CHAPTER 1

Positive Polynomials and Sums of Squares

This chapter provides the reader with a first look at the subject, and introduces some of the main ideas. We consider the basic question of when a non-negative polynomial is a sum of squares (of polynomials in Sections 1.2 and 1.3, rational functions in Section 1.4, and formal power series in Section 1.6). Examples and counterexamples are provided. We introduce the reader to Tarski's Transfer Principle, see 1.4.2, which plays an important role in what we are doing. As a first application, we explain how it can be used to solve Hilbert's 17th Problem, see 1.4.1. Tarski's Transfer Principle indicates the importance of having a good understanding of orderings on fields. The Baer-Krull Theorem, see 1.5.2, explains how orderings arise from valuations.

1.1 Preliminaries on Polynomials

We denote the polynomial ring $\mathbb{R}[X_1, \ldots, X_n]$ by $\mathbb{R}[\underline{X}]$ for short.

1.1.1 PROPOSITION. *If $f \in \mathbb{R}[\underline{X}]$, $f \neq 0$, then there exists a point $x \in \mathbb{R}^n$ such that $f(x) \neq 0$.*

PROOF. For $n = 1$ this follows from the well-known fact that a non-zero polynomial in one variable has only finitely many roots. For $n > 1$ it follows by induction on n, using $\mathbb{R}[X_1, \ldots, X_n] = \mathbb{R}[X_1, \ldots, X_{n-1}][X_n]$: Since $f \neq 0$, f decomposes as

$$f = g_0 + g_1 X_n + \cdots + g_k X_n^k,$$

$g_0, \ldots, g_k \in \mathbb{R}[X_1, \ldots, X_{n-1}]$, $g_k \neq 0$. By induction on n, there exists a point $(x_1, \ldots, x_{n-1}) \in \mathbb{R}^{n-1}$ such that $g_k(x_1, \ldots, x_{n-1}) \neq 0$. Then

$$f(x_1, \ldots, x_{n-1}, X_n) = \sum_{i=0}^{k} g_i(x_1, \ldots, x_{n-1}) X_n^i$$

is a non-zero polynomial in the single variable X_n, so, by the case $n = 1$, there exists $x_n \in \mathbb{R}$ such that $f(x_1, \ldots, x_n) \neq 0$. □

In fact, one can do much better. A simple modification of this same proof shows the following:

1.1.2 PROPOSITION. *If $f \in \mathbb{R}[\underline{X}]$, $f \neq 0$, then the set*

$$\mathbb{R}^n \setminus \mathcal{Z}(f) = \{x \in \mathbb{R}^n \mid f(x) \neq 0\}$$

is dense in $\mathbb{R}^n$.

PROOF. Exercise. □

The degree of the monomial $cX_1^{d_1}\cdots X_n^{d_n}$ ($c \in \mathbb{R}$, $c \neq 0$, $d_1, \ldots, d_n \geq 0$) is defined to be $\sum_{i=1}^n d_i$. Each $f \in \mathbb{R}[\underline{X}]$ decomposes (uniquely) as a finite sum of monomials. The degree of f is defined to be the maximum of the degrees of the various monomials appearing in this decomposition. By convention, the degree of the zero polynomial is $-\infty$. If $\deg(f) \leq d$ then, collecting together monomials of the same degree, f decomposes (uniquely) as

$$f = f_0 + f_1 + \cdots + f_d$$

where each $f_i \in \mathbb{R}[\underline{X}]$ is homogeneous of degree i (i.e., a sum of monomials of degree i or the zero polynomial).

1.1.3 COROLLARY. *Suppose $f = f_1^2 + \cdots + f_k^2$, $f_1, \ldots, f_k \in \mathbb{R}[\underline{X}]$, $f_1 \neq 0$. Then*

(1) *$f \neq 0$.*
(2) *$\deg(f) = 2\max\{\deg(f_i) \mid i = 1, \ldots, k\}$.*

PROOF. (1) By 1.1.1 there exists $x \in \mathbb{R}^n$ such that $f_1(x) \neq 0$. Then

$$f(x) = f_1(x)^2 + \cdots + f_k(x)^2 > 0$$

so $f \neq 0$. (2) Decompose f_i as $f_i = f_{i0} + \cdots + f_{id}$, where f_{ij} homogeneous of degree j, $d := \max\{\deg(f_i) \mid i = 1, \ldots, k\}$. Clearly $\deg(f) \leq 2d$ and the homogeneous part of degree $2d$ of f is $f_{1d}^2 + \cdots + f_{kd}^2$. Since $f_{id} \neq 0$ for some i, this is not zero, by (1). □

1.2 Positive Polynomials

For $f \in \mathbb{R}[\underline{X}]$:

— We write $f \geq 0$ on $\mathbb{R}^n$ to indicate that $f(x) \geq 0$ for all $x \in \mathbb{R}^n$.

— We write $f > 0$ on $\mathbb{R}^n$ to indicate that $f(x) > 0$ for all $x \in \mathbb{R}^n$.

Obviously, if f is a sum of squares, say $f = f_1^2 + \cdots + f_k^2$, then

$$f(x) = f_1(x)^2 + \cdots + f_k(x)^2 \geq 0$$

for all $x \in \mathbb{R}^n$. It is natural to ask the following:

QUESTION. Is the converse true, i.e., is it true that $f \geq 0$ on $\mathbb{R}^n \Rightarrow f$ is a sum of squares in $\mathbb{R}[\underline{X}]$?

This is easily seen to be the case if $n = 1$. In fact, we have the following:

1.2.1 PROPOSITION. *Suppose f is a non-zero polynomial in the single variable X, and let*

$$f = d\prod_i (X - a_i)^{k_i} \prod_j ((X - b_j)^2 + c_j^2)^{\ell_j}$$

be the factorization of f into irreducibles in $\mathbb{R}[X]$. Then the following are equivalent:

(1) *$f \geq 0$ on $\mathbb{R}$.*
(2) *$d > 0$ and each k_i is even.*
(3) *$f = g^2 + h^2$ for some $g, h \in \mathbb{R}[X]$.*

PROOF. (1) $\Rightarrow$ (2) is clear. For (2) $\Rightarrow$ (3), use the 'two squares identity'

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

(3) $\Rightarrow$ (1) is obvious. □

The answer is 'no' if $n \geq 2$. This was known already to Hilbert in 1888 [Hil1] although his proof was non-constructive. A concrete example was given by Motzkin in 1967 [Mot]. The Motzkin example is

$$s(X,Y) = 1 - 3X^2Y^2 + X^2Y^4 + X^4Y^2.$$

1.2.2 PROPOSITION. *For s as above:*
(1) *$s \geq 0$ on $\mathbb{R}^2$.*
(2) *s is not a sum of squares in $\mathbb{R}[X,Y]$.*

PROOF. (1) follows from the standard inequality

$$\frac{a+b+c}{3} \geq \sqrt[3]{abc} \text{ (if } a,b,c \geq 0)$$

relating the arithmetic mean and the geometric mean, taking $a=1$, $b=x^2y^4$, and $c=x^4y^2$.

For (2) we use brute force. Suppose, to the contrary, that $s = \sum f_i^2$ for some polynomials $f_i \in \mathbb{R}[X,Y]$. By 1.1.3(2), each f_i can have degree at most 3, so is some real linear combination of

$$1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, Y^3.$$

If X^3 appears in some f_i, then X^6 would appear in s with positive coefficient. Thus X^3 does not appear. Similarly, Y^3 does not appear. Arguing in the same way, we see that X^2 and Y^2 do not appear, and finally that X and Y do not appear. Thus f_i has the form

$$f_i = a_i + b_iXY + c_iX^2Y + d_iXY^2.$$

But then $\sum b_i^2 = -3$, a contradiction. □

1.2.3 REMARKS.

(1) The minimum value of s on $\mathbb{R}^2$ is zero. This occurs at each of the four points $(\pm 1, \pm 1)$. Refer to Figure 1.

(2) In fact, one can show that $N+s$ is not a sum of squares in $\mathbb{R}[X,Y]$, for any real constant N. The argument is exactly the same.

(3) In addition to the Motzkin example, many other examples have been considered. These include examples of Robinson in 1969 [Ro]; the Choi-Lam example

$$q(X,Y,Z) = 1 + X^2Y^2 + Y^2Z^2 + Z^2X^2 - 4XYZ$$

in 1977 [C-L]; the Schmüdgen example in 1979 [Sm1]

$$r(X,Y) = 200[(X^3-4X)^2+(Y^3-4Y)^2]+(Y^2-X^2)X(X+2)[X(X-2)+2(Y^2-4)]$$

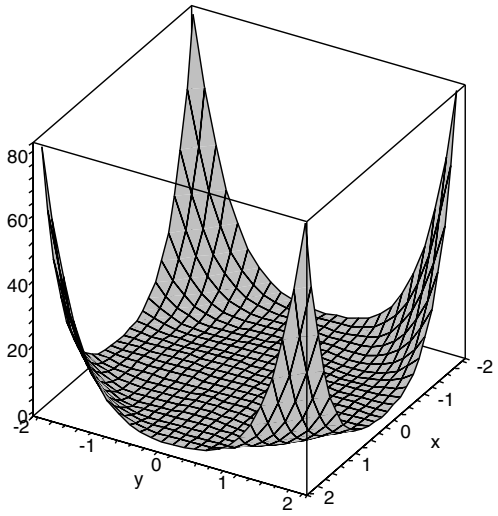

FIGURE 1. $s(X,Y) = 1 - 3X^2Y^2 + X^2Y^4 + X^4Y^2$

(produced without prior knowledge of earlier explicit examples); and the modified Motzkin example

$$p(X,Y) = 1 - X^2Y^2 + X^4Y^2 + X^2Y^4$$

given by Berg, Christensen and Jensen in 1979 [B-C-J]. Note that

$$p(X,Y) = \frac{1}{27}(26 + s(\sqrt{3}X, \sqrt{3}Y)).$$

(4) Although s is not a sum of squares of polynomials, it is a sum of 4 squares of rational functions, for example:

$$\begin{aligned} s =& \frac{X^2Y^2(X^2+Y^2+1)(X^2+Y^2-2)^2 + (X^2-Y^2)^2}{(X^2+Y^2)^2} \\ =& [\frac{X^2Y(X^2+Y^2-2)}{X^2+Y^2}]^2 + [\frac{XY^2(X^2+Y^2-2)}{X^2+Y^2}]^2 \\ &+ [\frac{XY(X^2+Y^2-2)}{X^2+Y^2}]^2 + [\frac{X^2-Y^2}{X^2+Y^2}]^2. \end{aligned}$$

(The first term in the numerator gives rise to the first three squares. The last term gives the final square.) This decomposition was pointed out to the author by M. Bremner.

Hilbert worked with homogeneous polynomials. Homogeneous polynomials are also called *forms*. Why did Hilbert restrict to this case? If f is any polynomial in $\mathbb{R}[\underline{X}]$ of degree $\leq d$, then

$$\overline{f}(X_0, \ldots, X_n) = X_0^d f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$$

(called the homogenization of f) is homogeneous of degree d in the $n+1$ variables $X_0, \ldots, X_n$. If $f(X_1, \ldots, X_n) = \sum c X_1^{d_1} \cdots X_n^{d_n}$, then

$$\begin{aligned}\overline{f}(X_0, \ldots, X_n) &= X_0^d \sum c (\frac{X_1}{X_0})^{d_1} \cdots (\frac{X_n}{X_0})^{d_n} \\ &= \sum c X_0^{d - \sum d_i} X_1^{d_1} \cdots X_n^{d_n} \\ &= \sum c X_0^{d_0} X_1^{d_1} \cdots X_n^{d_n},\end{aligned}$$

where $d_0 := d - \sum d_i$.

1.2.4 PROPOSITION. *Let $V_{d,n}$ = the vector space of all polynomials of degree $\leq d$ in n variables with coefficients in $\mathbb{R}$, $F_{d,n}$ = the vector space of forms of degree d in n variables with coefficients in $\mathbb{R}$. $f \mapsto \overline{f}$ defines a vector space isomorphism from $V_{d,n}$ onto $F_{d,n+1}$. If d is even, then $f \geq 0$ on $\mathbb{R}^n$ iff $\overline{f} \geq 0$ on $\mathbb{R}^{n+1}$, and f is a sum of squares of polynomials iff $\overline{f}$ is a sum of squares of forms of degree $\frac{d}{2}$ (iff $\overline{f}$ is a sum of squares of polynomials).*

PROOF. One checks easily that the map $f \to \overline{f}$ is linear. Since it sends the basis $X_1^{d_1} \cdots X_n^{d_n}$, $\sum d_i \leq d$ of $V_{d,n}$ to the basis $X_0^{d_0} X_1^{d_1} \cdots X_n^{d_n}$, $\sum d_i = d$ of $F_{d,n+1}$, it is a vector space isomorphism. Suppose d is even, $\deg(f) \leq d$. To prove $\overline{f} \geq 0$ on $\mathbb{R}^{n+1} \Rightarrow f \geq 0$ on $\mathbb{R}^n$, use $f(x_1, \ldots, x_n) = \overline{f}(1, x_1, \ldots, x_n)$. To prove $f \geq 0$ on $\mathbb{R}^n \Rightarrow \overline{f} \geq 0$ on $\mathbb{R}^{n+1}$, use $\overline{f}(x_0, \ldots, x_n) = x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$, if $x_0 \neq 0$, and $\overline{f}(0, x_1, \ldots, x_n) = \lim_{\epsilon \to 0} \overline{f}(\epsilon, x_1, \ldots, x_n)$, if $x_0 = 0$. If $f = \sum_{i=1}^k f_i^2$, then $\deg(f_i) \leq \frac{d}{2}$, by 1.1.3, and $\overline{f} = \sum_{i=1}^k [X_0^{d/2} f_i(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})]^2$, which is a sum of squares of forms of degree $\frac{d}{2}$. If $\overline{f} = \sum_{i=1}^k g_i^2$, then $f = \overline{f}(1, X_1, \ldots, X_n) = \sum_{i=1}^k g_i(1, X_1, \ldots, X_n)^2$. □

1.2.5 REMARK. Counting the number of monomials $X_1^{d_1} \cdots X_n^{d_n}$, $\sum d_i \leq d$, one sees that

$$\dim(V_{d,n}) = \dim(F_{d,n+1}) = \binom{d+n}{n} = \binom{d+n}{d} \quad \text{(Exercise)}.$$

We say $f \in \mathbb{R}[\underline{X}]$ is *positive semidefinite* (on $\mathbb{R}^n$) if $f \geq 0$ on $\mathbb{R}^n$. For $d, n \geq 1$, denote by $P_{d,n}$ the subset of the vector space $F_{d,n}$ consisting of forms of degree d in n variables which are positive semidefinite, and by $\Sigma_{d,n}$ the subset of $P_{d,n}$ consisting of sums of squares. The case where d is odd is not interesting. In his 1888 paper [Hil1], Hilbert proved the following:

1.2.6 THEOREM. *For d even, $P_{d,n} = \Sigma_{d,n}$ iff $n \leq 2$ or $d = 2$ or ($n = 3$ and $d = 4$).*

PROOF. Applying 1.2.4, we see that the homogenized Motzkin polynomial

$$X^6 s(\frac{Y}{X}, \frac{Z}{X}) = X^6 + Y^4 Z^2 + Y^2 Z^4 - 3X^2 Y^2 Z^2$$

is in $P_{6,3} \setminus \Sigma_{6,3}$. Similarly, the homogenized Choi-Lam polynomial

$$W^4 q(\frac{X}{W}, \frac{Y}{W}, \frac{Z}{W}) = W^4 + X^2 Y^2 + Y^2 Z^2 + Z^2 X^2 - 4WXYZ$$

is in $P_{4,4}\backslash\Sigma_{4,4}$. More generally, if $d \geq 6$ and $n \geq 3$, then $X_1^d s(\frac{X_2}{X_1}, \frac{X_3}{X_1})$ is in $P_{d,n}\backslash\Sigma_{d,n}$ and, if $d \geq 4$ and $n \geq 4$, then $X_1^d q(\frac{X_2}{X_1}, \frac{X_3}{X_1}, \frac{X_4}{X_1})$ is in $P_{d,n} \setminus \Sigma_{d,n}$. $P_{d,1} = \Sigma_{d,1}$ is trivial. $P_{d,2} = \Sigma_{d,2}$ is immediate from 1.2.1 (using 1.2.4). $P_{2,n} = \Sigma_{2,n}$ follows from 0.2.1 : Any quadratic form is expressible as

$$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j,$$

where $A = (a_{ij})$ is a symmetric matrix. If $f \geq 0$ on $\mathbb{R}^n$, then the matrix A is PSD, so A factors as $A = U^T U$ and

$$f(\underline{X}) = \underline{X}^T A \underline{X} = \underline{X}^T U^T U \underline{X} = (U\underline{X})^T (U\underline{X}) = \|U\underline{X}\|^2,$$

which is a sum of squares of linear forms. (To make sense of this, one needs to view $\underline{X}$ as a column vector.) It remains to show that $P_{4,3} = \Sigma_{4,3}$. This is non-trivial. See [B-C-R, Prop. 6.4.4] for the proof. □

The sets $P_{d,n}$ and $\Sigma_{d,n}$ are closed under addition and multiplication by positive reals, i.e., they are cones in the vector space $F_{d,n}$. See the book of Reznick [R1] for some basic properties of these cones and for additional references.

In a recent paper, Blekherman [Bl] defines a certain natural probability measure on $F_{d,n}$ and estimates the probability of an element of $P_{d,n}$ being in $\Sigma_{d,n}$. His results show that for fixed (even) $d \geq 4$ this approaches zero as $n \to \infty$. The methods of [Bl] do not generate explicit examples of nonnegative polynomials which are not sums of squares.

1.3 Extending Positive Polynomials

Another way of building examples is described by Scheiderer in [S1]. Recall that, for any subset C of $\mathbb{R}^n$, $\mathcal{I}(C)$ denotes the ideal of $\mathbb{R}[\underline{X}]$ consisting of all polynomials vanishing on C. Let $I = \mathcal{I}(C)$. The factor ring $\frac{\mathbb{R}[\underline{X}]}{I}$ is naturally identified with the ring of all polynomial functions from C to $\mathbb{R}$. In other words, $f, g \in \mathbb{R}[\underline{X}]$ define the same function on C iff $f \equiv g \mod I$.

1.3.1 Theorem. *If $C \subseteq \mathbb{R}^n$ is a non-singular irreducible algebraic curve and $f_0 \in \mathbb{R}[\underline{X}]$ is ≥ 0 on C, then there exists $f \in \mathbb{R}[\underline{X}]$ such that $f = f_0$ on C and $f \geq 0$ on $\mathbb{R}^n$.*

Proof. Omitted. See [S1, Th. 5.6]. □

An obvious necessary condition for f to be a sum of squares in $\mathbb{R}[\underline{X}]$ is that $f + I$ (the image of f in $\frac{\mathbb{R}[\underline{X}]}{I}$ under the natural homomorphism) is a sum of squares in $\frac{\mathbb{R}[\underline{X}]}{I}$. Thus, if we can produce $f_0 \in \mathbb{R}[\underline{X}]$, $f_0 \geq 0$ on C, such that $f_0 + I$ is not a sum of squares in $\frac{\mathbb{R}[\underline{X}]}{I}$, then, by 1.3.1, we have produced $f \in \mathbb{R}[\underline{X}]$, $f \geq 0$ on $\mathbb{R}^n$, which is not a sum of squares in $\mathbb{R}[\underline{X}]$. See [S1, Sect. 3] for examples of curves for which this method applies.

1.3.2 Example. Let C be the elliptic curve $Y^2 = X^3 + X$ in $\mathbb{R}^2$, see Figure 2, and let $I = \mathcal{I}(C)$. The polynomial X is obviously ≥ 0 on C. Take

$$t(X, Y) := Y^2 - X^3 + \frac{1}{2}(Y^2 - X^3 - X)^2 = X + g(X, Y) + \frac{1}{2} g(X, Y)^2$$

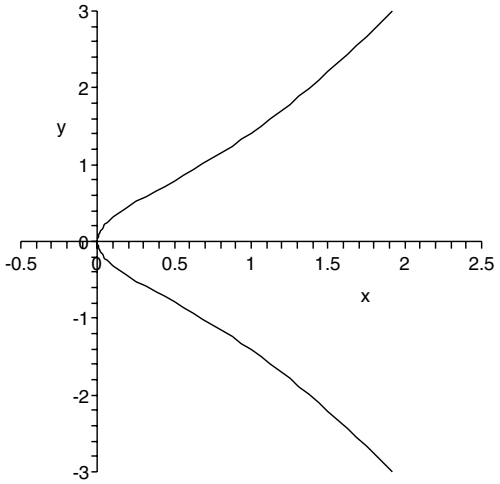

FIGURE 2. $Y^2 = X^3 + X$

where $g(X,Y) := Y^2 - X^3 - X$. See Figure 3. Since $g = 0$ on C, it is clear that $t = X$ on C. We prove that $t \geq 0$ on $\mathbb{R}^2$ and that $X + I$ is not a sum of squares in $\frac{\mathbb{R}[X,Y]}{I}$ (so t is not a sum of squares in $\mathbb{R}[X,Y]$).

Claim 1. $t \geq 0$ on $\mathbb{R}^2$.

PROOF. Let $(x,y) \in \mathbb{R}^2$. If $x \geq \frac{1}{2}$ then $t(x,y) \geq \frac{1}{2} + g(x,y) + \frac{1}{2}g(x,y)^2 = \frac{1}{2}(1 + g(x,y))^2 \geq 0$. At the same time, $x + g(x,y) = y^2 - x^3$, so, if $y^2 \geq x^3$, then $t(x,y) = y^2 - x^3 + \frac{1}{2}g(x,y)^2 \geq 0$. Thus, if t is negative at some point, then this point is in the bounded set

$$\{(x,y) \in \mathbb{R}^2 \mid y^2 < x^3,\ 0 < x < \frac{1}{2}\},$$

and t achieves its minimum value on this set. Say the minimum value of t occurs at the point (x,y). The partial derivatives

$$\frac{\partial t}{\partial X} = 1 - (3X^2 + 1)(1 + g), \quad \frac{\partial t}{\partial Y} = 2Y(1 + g)$$

vanish at (x,y). This forces $y = 0$ and

$$\frac{\partial t}{\partial X}(x,0) = 1 - (3x^2 + 1)(1 + (-x^3 - x)) = 3x^5 + 4x^3 - 3x^2 + x = 0$$

which implies in turn (since $x > 0$) that $3x^4 + 4x^2 - 3x + 1 = 0$. Since the polynomial $3X^4 + 4X^2 - 3X + 1$ is strictly positive on $\mathbb{R}$, this is a contradiction. □

Note: $X + g(X,Y) + rg(X,Y)^2$ is ≥ 0 on $\mathbb{R}^2$ when $r \in \mathbb{R}$ is 'large enough'. Claim 1 shows that $r = \frac{1}{2}$ is 'large enough' in this sense. There is no claim that $r = \frac{1}{2}$ is in any way optimal.

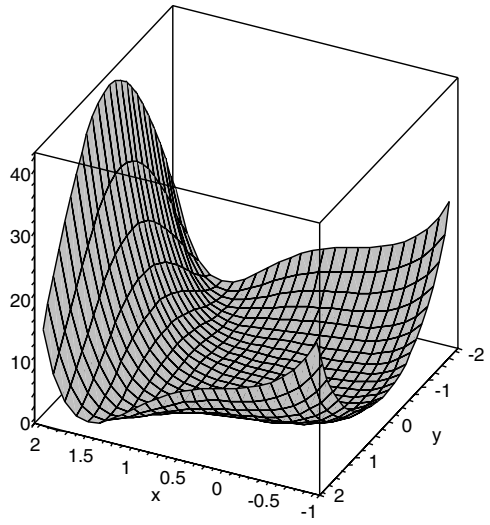

FIGURE 3. $t(X,Y) = Y^2 - X^3 + \frac{1}{2}(Y^2 - X^3 - X)^2$

Claim 2. $I = (g)$, the principal ideal in $\mathbb{R}[X,Y]$ generated by g.

PROOF. Clearly $g \in I$ so $(g) \subseteq I$. The polynomial g is irreducible in $\mathbb{R}[X,Y]$ (it is even irreducible in the ring $\mathbb{R}(X)[Y]$, where $\mathbb{R}(X)$ denotes the field of fractions of the domain $\mathbb{R}[X]$), so the ideal (g) is prime. If $\mathbb{R}$ were algebraically closed, Claim 2 would be immediate from Hilbert's Nullstellensatz. Since this is not the case, we need another argument. Real algebraic geometry provides various tools to deal with this situation, e.g., the Sign-Changing Criterion (See 12.7.1, Appendix 2). Rather than quote this result, we give the following argument, which is elementary: Since g is monic of degree 2, when viewed as a polynomial in Y with coefficients in $\mathbb{R}[X]$, we can divide any h in $\mathbb{R}[X,Y]$ by g to obtain $h = qg + r$ where $q, r \in \mathbb{R}[X,Y]$ and r has degree ≤ 1 in Y, i.e.,

$$r(X,Y) = a(X) + b(X)Y,\ a(X), b(X) \in \mathbb{R}[X].$$

If h vanishes on $Y^2 = X^3 + X$, this yields

$$a(x) \pm b(x)\sqrt{x^3 + x} = 0$$

for each real $x \geq 0$. Adding these equations yields $a(x) = 0$ for each real $x \geq 0$, so $a(X) = 0$. Multiplying these equations yields $a(x)^2 - b(x)^2(x^3 + x) = 0$ for each real $x \geq 0$, i.e., $b(x) = 0$ for each real $x > 0$, so $b(X) = 0$. This proves that $g \mid h$, which completes the proof. □

Claim 3. $X + I$ is not a sum of squares in the ring $\frac{\mathbb{R}[X,Y]}{I}$.

PROOF. We know $I = (g)$, so the ring $\frac{\mathbb{R}[X,Y]}{I}$ is obtained by formally adjoining $Y = \sqrt{X^3 + X}$ to the ring $\mathbb{R}[X]$. Elements of $\frac{\mathbb{R}[X,Y]}{I}$ are represented uniquely by

polynomials of the form $a(X) + b(X)Y$, $a(X), b(X) \in \mathbb{R}[X]$. If $X + I$ were a sum of squares in this ring, then we would have an expression

$$X \equiv \sum_{i=1}^{t} (a_i + b_i Y)^2 \mod I$$

for some $a_i, b_i \in \mathbb{R}[X]$. Expanding, this yields

$$X = \sum_{i=1}^{t} (a_i^2 + b_i^2(X^3 + X)) \text{ (and also } \sum_{i=1}^{t} 2a_i b_i = 0).$$

Since each non-zero a_i^2 has even degree and each non-zero $b_i^2(X^3 + X)$ has odd degree ≥ 3, and since the leading coefficient in each case is positive, this is a contradiction. □

1.4 Hilbert's 17th Problem

As one of his famous set of problems, Hilbert [Hil3] 1900 posed the following:

1.4.1 HILBERT'S 17TH PROBLEM. *For any $f \in \mathbb{R}[\underline{X}]$, is it true that $f \geq 0$ on $\mathbb{R}^n \Rightarrow f$ is a sum of squares of rational functions?*

— This is trivial when $n = 1$.

— Hilbert proved it, already in 1893, in the case $n = 2$ [Hil2].

— Artin proved it in the general case (and with $\mathbb{R}$ replaced by an arbitrary real closed field) in 1927 [A].

Artin's work represented a major breakthough. His proof combined two new ingredients. The first ingredient – a description of elements of a field positive at every ordering – has since developed into the larger subject known as real algebra. The second ingredient – certain 'specialization lemmas' for real closed fields – has evolved over time into what is referred to now as Tarski's Transfer Principle, which is an important result in the model theory of real closed fields.

We recall basic terminology: Let F be a field, $\text{char}(F) \neq 2$. A *preordering* of F is a subset T of F satisfying

$$T + T \subseteq T,\ TT \subseteq T, \text{ and } a^2 \in T \text{ for all } a \in F.$$

$\sum F^2$ denotes the set consisting of all finite sums $\sum a_i^2$, $a_i \in F$. $\sum F^2$ is the unique smallest preordering of F. An *ordering* of F is a subset P of F satisfying

$$P + P \subseteq P,\ PP \subseteq P,\ P \cup -P = F, \text{ and } P \cap -P = \{0\}.$$

Every ordering is a preordering. Orderings are also described as order relations: If P is an ordering of F, the associated order relation $\leq$ on F is defined by $a \leq b$ iff $b - a \in P$. P is recovered from $\leq$ via $P = \{a \in F \mid a \geq 0\}$. An *ordered field* is a pair $(F, \leq)$ where F is a field, and $\leq$ is an ordering on F. The field $\mathbb{R}$, of course, is uniquely ordered.

It is not our plan to say much about the model theory of real closed fields. Here, we simply assume what we need. For what we are doing here, we can get by with the following weak version of Tarski's Transfer Principle, which has the advantage of being easily understood.

1.4.2 Tarski's Transfer Principle. *Suppose $(F, \leq)$ is an ordered field extension of $(\mathbb{R}, \leq)$ and there exists $x = (x_1, \ldots, x_n) \in F^n$ satisfying some finite system of polynomial equations and inequalities with coefficients in $\mathbb{R}$. Then there exists $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ satisfying these same equations and inequalities.*

In fact, 1.4.2 is true with $\mathbb{R}$ replaced by any real closed field. It can be deduced from the Tarski-Seidenberg Theorem [T] 1931 [Sei] 1954. It can also be deduced from Lang's Homomorphism Theorem [La1] 1953. See Appendix 1 for more explanation.

The finite systems of polynomial equations and inequalities in question are expressible in the form

$$f_1 \rhd_1 0 \text{ and } \cdots \text{ and } f_r \rhd_r 0$$

where $f_i \in \mathbb{R}[\underline{X}]$ and $\rhd_i \in \{\geq, >, =, \neq\}$, $i = 1, \ldots, r$.

1.4.3 Remark. Any such system of polynomial equations and inequalities can be written in the form

$$f_1 \geq 0 \text{ and } \cdots \text{ and } f_s \geq 0 \text{ and } g \neq 0$$

for some $f_1, \ldots, f_s, g \in \mathbb{R}[\underline{X}]$. Just replace each equality $g = 0$ in the system by the pair of inequalities $g \geq 0$ and $-g \geq 0$ and each strict inequality $g > 0$ in the system by the pair of inequalities $g \geq 0$ and $g \neq 0$. Finally, replace all inequalities $g_i \neq 0$, $i = 1, \ldots, t$ in the resulting system by the single inequality $\prod_{i=1}^{t} g_i \neq 0$.

A subset of $\mathbb{R}^n$ is called *basic semialgebraic* if it is the set of solutions of such a finite system of polynomial equations and inequalities, and *semialgebraic* if it is a finite union of basic semialgebraic sets. One checks easily that a subset of $\mathbb{R}$ is semialgebraic iff it is a finite union of points and intervals (Exercise).

Assuming Tarski's Transfer Principle, one can prove 1.4.1 as follows:

Proof of 1.4.1. Let f be any element of $\mathbb{R}[\underline{X}]$. Let $F = \mathbb{R}(\underline{X})$, the field of fractions of $\mathbb{R}[\underline{X}]$. Let $T = \sum F^2$. We want to show:

$$f \notin T \Rightarrow f(x) < 0 \text{ for some } x \in \mathbb{R}^n.$$

We use a basic result from real algebra which dates back to work of Artin and Schreier in 1926 [A-S]:

1.4.4 Lemma. *Suppose $f \in F \setminus T$. Let $P \supseteq T$ be any preordering of F maximal such that $f \notin P$. (Such a preordering exists by Zorn's lemma). Then P is an ordering.*

In fact, this result holds for any field F, $\mathrm{char}(F) \neq 2$, any preordering T of F, and any $f \in F \setminus T$. The proof given here is due to Serre 1947 [Se].

Proof.

Claim 1: $-1 \notin P$. For, if $-1 \in P$, then

$$f = (\frac{f+1}{2})^2 + (-1)(\frac{f-1}{2})^2 \in P,$$

a contradiction.

Claim 2: $-f \in P$. For, if $-f \notin P$, consider $P - fP := \{a - fb \mid a, b \in P\}$. The trivial identities

$$\begin{cases} (a_1 - fb_1) + (a_2 - fb_2) = (a_1 + a_2) - f(b_1 + b_2), \\ (a_1 - fb_1)(a_2 - fb_2) = (a_1a_2 + b_1b_2f^2) - f(a_1b_2 + a_2b_1), \\ a = a - (f)(0^2), \\ -f = 0^2 - (f)(1^2) \end{cases}$$

show that $P - fP$ is a preordering containing P properly, so, by the maximality of P, $f \in P - fP$, so $f = a - bf$, $a, b \in P$. Then $(1+b)f = a$, and $1 + b \neq 0$ by Claim 1, so

$$f = \frac{a}{1+b} = (a)(1+b)(\frac{1}{1+b})^2 \in P,$$

a contradiction.

Claim 3: If $g \in F$, $g \notin P$, then $-g \in P$ (so $P \cup -P = F$). For consider $P + gP := \{a + bg \mid a, b \in P\}$. As above, $P + gP$ is a preordering containing P properly, so $f \in P + gP$, so $f = a + bg$, $a, b \in P$. Then $-bg = a + (-f) \in P$ (using Claim 2) and $a - f \neq 0$ (since $f \notin P$), so $b \neq 0$ and

$$-g = \frac{a-f}{b} = (a-f)(b)(\frac{1}{b})^2 \in P.$$

Claim 4: If $g \in P \cap -P$ then $g = 0$ (so $P \cap -P = \{0\}$). For otherwise

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

□

To finish the proof of 1.4.1, let $\leq$ be the order relation on F corresponding to P, i.e., $a \leq b$ iff $b - a \in P$. Since $F = \mathbb{R}(\underline{X})$, F is obviously an extension of $\mathbb{R}$. Since $\mathbb{R}$ is uniquely ordered, the restriction of $\leq$ to $\mathbb{R}$ is the usual ordering on $\mathbb{R}$. Thus $(F, \leq)$ is an ordered field extension of the ordered field $(\mathbb{R}, \leq)$. By construction, $f \notin P$, i.e., $f < 0$. Thus there exists $x = (x_1, ..., x_n) \in F^n$ such that $f(x) < 0$. (Just take $x_i = X_i$, $i = 1, ..., n$. Then $f(x) = f$.) Thus, by Tarski's Transfer Principle, there exists $x \in \mathbb{R}^n$ such that $f(x) < 0$. □

1.4.5 Remark. Various refinements of 1.4.1 have been considered. For example:

(i) Quantitative aspects: How many squares are required? In 1967 Pfister [Pf3] showed that 2^n squares suffice. This is trivial if $n = 1$, and had been proved already in the case $n = 2$ by Hilbert in 1893 [Hil2]. Not surprisingly, the methods here are from quadratic form theory. Pfister's proof uses the theory of multiplicative quadratic forms (now called Pfister forms).

(ii) What can be said if we replace the requirement that $f \geq 0$ on $\mathbb{R}^n$ by some other positivity requirement, e.g., that if $f \geq 0$ on some semialgebraic subset K of $\mathbb{R}^n$? The Krivine's Positivstellensatz [Kr1] (see Chapter 2) and Schmüdgen's Positivstellensatz [Sm2] (see Chapter 6) deal with questions of this type.

We do not consider topic (i) further. Topic (ii) is the main theme of the book. On the other hand, the reader will encounter quadratic form theory (including Pfister forms) in Chapter 8, in connection with the solution of the question of Putinar.