,H(u),\mathtt{y}) = H(u)G(u,H(u),\mathtt{y}),$$

and $H(u) \neq 0$. We know that the polynomial $G(u,H(u),\mathtt{y})$ is not constant; in particular it is not identically zero. Hence, it follows from Remark 4.14 (4) that there exists $\omega \in R^n$ such that $G(u,H(u),\omega) \neq 0$. Define $B_1(\mathtt{x}) := B_1(\mathtt{x} + H(\mathtt{x})\omega)$; in this way, $u \in Z$ satisfies

$$B_1(u) = B(u + H(u)\omega) = H(u)G(u,H(u),\omega) \neq 0,$$

that is, $u \in Z \setminus \mathcal{Z}_C(B_1)$. □

Lemma 4.16 *Let R be a real closed field and let $C := R[\sqrt{-1}]$ be its algebraic closure. Let $\mathfrak{p}, \mathfrak{a}$ and $\mathfrak{b}$ be ideals of $R[\mathtt{x}]$. Then,*

(1) *The equality $\mathfrak{a}C[\mathtt{x}] \cap R[\mathtt{x}] = \mathfrak{a}$ holds.*

(2) *If $\mathfrak{a}C[\mathtt{x}] = \mathfrak{b}C[\mathtt{x}]$, then $\mathfrak{a} = \mathfrak{b}$.*

(3) *If $\mathfrak{p}$ is a real prime ideal then, $\mathfrak{p}C[\mathtt{x}]$ is a prime ideal of $C[\mathtt{x}]$.*

Proof. (1) The inclusion $\mathfrak{a} \subset \mathfrak{a}C[\mathtt{x}]) \cap R[\mathtt{x}]$ is evident, and so it is enough to prove that $\mathfrak{g} := \mathfrak{a}C[\mathtt{x}] \cap R[\mathtt{x}] \subset \mathfrak{a}$. Given $g \in \mathfrak{g}$, its extension $G \in \mathfrak{a}C[\mathtt{x}]$, and so there exist $f_1, \ldots, f_r \in \mathfrak{a}$ and $H_1, \ldots, H_r \in C[\mathtt{x}]$ such that $G = F_1H_1 + \cdots + F_rH_r$. Let us write

$$A_i(\mathtt{x}) := \frac{H_i(\mathtt{x}) + \overline{H_i(\overline{\mathtt{x}})}}{2} \quad \& \quad B_i(\mathtt{x}) := \frac{H_i(\mathtt{x}) - \overline{H_i(\overline{\mathtt{x}})}}{2\sqrt{-1}}$$

where the operator $\overline{(\cdot)}$ denotes complex conjugation. Notice that the coefficients of A_i and B_i are in R, that is, there exist $a_i, b_i \in R[\mathtt{x}]$ such that A_i and B_i are the extensions of a_i and b_i, and $H_i = A_i + \sqrt{-1}B_i$. Thus,

$$G = F_1A_1 + \cdots + F_rA_r + \sqrt{-1}(F_1B_1 + \cdots + F_rB_r).$$

Since the coefficients of G are in R, comparing the coefficients of both members we get

$$G = F_1A_1 + \cdots + F_rA_r \quad \& \quad F_1B_1 + \cdots + F_rB_r = 0.$$

From the first equality $g = f_1a_1 + \cdots + f_ra_r \in \mathfrak{a}$.

(2) This is the immediate consequence of part (1).

(3) Let $A, B \in C[\mathtt{x}]$ such that $AB \in \mathfrak{p}C[\mathtt{x}]$. Define

$$A_1(\mathtt{x}) := \frac{A(\mathtt{x}) + \overline{A(\overline{\mathtt{x}})}}{2}, \ A_2(\mathtt{x}) := \frac{A(\mathtt{x}) - \overline{A(\overline{\mathtt{x}})}}{2\sqrt{-1}},$$
$$B_1(\mathtt{x}) := \frac{B(\mathtt{x}) + \overline{B(\overline{\mathtt{x}})}}{2}, \ B_2(\mathtt{x}) := \frac{B(\mathtt{x}) - \overline{B(\overline{\mathtt{x}})}}{2\sqrt{-1}},$$

and note that $A = A_1 + \sqrt{-1}A_2$ and $B = B_1 + \sqrt{-1}B_2$. Moreover, A_i, B_i are, respectively, the extensions of polynomials $a_i, b_i \in R[\mathtt{x}]$. Then,

$$(A(\mathtt{x})\overline{A(\overline{\mathtt{x}})})(B(\mathtt{x})\overline{B(\overline{\mathtt{x}})}) = AB(\mathtt{x})\overline{(AB)(\overline{\mathtt{x}})} \in \mathfrak{p}C[\mathtt{x}].$$

The coefficients of $F(\mathtt{x}) := (A(\mathtt{x})\overline{A(\overline{\mathtt{x}})})$ and $G(\mathtt{x}) := (B(\mathtt{x})\overline{B(\overline{\mathtt{x}})})$ are in R, and so F and G are, respectively, the extensions of two polynomials $f, g \in R[\mathtt{x}]$. Since $FG \in \mathfrak{p}C[\mathtt{x}]$ we have $fg \in \mathfrak{p}$ and, $\mathfrak{p}$ being a prime ideal, we may assume that $f \in \mathfrak{p}$. Note that $f = a_1^2 + a_2^2 \in \mathfrak{p}$ and, since $\mathfrak{p}$ is a real ideal, we deduce that $a_1, a_2 \in \mathfrak{p}$, and so $A_1, A_2 \in \mathfrak{p}C[\mathtt{x}]$. Thus, $A = A_1 + \sqrt{-1}A_2 \in \mathfrak{p}C[\mathtt{x}]$, that is, $\mathfrak{p}C[\mathtt{x}]$ is a prime ideal. □

Exercise 4.17 Find a prime ideal $\mathfrak{p}$ of $\mathbb{R}[\mathtt{x}]$ such that $\mathfrak{p}\mathbb{C}[\mathtt{x}]$ is not a prime ideal. Therefore, the condition $\mathfrak{p}$ *is a real prime ideal* in Lemma 4.16 (3) is necessary.

We are in a position to prove that the solution to Hilbert's 17th Problem with controlled denominators (**H17$_\mathbf{c}$**) together with Łojasiewicz's inequality (Ł) imply the Real Nullstellensatz (**RNSS**).

Proof. (Proof of (**H17$_\mathbf{c}$**) + (Ł) $\Longrightarrow$ **(RNSS)**) We must prove that $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt[r]{\mathfrak{a}}$ for every ideal $\mathfrak{a} \subset R[\mathtt{x}]$. We begin by proving this if $\mathfrak{a} = \mathfrak{p}$ is a real prime ideal. In this case $\sqrt[r]{\mathfrak{p}} = \mathfrak{p}$, and so we should prove that $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}$; note that the inclusion $\mathfrak{p} \subset \mathcal{I}(\mathcal{Z}(\mathfrak{p}))$ is clear.

Conversely, suppose that $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) \setminus \mathfrak{p} \neq \varnothing$. Let us see that this implies that

$$\mathcal{Z}_C(\mathfrak{p}C[\mathtt{x}]) \setminus \mathcal{Z}_C(\mathcal{I}(\mathcal{Z}(\mathfrak{p}))C[\mathtt{x}]) \neq \varnothing. \tag{4.3}$$

Otherwise, $\mathcal{Z}_C(\mathfrak{p}C[\mathtt{x}]) = \mathcal{Z}_C(\mathcal{I}(\mathcal{Z}(\mathfrak{p}))C[\mathtt{x}])$ and, by Hilbert's Nullstellensatz,

$$\sqrt{\mathfrak{p}C[\mathtt{x}]} = \mathcal{I}(\mathcal{Z}_C(\mathfrak{p}C[\mathtt{x}])) = \mathcal{I}(\mathcal{Z}_C(\mathcal{I}(\mathcal{Z}(\mathfrak{p}))C[\mathtt{x}])) = \sqrt{\mathcal{I}(\mathcal{Z}(\mathfrak{p}))C[\mathtt{x}]}.$$

We have proved in Lemma 4.16 (3) that $\mathfrak{p}C[\mathtt{x}]$ is a prime ideal; in particular it is a radical ideal and consequently

$$\mathfrak{p}C[\mathtt{x}] \subset \mathcal{I}(\mathcal{Z}(\mathfrak{p}))C[\mathtt{x}] \subset \sqrt{\mathcal{I}(\mathcal{Z}(\mathfrak{p}))C[\mathtt{x}]} = \sqrt{\mathfrak{p}C[\mathtt{x}]} = \mathfrak{p}C[\mathtt{x}],$$

that is, $\mathfrak{p}C[\mathtt{x}] = \mathcal{I}(\mathcal{Z}(\mathfrak{p}))C[\mathtt{x}]$. This implies, by Lemma 4.16 (2), that $\mathfrak{p} = \mathcal{I}(\mathcal{Z}(\mathfrak{p}))$ against our assumption $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) \setminus \mathfrak{p} \neq \varnothing$, which proves statement (4.3).

Hence, if we denote $Z := \mathcal{Z}_C(\mathfrak{p}C[\mathtt{x}])$ there exists $g \in \mathcal{I}(\mathcal{Z}(\mathfrak{p}))$ with $Z \not\subset \mathcal{Z}_C(G)$. Thus, in particular, $g \notin \mathfrak{p}$ since otherwise $G \in \mathfrak{p}C[\mathtt{x}]$, and so $Z \subset \mathcal{Z}_C(G)$.

We have pointed out in Remark 4.14 (2) that there exists $f \in \mathfrak{p}$ such that $\mathcal{Z}(f) = \mathcal{Z}(\mathfrak{p})$. But $\mathcal{Z}(f) \subset \mathcal{Z}(g)$ and so, by Łojasiewicz's inequality 4.12, there exist positive integers m, ℓ, and $L \in R$ satisfying

$$L(1 + \|x\|^2)f(x) - g(x)^{2m} \geq 0 \quad \forall\, x \in R^n.$$

Define $h(\mathtt{x}) := 2L(1 + \|\mathtt{x}\|^2)f - g^{2m} \in R[\mathtt{x}]$ and observe that $\mathcal{Z}(h) = \mathcal{Z}(f)$. Indeed, if $f(x) = 0$ then $g(x) = 0$ and therefore $h(x) = 0$. Conversely, if $h(x) = 0$ we have

$$L(1 + \|x\|^2)f(x) + (L(1 + \|x\|^2)f(x) - g(x)^{2m}) = 0,$$

and, both summands being nonnegative, both equal zero. Thus $f(x) = 0$, and so $\mathcal{Z}(h) = \mathcal{Z}(f) = \mathcal{Z}(\mathfrak{p})$.

Since $h(x) \geq 0$ for every point $x \in R^n$ there exist, by $\mathbf{H17_c}$, a polynomial $b \in R[\mathtt{x}]$ and $\sigma_1 \in \Sigma R[\mathtt{x}]^2$ such that $\mathcal{Z}(b) \subset \mathcal{Z}(h)$ and $b^2 h = \sigma_1$. By Lemma 4.15 there exists a vector $\omega \in R^n$ such that the polynomial $b_1(\mathtt{x}) := b(\mathtt{x} + h^2(\mathtt{x})\omega)$ satisfies $Z \not\subset \mathcal{Z}_C(B_1)$. In particular $b_1 \notin \mathfrak{p}$; otherwise $Z \subset \mathcal{Z}_C(B_1)$.

On the other hand, there exists $p \in R[\mathtt{x}, \mathtt{t}, \mathtt{y}]$ with $h(\mathtt{x} + \mathtt{t}\mathtt{y}) = h(\mathtt{x}) + \mathtt{t}p(\mathtt{x}, \mathtt{t}, \mathtt{y})$, and consequently

$$h(\mathtt{x} + h^2(\mathtt{x})\omega) = h(\mathtt{x}) + h^2(\mathtt{x})p(\mathtt{x}, h^2(\mathtt{x}), \omega) = h(\mathtt{x})(1 + h(\mathtt{x})p(\mathtt{x}, h^2(\mathtt{x}), \omega)) = h(\mathtt{x})q(\mathtt{x}),$$

where $q(\mathtt{x}) := 1 + h(\mathtt{x})p(\mathtt{x}, h^2(\mathtt{x}), \omega) \in R[\mathtt{x}]$. Notice that $q(x) \geq 0$ for every $x \in R^n$.

This is obvious if $h(x) = 0$, because in such a case $q(x) = 1$, while if $h(x) \neq 0$ then, $h(x) > 0$ and $h(x + h^2(x)\omega) \geq 0$, which implies

$$q(x) = \frac{h(x + h^2(x)\omega)}{h(x)} \geq 0.$$

This argument shows also that $\mathcal{Z}(q) \cap \mathcal{Z}(h) = \varnothing$, and so $q \notin \mathfrak{p}$. Otherwise $\mathcal{Z}(h) = \mathcal{Z}(\mathfrak{p})$ is contained in $\mathcal{Z}(q)$, and $\mathcal{Z}(\mathfrak{p}) = \mathcal{Z}(q) \cap \mathcal{Z}(h) = \varnothing$. However, we have seen in Remark 4.3 (8), that the hypothesis $\mathbf{H17_c}$ implies that $\mathcal{Z}(\mathfrak{p}) \neq \varnothing$.

But $q(x) \geq 0$ for every point $x \in R^n$, and this implies, by $\mathbf{H17_c}$ the existence of $c \in R[\mathtt{x}]$ and $\sigma_2 \in \Sigma R[\mathtt{x}]^2$ satisfying $\mathcal{Z}(c) \subset \mathcal{Z}(q)$ and $c^2 q = \sigma_2$. In particular, $\mathcal{Z}(c) \cap \mathcal{Z}(h) = \varnothing$, and again $c \notin \mathfrak{p}$. Moreover, since $b^2 h = \sigma_1$,

$$b_1(\mathtt{x})^2 h(\mathtt{x}) q(\mathtt{x}) = b(\mathtt{x} + h^2(\mathtt{x})\omega)^2 h(\mathtt{x} + h^2(\mathtt{x})\omega) = \sigma_1(\mathtt{x} + h^2(\mathtt{x})\omega) = \sigma_3(\mathtt{x}),$$

where $\sigma_3(\mathtt{x}) := \sigma_1(\mathtt{x} + h^2(\mathtt{x})\omega) \in \Sigma R[\mathtt{x}]^2$. Now,

$$b_1^2 c^2 q \cdot (2L(1 + \|\mathtt{x}\|^2) f = b_1^2 c^2 q \cdot (g^{2m} + h) = b_1^2 c^2 q g^{2m} + b_1^2 c^2 q h = b_1^2 \sigma_2 g^{2m} + c^2 \sigma_3.$$

Since $f \in \mathfrak{p}$ and $\mathfrak{p}$ is a real ideal, we deduce that each one of the summands in the sum of squares $b_1^2 \sigma_2 g^{2m} + c^2 \sigma_3$ belongs to $\mathfrak{p}$.

In particular, $b_1^2 c^2 q g^{2m} = b_1^2 \sigma_2 g^{2m} \in \mathfrak{p}$, but this is impossible, because $\mathfrak{p}$ is a prime ideal and $b_1, c, q, g \notin \mathfrak{p}$.

In this way, our assumption $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) \setminus \mathfrak{p} \neq \varnothing$ is false, and this means $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}$.

To finish we study the case of an arbitrary ideal $\mathfrak{a}$ of $R[\mathtt{x}]$. Since $R[\mathtt{x}]$ is a noetherian ring and, according to Remarks 4.3 (1) and (2), $\sqrt[r]{\mathfrak{a}}$ is a radical ideal, there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of $R[\mathtt{x}]$ such that

$$\sqrt[r]{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s \quad \& \quad \bigcap_{j \neq i} \mathfrak{p}_j \setminus \mathfrak{p}_i \neq \varnothing \quad \text{for each } 1 \leq i \leq s.$$

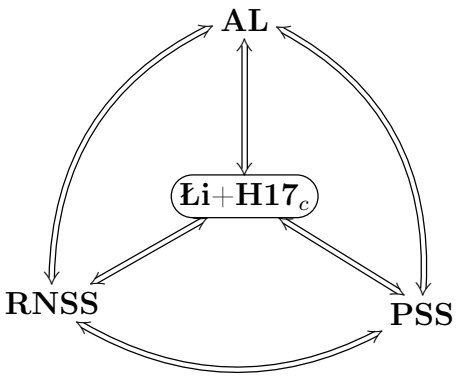
Let us see that each $\mathfrak{p}_i$ is a real ideal. Indeed, let $a_1, \ldots, a_\ell \in R[\mathtt{x}]$ such that $a_1^2 + \cdots + a_\ell^2 \in \mathfrak{p}_i$. Choose $h_i \in \bigcap_{j \neq i} \mathfrak{p}_j \setminus \mathfrak{p}_i$. Then $h_i^2(a_1^2 + \cdots + a_\ell^2) \in \sqrt[r]{\mathfrak{a}}$ and, this last being a real ideal, we deduce that each product $h_i a_k \in \sqrt[r]{\mathfrak{a}} \subset \mathfrak{p}_i$. Since $\mathfrak{p}_i$ is a prime ideal and $h_i \notin \mathfrak{p}_i$ it follows that $a_k \in \mathfrak{p}_i$ for each $1 \leq k \leq \ell$, and so $\mathfrak{p}_i$ is a real prime ideal.

Finally, using the case studied before,

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(\mathcal{Z}(\sqrt[r]{\mathfrak{a}})) = \mathcal{I}\Big(\mathcal{Z}\Big(\bigcap_{i=1}^{s} \mathfrak{p}_i\Big)\Big) = \bigcap_{i=1}^{s} \mathcal{I}(\mathcal{Z}(\mathfrak{p}_i)) = \bigcap_{i=1}^{s} \mathfrak{p}_i = \sqrt[r]{\mathfrak{a}},$$

which concludes the proof. □

To finish this section, we recall the employed notation and put together the relationship between the results obtained in the precedent sections.



H17$_c$: Solution to Hilbert's 17th Problem with controlled denominators.

Łi: Łojasiewicz's Inequality.

RNSS: Real Nullstellensatz.

AL: Artin-Lang's Theorem.

PSS: Positivstellensätze.

(4.18) Real Nullstellensatz and Positivstellensäzte for other rings of functions. Hilbert's 17th Problem, the Real Nullstellensatz and the Positivstellensätze can be formulated, introducing the suitable changes, in different function or function germ rings. Without any doubt, analytic set and function germs constitute the *most favorable setting* to attack these questions.

(4.18.1) **Rings of analytic function germs.** The first results are due to Risler, [Ri3], who proved that **H17** has affirmative answer for the ring $\mathcal{O}_n$ of analytic function germs at the origin of $\mathbb{R}^n$, and he presented the Real Nullstellensatz in this setting. The same results for the ring $\mathcal{F}_n$ of formal series were independently obtained by Merrien, [Me] and Robbin, [Rb]. Ruiz gave in [Rz2] an affirmative answer to **H17** for the ring $\mathcal{O}(X_0)$ of germs of analytic functions on an irreducible analytic germ set X_0.

It is natural to ask if each positive semidefinite function germ in $\mathcal{O}(X_0)$ is already a sum of squares in the ring $\mathcal{O}(X_0)$. Based on a previous result of Scheiderer [Sch1], Fernando proved in [F1] that this is not so if $\dim(X_0) \geq 3$. Moreover, it follows from another work of Scheiderer [Sch2], that the unique rings of analytic curve germs for which every positive semidefinite function germ is a sum of squares correspond to finite unions of lines. Thus, just the case of analytic germs of dimension 2 requires some care. A first result in this direction is due to Ruiz [Rz4], who proposed a finite list of surface germs X_0 which may have the property that all positive semidefinite germs in $\mathcal{O}(X_0)$ are sum of two squares. Later on, Fernando [F2] proved that Ruiz's list is exhaustive, and in fact that it coincides with the list of all bidimensional analytic germs X_0 with embedding dimension equal to 3 for which every positive semidefinite function germ is a sum of squares in the ring $\mathcal{O}(X_0)$.

(4.18.2) **Rings of global analytic functions.** The problems we are dealing with are more difficult for the ring $\mathcal{O}(X)$ of global analytic functions on a global analytic set X. The first significant result is due to Bochnak and Risler [BR], who restricted themselves to the case $\dim(X) \leq 2$, and proved two main results. The first one is

a version of the Real Nullstellensatz: given a finitely generated ideal $\mathfrak{a}$ of $\mathcal{O}(X)$ the equality $\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ holds if and only if $\mathfrak{a}$ is a real ideal. Moreover they obtained an affirmative answer to **H17** *without denominators* in two particular cases: if X is compact, and if X is not compact together with $H^1(X, \mathbb{Z}_2) = 0$. This result was proved using different methods by Jaworski in [JW1], and Bochnak, Kucharz and Shiota [BKS] proved that given an analytic real variety X and a positive semidefinite analytic function $f : X \to \mathbb{R}$ whose zero-set $\mathcal{Z}(f)$ is discrete, f is a sum of squares of meromorphic functions on X. Even more, they showed that in case $\dim(X) \leq 2$ then, 3 squares are enough.

Ruiz proved later [Rz4] the equality $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt[r]{\mathfrak{a}}$ for finitely generated ideals $\mathfrak{a}$ of $\mathcal{O}(X)$ without any restriction on the dimension of X but imposing the zero-set $\mathcal{Z}(\mathfrak{a})$ to be compact. Notice that, in particular, the hypothesis hold if X is compact. Concerning **H17**, it is proved in [Rz4] that in case X is compact and irreducible and $f : X \to \mathbb{R}$ is a positive semidefinite analytic function, then f is a sum of squares of meromorphic functions on X. Independently, Jaworski proved in [JW2] that if the zero-set of f is discrete outside a compact set, then it is a sum of squares of meromorphic functions.

The first result with neither compactness assumptions nor restrictions on the zero-set was proved by Acquistapace, Broglia, Fernando and Ruiz in [ABFR2] where, among many other results, they proved that given an analytic curve X, each positive semidefinite analytic function $f : X \to \mathbb{R}$ is a sum of squares in $\mathcal{O}(X)$ if and only if the function germ f_x is a sum of squares in the ring of analytic germs $\mathcal{O}(X_x)$ for every point $x \in X$. As one can expect, in this case two squares are enough.

Along these notes we have refrain ourselves from treating the very important quantitative aspects of **H17**, that is, to determine what is the minimum number of squares needed to express a given sum of squares. However, we must quote here that Andradas, Díaz Cano and Ruiz proved in [ADR] that given an integer $d \geq 2$ there exists an integer $p := p(d)$ such that each positive semidefinite analytic function $f \in \mathcal{O}(X)$ defined on a normal and irreducible analytic surface X whose embedding dimension equals d is a sum of p squares of meromorphic functions on X. Slightly later, Acquistapace, Broglia, Fernando and Ruiz improved in [ABFR1] the above result and they showed that $p \leq 5$. Although the proof is only supplied for normal surfaces it is also valid for coherent surfaces.

Hilbert's 17th Problem for the ring $\mathcal{O}(X)$, that is, without denominators, was succesfully approached by Fernando in [F3] for global analytic sets X with dimension ≤ 2 and whose embedding dimension is ≤ 3, without any extra condition. In this work the notions of *analytic germ with the extension property* and *analytic subset of* $\mathbb{R}^n$ *with the extension property* are introduced. It is said that an analytic germ $X_0 \subset \mathbb{R}^n_0$ enjoys the extension property if each positive semidefinite analytic germ

in $\mathcal{O}(X_0)$ is the restriction to X_0 of a positive semidefinite analytic germ in $\mathcal{O}(\mathbb{R}^n_0)$. Analogously, a global analytic subset $X \subset \mathbb{R}^n$ enjoys the extension property if each positive semidefinite function in $\mathcal{O}(X)$ is the restriction to X of a positive semidefinite function in $\mathcal{O}(\mathbb{R}^n)$. It is proved that a global analytic subset X of dimension ≤ 2 whose embedding dimension is ≤ 3 enjoys the extension property if and only if it is coherent and all germs X_x with $x \in X$ enjoy the extension property too. In such a case it is proved that every positive semidefinite analytic function in $\mathcal{O}(X)$ is a sum of squares in $\mathcal{O}(X)$.

It is recognized that **H17** is a harder problem for global analytic sets with $\dim(X) \geq 3$. The best result for $\dim(X) = 3$ appears in [F4], where it is proved that the obstruction for a positive semidefinite analytic function $f : \mathbb{R}^3 \to \mathbb{R}$ to be a sum of squares of meromorphic functions lies in those invariant factors of f whose zero-set is a curve, and on the existence of a common upper bound of the number of squares needed to represent each of such factors as a sum of squares. In fact, this result has been extended and deeply improved to the n-dimensional case by Acquistapace, Broglia and Fernando in [ABF2], where the authors focus the obstruction to solve **H17** for $\mathbb{R}^n$ in the analytic case in the invariant factors whose zero-set has dimension $1 \leq d \leq n-2$ and, again, on the existence of a common upper bound of the number of squares needed to represent each of such factors as a sum of squares. The proof requieres a previous work, which has its own interest, where the authors present "infinite" multiplicative formulae for countable collections of sums of squares (of meromorphic functions on $\mathbb{R}^n$) generalizing the classical Pfister's ones concerning the representation as a sum of 2^r squares of the product of two elements of a field which are sums of 2^r squares.

As the previous paragraph suggests, in this context also "strongly convergent" infinite sums of squares are admitted, and some conditions are obtained that guarantee the finiteness of the number of summands. It is worthwhile mentioning that Acquistapace, Broglia, Fernando and Ruiz proved in [ABFR3] that an affirmative answer to **H17** in this context implies the existence of a universal bound on the number of summands needed to express any positive semidefinite analytic function $f : \mathbb{R}^n \to \mathbb{R}$ as a sum of squares of meromorphic functions.

To finish this concise review of some milestones on the Real Algebra of rings of analytic functions, let us mention those concerning the Real Nullstellensatz and the Positivstellensätze. Ruiz proved in [Rz3] that given a basic closed semianalytic set $S := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$, where $g_1, \ldots, g_m \in \mathcal{O}(\mathbb{R}^n)$, and $f \in \mathcal{O}(\mathbb{R}^n)$ such that $S \cap \mathcal{Z}(f)$ is compact, then $f|_S \equiv 0$ if and only if there exists an integer $k \geq 0$ and sums of squares $\sigma_\nu \in \Sigma\mathcal{O}(\mathbb{R}^n)^2$ such that

$$\sum_{\nu=(\nu_1,\ldots,\nu_m)} \sigma_\nu g_1^{\nu_1} \cdots g_m^{\nu_m} + f^{2k} = 0. \tag{4.4}$$

In [ABF1], Acquistapace, Broglia and Fernando proved that the compactness of the intersection $S \cap \mathcal{Z}(f)$ is a necessary condition in the precedent result. Indeed, choose $f, g \in \mathcal{O}(\mathbb{R})$ satisfying $\mathcal{Z}(f) = \mathcal{Z}(g) = \{n \in \mathbb{Z} : n > 0\}$. Suppose that the initial forms of the germs f_n and g_n at each positive integer n are, respectively, $(-1)^n(\mathtt{t} - n)$ and $(-1)^n(\mathtt{t} - n)^{2n-1}$. Moreover, f vanishes identically on the set $S = \{t \in \mathbb{R} : -f(t) \geq 0,\ g(t) \geq 0\}$. Thus, if the equality (4.4) holds there would exist sums of squares $\sigma_{00}, \sigma_{10}, \sigma_{01}$ and σ_{11} in $\mathcal{O}(\mathbb{R})$ and an integer $k \geq 0$ such that

$$\sigma_{00} - \sigma_{10} f + \sigma_{01} g - \sigma_{11} f g + f^{2k} = 0 \quad \Longrightarrow \quad (\sigma_{10} + g\sigma_{11}) f = \sigma_{00} + \sigma_{01} g + f^{2k}. \tag{4.5}$$

Let $\omega(h)$ denote the order at $k+1$ of each series $h \in \mathbb{R}\{\mathtt{t}\}$. Then, comparing the orders at the point $k+1$ of both members in equality (4.5), it follows that

$$\min\{\omega(\sigma_{10})+1, \omega(\sigma_{11})+2k+2\} = \min\{2k, \omega(\sigma_{00}), \omega(\sigma_{01})+2k+1\} = \min\{2k, \omega(\sigma_{00})\}.$$

The order of a sum of squares is even, and so the order of the left-hand member is, either odd, or $\geq 2k+2$, while the order of the right-hand side is even and $\leq 2k$, a contradiction.

Consequently, there is no hope to obtain in this case the counterpart of the analogous result in either the polynomial or global analytic with compact data settings. In [ABF1] the authors present alternative statements that provide a Positivstellensatz for global analytic functions that involves infinite sums of squares and/or positive semidefinite analytic functions. In particular the result is fully satisfactory for analytic curves, normal analytic surfaces and coherent analytic sets whose connected components are compact. Some years before, Acquistapace, Andradas and Broglia obtained in [AAB1] another result which can be considered a Positivstellensatz: given analytic functions $f, g_1, \ldots, g_m \in \mathcal{O}(\mathbb{R}^n)$ such that f is strictly positive on the set $S := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$, there exist strictly positive analytic functions $h_0, \ldots, h_m \in \mathcal{O}(\mathbb{R}^n)$ such that

$$f = h_0^2 + \sum_{j=1}^{m} h_j^2 g_j.$$

The nice relationship, with suitable modifications, between the real and complex analytic cases is illustrated in the forthcoming article [ABF3]. Extending to the real framework some fruitful ideas of Forster, [F], Siu, [Si] and De Bartolomeis, [dB], the authors state a Real Nullstellensatz for the ring $\mathcal{O}(X)$ of analytic functions on a global analytic set $X \subset \mathbb{R}^n$ in terms of the closure (in the Frechet topology of $\mathcal{O}(X)$) of the Łojasiewicz's radical ideal. Namely, given an ideal $\mathfrak{a} \subset \mathcal{O}(X)$, the ideal $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ of the zero-set $\mathcal{Z}(\mathfrak{a})$ of $\mathfrak{a}$ coincides with the closure $\overline{\sqrt[\text{Ł}]{\mathfrak{a}}}$ of the Łojasiewicz's ideal

$$\sqrt[\text{Ł}]{\mathfrak{a}} := \{g \in \mathcal{O}(X) :\ \exists\, f \in \mathfrak{a}\ \&\ m \geq 1 \text{ such that } f - g^{2m} \geq 0\}$$

of $\mathfrak{a}$. Moreover, if the zero-set $\mathcal{Z}(\mathfrak{a})$ of $\mathfrak{a}$ has "good properties" then, $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \overline{\sqrt[r]{\mathfrak{a}}}$, where $\sqrt[r]{\mathfrak{a}}$ stands for the real radical ideal of $\mathfrak{a}$, and the same holds if $\sqrt[r]{\mathfrak{a}}$ is replaced by the *real analytic radical ideal* $\sqrt[ra]{\mathfrak{a}}$, which is a natural generalization of the real radical ideal in the global analytic setting.

On the other hand it must be pointed out that a Łojasiewicz's inequality for analytic functions, analogous to the one stated in Lemma 4.12, and proved by Acquistapace, Broglia and Shiota in [ABS], constitutes a main ingredient in the proof of the analytic Real Nullstellensatz. In fact, this viewpoint has strongly inspired the approach developed in these notes.

(4.18.3) **Rings of Nash functions.** (1) A subset $M \subset \mathbb{R}^n$ is *semialgebraic* if it admits a representation

$$M := \bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \{x \in \mathbb{R}^n : f_{ij} \varepsilon_{ij} 0\} \tag{4.6}$$

where each $f_{ij} \in \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ and for each $1 \leq i \leq s$ and $1 \leq j \leq r_i$, the symbol ε_{ij} denotes $<$ or $=$.

(2) Let $U \subset \mathbb{R}^n$ be an open semialgebraic set. An analytic function $g : U \to \mathbb{R}$ is said to be *a Nash function* if its graph is a semialgebraic subset of $\mathbb{R}^{n+1}$.

(3) An analytic diffeomorphism $\varphi : U \to V$, $x \mapsto (\varphi_1(x), \ldots, \varphi_n(x))$, where U and V are open semialgebraic subsets of $\mathbb{R}^n$, is a *Nash diffeomorphism* if each $\varphi_j : U \to \mathbb{R}$ is a Nash function.

(4) A semialgebraic subset $X \subset \mathbb{R}^n$ is a *Nash submanifold* of $\mathbb{R}^n$ of dimension $d \geq 0$ if for each $x \in X$ there exist open semialgebraic subsets $U, V \subset \mathbb{R}^n$ such that $0 \in U$ and $x \in V$, and a Nash diffeomorphism $\varphi : U \to V$ with $\varphi(0) = x$ and $\varphi((\mathbb{R}^d \times \{0\}) \cap U) = X \cap V$.

(5) A function $f : X \to \mathbb{R}$, where X is a Nash submanifold, is a *Nash function* if, with the notations in (4), each composition $f \circ (\varphi|_{\mathbb{R}^d \times \{0\}})$ is a Nash function. The set $\mathcal{N}(X)$ of Nash functions on X constitutes a ring with the sum and product defined pointwise, and it is an integral domain if and only if X is connected. It makes sense to study for the ring $\mathcal{N}(X)$ the problems we have studied in the polynomial case and whose main advances for analytic functions and germ functions have been described above.

The article [Mo] by Mostowski contains the Nullstellensatz and a positive answer to **H17** for the ring $\mathcal{N}(X)$, although some proofs are not complete. Complete proofs where provided by Efroymson, [E1] and [E2]; the first of these articles contains a proof of the noetherianity of $\mathcal{N}(X)$. It is worthwhile mentioning the excellence of the presentation and the transparence and elegance of the involved arguments of the work by Bochnak and Efroymson [BE]. The Positivstellensätze appear in the

book [BCR] by Bochnak, Coste and Roy. More generally, **H17**, the Nullstellensatz and the Positivstellensätze can be approached for the ring of Nash functions on a semialgebraic set S, and in [FG] the authors characterize those semialgebraic sets for which the previous questions have a solution. As a consequence, the analogous results for germs of Nash functions can be derived, although there exists an alternative presentation, just for germs, due to Ruiz [Rz1].

(4.18.4) **Rings of differentiable functions.** The Nullstellensatz and the affirmative solution to **H17** for the ring of germs of differentiable functions are due to Lassalle, [Ls]. In the global setting, Bochnak obtained in [Bo] a Nullstellensatz for the ring $\mathcal{C}^\infty(X)$ of functions of class $\mathcal{C}^\infty$ on an analytic manifold. More precisely, given an ideal $\mathfrak{a}$ of $\mathcal{C}^\infty(X)$ generated by a finite set of analytic functions on X, we denote $\mathfrak{a}_a$ the extended ideal to the ring $\mathcal{O}_a$ of germs of analytic functions at the point $a \in X$, and it is said that $a \in \mathcal{Z}(\mathfrak{a})$ is a *regular point* if the quotient ring $\mathcal{O}_a/\mathfrak{a}_a$ is local regular; otherwise it is said that a is a *singular point*. In this last case S_a denotes the germ at a of the set of singular points of $\mathcal{Z}(\mathfrak{a})$, and $\Sigma_a := \{g \in \mathcal{O}_a : g^{-1}(0) \subset S_a\}$. Bochnak proved the equivalence of the following statements:

(i) $\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$;

(ii) $\mathfrak{a} = \sqrt[r]{\mathfrak{a}}$;

(iii) The set of regular points of $\mathcal{Z}(\mathfrak{a})$ is dense in $\mathcal{Z}(\mathfrak{a})$ and for every singular point $a \in \mathcal{Z}(\mathfrak{a})$ and every germ $f \in \Sigma_a$, the class $f + \mathfrak{a}_a$ is not a zero divisor in the quotient ring $\mathcal{O}_a/\mathfrak{a}_a$.

Later on Risler proved in [Ri2] the following result, conjectured by Bochnak: given a principal ideal $\mathfrak{a}$ of $\mathcal{C}^\infty(\mathbb{R}^2)$, the equality $\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ holds if and only if $\mathfrak{a}$ is a real ideal and it is closed in $\mathcal{C}^\infty(\mathbb{R}^2)$ with its compact-open topology.

Hilbert's 17th Problem admits a very simple solution for $\mathcal{C}^r$ functions defined on a differentiable manifold X of class $\mathcal{C}^r$ for $0 \leq r \leq \infty$. In fact, Acquistapace, Andradas and Broglia proved in [AAB2] that for every positive semidefinite $f \in \mathcal{C}^r(X)$ there exist $g, h \in \mathcal{C}^r(X)$ such that $g^2 f = h^2$. The proof is elementary; it suffices to consider the auxiliary function

$$u : (0, +\infty) \to (0, +\infty),\ t \mapsto \begin{cases} \sqrt{t \exp(-1/t)} & \text{if } t \neq 0 \\ 0 & \text{if } t = 0 \end{cases}$$

and the functions $g := \sqrt{\exp(-1/f)}$ and $h := u \circ f$ satisfy the required equality. In the same article the authors prove that, in general, f is not a sum of squares in $\mathcal{C}^r(X)$. Even more, given $S := \{x \in X : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\} \neq \varnothing$ for some $g_1, \ldots, g_m \in \mathcal{C}^r(X)$, and $f \in \mathcal{C}^r(X)$, the following properties hold:

(1) If $f(x) \geq 0$ for every point $x \in S$, then there exist $h, u_0, \ldots, u_m \in \mathcal{C}^r(X) \setminus \{0\}$ with

$$h^2 f = u_0^2 + \sum_{j=1}^{m} u_j^2 f_j \quad \& \quad \mathcal{Z}(h) \subset \mathcal{Z}(f).$$

(2) If $f(x) > 0$ for every point $x \in S$, then there exist $u_0, \ldots, u_m \in \mathcal{C}^r(X) \setminus \{0\}$ with

$$f = u_0^2 + \sum_{j=1}^{m} u_j^2 f_j.$$

For further readings we also recommend the reader the article [BBCP] by Bony, Broglia, Colombini and Pernazza, where the authors approach **H17** in some distinguished classes of differentiable functions. Without enter into subtleties we point out that the authors prove that for $n \geq 4$ there exist positive semidefinite $\mathcal{C}^\infty$-functions $f : \mathbb{R}^n \to \mathbb{R}$ (and even flat ones if $n \geq 5$) which are not a finite sum of squares of $\mathcal{C}^2$-functions. For $n = 1$, where a representation as a sum of squares always exists, the authors prove that if f vanishes at all its local minima, then there exists a $\mathcal{C}^2$-function g such that $f = g^2$, but that one cannot require g to enjoy any additional regularity condition.

CHAPTER III

Spectral spaces

1 Zariski spectrum of a ring

As in the precedent chapters, all rings are commutative with unit. Our goal in this first section is to recall the main properties of the Zariski spectrum of a ring. For us, a topological space is said to be *compact* if each open covering admits a finite subcovering; thus a space could be compact but not Hausdorff. Given a subset Y of a topological space X we will denote $\mathrm{Cl}_X(Y)$, or just $\mathrm{Cl}(Y)$ if no confusion is possible, the smallest closed subset of X containing Y.

Definitions 1.1 (Zariski spectrum and topology) (1) In what follows $\mathrm{Spec}(A)$ denotes the set of all prime ideals of A. This space is called *prime spectrum* or *Zariski spectrum* of A, and it is usually endowed with a topology known as *Zariski topology,* having as a basis of open subsets the one constituted by those sets of the type

$$D(a) := \{\mathfrak{p} \in \mathrm{Spec}(A) : \ a \notin \mathfrak{p}\}, \quad \forall\, a \in A,$$

which are called *basic open.* Notice that given $a, b \in A$ we have

$$D(0) = \varnothing, \quad D(1) = \mathrm{Spec}(A) \quad \& \quad D(a) \cap D(b) = D(ab).$$

For every subset $X \subset A$ we denote

$$V(X) := \{\mathfrak{p} \in \mathrm{Spec}(A) : \ X \subset \mathfrak{p}\} = \mathrm{Spec}(A) \setminus \bigcup_{a \in X} D(a),$$

which is a closed subset of $\mathrm{Spec}(A)$. Conversely, the complementary of a given closed subset $C \subset \mathrm{Spec}(A)$ is a union of basic open subsets, that is, there exists $X \subset A$ such that

$$\mathrm{Spec}(A) \setminus C = \bigcup_{a \in X} D(a) \quad \Longrightarrow \quad C = V(X).$$

On the other hand, if a prime ideal $\mathfrak{p}$ of A contains a subset $X \subset A$ then it contains the smallest ideal $\mathfrak{a}_X$ of A containing X. Thus $V(X) = V(\mathfrak{a}_X)$, and so admitting

$A = (1)$ as a non proper ideal of A, the family of closed subsets of $\mathrm{Spec}(A)$ in the Zariski topology is

$$\mathcal{C} := \{V(\mathfrak{a}) : \ \mathfrak{a} \text{ is an ideal of } A\}.$$

To simplify the notation we denote $V(a) := V(aA) = \mathrm{Spec}(A) \setminus D(a)$ for every $a \in A$. Notice that $V(a) = V(a^m)$ for each positive integer m, because a prime ideal $\mathfrak{p}$ contains a^m if and only if $a \in \mathfrak{p}$.

(2) It is evident that if $X \subset Y \subset A$, then $V(Y) \subset V(X)$.

(3) Recall, see [AM], that for every ideal $\mathfrak{a}$ of a ring A the equality

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}.$$

holds. Thus, an element $a \in A$ satisfies $V(\mathfrak{a}) \subset V(a)$ if and only if $a \in \sqrt{\mathfrak{a}}$.

(4) If for each prime ideal $\mathfrak{p}$ of A we denote $C_{\mathfrak{p}}$ an algebraic closure of the quotient field $\kappa(\mathfrak{p}) = \mathrm{qf}(A/\mathfrak{p})$, each element $a \in A$ can be seen as a function

$$a : \mathrm{Spec}(A) \to \bigsqcup_{\mathfrak{p} \in \mathrm{Spec}(A)} C_{\mathfrak{p}},\ \mathfrak{p} \mapsto a(\mathfrak{p}) := a + \mathfrak{p} \in \kappa(\mathfrak{p}) \subset C_{\mathfrak{p}}.$$

Proposition 1.2 (Compactness) (1) *Let A be a ring and $a \in A$. Then, the subset $D(a)$ of* $\mathrm{Spec}(A)$ *is compact.*

(2) *For every ideal $\mathfrak{a}$ of A the subset $V(\mathfrak{a})$ is compact.*

Proof. (1) Let $\{U_i\}_{i \in I}$ be an open covering of $D(a)$, that is, each U_i is an open subset of $\mathrm{Spec}(A)$ and $D(a) \subset \bigcup_{i \in I} U_i$. We may assume that $U_i = D(a_i)$ for some $a_i \in A$, and so

$$\bigcap_{i \in I} V(a_i) = \bigcap_{i \in I} \mathrm{Spec}(A) \setminus D(a_i) = \mathrm{Spec}(A) \setminus \bigcup_{i \in I} D(a_i) \subset \mathrm{Spec}(A) \setminus D(a) = V(a).$$

Let us denote $\mathfrak{a}$ the ideal of A generated by the elements $\{a_i : i \in I\}$. Thus $V(\mathfrak{a}) = \bigcap_{i \in I} V(a_i)$, hence $V(\mathfrak{a}) \subset V(a)$. This implies, by 1.1 (3), that $a \in \sqrt{\mathfrak{a}}$, that is, there exist a positive integer m, indices $i_1, \ldots, i_s \in I$ and elements $f_{i_1}, \ldots, f_{i_s} \in A$ such that

$$a^m = f_{i_1} a_{i_1} + \cdots + f_{i_s} a_{i_s}.$$

The ideal $\mathfrak{b} := (a_{i_1}, \ldots, a_{i_s})A$ satisfies $a \in \sqrt{\mathfrak{b}}$, and so $\bigcap_{j=1}^{s} V(a_{i_j}) = V(\mathfrak{b}) \subset V(a)$. Thus

$$D(a) \subset \mathrm{Spec}(A) \setminus \bigcap_{j=1}^{s} V(a_{i_j}) = \bigcup_{j=1}^{s} (\mathrm{Spec}(A) \setminus V(a_{i_j})) = \bigcup_{j=1}^{s} D(a_{i_j}) = \bigcup_{j=1}^{s} U_{i_j},$$

which implies that $D(a)$ is compact.

(2) From part (1), $\mathrm{Spec}(A) = D(1)$ is compact; thus its closed subset $V(\mathfrak{a})$ is compact too. □

Remarks 1.3 (1) Observe that the compactness of $D(a)$ follows from the fact that the operations of the ring $(A, +, \cdot)$ involve finitely many elements.

(2) In general, the Zariski spectrum of a ring is not a Hausdorff space, but we will see right now that it is a T_0-space.

Lemma 1.4 *Let A be a ring and $\mathfrak{p} \in \mathrm{Spec}(A)$. Then:*

(1) $\mathrm{Cl}(\{\mathfrak{p}\}) = V(\mathfrak{p})$. *In other words, $\mathfrak{q} \in \mathrm{Cl}(\{\mathfrak{p}\})$ if and only if $\mathfrak{p} \subset \mathfrak{q}$.*

(2) *The singleton $\{\mathfrak{p}\}$ is a closed subset of $\mathrm{Spec}(A)$ if and only if $\mathfrak{p}$ is a maximal ideal of the ring A.*

(3) *The Zariski spectrum $\mathrm{Spec}(A)$ is a T_0-space.*

Proof. (1) Since $V(\mathfrak{p})$ is a closed subset of $\mathrm{Spec}(A)$ containing $\mathfrak{p}$ it contains $\mathrm{Cl}(\{\mathfrak{p}\})$. Conversely, $\mathfrak{p} \subset \mathfrak{q}$ for each $\mathfrak{q} \in V(\mathfrak{p})$, that is, $A \setminus \mathfrak{q} \subset A \setminus \mathfrak{p}$. Thus, $\mathfrak{p} \in D(a)$ for each $a \in A \setminus \mathfrak{q}$ or, equivalently, each basic open neighborhood of $\mathfrak{q}$ intersects $\{\mathfrak{p}\}$, that is, $\mathfrak{q} \in \mathrm{Cl}(\{\mathfrak{p}\})$.

(2) By part (1), $\{\mathfrak{p}\}$ is a closed subset if and only if $\{\mathfrak{p}\} = V(\mathfrak{p})$, that is, $\mathfrak{p}$ is the unique prime ideal of A containing $\mathfrak{p}$. Thus $\mathfrak{p}$ is a maximal ideal of A.

(3) Given two different prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of A we may assume that $\mathfrak{p} \not\subset \mathfrak{q}$. By part (1) this means that $\mathfrak{q} \notin V(\mathfrak{p}) = \mathrm{Cl}(\{\mathfrak{p}\})$, and so $\mathrm{Spec}(A)$ is a T_0-space. □

Exercise 1.5 Draw the Zariski spectrum of the rings $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}[\mathtt{t}]$ and $\mathbb{C}[\mathtt{t}]$.

Ring homomorphisms induce continuous maps between the corresponding Zariski spectra. The next proposition collects basic properties of this functorial construction.

Proposition 1.6 (Morphisms between Zariski spectra) *Let $\varphi : A \to B$ be a ring homomorphism and*

$$\mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A), \ \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}).$$

Then, the following properties hold:

(1) $\mathrm{Spec}(\varphi)^{-1}(D(a)) = D(\varphi(a))$ *for every* $a \in A$. *Thus* $\mathrm{Spec}(\varphi)$ *is a continuous map.*

(2) $\mathrm{Spec}(\psi \circ \varphi) = \mathrm{Spec}(\varphi) \circ \mathrm{Spec}(\psi)$ *for each ring homomorphism* $\psi : B \to C$.

Proof. (1) Note that $\mathfrak{p} \in \mathrm{Spec}(\varphi)^{-1}(D(a))$ if and only if $\varphi^{-1}(\mathfrak{p}) = \mathrm{Spec}(\varphi)$ belongs to $D(a)$, that is, $a \notin \varphi^{-1}(\mathfrak{p})$, for each $\mathfrak{p} \in \mathrm{Spec}(A)$. This means that $\varphi(a) \notin \mathfrak{p}$, which is the same as $\mathfrak{p} \in D(\varphi(a))$.

(2) For every $\mathfrak{p} \in \mathrm{Spec}(C)$, we have

$$\mathrm{Spec}(\psi \circ \varphi)(\mathfrak{p}) = (\psi \circ \varphi)^{-1}(\mathfrak{p}) = \varphi^{-1}(\psi^{-1}(\mathfrak{p})) = (\mathrm{Spec}(\varphi) \circ \mathrm{Spec}(\psi))(\mathfrak{p}),$$

as wanted. □

Exercise 1.7 (1) Let $\varphi : A \to B$ be a ring epimorphism and $\mathfrak{a} := \ker \varphi$. Prove that $V(\mathfrak{a})$ is the image of the map $\mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$, and that

$$\mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to V(\mathfrak{a})$$

is a homeomorphism.

(2) Let $\mathfrak{a} := \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)}$ be the nilradical of A and $\pi : A \to A/\mathfrak{a}$, $f \mapsto f + \mathfrak{a}$. Prove that the induced map

$$\mathrm{Spec}(\pi) : \mathrm{Spec}(A/\mathfrak{a}) \to \mathrm{Spec}(A)$$

is a homeomorphism.

Exercise 1.8 Let A be a ring. An element $a \in A$ is said to be *idempotent* if $a^2 = a$.

(1) Prove that $\mathrm{Spec}(A)$ is connected if and only if the unique idempotent elements of A are $a = 0$ and $a = 1$.

(2) Prove that the Zariski spectrum of a local ring is connected.

(3) Let X be a topological space and let $\mathcal{C}(X)$ be the ring of continuous $\mathbb{R}$-valued functions on X. Prove that X is connected if and only if the Zariski spectrum of $\mathcal{C}(X)$ is connected.

Example 1.9 Let A be a ring, $f \in A \setminus (0)$ and let $A_f := \{a/f^m : a \in A, m \geq 0\}$. Consider the ring homomorphism $\varphi : A \to A_f$, $a \mapsto a/1$. From the general theory of localization it is known that a subset $\mathfrak{P} \subset A_f$ is a prime ideal of A_f if and only if there exists a prime ideal $\mathfrak{p}$ of A such that $f \notin \mathfrak{p}$ and $\mathfrak{P} = \mathfrak{p}A_f$.

In this way, the map $\mathrm{Spec}(\varphi) : \mathrm{Spec}(A_f) \to D(f)$ is bijective and continuous. In fact it is a homeomorphism. To check this last it is enough to observe that $\mathrm{Spec}(\varphi)(\mathfrak{p}A_f) = \mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of A such that $f \in A \setminus \mathfrak{p}$, and so given $a \in A$ and an integer $m \geq 0$,

$$\mathrm{Spec}(\varphi)(D(a/f^m)) = D(a) \cap D(f).$$

Thus $\mathrm{Spec}(\varphi)$ is an *open* map, that is, it maps open subsets of $\mathrm{Spec}(A_f)$ onto open subsets of $D(f)$. In particular, the compactness of $\mathrm{Spec}(A_f)$ implies the compactness of $D(f)$.

Exercise 1.10 (1) Let A be a ring, $a \in A$ and let $\mathfrak{b}$ be an ideal of A. Prove that

$$B(a, \mathfrak{b}) := \{\mathfrak{p} \in \mathrm{Spec}(A) : \ a \notin \mathfrak{p}, \ \mathfrak{b} \subset \mathfrak{p}\}$$

is a compact subset of $\mathrm{Spec}(A)$.

(2) Let $\mathcal{F} := \{D(a) : a \in A\}$. A set $C \subset \mathrm{Spec}(A)$ is *constructible* if it can be expressed as a finite combination of boolean operations (finite union, finite intersection and complementary) applied to sets of the family $\mathcal{F}$. Prove that each constructible set can be represented as a finite union of sets of type $B(a, \mathfrak{b})$. Deduce that each constructible subset of $\mathrm{Spec}(A)$ is compact.

Exercise 1.11 (1) A topological space is said to be *irreducible* if every non-empty open subset is dense. Prove that $\mathrm{Spec}(A)$ is irreducible if and only if the nilradical of A is a prime ideal.

(2) Let Y be an irreducible subset of a topological space X. Prove that its closure $\mathrm{Cl}_X(Y)$ is irreducible too.

(3) Prove that every irreducible subspace of a topological space is contained in a maximal irreducible subspace. Prove that the maximal irreducible subspaces of a topological space X, which are called the *irreducible components* of X, are closed subsets of X.

(4) Prove that given a ring A, the irreducible components of $\mathrm{Spec}(A)$ are the sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A.

Definition and Remarks 1.12 (Maximal spectrum) Let us fix a ring A.

(1) The *maximal spectrum* of A is the subset $\mathrm{Spec}_{\max}(A)$ of $\mathrm{Spec}(A)$ whose points are the maximal ideals of A. By Lemma 1.4 (2) the points in $\mathrm{Spec}_{\max}(A)$ are, exactly, the closed points of $\mathrm{Spec}(A)$. In general, the maximal spectrum does not enjoy the nice functorial properties of Zariski spectrum, because the preimage by a ring homomorphism of a maximal ideal is not, in general, a maximal ideal. Consider, for

example, the inclusion map $\mathtt{j} : \mathbb{Z} \hookrightarrow \mathbb{Q}$; the zero ideal (0) is maximal in $\mathbb{Q}$ but it is not a maximal ideal of $\mathbb{Z}$. Thus, a ring homomorphism $\varphi : A \to B$ does not induce, in general, a continuous map $\mathrm{Spec}_{\mathrm{max}}(\varphi) : \mathrm{Spec}_{\mathrm{max}}(B) \to \mathrm{Spec}_{\mathrm{max}}(A)$.

(2) The maximal spectrum $\mathrm{Spec}_{\mathrm{max}}(A)$ is endowed with the topology induced by the Zariski topology of $\mathrm{Spec}(A)$; clearly it is a T_1-space, that is, each one of its points is a closed subset because, by Lemma 1.4, for every $\mathfrak{m} \in \mathrm{Spec}_{\mathrm{max}}(A)$ we have

$$\mathrm{Cl}_{\mathrm{Spec}_{\mathrm{max}}(A)}(\{\mathfrak{m}\}) = \mathrm{Cl}_{\mathrm{Spec}(A)}(\{\mathfrak{m}\}) \cap \mathrm{Spec}_{\mathrm{max}}(A) = \{\mathfrak{m}\} \cap \mathrm{Spec}_{\mathrm{max}}(A) = \{\mathfrak{m}\}.$$

(3) In general $\mathrm{Spec}_{\mathrm{max}}(A)$ is not Hausdorff. Consider for instance the polynomial ring $A := \mathbb{C}[\mathtt{t}]$ and two distinct complex numbers a_1 and a_2. There are no open disjoint neighborhoods in $\mathrm{Spec}_{\mathrm{max}}(A)$ of the maximal ideals $\mathfrak{m}_1 := (\mathtt{t} - a_1)$ and $\mathfrak{m}_2 := (\mathtt{t} - a_2)$. Otherwise there would exist $f_1, f_2 \in A$ such that $\mathfrak{m}_i \in D(f_i)$ and $D(f_1) \cap D(f_2) \cap \mathrm{Spec}_{\mathrm{max}}(A) = \varnothing$. Hence $D(f_1 f_2) \cap \mathrm{Spec}_{\mathrm{max}}(A) = \varnothing$, that is, the product $f_1 f_2$ belongs to all maximal ideals $(\mathtt{t} - a)$ of A, that is, $(f_1 f_2)(a) = 0$ for every $a \in \mathbb{C}$, and so $f_1 f_2 = 0$. Since $\mathbb{C}[\mathtt{t}]$ is a domain we may assume that $f_1 = 0$, which implies $\mathfrak{m}_1 \in D(f_1) = \varnothing$, and this is false.

Proposition 1.13 *The maximal spectrum* $\mathrm{Spec}_{\mathrm{max}}(A)$ *of a ring* A *is a compact space.*

Proof. Let $\{U_i\}_{i \in I}$ be an open covering of $\mathrm{Spec}_{\mathrm{max}}(A)$. We may assume that each $U_i := D(a_i)$ for some $a_i \in A$, and so

$$\bigcap_{i \in I} V(a_i) = \bigcap_{i \in I} \mathrm{Spec}(A) \setminus D(a_i) = \mathrm{Spec}(A) \setminus \bigcup_{i \in I} D(a_i) \subset \mathrm{Spec}(A) \setminus \mathrm{Spec}_{\mathrm{max}}(A).$$

Hence, the ideal $\mathfrak{a}$ generated by $\{a_i : i \in I\}$ satisfies

$$V(\mathfrak{a}) = \bigcap_{i \in I} V(a_i) \subset \mathrm{Spec}(A) \setminus \mathrm{Spec}_{\mathrm{max}}(A).$$

Thus, there is no maximal ideal of A containing $\mathfrak{a}$ or, in other words, $\mathfrak{a} = A$. Hence, there exist indices $i_1, \ldots, i_s \in I$ and $b_1, \ldots, b_s \in A$ such that $1 = a_{i_1} b_1 + \cdots + a_{i_s} b_s$. Consequently, $\bigcap_{j=1}^{s} V(a_{i_j}) = \varnothing$, which implies

$$\mathrm{Spec}_{\mathrm{max}}(A) \subset \mathrm{Spec}(A) \setminus \bigcap_{j=1}^{s} V(a_{i_j}) = \bigcup_{j=1}^{s} \mathrm{Spec}(A) \setminus V(a_{i_j}) = \bigcup_{j=1}^{s} D(a_{i_j}) = \bigcup_{j=1}^{s} U_{i_j},$$

and so $\mathrm{Spec}_{\mathrm{max}}(A)$ is compact. □

Examples 1.14 (1) The maximal spectrum is not, in general, a closed subset of the Zariski spectrum. Consider, for example, $A := \mathbb{C}[\mathtt{t}]$, and suppose that $\mathrm{Spec}_{\max}(A)$ is a closed subset of $\mathrm{Spec}(A)$. Then, $\mathrm{Spec}_{\max}(A) = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of A. Since A is a PID there exists $f \in A$ such that $\mathfrak{a} := fA$, hence $V(f) = V(\mathfrak{a}) = \mathrm{Spec}_{\max}(A)$. Thus, $f \in (\mathtt{t} - a)$ for every $a \in \mathbb{C}$, and so $f = 0$. Hence $\mathrm{Spec}_{\max}(A) = \mathrm{Spec}(A)$, and this is false because (0) is a prime but not maximal ideal of A.

(2) Consider the complex field $\mathbb{C}$ endowed with the topology whose open subsets are those whose complementary is finite. Then, the bijection

$$\Phi : \mathbb{C} \to \mathrm{Spec}_{\max}(A),\ a \mapsto (\mathtt{t} - a)$$

is a homeomorphism. Indeed, to check the continuity, let $U := D(f) \cap \mathrm{Spec}_{\max}(A)$ be a non-empty basic open set. Then, $f \neq 0$ and so there exist complex numbers $a_0, \ldots, a_r \in \mathbb{C}$ and positive integers m_i such that $a_0 \neq 0$ and

$$f := a_0(\mathtt{t} - a_1)^{m_1} \cdots (\mathtt{t} - a_r)^{m_r}.$$

The maximal ideals of A containing f are, exactly, those of the form $\mathfrak{m}_i := (\mathtt{t} - a_i)$ for $1 \leq i \leq r$. Therefore the complementary of $\Phi^{-1}(U) = \mathbb{C} \setminus \{a_1, \ldots, a_r\}$ is finite, and so $\Phi^{-1}(U)$ is open. On the other hand, for every finite subset $\mathcal{F} := \{a_1, \ldots, a_r\} \subset \mathbb{C}$,

$$\begin{aligned}\Phi(\mathbb{C} \setminus \mathcal{F}) &= \mathrm{Spec}_{\max}(A) \setminus \Phi(\mathcal{F}) \\ &= \mathrm{Spec}_{\max}(A) \setminus \{(\mathtt{t} - a_1), \ldots, (\mathtt{t} - a_r)\} = D(g) \cap \mathrm{Spec}_{\max}(A),\end{aligned}$$

where $g(\mathtt{t}) := \prod_{j=1}^{r}(\mathtt{t} - a_j)$, and so $\Phi(\mathbb{C} \setminus \mathcal{F})$ is an open subset of $\mathrm{Spec}_{\max}(A)$.

(3) Consider the ring $A := \mathcal{C}([0,1])$ of continuous real valued functions defined in the closed interval $[0,1]$. The space $\mathrm{Spec}_{\max}(A)$ is homeomorphic to $[0,1]$ with its Euclidean topology.

To prove this, let us see first that the maximal ideals of A are those of the form

$$\mathfrak{m}_p := \{f \in A : f(p) = 0\} :\ p \in [0,1].$$

Indeed, for every $p \in [0,1]$ the ideal $\mathfrak{m}_p$ is maximal because it is the kernel of the epimorphism $\mathrm{ev}_p : A \to \mathbb{R}$, $f \mapsto f(p)$, and so $A/\ker \mathrm{ev}_p \cong \mathbb{R}$. Conversely, let $\mathfrak{m}$ be a maximal ideal of A. It is enough to show that there exists $p \in [0,1]$ such that $\mathfrak{m} \subset \mathfrak{m}_p$; once this be proved the maximality of $\mathfrak{m}$ implies that $\mathfrak{m} = \mathfrak{m}_p$. Indeed, if $\mathfrak{m} \not\subset \mathfrak{m}_p$ for all $p \in [0,1]$, there would exist functions $f_p \in \mathfrak{m}$ such that $f_p(p) \neq 0$. Since $U^p = f_p^{-1}(\mathbb{R} \setminus \{0\})$ is an open neighborhood of p in $[0,1]$, the family $\{U^p :\ p \in [0,1]\}$ is an open covering of the compact space $[0,1]$, and so there exists a finite subset $\mathcal{F} \subset [0,1]$ such that

$$[0,1] \subset \bigcup_{p \in \mathcal{F}} U^p.$$

This means that the function $f := \sum_{p\in\mathcal{F}} f_p^2 \in \mathfrak{m}$ does not vanish at any point of the interval $[0,1]$; thus $1/f \in A$ and $1 = f\cdot(1/f) \in \mathfrak{m}$, which is false. Consequently, the map

$$\Psi : [0,1] \to \mathrm{Spec}_{\max}(A),\ p \mapsto \mathfrak{m}_p$$

is a well defined surjection. Moreover, it is injective too because given distinct points $p, q \in [0,1]$, the continuous function $f : [0,1] \to \mathbb{R}$, $x \mapsto |x-p|$ vanishes at p, but not at q, and this implies $f \in \mathfrak{m}_p \setminus \mathfrak{m}_q$.

To finish, let us check that Ψ is a homeomorphism. First, let $f \in A$ and consider the basic open set $U := D(f) \cap \mathrm{Spec}_{\max}(A)$. Then,

$$\Psi^{-1}(U) = \{x \in [0,1] :\ f(x) \neq 0\}$$

is an open subset of $[0,1]$ because f is continuous. This proves that Ψ is continuous. Moreover, given an open subset W of $[0,1]$ then $M := [0,1] \setminus W$ is closed in $[0,1]$. Hence, $M = \{x \in [0,1] :\ g(x) = 0\}$, where $g := \mathrm{dist}(\cdot, M) : [0,1] \to \mathbb{R}$ is a continuous function. Thus, $\Psi(W) = D(g) \cap \mathrm{Spec}_{\max}(A)$ is an open subset in the Zariski topology of $\mathrm{Spec}_{\max}(A)$, and Ψ is a homeomorphism.

(4) In general, there exist basic open non-compact subsets of $\mathrm{Spec}_{\max}(A)$. Consider the ring $A := \mathcal{C}([0,1])$ and, for each point $p \in [0,1]$, let $h_p : [0,1] \to \mathbb{R}$, $x \mapsto x - p$. By part (3), $D(h_p) \cap \mathrm{Spec}_{\max}(A)$ is homeomorphic to $[0,1] \setminus \{p\}$ with its Euclidean topology, which is not compact.

(5) For some topological spaces X there exist many rings $\mathcal{F}(X)$ of functions defined on X such that each point in X is identified with a maximal ideal of $\mathcal{F}(X)$. This provides a *set theoretical inclusion* $\mathtt{j} : X \hookrightarrow \mathrm{Spec}_{\max}(\mathcal{F}(X))$. However, the behaviour of this inclusion from the topological viewpoint, when $\mathrm{Spec}_{\max}(\mathcal{F}(X))$ is endowed with the Zariski topology, could be rather different. In part (2) we have studied the case $X := \mathbb{C}$ and $\mathcal{F}(X)$ the ring of polynomial functions. We observed that the Zariski topology induces, via $\mathtt{j}$, the topology in $\mathbb{C}$ whose open subsets are those whose complementary is finite.

However, in part (3) the Zariski topology induces in $[0,1]$, via $\mathtt{j}$, the Euclidean topology. In next sections we will address some situations in which the maximal spectrum of $\mathcal{F}(X)$ coincides with the *maximal real spectrum,* see 2.8, and its Zariski topology induces the original topology in X. In such cases the maximal spectrum of $\mathcal{F}(X)$ is a compactification of X with reminiscences of the classical Stone-Cěch compactification. In any case, we do not make a deeper study of the Zariski spectrum in these notes, and we shall use it to introduce in the next section the *real spectrum of a ring,* whose elements are prime cones instead of prime ideals, and constitutes the abstract object whose role is relevant in Real Algebraic Geometry.

2 Real spectrum of a ring

Definitions 2.1 (Real spectrum and spectral topology) (1) The goal in this section is the study of the main properties of the *real spectrum* $\mathrm{Spec}_r(A)$ of a ring A, whose elements are the prime cones of A. In particular, if K is a real field, its real spectrum $\mathrm{Spec}_r(K)$ coincides with the set of all orderings in K. Notice that although the Zariski spectrum is non-empty for each ring A, it follows from Lemma 1.10 (Ch.II), that $\mathrm{Spec}_r(A)$ is non-empty if and only if $-1 \notin \Sigma A^2$.

According to the kind of problems to be approached the real spectrum is endowed with different topologies. In these notes we will be mainly concerned with its *spectral topology.* The subsets

$$U(a_1,\ldots,a_r) := \{\alpha \in \mathrm{Spec}_r(A) : -a_1 \notin \alpha,\ldots,-a_r \notin \alpha\} :\ a_1,\ldots,a_r \in A,$$

constitutes a basis of open subsets of the spectral topology of $\mathrm{Spec}_r(A)$. Given $a \in A$ and $\alpha \in \mathrm{Spec}_r(A)$ we denote $a(\alpha) := a + \mathfrak{p}_\alpha \in A/\mathfrak{p}_\alpha$. In this way, the notation $a(\alpha) = 0$ means that $a \in \mathfrak{p}_\alpha = \alpha \cap (-\alpha)$ while $a(\alpha) \geq 0$ means that $a + \mathfrak{p}_\alpha$ is nonnegative with respect to the ordering $\leq_\alpha$ induced by α in the quotient field $\kappa(\mathfrak{p}_\alpha) = \mathrm{qf}(A/\mathfrak{p}_\alpha)$, that is, $a(\alpha) \geq 0$ if and only if $a \in \alpha$.

Analogously, $a(\alpha) \leq 0$ means that $(-a)(\alpha) \geq 0$, that is, $a \in (-\alpha)$, while $a(\alpha) > 0$ if $a(\alpha) \geq 0$ but $a(\alpha) \neq 0$ or, equivalently, $-a \notin \alpha$, and $a(\alpha) < 0$ means that $a \notin \alpha$. With these notations,

$$U(a_1,\ldots,a_r) := \{\alpha \in \mathrm{Spec}_r(A) :\ a_1(\alpha) > 0,\ldots,a_r(\alpha) > 0\}.$$

The same idea of 1.1 (4) allows us to interpret the elements in A as functions on the real spectrum $\mathrm{Spec}_r(A)$. For each prime cone $\alpha := (\mathfrak{p}_\alpha, \leq_\alpha)$ in A let R_α be the real closure of the ordered field $(\kappa(\mathfrak{p}_\alpha), \leq_\alpha)$. Since $A/\mathfrak{p}_\alpha \subset \kappa(\mathfrak{p}_\alpha) \subset R_\alpha$, each element $a \in A$ can be seen as a function

$$a : \mathrm{Spec}_r(A) \to \bigsqcup_{\alpha \in \mathrm{Spec}_r(A)} R_\alpha,\ \alpha \mapsto a(\alpha) \in R_\alpha.$$

Exercise 2.2 A *cut* in an ordered field $(E, \leq)$ is an ordered pair (I, J) where I and J are subsets of E such that $E = I \cup J$, and $x < y$ for every pair of elements $x \in I$ and $y \in J$.

(1) Prove that for each ordering $\leq$ of the field $\mathbb{R}(\mathtt{t})$ the pair (I, J), where

$$I := \{x \in \mathbb{R} :\ x < \mathtt{t}\} \quad \& \quad J := \{x \in \mathbb{R} :\ x > \mathtt{t}\},$$

is a cut in $\mathbb{R}$. We will denote the cuts

$$-\infty := (\varnothing, \mathbb{R}), \quad a^- := ((-\infty, a),\ [a, +\infty)),$$
$$a^+ := ((-\infty, a],\ (a, +\infty)), \quad +\infty := (\mathbb{R}, \varnothing).$$

(2) Find a bijection between the orderings in $\mathbb{R}(\mathtt{t})$ and the cuts in $\mathbb{R}$.

Exercise 2.3 Draw the real spectra of the rings $\mathbb{Z}$, $\mathbb{R}[\mathtt{t}]$ and $\mathbb{R}(\mathtt{t})$. Compare this Exercise with Exercise 1.5.

Exercise 2.4 Let A be a real ring and consider the map

$$\mathrm{supp} : \mathrm{Spec}_r(A) \to \mathrm{Spec}(A),\ \alpha \mapsto \mathfrak{p}_\alpha = \alpha \cap (-\alpha).$$

(1) Prove that its image is the set of real prime ideals of A.

(2) Prove that $\mathrm{supp}^{-1}(D(a)) = U(a) \cup U(-a)$ for each $a \in A$. Deduce that supp is a continuous map where both spaces are endowed with the spectral topology.

Remarks 2.5 (1) Hochster characterized in [Ho] those topological spaces homeomorphic to Zariski spectra of rings with their spectral topology, and called them *spectral spaces*. The real spectrum of a real ring is a spectral space; in fact Schwartz associated in [Sch2] to every real ring A another real ring B such that $\mathrm{Spec}(B)$ is homeomorphic to $\mathrm{Spec}_r(A)$. The converse is not true: there exist many rings A whose Zariski spectrum is not a *normal space* and, however, we will prove in Proposition 2.25 that the real spectrum of a real ring is a normal space, that is, given two disjoint closed subsets C_1 and C_2 there exist open disjoint subsets G_1 and G_2 such that $C_i \subset G_i$.

Thus the non-normal spectral spaces are not homeomorphic to real spectra of real rings, and so, the structure "real spectrum" is more restrictive than the one of Zariski spectrum. This mainly obeys to two reasons; one of them is that only real prime ideals are the support of some prime cone. The second one, which is more important, relies on the fact that given a real prime ideal $\mathfrak{p}$ of the ring A the quotient field $\mathrm{qf}(A/\mathfrak{p})$ could admit many distinct orderings, which provide many prime cones (even infinitely many), with the same support $\mathfrak{p}$. This happens, for example, if $A := \mathbb{R}[\mathtt{t}]$ and $\mathfrak{p} = (0)$.

(2) If we denote $\mathbb{R}[\mathtt{x}] := \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, the real spectrum $\mathrm{Spec}_r(\mathbb{R}[\mathtt{x}])$ contains $\mathbb{R}^n$ via the injective map

$$\mathtt{j} : \mathbb{R}^n \hookrightarrow \mathrm{Spec}_r(\mathbb{R}[\mathtt{x}]),\ p \mapsto \alpha_p = \{f :\ f(p) \geq 0\}.$$

In contrast with what happens in Example 1.14 (2) with the complex line, the map $\mathtt{j}$ is a topological embedding of $\mathbb{R}^n$, endowed with its Euclidean topology, into $\mathrm{Spec}_r(\mathbb{R}[\mathtt{x}])$ endowed with its spectral topology. We will study this more in detail in Section §3 of this Chapter.

(3) For every real ring A and each ideal $\mathfrak{a}$ of A let us denote

$$\mathcal{Z}(\mathfrak{a}) := \{\alpha \in \mathrm{Spec}_r(A) :\ \mathfrak{a} \subset \mathfrak{p}_\alpha\} = \{\alpha \in \mathrm{Spec}_r(A) : f(\alpha) = 0 \quad \forall f \in \mathfrak{a}\}.$$

Then, for $A := \mathbb{R}[\mathtt{x}]$ the following equality holds:

$$\mathtt{j}^{-1}(\mathcal{Z}(\mathfrak{a})) = \mathcal{Z}(\mathfrak{a}) = \{x \in \mathbb{R}^n : f(x) = 0 \quad \forall f \in \mathfrak{a}\}.$$

(2.6) Chains of prime cones. Before proving some compactness properties of the real spectrum, we study first a specific property of the real spectrum which has no counterpart in the Zariski spectrum: the set of prime cones containing a given prime cone is a chain, that is, a totally ordered set with respect to inclusion. This guarantees that each prime cone is contained in a unique maximal prime cone.

Lemma 2.7 *Let A be a ring, α a prime cone in A and let $\mathcal{F}_\alpha$ be the collection of all prime cones of A containing α. Then, $\mathcal{F}_\alpha$ is a chain.*

Proof. Let $\beta, \gamma \in \mathcal{F}_\alpha$ and suppose, by way of contradiction, that $\beta \not\subset \gamma$ and $\gamma \not\subset \beta$. Then, there exist $b \in \beta \setminus \gamma$ and $c \in \gamma \setminus \beta$. Since $A = \alpha \cup (-\alpha)$, either $b - c \in \alpha$ or $c - b \in \alpha$. In the first case, $b = c + (b - c) \in \gamma$ (because $\alpha \subset \gamma$) and in the second one $c = b + (c - b) \in \beta$ (because $\alpha \subset \beta$); in both cases this is a contradiction. Therefore, $\mathcal{F}_\alpha$ is a chain. □

Remarks 2.8 (1) Fixed a prime cone α in A the union $\gamma := \bigcup_{\beta \in \mathcal{F}_\alpha} \beta$ is a prime cone. Thus, $\rho(\alpha) := \gamma$ is a maximal element of $\mathcal{F}_\alpha$. In particular α is contained in a unique maximal prime cone $\rho(\alpha)$. In fact, the checking of the conditions $\gamma + \gamma \subset \gamma$, $\gamma \cdot \gamma \subset \gamma$, $A^2 \subset \gamma$ and $-1 \notin \gamma$ is straightforward. Moreover, $\gamma \cup (-\gamma) = A$, because

$$A = \alpha \cup (-\alpha) \subset \gamma \cup (-\gamma) = A,$$

and so all reduces to see that $\mathfrak{p}_\gamma := \gamma \cap (-\gamma)$ is a prime ideal. Indeed, let $a, b \in A$ such that $ab \in \mathfrak{p}_\gamma$. Then, there exist $\beta_1, \beta_2 \in \mathcal{F}_\alpha$ such that $ab \in \beta_1$ and $ab \in (-\beta_2)$. By Lemma 2.7 we can suppose that $\beta_1 \subset \beta_2$, and consequently $ab \in \beta_2 \cap (-\beta_2) = \mathfrak{p}_{\beta_2}$. Since β_2 is a prime cone, we may assume that $a \in \mathfrak{p}_{\beta_2} \subset \mathfrak{p}_\gamma$, and therefore γ is a prime cone.

(2) In general, the maximality of a prime cone α does not imply the maximality of its support. Consider for instance the ordering $\leq$ in $\mathbb{R}(\mathtt{t})$ whose set of positive elements is

$$P_\leq := \{(a_n \mathtt{t}^n + \cdots + a_0)/(b_m \mathtt{t}^m + \cdots + b_0) \in \mathbb{R}(\mathtt{t}) : \ a_n b_m > 0\}.$$

The prime cone $\alpha := ((0), \leq)$ in $A := \mathbb{R}[\mathtt{t}]$ is maximal, but its support $\mathfrak{p}_\alpha = (0)$ is not a maximal ideal of A.

Exercise 2.9 Prove that the unique maximal prime cones in $\mathbb{R}[\mathtt{t}]$ whose support is not a maximal ideal are the prime cones whose support is (0) and whose associated orderings in $\mathbb{R}(\mathtt{t})$ are those corresponding to the cuts $-\infty$ and $+\infty$ of $\mathbb{R}$, (see Exercise 2.2).

Next, we characterize the supports of all prime cones containing a given prime cone. This requires to introduce two new notions.

Definition 2.10 Let P be a cone and let $\mathfrak{a}$ be an ideal of a ring A.

(1) It is said that $\mathfrak{a}$ is a *P-convex* ideal if whenever two elements $p, q \in P$ satisfy $p + q \in \mathfrak{a}$, then $p, q \in \mathfrak{a}$.

(2) The ideal $\mathfrak{a}$ is said to be *P-radical* if given $a \in A$ and $p \in P$ such that $a^2 + p \in \mathfrak{a}$ then $a \in \mathfrak{a}$.

Remarks 2.11 (1) An ideal $\mathfrak{a}$ is P-radical if and only if it is radical and P-convex.

Indeed, suppose first that $\mathfrak{a}$ is P-radical and let us see that $\mathfrak{a}$ is a radical ideal. If $a^m \in \mathfrak{a}$ for some positive integer m, then $a^{2^m} = a^m \cdot a^{2^m - m} \in \mathfrak{a}$. Let us prove, by induction on m, that $a \in \mathfrak{a}$. For $m = 1$ we have $a^2 + 0 = a^2 \in \mathfrak{a}$, and since $\mathfrak{a}$ is P-radical it follows that $a \in \mathfrak{a}$. For the inductive step, denote $b := a^{2^{m-1}}$, that satisfes $b^2 + 0 = a^{2^m} \in \mathfrak{a}$. Since $\mathfrak{a}$ is P-radical, $a^{2^{m-1}} = b \in \mathfrak{a}$ and, by induction, $a \in \mathfrak{a}$.

On the other hand, let $p, q \in P$ be such that $p+q \in \mathfrak{a}$; then, $p^2+pq = p(p+q) \in \mathfrak{a}$ and, $\mathfrak{a}$ being a P-radical ideal, $p \in \mathfrak{a}$. Consequently, also $q \in \mathfrak{a}$, that is, $\mathfrak{a}$ is a P-convex ideal.

Conversely, suppose that $\mathfrak{a}$ is a radical and P-convex ideal and let $a \in A$ and $p \in P$ such that $a^2 + p \in \mathfrak{a}$; its P-convexity implies, since $a^2 \in P$, that $a^2 \in \mathfrak{a}$ and, $\mathfrak{a}$ being a radical ideal, it follows that $a \in \mathfrak{a}$.

(2) Observe that if $P := \Sigma A^2$, an ideal $\mathfrak{a}$ of A is P-radical if and only if it is a real ideal.

(3) Let P be a cone and let $\mathfrak{a}$ be a P-convex ideal of A. Then, $P \cap (-P) \subset \mathfrak{a}$.

Indeed, if $a \in P \cap (-P)$ then $a, -a \in P$ and $a + (-a) = 0 \in \mathfrak{a}$. Since $\mathfrak{a}$ is a P-convex ideal it follows that $a \in \mathfrak{a}$, and so $P \cap (-P) \subset \mathfrak{a}$.

Lemma 2.12 *Let A be a real ring and $\alpha \in \mathrm{Spec}_r(A)$. Then, the* supp *map*

$$\mathrm{supp} : \mathcal{F}_\alpha := \{\beta \in \mathrm{Spec}_r(A) : \alpha \subset \beta\} \to \mathcal{G}_\alpha := \{\mathfrak{q} \in \mathrm{Spec}(A) : \mathfrak{q} \textit{ is } \alpha\textit{-convex}\}$$

defined by $\mathrm{supp}(\beta) = \mathfrak{p}_\beta$ *is bijective, and its inverse is the map* $\mathfrak{q} \mapsto \mathfrak{q} \cup \alpha$.

Proof. Let us see first that the map supp : $\mathcal{F}_\alpha \to \mathcal{G}_\alpha$ is well defined, that is, the ideal $\mathfrak{p}_\beta$ is α-convex for every $\beta \in \mathcal{F}_\alpha$. Let $a, b \in \alpha$ such that $a+b \in \mathfrak{p}_\beta$. Then, both $a, b \in \beta$ and $-(a+b) \in \beta$; thus

$$-a = -(a+b) + b \in \beta \quad \Longrightarrow \quad a \in \beta \cap (-\beta) = \mathfrak{p}_\beta,$$

and so $b = (a+b) - a \in \mathfrak{p}_\beta$.

Let us prove that if $\beta \in \mathcal{F}_\alpha$, then $\beta = \mathfrak{p}_\beta \cup \alpha$. The inclusion $\mathfrak{p}_\beta \cup \alpha \subset \beta$ is evident. Conversely, let $x \in \beta \backslash \mathfrak{p}_\beta$. Then, $x \in A \backslash (-\beta)$, that is, $-x \in A \backslash \beta$, and so $-x \in A \backslash \alpha$, which implies $x \in \alpha$. This proves the injectivity of the map supp : $\mathcal{F}_\alpha \to \mathcal{G}_\alpha$ because given $\beta_1, \beta_2 \in \mathcal{F}_\alpha$ such that $\mathfrak{p}_{\beta_1} = \mathfrak{p}_{\beta_2}$ then, $\beta_1 = \mathfrak{p}_{\beta_1} \cup \alpha = \mathfrak{p}_{\beta_2} \cup \alpha = \beta_2$. Hence, once the surjectivity of the map supp : $\mathcal{F}_\alpha \to \mathcal{G}_\alpha$ is proved, its inverse is given by the formula in the statement.

Let us see that the support map supp is surjective. Let $\mathfrak{q}$ be an α-convex prime ideal of A. By Remark 2.11 (3), $\mathfrak{p}_\alpha \subset \mathfrak{q}$. Define

$$\mathcal{F}_\mathfrak{q} := \{\beta \subset A : \ \beta \ \text{ is a cone, } \alpha \subset \beta \ \& \ \mathfrak{q} \text{ is } \beta\text{-convex}\},$$

which contains α, and so it is a non-empty set. Consider in $\mathcal{F}_\mathfrak{q}$ the order relation $\preceq$ defined by the inclusion and let us show that $(\mathcal{F}_\mathfrak{q}, \preceq)$ is an inductive ordered set. Given a chain $\mathcal{C}$ in $\mathcal{F}_\mathfrak{q}$ we are going to see that

$$\alpha_0 := \bigcup_{\beta \in \mathcal{C}} \beta$$

is an upper bound of $\mathcal{C}$ in $\mathcal{F}_\mathfrak{q}$; for that we must check that α_0 is a cone that contains α and that $\mathfrak{q}$ is an α_0-convex ideal. We omit the first part since we have repeated a similar argument along these notes. About the α_0-convexity of $\mathfrak{q}$, let $p, q \in \alpha_0$ such that $p+q \in \mathfrak{q}$. Let $\beta_1, \beta_2 \in \mathcal{C}$ such that $p \in \beta_1$ and $q \in \beta_2$. Since $\mathcal{C}$ is a chain we can suppose that $\beta_1 \subset \beta_2$. Hence $p, q \in \beta_2$ and, $\mathfrak{q}$ being β_2-convex, $p, q \in \mathfrak{q}$, and so $\mathfrak{q}$ is an α_0-convex ideal. By Zorn's Lemma, the family $\mathcal{F}_\mathfrak{q}$ has a maximal element, say γ.

Notice that γ is a proper cone; otherwise $1, -1 \in \gamma$ and $1+(-1) = 0 \in \mathfrak{q}$ and the γ-convexity of $\mathfrak{q}$ implies that $1 \in \mathfrak{q}$, a contradiction. Even more, γ is a prime cone and $\mathfrak{p}_\gamma = \mathfrak{q}$. Let us check first this equality. Since $\mathfrak{q}$ is a γ-convex ideal it follows from Remark 2.11 (3) that $\mathfrak{p}_\gamma = \gamma \cap (-\gamma) \subset \mathfrak{q}$. Conversely, we must prove that $\mathfrak{q} \subset \mathfrak{p}_\gamma$; to that end, let $a \in \mathfrak{q}$ and we have to show that $\varepsilon a \in \gamma$ for both $\varepsilon = \pm 1$. Consider the cone

$$\gamma[\varepsilon a] := \{p + q\varepsilon a : \ p, q \in \gamma\},$$

that contains γ, and so it contains α too. Let us see that $\mathcal{F}_\mathfrak{q}$ contains $\gamma[\varepsilon a]$, that is, $\mathfrak{q}$ is a $\gamma[\varepsilon a]$-convex ideal. Let $\rho_1, \rho_2 \in \gamma[\varepsilon a]$ be such that $\rho_1 + \rho_2 \in \mathfrak{q}$. Let us write

$\rho_i = p_i + q_i a\varepsilon$ for $i = 1, 2$, where $p_i, q_i \in \gamma$, and we have

$$(p_1 + p_2) + (q_1 + q_2)\varepsilon a = (p_1 + q_1\varepsilon a) + (p_2 + q_2\varepsilon a) = \rho_1 + \rho_2 \in \mathfrak{q}.$$

Since $(q_1 + q_2)\varepsilon a \in \mathfrak{q}$ we deduce that $p_1 + p_2 \in \mathfrak{q}$ and, $\mathfrak{q}$ being a γ-convex ideal, $p_1, p_2 \in \mathfrak{q}$, and this implies that $\rho_1, \rho_2 \in \mathfrak{q}$, which proves that $\mathfrak{q}$ is a $\gamma[\varepsilon a]$-convex ideal. Now, γ is a maximal element of $\mathcal{F}_\mathfrak{q}$ contained in $\gamma[\varepsilon a] \in \mathcal{F}_\mathfrak{q}$, that is, $\gamma = \gamma[\varepsilon a]$. Henceforth $\varepsilon a \in \gamma$, or equivalently, $a \in \gamma \cap (-\gamma) = \mathfrak{p}_\gamma$.

To finish, it is enough to prove that $\gamma \cup (-\gamma) = A$. In such a case γ would be a prime cone in A containing α whose support is $\mathfrak{q}$, which proves the surjectivity of $\mathrm{supp} : \mathcal{F}_\alpha \to \mathcal{G}_\alpha$. Suppose, by way of contradiction, the existence of an element $b \in A \setminus (\gamma \cup (-\gamma))$. This implies, with the notations above, that $\gamma \subsetneq \gamma[\varepsilon b]$ for $\varepsilon = \pm 1$ and, γ being maximal in $\mathcal{F}_\mathfrak{q}$, we have $\gamma[\varepsilon b] \notin \mathcal{F}_\mathfrak{q}$, that is, the ideal $\mathfrak{q}$ is not $\gamma[\varepsilon b]$-convex. It follows from Remark 2.11 (1) that $\mathfrak{q}$ is not a $\gamma[\varepsilon b]$-radical ideal for $\varepsilon = \pm 1$. This means that there exist $c_\varepsilon \in A$ and $p_\varepsilon, q_\varepsilon \in \gamma$ such that $c_\varepsilon \notin \mathfrak{q}$ but $c_\varepsilon^2 + p_\varepsilon + q_\varepsilon\varepsilon b \in \mathfrak{q}$. After multiplying we get

$$q_{-1}c_1^2 + q_{-1}p_1 + q_1c_{-1}^2 + q_1p_{-1} = q_{-1}(c_1^2 + p_1 + q_1 b) + q_1(c_{-1}^2 + p_{-1} + q_{-1}(-b)) \in \mathfrak{q},$$

and, $\mathfrak{q}$ being γ-convex, it contains $q_{-1}c_1^2, q_{-1}p_1, q_1c_{-1}^2$ and q_1p_{-1}. Since $c_1, c_{-1} \notin \mathfrak{q}$, each $q_\varepsilon \in \mathfrak{q}$. But $c_\varepsilon^2 + p_\varepsilon + q_\varepsilon\varepsilon b \in \mathfrak{q}$, and so $p_\varepsilon + c_\varepsilon^2 \in \mathfrak{q}$. Since $\mathfrak{q}$ is a γ-radical ideal, we deduce that $c_\varepsilon \in \mathfrak{q}$, a contradiction. Thus, $\gamma \cup (-\gamma) = A$. □

Remark 2.13 It follows from Lemmata 2.7 and 2.12 that fixed $\alpha \in \mathrm{Spec}_r(A)$, the family $\mathcal{G}_\alpha$ consisting of all α-convex prime ideals of A is a chain. By Remark 2.11 (3), $\mathfrak{p}_\alpha = \alpha \cap (-\alpha)$ is the minimum element of this chain, whose maximum element is, by Remark 2.8 (1), $\mathfrak{p}_{\rho(\alpha)} = \rho(\alpha) \cap (-\rho(\alpha))$.

Next we introduce a notion that extends the concept of real radical of an ideal.

Definition and Proposition 2.14 Let P be a cone and $\mathfrak{a}$ an ideal of a ring A.

(1) The *P-radical* of $\mathfrak{a}$ is the ideal

$$\sqrt[P]{\mathfrak{a}} := \{a \in A : \ \exists p \in P, \ m \geq 1 \ \text{ such that } \ a^{2m} + p \in \mathfrak{a}\}.$$

(2) *The P-radical of $\mathfrak{a}$ is the smallest P-radical ideal of A containing $\mathfrak{a}$.*

(3) *Let $\mathcal{R}_P(\mathfrak{a})$ denote the set of all P-convex prime ideals of A containing $\mathfrak{a}$. Then,*

$$\sqrt[P]{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in \mathcal{R}_P(\mathfrak{a})} \mathfrak{p},$$

where, if the set $\mathcal{R}_P(\mathfrak{a})$ is empty, this intersection is A.

(4) *The real radical $\sqrt[r]{\mathfrak{a}}$ of an ideal $\mathfrak{a}$ of a ring A is the P-radical of $\mathfrak{a}$ for $P := \Sigma A^2$.*

Proof. (1) We must prove that $\sqrt[P]{\mathfrak{a}}$ is an ideal. Given $a, b \in \sqrt[P]{\mathfrak{a}}$ there exist positive integers m, n, and $p, q \in P$ such that $a^{2m} + p \in \mathfrak{a}$ and $b^{2n} + q \in \mathfrak{a}$. Let $\ell := m + n$ and note that

$$(a+b)^{2\ell} + (a-b)^{2\ell} = \sum_{k=0}^{2\ell} \binom{2\ell}{k} a^k b^{2\ell-k} + \sum_{k=0}^{2\ell} \binom{2\ell}{k} (-1)^k a^k b^{2\ell-k}.$$

Denote $k = 2j$ for those summands with even k; then,

$$(a+b)^{2\ell} + (a-b)^{2\ell} = 2\sum_{j=0}^{\ell} \binom{2\ell}{2j} a^{2j} b^{2(\ell-j)} = a^{2m}\sigma_3 + b^{2n}\sigma_4$$

for some $\sigma_3, \sigma_4 \in \Sigma A^2 \subset P$ because, for each $0 \leq j \leq \ell$,

$$2j + 2(\ell - j) = 2\ell = 2(m+n) = 2m + 2n,$$

and so, either $2j \geq 2m$ or $2(\ell - j) \geq 2n$. Note that, $p\sigma_3 + q\sigma_4 \in P$ and

$$\begin{aligned}(a+b)^{2\ell} + (a-b)^{2\ell} + p\sigma_3 + q\sigma_4 &= a^{2m}\sigma_3 + b^{2n}\sigma_4 + p\sigma_3 + q\sigma_4 \\ &= (a^{2m} + p)\sigma_3 + (b^{2n} + q)\sigma_4 \in \mathfrak{a}.\end{aligned}$$

This implies that $a + b \in \sqrt[P]{\mathfrak{a}}$. Moreover, given $b \in \sqrt[P]{\mathfrak{a}}$ and $a \in A$ there exist an integer $m \geq 1$ and $p \in P$ such that $b^{2m} + p \in \mathfrak{a}$, and so

$$(ab)^{2m} + a^2 p = a^2(b^{2m} + p) \in \mathfrak{a} \quad \& \quad a^2 p \in P.$$

Thus $ab \in \sqrt[P]{\mathfrak{a}}$. All this proves that $\sqrt[P]{\mathfrak{a}}$ is an ideal of A.

(2) The inclusion $\mathfrak{a} \subset \sqrt[P]{\mathfrak{a}}$ is evident, because $0 \in P$ and $a^2 + 0 = a^2 \in \mathfrak{a}$. Moreover, $\sqrt[P]{\mathfrak{a}}$ is a P-radical ideal, since given $a \in A$ and $p \in P$ satisfying $a^2 + p \in \sqrt[P]{\mathfrak{a}}$, there exist an integer $m \geq 1$ and $q \in P$ such that $(a^2 + p)^{2m} + q \in \mathfrak{a}$. Therefore,

$$a^{4m} + \sum_{j=0}^{2m-1} \binom{2m}{j} a^{2j} p^{2m-j} + q = (a^2 + p)^{2m} + q \in \mathfrak{a},$$

which implies $a \in \sqrt[P]{\mathfrak{a}}$. Finally, we must check that each P-radical ideal $\mathfrak{b}$ containing $\mathfrak{a}$ contains $\sqrt[P]{\mathfrak{a}}$ too. Given $a \in \sqrt[P]{\mathfrak{a}}$ there exist an integer $m \geq 1$ and $p \in P$ such that $a^{2m} + p \in \mathfrak{a} \subset \mathfrak{b}$. Hence $(a^m)^2 + p \in \mathfrak{b}$ and, $\mathfrak{b}$ being a P-radical ideal, $a^m \in \mathfrak{b}$. By Remark 2.11 (1) $\mathfrak{b}$ is a radical ideal, and so $a \in \mathfrak{b}$.

(3) Each ideal $\mathfrak{p} \in \mathcal{R}_P(\mathfrak{a})$ is a radical and P-convex ideal; hence it is a P-radical ideal, by Remark 2.11 (1). Thus, by (1) above, $\sqrt[P]{\mathfrak{a}} \subset \mathfrak{p}$ for every $\mathfrak{p} \in \mathcal{R}_P(\mathfrak{a})$, and this proves one inclusion. For the converse suppose, by way of contradiction, the

existence of $f \in A \setminus \sqrt[P]{\mathfrak{a}}$ such that $f \in \mathfrak{p}$ for every $\mathfrak{p} \in \mathcal{R}_P(\mathfrak{a})$. Therefore, the set $\mathcal{F}$ of those P-radical ideals of A containing $\mathfrak{a}$ but not containing f is non-empty, and we order it by inclusion. It is straightforwardly checked that it is an inductive set and so it contains, by Zorn's Lemma, a maximal element $\mathfrak{q} \in \mathcal{F}$. We will prove that $\mathfrak{q}$ is a prime ideal of A; in this way $\mathfrak{q} \in \mathcal{R}_P(\mathfrak{a})$, which implies that $f \in \mathfrak{q}$, but this contradicts the fact that $\mathfrak{q} \in \mathcal{F}$.

Suppose there exist $a, b \in A \setminus \mathfrak{q}$ such that $ab \in \mathfrak{q}$. By part (2) both $\mathfrak{b}_1 := \sqrt[P]{aA + \mathfrak{q}}$ and $\mathfrak{b}_2 := \sqrt[P]{bA + \mathfrak{q}}$ are P-radical ideals containing $\mathfrak{q}$. In fact $\mathfrak{q} \subsetneq \mathfrak{b}_i$ for $i = 1, 2$, because $a \in \mathfrak{b}_1 \setminus \mathfrak{q}$ and $b \in \mathfrak{b}_2 \setminus \mathfrak{q}$. From the maximality of $\mathfrak{q}$ in $\mathcal{F}$ it follows that $f \in \mathfrak{b}_1 \cap \mathfrak{b}_2$, that is, there exist integers $m_1, m_2 \geq 1$ and $p_1, p_2 \in P$, $c_1, c_2 \in A$, $g_1, g_2 \in \mathfrak{q}$ satisfying

$$f^{2m_1} + p_1 = ac_1 + g_1 \quad \& \quad f^{2m_2} + p_2 = bc_2 + g_2.$$

Let $m := m_1 + m_2$. Multiplying the expressions above we deduce that

$$f^{2m} + p_1 f^{2m_2} + p_2 f^{2m_1} + p_1 p_2 = abc_1c_2 + g_1bc_2 + g_2ac_1 + g_1g_2 \in \mathfrak{q}.$$

Since $p := p_1 f^{2m_2} + p_2 f^{2m_1} + p_1 p_2 \in \Sigma A^2$ and $f^{2m} + p \in \mathfrak{q}$ it follows that $f \in \mathfrak{q}$, because $\mathfrak{q}$ is a P-radical ideal. This is a contradiction.

(4) This is immediate. □

Exercise 2.15 (1) With the notations in Proposition 2.14, prove that given two cones $P \subset Q$ in a ring A and an ideal $\mathfrak{a}$ of A, then $\mathcal{R}_Q(\mathfrak{a}) \subset \mathcal{R}_P(\mathfrak{a})$.

(2) Prove that if $P \subset Q$ are cones of A, then $\sqrt[P]{\mathfrak{a}} \subset \sqrt[Q]{\mathfrak{a}}$.

(3) Prove that $\sqrt{\mathfrak{a}} \subset \sqrt[P]{\mathfrak{a}}$ for every ideal $\mathfrak{a}$ and every cone P in the ring A.

The next result shows that if α is a prime cone in a ring A, the α-convexity is a very restrictive notion.

Proposition 2.16 *Let α be a prime cone in a ring A and let $\mathfrak{a}$ be a proper α-convex ideal in A. Then, $\sqrt{\mathfrak{a}} = \sqrt[\alpha]{\mathfrak{a}}$ is a prime α-convex ideal of A.*

Proof. Let us see that $\sqrt{\mathfrak{a}}$ is an α-convex ideal, which by Remark 2.11 (1) implies that $\sqrt{\mathfrak{a}}$ is an α-radical ideal, because $\sqrt{\mathfrak{a}}$ is a radical ideal. Let $p_1, p_2 \in \alpha$ such that $p_1 + p_2 \in \sqrt{\mathfrak{a}}$; then, there exists an integer $m \geq 1$ such that $(p_1 + p_2)^m \in \mathfrak{a}$, that is,

$$\sum_{k=0}^{m} \binom{m}{k} p_1^k p_2^{m-k} = (p_1 + p_2)^m \in \mathfrak{a}.$$

Note that $p := p_2^m \in \alpha$, $p' := \sum_{k=1}^m \binom{m}{k} p_1^k p_2^{m-k} \in \alpha$, and $p + p' = (p_1 + p_2)^m \in \mathfrak{a}$. Since $\mathfrak{a}$ is an α-convex ideal we deduce that $p, p' \in \mathfrak{a}$. In particular $p_2^m \in \mathfrak{a}$, which implies that $p_2 \in \sqrt{\mathfrak{a}}$ and $p_1 = (p_1 + p_2) - p_2 \in \sqrt{\mathfrak{a}}$.

By Proposition 2.14, $\sqrt[\alpha]{\mathfrak{a}}$ is the smallest α-radical ideal of A containing $\mathfrak{a}$, and we have just proved that $\sqrt{\mathfrak{a}}$ is one of them; hence, $\sqrt[\alpha]{\mathfrak{a}} \subset \sqrt{\mathfrak{a}}$. Conversely, it follows from Remark 2.11 that $\sqrt[\alpha]{\mathfrak{a}}$, which contains $\mathfrak{a}$, is a radical ideal because it is an α-radical ideal. Henceforth, $\sqrt{\mathfrak{a}} = \sqrt[\alpha]{\mathfrak{a}}$.

To finish we just need to prove that $\sqrt{\mathfrak{a}}$ is a prime ideal of A, but this requires some preparation. Denote $\mathcal{R}_\alpha(\mathfrak{a})$ the set consisting of those prime α-convex ideals of A containing $\mathfrak{a}$. By Proposition 2.14 we have

$$\sqrt{\mathfrak{a}} = \sqrt[\alpha]{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in \mathcal{R}_\alpha(\mathfrak{a})} \mathfrak{p}.$$

On the other hand, $\mathcal{R}_\alpha(\mathfrak{a})$ is a subset of the chain $\mathcal{G}_\alpha$ consisting of all prime α-convex ideals of A, and so $\mathcal{R}_\alpha(\mathfrak{a})$ is a chain too. Since $\mathfrak{a}$ is a proper ideal of A, also $\sqrt{\mathfrak{a}} \neq A$. Therefore the family $\mathcal{R}_\alpha(\mathfrak{a})$ is non-empty, and for every $\mathfrak{p} \in \mathcal{R}_\alpha(\mathfrak{a})$ we have $\sqrt{\mathfrak{a}} \subset \mathfrak{p} \subset \mathfrak{p}_{\rho(\alpha)}$.

Let us show that $\sqrt{\mathfrak{a}}$ is a prime ideal of A. Let $a, b \in A$ with $ab \in \sqrt{\mathfrak{a}}$ and $a \notin \sqrt{\mathfrak{a}}$; then, there exists $\mathfrak{q} \in \mathcal{R}_\alpha(\mathfrak{a})$ with $a \notin \mathfrak{q}$. But $ab \in \mathfrak{p}$ for every ideal $\mathfrak{p} \in \mathcal{R}_\alpha(\mathfrak{a})$; hence, $b \in \mathfrak{p}$ for every $\mathfrak{p} \in \mathcal{R}_\alpha(\mathfrak{a})$ satisfying $\mathfrak{p} \subset \mathfrak{q}$. Thus $b \in \mathfrak{q}$, and so $b \in \mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{R}_\alpha(\mathfrak{a})$ such that $\mathfrak{q} \subset \mathfrak{p}$. Since $\mathcal{R}_\alpha(\mathfrak{a})$ is a chain we conclude that $b \in \mathfrak{p}$ for every $\mathfrak{p} \in \mathcal{R}_\alpha(\mathfrak{a})$, and this implies that $b \in \sqrt{\mathfrak{a}}$. Thus, $\sqrt{\mathfrak{a}}$ is an α-convex prime ideal of A. □

Remark 2.17 Let α be a prime cone and let $\mathfrak{a}$ be an α-convex ideal of a ring A. It follows straightforwardly from Proposition 2.16 and Exercise 2.15 (3) that

$$\sqrt{\mathfrak{a}} \subset \sqrt[r]{\mathfrak{a}} \subset \sqrt[\alpha]{\mathfrak{a}} = \sqrt{\mathfrak{a}},$$

and so $\sqrt{\mathfrak{a}} = \sqrt[r]{\mathfrak{a}}$ is an α-convex prime ideal of A. Moreover, it follows from Lemma 2.12 that $\sqrt{\mathfrak{a}}$ is the support of the prime cone $\beta := \sqrt{\mathfrak{a}} \cup \alpha$.

In what follows in this section we approach the study of the topology of the real spectrum $\mathrm{Spec}_r(A)$ of a ring A, and we begin by proving that it is a compact space. The proof is more sophisticated than the one of the Zariski spectrum $\mathrm{Spec}(A)$.

Proposition 2.18 (Compactness of the real spectrum) *Let A be a real ring. Then, $\mathrm{Spec}_r(A)$ is a compact space.*

Proof. The proof of this result consists of several steps. To simplify the notation we denote $Y := \{0,1\}^A$ the set of all functions from A to $\{0,1\}$.

STEP 1. *Set theoretical embedding of* $\mathrm{Spec}_r(A)$ *in* Y.

For every prime cone $\alpha \in \mathrm{Spec}_r(A)$ consider the characteristic function of the set $\alpha \setminus (-\alpha)$, that is, the function

$$f_\alpha : A \to \{0,1\},\ a \mapsto \begin{cases} 1 & \text{if } a(\alpha) > 0, \\ 0 & \text{if } a(\alpha) \leq 0. \end{cases}$$

Note that $f_\alpha^{-1}(0) = -\alpha$, and this implies the injectivity of the map

$$\Phi : \mathrm{Spec}_r(A) \to Y,\ \alpha \mapsto f_\alpha.$$

Indeed, if $\alpha, \beta \in \mathrm{Spec}_r(A)$ with $f_\alpha = f_\beta$, then $-\alpha = f_\alpha^{-1}(0) = f_\beta^{-1}(0) = -\beta$, and so $\alpha = \beta$. In what follows we interpret Φ as a set theoretical inclusion, that is, we identify each prime cone α of A with the function f_α.

STEP 2. *A basis of the topology of the space* Y.

Endow the set $\{0,1\}$ with the discrete topology and let us fix in Y the product topology, that is, the coarser topology on Y among those making continuous the projections

$$\pi_a : Y \to \{0,1\},\ f \mapsto f(a)$$

for every $a \in A$. Thus, a subbasis of this topology is the family $\{H(a,\varepsilon) : a \in A,\ \varepsilon = 0,1\}$, with

$$H(a,\varepsilon) := \pi_a^{-1}(\varepsilon) = \{f \in Y :\ f(a) = \varepsilon\}.$$

Consequently, a basis of this topology is the family of sets

$$\mathcal{B} := \{H(a_1,\varepsilon_1;\ldots;a_r,\varepsilon_r) :\ a_i \in A,\ \varepsilon_i = 0,1\},$$

where $H(a_1,\varepsilon_1;\ldots;a_r,\varepsilon_r) = \bigcap_{i=1}^r H(a_i,\varepsilon_i)$. From the compactness of $\{0,1\}$ and Tychonoff's Theorem it follows that Y is compact too.

STEP 3. *The topology induced in* $\mathrm{Spec}_r(A)$ *by the one of* Y *is called the* Tychonoff topology, *and it is finer that the spectral topology.*

This follows at once from the equality

$$\begin{aligned} H(a_1,1;\ldots;a_r,1) \cap \mathrm{Spec}_r(A) &= \{\alpha \in \mathrm{Spec}_r(A) :\ f_\alpha(a_1) = 1,\ldots,f_\alpha(a_r) = 1\} \\ &= \{\alpha \in \mathrm{Spec}_r(A) :\ a_1(\alpha) > 0,\ldots,a_r(\alpha) > 0\} \\ &= U(a_1,\ldots,a_r). \end{aligned}$$

STEP 4. $\mathrm{Spec}_r(A)$ *is a closed subspace of* Y *and so, endowed with the Tychonoff topology,* $\mathrm{Spec}_r(A)$ *is a compact topological space.*

Once this be proved it follows from STEP 3 that, endowed with the spectral topology, $\mathrm{Spec}_r(A)$ is a compact space too.

To prove STEP 4 we check that $Y \setminus \mathrm{Spec}_r(A)$ is an open subset of Y. To that end we identify first those functions $f \in Y$ belonging to $\mathrm{Spec}_r(A)$, that is, under what conditions there exists a prime cone α such that $f = f_\alpha$. This is equivalent to say that $\alpha_f := -(f^{-1}(0))$ is a prime cone and, by the alternative definition of prime cone 1.4 and Exercise 1.5 (Ch.II), this is nothing else but

$$\begin{aligned} \alpha_f + \alpha_f \subset \alpha_f, \quad \alpha_f \cdot \alpha_f \subset \alpha_f, \quad A^2 \subset \alpha_f, \quad -1 \notin \alpha_f \quad \& \\ ab \in \alpha_f \quad \Longrightarrow \quad a \in \alpha_f \quad \text{or} \quad -b \in \alpha_f. \end{aligned}$$

To show that $Y \setminus \mathrm{Spec}_r(A)$ is an open subset of Y we will prove that if a function $f \in Y$ does not satisfy any of the above conditions, then there exists a basic open subset H containing f which does not intersect $\mathrm{Spec}_r(A)$. Thus we should distinguish several situations.

(i) Condition $\alpha_f + \alpha_f \not\subset \alpha_f$ is equivalent to the existence of $a, b \in \alpha_f$ such that $a + b \notin \alpha_f$, that is, $f(-a) = f(-b) = 0$ and $f(-(a+b)) = 1$ or, in other words,

$$f \in H(-a, 0; -b, 0; -(a+b), 1) := H \quad \& \quad H \cap \mathrm{Spec}_r(A) = \varnothing.$$

(ii) Condition $\alpha_f \cdot \alpha_f \not\subset \alpha_f$ is equivalent to the existence of $a, b \in \alpha_f$ such that $ab \notin \alpha_f$, that is, $f(-a) = f(-b) = 0$ and $f(-ab) = 1$, and this means,

$$f \in H(-a, 0; -b, 0; -ab, 1) := H \quad \& \quad H \cap \mathrm{Spec}_r(A) = \varnothing.$$

(iii) Condition $A^2 \not\subset \alpha_f$ says that there exists $a \in A$ such that $a^2 \notin \alpha_f$, that is, $f(-a^2) = 1$, or equivalently,

$$f \in H(-a^2, 1) := H \quad \& \quad H \cap \mathrm{Spec}_r(A) = \varnothing.$$

(iv) Condition $-1 \notin \alpha_f$ means that $f(-1) = 1$, that is,

$$f \in H(-1, 1) := H \quad \& \quad H \cap \mathrm{Spec}_r(A) = \varnothing.$$

(v) Finally, condition "there exist $a, b \in A$ such that $ab \in \alpha_f$, $a \notin \alpha_f$ and $-b \notin \alpha_f$" is equivalent to $f(-ab) = 0$ and $f(-a) = f(b) = 1$ or, in other words,

$$f \in H(-ab, 0; -a, 1; b, 1) := H \quad \& \quad H \cap \mathrm{Spec}_r(A) = \varnothing,$$

as wanted. □

Remarks 2.19 (1) Notice that for every $a_1, \ldots, a_r \in A$ and $\varepsilon_1, \ldots, \varepsilon_r \in \{0,1\}$, the set $H(a_1, \varepsilon_1; \ldots; a_r, \varepsilon_r)$ is an open and closed (*clopen* in what follows) subset of Y. Its openness is clear, since it belongs to the basis $\mathcal{B}$ introduced in STEP 2 of the precedent proof. To prove its closedness it suffices to see that its complementary is open, and this follows at once from the equality

$$H(a_1, \varepsilon_1; \ldots; a_r, \varepsilon_r) = Y \setminus \bigcup_{\substack{\delta \in \{0,1\}^r \\ \delta \neq (\varepsilon_1, \ldots, \varepsilon_r)}} H(a_1, \delta_1; \ldots; a_r, \delta_r),$$

where $\delta := (\delta_1, \ldots, \delta_r)$.

(2) In particular, it follows from the equality

$$U(a_1, \ldots, a_r) = H(a_1, 1; \ldots; a_r, 1) \cap \operatorname{Spec}_r(A),$$

proved in STEP 3 of the precedent proof, that $U(a_1, \ldots, a_r)$ is a clopen subset in $\operatorname{Spec}_r(A)$ endowed with the Tychonoff topology, and so it is also compact with this topology. This implies, since the spectral topology is coarser than Tychonoff topology, that $U(a_1, \ldots, a_r)$ is also compact as a subspace of $\operatorname{Spec}_r(A)$ endowed with the spectral topology.

Definition 2.20 (Constructible sets) Let A be a real ring. A subset of $\operatorname{Spec}_r(A)$ is *constructible* if it can be represented as a finite combination of boolean operations (finite union, finite intersection, complementary) applied to all sets of the type $U(a) := \{\alpha \in \operatorname{Spec}_r(A) : a(\alpha) > 0\}$, where $a \in A$.

Remarks 2.21 (1) Both the basic open set $U(a_1, \ldots, a_r) = \bigcap_{i=1}^r U(a_i)$ and its complementary

$$\operatorname{Spec}_r(A) \setminus U(a_1, \ldots, a_r) = \bigcup_{i=1}^r \operatorname{Spec}_r(A) \setminus U(a_i)$$

are constructible subsets of $\operatorname{Spec}_r(A)$. Using inductively De Morgan's laws it follows immediately that a subset of $\operatorname{Spec}_r(A)$ is constructible if and only if it is a finite union of sets of the form

$$\begin{aligned}\{\alpha \in \operatorname{Spec}_r(A) : \ & a_1(\alpha) > 0, \ldots, a_r(\alpha) > 0, \ b_1(\alpha) \leq 0, \ldots, b_s(\alpha) \leq 0\} \\ & = H(a_1, 1; \ldots; a_r, 1; b_1, 0; \ldots; b_s, 0) \cap \operatorname{Spec}_r(A),\end{aligned}$$

where $a_i, b_j \in A$. Since the finite union of compact subsets is compact too, it follows that constructible subsets of $\operatorname{Spec}_r(A)$ are compact with the spectral topology.

Moreover, they are clopen subsets in the Tychonoff topology of $\mathrm{Spec}_r(A)$ since they are finite union of clopen subsets.

(2) Conversely, we will see that those subsets of $\mathrm{Spec}_r(A)$ which are clopen with respect to the Tychonoff topology are constructible. Hence, the constructible subsets of $\mathrm{Spec}_r(A)$ are, exactly, those subsets which are clopen in the Tychonoff topology of $\mathrm{Spec}_r(A)$.

Indeed, let $C \subset \mathrm{Spec}_r(A)$ be a clopen subset in the Tychonoff topology of $\mathrm{Spec}_r(A)$. Since C is open there exist a set I, $a_{i1}, \ldots, a_{ir_i} \in A$ and $\varepsilon_{i1}, \ldots, \varepsilon_{ir} \in \{0,1\}$ for each $i \in I$, such that

$$C := \bigcup_{i \in I} H(a_{i1}, \varepsilon_{i1}; \ldots; a_{ir_i}, \varepsilon_{ir_i}) \cap \mathrm{Spec}_r(A).$$

Since C is a closed subset in the compact space $\mathrm{Spec}_r(A)$, with the Tychonoff topology, C is compact too. Therefore, there exists a finite subset $J \subset I$ such that

$$C = \bigcup_{i \in J} H(a_{i1}, \varepsilon_{i1}; \ldots; a_{ir_i}, \varepsilon_{ir_i}) \cap \mathrm{Spec}_r(A),$$

that is, C is constructible.

(3) An open subset $U \subset \mathrm{Spec}_r(A)$, in the spectral topology, is compact with the Tychonoff topology if and only if U is constructible. Indeed we have proved in part (1) that if U is constructible then it is compact with the Tychonoff topology. Conversely, U being open in the spectral topology of $\mathrm{Spec}_r(A)$, it admits a representation of the form

$$U := \bigcup_{i \in I} H(a_{i1}, \varepsilon_{i1}; \ldots; a_{ir_i}, \varepsilon_{ir_i}) \cap \mathrm{Spec}_r(A)$$

for a set I, some elements $a_{i1}, \ldots, a_{ir_i} \in A$ and $\varepsilon_{i1}, \ldots, \varepsilon_{ir_i} \in \{0,1\}$. If U is compact with the Tychonoff topology, we may assume that I is finite, and so U is constructible.

(4) In general, the real spectrum of a ring endowed with its spectral topology is not a Hausdorff space. However it enjoys some separation properties that we study right now.

Lemma 2.22 *Let A be a real ring and let $\alpha \in \mathrm{Spec}_r(A)$. Then:*

(1) $\mathrm{Cl}(\{\alpha\}) = \mathcal{F}_\alpha := \{\beta \in \mathrm{Spec}_r(A) : \alpha \subset \beta\}$.

(2) *The singleton $\{\alpha\}$ is a closed subset of $\mathrm{Spec}_r(A)$ if and only if α is a maximal prime cone.*

(3) *$\mathrm{Spec}_r(A)$ is a T_0-space.*

Proof. (1) Let $\beta \in \mathrm{Cl}(\{\alpha\})$ and let $a \in A \setminus \beta$. Then $a(\beta) < 0$, that is, $U(-a)$ is an open neighborhood of β in $\mathrm{Spec}_r(A)$, and so it contains α, that is, $a(\alpha) < 0$. This means that $a \in A \setminus \alpha$, and we have proved that $\alpha \subset \beta$.

Conversely, if $\alpha \subset \beta$ and $U := U(a_1, \ldots, a_r)$ is a basic open neighborhood of β in $\mathrm{Spec}_r(A)$, each $a_i(\beta) > 0$, that is, $a_i \in A \setminus (-\beta) \subset A \setminus (-\alpha)$. Therefore, $a_i(\alpha) > 0$, and so $\alpha \in U$. This proves that $\beta \in \mathrm{Cl}(\{\alpha\})$.

(2) This follows straightforwardly from part (1).

(3) Let $\alpha, \beta \in \mathrm{Spec}_r(A)$ with $\alpha \neq \beta$. We can suppose that $\beta \not\subset \alpha$, and so there exists $a \in \beta \setminus \alpha$, that is, $a(\beta) \geq 0$ and $a(\alpha) < 0$. Thus, $U(-a)$ is an open neighborhood of α and $\beta \notin U(-a)$. □

We present next a separation result which is specific of real spectra and does not hold, in general, for Zariski spectra. As a consequence we will see in Proposition 2.31 that the maximal real spectrum endowed with its spectral topology is a Hausdorff space.

Lemma 2.23 *Let A be a real ring and let $\alpha, \beta \in \mathrm{Spec}_r(A)$. The following statements are equivalent:*

(1) *$\alpha \not\subset \beta$ and $\beta \not\subset \alpha$.*

(2) *There exists $c \in A$ such that $\alpha \in U(c)$ and $\beta \in U(-c)$.*

(3) *There exist open disjoint neighborhoods of α and β in the spectral topology of $\mathrm{Spec}_r(A)$.*

Proof. To prove (2) $\Longrightarrow$ (3) it suffices to observe that $V_1 := U(c)$ and $V_2 := U(-c)$ are open disjoint subsets with $\alpha \in V_1$ and $\beta \in V_2$, while (3) $\Longrightarrow$ (1) follows from Lemma 2.22. Thus, all reduces to see that (1) implies (2). Let $a \in \alpha \setminus \beta$ and $b \in \beta \setminus \alpha$, that is,

$$a(\alpha) \geq 0, \quad a(\beta) < 0, \quad b(\beta) \geq 0 \quad \& \quad b(\alpha) < 0.$$

Notice that $c := a - b \in A$ satisfies

$$c(\alpha) = a(\alpha) - b(\alpha) > 0 \quad \& \quad c(\beta) = a(\beta) - b(\beta) < 0,$$

that is, $\alpha \in U(c)$ and $\beta \in U(-c)$. □

The precedent result shows that the real spectrum is an "almost Hausdorff" space: the only pairs of points which cannot be separated by disjoint neighborhoods are those occurring in the same chain.

Exercise 2.24 Let A be a real ring and consider in $\mathrm{Spec}_r(A)$ the spectral topology. Let $X \subset \mathrm{Spec}_r(A)$ be a constructible subset.

(1) Prove that

$$\mathrm{Cl}(X) = \{\beta \in \mathrm{Spec}_r(A) : \exists\, \alpha \in X \quad \text{such that} \quad \alpha \subset \beta\}.$$

(2) Prove that

$$\mathrm{Int}(X) = \{\beta \in \mathrm{Spec}_r(A) : \exists\, \alpha \in X \quad \text{such that} \quad \beta \subset \alpha\}.$$

We present now a last separation result in real spectra. Recall the notation introduced in Remark 2.8 (1); for every $\alpha \in \mathrm{Spec}_r(A)$ we denote $\rho(\alpha)$ the maximum element, with respect to the inclusion, of the chain $\mathrm{Cl}(\{\alpha\}) = \{\beta \in \mathrm{Spec}_r(A) : \alpha \subset \beta\}$.

Proposition 2.25 (Normality) *Let A a be a real ring and let C_1 and C_2 be two closed disjoint subsets in the spectral topology of* $\mathrm{Spec}_r(A)$*. Then, there exist disjoint constructible subsets U and V, which are open in the spectral topology of* $\mathrm{Spec}_r(A)$*, such that $C_1 \subset U$ and $C_2 \subset V$. In particular,* $\mathrm{Spec}_r(A)$ *is a normal topological space.*

Proof. Let us denote $\mathcal{U} := \{U_i : i \in I\}$ and $\mathcal{V} := \{V_j : j \in J\}$ the sets consisting of, respectively, all open constructible subsets of $\mathrm{Spec}_r(A)$ containing C_1 and C_2 and suppose, by way of contradiction, that each intersection $W_{ij} := U_i \cap V_j \neq \varnothing$. Notice that both U_i and V_j are closed in the Tychonoff topology of $\mathrm{Spec}_r(A)$, and so W_{ij} is closed too.

The assumption means that the family of closed subsets $\{W_{ij} : i \in I, j \in J\}$ enjoys the finite intersection property, because given $i_1, \ldots, i_r \in I$ and $j_1, \ldots, j_r \in J$,

$$W_{i_1 j_1} \cap \cdots \cap W_{i_r j_r} = (U_{i_1} \cap \cdots \cap U_{i_r}) \cap (V_{j_1} \cap \cdots \cap V_{j_r}) \neq \varnothing$$

since $\widehat{U} := U_{i_1} \cap \cdots \cap U_{i_r} \in \mathcal{U}$ and $\widehat{V} := V_{j_1} \cap \cdots \cap V_{j_r} \in \mathcal{V}$. But, endowed with the Tychonoff topology, $\mathrm{Spec}_r(A)$, is a compact space, and consequently the intersection

$$W := \Big(\bigcap_{i \in I} U_i\Big) \cap \Big(\bigcap_{j \in J} V_i\Big) = \bigcap_{(i,j) \in I \times J} W_{ij}$$

is non-empty, and we choose a point $\alpha \in W$.

Let us show, by way of contradiction, that $\mathrm{Cl}(\{\alpha\}) \cap C_1 \neq \varnothing$. Otherwise, by Lemma 2.22 (1), $\alpha \not\subset \beta$ for every $\beta \in C_1$, and so there exists $f_\beta \in \alpha \setminus \beta$, that is, $f_\beta(\alpha) \geq 0$ and $f_\beta(\beta) < 0$. Henceforth,

$$C_1 \subset \bigcup_{\beta \in C_1} U(-f_\beta)$$

and, C_1 being compact in the spectral topology, there exists a finite subset $\mathcal{F} \subset C_1$ such that $C_1 \subset \bigcup_{\beta\in\mathcal{F}} U(-f_\beta)$. This is impossible because it implies that

$$U := \bigcup_{\beta\in\mathcal{F}} U(-f_\beta) \in \mathcal{U},$$

and so $\alpha \in W \subset U$, but each $f_\beta(\alpha) \geq 0$. Thus, there exists a point $\beta_1 \in \mathrm{Cl}(\{\alpha\})\cap C_1$. The same argument shows the existence of a point $\beta_2 \in \mathrm{Cl}(\{\alpha\}) \cap C_2$. Since the set $\mathrm{Cl}(\{\alpha\})$ is, by Lemmata 2.7 and 2.22, a chain, its maximum element $\rho(\alpha)$ contains β_1 and β_2. But both C_1 and C_2 are closed subsets of $\mathrm{Spec}_r(A)$ endowed with the spectral topology, and this implies that

$$\rho(\alpha) \in \mathrm{Cl}(\{\beta_i\}) \subset \mathrm{Cl}(C_i) = C_i.$$

In particular $\rho(\alpha) \in C_1 \cap C_2$, a contradiction. □

Exercise 2.26 Let X be a topological space and consider the ring of continuous functions $\mathcal{C}(X)$ on X.

(1) Prove that for every prime ideal $\mathfrak{p} \in \mathrm{Spec}(\mathcal{C}(X))$ and each function $f \in \mathcal{C}(X)$, either $f = |f| \bmod \mathfrak{p}$ or $f = -|f| \bmod \mathfrak{p}$.

(2) Prove that the map

$$\mathrm{supp} : \mathrm{Spec}_r(\mathcal{C}(X)) \to \mathrm{Spec}(\mathcal{C}(X)),\ \alpha \mapsto \mathfrak{p}_\alpha$$

is a homeomorphism where both spaces are endowed with the spectral topology. Show that

$$\mathrm{supp}(U(f)) = D(f + |f|) \quad \& \quad \mathrm{supp}(\mathcal{Z}(f)) = \mathcal{Z}(f)$$

for every $f \in \mathcal{C}(X)$.

(3) Let $f \in \mathcal{C}(X)$ and denote $h := f + |f|$ and $\mathfrak{a}_f := \{g \in \mathcal{C}(X) : gh = 0\}$.

(3.1) Prove that $\mathrm{Cl}(U(f)) = \bigcap_{g\in\mathfrak{a}_f} \mathcal{Z}(g)$.

(3.2) Prove that if $\mathrm{Cl}(U(f))$ is a constructible set, then there exists a continuous function $g : X \to \mathbb{R}$ such that $\mathfrak{a}_f = \sqrt{(g)}$.

(4) Let $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x$. Show that $\mathrm{Cl}(U(f))$ is not a constructible subset of $\mathrm{Spec}_r(\mathcal{C}(\mathbb{R}))$.

Remarks 2.27 (1) The example in the previous Exercise 2.26 appears in [G3]. Later, Andradas, Bröcker and Ruiz proved in [ABR] that if A is an *excellent ring,* see [M], and Y is a constructible subset of $\mathrm{Spec}_r(A)$, then $\mathrm{Cl}(Y)$ is constructible too.

(2) Schwartz generalized in [Sch1] the example of Exercise 2.26 and he proved that if X is a completely regular and connected topological space and U is a constructible subset, open and not dense in $\mathrm{Spec}_r(\mathcal{C}(X))$, then $\mathrm{Cl}(U)$ is not constructible.

Exercise 2.28 Prove that given a real ring A and a closed and irreducible subset C, see Exercise 1.11, of $\mathrm{Spec}_r(A)$, there exists $\alpha \in \mathrm{Spec}_r(A)$ such that $C = \mathrm{Cl}(\{\alpha\})$.

Exercise 2.29 Let X be a topological space and let $f, g : X \to \mathbb{R}$ be two continuous functions such that

$$\{x \in X : g(x) = 0\} \subset \{x \in X : f(x) > 0\}.$$

Prove that there exist continuous functions $h_i : X \to \mathbb{R}$ with $i = 1, 2, 3$ such that $(1 + h_1^2)f = 1 + h_2 g + h_3^2$.

Remarks 2.30 (1) The statement in the previous Exercise 2.29 is proved in [G2].

(2) We have seen in Remark 2.8 (1) that the maximal real spectrum of a real ring A is the subset

$$\mathrm{Max}(A) := \{\alpha \in \mathrm{Spec}_r(A) : \ \alpha = \rho(\alpha)\}, \tag{2.1}$$

where $\rho(\alpha)$ is the maximum, with respect to the inclusion, of the chain

$$\mathrm{Cl}(\{\alpha\}) = \{\beta \in \mathrm{Spec}_r(A) : \ \alpha \subset \beta\}.$$

Consider in $\mathrm{Max}(A)$ the topology induced by the spectral topology of $\mathrm{Spec}_r(A)$. It follows from Lemma 2.12 that every prime cone $\alpha \in \mathrm{Spec}_r(A)$ whose support is a maximal ideal of A, is a maximal prime cone. However, we saw in Remark 2.8 (2) that the converse is not true in general.

Next proposition collects the two main results concerning the maximal real spectrum of a real ring.

Proposition 2.31 *Let A be a real ring. Then, $\mathrm{Max}(A)$ is a compact and Hausdorff space and the retraction $\rho : \mathrm{Spec}_r(A) \to \mathrm{Max}(A)$ is a continuous, closed and surjective map.*

Proof. It follows straightforwardly from Lemma 2.23 that $\mathrm{Max}(A)$ is a Hausdorff space, and the surjectivity of ρ is nothing else but equality (2.1) in Remark 2.30 (2). Let us see now that ρ is a continuous map at each point $\alpha \in \mathrm{Spec}_r(A)$.

Let U be an open subset of $\mathrm{Spec}_r(A)$ containing $\rho(\alpha)$, and its complementary $C := \mathrm{Spec}_r(A) \setminus U$. Since C and $\{\rho(\alpha)\}$ are disjoint closed subsets of $\mathrm{Spec}_r(A)$ it follows from Proposition 2.25 the existence of disjoint open constructible subsets U_1

and U_2 of $\mathrm{Spec}_r(A)$ such that $C \subset U_1$ and $\rho(\alpha) \in U_2$. But $\rho(\alpha) \in \mathrm{Cl}(\{\alpha\})$; hence $\alpha \in U_2$ and it suffices to prove that $\rho(U_2) \subset U$. Otherwise there would exist a prime cone $\beta \in U_2$ such that $\rho(\beta) \in \mathrm{Spec}_r(A) \setminus U = C \subset U_1$. This implies, since $\rho(\beta) \in \mathrm{Cl}(\{\beta\})$, that $\beta \in U_1$, and so $\beta \in U_1 \cap U_2 = \varnothing$, a contradiction.

In particular, the compactness of $\mathrm{Spec}_r(A)$ implies that $\mathrm{Max}(A) = \rho(\mathrm{Spec}_r(A))$ is compact too. Finally, ρ is a closed map because it is surjective and continuous, its domain is compact and its image is Hausdorff. □

Remarks 2.32 (1) Since ρ is continuous, closed and surjective, the topology in $\mathrm{Max}(A)$ is the quotient topology of $\mathrm{Spec}_r(A)$ induced by ρ.

(2) Since $\mathrm{Max}(A)$ is compact and Hausdorff it is also a normal space, that is, given two closed disjoint subsets $C_1, C_2 \subset \mathrm{Max}(A)$ there exist open disjoint subsets V_1, V_2 of $\mathrm{Max}(A)$ such that $C_i \subset V_i$ for $i = 1, 2$.

Exercise 2.33 Draw the maximal real spectra of the real rings $\mathbb{Z}$, $\mathbb{R}(\mathtt{t})$ and $\mathbb{R}[\mathtt{t}]$ and determine their topologies.

To finish this section we study the behaviour of the functors Spec_r and Max.

Proposition 2.34 (Morphisms between real spectra) (1) *Let A and B be two real rings and let $\varphi : A \to B$ be a ring homomorphism. Then, the map*

$$\mathrm{Spec}_r(\varphi) : \mathrm{Spec}_r(B) \to \mathrm{Spec}_r(A), \ \beta \mapsto \varphi^{-1}(\beta)$$

is well defined, and for every $a_1, \ldots, a_r \in A$ the following equality holds:

$$\mathrm{Spec}_r(\varphi)^{-1}(U(a_1, \ldots, a_r)) = U(\varphi(a_1), \ldots, \varphi(a_r)).$$

In particular, the spectral map $\mathrm{Spec}_r(\varphi)$ *induced by φ is continuous.*

(2) *Denote $\mathtt{j}_B : \mathrm{Max}(B) \hookrightarrow \mathrm{Spec}_r(B)$ the inclusion map, and let us consider the continuous retraction $\rho_A : \mathrm{Spec}_r(A) \to \mathrm{Max}(A)$ introduced in 2.8. Then the map*

$$\mathrm{Max}(\varphi) := \rho_A \circ \mathrm{Spec}_r(\varphi) \circ \mathtt{j}_B : \mathrm{Max}(B) \to \mathrm{Max}(A).$$

is continuous.

(3) *Let C be a real ring and let $\psi : B \to C$ be a ring homomorphism. Then,*

$$\mathrm{Spec}_r(\psi \circ \varphi) = \mathrm{Spec}_r(\varphi) \circ \mathrm{Spec}_r(\psi) \quad \& \quad \mathrm{Max}(\psi \circ \varphi) = \mathrm{Max}(\varphi) \circ \mathrm{Max}(\psi).$$

Proof. (1) Let us check that $\mathrm{Spec}_r(\varphi)$ is well defined. For every $\beta \in \mathrm{Spec}_r(B)$ there exist a real closed field R and a homomorphism $\eta : B \to R$ such that $\eta^{-1}(R^2) = \beta$. Then, $\varphi^{-1}(\beta) = \varphi^{-1}(\eta^{-1}(R^2)) = (\eta \circ \varphi)^{-1}(R^2)$ is, by 1.7 (Ch.II), a prime cone in A, and so the map $\mathrm{Spec}_r(\varphi)$ is well defined.

Given $a_1, \ldots, a_r \in A$, the prime cone $\beta \in \mathrm{Spec}_r(B)$ belongs to the preimage $\mathrm{Spec}_r(\varphi)^{-1}(U(a_1, \ldots, a_r))$ if and only if $\varphi^{-1}(\beta) = \mathrm{Spec}_r(\varphi)(\beta) \in U(a_1, \ldots, a_r)$, that is, $-a_i \notin \varphi^{-1}(\beta)$ for each $1 \leq i \leq r$, or equivalently, $\beta \in U(\varphi(a_1), \ldots, \varphi(a_r))$. Since the sets of the form $U(a_1, \ldots, a_r)$ constitute a basis of the spectral topology of $\mathrm{Spec}_r(A)$ this proves the continuity of $\mathrm{Spec}_r(\varphi)$.

(2) The continuity of $\mathrm{Max}(\varphi)$ follows at once from the one of ρ_A, $\mathrm{Spec}_r(\varphi)$ and $\mathtt{j}_B$.

(3) For the first equality it suffices to note that for every prime cone $\gamma \in \mathrm{Spec}_r(C)$ we have

$$\mathrm{Spec}_r(\psi \circ \varphi)(\gamma) = (\psi \circ \varphi)^{-1}(\gamma) = \varphi^{-1}(\psi^{-1}(\gamma)) = (\mathrm{Spec}_r(\varphi) \circ \mathrm{Spec}_r(\psi))(\gamma).$$

For the second one, let us denote $\mathtt{j}_C : \mathrm{Max}(C) \hookrightarrow \mathrm{Spec}_r(C)$ the inclusion map, and consider the canonical retractions

$$\rho_B : \mathrm{Spec}_r(B) \to \mathrm{Max}(B) \quad \& \quad \rho_C : \mathrm{Spec}_r(C) \to \mathrm{Max}(C).$$

For each maximal cone $\gamma \in \mathrm{Max}(C)$ the closure $\mathrm{Cl}(\mathrm{Spec}_r(\psi)(\gamma))$ is compact, because it is a closed subspace of the compact space $\mathrm{Spec}_r(B)$. Thus, the composition

$$\rho_A \circ \mathrm{Spec}_r(\varphi)|_{\mathrm{Cl}(\mathrm{Spec}_r(\psi)(\gamma))} : \mathrm{Cl}(\mathrm{Spec}_r(\psi)(\gamma)) \to \mathrm{Max}(A)$$

is a continuous map whose domain is a compact space and whose target is a Hausdorff space; hence, it is a proper map.

In particular, if $\beta := \mathrm{Spec}_r(\psi)(\gamma)$ we have $\rho_B(\beta) \in \mathrm{Cl}(\{\beta\})$, and so

$$(\mathrm{Max}(\varphi) \circ \mathrm{Max}(\psi))(\gamma) = (\rho_A \circ \mathrm{Spec}_r(\varphi))(\rho_B(\mathrm{Spec}_r(\psi)(\gamma)))$$

belongs to the set

$$(\rho_A \circ \mathrm{Spec}_r(\varphi))(\mathrm{Cl}(\{\beta\}) = \mathrm{Cl}(\rho_A \circ \mathrm{Spec}_r(\varphi)(\beta)) = \rho_A(\mathrm{Spec}_r(\varphi)(\beta));$$

the last equality above follows because $\rho_A(\alpha)$ is a closed point of $\mathrm{Spec}_r(A)$ if we denote $\alpha := \mathrm{Spec}_r(\varphi)(\beta)$. On the other hand,

$$\begin{aligned}\rho_A(\mathrm{Spec}_r(\varphi)(\beta)) &= \rho_A(\mathrm{Spec}_r(\varphi)(\mathrm{Spec}_r(\psi)(\gamma))) \\ &= \rho_A(\mathrm{Spec}_r(\psi \circ \varphi)(\gamma)) = \mathrm{Max}(\psi \circ \varphi)(\gamma),\end{aligned}$$

and so the equality $\mathrm{Max}(\varphi) \circ \mathrm{Max}(\psi) = \mathrm{Max}(\psi \circ \varphi)$ is proved. □

Exercise 2.35 Let A be a real ring, $a_1, \ldots, a_r \in A$ and consider the ideal

$$\mathfrak{a} := (a_1\mathtt{x}_1^2 - 1, \ldots, a_r\mathtt{x}_r^2 - 1)A[\mathtt{x}],$$

where $\mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_r)$. Denote $\pi : A[\mathtt{x}] \to A[\mathtt{x}]/\mathfrak{a}$ the canonical projection, consider the inclusion homomorphism $\mathtt{j} : A \hookrightarrow A[\mathtt{x}]$ and let $\varphi := \pi \circ \mathtt{j} : A \to B = A[\mathtt{x}]/\mathfrak{a}$. Prove the equality

$$\mathrm{Spec}_r(\varphi)(\mathrm{Spec}_r(B)) = U(a_1, \ldots, a_r),$$

which provides a new proof of the compactness of $U(a_1, \ldots, a_r)$ from the one of $\mathrm{Spec}_r(B)$.

3 Polynomial Stone-Cěch compactification

For simplicity, we work in this section over the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers, instead of an arbitrary real closed field R and its algebraic closure C. We denote $\mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ and $A[\mathtt{x}] := A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ for each positive integer n and every ring A.

Remarks 3.1 (1) *Zariski maximal spectrum of* $\mathbb{C}[\mathtt{x}]$. It follows immediately from Hilbert's Nullstellensatz that the map

$$\mathtt{j} : \mathbb{C}^n \to \mathrm{Spec}_{\max}(\mathbb{C}[\mathtt{x}]),\ p \mapsto \mathfrak{m}_p := \{F \in \mathbb{C}[\mathtt{x}] :\ F(p) = 0\},$$

is a bijection. The topology of $\mathbb{C}^n$ induced via $\mathtt{j}$ by the Zariski topology of the maximal spectrum $\mathrm{Spec}_{\max}(\mathbb{C}[\mathtt{x}])$ is called the *Zariski topology* of $\mathbb{C}^n$. It is rather different from the Euclidean topology in $\mathbb{C}^n$ because each non-empty open subset W in the Zariski topology of $\mathbb{C}^n$ is a dense subset in the Euclidean topology of $\mathbb{C}^n$.

Suppose, by way of contradiction, that $W \cap U = \varnothing$ for some non-empty open subset U in the Euclidean topology of $\mathbb{C}^n$. There exists a polynomial $F \in \mathbb{C}[\mathtt{x}] \setminus \{0\}$ such that $D(F) \cap \mathrm{Spec}_{\max}(\mathbb{C}[\mathtt{x}]) \subset \mathtt{j}(W)$. Then, $\{p \in U : F(p) \neq 0\} = \varnothing$, against the Identity Principle 3.2, (Ch.I).

Consequently, the identification $\mathbb{C}^n \equiv \mathrm{Spec}_{\max}(\mathbb{C}[\mathtt{x}])$ "forgets" the Euclidean topology of $\mathbb{C}^n$; in fact, this is not a surprise because we know from Proposition 1.13 that, endowed with the Zariski topology, $\mathbb{C}^n$ is a compact space.

(2) *Real maximal spectrum of* $\mathbb{R}[\mathtt{x}]$. In dealing with the real spectrum of $\mathbb{R}[\mathtt{x}]$ the situation is rather different. By the Real Nullstellensatz 3.4 (Ch.II), the maximal real ideals of $\mathbb{R}[\mathtt{x}]$ are those of the form

$$\mathfrak{m}_p := \{f \in \mathbb{R}[\mathtt{x}] : f(p) = 0\},$$

where $p \in \mathbb{R}^n$. Indeed, if $\mathfrak{m}$ is a maximal real ideal of $\mathbb{R}[\mathtt{x}]$ it coincides with its real radical, that is, $\mathcal{I}(\mathcal{Z}(\mathfrak{m})) = \mathfrak{m}$. In particular $\mathcal{Z}(\mathfrak{m})$ is non-empty, and we choose a point $p \in \mathcal{Z}(\mathfrak{m})$. Then,

$$\mathfrak{m} = \mathcal{I}(\mathcal{Z}(\mathfrak{m})) \subset \mathcal{I}(\{p\}) = \mathfrak{m}_p$$

and, $\mathfrak{m}$ being a maximal ideal, $\mathfrak{m} = \mathfrak{m}_p$. Conversely, for each point $p \in \mathbb{R}^n$ the ideal $\mathfrak{m}_p$ is the kernel of the surjective homomorphism

$$\mathrm{ev}_p : \mathbb{R}[\mathtt{x}] \to \mathbb{R},\ f \mapsto f(p).$$

Consequently, the quotient $\mathbb{R}[\mathtt{x}]/\mathfrak{m}_p$ is isomorphic to $\mathbb{R}$, which is a real closed field; in particular it admits a unique ordering. Hence, $\mathfrak{m}_p$ is a real prime ideal and there exists a unique prime cone $\alpha_p := (\mathfrak{m}_p, \leq) \in \mathrm{Spec}_r(\mathbb{R}[\mathtt{x}])$ whose support is $\mathfrak{m}_p$. In fact α_p is identified, as a subset of $\mathbb{R}[\mathtt{x}]$, with

$$\alpha_p := \{f \in \mathbb{R}[\mathtt{x}] :\ f(p) \geq 0\},$$

and the map

$$\mathsf{e}_n : \mathbb{R}^n \to \mathrm{Max}(\mathbb{R}[\mathtt{x}]),\ p \mapsto \alpha_p$$

is injective. Indeed, given distinct points $p, q \in \mathbb{R}^n$ the polynomial $f(\mathtt{x}) = -\|\mathtt{x} - p\|^2$ satisfies $f(p) = 0$ and $f(q) < 0$, which implies that $f \in \alpha_p \setminus \alpha_q$.

Notice that a basis of open subsets of the topology induced in $\mathbb{R}^n$ via e_n by the spectral topology of the real maximal spectrum $\mathrm{Max}(\mathbb{R}[\mathtt{x}])$ consists of the subsets

$$\mathsf{e}_n^{-1}(U(f_1, \ldots, f_r) \cap \mathrm{Max}(\mathbb{R}[\mathtt{x}])) = \{p \in \mathbb{R}^n : f_1(p) > 0, \ldots, f_r(p) > 0\} \tag{3.1}$$

with $f_1, \ldots, f_r \in \mathbb{R}[\mathtt{x}]$, since $f(\alpha_p) = f + \mathfrak{m}_p = f(p)$ for each $f \in \mathbb{R}[\mathtt{x}]$ and every $p \in \mathbb{R}^n$.

Since polynomial functions are continuous with respect to the Euclidean topology, the sets of the form (3.1) are open in the Euclidean topology of $\mathbb{R}^n$. In fact they constitute a basis of this topology, because for every point $p \in \mathbb{R}^n$ and each positive real number ε, the polynomial $f_{p,\varepsilon} := \varepsilon^2 - \|\mathtt{x} - p\|^2 \in \mathbb{R}[\mathtt{x}]$ satisfies

$$\mathsf{e}_n^{-1}(U(f_{p,\varepsilon}) \cap \mathrm{Max}(\mathbb{R}[\mathtt{x}])) = \{x \in \mathbb{R}^n : \varepsilon^2 - \|x-p\|^2 > 0\} = \{x \in \mathbb{R}^n :\ \|x-p\|^2 < \varepsilon^2\},$$

that is, $\mathsf{e}_n^{-1}(U(f_{p,\varepsilon}) \cap \mathrm{Max}(\mathbb{R}[\mathtt{x}]))$ is the open ball centered at p with radius $\varepsilon > 0$. Henceforth, the Euclidean topology of $\mathbb{R}^n$ coincides with its *spectral topology,* that is, the topology induced in $\mathbb{R}^n$ via the map e_n by the spectral topology of $\mathrm{Max}(\mathbb{R}[\mathtt{x}])$.

(3) In particular e_n is not a surjective map since in such a case it would be a homeomorphism, and this is false because $\mathrm{Max}(\mathbb{R}^n)$ is a compact space and $\mathbb{R}^n$ is not compact. In Proposition 3.2 we will prove that $\mathsf{e}_n(\mathbb{R}^n)$ is a dense subset of

$\mathrm{Max}(\mathbb{R}^n)$, and so the pair $(\mathrm{Max}(\mathbb{R}^n), \mathtt{e}_n)$ constitutes a Hausdorff compactification of $\mathbb{R}^n$ to which all polynomial functions $\mathbb{R}^n \to \mathbb{R}$ "can be extended", in a sense that will be specified right now. In the sequel we denote

$$\mathtt{e}_1 : \mathbb{R} \to \overline{\mathbb{R}} := \mathrm{Max}(\mathbb{R}[\mathtt{t}]),\ t \mapsto \alpha_t := \{f \in \mathbb{R}[\mathtt{t}] :\ f(t) \geq 0\}. \tag{3.2}$$

Proposition 3.2 (1) *With the notations in Remark* 3.1 (2)*, the image of the embedding*

$$\mathtt{e}_n : \mathbb{R}^n \to \mathrm{Max}(\mathbb{R}[\mathtt{x}]),\ p \mapsto \alpha_p$$

is a dense subset of $\mathrm{Max}(\mathbb{R}[\mathtt{x}])$*. Thus, the pair* $(\mathrm{Max}(\mathbb{R}[\mathtt{x}]), \mathtt{e}_n)$ *is a Hausdorff compactification of* $\mathbb{R}^n$*.*

(2) *For each polynomial* $f \in \mathbb{R}[\mathtt{x}]$ *there exists a continuous function*

$$\widehat{f} : \mathrm{Max}(\mathbb{R}[\mathtt{x}]) \to \mathrm{Max}(\mathbb{R}[\mathtt{t}])$$

extending the polynomial function $f : \mathbb{R}^n \to \mathbb{R}$*, that is,* $\widehat{f} \circ \mathtt{e}_n = \mathtt{e}_1 \circ f$*.*

Proof. (1) Let $U \subset \mathrm{Max}(\mathbb{R}[\mathtt{x}])$ be a non-empty open subset. Then, there exist polynomials $f_1, \ldots, f_m \in \mathbb{R}[\mathtt{x}]$ such that

$$\varnothing \neq U(f_1, \ldots, f_m) \cap \mathrm{Max}(\mathbb{R}[\mathtt{x}]) \subset U,$$

and it is enough to prove that the set

$$W := \{x \in \mathbb{R}^n :\ f_1(x) > 0, \ldots, f_m(x) > 0\}$$

is non-empty. Consider the $\mathbb{R}$-algebra $A := \mathbb{R}[\mathtt{x}, \mathtt{y}]/\mathfrak{a}$, where $\mathtt{y} := (\mathtt{y}_1, \ldots, \mathtt{y}_m)$ and

$$\mathfrak{a} := (f_1(\mathtt{x})\mathtt{y}_1^2 - 1, \ldots, f_m(\mathtt{x})\mathtt{y}_m^2 - 1).$$

We claim that if $W = \varnothing$ there is no $\mathbb{R}$-algebras homomorphism $\eta : A \to \mathbb{R}$. Otherwise let us denote $\pi : \mathbb{R}[\mathtt{x}, \mathtt{y}] \to A$ the canonical projection, $\rho := \eta \circ \pi$ and consider the point $p = (p_1, \ldots, p_n) \in \mathbb{R}^n$ with $p_j := \rho(\mathtt{x}_j) \in \mathbb{R}$, for $1 \leq j \leq n$. Therefore $p \in W$ because $1 = \rho(f_i(\mathtt{x})\mathtt{y}_i^2) = f_i(p)\rho(\mathtt{y}_i)^2$, against our assumption.

Hence, by Robinson's formulation 2.5 of Artin-Lang's Theorem (Ch.II), there is no $\mathbb{R}$-algebras homomorphism $A \to R_1$ for any real closed field R_1. Hence, by 1.7 (Ch.II), the real spectrum $\mathrm{Spec}_r(A)$ is empty. Then, by Exercise 2.35, $U(f_1, \ldots, f_m)$ is empty too, and this is false.

(2) Consider the ring homomorphism $\varphi : \mathbb{R}[\mathtt{t}] \to \mathbb{R}[\mathtt{x}],\ g \mapsto g \circ f$ induced by the polynomial f, the embedding $\mathtt{i} : \mathrm{Max}(\mathbb{R}[\mathtt{x}]) \hookrightarrow \mathrm{Spec}_r(\mathbb{R}[\mathtt{x}])$ and let

$$\widehat{f} := \mathrm{Max}(\varphi) = \rho \circ \mathrm{Spec}_r(\varphi) \circ \mathtt{i} : \mathrm{Max}(\mathbb{R}[\mathtt{x}]) \to \mathrm{Max}(\mathbb{R}[\mathtt{t}]) = \overline{\mathbb{R}},$$

where $\mathrm{Spec}_r(\varphi) : \mathrm{Spec}_r(\mathbb{R}[\mathtt{x}]) \to \mathrm{Spec}_r(\mathbb{R}[\mathtt{t}])$ is the spectral map induced by φ and $\rho : \mathrm{Spec}_r(\mathbb{R}[\mathtt{t}]) \to \mathrm{Max}(\mathbb{R}[\mathtt{t}])$ is the continuous retraction introduced in Propositon 2.31.

We observed in Proposition 2.34 that $\widehat{f}$ is continuous. Moreover, with the notations in Remark 3.1 (2), $\widehat{f}(\alpha_p) = \alpha_{f(p)}$ for each $p \in \mathbb{R}^n$, that is, the maps

$$\mathtt{e}_n : \mathbb{R}^n \to \mathrm{Max}(\mathbb{R}[\mathtt{x}]),\ p \mapsto \alpha_p \quad \& \quad \mathtt{e}_1 : \mathbb{R} \to \mathrm{Max}(\mathbb{R}[\mathtt{t}]),\ t \mapsto \alpha_t,$$

satisfy $\widehat{f} \circ \mathtt{e}_n = \mathtt{e}_1 \circ f$. Indeed, for every point $p \in \mathbb{R}^n$ we compute

$$\begin{aligned}(\mathtt{e}_1 \circ f)(p) = \alpha_{f(p)} &= \{g \in \mathbb{R}[\mathtt{t}] :\ g(f(p)) \geq 0\} = \{g \in \mathbb{R}[\mathtt{t}] :\ \varphi(g)(p) \geq 0\} \\ &= \varphi^{-1}(\alpha_p) = \mathrm{Spec}_r(\varphi)(\alpha_p).\end{aligned}$$

This proves that $\mathrm{Spec}_r(\varphi)(\alpha_p)$ is a maximal prime cone, since $(\mathtt{e}_1 \circ f)(p)$ is a maximal prime cone, and consequently

$$(\widehat{f} \circ \mathtt{e}_n)(p) = \rho(\mathrm{Spec}_r(\varphi)(\alpha_p)) = \mathrm{Spec}_r(\varphi)(\alpha_p) = (\mathtt{e}_1 \circ f)(p).$$

Thus, using the identifications $p \equiv \alpha_p$ and $f(p) \equiv \alpha_{f(p)}$, it follows that $\widehat{f}$ is a continuous extension of f to $\mathrm{Max}(\mathbb{R}[\mathtt{x}])$ whose image is contained in $\overline{\mathbb{R}}$. □

Remark 3.3 We have $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ from Exercises 2.2 and 2.9 and Remark 3.1 (2), and the spectral topology in $\overline{\mathbb{R}}$ is determined by a basis of open neighborhoods of each point α_t with $t \in \mathbb{R}$, which consists of all open intervals in $\mathbb{R}$ centered at t, and the basis of open neighborhoods of the additional points $-\infty$ y $+\infty$, described in Exercise 3.4.

Exercise 3.4 (1) Prove that the families

$$\mathcal{B}_{-\infty} := \{\{-\infty\} \cup (-\infty, a) :\ a \in \mathbb{R}\} \quad \& \quad \mathcal{B}_{+\infty} := \{(a, +\infty) \cup \{+\infty\} :\ a \in \mathbb{R}\}$$

are, respectively, basis of open neighborhoods of $-\infty$ and $+\infty$ in $\overline{\mathbb{R}}$.

(2) Prove that $\overline{\mathbb{R}}$ is homeomorphic to the closed interval $[-1, 1]$.

(3.5) Polynomial Stone-Cěch compactification. Our next goal is to prove that $\mathrm{Max}(\mathbb{R}[\mathtt{x}])$ is the smallest Hausdorff compactification of $\mathbb{R}^n$ to which every polynomial map $f : \mathbb{R}^n \to \mathbb{R}$ admits a continuous extension $\mathrm{Max}(\mathbb{R}[\mathtt{x}]) \to \overline{\mathbb{R}}$. This provides a purely topological meaning to the space $\mathrm{Max}(\mathbb{R}[\mathtt{x}])$, which is independent of its algebraic definition.

To begin with we introduce some notions which give a precise meaning to the word "smallest" used in the precedent paragraph and allow us to handle in a suitable way the "extension property" required to the involved compactifications.

Definitions 3.6 (1) A *Hausdorff compactification* of $\mathbb{R}^n$ is a pair $(X, \mathtt{j})$ where X is a Hausdorff topological space and $\mathtt{j} : \mathbb{R}^n \to X$ is a *dense embedding,* that is, a continuous injective map that is a homeomorphism onto its image $\mathtt{j}(\mathbb{R}^n)$, which is a dense subset of the space X.

(2) Given two Hausdorff compactifications $(X_1, \mathtt{j}_1)$ and $(X_2, \mathtt{j}_2)$ of $\mathbb{R}^n$, we say that $(X_2, \mathtt{j}_2)$ *dominates* $(X_1, \mathtt{j}_1)$, and we write $(X_1, \mathtt{j}_1) \preccurlyeq (X_2, \mathtt{j}_2)$, if there exists a continuous surjection $\rho : X_2 \to X_1$ with $\rho \circ \mathtt{j}_2 = \mathtt{j}_1$. Notice that, $\mathtt{j}_i(\mathbb{R}^n)$ being dense in X_i for $i = 1, 2$, ρ is the unique continuous map whose composition with $\mathtt{j}_2$ is $\mathtt{j}_1$.

(3) We say that a Hausdorff compactification $(X, \mathtt{j})$ of $\mathbb{R}^n$ is *polynomially complete* if for every $f \in \mathbb{R}[\mathtt{x}]$ there exists a continuous function $F : X \to \overline{\mathbb{R}}$ such that $\mathtt{e}_1 \circ f = F \circ \mathtt{j}$, where $\mathtt{e}_1 : \mathbb{R} \to \overline{\mathbb{R}}$ was defined in 3.2.

Notice that $\preccurlyeq$ is an order relation (up to homeomorphism compatible with the dense embeddings $\mathtt{j}$) in the set of Hausdorff compactifications of $\mathbb{R}^n$, and we look for the smallest among those polynomially complete ones. Before that we need some preliminaries.

Lemma 3.7 *Let $(X_1, \mathtt{j}_1)$ and $(X_2, \mathtt{j}_2)$ be two Hausdorff compactifications of $\mathbb{R}^n$ such that $(X_1, \mathtt{j}_1) \preccurlyeq (X_2, \mathtt{j}_2)$, and let $\rho : X_2 \to X_1$ be the unique continuous surjection satisfying $\rho \circ \mathtt{j}_2 = \mathtt{j}_1$. Then,*

(1) $\rho^{-1}(X_1 \setminus \mathtt{j}_1(\mathbb{R}^n)) = X_2 \setminus \mathtt{j}_2(\mathbb{R}^n)$. *In particular,* $\rho(X_2 \setminus \mathtt{j}_2(\mathbb{R}^n)) = X_1 \setminus \mathtt{j}_1(\mathbb{R}^n)$.

(2) *Suppose that, moreover, $(X_2, \mathtt{j}_2) \preccurlyeq (X_1, \mathtt{j}_1)$. Then, ρ is a homeomorphism.*

(3) *Let $f : X_1 \to \overline{\mathbb{R}}$ be a continuous function. Then, $f \circ \rho : X_2 \to \overline{\mathbb{R}}$ is the unique continuous function such that $f \circ \mathtt{j}_1 = (f \circ \rho) \circ \mathtt{j}_2$.*

Proof. (1) Let $x_2 \in \rho^{-1}(X_1 \setminus \mathtt{j}_1(\mathbb{R}^n))$. Then $\rho(x_2) \in X_1 \setminus \mathtt{j}_1(\mathbb{R}^n)$. This implies that the point $x_2 \in X_2 \setminus \mathtt{j}_2(\mathbb{R}^n)$, since otherwise there would exist $p \in \mathbb{R}^n$ such that $x_2 = \mathtt{j}_2(p)$, and so $\rho(x_2) = (\rho \circ \mathtt{j}_2)(p) = \mathtt{j}_1(p) \in \mathtt{j}_1(\mathbb{R}^n)$, and this is false. Conversely, for each point $x_2 \in X_2 \setminus \mathtt{j}_2(\mathbb{R}^n)$, and $\mathtt{j}_2(\mathbb{R}^n)$ being a dense subset of X_2, there exists a net $\{s_d, D, \leq\}$ in $\mathbb{R}^n$ such that the net $\{\mathtt{j}_2(s_d), D, \leq\}$ converges to x_2. Since ρ is a continuous map, the net $\{\mathtt{j}_1(s_d) = (\rho \circ \mathtt{j}_2)(s_d), D, \leq\}$ converges to $\rho(x_2)$. If this point would belong to $\mathtt{j}_1(\mathbb{R}^n)$, then the net $\{s_d, D, \leq\}$ converges to a point $y \in \mathbb{R}^n$. Thus, the points x_2 and $\mathtt{j}_2(y)$ coincide because X_2 is a Hausdorff space and x_2 and $\mathtt{j}_2(y)$ are limit points of the net $\{j_2(s_d), D, \leq\}$; a contradiction.

The second part follows from what is just proved and the surjectivity of the map ρ:

$$\rho(X_2 \setminus \mathtt{j}_2(\mathbb{R}^n)) = \rho(\rho^{-1}(X_1 \setminus \mathtt{j}_1(\mathbb{R}^n))) = X_1 \setminus \mathtt{j}_1(\mathbb{R}^n).$$

(2) If $(X_2, \mathtt{j}_2) \preccurlyeq (X_1, \mathtt{j}_1)$ there exists a continuous surjection $\rho' : X_1 \to X_2$ such that $\rho' \circ \mathtt{j}_1 = \mathtt{j}_2$. In particular,

$$(\rho \circ \rho') \circ \mathtt{j}_1 = \rho \circ \mathtt{j}_2 = \mathtt{j}_1 = \mathrm{id}_{X_1} \circ \mathtt{j}_1 \quad \& \quad (\rho' \circ \rho) \circ \mathtt{j}_2 = \rho' \circ \mathtt{j}_1 = \mathtt{j}_2 = \mathrm{id}_{X_2} \circ \mathtt{j}_2,$$

and from the uniqueness it follows that $\rho \circ \rho' = \mathrm{id}_{X_1}$ and $\rho' \circ \rho = \mathrm{id}_{X_2}$. Therefore, ρ and ρ' are mutually inverse homeomorphisms.

(3) Note that $(f \circ \rho) \circ \mathtt{j}_2 = f \circ (\rho \circ \mathtt{j}_2) = f \circ \mathtt{j}_1$. About the uniqueness, let $g : X_2 \to \overline{\mathbb{R}}$ be a continuous function such that $f \circ \mathtt{j}_1 = g \circ \mathtt{j}_2$. Then,

$$(f \circ \rho) \circ \mathtt{j}_2 = f \circ (\rho \circ \mathtt{j}_2) = f \circ \mathtt{j}_1 = g \circ \mathtt{j}_2,$$

and so $(f \circ \rho)|_{\mathtt{j}_2(\mathbb{R}^n)} = g|_{\mathtt{j}_2(\mathbb{R}^n)}$. Since both $f \circ \rho$ and g are continuous maps and $\mathtt{j}_2(\mathbb{R}^n)$ is a dense subspace of X_2, the equality $f \circ \rho = g$ holds. □

To construct the smallest polynomially complete Hausdorff compactification of $\mathbb{R}^n$ we will adapt to our setting the classical method used to construct the Stone–Čech compactification of a completely regular topological space.

(3.8) Construction of the Stone–Čech polynomial compactification. The space

$$\overline{\mathbb{R}}^{\mathbb{R}[\mathtt{x}]} := \{z : \mathbb{R}[\mathtt{x}] \to \overline{\mathbb{R}}\} = \prod_{f \in \mathbb{R}[\mathtt{x}]} \overline{\mathbb{R}},$$

endowed with the product topology is, by Tychonoff's Theorem, a compact and Hausdorff space, because so is $\overline{\mathbb{R}}$. For every $g \in \mathbb{R}[\mathtt{x}]$ consider the projection

$$\Pi_g : \overline{\mathbb{R}}^{\mathbb{R}[\mathtt{x}]} \to \overline{\mathbb{R}},\ (z_f)_{f \in \mathbb{R}[\mathtt{x}]} \mapsto z_g.$$

Let us see first the following:

(3.8.1) *Given a point $p \in \mathbb{R}^n$ and a closed subset $C \subset \mathbb{R}^n$ not containing p, there exists a polynomial $f \in \mathbb{R}[\mathtt{x}]$ such that $f(p) = 1$ and $f(C) \subset (-\infty, 0)$.*

Indeed we may assume, without loss of generality, that p is the origin in $\mathbb{R}^n$ and the open ball of radius 2 centered at p does not intersect C. A straightforward computation shows that $f(\mathtt{x}) := 1 - \|\mathtt{x}\|^2$ satisfies $f(p) = 1$ and $f(C) \subset (-\infty, 0)$.

(3.8.2) *The map $\varphi : \mathbb{R}^n \to \overline{\mathbb{R}}^{\mathbb{R}[\mathtt{x}]}$, $x \mapsto ((\mathtt{e}_1 \circ f)(x))_{f \in \mathbb{R}[\mathtt{x}]}$ is a topological embedding, that is,* it is injective, continuous and a homeomorphism onto its image.

The injectivity of φ follows from (3.8.1). Moreover φ is continuous because the topology we are dealing with in $\overline{\mathbb{R}}^{\mathbb{R}[\mathtt{x}]}$ is the product topology and for every $g \in \mathbb{R}[\mathtt{x}]$ the composition

$$\mathtt{e}_1 \circ g = \Pi_g \circ \varphi : \mathbb{R}^n \to \overline{\mathbb{R}},\ x \mapsto (\mathtt{e}_1 \circ g)(x)$$

is a continuous function. Let us see that φ is a homeomorphism onto its image. We already know that $\varphi : \mathbb{R}^n \to \varphi(\mathbb{R}^n)$ is a continuous bijection, and we need to prove that it is also an open map.

Let $U \subset \mathbb{R}^n$ be an open subset and $z_0 = \varphi(x_0) \in \varphi(U)$, for some point $x_0 \in U$. Since $x_0 \notin C := \mathbb{R}^n \setminus U$ there exists, by (3.8.1), a polynomial $f \in \mathbb{R}[\mathbf{x}]$ such that $f(x_0) = 1$ and $f(C) \subset (-\infty, 0)$. Note that $W := \Pi_f^{-1}((0,\infty))$ is an open subset of $\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}$ and it contains z_0, because

$$\Pi_f(z_0) = \Pi_f(\varphi(x_0)) = f(x_0) = 1 \in (0,\infty).$$

Thus $V := W \cap \varphi(\mathbb{R}^n)$ is an open neighborhood of z_0 in $\varphi(\mathbb{R}^n)$, and it is enough to see that $V \subset \varphi(U)$. For every $z \in V$ there exists $x \in \mathbb{R}^n$ such that $\varphi(x) = z$ and, since $z \in W$,

$$f(x) = \Pi_f(\varphi(x)) = \Pi_f(z) \in (0,\infty).$$

Therefore $x \notin C \subset f^{-1}(-\infty, 0)$, that is, $x \in U$ and so $z = \varphi(x) \in \varphi(U)$.

(3.8.3) The set $\beta\,\mathbb{R}^n := \mathrm{Cl}_{\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}}(\varphi(\mathbb{R}^n))$ contains $\varphi(\mathbb{R}^n)$ as a dense subset and, since it is closed in $\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}$, it is compact and Hausdorff. Besides, the pair $(\beta\,\mathbb{R}^n, \varphi)$ is a polynomially complete compactification of $\mathbb{R}^n$ because, for every polynomial $g \in \mathbb{R}[\mathbf{x}]$, the projection

$$\Pi_g : \beta\,\mathbb{R}^n \to \overline{\mathbb{R}},\ (z_f)_{f\in\mathbb{R}[\mathbf{x}]} \to z_g$$

is a continuous function and $\Pi_g \circ \varphi = \mathsf{e}_1 \circ g$.

(3.8.4) Even more, $(\beta\,\mathbb{R}^n, \varphi)$ is the smallest polynomially complete compactification of $\mathbb{R}^n$. To show this, let (Y, ψ) be another polynomially complete compactification of $\mathbb{R}^n$. For each $f \in \mathbb{R}[\mathbf{x}]$ denote $\widehat{f} : Y \to \overline{\mathbb{R}}$ the unique continuous function such that $\widehat{f} \circ \psi = \mathsf{e}_1 \circ f$. Then, the continuous map

$$\Psi : Y \to \overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]},\ y \mapsto (\widehat{f}(y))_{f\in\mathbb{R}[\mathbf{x}]}$$

satisfies the equality $\Psi \circ \psi = \varphi$ because for every point $x \in \mathbb{R}^n$ we have

$$(\Psi \circ \psi)(x) = \Psi(\psi(x)) = (\widehat{f}(\psi(x)))_{f\in\mathbb{R}[\mathbf{x}]} = (\mathsf{e}_1 \circ f(x))_{f\in\mathbb{R}[\mathbf{x}]} = \varphi(x).$$

It just remains to check that $\operatorname{im}\Psi = \beta\,\mathbb{R}^n$. But, Y being compact and $\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}$ being Hausdorff, the continuous map Ψ is also a closed map. Therefore,

$$\operatorname{im}\Psi = \Psi(\mathrm{Cl}_Y(\psi(\mathbb{R}^n))) = \mathrm{Cl}_{\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}}(\Psi(\psi(\mathbb{R}^n))) = \mathrm{Cl}_{\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}}(\varphi(\mathbb{R}^n)) = \beta\,\mathbb{R}^n.$$

(3.8.5) The precedent properties lead us to call $(\beta\,\mathbb{R}^n, \varphi)$ the *polynomial Stone–Čech compactification of* $\mathbb{R}^n$. It is worthwhile mentioning that the adjective polynomial refers to the nature of the functions that extend continuously from $\mathbb{R}^n$ to $\beta\,\mathbb{R}^n$, and not to the nature of this last set, which is not algebraic for any $n \geq 1$. To finish, we present another model of the polynomial Stone–Čech compactification of $\mathbb{R}^n$.

Proposition 3.9 *We keep the notations in Construction 3.8, and consider the map*

$$\phi : \mathbb{R}^n \to \mathrm{Max}(\mathbb{R}[\mathbf{x}]),\ x \mapsto \alpha_x := \{f \in \mathbb{R}[\mathbf{x}] :\ f(x) \geq 0\}.$$

Then, there exists a homeomorphism $\Psi : \mathrm{Max}(\mathbb{R}[\mathbf{x}]) \to \beta\,\mathbb{R}^n$ *such that* $\Psi \circ \phi = \varphi$.

We abbreviate this by saying that the pair $(\mathrm{Max}(\mathbb{R}[\mathbf{x}]), \phi)$ is *homeomorphic* to the polynomial Stone–Čech compactification $(\beta\,\mathbb{R}^n, \varphi)$ of $\mathbb{R}^n$, or that $(\mathrm{Max}(\mathbb{R}[\mathbf{x}]), \phi)$ is *a model* of the polynomial Stone–Čech compactification of $\mathbb{R}^n$.

Proof. By Proposition 3.2, $(\mathrm{Max}(\mathbb{R}[\mathbf{x}]), \phi)$ is a polynomially complete Hausdorff compactification of $\mathbb{R}^n$. For every $f \in \mathbb{R}[\mathbf{x}]$ let us denote, as in Proposition 3.2, $\widehat{f} : \mathrm{Max}(\mathbb{R}[\mathbf{x}]) \to \overline{\mathbb{R}}$ the unique continuous function satisfying $\widehat{f} \circ \mathsf{e}_n = \mathsf{e}_1 \circ f$. We shall prove that the map

$$\Psi : \mathrm{Max}(\mathbb{R}[\mathbf{x}]) \to \overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]},\ \alpha \mapsto (\widehat{f}(\alpha))_{f \in \mathbb{R}[\mathbf{x}]},$$

is a topological embedding whose image is $\beta\,\mathbb{R}^n$ and that $\Psi \circ \phi = \varphi$, where

$$\varphi : \mathbb{R}^n \to \overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]},\ x \mapsto ((\mathsf{e}_1 \circ f)(x))_{f \in \mathbb{R}[\mathbf{x}]}$$

is the embedding defined in (3.8.2). Observe first that for each point $x \in \mathbb{R}^n$,

$$\begin{aligned}(\Psi \circ \phi)(x) = \Psi(\phi(x)) = \Psi(\alpha_x) = (\widehat{f}(\alpha_x))_{f \in \mathbb{R}[\mathbf{x}]} = ((\widehat{f} \circ \mathsf{e}_n)(x))_{f \in \mathbb{R}[\mathbf{x}]} \\ = ((\mathsf{e}_1 \circ f)(x))_{f \in \mathbb{R}[\mathbf{x}]} = \varphi(x),\end{aligned}$$

which proves that $\Psi \circ \phi = \varphi$. Since $\mathrm{Max}(\mathbb{R}[\mathbf{x}])$ is compact and $\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}$ is Hausdorff, to see that Ψ is a topological embedding it suffices to show that it is continuous and injective. The continuity of Ψ follows straightforwardly, since $\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}$ is endowed with the product topology. Moreover, let $\alpha, \beta \in \mathrm{Max}(\mathbb{R}[\mathbf{x}])$ be distinct points. Since both are maximal prime cones, $\alpha \not\subset \beta$ and $\beta \not\subset \alpha$, and it follows from Lemma 2.23 the existence of $f \in \mathbb{R}[\mathbf{x}]$ such that $\alpha \in U(f)$ and $\beta \in U(-f)$, that is, $\widehat{f}(\alpha) > 0$ and $\widehat{f}(\beta) < 0$. Thus $\Psi(\alpha) \neq \Psi(\beta)$. Finally we check the equality $\mathrm{im}\,\Psi = \beta\,\mathbb{R}^n$. Indeed, since Ψ is a continuous and closed map,

$$\beta\,\mathbb{R}^n = \mathrm{Cl}_{\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}}(\varphi(\mathbb{R}^n)) = \mathrm{Cl}_{\overline{\mathbb{R}}^{\mathbb{R}[\mathbf{x}]}}(\Psi(\phi(\mathbb{R}^n)) = \Psi(\mathrm{Cl}_{\mathrm{Max}(\mathbb{R}[\mathbf{x}])}(\phi(\mathbb{R}^n)) = \Psi(\mathrm{Max}(\mathbb{R}[\mathbf{x}])),$$

and we are done. □

Remark 3.10 Notice that the remainder $\partial\mathbb{R}^n = \mathrm{Max}(\mathbb{R}[\mathbf{x}]) \setminus \mathbb{R}^n$ of the polynomial Stone–Čech compactification of $\mathbb{R}^n$ is the set of maximal prime cones of $\mathbb{R}[\mathbf{x}]$ whose support is not a real ideal, since we proved in Remark 3.1 (2) that the real maximal ideals of $\mathbb{R}[\mathbf{x}]$ are those of the form $\mathfrak{m}_p := \{f \in \mathbb{R}[\mathbf{x}] : f(p) = 0\}$.

Bibliography

[AAB1] F. Acquistapace, C. Andradas, F. Broglia: The strict Positivstellensatz for global analytic functions and the moment problem for semianalytic sets. *Math. Ann.* **316** (2000) no. 4, 609–616.

[AAB2] F. Acquistapace, C. Andradas, F. Broglia: The Positivstellensatz for definable functions on o-minimal structures. *Illinois J. Math.* **46** (2002) no. 3, 685–693.

[ABF1] F. Acquistapace, F. Broglia, J.F. Fernando: On a global analytic Positivstellensatz. *Ark. Mat.* **47** (2009) no. 1, 13–39.

[ABF2] F. Acquistapace, F. Broglia, J.F. Fernando: On Hilbert's 17th Problem and Pfister's multiplicative formulae for the ring of real analytic functions. *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **XXX** (2012, accepted), no. X, XXX-XXX.

[ABF3] F. Acquistapace, F. Broglia, J.F. Fernando: The Nullstellensatz for Stein spaces and real C-sets. *Preprint* RAAG, 2012.

[ABFR1] F. Acquistapace, F. Broglia, J.F. Fernando, J.M. Ruiz: On the Pythagoras numbers of real analytic surfaces. *Ann. Sci. École Norm. Sup.* **38** (2005) no. 2, 751–772.

[ABFR2] F. Acquistapace, F. Broglia, J.F. Fernando, J.M. Ruiz: On the Pythagoras numbers of real analytic curves. *Math. Z.* **257** (2007) no. 1, 13–21.

[ABFR3] F. Acquistapace, F. Broglia, J.F. Fernando, J.M. Ruiz: On the finiteness of Pythagoras numbers of real meromorphic functions. *Bull. Soc. Math. France.* **138**, (2010) no. 2, 231–247.

[ABS] F. Acquistapace, F. Broglia, M. Shiota: The finiteness property and Łojasiewicz's inequality for global semianalytic sets. *Adv. in Geom.* **5** (2005), 453–466.

[ABR] C. Andradas, L. Bröcker, J.M. Ruiz: Minimal generation of basic open semianalytic sets. *Invent. Math.* **92** (1988) no. 2, 409–430.

[ADR] C. Andradas, A. Díaz Cano, J.M. Ruiz: The Artin-Lang property for normal real analytic surfaces. *J. Reine Angew. Math.* **556** (2003), 99–111.

[A] E. Arrondo: Another elementary proof of the Nullstellensatz. *Amer. Math. Monthly.* **113** (2006) no. 2, 169–171.

[Ar] E. Artin: The collected papers of Emil Artin. Edited by S. Lang & J.T. Tate. Addison–Wesley Publishing Co., Inc., Reading, Mass.-London: 1965.

[AS] E. Artin, O. Schreier: Eine Kennzeichnung der reell abgeschlossenen Körper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg,* Springer-Berlin-Heidelberg, **5** (1927), 225–231.

[AM] J. Atiyah, I.G. MacDonald: Introduction to Commutative Algebra. Addison–Wesley Publishing Co., Inc., Reading, Mass.-London: 1969.

[dB] P. De Bartolomeis: Algebre di Stein nel caso reale. *Rend. Accad. Naz.* XL (5) no. 1/2 (1975/76), 105–144 (1977).

[Bo] J. Bochnak: Sur le théorème des zéros de Hilbert "différentiable". *Topology.* **12** (1973), 417–424.

[BCR] J. Bochnak, M. Coste and M.F. Roy, "Real algebraic geometry". Translated from the 1987 French original. Revised by the authors. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **36**. Springer-Verlag, Berlin: 1998.

[BE] J. Bochnak, G. Efroymson: Real algebraic geometry and the 17th Hilbert Problem. *Math. Ann.* **251** (1980), 213–241.

[BKS] J. Bochnak, W. Kucharz, M. Shiota: On equivalence of ideals of real global analytic functions and the 17th Hilbert Problem. *Invent. Math.* **63** (1981), 403–421.

[BR] J. Bochnak, J.J. Risler: Le théorème des zéros pour les varietés analytiques réelles de dimension 2. *Ann. Sci. École Norm. Sup.* **8** (1975) no. 3, 353–363.

[BBCP] J.M. Bony, F. Broglia, F. Colombini, L. Pernazza: Nonnegative functions as squares or sums of squares. *J. of Funct. Analysis* **232** (2006), 137–147.

[BCP] R. Brown, T.C. Craven, M.J. Pelling: Ordered fields satisfying Rolle's theorem. *Rocky Mountain J. Math.* **14** (1984) no. 4, 819–820.

[CT] J.L. Colliot-Thélène: Variantes du Nullstellensatz réel et anneaux formellement réels. Geometrie algébrique réelle et formes quadratiques. *Lecture Notes in Math.* **959**, pp. 98-108, Berlin: Springer-Verlag: 1982.

[CR] M. Coste, M.F. Roy: Le spectre réel et la topologie des variétés algébriques sur un corps réel clos. Algebra Colloquium (Rennes, 1980), pp. 151–168, Univ. Rennes, Rennes: 1980.

[D] C.N. Delzell: A continuous, constructive solution to Hilbert's 17th Problem. *Invent. Math.* **76** (1984) no. 3, 365–384.

[Du] D. W. Dubois: Note on Artin's solution of Hilbert's 17th Problem. *Bull. Amer. Math. Soc.* **73** (1967), 365–384.

[Du1] D.W. Dubois: A Nullstellensatz for ordered fields. *Ark. Mat.* **8** (1969), 111–114.

[DE] D.W. Dubois, G. Efroymson: Algebraic theory of real varieties. I. *Studies and Essays* (Presented to Yu-why Chen on his 60th Birthday, April 1, 1970) pp. 107–135 Math. Res. Center, Nat. Taiwan Univ., Taipei: 1970.

[E1] G. Efroymson: A Nullstellensatz for Nash rings. *Pacific J. Math.* **54** (1974), 101–112.

[E2] G. Efroymson: Substitution in Nash functions. *Pacific J. Math.* **63** (1976), 137–145.

[EV] J. Endler, T.M. Viswanathan: Digging holes in algebraic closures a la Artin I. *Math. Ann.* **265** (1983), 263–271.

[FL1] F. Fernández, A. Llerena: Extending automorphisms to the rational quotient field. *Extracta Math.* **6** (1991) no. 1, 25–27.

[FL2] F. Fernández, A. Llerena: On fields having the extension property. *J. Pure Appl. Algebra.* **77** (1992), 183–187.

[F1] J.F. Fernando: Sums of squares in real analytic rings. *Trans. Amer. Math. Soc.* **354** (2001) no. 1, 321–338.

[F2] J.F. Fernando: Positive semidefinite germs in real analytic surfaces. *Math. Ann.* **322** (2002) no. 1, 49–67.

[F3] J.F. Fernando: On the positive extension property and Hilbert's 17th Problem for real analytic sets. *J. Reine Angew. Math.* **618** (2008) no. 1, 1–49.

[F4] J.F. Fernando: On Hilbert's 17th Problem for global analytic functions in dimension 3. *Comment. Math. Helv.* **83** (2008) no. 1, 67–100.

[FG] J.F. Fernando, J.M. Gamboa: On the irreducible components of a semialgebraic set. *Int. J. of Math.* **23** (2012) no. 4, 40 pages.

[F] O. Forster: Primärzerlung in Steinschen Algebren. *Math. Ann.* **154** (1964), 307–329.

[G1] J.M. Gamboa: Some new results on ordered fields. *J. of Algebra.* **110** (1987) no. 1, 1–12.

[G2] J.M. Gamboa: A Positivstellensatz for rings of continuous functions. *J. Pure Appl. Algebra.* **45** (1987), 211–212.

[G3] J.M. Gamboa: Un exemple d'ensemble constructible à adhérence non constructible. *C.R. Acad. Sci. Paris* **306** (1988) Série I, 617–619.

[G4] J.M. Gamboa: On prime ideals in rings of semialgebraic functions. *Proc. Amer. Math. Soc.* **118** (1993) no. 4, 1037–1041.

[GR] J.M. Gamboa, T. Recio: Ordered fields with the dense orbits property. *J. Pure Appl. Algebra.* **30** (1983), 263–271.

[H] W. Habicht: Über die Zerlegung strikte definiter Formen in Quadrate. *Comment. Math. Helv.* **12** (1940), 317–322.

[He] E. Hewitt: Rings of real-valued continuous functions. I. *Trans. Amer. Math. Soc.* **64** (1948), 45–99.

[Hi] D. Hilbert: Über die Darstellung definiter Formen als Summe von Formenquadraten. *Math. Ann.* **32** (1888) no. 3, 342–350.

[Hi1] D. Hilbert: Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). *Math. Ann.* **67** (1909) no. 3, 281-300.

[Ho] M. Hochster: Prime ideal structure in commutative rings. *Trans. Amer. Math. Soc.* **142** (1969), 43–60.

[J] N. Jacobson: Lectures in abstract algebra. Vol III. Theory of fields and Galois theory. D. Van Nostrand Co., Inc. Princeton, N.J.-Toronto, Ont.-London-New York: 1964.

[JW1] P. Jaworski: Positive definite analytic functions and vector bundles. *Bull. Acad. Pol. Sci.*, **30** (1982) no. 11-12, 501-506.

[JW2] P. Jaworski: Extension of orderings on fields of quotients of rings of real analytic functions. *Math. Nach.*, **125** (1986), 329-339.

[K] M. Knebusch: Specialization of quadratic and symmetric bilinear forms and a norm theorem. *Acta Arith.* **24** (1973), 279-299.

[Kr] G. Kreisel: Sums of squares. *Summaries Summer Inst. Symbolic Logic,* Cornell Univ. **1957** (1960), 313-320.

[Kri] J.L. Krivine: Anneaux préordonnés. *J. Anal. Math.* **12** (1964), 307-326.

[L1] S. Lang: The theory of real places. *Ann. of Math.* (2) **57** (1953), 378–391.

[L2] S. Lang: Algebra. Revised third edition. Graduate Texts in Mathematics, **211** Springer-Verlag, New York: 2002.

[Ls] G. Lasalle: Sur le théorème des zéros différentiable. In *Singularités d'applications différentiables,* Plans-sur-Bex, *Lecture Notes in Math.* **535**, (1975), 87-136.

[Ł] S. Łojasiewicz: Sur le problème de la division. *Studia Math.* **18** (1959), 87-136.

[M] H. Matsumura: Commutative ring theory. W. A. Benjamin, Inc. New York: 1970.

[Me] J.P. Merrien: Idéaux de l'anneau des séries formelles à coefficients réels et variétes associées. *J. Math. Pures et Appl.* **50** (1971), 169-187.

[Mo] T. Mostowski: Some properties of the ring of Nash functions. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **3** (1976), 245-266.

[Mz] T.S. Motzkin: The arithmetic-geometric inequality. Inequalities (*Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965*) Academic Press, New York, (1967), 205–224.

[P] A. Prestel: Lectures on formally real fields. Lecture Notes in Math. **1093** Berlin. Springer-Verlag: 1984.

[Ri1] J.J. Risler: Une charactérization des idéaux des variétés algébriques réelles. *C.R. Acad. Sci. Paris* **t. 271** Série I (1970), 1171–1173.

[Ri2] J.J. Risler: Un théorème des zéros pour les functions différentiables dans le plan. *Fonctions de plusieurs variables complexes* (Sém. François Norguet, 1970–1973; à la mémoire d'André Martineau). *Lecture Notes in Math.* **409**, pp. 603–612, Springer. Berlin: 1974.

[Ri3] J.J. Risler: Le théorème des zéros en geometries algébrique et analytique réelles. *Bull. Soc. Math. France* **104** (1976) no. 2, 113–127.

[Rb] J.W. Robbin: Evaluation fields for power series. *J. of Algebra.* **57** I. 196-211 & II. 212-222 (1979).

[Ro] A. Robinson: On ordered fields and definite functions. *Math. Ann.* **130** (1955), 257–271.

[Rz1] J.M. Ruiz: Sobre álgebras de Nash. *Pub. Mat. UAB.* **20** (1980), 199–203.

[Rz2] J.M. Ruiz: Central orderings in fields of real meromorphic function germs. *Manuscripta. Math.* **46** (1984), 193–214.

[Rz3] J.M. Ruiz: On Hilbert's 17'th Problem and Real Nullstellensatz for Global Analytic Functions. *Math. Z.* **190** (1985), 447–454.

[Rz4] J.M. Ruiz: Sums of two squares in analytic rings. *Math. Z.* **230** (1999), 317–328.

[S] J.P. Serre: Extensions de corps ordonnés. *C. R. Acad. Sci. Paris* **229** (1949), 576–577.

[Sch1] N. Schwartz: The basic theory of real closed spaces. *Mem. Amer. Math. Soc.* **77** (1989), no. 397.

[Sch2] N. Schwartz: Rings of continuous functions as real closed spaces. *Ordered algebraic structures.* Kluwer Acad. Publ., Dordrecht: 1997.

[Sch1] C. Scheiderer: Sums of squares of regular functions on real algebraic varieties. *Trans. Amer. Math. Soc.* **352** (1999) no. 3, 1039-1069.

[Sch2] C. Scheiderer: On sums of squares in local rings. *J. Reine Angew. Math.* **540** (2001), 205-227.

[Si] Y.T. Siu: Hilbert's Nullstellensatz in global complex-analytic case. *Proc. Amer. Math. Soc.* **19** (1969), 296–298.

[St] G. Stengle: A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Math. Annalen.* **207** (1974), 87-97.

[Stu] C. Sturm: Mémoire sur la résolution des équations numériques. *Inst. France Sc. Math. Phys.* **6** (1835).

[T] A. Tarski: A decision method for elementary algebra and geometry. Prepared for publication by J.C.C. Mac Kinsey, Berkeley: 1951.