University of Helsinki

Faculty of Science

Department of Mathematics and Statistics

Stability Index of Real Varieties: Theorem of Bröcker and Scheiderer

Author:
Valter Uotila

Supervisor:
Pekka Pankka

January 12, 2022

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty Matemaattis-luonnontieteellinen	Laitos — Institution — Department Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author
Valter Uotila

Työn nimi — Arbetets titel — Title

Stability Index of Real Varieties: Theorem of Bröcker and Scheiderer

Oppiaine — Läroämne — Subject

Matematiikka

Työn laji — Arbetets art — Level Pro gradu -tutkielma	Aika — Datum — Month and year Tammikuu 2022	Sivumäärä — Sidoantal — Number of pages 59 s.

Tiivistelmä — Referat — Abstract

Tässä työssä todistan Bröckerin ja Scheidererin teorian avoimille semi-algebrallisille perusjoukoille. Teoria osoittaa, että jokaiselle reaaliselle algebralliselle varistolle on olemassa yläraja niiden polynomien lukumäärässä, joiden avulla variston osajoukkona olevia avoimia semi-algebrallisia perusjoukkoja määritellään. Tätä lukuarvoa kutsutaan reaalisen variston vakausindeksiksi. Teoria pohjaa suljetuille reaalisille kunnille, jotka yleistävät reaalilukujen kuntaa. Reaalinen algebrallinen varisto on suljetun reaalisen kunnan osajoukko, joka on määritelty polynomiyhtälöiden ratkaisujoukkona.

Jokainen semi-algebrallinen joukko on määritelty Boolen yhdistelmänä äärellisestä määrästä polynomien merkkiehtoja, jotka toteuttavat tietyt yhtäsuuruudet ja epäyhtälöt. Semi-algebralliset perusjoukot ovat ne semi-algebralliset joukot, jotka toteuttavat ainoastaan annetut yhtäsuuruudet ja epäyhtälöt polynomien merkkiehdoissa. Semi-algebrallisista perusjoukoista voidaan siis rakentaa kaikki semi-algebralliset joukot ottamalla perusjoukkojen äärelliset yhdisteet, leikkaukset ja joukkoerotukset.

Tämä työ pyrkii esittämään riittävät esitiedot päätuloksen todistuksen syvällistä ja yksityiskohtaista ymmärtämistä varten. Ensimmäinen luku esittelee ja motivoi tulosta yleisellä tasolla. Toinen luku käsittelee tiettyjä edistyneitä algebrallisia rakenteita, joita vaaditaan päätuloksen todistuksessa. Näitä ovat muun muassa radikaalit, alkuideaalit, assosiatiiviset algebrat, renkaan ulottuvuuden käsite sekä tietyt tekijärakenteet. Kolmas luku määrittelee suljetut reaaliset kunnat ja semi-algebralliset joukot, jotka ovat tämän työn kulmakiviä. Kolmannessa luvussa myös kehitetään neliömuotojen teoriaa. Kolmannen luvun päätulos on Wittin teoria.

Neljäs luku käsittelee Pfisterin muotoja, jotka ovat tietynlaisia neliömuotoja. Työssä määritellään yleiset Pfisterin muodot kuntien yli. Tämän jälkeen kehitään niiden teoriaa rationaalifunktioiden kunnan yli. Viidennessä luvussa esitetään kaksi konstruktiivista esimerkkiä Bröckerin ja Scheidererin teorian käytöstä yhdessä ja kahdessa ulottuvuudessa. Nämä esimerkit edelleen motivoivat tulosta ja sen mahdollisia algoritmisia ominaisuuksia. Työn päätteeksi todistetaan Bröckerin ja Scheidererin teoria, joka osoittaa, että reaalisen variston vakausindeksi on olemassa ja se on äärellinen kaikille reaalisille varistoille.

Avainsanat — Nyckelord — Keywords
Bröckerin and Scheidererin teoria, suljetut reaaliset kunnat, semi-algebrallinen geometria, Pfister muodot

Säilytyspaikka — Förvaringsställe — Where deposited
Helsingin yliopiston digitaalinen arkisto E-thesis

Muita tietoja — Övriga uppgifter — Additional information

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty Faculty of Science	Laitos — Institution — Department Department of Mathematics and Statistics

Tekijä — Författare — Author
Valter Uotila

Työn nimi — Arbetets titel — Title

Stability Index of Real Varieties: Theorem of Bröcker and Scheiderer

Oppiaine — Läroämne — Subject
Mathematics

Työn laji — Arbetets art — Level Master's thesis	Aika — Datum — Month and year January 2022	Sivumäärä — Sidoantal — Number of pages 59 pages

Tiivistelmä — Referat — Abstract

In this work, I prove the theorem of Bröcker and Scheiderer for basic open semi-algebraic sets. The theorem provides an upper bound for a stability index of a real variety. The theory is based on real closed fields which generalize real numbers. A real variety is a subset of a real closed field that is defined by polynomial equalities. Every semi-algebraic set is defined by a boolean combination of polynomial equations and inequalities of the sign conditions involving a finite number of polynomials. The basic semi-algebraic sets are those semi-algebraic sets that are defined solely by the sign conditions. In other words, we can construct semi-algebraic sets from the basic semi-algebraic sets by taking the finite unions, intersections, and complements of the basic semi-algebraic sets.

Then the stability index of a real variety indicates the upper bound of numbers of polynomials that are required to express an arbitrary semi-algebraic subset of the variety. The theorem of Bröcker and Scheiderer shows that such upper bound exists and is finite for basic open semi-algebraic subsets of a real variety.

This work aims to be detailed in the proofs and represent sufficient prerequisites and references. The first chapter introduces the topic generally and motivates to study the theorem. The second chapter provides advanced prerequisites in algebra. One of such results is the factorial theorem of a total ring of fractions. Other advanced topics include radicals, prime ideals, associative algebras, a dimension of a ring, and various quotient structures.

The third chapter defines real closed fields and semi-algebraic sets that are the fundamental building blocks of the theory. The third chapter also develops the theory of quadratic forms. The main result of this chapter is Witt's cancellation theorem. We also shortly describe the Tsen-Lang theorem.

The fourth chapter is about Pfister forms. Pfister forms are special kinds of quadratic forms that we extensively use in the proof of the main theorem. First, we define general Pfister forms over fields. Then we develop their theory over the fields of rational functions. Generally, Pfister forms share multiple similar properties as quadratic forms.

The fifth chapter represents one- and two-dimensional examples of the main theorem. These examples are based on research that is done on constructive approaches to the theorem of Bröcker and Scheiderer. The examples clarify and motivate the result from an algorithmic perspective. Finally, we prove the main theorem of the work. The proof is heavily based on Pfister forms.

Avainsanat — Nyckelord — Keywords
theorem of Bröcker and Scheiderer, real closed field, semi-algebraic geometry, Pfister forms

Säilytyspaikka — Förvaringsställe — Where deposited
Electronic thesis archive E-thesis

Muita tietoja — Övriga uppgifter — Additional information

Contents

Chapter 1

Introduction

1.1 Foreword

One of the most beautiful results in the field of semi-algebraic geometry is the theorem of Bröcker and Scheiderer. The theorem sets upper bounds for the so-called stability index of real varieties. Semi-algebraic geometry is a sort of relaxed version of algebraic geometry. In algebraic geometry, we study polynomial equalities, whereas in semi-algebraic geometry we study polynomial inequalities. Since inequalities can be used to represent equalities, in some sense semi-algebraic geometry subsumes algebraic geometry. Many theorems in algebraic and semi-algebraic geometry overlap. For example, the definition of the dimension is the same for algebraic and semi-algebraic sets in this work.

Semi-algebraic geometry is strongly connected to real closed fields. If a field is real, it roughly means that it resembles real numbers. A field is real closed if it cannot be extended into a larger real field. Instead of developing semi-algebraic geometry in real numbers, we develop the theory in a more general setting considering real closed fields.

Let $\mathcal{R}$ be a real closed field. We define a real variety to be the subset $V \subset \mathcal{R}^n$ which is a solution set for some polynomial equalities. Our main object is to study sets of form

$$S = \{x \in V \mid f_1(x) > 0, \dots, f_k(x) > 0\}$$

and

$$\bar{S} = \{x \in V \mid f_1(x) \geq 0, \dots, f_k(x) \geq 0\},$$

where $f_1, \dots, f_n \in \mathcal{R}[X_1, \dots, X_n]$ are polynomials in n variables with coefficients in $\mathcal{R}$. The sets like S are called basic *open* semi-algebraic sets and respectively sets like $\bar{S}$ are called basic *closed* semi-algebraic sets. Now the fascinating result of Bröcker and Scheiderer is the following.

Theorem 1.1.1 (Theorem of Bröcker and Scheiderer for basic open semi-algebraic sets)**.** *Let V be an algebraic subset of $\mathcal{R}^n$ with dimension $d > 0$. Then* *every basic open semi-algebraic subset $U \subset V$ can be defined by d simultaneously strict inequalities. In other words, if $k > 0$ and*

$$U = \{x \in V \mid g_1(x) > 0, \ldots, g_k(x) > 0\}$$

where $g_i \in \mathcal{R}[X_1, \ldots, X_n]$ for $1 \leq i \leq k$, then there exist $f_1, \ldots, f_d \in \mathcal{P}(V)$ so that

$$U = \mathcal{U}(f_1, \ldots, f_d) = \{x \in V \mid f_1(x) > 0, \ldots, f_d(x) > 0\}.$$

In this work we consider the theorem of Bröcker and Scheiderer for basic open semi-algebraic sets. On the other hand, there is a similar result for basic closed semi-algebraic sets. In other words, we can state the content of these two theorems in the following way.

Theorem 1.1.2. *For an algebraic variety V the number of polynomials, which represent a non-empty basic semi-algebraic set $S \subset V$ (or $\bar{S} \subset V$), is finite and bounded.*

Even if the constant k in the definitions of S and $\bar{S}$ is large, we can always theoretically reduce the number of polynomials under the bounds. The theorem consists of two parts which provide two upper bounds depending if the semi-algebraic set is basic open or basic closed. Besides, these bounds are proved to be tight and they only depend on the dimension of the algebraic variety V.

The theorem of Bröcker and Scheiderer is a deep result. In this work, we prove the result for basic open semi-algebraic sets. To prove the result for the basic closed semi-algebraic sets requires surprisingly much machinery from semi-algebraic geometry and a real spectrum. This work aims to be self-sufficient and to provide a comprehensive introduction to the theorem with suitable prerequisites in semi-algebraic geometry. We demonstrate the main theorem with simple one- and two-dimensional examples to illustrate how it works in the low-dimensional cases. This work also represents some of the most important literature related to the theorem.

1.2 Motivation of theorem of Bröcker and Scheiderer

In 2018 I started as a summer intern at the Unified Database Management Systems research group in the University of Helsinki. The problem we researched was a classical relational database problem. We wanted to estimate size bounds of conjunctive queries when they are executed over a relational instance. The problem is relatively well-studied [1, 2] and it was already partially solved. Basically, the size bound can be solved in such cases when we do not have functional dependencies or we have a single functional dependency between tables in a relational database. The general case of arbitrary functional dependencies appeared to be hard.

In [1] the authors formulated solutions to the two simple cases based on a so-called coloring number which is a simplified version of the information theoretical entropy. In the case of arbitrary functional dependencies they formulated the size bound problem using entropy. Practically all the formulations produced a linear programming problem. The solution to the linear program provides the optimal exponent to a certain size bound inequality. Although the solution to the general case is theoretically accurate, it has a problem related to the information theoretical entropy. This problem makes the proposed solution practically infeasible to solve.

Of course, this is just one example where the linear programming problems become combinatorically very challenging because of a huge number of constraints. It should be easy to find other examples everywhere in science. Any of these examples motivates to study and understand the theorem of Bröcker and Scheiderer. The theorem states that there always exists relatively few constraints which describe the same linear program. The "relatively few constraints" means that the number of the constraints depends on the dimension of the space. Still, the reformulation of the constraints might not be useful because the constraints become non-linear and infeasible large.

The practical problem in the theorem of Bröcker and Scheiderer is that it is purely existential result. It does not provide an algorithm to perform the reduction of inequalities. Anyway, we will study of one constructive algorithm in the two-dimensional space. It is an open question if such algorithm exists for higher dimensions. Developing such algorithm would require very throughout understanding of the theorems and their proofs. One of the motivations behind this work is to open the proof of the theorem of Bröcker and Scheiderer in a way which would enable better understanding and provide algorithmic methods to reduce the number of polynomials.

Chapter 2

Introduction to algebra

2.1 Basics of algebra and radicals

This section introduces some selected and advanced concepts from algebra that are used throughout the work. We assume that the reader is familiar with the basics of algebra such as monoids, groups, rings, ideals, maximal ideals, fields, modules, and various homomorphisms related to these structures. In this section, we assume that rings are always commutative. The content of this section is based on [3] which is also a comprehensive introduction to algebra.

Definition 2.1.1 (Integral domain)**.** Let I be a ring and $a, b, c \in I$ and $a \neq 0$. The ring I is an *integral domain* if the property $ab = ac$, implies $b = c$.

Definition 2.1.2 (Generating set)**.** A set S is a *generating set* of a ring A if A is the intersection of all the rings containing the set S. An element of the set S is called a *generator*.

Definition 2.1.3 (Zero divisor)**.** Let A be a commutative ring. An element $a \in A$ is a *zero divisor* if there exists a nonzero $x \in A$ such that $ax = 0$.

Definition 2.1.4 (Characteristic of ring or field)**.** Let R be a ring (or a field), 1 be its neutral element of multiplication and 0 be its neutral element of addition. If n is the smallest positive number for which $\sum_0^n 1 = 0$, then the *characteristic* of R is n. If there does not exist such a number, the characteristic of R is 0.

When we will study quadratic forms in the following chapters, we utilize some basic properties of radicals. Informally, we can describe radicals as ideals that contain ”not-good” elements of the underlying ring. Radicals are represented as classes that are homomorphically closed, closed under extensions, and they satisfy a certain inductive property. The following definition is from [4].

Definition 2.1.5 (Radical class of rings)**.** A *radical class of rings* is a collection $\mathcal{A}$ of rings so that the following properties are satisfied:

1. The collection $\mathcal{A}$ is homomorphically closed. This means that if a ring $A \in \mathcal{A}$ and there exists a ring homomorphism $A \to B$, then $B \in \mathcal{A}$.
2. The collection $\mathcal{A}$ is closed under extensions. This means that if $I_1 \subset \ldots \subset I_k \subset \ldots$ is an ascending chain of ideals of a ring $A \in \mathcal{A}$ and each $I_i \in \mathcal{A}$, then $\cup_i I_i \in \mathcal{A}$.
3. The collection $\mathcal{A}$ has an inductivity property. This means that if I is an ideal of the ring A and both $I \in \mathcal{A}$ and $A/I \in \mathcal{A}$, then $A \in \mathcal{A}$.

A ring A is called *radical* if it belongs to some radical class of rings.

Definition 2.1.6 (Nilpotent element)**.** Let A be a ring. An element $x \in A$ is *nilpotent* if $x^n = 0$ for some $n > 0$.

The following radical serves as an example of a radical and we will utilize it later in this work.

Definition 2.1.7 (Nilradical of ring)**.** A *nilradical* N of a ring A is the ideal consisting of nilpotent elements i.e.

$$N = \{x \in A \mid x^n = 0 \text{ for some } n > 0\}.$$

The nilradical of a ring is also sometimes called Köthe's nilradical. Historically it is the first radical that was found in 1930 by Austrian mathematician Gottfried Köthe. For the proof that the nilradical is a radical see Example 2.1.6 in [4].

2.2 Special ideals, dimension and R-algebras

This section introduces some special ideals such as prime ideals and real ideals.

The concept of a dimension is important throughout this work. In some sense, there exists a foundational definition for the dimension in algebra which we represent in this subsection. Usually, the dimension is tied to the length or size of certain elements in the bases. In our algebraic definition, the dimension is connected to the length of prime ideal chains.

In the end of this subsection, we define and discuss the basics of R-algebras. The content of this subsection is based on [3, 5].

Definition 2.2.1 (Prime ideal)**.** Let I be an ideal of a commutative ring A. The ideal I is a *prime ideal* if it holds that whenever $ab \in I$, then either $a \in I$ or $b \in I$ and $I \neq A$.

Definition 2.2.2 (Minimal and maximal ideals)**.** An ideal I of a ring A is *minimal* (resp. *maximal*) if it is minimal (resp. maximal) in the set of ideals of A ordered by set inclusion.

Definition 2.2.3 (Real ideal)**.** An ideal I of a commutative ring A is called *real* if the following condition holds for all elements $a_1, \dots, a_n \in A$:

$$a_1^2 + \ldots + a_n^2 \in I \Rightarrow a_i \in I \text{ for } i = 1, \dots, n.$$

Based on prime ideals, we define a dimension of a ring. In many cases the dimension of a ring is infinite. The dimension of a ring will be the foundational definition for any dimension concept which appears in this work.

Definition 2.2.4 (Dimension of ring)**.** Let A be a ring. We define that a prime ideal chain $I_0 \subsetneq \ldots \subsetneq I_n$, where $I_0, \dots, I_n$ are prime ideals of the ring A, has a length n. Note that the number n is the number of strict inclusions in the chain, not the number of prime ideals. The *dimension* $\dim(A)$ *of the ring* A is the supremum over all the lengths of the prime ideal chains of the ring A. The dimension of a ring is also often called the *Krull dimension.*

Next we proceed to R-algebras. See Chapter 15, Section 6 in [3] for more details about R-algebras.

Definition 2.2.5 (R-algebra i.e. associative algebra)**.** Let R be a commutative ring. An *associative* R*-algebra* A is a ring that also has R-module structure. In R-algebra the ring addition and module addition are the same operation. Besides R-algebra A satisfies

$$r \cdot (xy) = (r \cdot x)y = x(r \cdot y)$$

for all $r \in R$ and $x, y \in A$. An R-algebra of *finite type* is an R-algebra that has finitely many generators. Recall Definition 2.1.2 of generators.

Equivalently, an R-algebra A is a ring together with a ring homomorphism $h\colon R \to Z(A)$ where $Z(A)$ the center of A. The center of A consists of the elements which commute with respect to the multiplication in A. Then the scalar multiplication $\cdot$ of the R-module structure is defined by $r \cdot x = h(r)x$.

Let A be a finitely generated R-algebra with $a_1, \dots, a_n$ as generators. Then there exists an algebra homomorphism $f\colon R[X_1, \dots, X_n] \to A$ so that coefficients of a polynomial $p \in R[X_1, \dots, X_n]$ are mapped using the ring homomorphism $h\colon R \to Z(A)$ in Definition 2.2.5 and the variables x_i are mapped to the generators a_i, for $i = 1, \dots, n$. The algebra homomorphism f is surjective.

Definition 2.2.6 (R-algebra homomorphism)**.** Let A_1 and A_2 be two R-algebras. An R-algebra homomorphism $\phi\colon A_1 \to A_2$ is the R-linear ring homomorphism that satisfies properties

- $\phi(r \cdot x) = r \cdot \phi(x)$,
- $\phi(x + y) = \phi(x) + \phi(y)$,
- $\phi(xy) = \phi(x)\phi(y)$ and
- $\phi(1_{R_1}) = 1_{R_2}$

for all $r \in R$ and $x, y \in A_1$.

2.3 Quotient structures

Different kinds of quotient structures have an important role in algebra as well as in this work. Along with quotient structures we always have the associated canonical homomorphisms.

Definition 2.3.1 (Quotient ring)**.** Let I be an ideal of a ring A and $a, b \in A$. The *quotient ring* A/I consists of equivalence classes defined by the equivalence relation

$$a \sim b \text{ if and only if } b - a \in I.$$

The corresponding equivalence class is denoted by

$$\bar{a} = a + I = \{a + r \mid r \in I\}.$$

It is a well-known algebraic fact that A/I becomes a ring and that there exists a canonical surjective homomorphism $A \to A/I$ that sends an element of A to the element's equivalence class in A/I.

Using the dimension of a ring in Definition 2.2.4 we define a dimension of an ideal.

Definition 2.3.2 (Dimension of ideal)**.** Let $I \subset A$ be an ideal. The dimension of the ideal I is the dimension of the quotient ring A/I i.e. $\dim(I) = \dim(A/I)$.

Recall Definition 2.2.2 of a maximal ideal.

Definition 2.3.3 (Residue field)**.** Let A be a commutative ring and I a maximal ideal of A. A *residue field of A at I* is the quotient ring A/I.

We do not prove here that when $I \subset A$ is a maximal ideal, the quotient ring A/I becomes a field. For the proof of this result see the section of commutative rings in [3].

Definition 2.3.4 (Field extension)**.** Let L be a field. If $K \subset L$ is a subfield of L, then L is a *field extension of K*. We denote the field extension by L/K.

Definition 2.3.5 (Algebraic extension)**.** A field extension L/K is called *algebraic* if every element of L is algebraic over K. This means that every element of L is a root of a non-zero polynomial with coefficients in K.

Theorem 2.3.1. *The following conditions are equivalent:*

1. *A field F is algebraically closed.*
2. *Every non-constant polynomial of $F[X]$ is a product of linear (first degree) polynomials.*

3. *Every irreducible polynomial in $F[X]$ is linear i.e first degree polynomial.*
4. *Every non-constant polynomial in $F[X]$ has a root in F.*
5. *Every polynomial of prime degree in $F[X]$ has a root in F.*

Proof. See Theorem-Definition 1.23 in [6], and [7] for the last part. □

Definition 2.3.6 (Algebraically independent subset)**.** Let F be a field and $S \subset F$ a subset. The set S is *algebraically independent over* F if for all nonzero polynomials $f \in F[X_1, \dots, X_n]$ and for all distinct $x_1, \dots, x_n \in S$, it holds that $f(x_1, \dots, x_n) \neq 0$. A *maximal algebraically independent* subset S over F is the maximal subset with respect the set inclusion in the set of all the algebraically independent subsets over F.

Definition 2.3.7 (Transcendence base and degree)**.** Let L/K be a field extension. A maximal algebraically independent subset $S \subset L$ over the field K is called a *transcendence base* for the extension L/K. The *transcendence degree* of the extension L/K is the cardinality of the transcendence base S.

Note that transcendence degree is defined for field extensions since the algebraically independent subset S is defined over the subfield K. Considering Definition 2.3.5, we see that an extension is algebraic if and only if its transcendence degree is 0. In that case, the empty set serves as a transcendence base. Because it is often very difficult to show if elements are algebraically independent, the transcendence degree is difficult to determine in practice. For example, it is not known if the transcendence degree of the extension $\mathbb{Q}(\pi, e)$ is 1 or 2 since π and e might be algebraically dependent.

In the following definition, we mention multiplicative submonoids. A *multiplicative submonoid of a ring* A simply means a subset of A that is a monoid with respect to the multiplication operation.

Definition 2.3.8 (Ring of fractions)**.** Let A be a commutative ring. Let S be a multiplicative submonoid of A. We define an equivalence relation on $A \times S$ by setting that $(a, s) \sim (a', s')$ if there exists $s_1 \in S$ so that $s_1(s'a - sa') = 0$. The set of equivalence classes, denoted by $Q(A)$ or $S^{-1}A$, is called the *ring of fractions at* S and it satisfies the ring properties.

For the following definition recall Definition 2.1.3 of zero divisors.

Definition 2.3.9 (Total ring of fractions)**.** A *total ring of fractions* $Q(A)$ of a commutative ring A is the ring of fractions of A where S is the set that does not include any zero divisors of A.

The total ring of fractions is also called a *total quotient ring.* Next we prove that the canonical homomorphism from the ring A to its total ring of fractions is always injective.

Theorem 2.3.2. *The ring homomorphism $i\colon A \to S^{-1}A$ is injective if S does not contain any zero divisors of A.*

Proof. Assume that S does not contain any zero divisors. The canonical homomorphism $i\colon\colon A \to S^{-1}A$ maps the element $a \in A$ to the equivalence class represented by the element $(a, 1)$. Assume $i(a) = i(a')$ for $a, a' \in A$. By Definition 2.3.8, this means that there exists a nonzero $s \in S$ so that $s(a - a') = 0$. Recall Definition 2.1.3 of zero divisors. Because by the assumption s cannot be a zero divisor, there does not exists a nonzero element $a \in A$ so that $sa = 0$. Thus it must be that $a - a' = 0$. This proves the injectivity. □

The implication of Theorem 2.3.2 holds to another direction as well, but we do not need that direction in this work.

For the following definition recall integral domains from Definition 2.1.1.

Definition 2.3.10 (Field of fractions)**.** Let I be an integral domain. The *field of fractions* $\mathrm{Frac}(I) = I \times I/{\sim}$ is the field that consists of equivalence classes where the equivalence is defined

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$$

for $a, b, a', b' \in I$ and $b \neq 0$.

We do not explicitly prove that the field of fractions is a field. The total ring of fractions in Definition 2.3.9 generalizes the field of fractions so that the integral domain is replaced by a commutative ring. The field of fractions $\mathrm{Frac}(I)$ is the smallest field where I can be embedded. We commonly use the field of fractions of the polynomial ring $F[X_1, \dots, X_n]$ which is called a field of rational functions.

Definition 2.3.11 (Field of rational functions)**.** Let F be a field. The *field of rational functions* $F(X_1, \dots, X_n)$ in variables $X_1, \dots, X_n$ is the field of fractions of the polynomial ring $F[X_1, \dots, X_n]$.

Informally both a ring of fractions and a field of fractions introduce ”denominators” to the structures. The ring of fractions and the field of fractions are special cases of a mathematical construction called localization [8]. Localization can also be defined using category theoretical universal constructions.

Often we consider cases when the set S is an ideal of A. If A is an integral domain, then its total ring of fractions coincides with its field of fractions. The classical result in algebra states that every total ring of fractions is a certain kind of a factorial ring. In a factorial ring, every element has a unique factorization. The result is not discussed in standard introductory textbooks to algebra. The following formulation of the factorial theorem of total ring of fractions is from [5]. Recall Definition 2.2.2 of minimal prime ideals.

Theorem 2.3.3 (Factorial theorem of total ring of fractions)**.** *Let A be a Noetherian reduced ring with the minimal prime ideals $p_1, \dots, p_n$. Then the total ring of fractions $Q(A)$ of the ring A is isomorphic to the product of the total ring of fractions $Q(A/p_i)$ at the minimal prime ideals p_i for $i = 1, \dots, n$ i.e.*

$$Q(A) \cong \prod_{i=1}^{n} Q(A/p_i).$$

Proof. See Chapter V, §1.3, Corollary 1 on page 309 in [5]. □

We will utilize the factorization theorem later in the proof of the theorem of Bröcker and Scheiderer.

Chapter 3

Fundamentals of semi-algebraic geometry

3.1 Introduction

The story of real algebra starts from Hilbert's famous publication [9] of 23 problems which he collected and formulated in 1900. Ten of them he presented at a conference in Paris. From the real algebraic perspective, the 17th problem is the most important.

Problem 1 (Hilbert's 17th problem)**.** *Let $f \in \mathbb{R}[X_1, \ldots, X_n]$ be a real polynomial in n variables and $f(x) \geq 0$ for all $x \in \mathbb{R}^n$. Does there necessarily exists a presentation of f as a sum of squares in real rational functions i.e. in the form*

$$f = \sum_{i=1}^{m} r_i^2,$$

where $r_i \in \mathbb{R}(X_1, \ldots, X_n)$ for $i = 1, \ldots, m$ are rational functions?

A rational function $r(x)$ is a simply a function of form $r(X) = p(X)/q(X)$ where $p(X)$ and $q(X)$ are polynomials in $\mathbb{R}[X_1, \ldots, X_n]$ and $q(X) \neq 0$ for all $x \in \mathbb{R}$. Artin [10] represented proof to the 17th problem in the 1920s. To prove the Hilbert's 17th problem, he developed the theory of ordered fields that is foundational for real algebra. The theory of real fields and real closed fields dates back to Artin and Schreier's work [11]. The material in this chapter is based on [12].

3.2 Real closed fields

We recall that a relation $R \subset X \times X$ is called *total* if for all elements $a, b \in X$ either $(a, b) \in R$ or $(b, a) \in R$. In this section we first define a real field and then a real closed field.

Definition 3.2.1 (Ordered field)**.** Let $\mathcal{F}$ be a field and $x, y \in \mathcal{F}$. The *ordered field* $\mathcal{F}$ is a field that has a total order relation $\leq$ which satisfies the following conditions:

- If $x \leq y$, then $x + z \leq y + z$ for all $z \in \mathcal{F}$.
- If $0 \leq x$ and $0 \leq y$, then $0 \leq xy$.

In this work, we will follow a convention that $\mathcal{F}$ denotes an ordered field.

The most familiar examples of ordered fields are the real numbers $\mathbb{R}$ and the rational numbers $\mathbb{Q}$ with their natural orderings. On the other hand, the complex numbers $\mathbb{C}$ cannot be ordered so that they form an ordered field.

Definition 3.2.2 (Cone, positive cone, and proper cone)**.** Assume that $\mathcal{F}$ is an ordered field. A subset $P \subset \mathcal{F}$ is called a *cone* if it satisfies the following properties:

1. If $x, y \in P$, then $x + y \in P$.
2. If $x, y \in P$, then $xy \in P$.
3. If $x \in \mathcal{F}$, then $x^2 \in P$.

The cone P is a *proper cone* if additionally $-1 \notin P$. The subset

$$P_+ = \{x \in \mathcal{F} \mid x \geq 0\}$$

is called a *positive cone of* $\mathcal{F}$.

Note that a positive cone is a proper cone. The concepts of a cone and a proper cone can be defined for a commutative ring A when we replace the field $\mathcal{F}$ in Definition 3.2.2 with a commutative ring A.

Definition 3.2.3. The set of the sum of squares of elements of $\mathcal{F}$ is denoted by $\Sigma\mathcal{F}^2$.

Lemma 3.2.1. *The set $\Sigma\mathcal{F}^2$ is a cone and it is contained in every cone of $\mathcal{F}$.*

Proof. If $a^2, b^2 \in \Sigma\mathcal{F}^2$, then $a^2 + b^2 \in \Sigma\mathcal{F}^2$ by the definition. Also, we have $a^2b^2 = (ab)^2 \in \Sigma\mathcal{F}^2$. Finally, if $x \in \mathcal{F}$, then $x^2 \in \Sigma\mathcal{F}^2$ by the definition.

Let $P \subset \mathcal{F}$ be a cone. Let $x \in \Sigma\mathcal{F}^2$. Now $x = a_1^2 + \ldots + a_n^2$. Since $a_i \in \mathcal{F}$ for all $i = 1, \ldots, n$, then $a_i^2 \in P$ for all $i = 1, \ldots, n$ by Definition 3.2.2. Besides, $x = a_1^2 + \ldots + a_n^2 \in P$ again by Definition of a cone. Thus $\Sigma\mathcal{F}^2 \subset P$. □

The following theorem will serve as a basis for the definition of a real field. We use Zorn's lemma in the proof and assume that the reader is familiar with it. Informally, the idea of Zorn's lemma is that a partially ordered set, where every chain of ordered elements has an upper bound, contains a maximal element. See Zorn's lemma in [3, 13] for more detailed descriptions.

Theorem 3.2.2. *Let $\mathcal{F}$ be a field. The following claims are equivalent:*

1. *The field $\mathcal{F}$ can be ordered.*
2. *The field $\mathcal{F}$ has a proper cone.*
3. *It holds that $-1 \notin \Sigma\mathcal{F}^2$.*
4. *For every $x_1, \dots, x_n \in \mathcal{F}$, it holds: if $\sum_{i=1}^n x_i^2 = 0$, then $x_1 = \dots = x_n = 0$.*

Proof. Condition 1. implies condition 2. If $\mathcal{F}$ can be ordered, then it has a subset $P = \{x \in \mathcal{F} \mid x \geq 0\}$ which is a proper cone by Definition 3.2.2.

Condition 2. implies condition 3. Assume that P is a proper cone of $\mathcal{F}$ that by Definition 3.2.2 means $-1 \notin P$. We see that $\Sigma\mathcal{F}^2 \subset P$ because $\Sigma\mathcal{F}^2$ is contained in every cone of $\mathcal{F}$ by Lemma 3.2.1. Thus $-1 \notin \Sigma\mathcal{F}^2$.

Condition 3. implies condition 4. Assume $-1 \notin \Sigma\mathcal{F}^2$ and $x_1, \dots, x_n \in \mathcal{F}$. Assume $\sum_{i=1}^n x_i^2 = 0$ and $x_j \neq 0$ for some $1 \leq j \leq n$. Now for the indexes $I = \{1, \dots, n\} \setminus \{j\}$ we have $\sum_{i \in I} x_i^2 = -x_j^2 \in \Sigma\mathcal{F}^2$. By Lemma 3.2.1, the set $\Sigma\mathcal{F}^2$ is a cone and $1/x_j^2 \in \Sigma\mathcal{F}^2$. Thus we have $-x_j^2(1/x_j^2) = -1 \in \Sigma\mathcal{F}^2$. This is a contradiction. Thus $x_1 = \dots = x_n = 0$.

Condition 4. implies condition 3. Assume condition 4. holds. Assume that $-1 \in \Sigma\mathcal{F}^2$. Then there exist elements $y_1, \dots, y_n \in \mathcal{F}$ such that $\sum_{i=1}^n y_i^2 = -1$. Now $\sum_{i=1}^n y_i^2 + 1 = 0$ which contradicts with condition 4. Thus $-1 \notin \Sigma\mathcal{F}^2$.

Condition 3. implies condition 1. If $-1 \notin \Sigma\mathcal{F}^2$, then $\Sigma\mathcal{F}^2$ is a proper cone by Definition 3.2.2. We claim that $\Sigma\mathcal{F}^2$ is contained in a positive cone of $\mathcal{F}$. This positive cone induces ordering to $\mathcal{F}$. The collection of proper cones of $\mathcal{F}$ is partially ordered by inclusion and every chain of inclusions has an upper bound. After applying Zorn's lemma, we obtain that there exists a maximal proper cone Q that contains $\Sigma\mathcal{F}^2$. We show that $Q \cup -Q = \mathcal{F}$ where $-Q = \{x \mid -x \in Q\}$. Since Q is a proper cone, this proves that Q is a positive cone.

Let $a \in \mathcal{F}$ be such that $a \notin Q$. We prove that $-a \in Q$. Now $Q[-a] = \{x - ay \mid x, y \in Q\}$ is a proper cone because if $-1 \in Q[-a]$ then either $-1 = x - ay$ and $-1 \in Q$, or $a = (x+1)/y = (1/y^2)y(x+1) \in Q$. The both outcomes are contradictions. Thus $Q[-a]$ is a proper and $Q = Q[-a]$ because Q is a maximal proper cone. This implies that $-a \in Q$. This proves that $Q \cup -Q = \mathcal{F}$. Thus condition 3. implies condition 1. □

Definition 3.2.4 (Real field)**.** A field $\mathcal{F}$ satisfying Theorem 3.2.2 is called a *real field.*

The real fields are called real because they resemble real numbers in the sense that the equation $x^2 + 1 = 0$ does not have a solution. Part 4. in Theorem 3.2.2 shows that the characteristic (Definition 2.1.4) of every real field is always 0. For the next definition recall Definition 2.3.5 of algebraic extensions. A real field is closed in a similar manner as a ring or a field is closed.

Definition 3.2.5 (Real closed field)**.** A real field $\mathcal{F}$ is *closed* if it does not have a nontrivial algebraic extension $F' \supsetneq F$.

Example 1. Besides that real numbers $\mathbb{R}$ and algebraic real numbers $\mathbb{R}_{\text{alg}}$ form real closed fields, we represent a non-trivial example. An interesting example of a real closed field is a field of Puiseux series. A Puiseux series with coefficients in $\mathbb{R}$ is a generalization of power series of the form

$$\sum_{i=k_0}^{\infty} a_i X^{i/n},$$

where $a_k \in \mathbb{R}$, $k \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. For more details and the proof that the field of Puiseux series with coefficients in $\mathbb{C}$ is algebraically closed see §3. Factorial power series in [14]. The ordering on the field of Puiseux series with coefficients in $\mathbb{R}$ is inherited from the ordering of $\mathbb{R}$ and defined by the condition

$$\sum_{i=k_0}^{\infty} a_i X^{i/n} > 0 \Leftrightarrow a_{k_0} > 0.$$

Theorem 3.2.3. *Let $P(X) = c_p X^p + \ldots + c_1 X_1 + c_0$ be a polynomial with coefficients in an ordered field $\mathcal{R}$ and $c_p \neq 0$. If $x \in \mathcal{R}$ is sufficiently large, namely*

$$|x| > 2 \sum_{i=0}^{p} \left| \frac{c_i}{c_p} \right|, \tag{3.1}$$

then $P(x)$ and $c_p x^p$ have the same sign.

Proof. Let $x \in \mathcal{R}$ and assume that Inequality (3.1) holds for x. Especially, it implies that $|x| > 2$. Dividing the polynomial $P(x)$ by $c_p x^p \neq 0$, we obtain

$$\frac{P(x)}{c_p x^p} = 1 + \sum_{i=0}^{p-1} \frac{c_i}{c_p} x^{i-p}.$$

We may estimate

$$\begin{aligned}
\frac{P(x)}{c_p x^p} &\geq 1 - \sum_{i=0}^{p-1} \left| \frac{c_i}{c_p} \right| |x|^{i-p} \\
&\geq 1 - \left(\sum_{i=0}^{p} \left| \frac{c_i}{c_p} \right| \right) (|x|^{-1} + \ldots + |x|^{-p}) \\
&\geq 1 - \frac{1}{2}(1 + |x|^{-1} + \ldots + |x|^{-p+1}) \\
&= 1 - \frac{1}{2} \left(\frac{1 - |x|^p}{1 - |x|^{-1}} \right) > 0
\end{aligned}$$

where $\frac{1}{2}\left(\frac{1-|x|^p}{1-|x|^{-1}}\right) < 1$ because we assumed Inequality (3.1). Because the fraction $P(x)/c_p x^p$ is positive, it proves that $P(x)$ and $c_p x^p$ have the same sign. □

The following theorem is important and it originates to [11]. This version is a combination of theorems presented in [12, 15]. The theorem is interesting because it characterizes real closed fields in multiple equivalent ways which are seemingly different.

Theorem 3.2.4. *Let $\mathcal{F}$ be an ordered field. Then the following properties are equivalent:*

1. *The field $\mathcal{F}$ is real closed in the sense of Definition 3.2.5.*
2. *There is a unique ordering of $\mathcal{F}$ whose positive cone is the set of squares $\Sigma\mathcal{F}^2$ and where every polynomial of $\mathcal{F}[X]$ of odd degree has a root in $\mathcal{F}$.*
3. *Let $i = \sqrt{-1}$. The ring $\mathcal{F}[i] = \mathcal{F}[\sqrt{-1}] \cong \mathcal{F}[X]/(X^2+1)$ is an algebraically closed field.*
4. *The field $\mathcal{F}$ has an intermediate value property: Let $f \in \mathcal{F}[X]$ be a polynomial and $a, b \in \mathcal{F}$ be elements such that $a < b$ and $f(a)f(b) < 0$. Then there exists $x \in]a, b[$ for which $f(x) = 0$.*

Proof. Condition 1. *implies condition* 2. Let $a \in \mathcal{F}$. In the case that a is not a square, the field extension $\mathcal{F}[\sqrt{a}] = \mathcal{F}[X]/(X^2 - a)$ is a non-trivial, algebraic extension of $\mathcal{F}$. By part 1. the field $\mathcal{F}$ is real closed which means that it does not have real, algebraic extensions. Hence it follows that $\mathcal{F}[\sqrt{a}]$ cannot be real. By Theorem 3.2.2, we obtain that $-1 \in \Sigma\mathcal{F}[\sqrt{a}]^2$ which implies that

$$-1 = \sum_{i=1}^{n} (x_i + \sqrt{a} y_i)^2 \quad \text{and} \quad -1 = \sum_{i=1}^{n} x_i^2 + a \sum_{i=1}^{n} y_i^2,$$

where the later equation holds in $\mathcal{F}$. Because $\mathcal{F}$ is real, $-1 \notin \Sigma\mathcal{F}^2$ by Theorem 3.2.2 and thus $-1 \neq \sum_{i=1}^{n} x_i^2$. Hence we must have $\sum_{i=1}^{n} y_i^2 \neq 0$. When we solve $-a$, we obtain that

$$-a = \left(\sum_{i=1}^{n} y_i^2\right)^{-1} \left(1 + \sum_{i=1}^{n} x_i^2\right) \in \Sigma\mathcal{F}^2.$$

Thus we see that $-\Sigma\mathcal{F}^2 \cup \Sigma\mathcal{F}^2 = \mathcal{F}$. We know that $\Sigma\mathcal{F}^2$ is exactly the positive cone defined in Definition 3.2.2. Compare this argument to the similar one we made in the last part of the proof of Theorem 3.2.2. The unique ordering is defined by the condition: $x \leq y$ if and only if $y - x \in \Sigma\mathcal{F}^2$.

Next we show that every polynomial of $\mathcal{F}[X]$ of odd degree has a root in $\mathcal{F}$. Let $f \in \mathcal{F}[X]$ be an odd degree polynomial of degree $d > 1$ so that every odd degree polynomial of degree less than d has a root in $\mathcal{F}$. Suppose towards contradiction that f does not have a such root. Since f is an odd degree polynomial, it has an irreducible factor of odd degree. The quotient $\mathcal{F}[X]/(f)$ is a non-trivial algebraic extension of $\mathcal{F}[X]$ since we assumed that f does not have a root in $\mathcal{F}$. Because $\mathcal{F}[X]/(f)$ is not real, $-1 \in \Sigma(\mathcal{F}[X]/(f))^2$ by Theorem 3.2.2. That is a similar argument as we used in the previous part. We obtain that

$$-1 = \sum_{i=1}^{n} h_i^2 + fg, \tag{3.2}$$

where $\deg(h_i) < d$. Now $\sum_{i=1}^{n} h_i^2$ is a polynomial that has a degree less or equal than $2\max\{\deg(h_i) \mid i = 1, \dots, n\} \leq 2(d-1) = 2d-2$. Thus the polynomial g must be an odd degree polynomial whose degree is less or equal than $d-2$ because

$$0 = \deg(-1) = \deg(\sum_{i=1}^{n} h_i^2) - \deg(f)\deg(g) \leq 2d - 2 - d - \deg(g)$$

which implies $\deg(g) \leq d-2$. By the assumption we made in the beginning, the polynomial g has a root x in $\mathcal{F}$. Hence, using Equation (3.2), we obtain

$$-1 = \sum_{i=1}^{n} h_i(x)^2 + f(x)g(x) = \sum_{i=1}^{n} h_i(x)^2$$

which implies $-1 \in \Sigma\mathcal{F}^2$. By Theorem 3.2.2, this contradicts with the fact that $\mathcal{F}$ is real.

Condition 2. *implies condition* 3. Let $f \in \mathcal{F}[X]$ be a polynomial of degree $d = 2^m n$ with n odd. We show by induction on m that f has a root in $\mathcal{F}[\sqrt{-1}]$. When $m = 0$, f is an odd degree polynomial and by part 2. it has a root in $\mathcal{F} \subset \mathcal{F}[\sqrt{-1}]$. Now assume that the claim is true for $m-1$. Let $y_1, \dots, y_d$ be the roots of f in an algebraic closure of $\mathcal{F}$ and define

$$g_h = \prod_{i<j}(X - y_i - y_j - hy_iy_j),$$

where $h \in \mathbb{Z}$. Now $g_h \in \mathcal{F}[X]$. The polynomial g_h is a product of polynomials of degrees $1, \dots, d-1$ and thus its degree is the sum $1 + \ldots + (d-1) = d(d-1)/2 = 2^{m-1}n'$ where n' is an odd number. By induction assumption, g_h has a root in $\mathcal{F}[\sqrt{-1}]$. Because of the root, one of the terms in the polynomial is zero which leads to the fact that there exist i and j so that $0 = y_i + y_j + hy_iy_j \in \mathcal{F}[\sqrt{-1}]$. Because there are infinitely many integers and only finitely many indexes i and j between 0 and d, it follows that there exist i, j, h and h' with $h \neq h'$ so that $y_i + y_j + hy_iy_j \in \mathcal{F}[\sqrt{-1}]$ and $y_i + y_j + h'y_iy_j \in \mathcal{F}[\sqrt{-1}]$. This implies that $y_i + y_j \in \mathcal{F}[\sqrt{-1}]$ and $y_iy_j \in \mathcal{F}[\sqrt{-1}]$. For example, the calculation $y_i + y_j + hy_iy_j - (y_i + y_j + h'y_iy_j) = (h - h')y_iy_j \in \mathcal{F}[\sqrt{-1}]$ shows that $y_iy_j \in \mathcal{F}[\sqrt{-1}]$.

Now $(X - y_i)(X - y_j) = X^2 - y_iX - y_jX + y_iy_j \in \mathcal{F}[\sqrt{-1}][X]$ so we see that y_i and y_j are solutions to a quadratic equation with coefficients in $\mathcal{F}[\sqrt{-1}]$. Because $(X - y_i)(X - y_j)$ is part of the factorization of f, the polynomial f has a root in $\mathcal{F}[\sqrt{-1}]$.

Let us take a complex number perspective and define $i = \sqrt{-1}$. Then the conjugate is $\overline{a + bi} = a - bi$ for $a, b \in \mathcal{F}$. Consider the field $\mathcal{F}[\sqrt{-1}]$ as $\mathcal{F}[i]$. Assume $f \in \mathcal{F}[i]$. We define the conjugate polynomial $\bar{f}$ to be the polynomial where the coefficients of f are replaced with their conjugates. Because $f\bar{f} \in \mathcal{F}[X]$, $f\bar{f}$ has a root x in $\mathcal{F}[i]$. Then either x is a root of f or it is a root of $\bar{f}$ in which case the conjugate $\bar{x}$ is the root of f. This proves that $\mathcal{F}[\sqrt{-1}]$ is algebraically closed.

Condition 3. *implies condition* 4. Assume that $f \in \mathcal{F}[i][X]$ is a polynomial. Because $\mathcal{F}[i]$ is assumed to be algebraically closed, the polynomial f factors into linear factors over $\mathcal{F}[i]$ by Theorem 2.3.1. If $x = a + ib$ is a root of f, then the complex conjugate $\bar{x} = a - ib$ is a root as well. We can deduce this easily when we note that $a = \bar{a} \in \mathcal{F}$ and use the properties of complex conjugates

$$f(\bar{x}) = \sum_{i=0}^{n-1} a_i(\bar{x})^i = \sum_{i=0}^{n-1} a_i\overline{x^i} = \sum_{i=0}^{n-1} \overline{a_i x^i} = \overline{\sum_{i=0}^{n-1} a_i x^i} = \overline{f(x)} = \bar{0} = 0.$$

Hence the irreducible factors of f are either linear or form $(X - c)^2 + d^2 = (X - c - id)(X - c + id)$. If $f(a)$ and $f(b)$ have opposite signs, then some linear factors $q(a)$ and $q(b)$ of the polynomial f have opposite signs. Thus the root of q is in $]a, b[$.

Condition 4. *implies condition* 1. By Theorem 3.2.3, the polynomial $X^2 - y \in \mathcal{F}[X]$ has a positive sign for sufficiently large x and it has a negative sign at zero. By the intermediate value property, the polynomial has a root which is the square root of y. Similarly an odd degree polynomial has a positive sign for sufficiently large x and a negative sign for sufficiently small y by Theorem 3.2.3. Thus it has a root by the intermediate value property. Since $\mathcal{F}$ is assumed to be ordered, by Definition 3.2.5 this proves that $\mathcal{F}$ is a real closed field. □

Real numbers $\mathbb{R}$ is a real closed field since every polynomial of odd degree has a root and $\Sigma\mathbb{R}^2$ has the unique ordering defined by $x \leq y$ if and only if $y - x \in \Sigma\mathbb{R}^2$. On the other hand, rational numbers $\mathbb{Q}$ form a real field but not a real closed field since, for example, the polynomial $x^3 - 2$ has no root in $\mathbb{Q}$.

3.3 Semi-algebraic sets

In this section, we introduce the basics of semi-algebraic sets. Throughout the chapter, we assume that $\mathcal{R}$ is a real closed field. As the name semi-algebraic suggests, we relax the equality requirement in algebraic sets and include inequalities. This section is based on [12].

Definition 3.3.1 (Algebraic set)**.** Let F be a field. An *algebraic set* has a form of

$$\mathcal{Z}(P) = \{x \in F^n \mid f(x) = 0 \text{ for all } f \in P\},$$

where P is a set of polynomials in $F[X_1, \ldots, X_n]$. The set $\mathcal{Z}(P)$ is the *set of zeros* of P.

Definition 3.3.2 (Polynomials vanishing on S)**.** Let F be a field and let $S \subset F^n$ be a subset. We denote by

$$\mathcal{I}(S) = \{f \in F[X_1, \ldots, X_n] \mid f(x) = 0 \text{ for all } x \in S\}$$

the *ideal of polynomials vanishing on the set S.*

We omit the proof that $\mathcal{I}(S)$ is an ideal. The following definition is from [16].

Definition 3.3.3 (Boolean combination of polynomial equations and inequalities)**.** Let $\mathcal{R}$ be a real closed field and $y \in \mathcal{R}^n$. A *boolean combination of polynomial equations and inequalities* $\mathcal{B}(y)$ is a finite boolean expression of polynomial equations and inequalities in the variable y with coefficients in $\mathbb{Z}$ that are composed of negations, conjunctions, and disjunctions.

Now we define semi-algebraic sets which are the main interest and the cornerstone of this work.

Definition 3.3.4 (Semi-algebraic sets I)**.** Semi-algebraic sets $\mathcal{S}_n$ are the smallest class of subsets of $\mathcal{R}^n$ that satisfy the following two conditions.

1. If $f \in \mathcal{R}[X_1, \ldots, X_n]$ is a polynomial, then

$$\{x \in \mathcal{R}^n \mid f(x) = 0\} \in \mathcal{S}_n \text{ and } \{x \in \mathcal{R}^n \mid f(x) > 0\} \in \mathcal{S}_n.$$

2. If $A \in \mathcal{S}_n$ and $B \in \mathcal{S}_n$, then $A \cup B \in \mathcal{S}_n$, $A \cap B \in \mathcal{S}_n$ and $\mathcal{R}^n \setminus A \in \mathcal{S}_n$.

A *semi-algebraic set* is a set belonging to $\mathcal{S}_n$. In the other words, if $f(x) < 0$, $f(x) > 0$, $f(x) = 0$ are sign conditions on the polynomial f, then a semi-algebraic set is defined by a boolean combination (Definition 3.3.3) of polynomial equations and inequalities of the sign conditions involving a finite number of polynomials.

On the other hand, in [12] is represented a slightly different definition for semi-algebraic sets.

Definition 3.3.5 (Semi-algebraic sets II)**.** Semi-algebraic set is a subset of $\mathcal{R}^n$ that has the form

$$\bigcup_{i=1}^{n_1} \bigcap_{j=1}^{n_2} \{x \in \mathcal{R}^n \mid f_{i,j}(x) \,\square_{i,j}\, 0\} \,,$$

where $f_{i,j} \in \mathcal{R}[X_1, \ldots, X_n]$ and the square $\square_{i,j}$ corresponds either $>$ or $=$ for $1 \leq i \leq n_1$ and $1 \leq j \leq n_2$.

The following formulation for semi-algebraic sets is useful.

Theorem 3.3.1 (Finite union formulation)**.** *Every semi-algebraic set of $\mathcal{R}^n$ can be written as a finite union of semi-algebraic sets of form*

$$\{x \in \mathcal{R}^n \mid f_i(x) = 0,\ i = 1, \ldots, m \text{ and } g_j(x) > 0,\ j = 1, \ldots, l\} \,, \tag{3.3}$$

where $f_i,\ g_j \in \mathcal{R}[X_1, \ldots, X_n]$ for $i = 1, \ldots, m$ and $j = 1, \ldots, l$.

Proof. The collection of the unions of the sets of form (3.3) is closed under finite unions and intersections. Also, it is closed under complements because $(A \cup B)^c = A^c \cap B^c$ by De Morgan's laws. For example, if $A = \{x \in \mathcal{R}^n \mid f(x) < 0\}$, then the complement $\mathcal{R}^n \setminus A$ is $\{x \in \mathcal{R}^n \mid f(x) = 0\} \cup \{x \in \mathcal{R}^n \mid f(x) > 0\}$ which has the right form. Hence the complement of the set of form (3.3) has again the same form. □

The theorem of Bröcker and Scheiderer is a results about basic open semi-algebraic sets. Thus they have an important role in this work.

Definition 3.3.6 (Basic open semi-algebraic set)**.** A *basic open* semi-algebraic set of $\mathcal{R}^n$ has a form

$$\{x \in \mathcal{R}^n \mid f_i(x) > 0,\ i = 1, \ldots, m\} \,,$$

where $f_i \in \mathcal{R}[X_1, \ldots, X_n]$ for $i = 1, \ldots, m$.

Next, we define a dimension of a semi-algebraic set. To motivate the definitions here, we discuss how the concepts of dimension are defined in various contexts in algebra. The idea behind the dimension of a semi-algebraic set is to give a definition that coincides with the definition of a dimension of an algebraic set. The definition is algebraic in the sense that we do not, for example, count sizes of basis elements. Because the definition is algebraic, it does not give much of an intuition behind its geometric interpretation.

Recall that the dimension of ring is defined in Definition 2.2.4 and the ideal $\mathcal{I}(A)$ is defined in Definition 3.3.2.

Definition 3.3.7 (Dimension of semi-algebraic (and algebraic) set)**.** Let $A \subset \mathcal{R}^n$ be a semi-algebraic set and

$$\mathcal{P}(A) = \mathcal{R}[X_1, \ldots, X_n]/\mathcal{I}(A)$$

be the ring of polynomial functions on A where $\mathcal{I}(A)$ is the ideal of polynomials vanishing on A. The dimension $\dim(A)$ of A is defined to be the dimension of the ring $\mathcal{P}(A)$ i.e. the maximal length of chains of prime ideals of $\mathcal{P}(A)$.

Every algebraic subset is also a semi-algebraic set. In this work, the definition of the dimension of a semi-algebraic set also defines the dimension of an algebraic set. This definition is not standard in algebraic geometry, but both definitions are equivalent. In algebraic geometry the following theorem is usually provided as a definition for the dimension of an algebraic set, for example, see Definition of dimension in §6.1 in [17].

Recall Definition 2.3.2 of the dimension of an ideal. Often we do not say that the dimension of the semi-algebraic set A is the dimension of the ring $\mathcal{P}(A)$ but the dimension of the ideal $\mathcal{I}(A)$. This is naturally the equivalent formulation because $\mathcal{P}(A) = \mathcal{R}[X_1, \ldots, X_n]/\mathcal{I}(A)$.

Recall Definition 2.3.10 of field of fractions and Definition 2.3.7 of the transcendence degree.

Theorem 3.3.2 (Field of fractions and dimension of algebraic set)**.** *Let $V \subset \mathcal{R}^n$ be an algebraic subset. Let $\mathcal{K}(V)$ be the field of fractions of the polynomial ring $\mathcal{P}(V)$. The dimension of V is the transcendence degree of $\mathcal{K}(V)$ over the field $\mathcal{R}$.*

Proof. We can use the normalisation theorem of Noether (Theorems 1.17 and 1.18 in [17], or also Corollary 1, Chapter 5, §14.G in [8], or also Theorem l.8A, Chapter I, §1 [18]). By Definition 3.3.7, $\dim(V) = \dim(\mathcal{P}(V)) = \dim(\mathcal{R}[X_1, \ldots, X_n]/\mathcal{I}(V))$. Because $\mathcal{P}(V)$ is especially an integral domain which is a finitely generated $\mathcal{R}$-algebra, the result follows immediately from the normalisation theorem of Noether. □

As described in [17], the dimension of an algebraic set is motivated by the famous normalization theorem of Noether. We used the normalization theorem to prove that our Definition 3.3.7 for a semi-algebraic (and algebraic) set coincides with the common definition (Theorem 3.3.2) for the dimension of an algebraic set given in literature, for example, in [17].

3.4 Basics of quadratic forms

This section introduces the basics of quadratic forms and it is based on [19]. The set $F^\star = F \setminus \{0\}$ denotes the multiplicative group of F. We develop the theory of quadratic forms further when we are studying Pfister forms. The Pfister forms are very useful when we are proving the theorem of Bröcker and Scheiderer for basic open semi-algebraic sets.

Definition 3.4.1 (Quadratic form)**.** Let F be a field. A *quadratic form* f over F is a homogeneous polynomial in $F[X_1, \ldots, X_n]$ of degree 2 i.e.

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

where $a_{i,j} \in F$ for $i, j = 1, \ldots, n$. The constant n is the dimension of f, denoted by $\dim(f)$.

If $M_f = (a_{i,j})_{i,j=1,\ldots,n}$ is the symmetric $n \times n$ matrix, then the quadratic form can be written

$$f(x) = x^\top M_f x.$$

For example, $2X^2 + XY - 3Y^2$ is a quadratic form. Quadratic forms have strong connection to linear algebra. We see that every quadratic form f defines a symmetric bilinear form

$$\phi_f(x, y) = x^\top M_f y \tag{3.4}$$

on the F-vector space $F^{(n)}$.

Definition 3.4.2 (Equivalence on quadratic forms)**.** The quadratic forms f and g over the field F are equivalent, denoted by $f \cong g$, if $\dim(f) = \dim(g)$ and $P^\top M_f P = M_g$ for some invertible $n \times n$ matrix P over F.

Clearly, $\cong$ is an equivalence relation over the quadratic forms over F.

Definition 3.4.3 (Diagonal form)**.** If a quadratic form $f \in F[X_1, \ldots, X_n]$ has form

$$f = \sum_{i=1}^{n} a_i X_i^2,$$

then f is called a *diagonal form* and denoted by $\langle a_1, \ldots, a_n \rangle$.

Although we can define a tensor product for general quadratic forms, in this work we need the tensor product only for diagonal forms. The reason is that in the following chapters we are dealing with Pfister forms which are special kinds of diagonal forms. The reader, who is interested in the general definition of a tensor product for quadratic forms, can see section Kronecker product of quadratic spaces in [20].

Definition 3.4.4 (Tensor product of diagonal forms)**.** Let $a = \langle a_1, \ldots, a_n \rangle$ and $b = \langle b_1, \ldots, b_m \rangle$ be two diagonal forms over a field F. We define the *tensor product* of a and b as a diagonal form

$$a \otimes b = \langle a_1 b_1, a_2 b_1, \ldots, a_n b_1, \ldots, a_1 b_m, \ldots, a_n b_m \rangle.$$

The following theorem is in the heart of quadratic forms. It states that every quadratic form is equivalent to some diagonal form. In other words, this means that every symmetric matrix is diagonalizable. In the most of the cases, we can assume that a quadratic form is expressed in its equivalent diagonal form. In this work, we will use the result in the proof of Witt's cancellation theorem.

Theorem 3.4.1. *Let f be a quadratic form of dimension n. Then there exist $a_1, \ldots, a_n \in F^\star$ such that $f \cong \langle a_1, \ldots, a_n \rangle$.*

Proof. We use the bilinear form for f defined in Equation (3.4). The idea of the proof is to show that there exists a basis $x_1, \ldots, x_n$ such that $\phi_f(x_i, x_j) = 0$ for all $i \neq j$. In other words, the basis is orthogonal with respect to the bilinear form of f. When we choose $a_i = \phi_f(x_i, x_i) = f(x_i)$, we obtain that $f \cong \langle a_1, \ldots, a_n \rangle$. This can be easily seen when we write the forms open

$$\begin{aligned}
\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}^\top M_f \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} &= \begin{bmatrix} x_1^\top M_f x_1 & x_1^\top M_f x_2 & \ldots & x_1^\top M_f x_n \\ \vdots & \ddots & \ddots & \vdots \\ x_n^\top M_f x_1 & \ldots & x_n^\top M_f x_{n-1} & x_n^\top M_f x_n \end{bmatrix} \\
&= \begin{bmatrix} x_1^\top M_f x_1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & x_n^\top M_f x_n \end{bmatrix} \\
&= \begin{bmatrix} a_1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_n \end{bmatrix} \\
&= \langle a_1, \ldots, a_n \rangle.
\end{aligned}$$

where $x_i^\top M_f x_j = 0$ for all $i \neq j$ because we chose the elements $x_1, \ldots, x_n$ so that $\phi_f(x_i, x_j) = 0$ for all $i \neq j$. Now only the diagonals are left and these are exactly the elements $a_i = \phi_f(x_i, x_i) = f(x_i)$.

Let us prove that the suitable basis $x_1, \ldots, x_n$ exists. First we note that every basis of $F^{(n)}$ is orthogonal with respect to ϕ_f if for all vectors $x \in F^{(n)}$ holds $f(x) = 0$. Thus let $x_1 \in F^{(n)}$ be such that $a_1 = f(x_1) \neq 0$. We define a set

$$U = \left\{ x \in F^{(n)} \mid \phi_f(x_1, x) = 0 \right\}.$$

Now U is a subspace of $F^{(n)}$ because ϕ_f is bilinear form. Besides $F^{(n)} = Fx_1 \oplus U$. Let $v \in F^{(n)}$ be a vector. We define

$$u = v - \frac{\phi_f(x_1, v)}{a_1} x_1.$$

Then we can calculate

$$\begin{aligned}\phi_f(x_1,u) &= \phi_f(x_1,v) - \phi_f(x_1,v)\phi_f(x_1,x_1)/a_1 \\ &= \phi_f(x_1,v) - \phi_f(x_1,v)f(x_1)/a_1 \\ &= \phi_f(x_1,v) - \phi_f(x_1,v) = 0.\end{aligned}$$

This shows that x_1 is not in the basis of U which means that $\dim(U) = n-1$. If we assume that by induction the subspace U already admits a basis $x_2,\ldots,x_n$ with respect to ϕ_f restricted to U, then this proves the claim that $x_1,\ldots,x_n$ is the orthogonal basis for $F^{(n)} = Fx_1 \oplus U$ with respect to ϕ_f. □

The following definition of a signature of a quadratic form at an ordering is from [21].

Definition 3.4.5 (Signature of quadratic form at ordering)**.** Let $\mathcal{R}$ be a real closed field with an ordering α. Let f be a quadratic form over $\mathcal{R}$. The signature of f at α is the number of coefficients in a diagonal form of f that are positive with respect to the ordering α minus the number of coefficients that are negative with respect to the ordering α.

Theorem 3.4.1 shows that a signature can always be defined. Although the diagonal representation for a quadratic form is not unique, the number of positive and negative elements in the diagonal form stays the same. We can easily see this from the proof of Theorem 3.4.1. There we chose $a_i = \phi_f(x_i,x_i) = f(x_i)$ for a basis $x_1,\ldots,x_n$. Because the difference of positive and negative elements in the basis needs to stay the same and the quadratic form is a linear mapping, it indicates that the difference of the positive and negative elements in $\langle a_1,\ldots,a_n\rangle$ stays the same. This motivates the definition of a signature.

Definition 3.4.6 (Orthogonal sum)**.** The *orthogonal sum* of the quadratic forms f and g over the field F is defined by the block matrix

$$f \perp g = \left[\begin{array}{c|c} M_f & 0 \\ \hline 0 & M_g \end{array}\right].$$

The following theorem provides the connection between orthogonal sums and tensor products.

Lemma 3.4.2. *Let $\phi = \langle b_1,\ldots,b_n\rangle$ be a diagonal quadratic form and $a \in F^\star$. Then*

$$\phi \perp a\phi = \langle 1,a\rangle \otimes \phi.$$

Proof. We can calculate that the bilinear forms are equal. By Definition 3.4.6 of an orthogonal sum, we have

$$\begin{aligned}
\phi\perp a\phi &= \left[\begin{array}{c|c} M_\phi & 0 \\ \hline 0 & M_{a\phi} \end{array}\right] \\
&= \begin{bmatrix} b_1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & b_n & 0 & \dots & 0 \\ 0 & \dots & 0 & ab_1 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & ab_n \end{bmatrix} \\
&= \langle b_1, \dots b_n, ab_1, \dots, ab_n \rangle.
\end{aligned}$$

On the other hand, by Definition 3.4.4 of tensor product of diagonal quadratic forms, we obtain

$$\begin{aligned}
\langle 1, a\rangle \otimes \phi &= \langle 1, a\rangle \otimes \langle b_1, \dots, b_n\rangle \\
&= \langle b_1, ab_1, \dots, b_n, ab_n\rangle \\
&= \langle b_1, \dots b_n, ab_1, \dots, ab_n\rangle.
\end{aligned}$$

The calculations prove the claim. □

Definition 3.4.7 (Multiplicative quadratic form)**.** Let f be a quadratic form of dimension n over the field F. The form f is said to be *multiplicative* if for all $x \in F^{(n)}$ such that $f(x) \neq 0$, it follows $f(x)f \cong f$.

Recall that the set $F^\star$ denotes the multiplicative group of F.

Definition 3.4.8 (Nondegenerate quadratic form)**.** Let $f(x) = x^\top M_f x$ be a quadratic form. If $\det(M_f) \neq 0$, the form f is called *nondegenerate.* A diagonal quadratic form $\langle a_1, \dots, a_n\rangle$ is nondegenerate if $a_1, \dots, a_n \in F^\star$.

Sometimes nondegenerate quadratic forms are called *regular* [19].

Definition 3.4.9 (Isotropic and anisotropic quadratic forms)**.** Let f be a quadratic form of dimension n over F. Let $b \in F$. If there exists $x \in F^(n)$ such that $f(x) = b$, we say that f *represents* b. If there exists an element $x \neq 0$ such that $f(x) = 0$, we say that f is *isotropic.* Otherwise f is *anisotropic.*

We will use isotropic and anisotropic quadratic forms when we are dealing with Pfister forms.

Lemma 3.4.3. *1. Let $a \in F^\star$. Then $\langle a, -a\rangle \cong \langle 1, -1\rangle$.*

2. If the diagonal form $\langle a, b\rangle$ represents $c \in F^\star$, then $\langle a, b\rangle \cong c\langle 1, ab\rangle$.

Proof. By Definition 3.4.2, the explicit calculation

$$\begin{aligned}&\left(\frac{1}{2}\begin{bmatrix} a+1 & a-1 \\ a-1 & a+1 \end{bmatrix}\right)^{\top}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\left(\frac{1}{2}\begin{bmatrix} a+1 & a-1 \\ a-1 & a+1 \end{bmatrix}\right)\\ &=\frac{1}{4}\begin{bmatrix} a+1 & -a+1 \\ a-1 & -a-1 \end{bmatrix}\begin{bmatrix} a+1 & a-1 \\ a-1 & a+1 \end{bmatrix}\\ &=\begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix}\end{aligned}$$

proves the first part of the lemma. For the second part, we calculate

$$\begin{bmatrix} u & v \\ -bv & au \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} u & -bv \\ v & au \end{bmatrix}=c\begin{bmatrix} 1 & 0 \\ 0 & ab \end{bmatrix},$$

which proves the second part. □

The following theorem is a special version of Theorem 3.4.1. We show that we can choose the first two elements of the diagonal form to be 1 and -1 if f is isotropic.

Theorem 3.4.4. *Let f be a nondegenerate quadratic form of dimension n over F. The quadratic form f is isotropic if and only if there exist elements $a_3, \ldots, a_n \in F^{\star}$ such that $f \cong \langle 1, -1, a_3, \ldots, a_n \rangle$.*

Proof. If $f \cong \langle 1, -1, a_3, \ldots, a_n \rangle$ holds, then f is isotropic because

$$f(1, 1, 0, \ldots, 0) = 0.$$

Let f be an isotropic and nondegenerate quadratic form. By Theorem 3.4.1, we can write $f \cong \langle a_1, a_2, \ldots, a_n \rangle$ for $a_i \in F^{\star}$ for $i = 1, \ldots, n$. Because f is nondegenerate, $\det(M_f) \neq 0$ and thus $a_i \neq 0$ for $i = 1, \ldots, n$. Because f is isotropic, there exists such $x \in F$, that $x \neq 0$ and $\sum_{i=1}^{n} a_i x_i^2 = 0$. We can assume $x_1 \neq 0$. By dividing x_1 and subtracting the first term of the sum on the both sides, we obtain

$$-a_1 = \sum_{i=2}^{n} a_i \left(\frac{x_i}{x_1}\right)^2 .$$

This means that $\langle a_2, \ldots, a_n \rangle$ represents $-a_1$. The proof of Theorem 3.4.1 shows that if $\langle a_2, \ldots, a_n \rangle$ represents $-a_1$, then there exists $b_3, \ldots, b_n \in F^{\star}$ so that

$$\langle a_2, a_3, \ldots, a_n \rangle \cong \langle -a_1, b_3, \ldots, b_n \rangle.$$

In other words, in the proof of Theorem 3.4.1 we chose $f(x_1) = a_1$ which means that f represents a_1. Then the proof showed that $f \cong \langle a_1, \ldots, a_n \rangle$. In this case, $f = \langle a_2, \ldots, a_n \rangle$ and we can choose $b_i = a_i$ for $i = 3, \ldots, n$.

By the first part of Lemma 3.4.3, we obtain

$$\begin{aligned} f &\cong \langle a_1, a_2, \ldots, a_n\rangle \cong \langle a_1\rangle \perp \langle a_2, \ldots, a_n\rangle \cong \langle a_1\rangle \perp \langle -a_1, b_3, \ldots, b_n\rangle \\ &\cong \langle a_1, -a_1\rangle \perp \langle b_3, \ldots, b_n\rangle \cong \langle 1, -1\rangle \perp \langle b_3, \ldots, b_n\rangle = \langle 1, -1, b_3, \ldots, b_n\rangle, \end{aligned}$$

which proves the result. □

3.5 Witt's cancellation theorem

In this section, we prove Witt's cancellation theorem. The proof is based on [19] but one can find it also from [3]. The action of cancellation is done over the equivalence relation on quadratic forms defined in Definition 3.4.2. Witt's cancellation theorem enables us to cancel certain quadratic forms in orthogonal sums.

Lemma 3.5.1. *Let A and B be $n \times n$ matrices over F and $c \in F$ be a constant. Let P be an $(n+1) \times (n+1)$ matrix over F so that*

$$\left[\begin{array}{c|c} c & 0 \ldots 0 \\ \hline 0 & \\ \vdots & B \\ 0 & \end{array}\right] = P^\top \left[\begin{array}{c|c} c & 0 \ldots 0 \\ \hline 0 & \\ \vdots & A \\ 0 & \end{array}\right] P. \tag{3.5}$$

Then there exists $n \times n$ matrix Q over F so that

$$B = Q^\top A Q.$$

Proof. We write

$$P = \left[\begin{array}{c|c} d & v^\top \\ \hline w & S \end{array}\right],$$

where S is an $n \times n$ matrix, $d \in F$, and $v, w \in F^{(n)}$ are column vectors. The block matrices can be multiplied and manipulated similarly as ordinary matrices. By the assumption that the matrix P satisfies Equation (3.5), we can calculate

$$\begin{aligned} \left[\begin{array}{c|c} c & 0 \ldots 0 \\ \hline 0 & \\ \vdots & B \\ 0 & \end{array}\right] &= \left[\begin{array}{c|c} d & w^\top \\ \hline v & S^\top \end{array}\right] \left[\begin{array}{c|c} c & 0 \ldots 0 \\ \hline 0 & \\ \vdots & A \\ 0 & \end{array}\right] \left[\begin{array}{c|c} d & v^\top \\ \hline w & S \end{array}\right] \\ &= \left[\begin{array}{c|c} d & w^\top \\ \hline v & S^\top \end{array}\right] \left[\begin{array}{c|c} cd & cv^\top \\ \hline Aw & AS \end{array}\right] \\ &= \left[\begin{array}{c|c} cd^2 + w^\top Aw & cdv^\top + w^\top AS \\ \hline cdv + S^\top Aw & cvv^\top + S^\top AS \end{array}\right]. \end{aligned}$$

When we compare the blocks we obtain the system of equations

$$\begin{cases} c = cd^2 + w^\top Aw, \\ B = cvv^\top + S^\top AS, \\ 0 = cdv^\top + w^\top AS \text{ and} \\ 0 = cdv + S^\top Aw. \end{cases} \tag{3.6}$$

From Equations (3.6) we obtain that

$$\begin{aligned} &S^\top AS = B - cvv^\top \text{ and} \\ &w^\top Aw = c(1-d^2). \end{aligned}$$

Let $Q = S + \lambda wv^\top$ where the constant $\lambda \in F$ can be chosen later. Now we can continue calculating

$$\begin{aligned} Q^\top AQ &= (S + \lambda wv^\top)A(S + \lambda wv^\top) && (3.7) \\ &= S^\top AS + \lambda S^\top Awv^\top + \lambda vw^\top AS + \lambda^2 vw^\top Awv^\top && (3.8) \\ &= B - cvv^\top + \lambda cdvv^\top - \lambda cdvv^\top + \lambda^2 c(1-d^2)vv^\top && (3.9) \\ &= B + (\lambda^2(1-d^2) - 2d\lambda - 1)cvv^\top && (3.10) \\ &= B + \mu cvv^\top, \end{aligned}$$

where we denote

$$\mu = \lambda^2(1-d^2) - 2d\lambda - 1 = \lambda^2 - (d\lambda + 1)^2.$$

Equation (3.7) follows from the definition of the matrix Q. Equation (3.8) follows from Equation (3.7) when we open it. Equation (3.9) follows from Equations (3.6). Finally, Equation (3.10) is just rearranged form of Equation (3.9).

Now we choose lambda so that $\mu = 0$ i.e.

$$\lambda = \begin{cases} \frac{1}{1-d} & \text{if } d \neq 1, \\ -\frac{1}{2} & \text{if } d = 1. \end{cases}$$

When $\mu = 0$, we have $Q^\top AQ = B$ which proves the lemma. □

Theorem 3.5.2 (Witt's cancellation theorem)**.** *Let f, g, h be quadratic forms over F. If $h \perp f \cong h \perp g$, then $f \cong g$.*

Proof. By Theorem 3.4.1, we can assume that the matrices corresponding the quadratic forms f, g and h are diagonal. Let $f = \langle f_1, \dots, f_n \rangle$, $g = \langle g_1, \dots, g_n \rangle$ and $h = \langle h_1, \dots, h_k \rangle$. We apply Lemma 3.5.1 $\dim(h) = k$ times.

Let $1 \leq i \leq k$ be the indexing how many times we have applied Lemma 3.5.1. Following the notation in Lemma 3.5.1 and considering the first application of the lemma i.e. the step $i = 1$, we choose that

$$B = \langle h_2, \ldots, h_k, f_1, \ldots, f_n \rangle,\ A = \langle h_2, \ldots, h_k, g_1, \ldots g_n \rangle \text{ and } c = h_1.$$

Initially, there exists a matrix P because we assumed that $h \perp f \cong h \perp g$ and thus the Equation (3.5) is satisfied by Definition 3.4.2. Each time when we apply Lemma 3.5.1, the element h_i, for $1 \leq i \leq k$, vanishes from the diagonal representation. For the general step i, the matrix P in Lemma 3.5.1 is always the matrix Q_{i-1} which we obtained from the previous application of Lemma 3.5.1. Thus the assumptions of Lemma 3.5.1 are always satisfied. Finally, the lemma gives us a matrix Q such that $Q^\top M_g Q = M_f$. This does not yet prove that Q is invertible which is required by Definition 3.4.2.

Next we argue why there exists an invertible $n \times n$ matrix Q_1 so that $Q_1^\top M_g Q_1 = M_f$. We can write $f = \langle f_1, \ldots, f_n \rangle$ and $g = \langle g_1, \ldots, g_n \rangle$ so that we collect the zeros at the beginning. Without loss of generality, we can assume $f_1 = \ldots = f_r = 0$ and $g_1 = \ldots = g_s = 0$ for $r \leq s$.

By the previous reasoning we obtained an $n \times n$ matrix Q_0 so that $Q_0^\top M_g Q_0 = M_f$ and thus the assumptions of Lemma 3.5.1 are satisfied and we can apply the lemma again.

We apply Lemma 3.5.1 again r times. At every step, Lemma 3.5.1 removes a zero in the diagonal representations of f and g. Finally, we obtain the representation

$$\begin{bmatrix} f_{r+1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & f_n \end{bmatrix} = S^\top \begin{bmatrix} g_{r+1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & g_n \end{bmatrix} S.$$

The determinant of the matrix

$$\begin{bmatrix} f_{r+1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & f_n \end{bmatrix}$$

is non-zero because all the elements $f_{r+1}, \ldots, f_n$ are non-zero. Thus also the determinant

$$\det\left(S^\top \begin{bmatrix} g_{r+1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & g_n \end{bmatrix} S \right) = \det\left(S^\top\right) \det\left(\begin{bmatrix} g_{r+1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & g_n \end{bmatrix} \right) \det(S)$$

is non-zero and $\det(S) \neq 0$. This proves that S is invertible. Hence $\langle f_{r+1}, \ldots, f_n \rangle \cong \langle g_{r+1}, \ldots, g_n \rangle$. Furthermore, this implies that $f \cong g$. This finalizes the proof of the Witt's cancellation theorem. □

3.6 Tsen-Lang theorem

Recall isotropic quadratic forms from Definition 3.4.9. Because Tsen-Lang theorem does not have a big role in this work, we omit its proof.

Theorem 3.6.1 (Tsen-Lang)**.** *Let L be an algebraically closed field and F a finitely generated field extension of transcendence degree n over the field L. Then every nonzero polynomial $f \in F[X_1, \ldots, X_m]$ where $m > \deg(f)^n$ has a nontrivial zero in F^m. Besides, every quadratic form over F of dimension greater than 2^n is isotropic.*

Proof. See Theorem 3.4.1 in [19] or Theorem 6.4.16 in [12]. □

Chapter 4

Pfister forms

4.1 Introduction to Pfister forms

The German mathematician Albrecht Pfister introduced Pfister forms in 1965. Pfister forms are special kinds of quadratic forms that have a crucial role in the proof of the theorem of Bröcker and Scheiderer for basic open semi-algebraic sets. As in the previous chapters, we only focus on those definitions and properties of Pfister forms which will be useful to prove the main theorem.

In this chapter, F is a field whose characteristic is different from two. Recall Definition 2.1.4 of characteristic. The set $F^\star = F \setminus \{0\}$ denotes the multiplicative group of F. Recall Definition 3.4.4 of the tensor product for diagonal forms. The content of this section is based on [12, 19].

Definition 4.1.1 (Pfister form)**.** Let F be a field and $a_1, \dots, a_n \in F$. A *Pfister form* ϕ is a quadratic form

$$\phi = \langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle \otimes \ldots \otimes \langle 1, a_n \rangle$$

of dimension 2^n over the field F. We denote $\phi = \langle\langle a_1, \dots, a_n \rangle\rangle$. The form of dimension $2^n - 1$

$$\phi' = \langle a_1, \dots, a_n, a_1 a_2, \dots, a_1 a_2 \dots a_n \rangle$$

is called a *pure subform of the Pfister form* ϕ. We note that the only difference between the form ϕ and the pure subform ϕ' is the element 1 in the beginning of the diagonal representation. Thus we see that $\phi = \langle 1 \rangle \perp \phi'$.

Example 2. For example, $\otimes_{i=1}^n \langle 1, 1 \rangle$ is a Pfister form. We can write open some simple Pfister forms:

- $\langle\langle a \rangle\rangle = \langle 1, a \rangle = X^2 + aY^2$ and
- $\langle\langle a, b \rangle\rangle = \langle 1, a \rangle \otimes \langle 1, b \rangle = \langle 1, a, b, ab \rangle = X^2 + aY^2 + bZ^2 + abK^2$.

In Definition 3.4.8 we defined nondegenerate quadratic and diagonal forms. Similarly, we can define nondegenerate Pfister forms.

Definition 4.1.2 (Nondegenerate Pfister form)**.** A Pfister form $\langle\langle a_1, \dots, a_n\rangle\rangle$ is *nondegenerate* if $a_1, \dots, a_n \in F^\star = F \setminus \{0\}$.

Because a Pfister form is a special kind of diagonal form, this definition is clearly equivalent with Definition 3.4.8. Recall that we defined multiplicative quadratic forms in Definition 3.4.7.

Theorem 4.1.1 (Multiplicative Pfister forms)**.** *Every Pfister form over a field F is multiplicative.*

Proof. Let ϕ be a Pfister form of dimension 2^n over the field F. We prove the claim by induction with respect to n. Let $n = 0$. Then $\phi = \langle 1\rangle$ is a Pfister form of dimension 1 and $\phi(X) = X^2$. If $\phi(x) \neq 0$, then $\phi(x)$ is an invertible element in F and thus $\phi(x)\phi \cong \phi$.

The induction assumption is that the Pfister form ϕ of dimension 2^{n-1} is multiplicative. It then suffices to prove that $\langle 1, a\rangle \otimes \phi$ for $a \in F^\star$ is multiplicative. By Theorem 3.4.2, we have $\phi \perp a\phi = \langle 1, a\rangle \otimes \phi$. When the quadratic form is evaluated in points $x, x' \in F^{2^n}$, we obtain $\phi\perp a\phi(x \otimes x') = \phi(x) + a\phi(x')$. By Definition 3.4.7, we assume $\phi(x) + a\phi(x') \neq 0$. We need to prove that

$$(\phi\perp a\phi(x \otimes x'))(\phi\perp a\phi) = (\phi(x) + a\phi(x'))\phi\perp a\phi \cong \phi\perp a\phi. \tag{4.1}$$

We divide the proof into three cases. First, assume that $\phi(x') = 0$. Then Equation (4.1) becomes $\phi(x)(\phi\perp a\phi) = \phi(x)\phi\perp a\phi(x)\phi \cong \phi\perp a\phi$ where we use the induction assumption $\phi(x)\phi \cong \phi$.

Second, assume $\phi(x) = 0$ and $\phi(x') \neq 0$. In this case Equation (4.1) becomes

$$a\phi(x')(\phi\perp a\phi) = (a\phi(x')\phi)\perp(a^2\phi(x')\phi) \cong \phi\perp a^2\phi \cong \phi\perp a\phi,$$

where we again use the induction assumption $\phi(x')\phi \cong \phi$.

Third, assume both $\phi(x) \neq 0$ and $\phi(x') \neq 0$. Now we have

$$\begin{align}
(\phi(x) + a\phi(x'))(\phi\perp a\phi) &\cong (\phi(x) + a\phi(x'))(\phi\perp a\phi(x)\phi(x')\phi) \tag{4.2}\\
&\cong (\phi(x) + a\phi(x'))(\langle 1, a\phi(x)\phi(x')\rangle \otimes \phi) \tag{4.3}\\
&\cong \langle \phi(x), a\phi(x')\rangle \otimes \phi \tag{4.4}\\
&\cong \phi(x)\phi\perp a\phi(x')\phi \tag{4.5}\\
&\cong \phi\perp a\phi. \tag{4.6}
\end{align}$$

Equivalence (4.2) follows from the induction assumption that ϕ is multiplicative i.e. $\phi(x)\phi(x')\phi \cong \phi$. Equivalence (4.3) follows from Theorem 3.4.2.

Then Equivalence (4.4) follows from the second part of Lemma 3.4.3. Equivalence (4.5) follows again from Theorem 3.4.2 and the last equivalence follows from the induction assumption. We have proved that every Pfister form is multiplicative. □

We need the following short lemma. The lemma can be viewed as a Pfister version of Lemma 3.4.3.

Lemma 4.1.2. *1. If a, b, $a+b \in F^\star$, then $\langle\langle a, b\rangle\rangle \cong \langle\langle a+b, ab\rangle\rangle$.*

2. If $b \in F^\star$ and b is represented by the Pfister form ϕ, then $\phi \otimes \langle\langle a\rangle\rangle \cong \phi \otimes \langle\langle ab\rangle\rangle$.

Proof. The first part follows immediately from Lemma 3.4.3 when we choose $c = a+b$.

This follows from the property that ϕ is multiplicative. More precisely, because b is represented by the Pfister form ϕ, there exists $x \in F$ such that $\phi(x) = b \neq 0$. Thus

$$\phi \otimes \langle\langle ab\rangle\rangle = \phi \otimes \langle 1, ab\rangle = ab\phi \perp \phi = a\phi(x)\phi \perp \phi \cong a\phi \perp \phi \cong \phi \otimes \langle\langle a\rangle\rangle$$

where we utilized Lemma 3.4.3 and multiplicativity of ϕ. This proves the second part. □

Theorem 4.1.3. *Let $a_1, \ldots, a_n \in F^\star$. For each $i = 1, \ldots, n$ we denote $\phi_i = \langle\langle a_1, \ldots, a_i\rangle\rangle$ the Pfister form. Let u_1 be a square in $F^\star$. For $i = 2, \ldots, n$ let u_i denote the element represented by ϕ_{i-1}. Let $b_i = \sum_{j=i}^{n} a_j u_j$ for each $i = 1, \ldots, n$. If all $b_1, \ldots, b_n$ belong to $F^\star$, then $\phi_n \cong \langle\langle b_1, a_1 b_2, \ldots, a_{n-1} b_n\rangle\rangle$.*

Proof. In this proof we use decreasing induction with respect to k. We prove that

$$\phi_n \cong \phi_k \otimes \langle\langle b_{k+1}, a_{k+1} b_{k+2}, \ldots, a_{n-1} b_n\rangle\rangle$$

holds for $0 \leq k \leq n-1$. We get the wanted result when $k = 0$ and $\phi_0 = \langle 1\rangle$. First we prove that the claim holds in the case $k = n-1$. Then we assume that it holds for the case k and prove that it also holds for the case $k-1$. Then by induction it holds for all $0 \leq k \leq n-1$.

Especially in the case $n-1$, we have $b_n = a_n u_n$ where $u_n \neq 0$ because $b_n \in F^*$. Since u_n is represented by ϕ_{n-1}, we obtain the following

$$\phi_n = \langle\langle a_1, \ldots, a_n\rangle\rangle = \phi_{n-1} \otimes \langle\langle a_n\rangle\rangle \cong \phi_{n-1} \otimes \langle\langle a_n u_n\rangle\rangle = \phi_{n-1} \otimes \langle\langle b_n\rangle\rangle \quad (4.7)$$

where the equivalence follows from the the second part of Lemma 4.1.2. The equivalence

$$\phi_n \cong \phi_{n-1} \otimes \langle\langle b_n\rangle\rangle$$

is exactly the wanted equivalence when we substitute $k = n-1$ to the Equivalence (4.7). This proves that the claim holds in the case $n-1$.

We assume that the claim holds in the case k meaning

$$\phi_n \cong \phi_k \otimes \langle\langle b_{k+1}, a_{k+1}b_{k+2}, \dots, a_{n-1}b_n \rangle\rangle, \tag{4.8}$$

and we study the case $k-1$. We have $\phi_k \otimes \langle\langle b_{k+1} \rangle\rangle \cong \phi_{k-1} \otimes \langle\langle a_k, b_{k+1} \rangle\rangle$ by the definition of ϕ_i. Thus it is sufficient to show that

$$\phi_{k-1} \otimes \langle\langle a_k, b_{k+1} \rangle\rangle \cong \phi_{k-1} \otimes \langle\langle b_k, a_k b_{k+1} \rangle\rangle, \tag{4.9}$$

because when we add the terms $a_{k+1}b_{k+2}, \dots, a_{n-1}b_n$ to the both sides of Equivalence (4.9) we obtain the case k in Equivalence (4.8) which holds by the induction assumption.

First assume $u_k \neq 0$. We can manipulate the form $\phi_{k-1} \otimes \langle\langle a_k, b_{k+1} \rangle\rangle$ using parts 1 and 2 in Lemma 4.1.2. We obtain

$$\begin{aligned} \phi_{k-1} \otimes \langle\langle a_k, b_{k+1} \rangle\rangle &\cong \phi_{k-1} \otimes \langle\langle u_k a_k, b_{k+1} \rangle\rangle & (4.10) \\ &\cong \phi_{k-1} \otimes \langle\langle a_k u_k + b_{k+1}, a_k u_k b_{k+1} \rangle\rangle & (4.11) \\ &\cong \phi_{k-1} \otimes \langle\langle b_k, a_k b_{k+1} \rangle\rangle, & (4.12) \end{aligned}$$

where Equivalence (4.10) follows from the first part of Lemma 4.1.2 (choose $b = u_k \neq 0$), and Equivalence (4.11) follows from the second part of Lemma 4.1.2 (choose $a = a_k u_k$ and $b = b_{k+1}$). Finally, Equivalence (4.12) follows from the first part of Lemma 4.1.2 and the fact that by definition of b_k, we can extract $a_k u_k$ from the sum by

$$b_k = \sum_{j=k}^{n} a_j u_j = a_k u_k + \sum_{j=k+1}^{n} a_j u_j = a_k u_k + b_{k+1}. \tag{4.13}$$

Next assume $u_k = 0$. Then $b_k = b_{k+1}$ which we can immediately see in Equation (4.13). Now

$$\langle\langle a_k, b_{k+1} \rangle\rangle \cong \langle\langle b_k, a_k \rangle\rangle \cong \langle\langle b_k, a_k b_{k+1} \rangle\rangle$$

where we use the second part of Lemma 4.1.2. This finalizes the proof. □

We defined pure subforms of Pfister forms in Definition 4.1.1.

Theorem 4.1.4. *Let $\phi = \langle\langle a_1, \dots, a_n \rangle\rangle$ be a Pfister form over the field F with $a_i \in F^\star$ for $i = 1, \dots, n$. Let b_1 be an element in $F^\star$ represented by a pure subform ϕ'. Then there exists $c_2, \dots, c_n \in F^\star$ such that $\phi \cong \langle\langle b_1, c_2, \dots, c_n \rangle\rangle$.*

Proof. We use the same notation as in the poof of Theorem 4.1.3. We recall that we defined $\phi_i = \langle\langle a_1, \dots, a_i \rangle\rangle$. Now

$$\phi'_i = \langle a_1 \rangle \perp a_2 \phi_2 \perp \cdots \perp a_i \phi_{i-1}, \tag{4.14}$$

where ϕ'_i is the pure subform of ϕ_i for $1 \leq i \leq n$. Equation (4.14) is easy to see, for example, in the case $i = 2$, we have

$$\phi'_2 = \langle a_1, a_2, a_1a_2\rangle = \langle a_1\rangle \perp \langle a_2, a_2a_1\rangle = \langle a_1\rangle \perp a_2\langle 1, a_1\rangle = \langle a_1\rangle \perp a_2\phi_1.$$

Because $\phi'(x) = b_1$ for some $x \in F$, we have $b_1 = a_1u_1 + \ldots + a_nu_n$ where u_1 is a square and u_i is represented by ϕ_i for $i = 2, \ldots, n$. Without loss of generality we can assume that n is the smallest integer of those integers $i \geq 1$ for which ϕ'_i represents b_1. Then $b_1, \ldots, b_n \in F^\star$. By Theorem 4.1.3, it follows that $\phi \cong \langle\langle b_1, a_1b_2, \ldots, a_{n-1}b_n\rangle\rangle$. This proves the result. □

4.2 Pfister forms over fields of rational functions

To benefit from the theory developed for Pfister forms in the context of the theorem of Bröcker and Scheiderer, we represent some results for Pfister forms over the field of rational functions $F(X)$ in the variable X with the coefficients in the field F. The following theorems and their proofs are based on [12]. Recall Definition 3.4.9 of an isotropic quadratic form.

Theorem 4.2.1. *Let ϕ be an anisotropic quadratic form over the field F. Then ϕ is anisotropic over $F(X)$.*

Proof. The theorem can be written equivalently so that if ϕ is isotropic over $F(X)$, then ϕ is an isotropic quadratic form over the field F. Let ϕ be an isotropic quadratic form over $F(X)$. Then there exist $f_1, \ldots, f_n \in F(X)$ so that $\phi(f_1, \ldots, f_n) = 0$ and not every f_i is zero for $i = 1, \ldots, n$. We can assume that all f_i are defined at 0. If f_i is not defined at 0 for some $i = 1, \ldots, n$, then we can multiply f_i by an appropriate power of X. Besides not all $f_i(0)$ are zero for $i = 0, \ldots, n$. Then $(f_1(0), \ldots, f_n(0)) \neq 0$ but $\phi(f_1(0), \ldots, f_n(0)) = 0$ which shows that ϕ is an isotropic over the field F. □

We state the following lemma because the results in this section require estimations with respect to the degrees of quadratic forms.

Lemma 4.2.2. *Let $\phi \in F[X]$ be an anisotropic quadratic form. Then for all $(f_1, \ldots, f_n) \in (F[X])^n$, it holds that*

$$\deg(\phi(f_1, \ldots, f_n)) = 2 \max\{\deg(f_i) \mid i = 1, \ldots, n\}.$$

Proof. This lemma follows immediately from the definition of a quadratic form. Because ϕ is anisotropic, then $\phi(f_1, \ldots, f_n) \neq 0$ for all $(f_1, \ldots, f_n) \in F[X]^n$ by Definition 3.4.9. Because $\deg(f^2) = 2\deg(f)$ for any polynomial, we obtain

$$\deg(\phi(f_1, \ldots, f_n)) = \deg\left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}f_if_j\right) \leq 2 \max\{\deg(f_i) \mid i = 1, \ldots, n\}.$$

Because $\phi(f_1, \ldots, f_n) \neq 0$ for all $(f_1, \ldots, f_n) \in F[X]^n$, we obtain

$$\deg(\phi(f_1, \ldots, f_n)) \geq 2 \max \{\deg(f_i) \mid i = 1, \ldots, n\}.$$

This proves the claim. □

Theorem 4.2.3. *Let $f \in F[X]$ be a polynomial in a single variable with the coefficients in the field F. Let ϕ be a nondegenerate quadratic form over F. If there exists a rational function $q \in (F(X))^n$ such that $\phi(q) = f$, then there exists a polynomial $g \in (F[X])^n$ such that $\phi(g) = f$. In other words, if ϕ represents f over the field $F(X)$, then ϕ represents f over the ring $F[X]$.*

Proof. First, assume that ϕ is isotropic. By Definition 3.4.9, there exists $x \neq 0$ such that $\phi(x) = 0$. By Theorem 3.4.4, there exist $a_3, \ldots, a_n \in F^\star$ such that $\phi \cong \langle 1, -1, a_3, \ldots, a_n \rangle$. Clearly we can write

$$f = ((f-1)/2)^2 - ((f+1)/2)^2.$$

Now we can evaluate the quadratic form

$$\begin{aligned}\phi(((f-1)/2)^2, &((f+1)/2)^2, 0, \ldots, 0) \\ &= \langle 1, -1, a_3, \ldots, a_n \rangle (((f-1)/2)^2, ((f+1)/2)^2, 0, \ldots, 0) \\ &= ((f-1)/2)^2 - ((f+1)/2)^2 = f.\end{aligned}$$

Without even assuming that ϕ represents f over the field $F(X)$, we see that ϕ represents f over the ring $F[X]$ since ϕ represents every element of $F[X]$ over $F[X]$.

Next, assume that ϕ is anisotropic and $f \neq 0$. We consider the following representation of f over $F(X)$

$$f = \phi(g_1/g_0, \ldots, g_n/g_0), \tag{4.15}$$

where $g_1, \ldots, g_n \in F[X]$ and $g_0 \neq 0$. We define a quadratic form

$$\psi = \langle -f \rangle \perp \phi$$

of dimension $n+1$ over $F(X)$. By Definition 3.4.6, this quadratic form is evaluated as $\psi(u) = -fu_0^2 + \phi(u_1, \ldots, u_n)$ for $u = (u_0, \ldots, u_n) \in (F(X))^{n+1}$. We denote $g = (g_0, \ldots, g_n) \in (F[X])^{n+1}$. Using Equation (4.15) we see that

$$\psi(g) = -fg_0^2 + \phi(g_1, \ldots, g_n) = -\phi(g_1/g_0, \ldots, g_n/g_0)g_0^2 + \phi(g_1, \ldots, g_n) = 0. \tag{4.16}$$

If we construct such $x = (1, p_1, \ldots, p_n) \in (F[X])^{n+1}$ that $\psi(x) = 0$, then

$$\phi(p_1, \ldots, p_n) = f.$$

Thus $(p_1, \ldots, p_n)$ is the wanted representation of f over $F[X]$. The suitable zero $(1, p_1, \ldots, p_n)$ can be constructed using the tuple g.

We continue by utilizing an Euclidean division argument. Let $g_i = q_i g_0 + r_i$ be the Euclidean division decomposition for $i = 1, \dots, n$ with $\deg(r_i) < \deg(g_0)$ or $r_i = 0$. If $q = (1, q_1, \dots, q_n)$ is a zero of ψ, we are done. Otherwise, we continue and we can assume $\psi(q) \neq 0$. In this case, g_i and q_i for $i = 1, \dots, n$ are linearly independent in $F(X)$. We use the bilinear form

$$B_\psi(g, q) = g^\top M_\psi q,$$

where the form is defined by Equation (3.4). Now the matrix M_ψ has the dimension $(n+1) \times (n+1)$ and the lengths of g and q are $n+1$. Thus the bilinear form is well-defined. Especially, $\psi(q)g \neq 2B_\psi(g,q)q$ because otherwise g and q would be linearly dependent vectors. This makes $h = \psi(q)g - 2B_\psi(g,q)q$ a nonzero vector of $F(X)^{n+1}$. Now we can calculate that h is actually a zero of ψ

$$\psi(h) = (\psi(q))^2\psi(g) - 4\psi(q)(B_\psi(g,q))^2 + 4(B_\psi(g,q))^2\psi(q) = 0,$$

because $\psi(g) = 0$ by Equation (4.16). The first component h_0 of h is

$$h_0 = \phi(q)g_0 - 2B_\psi(g,q) = \frac{1}{g_0}\phi(r_1, \dots, r_n), \tag{4.17}$$

where some of the $r_1, \dots, r_n$ is nonzero since otherwise we would have $g = g_0 q$ in the Euclidean division. We assumed that ϕ is anisotropic and thus $\phi(r_1, \dots, r_n) \neq 0$. We can estimate the degrees using Lemma 4.2.2

$$\deg(h_0 g_0) = \deg(\phi(r_1, \dots, r_n)) = 2\max(\{\deg(r_i) \mid i = 1, \dots, n\}) < 2\deg(g_0).$$

The first equality follows from Equation (4.17), the second follows Lemma 4.2.2 and the final inequality follows from the fact that all r_i are part of the Euclidean division decomposition with $\deg(r_i) < \deg(g_0)$.

We conclude that we have constructed a zero h of ψ so that $h_0 \neq 0$ and $\deg(h_0) < \deg(g_0)$. Since the degree decreased, we can iterate the process and eventually obtain a zero $(1, p_1, \dots, p_n) \in (F[X])^{n+1}$. This proves the claim. □

Theorem 4.2.4. *Let $a \in F$ and $b_1, \dots, b_n \in F^\star$. Let $n > 1$ and $\phi = \langle b_1, \dots, b_n \rangle$. Assume ϕ is anisotropic. If the form ϕ represents $b_1 X^2 + a$ over $F(X)$, then the diagonal form $\phi' = \langle b_2, \dots, b_n \rangle$ represents a over F.*

Proof. By Theorem 4.2.3, the form ϕ represents $b_1 X^2 + a$ over the ring $F[X]$. This means that there exists an element $f = (f_1, \dots, f_n) \in (F[X])^n$ such that

$$\phi(f) = \sum_{j=1}^{n} b_j f_j^2 = b_1 X^2 + a. \tag{4.18}$$

If ϕ is anisotropic over F, then by Lemma 4.2.2, we have

$$\deg\left(\sum_{j=1}^{n} b_j f_j^2\right) = 2\max(\{\deg(f_j) \mid j = 1, \ldots, n\}).$$

Hence $f_j = c_j X + d_j$ where $c_j, d_j \in F$ for $j = 1, \ldots, n$.

Next we show that there exists at least one such $e \in F$ that $e^2 = (c_1 e + d_1)^2$. Precisely, if $c_1 \neq 1$, then $e = d_1/(1 - c_1) \in F$ is a solution to $e^2 = (c_1 e + d_1)^2$. If $c_1 = 1$, then the equation reduces into a form $2d_1 e + d_1^2 = 0$ which obviously has a solution $e = -d_1/2 \in F$. Thus there exists an element $e \in F$ so that $e^2 = (c_1 e + d_1)^2$.

When we substitute the element e into Equation (4.18), we are able to extract the term $b_1 e^2$ from the sum

$$b_1(c_1 e + d_1)^2 + \sum_{j=2}^{n} b_j(c_j e + d_j)^2 = b_1 e^2 + \sum_{j=2}^{n} b_j(c_j e + d_j)^2 = b_1 e^2 + a,$$

which means that

$$\sum_{j=2}^{n} b_j(c_j e + d_j)^2 = \phi'(c_2 e + d_2, \ldots, c_n e + d_n) = a.$$

By Definition 3.4.9, this proves that ϕ' represents a over the field F. This concludes the proof. □

Theorem 4.2.5. *Let ϕ be a quadratic form over the field F and $f \in F[X_1, \ldots, X_m]$. If ϕ represents f over $F(X_1, \ldots, X_m)$, then ϕ represents $f(a_1, \ldots, a_m)$ over F for every $a_1, \ldots, a_m \in F$.*

Proof. Let ϕ be a quadratic form that represents f over the field

$$F(X_1, \ldots, X_m) = F(X_1, \ldots, X_{m-1})(X_m).$$

This means that there exists a rational function $q \in F(X_1, \ldots, X_{m-1})(X_m)$ with coefficients in $F(X_1, \ldots, X_{m-1})$ so that $\phi(q) = f$. By Theorem 4.2.3, there exists $g \in F(X_1, \ldots, X_{m-1})[X_m]$ so that $\phi(g) = f$. We can express the element g with polynomials $A_1, \ldots, A_n$ with coefficients in $F(X_1, \ldots, X_{m-1})$ so that $f = \phi(A_1(X_m)), \ldots, A_n(X_m))$ where $n = \dim(\phi)$. For every $a_m \in F$ we obtain

$$f(X_1, \ldots, X_{m-1}, a_m) = \phi(A_1(a_m)), \ldots, A_n(a_m)).$$

Thus ϕ represents $f(X_1, \ldots, X_{m-1}, a_m)$ over $F(X_1, \ldots, X_{m-1})$.

We can prove the actual result by induction on m. Assume $m = 1$. Then the result follows immediately from Theorem 4.2.3. We assume that the claim holds for the case $m - 1$ which means that if ϕ represents f

over $F(X_1, \dots, X_{m-1})$, then ϕ represents $f(a_1, \dots, a_{m-1})$ over F for every $a_1, \dots, a_{m-1} \in F$. In the beginning we showed that ϕ represents

$$f(X_1, \dots, X_{m-1}, a_m)$$

over $F(X_1, \dots, X_{m-1})$. That result along with the induction assumption shows that ϕ represents $f(a_1, \dots, a_m)$ over F for every $a_1, \dots, a_m \in F$. This proves the result. □

Theorem 4.2.6. *Let $\phi = \langle a_1, \dots, a_m \rangle$ and $\psi = \langle b_1, \dots, b_n \rangle$ be diagonal quadratic forms over a field F where $a_1, \dots, a_m, b_1, \dots, b_n \in F^\star$. Assume ϕ is anisotropic and represents $\psi(X_1, \dots, X_n) = \sum_{i=1}^n b_i X_i^2$ over the field $F(X_1, \dots, X_n)$. Then there exists a quadratic form θ over F such that ϕ is equivalent to $\psi \perp \theta$. In this case we call that ϕ contains ψ.*

Proof. Again, we proceed by induction on the dimension m of ϕ. When $m = 0$, there is nothing to prove. For $m = 1$, we have $\phi = \langle a_1 \rangle$. Because ϕ represents $\psi(X_1, \dots, X_n)$, we must have $n = 1$. By Theorem 4.2.5, ϕ represents $\psi(c)$ for all $c \in F$. Especially $\langle a_1 \rangle$ represents b_1 when $c = 1$. This means $a_1 x^2 = b_1$ for some $x \in F$. By Definition 3.4.2, $\langle a_1 \rangle \cong \langle b_1 \rangle$ in the case that the dimension of the forms is 1. This proves the claim when $m = 1$.

Assume $m > 0$ and the claim holds for the case $m - 1$. Because ϕ represents $\psi(X_1, \dots, X_n)$, by Theorem 4.2.5 ϕ represents $\psi(a_1, \dots, a_n)$ for all $a_1, \dots, a_n \in F$. When we choose $a_1 = 1$ and $a_i = 0$ otherwise, we obtain that ϕ represents b_1 over the field F. Hence $\phi \cong \langle b_1 \rangle \perp \rho$ for some quadratic form ρ.

By Theorem 4.2.1, ϕ is anisotropic over $F(X_2, \dots, X_n)$. By the assumption, ϕ represents $b_1 X_1^2 + (b_2 X_2^2 + \cdots + b_n X_n^2)$ over the field $F(X_2, \dots, X_n)(X_1)$. By Theorem 4.2.4, the quadratic form ρ represents $(b_2 X_2^2 + \cdots + b_n X_n^2)$ over the field $F(X_2, \dots, X_n)$. The form ρ is anisotropic over F because $\phi \cong \langle b_1 \rangle \perp \rho$ and ϕ and $\langle b_1 \rangle$ are anisotropic. It follows from the induction assumption that $\rho \cong \langle b_2, \dots, b_n \rangle \perp \theta$ for a quadratic form θ over F. Thus

$$\phi \cong \langle b_1 \rangle \perp \rho \cong \langle b_1 \rangle \perp \langle b_2, \dots, b_n \rangle \perp \theta \cong \langle b_1, b_2, \dots, b_n \rangle \perp \theta \cong \psi \perp \theta,$$

which proves the result. □

Recall that in Definition 4.1.1 the pure subform ϕ' of form ϕ satisfy $\phi = \langle 1 \rangle \perp \phi'$. In the following proof we also use an argument related to minimal polynomials. Recall that a minimal polynomial of an element x in the field F is the polynomial f with coefficients in F so that $f(x) = 0$ and the degree of f is the lowest among all the polynomials which have x as a root. More about minimal polynomials can be found in [3].

Theorem 4.2.7. *Let F be a field of transcendence degree d over a real closed field $\mathcal{R}$. Let $\phi = \langle\langle a_1, \dots, a_k \rangle\rangle$ be a Pfister form over the field F where $k > \max\{d, 1\}$. Let ϕ' be a pure subform of ϕ. Then ϕ' represents 1 over F.*

Proof. First, let ϕ be an isotropic form. By Theorem 3.4.4, there exist $a_3, \ldots, a_n \in F^\star$ such that

$$\langle 1 \rangle \perp \phi' = \phi \cong \langle 1, -1, a_3, \ldots, a_n \rangle = \langle 1 \rangle \perp \langle -1, a_3, \ldots, a_n \rangle$$

By Witt's cancellation theorem 3.5.2, we obtain that $\phi' \cong \langle -1, a_3, \ldots, a_n \rangle$. When we evaluate the form $\langle -1, a_3, \ldots, a_n \rangle$ at the point $(1, 0, \ldots, 0) \in F^{n-1}$, we see that the pure subform ϕ' represents -1.

Because the pure subform ϕ' represents -1, by Theorem 4.1.4 there exist $b_2, \ldots, b_k \in F^\star$ so that $\phi \cong \langle\langle -1, b_2, \ldots, b_k \rangle\rangle$. Now we have

$$\langle 1 \rangle \perp \phi' = \phi \cong \langle\langle -1, b_2, \ldots, b_k \rangle\rangle = \langle 1, -1 \rangle \otimes \langle 1, b_2 \rangle \otimes \ldots \otimes \langle 1, b_k \rangle, \quad (4.19)$$

where the form $\langle 1, -1 \rangle \otimes \langle 1, b_2 \rangle \otimes \ldots \otimes \langle 1, b_k \rangle$ contains the form $\langle 1, -1 \rangle \otimes \langle 1, b_2 \rangle$. By Theorem 3.4.2, we manipulate the form $\langle 1, -1 \rangle \otimes \langle 1, b_2 \rangle$ and rewrite it

$$\langle 1, -1 \rangle \otimes \langle 1, b_2 \rangle = \langle 1, b_2 \rangle \perp - \langle 1, b_2 \rangle = \langle 1 \rangle \perp \langle b_2, -b_2 \rangle. \quad (4.20)$$

Now we can substitute the form in Equation (4.20) into Equation (4.19):

$$\langle 1 \rangle \perp \phi' = \langle 1 \rangle \perp \langle b_2, -b_2 \rangle \otimes \ldots \otimes \langle 1, b_k \rangle.$$

Again, by Witt's cancellation theorem 3.5.2 and by the fact that $k \geq 2$, it follows that the subform ϕ' is equivalent to the form $\langle b_2, -b_2 \rangle \otimes \ldots \otimes \langle 1, b_k \rangle$ which contains the form $\langle b_2, -b_2 \rangle$.

The form $\langle b_2, -b_2 \rangle$ represents 1 when we evaluate it at the point $(1/b_2, 0)$. Note that $1/b_2$ is defined because $b_2 \in F^\star$. Thus ϕ' represents 1.

Hence we can assume that ϕ is anisotropic over F. By Definition 4.1.1, the form ϕ has dimension $2^k (> 2^d)$. By Tsen-Lang Theorem 3.6.1, every quadratic form of dimension greater than 2^d is isotropic over the field $F(\sqrt{-1})$ where $\sqrt{-1}$ is the solution to the equation $X^2 + 1 = 0$. This implies that $\sqrt{-1} \notin F$ because otherwise there would exist the anisotropic quadratic form $X^2 + 1$ which contradicts the fact following from the Tsen-Lang theorem.

Also, we have that ϕ is universal over $F(\sqrt{-1})(X, Y)$ which means that ϕ represents every element of the field $F(\sqrt{-1})(X, Y)$. Especially, ϕ represents $X + \sqrt{-1}Y$. Now every element in $F(\sqrt{-1})(X, Y)$ has a form $f + (X + \sqrt{-1}Y)g$ for some $f, g \in F(X, Y)^{2^k}$. Because ϕ represents $X + \sqrt{-1}Y$, by definition there exist $f, g \in F(X, Y)^{2^k}$ so that $\phi(f + (X + \sqrt{-1}Y)g) = X + \sqrt{-1}Y$. Thus we have

$$\phi(g)(X + \sqrt{-1}Y)^2 + (2B_\phi(f, g) - 1)(X + \sqrt{-1}Y) + \phi(f) = 0, \quad (4.21)$$

where B_ϕ is the symmetric bilinear form associated to ϕ as defined in Definition 3.4.1. The rational function $g \neq 0$ because otherwise only $f \in F(X, Y)^{2^k}$ would represent element $X + \sqrt{-1}Y$ where $\sqrt{-1} \notin F$. That is not possible.

Because ϕ is anisotropic over the field $F(X, Y)$ and by Theorem 4.2.1, it follows that $\phi(g) \neq 0$.

We see that the minimal polynomial of the element $X + \sqrt{-1}Y$ is

$$T^2 - 2XT + X^2 + Y^2.$$

Because $\phi(g) \neq 0$, we can divide Equation (4.21) by $\phi(g)$. We obtain

$$(X + \sqrt{-1}Y)^2 + 2\frac{B_\phi(f, g) - 1}{\phi(g)}(X + \sqrt{-1}Y) + \frac{\phi(f)}{\phi(g)} = 0.$$

The last term $\phi(f)/\phi(g)$ corresponds to the term $X^2 + Y^2$ in the minimal polynomial. Thus we obtain

$$\phi(g)(X^2 + Y^2) = \phi(f).$$

Because every Pfister form is multiplicative by Theorem 4.1.1 and $\phi(g) \neq 0$, we obtain

$$\phi(f) = \phi(g)(X^2 + Y^2) \cong X^2 + Y^2.$$

Thus the form ϕ represents $X^2 + Y^2$ over the field $F(X, Y)$. By Theorem 4.2.6, we have $\phi \cong \langle 1, 1\rangle \perp \theta = \langle 1\rangle \perp \langle 1\rangle \perp \theta$. By Witt's cancellation theorem 3.5.2, we obtain $\phi' \cong \langle 1\rangle \perp \theta$. Hence we conclude that ϕ' represents 1 over the field F. □

4.3 Quadratic forms over commutative rings

The theory of quadratic forms of fields naturally extends to quadratic forms over commutative rings. In this subsection, we represent a theorem which is a generalization of Theorem 4.2.7 in the sense that instead of fields, the quadratic forms are defined over commutative rings.

The following definitions generalize the previous Definitions 3.4.8 and 3.4.9. The content of this subsection is based on [12].

Definition 4.3.1 (Nondegenerate quadratic form over ring)**.** Let R be a commutative ring and B be an R-algebra. A quadratic form $\phi = \langle a_1, \ldots, a_m\rangle$ is *nondegenerate over* B if the image of the product $\prod_{i=1}^m a_i$ is invertible in B.

Definition 4.3.2 (Weakly represented)**.** Let R be a ring and B an R-algebra. Let $\phi = \langle a_1, \ldots, a_n\rangle$ be a quadratic form with coefficients in R. An element $b \in B$ is *weakly represented* by ϕ over B if there exist such elements $x_1, \ldots, x_m \in B^m$ that $b = \phi(x_1) + \ldots + \phi(x_m)$.

Recall Definition 2.3.8 of a ring of fractions.

Definition 4.3.3 (Regular functions ring)**.** Let A be a ring of fractions of R-algebra of finite type. The ring A is a *regular functions ring* over $\mathcal{R}$ if every element of form $1 + \sum_{i=1}^{k} a_i^2$ is invertible in A. The transcendence degree of the regular functions ring A over $\mathcal{R}$ is the maximum of transcendence degrees of the residue fields of A over $\mathcal{R}$.

Recall that $\mathcal{P}(V)$ for an algebraic set $V \subset \mathcal{R}^n$ denotes the ring of polynomial functions on V defined in Definition 3.3.7. The following example clarifies how the weakly represented elements in Definition 4.3.2 are connected to represented elements in Definition 3.4.9.

Example 3. In this example we show a simple example of how to understand the connection between weak representations and representations defined in Definition 3.4.9. The example also clarifies the idea behind the proof of the following theorem.

Let $V \subset \mathcal{R}^m$ be an algebraic subset. If the element $v \in \mathcal{P}(V)$ is weakly represented by a Pfister form $\phi = \langle\langle g_1, g_2 \rangle\rangle$ over the ring $\mathcal{P}(V)$, then the element $v(x)$ is represented by $\phi_x = \langle\langle g_1(x), g_2(x) \rangle\rangle$ over the real closed field $\mathcal{R}$.

By Definition 4.1.1 of a Pfister form, we can open the form

$$\begin{aligned}\phi &= \langle\langle g_1, g_2 \rangle\rangle \\ &= \langle 1, g_1 \rangle \otimes \langle 1, g_2 \rangle \\ &= \langle 1, g_1, g_2, g_1 g_2 \rangle \\ &= X^2 + g_1 Y^2 + g_2 Z^2 + g_1 g_2 K^2. \end{aligned} \tag{4.22}$$

For simplicity we consider that v is weakly represented by functions $f_1 \in \mathcal{P}(V)^2$ and $f_2 \in \mathcal{P}(V)^2$. Because v is weakly represented by ϕ over $\mathcal{P}(V)$, then $v = \phi(f_1) + \phi(f_2)$ by Definition 4.3.2. Moreover, we can evaluate the form v at the point $x \in \mathcal{R}^2$ using Equation (4.22). We obtain

$$\begin{aligned} v &= \phi(f_1) + \phi(f_2) \\ &= \langle\langle g_1, g_2 \rangle\rangle(f_1) + \langle\langle g_1, g_2 \rangle\rangle(f_2) \\ &= f_1^2 + g_1 f_1^2 + g_2 f_1^2 + g_1 g_2 f_1^2 + f_2^2 + g_1 f_2^2 + g_2 f_2^2 + g_1 g_2 f_2^2 \\ &= f_1^2 + f_2^2 + g_1(f_1^2 + f_2^2) + g_2(f_1^2 + f_2^2) + g_1 g_2 (f_1^2 + f_2^2). \end{aligned} \tag{4.23}$$

Now we note that when we evaluate the polynomials $f_1, f_2, g_1, g_2 \in \mathcal{P}(V)^2$ at the point $x \in \mathcal{R}^2$, we are able to use the field structure of $\mathcal{R}^2$ in the calculations. In the field $\mathcal{R}^2$ we can write

$$0 \leq f_1(x)^2 + f_2(x)^2 = \left(\sqrt{f_1(x)^2 + f_2(x)^2}\right)^2.$$

Note that such formulation is not possible in the ring $\mathcal{P}(V)^2$. Now we use

Equation (4.23) and evaluate the forms at the point x. We obtain

$$\begin{aligned}
v(x) &= \left(\sqrt{f_1(x)^2+f_2(x)^2}\right)^2 + g_1(x)\left(\sqrt{f_1(x)^2+f_2(x)^2}\right)^2 + \\
&\quad g_2(x)\left(\sqrt{f_1(x)^2+f_2(x)^2}\right)^2 + g_1(x)g_2(x)\left(\sqrt{f_1(x)^2+f_2(x)^2}\right)^2 \\
&= y^2 + g_1(x)y^2 + g_2(x)y^2 + g_1(x)g_2(x)y^2 \\
&= \langle 1, g_1(x), g_2(x), g_1(x)g_2(x)\rangle(y) \\
&= \langle\langle g_1(x), g_2(x)\rangle\rangle(y) = \phi_x(y)
\end{aligned}$$

where $y = \sqrt{f_1(x)^2+f_2(x)^2}$. This shows that the form $\phi_x = \langle\langle g_1(x), g_2(x)\rangle\rangle$ represents the element $v(x)$ if the form ϕ weakly represents the element v.

Theorem 4.3.1. *Let $V \subset \mathcal{R}^m$ be an algebraic subset. If the element $v \in \mathcal{P}(V)$ is weakly represented by a Pfister form $\phi = \langle\langle g_1, \dots, g_n\rangle\rangle$ over the ring $\mathcal{P}(V)$, then the element $v(x)$ is represented by $\phi_x = \langle\langle g_1(x), \dots, g_n(x)\rangle\rangle$ over the real closed field $\mathcal{R}$.*

Proof. Because v is weakly represented by ϕ over $\mathcal{P}(V)$, it follows that there exist elements $f_1, \dots, f_k \in (\mathcal{P}(V))^n$ such that $v = \phi(f_1) + \ldots + \phi(f_k)$ by Definition 4.3.2. When we open the Pfister forms as in Example 3, we obtain that

$$\begin{aligned}
v(x) &= (\phi(f_1) + \ldots + \phi(f_k))(x) \\
&= \langle\langle g_1(x), \dots, g_n(x)\rangle\rangle(y) \\
&= \phi_x(y)
\end{aligned}$$

where $y = \sqrt{f_1(x)^2 + \ldots + f_k(x)^2}$. This shows that ϕ_x represents element $v(x)$. □

The following lemma is technical but in some sense, it is the Pfister version of Theorem 4.1.3. Recall Definition 4.1.2 of a nondegenerate Pfister form.

Lemma 4.3.2. *Let $V \subset \mathcal{R}^n$ be an algebraic subset. Let $g_1, \dots, g_m \in \mathcal{P}(V)$ be polynomials and let $\phi_i = \langle\langle g_1, \dots, g_i\rangle\rangle$ denote the Pfister form for each $i = 1, \dots, m$. Let v_1 be a sum of squares in $\mathcal{P}(V)$ and v_{i+1} be an element which is weakly represented by ϕ_i over $\mathcal{P}(V)$ for $i = 1, \dots, m-1$. Define $w_i = \sum_{j=i+1}^{m} g_j v_j$ for $i = 1, \dots, m-1$. Let $\psi = \langle\langle w_0, g_1w_1, \dots, g_{m-1}w_{m-1}\rangle\rangle$ be a Pfister form. Let $x \in V$ be such that both forms $(\phi_m)_x = \langle\langle g_1(x), \dots, g_m(x)\rangle\rangle$ and $\psi_x = \langle\langle w_0(x), g_1w_1(x), \dots, g_{m-1}w_{m-1}(x)\rangle\rangle$ are nondegenerate. Then $(\phi_m)_x \cong \psi_x$.*

Proof. First we argue why the assumptions of Theorem 4.1.3 are satisfied. We choose $b_1 = w_0(x)$, $a_i = g_i$ and $u_i = v_i$. First, $v_1(x)$ is a square in $\mathcal{R}$ because v_1 is a sum of squares in $\mathcal{P}(V)$. Second, $v_{i+1}(x)$ is represented by $(\phi_i)_x$ over $\mathcal{R}$ for $i = 1, \ldots, m-1$ by Lemma 4.3.1. Third, all $w_i(x)$ are invertible because both forms $(\phi_m)_x = \langle\langle g_1(x), \ldots, g_m(x)\rangle\rangle$ and $\psi_x = \langle\langle w_0(x), g_1 w_1(x), \ldots, g_{m-1}w_{m-1}(x)\rangle\rangle$ are nondegenerate and thus $w_i(x) = \sum_{j=i+1}^{m} g_j v_j(x) \neq 0$ for $i = 1, \ldots, m-1$.

Using the notation in Theorem 4.1.3, we obtain $b_{i+1} = \sum_{j=i+1}^{m} a_j u_j = \sum_{j=i+1}^{m} g_j v_j = w_i$. We deduce that

$$\begin{aligned}(\phi_m)_x &= \langle\langle g_1(x), \ldots, g_m(x)\rangle\rangle \\ &= \langle\langle a_1(x), \ldots, a_m(x)\rangle\rangle \\ &\cong \langle\langle b_1(x), a_1 b_2(x), \ldots, a_{n-1}b_n(x)\rangle\rangle \\ &= \langle\langle w_0(x), g_1 w_1(x), \ldots, g_{m-1}w_{m-1}(x)\rangle\rangle \\ &= \psi_x\end{aligned}$$

where the equivalency of the Pfister forms is based on Theorem 4.1.3. This proves the theorem. □

The beginning of the proof of the following theorem utilizes nilradicals and nilpotent elements of a ring that we defined in Definitions 2.1.6 and 2.1.7. The theorem can be viewed as a Pfister version of Theorem 4.2.7 for commutative rings. Recall Definition 2.3.7 of transcendence degree and Definition 4.3.3 of a regular functions ring.

Theorem 4.3.3. *Let A be a regular functions ring of transcendence degree d over $\mathcal{R}$. Let $\phi = \langle\langle a_1, \ldots, a_n\rangle\rangle$ be a nondegenerate Pfister form with coefficients in A where $n > \max(d, 1)$. Then the pure subform ϕ' weakly represents the element 1 over A.*

Before the theorem we prove two lemmas. Recall Definition 2.1.7 of a nilradical ideal.

Lemma 4.3.4. *Let A be a regular functions ring of transcendence degree d over $\mathcal{R}$. Let N be the nilradical of A. Then the quotient ring A/N is also a regular functions ring of transcendence degree d over $\mathcal{R}$.*

Proof. If A is a regular functions ring, then every quotient ring of A is also regular functions ring because all the elements of the form $[1] + \sum_{i=1}^{k}[a_i]^2$ are invertible in the quotient ring. Here the brackets denote the equivalence classes of A/N.

The transcendence degree for A/N over $\mathcal{R}$ is the same as for A because the transcendence basis for A/N consist of equivalence classes of the transcendence basis of A i.e. there is bijective mapping between the bases. We consider this more precisely in the following.

Clearly the correspondence between the transcendence basis of A and the transcendence basis of A/N is surjective since every equivalence class in the transcendence basis of A/N corresponds some element in A.

Next, we consider injectivity. If x_1, x_2 are two distinct elements in the transcendence basis of A, then it means that they belong to separate equivalence classes in the quotient ring A/N. If the elements belong to the same class, for example, $x_1 \in x_2 + N$, then $x_1 - x_2 \in N$. Then by Definition 2.1.7 we have $(x_1 - x_2)^n = 0$ for some positive n. The condition $(x_1 - x_2)^n = 0$ also indicates that there is a polynomial $f \in R[X, Y]$ so that $f(x_1, x_2) = 0$. This contradicts the assumption that x_1 and x_2 are algebraically independent which we defined in Definition 2.3.6. □

Recall that radicals are defined in Definition 2.1.5.

Lemma 4.3.5. *In Theorem 4.3.3 it suffices to consider that the regular functions ring A is the radical A/N.*

Proof. Let N be the nilradical of A. Now we show that if 1 is weakly represented by ϕ' over the radical A/N, then 1 is weakly represented by ϕ' over A. Thus, in the context of Theorem 4.3.3, it suffices to consider that A is the radical A/N.

If 1 is weakly represented by ϕ' over A/N, then there exists a nilpotent element $b \in N$ so that

$$\phi'(a_1) + \ldots + \phi'(a_k) = 1 + b,$$

where $a_1, \ldots, a_k \in A$. The element $1 + b \neq 0$ and thus it is invertible in A. Also, $1 + b$ has a square root s in A because it is weakly represented by a sum of Pfister forms i.e. if we open the sum $\phi'(a_1) + \ldots + \phi'(a_k)$, we obtain the element s so that $s^2 = 1 + b$.

Because $\phi'(a_1) + \ldots + \phi'(a_k) = s^2$ and by dividing both sides by s, we obtain the weak representation $\phi'(a_1/s) + \ldots + \phi'(a_k/s) = 1$. Thus we can assume that A is radical. □

Now we proceed to the proof of Theorem 4.3.3. Recall Definition 2.3.9 of total ring of fractions.

Proof. We proceed by induction on the transcendence degree d. First, let $d = 0$. That means that A is algebraic over $\mathcal{R}$. It also means that A is a finite product of spaces $\mathcal{R}$. If A is an infinite product of spaces $\mathcal{R}$, then we can construct an element $x \in A$ such that x is not algebraic over A.

Because $n \geq 2$, then it is not possible that all the coefficients of ϕ' are negative in each copy of $\mathcal{R}$ since if $a_i < 0$ and $a_j < 0$ are coefficients of ϕ' in some copy of $\mathcal{R}$, then the coefficient $a_i a_j$ is positive in $\mathcal{R}$. Without loss of generality, we assume that the positive coefficient is a_1. Then

$$\begin{aligned}\phi'\left(1/\sqrt{a_1}, 0, \ldots, 0\right) &= \langle a_1, \ldots, a_n, a_1a_2, \ldots, a_1a_2 \ldots a_n\rangle \left(1/\sqrt{a_1}, 0, \ldots, 0\right) \\ &= a_1 \left(1/\sqrt{a_1}\right)^2 = 1\end{aligned}$$

Thus ϕ' represents 1 over A.

Assume then that $d > 0$ and the claim holds for all regular functions fields of transcendence degree less than d over $\mathcal{R}$. By Theorem 2.3.2, we can embed A into the total ring of fractions denoted by K. The ring K consists of all the elements of A and their multiplicative inverses. By Theorem 2.3.3, the ring of fractions K is the product of residue fields of A at its minimal prime ideals. Each of these residue fields has a transcendence degree at most d over $\mathcal{R}$ which we can deduce similarly as in the proof of Lemma 4.3.4. Thus the transcendence degree of K is at most d.

Now we can apply Theorem 4.2.7 and obtain that ϕ' represents 1 over the field K. Thus there exists $u/f \in K$ such that $1 = \phi'(u/f)$ where $u, f \in A$. When we clear the denominator by multiplying f^2, we obtain $f^2 = \phi'(u)$. If f is invertible in A, then we immediately obtain $1 = \phi'(u/f)$ as a weak representation of 1.

Let us consider the case that f is not invertible. We denote (f) the ideal of A generated by the element f. The ring $A/(f)$ is a regular functions ring of transcendence degree less than d over A which we can argue similarly as in the proof of Lemma 4.3.4. By the induction assumption, 1 is weakly represented by ϕ' over the ring $A/(f)$. This means that there exist elements $a_1, \ldots, a_k \in A/(f)$ such that

$$1 - bf = \phi'(a_1) + \ldots + \phi'(a_k).$$

When we reorganize the terms, take the squares and use the previous fact that $f^2 = \phi'(u)$, we obtain

$$\begin{aligned}(1 - \phi'(a_1) - \ldots - \phi'(a_k))^2 &= 1 - 2(\phi'(a_1) + \ldots + \phi'(a_k)) \\ &\quad + (\phi'(a_1) + \ldots + \phi'(a_k))^2 \\ &= 1 - (\phi'(\sqrt{2}a_1) + \ldots + \phi'(\sqrt{2}a_k)) \\ &\quad + (\phi'(a_1) + \ldots + \phi'(a_k))^2 \\ &= b^2 f^2 = b^2 \phi'(u) = \phi'(bu).\end{aligned}$$

When we reorganize the terms, we obtain

$$1 + s^2 = \phi'(y_1) + \ldots + \phi'(y_{k+1}),$$

where $s = \phi'(a_1) + \ldots + \phi'(a_k)$, $y_1 = bu$, and $y_{i+1} = \sqrt{2}a_i$ for $i = 1, \ldots, k$. By Definition 4.3.3 of regular functions ring, the element $1 + s^2$ is invertible in A. Thus we can manipulate the expression the following way

$$\begin{aligned}(1+s^2)^2 &= (1+s^2)\sum_{i=1}^{k+1}\phi'(y_i)\\ &= \sum_{i=1}^{k+1}\phi'(y_i) + s^2\sum_{i=1}^{k+1}\phi'(y_i)\\ &= \sum_{i=1}^{k+1}\phi'(y_i) + \sum_{i=1}^{k+1}\phi'(sy_i).\end{aligned}$$

When we divide the expression by $(1+s^2)^2$, we obtain

$$1 = \sum_{i=1}^{k+1}\phi'\left(\frac{y_i}{1+s^2}\right) + \sum_{i=1}^{k+1}\phi'\left(\frac{sy_i}{1+s^2}\right),$$

which proves that 1 is weakly represented by ϕ' over A. □

Chapter 5

Theorem of Bröcker and Scheiderer

5.1 One-dimensional example

Before we formally present and prove the main theorem, we introduce a few examples which motivate the result as well as give insights into the constructive perspectives of the main theorem. The thesis [22] is studying constructive approaches to the theorem of Bröcker and Scheiderer.

We formulate one of the simplest examples in the one-dimensional case where the reals $\mathbb{R}$ serve as the real closed field. Let us fix a basic semi-algebraic subset

$$V = \{x \in \mathbb{R} \mid x < 1,\ x > -1\} = \{x \in \mathbb{R} \mid 1 - x > 0,\ x + 1 > 0\} =]-1, 1[.$$

Now the theorem of Bröcker and Scheiderer implies that there exists a single polynomial $f \in \mathbb{R}[X]$ so that $V = \{x \in \mathbb{R} \mid f(x) > 0\}$. It is easy to see that the polynomial is $f(x) = -(1-x)(x+1) = 1 - x^2$ which is a parabola opening downwards and positive on $]-1, 1[$. Often in the constructive methods, one of the polynomials is the product of all the polynomials that define the basic semi-algebraic set. This leads to the property that the degree of the reduced polynomials tends to grow large compared to the original polynomials.

5.2 Two-dimensional example

The author in [22] develops a constructive method for a two-dimensional case where the polynomials are linear. We demonstrate the constructive method

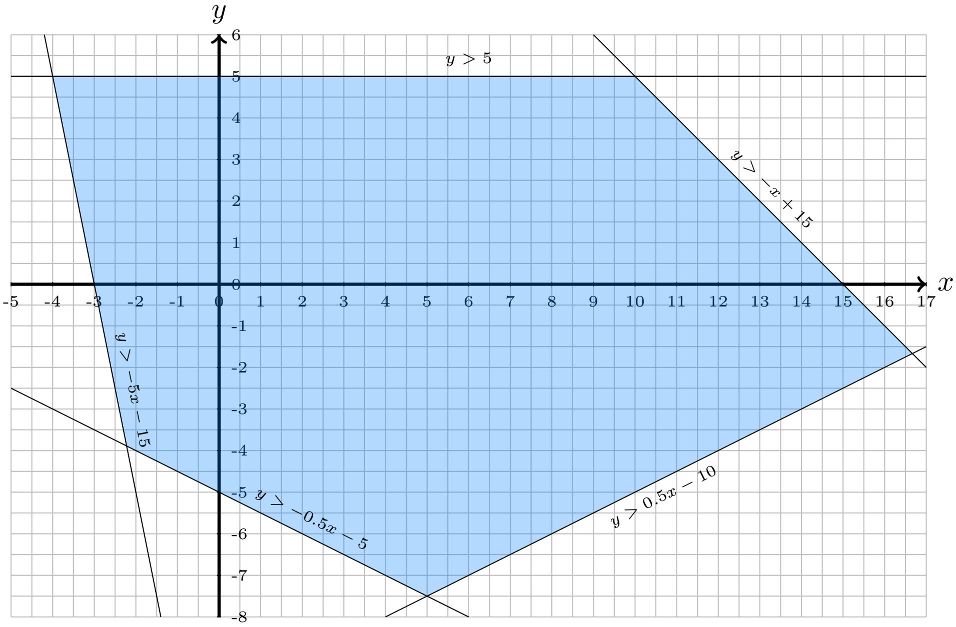

Figure 5.1: Semi-algebraic set V defined by the polynomials f_1, f_2, f_3, f_4 and f_5.

by a concrete example. For example, let the semi-algebraic set be

$$V = \{(x, y) \in \mathbb{R}^2 \mid f_1(x, y) = -y + 5 > 0,\ f_2(x, y) = y + 5x + 15 > 0,$$
$$f_3(x, y) = y + \frac{1}{2}x + 5 > 0,\ f_4(x, y) = y - \frac{1}{2}x + 10 > 0,\ f_5(x, y) = -y - x + 15 > 0\}.$$

Figure 5.1 shows the semi-algebraic set in the plane. By the theorem of Bröcker and Scheiderer, there exist two polynomials that define the set V. As in the one dimensional case, the first polynomial is simply $f(x, y) = \prod_{1=1}^{5} f_i(x, y)$.

Next we construct the second polynomial. First, we see that the points, where the polynomials $f_1, \ldots, f_5$ are intersecting, are the following:

- f_1 intersects with f_2 at $y_1 = (-4, 5)$,
- f_2 intersects with f_3 at $y_2 = (-20/9, -35/9) \approx (-2.22, -3.89)$,
- f_3 intersects with f_4 at $y_3 = (5, -15/2)$,
- f_4 intersects with f_5 at $y_4 = (50/3, -5/3) \approx (16.67, -1.667)$, and
- f_5 intersects with f_1 at $y_5 = (10, 5)$.

Following the construction presented in [22], we choose linear functions $g_i \colon \mathbb{R}^2 \to \mathbb{R}$ so that $g_i(y_i) > 0$ and $g_i(y_j) < 0$ for $i \neq j$. We can find these linear functions by solving five systems of linear inequalites. For example, the system for the first polynomial $g_1(x,y) = ax + by + c$ is

$$\begin{cases} -4a + 5b + c > 0 \\ -\frac{20}{9}a - \frac{35}{9}b + c < 0 \\ 5a - \frac{15}{2}b + c < 0 \\ \frac{50}{3}a - \frac{5}{3}b + c < 0 \\ 10a + 5b + c < 0. \end{cases}$$

For example, we can choose the following polynomials: $g_1(x,y) = -x + y$, $g_2(x,y) = -x - y - 3$, $g_3(x,y) = x - 9y - 33$, $g_4(x,y) = x - 11$ and $g_5(x,y) = x + 4y - 17$.

We set $p_i(x) = g_i(x)^2$ for $i = 1, \ldots, 5$. Next, we need to solve the coefficients c_i for $j = 1, \ldots, 5$ from the equation:

$$\sum_{i=1}^{5} c_i p_i(y_j) = 1.$$

We express the equation as

$$\begin{bmatrix} p_1(y_1) & \ldots & p_5(y_1) \\ \vdots & \vdots & \vdots \\ p_1(y_5) & \ldots & p_5(y_5) \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_5 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}.$$

The thesis [22] proves that the solution always exists and it is unique. In this example we obtain the solution

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 173029/297265948 \\ 639747/297265948 \\ 3450/74316487 \\ 32671/12133304 \\ 249119/594531896 \end{bmatrix}$$

Then the second polynomial is

$$g(x,y) = 1 - \sum_{i=1}^{5} c_i g_i(x,y)$$

and $V = \{(x,y) \in \mathbb{R}^2 \mid f(x,y) > 0,\ g(x,y) > 0\}$. See Figure 5.2 for visualization of these polynomials.

5.3 Theorem of Bröcker and Scheiderer for basic open semi-algebraic sets

The following theorem is the main result of this work. Note that the constant $k > 0$ can be much larger than the dimension of the algebraic set. The proof is based on [12]. Another proof can be found in [23].

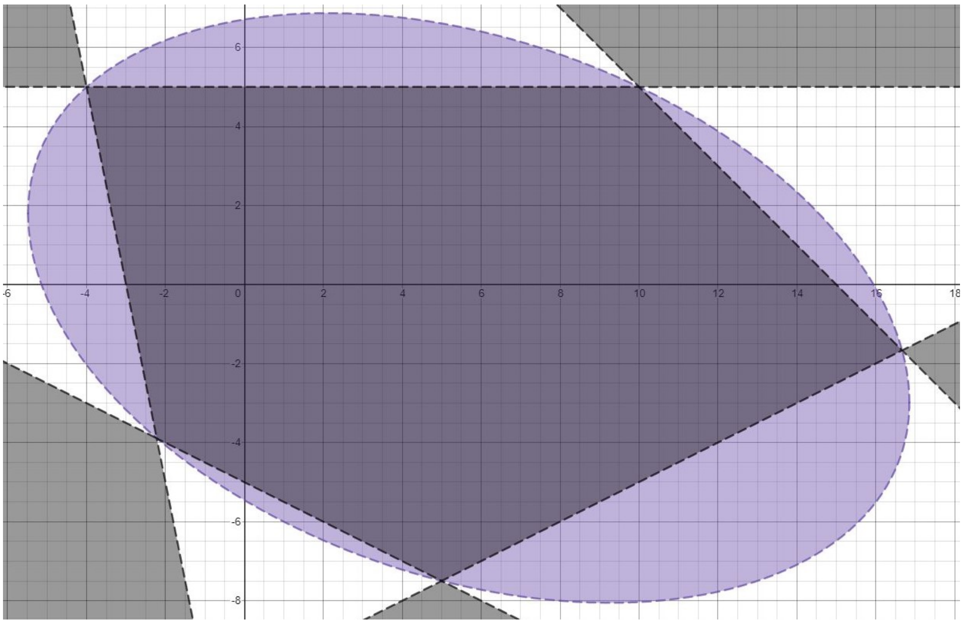

Figure 5.2: The semi-algebraic set V expressed with the polynomials f and g. The set $\{(x, y) \mid f(x, y) > 0\}$ defines the gray area and the set $\{(x, y) \mid g(x, y) > 0\}$ defines the purple area. Their intersection is the set V.

Theorem 5.3.1 (Theorem of Bröcker and Scheiderer for basic open semi-algebraic sets)**.** *Let V be an algebraic subset of $\mathcal{R}^n$ with dimension $d > 0$. Then every basic open semi-algebraic subset $U \subset V$ can be defined by d simultaneously strict inequalities. In other words, if $k > 0$ and*

$$U = \{x \in V \mid g_1(x) > 0, \ldots, g_k(x) > 0\} \tag{5.1}$$

where $g_i \in \mathcal{R}[X_1, \ldots, X_n]$ for $1 \leq i \leq k$, then there exist $f_1, \ldots, f_d \in \mathcal{P}(V)$ so that

$$U = \{x \in V \mid f_1(x) > 0, \ldots, f_d(x) > 0\}.$$

Proof. Let V be an algebraic subset of $\mathcal{R}^n$ with dimension $d > 0$. It suffices to prove the theorem in the case when $U = \mathcal{U}(g_1, \ldots, g_{d+1})$. For the cases when we have more than $d+1$ inequalities, we can iteratively apply the result until we reach the system of d inequalities. Let

$$\Sigma U = \{h \in \mathcal{P}(V) \mid h(x) > 0 \text{ for all } x \in U\}$$

be the set of those polynomials which are positive on U. Let

$$B = (\Sigma U)^{-1}\mathcal{P}(V)$$

be the ring of fractions which is well-defined since ΣU is multiplicative submonoid of $\mathcal{P}(V)$. Recall the notation $(\Sigma U)^{-1}\mathcal{P}(V)$ and the definition of the ring of fractions in Definition 2.3.8. Considering the notation in the definition we choose $S = \Sigma U$.

The ring B is a regular functions ring of transcendence degree at most d over $\mathcal{R}$ because the elements $1 + \sum_{i=1}^{m} f_i^2$ are invertible for $f_i \in B$. The fact that the elements of form $1+\sum_{i=1}^{m} f_i^2$ are invertible follows immediately from the construction of B where we include the inverses of the nonzero elements by Definition 2.3.8.

Next we show that the transcendence degree of B is at most d. By Definition 3.3.7, we have $\dim(V) = \dim(\mathcal{P}(V))$. The canonical ring homomorphism $i\colon \mathcal{P}(V) \to (\Sigma U)^{-1}\mathcal{P}(V)$ (see Theorem 2.3.2) shows that

$$d = \dim(V) = \dim(\mathcal{P}(V)) \geq \dim((\Sigma U)^{-1}\mathcal{P}(V)) = \dim(B).$$

By Theorem 3.3.2, we obtain that the transcendence degree of B is at most d.

For nondegenerate Pfister forms recall Definition 4.1.2. The Pfister form $\phi = \langle\langle g_1, \ldots, g_{d+1}\rangle\rangle$ is nondegenerate over B because $g_1, \ldots, g_{d+1} \in B \setminus \{0\}$ by assumption that $g_i(x) > 0$ for all $x \in U$ and for $i = 1, \ldots, d+1$.

In the following we will reformulate Pfister forms so that we can utilize Lemma 4.3.2. By Theorem 4.3.3, the pure subform ϕ' of the Pfister form ϕ weakly represents 1 over the ring B. By Definition 4.3.2, this means that there exist elements $p_1, \ldots, p_l \in B$ such that $1 = \phi'(p_1) + \ldots + \phi'(p_l)$. When we multiply the representation by the square $(1 - g_{d+1} + g_{d+1}^2)^2$, we obtain that

$$(1-g_{d+1}+g_{d+1}^2)^2 = \phi'(p_1(1-g_{d+1}+g_{d+1}^2))+\ldots+\phi'(p_l(1-g_{d+1}+g_{d+1}^2)). \quad (5.2)$$

Hence ϕ' also weakly represents the square $(1-g_{d+1}+g_{d+1}^2)^2$ over the ring B. Following the convention we denote $\phi_i = \langle\langle g_1, \ldots, g_i\rangle\rangle$ for $i = 1, \ldots, d+1$. When we repeat Theorem 3.4.2 for the subform ϕ', we can write

$$\phi' = g_1\langle 1\rangle \perp g_2\phi_1 \perp \ldots \perp g_{d+1}\phi_d. \quad (5.3)$$

We can compare this representation for the similar one we obtained in the proof of Theorem 4.1.4. When we open the square, we have the following equation

$$(1 - g_{d+1} + g_{d+1}^2)^2 = (1 + g_{d+1}^2)^2 - 2(1 + g_{d+1}^2)g_{d+1} + g_{d+1}^2.$$

Next we evaluate each ϕ' in Equation (5.2) using Equation (5.3). More precisely, let $y_i = p_i(1 - g_{d+1} + g_{d+1}^2)$ for $1 \leq i \leq l$. Using Equation (5.3) we obtain

$$\phi'(y_i) = g_1(y_i)^2 + g_2\phi_1(y_i) + \ldots g_{d+1}\phi_d(y_i) \quad (5.4)$$

for $1 \leq i \leq l$. Thus we can calculate

$$\begin{aligned}
(1 + g_{d+1}^2)^2 &= \phi'(p_1(1 - g_{d+1} + g_{d+1}^2)) + \ldots + \phi'(p_l(1 - g_{d+1} + g_{d+1}^2)) \\
&\quad + 2(1 + g_{d+1}^2)g_{d+1} - g_{d+1}^2 && (5.5)\\
&= \phi'(y_1) + \ldots + \phi'(y_l) + 2(1 + g_{d+1}^2)g_{d+1} - g_{d+1}^2 && (5.6)\\
&= 2(1 + g_{d+1}^2)g_{d+1} - g_{d+1}^2 + \\
&\quad \sum_{i=1}^{l} \left(g_1 y_i^2 + g_2\phi_1(y_i) + \ldots + g_{d+1}\phi_d(y_i)\right) && (5.7)\\
&= g_1\left(\sum_{i=1}^{l} y_i^2\right) + g_2\left(\sum_{i=1}^{l} \phi_1(y_i)\right) + \ldots \\
&\quad + g_{d+1}\left(2(1 + g_{d+1}^2) - g_{d+1} + \sum_{i=1}^{l} \phi_d(y_i)\right) && (5.8)\\
&= g_1u_1 + g_2u_2 + \ldots + g_du_d + g_{d+1}(u_{d+1} + 2(1 + g_{d+1}^2)). && (5.9)
\end{aligned}$$

We obtain Equation (5.5) by adding the term $2(1 + g_{d+1}^2)g_{d+1} - g_{d+1}^2$ on the both sides of Equation (5.2). Equation (5.6) follows from the property that we set $y_i = p_i(1 - g_{d+1} + g_{d+1}^2)$ for $1 \leq i \leq l$. Equation (5.7) follows from the calculation where we open the forms $\phi'(y_i)$ using Equation (5.4) for $1 \leq i \leq l$. Equation (5.8) is obtained by reorganizing the terms and taking g_i for $1 \leq i \leq d+1$ as a common divisor. Finally, we obtain Equation

(5.9) by writing that $u_1 = \sum_{i=1}^{l} y_i^2$ and $u_{j+1} = \sum_{i=1}^{l} \phi_j(y_i)$ for $j = 1, \ldots, d$. We immediately see that u_1 is a sum of squares in B and u_{j+1} is weakly represented by ϕ_j over B for $j = 1, \ldots, d$.

We note that $u_{d+1} + 2(1+g_{d+1}^2)$ is positive on U. When we multiply Equation (5.9) with suitable squares so that we clear the possible denominators, we get the following equation in $\mathcal{P}(V)$

$$w_0 = g_1 v_1 + g_2 v_2 + \ldots + g_d v_d + g_{d+1} v_{d+1}, \tag{5.10}$$

where the setting satisfies the assumptions of Lemma 4.3.2. More precisely, the element w_0 is a square in $\mathcal{P}(V)$ since it is $(1 + g_{d+1}^2)^2$ multiplied by squared terms, v_1 is a sum of squares in $\mathcal{P}(V)$ since u_1 is a sum of squares, and v_{i+1} are weakly represented by ϕ_i over $\mathcal{P}(V)$ because u_i are weakly represented by ϕ_i over $\mathcal{P}(V)$ for $i = 1, \ldots, d$. Besides, v_{d+1} is positive on U since $u_{d+1} + 2(1 + g_{d+1}^2)$ is positive on U.

Let $w_i = \sum_{j=i+1}^{d+1} g_j v_j$ for $i = 0, \ldots, d$ and $\psi = \langle\langle w_0, g_1 v_1, \ldots, g_d w_d \rangle\rangle$. Now we can use Lemma 4.3.2. For $x \in V$, we used the notation

$$\psi_x = \langle\langle w_0(x), g_1 w_1(x), \ldots, g_d w_d(x) \rangle\rangle$$

in the proof of Lemma 4.3.2. For every $x \in V$ so that ϕ_x and ψ_x are nondegenerate, we have that $\phi_x \cong \psi_x$. We define $f_i = g_i w_i$ for $i = 1, \ldots, d$. Now we are ready to prove that

$$U = \mathcal{U}(f_1, \ldots, f_d) = \{x \in V \mid f_1(x) > 0, \ldots, f_d(x) > 0\}.$$

We note that v_j are positive for $j = 1, \ldots, d$ on U. This follows from the fact that v_j are the sum of squares divided by suitable positive elements as the previous construction showed. This means that w_j are also positive for $j = 1, \ldots, d$ on U. Thus we can estimate $f_i = g_i w_i \geq g_i > 0$. Because $g_i > 0$, it follows that $f_i > 0$ on U. Hence the inclusion to the first direction follows easily

$$\begin{aligned} U &= \mathcal{U}(g_1, \ldots, g_{d+1}) \\ &= \{x \in V \mid g_1(x) > 0, \ldots, g_{d+1}(x) > 0\} \\ &\subset \{x \in V \mid f_1(x) > 0, \ldots, f_d(x) > 0\} \\ &= \mathcal{U}(f_1, \ldots, f_d). \end{aligned}$$

Next we show that $\mathcal{U}(f_1, \ldots, f_d) \subset U$. Let $x \in \mathcal{U}(f_1, \ldots, f_d)$. Every polynomial $g_1, \ldots, g_{d+1}$ divide the product $\prod_{i=1}^{d} f_i$ because by definition $f_i = g_i w_i$ for $i = 1, \ldots, d$. The case that g_{d+1} divides the product follows from the fact that we defined $w_i = \sum_{j=i+1}^{d+1} g_j v_j$ and the polynomial g_{d+1} is a part of the sum. It follows that the form $\psi_x = \langle\langle w_0(x), g_1 w_1(x), \ldots, g_d w_d(x) \rangle\rangle$ is nondegenerate in the sense of Definition 4.3.1. Because

$$w_0 = \sum_{j=1}^{d+1} g_j v_j = g_1 v_1 + \sum_{j=2}^{d+1} g_j v_j = g_1 v_1 + w_1$$

we obtain by multiplying g_1 that $g_1 w_0 = g_1^2 v_1 + g_1 w_1 = g_1^2 v_1 + f_1$ because we set $f_1 = g_1 w_1$. Because $g_1 w_0 = g_1^2 v_1 + f_1$ is positive on $\mathcal{U}(f_1, \ldots, f_d)$ and w_0 is square, we have $w_0(x) > 0$. Thus the form

$$\psi_x = \langle\langle w_0(x), g_1 w_1(x), \ldots, g_{m-1} w_{m-1}(x) \rangle\rangle$$

is nondegenerate and it has a positive signature. Recall Definition 3.4.5 of a signature. By the reasoning we did in the beginning of the proof, we concluded that $\phi_x \cong \psi_x$ for nondegenerate forms ϕ_x and ψ_x. Thus it follows that the signature of ϕ_x is also positive which implies that $g_i(x) > 0$ for $i = 1, \ldots, d+1$ by Definition 3.4.5. Thus $x \in U$. This proves the theorem of Bröcker and Scheiderer for basic open semi-algebraic sets. □

The result is fascinating for a reason. Despite the fact that k can be arbitrarily large, there always exist polynomials f_i and their number depends only on the dimension of V. Generally, we can drop the requirement of strict inequalities in Equation (5.1). In this case the bound will increase to $d(d+1)/2$. Nevertheless, the bound still depends on the dimension of the algebraic subset V.

5.4 Conclusion

Semi-algebraic geometry is not as widely studied a topic as algebraic geometry. Despite this, we believe that semi-algebraic geometry contains intriguing results that are also interesting for those mathematicians who are not specialized in algebraic or semi-algebraic geometry.

The theorem of Bröcker and Scheiderer is one of the most fascinating results in this field. In this work, we represented and proved the theorem of Bröcker and Scheiderer for basic open semi-algebraic sets. We left out the part of the theorem which shows that a similar bound holds for basic closed semi-algebraic sets for a fixed algebraic variety.

We aimed to be detailed in the proofs and represent sufficient prerequisites and references. On the other hand, we represented only one version of how to prove the theorem. We left out many important results from semi-algebraic geometry that did not have a role in this work. Some of these results have a connection to the main theorem although they are not immediately needed in the proof.

Although this work has been abstract, we believe that semi-algebraic geometry is widely useful in various applications where we rigorously need to manipulate sets defined by polynomial inequalities. The proofs in semi-algebraic geometry can provide starting points for the development of constructive algorithms which could be used, for example, in linear programming. One of the primary motivations for this work has been to understand the theorems and write the proofs sufficiently detailed manner so that future work in the development of constructive methods will be easier.

Bibliography

[1] Georg Gottlob, Stephanie Tien Lee, Gregory Valiant, and Paul Valiant. Size and treewidth bounds for conjunctive queries. *J. ACM*, 59(3), June 2012.

[2] Albert Atserias, Martin Grohe, and Dániel Marx. Size bounds and query plans for relational joins. *SIAM Journal on Computing*, 42(4):1737–1767, 2013.

[3] Serge Lang. *Algebra.* Graduate Texts in Mathematics. Springer New York, 2005.

[4] J.W. Gardner and R. Wiegandt. *Radical Theory of Rings.* Chapman & Hall/CRC Pure and Applied Mathematics. CRC Press, 2003.

[5] N. Bourbaki. *Commutative Algebra: Chapters 1-7.* Number v. 1 in Elements de mathematique. English. Springer, 1998.

[6] Henri Bourlès. *Fundamentals of advanced mathematics. 2. Field extensions, 2. Field extensions,.* Elsevier Ltd., 2018.

[7] Joseph Shipman. Improving the fundamental theorem of algebra. *The Mathematical Intelligencer*, 29(4):9–14, Sep 2007.

[8] H. Matsumura. *Commutative Algebra.* Math Lecture Notes Series. Benjamin/Cummings Publishing Company, 1980.

[9] David Hilbert. Mathematical problems. *Bulletin of the American Mathematical Society*, 8(10):437–480, Jul 1902.

[10] Emil Artin. Über die zerlegung definiter funktionen in quadrate. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):100–115, Dec 1927.

[11] Emil Artin and Otto Schreier. Algebraische konstruktion reeller körper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):85–99, Dec 1927.

[12] J. Bochnak, M. Coste, and M-F. Roy. *Real Algebraic Geometry.* Springer-Verlag Berlin Heidelberg, 1998.

[13] Herbert B Enderton. *Elements of set theory.* Academic Press, San Diego, 1977.

[14] Robert J. Walker. *Algebraic curves.* Springer-Verlag, 1978.

[15] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics.* Springer Berlin Heidelberg, 2006.

[16] M. Coste. *An Introduction to Semialgebraic Geometry.* Dottorato di ricerca in matematica / Università di Pisa, Dipartimento di Matematica. Istituti editoriali e poligrafici internazionali, 2002.

[17] Igor R. Shafarevich. *Basic Algebraic Geometry 1.* Springer Berlin Heidelberg, 2013.

[18] Robin Hartshorne. *Algebraic geometry.* Graduate texts in mathematics. Springer, 14 edition, 2008.

[19] Alexander Prestel and Charles N. Delzell. *Positive Polynomials: From Hilbert's 17th Problem to Real Algebra.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2001.

[20] Tsit-Yuen Lam. *Introduction to quadratic forms over fields.* American Mathematical Society, 2012.

[21] E. T. Browne. On the signature of a quadratic form. *Annals of Mathematics*, 30(1/4):517–525, 1928.

[22] Andreas Bernig and Louis Mahé. *Constructions for the theorem of Bröcker and Scheiderer.* PhD thesis, Master's thesis, Universität Dortmund, 1998.

[23] Carlos Andradas, Ludwig Bröcker, and Jesús M. Ruiz. *Constructible Sets in Real Geometry.* Springer Berlin Heidelberg, 1996.