Technische Universität Kaiserslautern

Fachbereich Mathematik

On the computation of the real radical

Diplomarbeit im Fachbereich Mathematik

eingereicht von: Silke J. Spang

eingereicht am: 2. März 2007

1. Gutachterin: Frau Dr. Anne Frühbis-Krüger
2. Gutachter: Herr Prof. Dr. Gerhard Pfister

Contents

Introduction **5**

1 Real radicals, definition and properties **11**
1.1 Motivation 11
1.2 The real radical 12
1.3 Associated primes of real radical ideals 14
1.3.1 One-to-one correspondences in real algebraic geometry 16

2 Special univariate case **19**
2.1 Sturm sequences and Sturm's theorem 20
2.2 The procedure `RealPoly` 24

3 The general univariate case **27**
3.1 How to compute an isolating set of a univariate polynomial $f \in \mathbb{Q}[x]$. 29
3.1.1 Bernstein polynomials and coefficients 29
3.1.2 A procedure to isolate real roots 37
3.2 An algorithm for the decision problem 40
3.2.1 How to find the polynomial p in $\mathbb{Q}[x_n]$ 41
3.3 The generalized procedure `RealPoly` 47

4 The zero-dimensional case **51**
4.1 General position and the theory of primary decomposition 51
4.2 The theory of zero-dimensional radical computation 53
4.3 How to decide whether a maximal ideal is real 56
4.3.1 The procedure `prepare_max` 61
4.3.2 A short overview on coordinate changes into general position . . 63
4.4 An algorithm to compute the zero-dimensional radical 67

5 An algorithm to compute the real radical of an arbitrary polynomial ideal **73**
5.1 Isolated real points 73
5.1.1 Singular points 75
5.1.2 The procedure `zeroreduct` 77
5.2 The theory of higher dimensional computation 81
5.2.1 A solution to the special radical contraction problem 82
5.2.2 The algorithm to compute the real radical of polynomial ideals I over $\mathbb{Q}(x_1, \ldots, x_n)$ 84

A General concepts and basic definitions of real algebra **89**
A.1 Ordered fields and their real closures 89
A.1.1 Orderings and pre-orderings of fields 89
A.2 Real closed fields and the real closure 93
A.2.1 Real closed fields 93
A.2.2 The Real Closure 94

B τ-real ideals and the real radical **97**
B.1 Some properties of the $\sqrt[\tau]{}$-functor 99
B.1.1 The Real Nullstellensatz 102

Introduction

In Real Algebraic Geometry the notion of real radicals is a fundamental tool.It takes the role of the radical ideal in complex Algebraic Geometry. In this work an algorithm to compute the real radical for polynomials ideals I is presented.

Similar to the radical of an ideal $J \trianglelefteq K[x_1, \ldots, x_n]$, which describes the variety of J over the algebraic closure $\overline{K}$, there exists the notion of the real radical $\sqrt[re]{J}$. It corresponds to the real points $V_{re}(J)$ (see definition B.13) of an ideal J in $\mathbb{Q}[x_1, \ldots, x_n]$ or a transcendent extension $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x_1, \ldots, x_n]$. Analogous to Hilbert's Nullstellensatz the following property holds:
Let K be a formally real field and $J \trianglelefteq K[x_1, \ldots, x_n]$ be any ideal. Then

$$I_K(V_{re}(J)) = \sqrt[re]{J}.$$

The real radical an of ideal over $J \trianglelefteq A := \mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ is defined as follows:

$$\sqrt[re]{J} := \langle f \in A : \exists r, m \in \mathbb{N} : f^{2r} + \sum_{i=1}^{m} k_i g_i^2 \in J,\ k_i \in K_{\geq 0}, g_i \in A \rangle$$

The aim of this work is to explicitly state and implement an algorithm to compute the real radical of an arbitrary polynomial ideal $J \trianglelefteq A$, where $m \geq 0$. To this end, we also need to recall some basics of Real Algebra and Real Algebraic Geometry. The original task arose from an article by Becker and Neuhaus written in 1998 (see [BN98]), where they present an idea to compute the real radical of a polynomial ideal. In Chapter 4, some gaps in the original article have been filled to speed up the computation:

The idea is to study the properties of maximal ideals M and to find a heuristic for the case when they are real, i.e. when $\sqrt[re]{M} = M$. This idea arose from the fact that the primary decomposition in Singular is well implemented and very efficient in the average case.

The abstract is structured in two major parts. The first part consists the five main chapters and the second refers to the two appendix chapters.

The appendix chapters present some basics of Real Algebra and Real Algebraic Geometry which are needed to obtain the theorems and methods for the higher dimensional

radical computations over $\mathbb{Q}(y_1, y_2, \ldots, y_m)$. In Appendix Chapter A a generalization of the properties of subfields of $\mathbb{R}$ and orderings is introduced:
As we know every subfield of $\mathbb{R}$ admits the unique ordering $\geq$ of $\mathbb{R}$ we need to study a generalization for these orderings. Here a field will be called real if we can order it. Therefore we define pre-orderings σ of a field K to be a substructure satisfying the following conditions:

1. $\sigma + \sigma \subset \sigma$ and $\sigma \cdot \sigma \subset \sigma$

2. $-1 \notin \sigma$

3. $K^2 \subset \sigma$, i.e. $a^2 \in \sigma$ for all $a \in K$

A pre-ordering τ additionally satisfying the property $\tau \cup (-\tau) = K$ is called an ordering. The field (K, σ) (resp. (K, τ)) is called a pre-ordered (ordered) field. From the convention $\alpha \geq 0$ iff $\alpha \in \sigma$ (resp. $\alpha \in \tau$) follows that every pre-ordering σ is a partial ordering of the field K which is compatible with the field axioms and we obtain that any ordering τ is a total ordering. Obviously every pre-ordering is contained in the smallest pre-ordering $re := \sum K^2$ which is the sum of all squares in K. Every pre-ordering σ is the intersection of several orderings $\tau_1, \tau_2, \ldots, \tau_r$ and thus every pre-ordered field can be ordered. In perticular every field F, in which $re := \{a_1^2 + \ldots a_r^2 : r \in \mathbb{N}, a_i \in F\}$ is a pre-ordering (i.e. $-1 \notin re$) is real. Thus **real fields** as generalization of subfields of $\mathbb{R}$, are fields which admit an ordering τ. Hence a field F is real iff -1 is no sum of squares.

The notion of **real closed fields** and a **real closure** are defined as a generalization of $\mathbb{R}$ in which the fundamental theorem of algebra holds. Here a field R is called real closed if it is real, R^2 is its unique ordering and it fulfills the fundamental theorem of algebra in one variable. As for the real numbers, the algebraic closure of a real closed field R is $R(\sqrt{-1})$. We will see that every ordered field F has a real closure R which is unique up to isomorphism.

The chapter finishes with the **Tarski-Seidenberg principle** for real closed fields: Let R and R' be two real closed fields satisfying $R \subset R'$ and let $\Phi(Y)$ be any statement over R using $>, <, =, \geq, \leq, \text{sign}$. Then $\Phi(Y)$ is true over R iff it is true over R'. This theorem is mainly used in Chapter 3. Here we obtain that a polynomial $f \in \mathbb{Q}[x_1, \ldots, x_n]$ is non-negative over $R_{alg} := \overline{\mathbb{Q}} \cap \mathbb{R}$ (which is the real closure of $\mathbb{Q}$) iff it is non-negative over $\mathbb{R}$. Indeed every assertion of being real which should be done over $\mathbb{R}_{alg}$ can be done over $\mathbb{R}$ by means of this principle.

In the second appendix chapter we see that the notion of the real radical is only a specialization of the stronger notion of σ-radicals for arbitrary pre-orderings σ of real fields K.

Let (K,τ) be a pre-ordered field, A a K-algebra and $I \trianglelefteq A$ an arbitrary ideal. Then the τ-radical of I is

$$\sqrt[\tau]{I} = \{f \in A \ : \ f^{2r} + \sum_{i=1}^{m} a_i g_i^2 \in I \text{ with } r,m \in \mathbb{N}, g_i \in A \text{ and } a_i \in \tau \ \forall i\}.$$

For any ideal $I \trianglelefteq K[x_1,\ldots,x_n]$ we the define the σ-real points of I to be the union of the real points of every real closure R_α of K where α is an ordering extending σ. Hence $V_\sigma(I) := \bigcup_{\alpha \supset \sigma} V_{R_\alpha}(I)$ where $V_{R_\alpha}(I) := \{x \in R_\alpha^n : f(x) = 0 \forall f \in I\}$.

The most important theorems in this chapter are the Real Nullstellensatz, proved by Krivine which says that $I_F(V_\sigma(I)) = \sqrt[\sigma]{I}$ and in particular $I_K(V_{re}(I)) = \sqrt[re]{I}$ and the **sign change criterion** of Dubois (B.10). With the aid of this criterion we get the Remark B.11 which is again important for Chapter 3. In this chapter some properties of the $\sqrt[\sigma]{}$-functor and σ-real prime ideals are introduced. Both appendix chapters are fundamental for understanding Chapters 3-5.

The main chapters describe the algorithm in detail. The algorithm for the higher dimensional case for an ideal $I \trianglelefteq \mathbb{Q}(y_1,y_2,\ldots,y_m)[x_1,\ldots,x_n]$ is implemented by two reductions. The first is a reduction to the zero-dimensional case via the computation of zero-dimensional ideals $J^{(S)}$. These ideals are contained in the ideal of the real isolated points of $I \cdot (\mathbb{Q}(y_1,y_2,\ldots,y_m))(S)[\{x_1,\ldots,x_n\} \setminus S]$ where $S \subset \{x_1,\ldots,x_n\}$.

The heart of the whole Diplomarbeit are Chapter 2 and 3. Here the special case of univariate polynomials is explained. Every real radical computation mainly reduces to this special case.

Chapter 1 gives a short overview and motivation to the notion of the real radicals. Some examples are given of how the $\sqrt[re]{}$ functor can behave. We will see first properties on $\mathbb{Q}$-algebras A. The real radical commutes with intersection and localization. For an arbitrary ideal $I \trianglelefteq A$, we know $\sqrt[re]{I} = \sqrt[re]{\sqrt[re]{I}}$, and $\sqrt[re]{I}$ is a radical ideal by definition. A special form of the Real Nullstellensatz over $\mathbb{Q}$ is stated. The general form was proved in the appendix chapters.
One of the fundamental statements is Proposition 1.8 which tells us that the real radical of I is the intersection of all real prime ideals P containing I. In fact, to give rise to all real points, the real radical of I is the intersection of all real maximal ideals M containing I.
The chapter finishes by sketching how the one-to-one correspondences from Algebraic Geometry over algebraically closed fields are translated to Real Algebraic geometry by means of the real radical. Thus a real maximal ideal corresponds to a zero-dimensional real zero-set which can be seen as finitely many conjugate points in the field extension of $\mathbb{Q}$ to $\mathbb{R}_{alg}$ (or $\mathbb{R}$ by the Tarski Seidenberg principle).
Prime ideals correspond to irreducible $\mathbb{Q}$-varieties in $\mathbb{R}^n$ and the primary decomposition is just the decomposition of a Q-variety $V_{re}(I) \subset \mathbb{R}^n$ in its irreducible components.

The univariate case of polynomials $f \in \mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ which corresponds to the leaves of the reduction tree, is explained in Chapters 2 and 3.

The main idea is the following: Let

$$f = \varepsilon \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

If we could decide whether a prime polynomial p_i is real or not, then the real radical of the principal ideal $\langle f \rangle \trianglelefteq \mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ is

$$\sqrt[re]{\langle f \rangle} = \langle \prod_{p_i \text{ is real}} p_i \rangle.$$

This provides an idea how to compute the real radical of a univariate polynomial. Chapter 2 does this in the special case $m = 0$. A classical solution to the problem is due Sturm using Sturm sequences. Other methods to count real roots are e.g. the Silvester-Habicht sequence. As Chapter 2 is only the special case preparing the more the general case in Chapter 3, I decided to explain only the main ideas of the Sturm sequence which is defined nearly like the remainders in the Euclidean algorithm but with a sign change. Sturm's theorem counts all distinct roots without counting their multiplicity, but as irreducible polynomials in $\mathbb{Q}[x]$ are square-free all roots are distinct. Additionally, we are only interested in the existence of these zeroes.

Among all statements in Chapter 3 there is Lemma 3.1. It says if $p \in \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ is an irreducible polynomial such that $\deg_x p > 0$, then $\overline{p} := p \cdot \mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ (which is obviously prime) is real iff p is indefinite over $\mathbb{R}$, i.e. there exist $a, b \in \mathbb{R}^{m+1}$ such that $p(a) \cdot p(b) < 0$. Hence we need to decide if the irreducible polynomial p has a sign change. The solution to this problem is obtained from an article of Zeng & Zeng (see [GX04]). The main idea of the algorithm is described in the following theorem.

Theorem (Zeng & Zeng)
Let f be a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ with $n \geq 2$. Then a non-zero univariate polynomial $p \in \mathbb{Q}[x_n]$ can be computed effectively such that for every isolating set Γ of p, $f(x_1, \ldots, x_n) \geq 0$ in $\mathbb{R}^n$ iff $f(x_1, \ldots, x_{n-1}, a) \geq 0$ for every $a \in \Gamma$.

Hence the idea of our algorithm is to compute a *new* polynomial $p \in \mathbb{Q}[x_n]$ and on of its isolating sets. Then we check if Zeng&Zeng's holds. If not we conclude that f is indefinite. An isolating set Γ of a polynomial $g \in \mathbb{Q}[x]$ is a finite subset $\{a_1, \ldots, a_m\}$ satisfying $g(a_i) \neq 0$ for every i. The intervals (a_i, a_{i+1}) contain at most one zero of g and every zero α of g is contained in an interval (a_l, a_{l+1}). This means that the roots are partitioned by the a_i. The idea to compute such an isolating set is introduced in the first subsection of Chapter 3. It uses Bernstein polynomials and Bernstein coefficients. As a reference I used the book of S.Basu, R.Pollack and M.-F.Roy (see [BPR03] Chapter 10). The advantage of Bernstein coefficient instead of Sturm sequences is that, if we shorten our interval (a, b), in which we want to know if the polynomial g has exactly

one root, it costs only additions and multiplications. The Sturm sequences always use the evaluation of points in the whole sequence. Thus using Bernstein polynomials, which give a a more efficient data structure, is a better choice for implementing fast isolating set computations. The whole idea of the algorithm to compute such an isolating set is given in the first subsection of Chapter 3. The second subsection shortly states the algorithm to decide whether a multivariate polynomial is indefinite or not. For this algorithm the definition of characteristic sets and pseudo remainders is used. Ritt-Wu's algorithm (see `char_series`) computes these sets. According to von zur Gathen ([vzGG99]) such a characteristic set is similar to a lexicographical Groebner basis. In the last subsection I describe how to extend the `RealPoly` algorithm which was introduced in Chapter 2 for the special case $m = 0$.

After describing the machinery for the univariate case, an algorithm to compute the zero-dimensional radical is explained in Chapter 4. In contrast to the article of Becker and Neuhaus, the decision was to compute the primary decomposition of the zero-dimensional input and to give a heuristic to decide whether a maximal ideal is real or not. This heuristic yields a procedure `prepare_max`. The procedure `prepare_max` prepares a maximal ideal in such a way that we can avoid a coordinate change into general position as often as possible. If a coordinate change can't be avoided we use the procedure `GeneralPos`. The input is a list of maximal ideals where this change can't be avoided. Here a suitably randomized coordinate change is computed such that we can check the properties of `prepare_max` for the transformed maximal ideals and afterwards we intersect all real maximal ideals of this list. The procedure `RealZero` gets a zero-dimensional input I and computes its primary decomposition. Then it picks every maximal ideal and tests if a change is needed to compute the real part. Afterwards it intersects the real radicals of all these 'nice' maximal ideals and restarts the procedure `GeneralPos` for the list of 'bad' ideals.

Finally, Chapter 5 describes the root of the reduction, the final algorithm for the higher dimensional computations. This part mainly follows the ideas of the article from Becker and Neuhaus.
In the first section the concept of **real isolated** points is introduced. Here a point $a \in V_{\overline{F}}(I)$ is called real isolated in the topological space $V_{re}(I)$ if it is isolated in some variety $V_R(I)$ with respect to the order topology for some real closed intermediate field R of the field extension $[\overline{F} : F]$. The set of all these isolated points (i.e. we choose every real closed field R in this extension and merge all these sets) is denoted by $V_{Iso}(I)$. We will see that the vanishing ideal $I_{Iso} := V_F(V_{Iso}(I))$ is the (finite) intersection of maximal ideals $M_1, \ldots, M_r$ such that any zero-dimensional component of $\sqrt[re]{I}$ occurs among the M_i. This fact allows the construction of the zero-dimensional components of $\sqrt[re]{I}$: Although we do not know how to compute I_{Iso} exactly we are able to give a recursive method for the construction of an ideal J such that $\dim J \leq 0$ and $I \subseteq J \subseteq I_{Iso}$, which meets our requirement in connection with the computation of real radicals. In the final section the algorithm for the higher dimensional computation is described. The central result of this subsection which describes the whole algorithm

is

$$\sqrt[re]{I} = \bigcap_{S \subsetneq \{x_1,\ldots,x_n\}} (\sqrt[re]{J^{(S)}} \cap F[x_1,\ldots,x_n]),$$

where $F = \mathbb{Q}(y_1, y_2, \ldots, y_m)$ and $I \trianglelefteq F[x_1, \ldots, x_n]$ are of arbitrary dimension. This gives the algorithm and finishes my Diplomarbeit.

Acknowledgments

First of all I want to thank my advisor Dr. Anne Frühbis-Krüger, who was always a good friend and a good advisor for me, for supporting me when I needed a helping hand or just someone to talk to, for helping me to find and acquire literature for this Diplomarbeit. I also thank Prof. Dr. Gerhard Pfister initially suggesting me the subject of this Diplomarbeit and for being a good contact person during my studies.

I thank my family, especially my mother Johanna Spang. I thank you for your love and trust. You have always been there when I needed you and that's why I love you. Last but not least I want to thank my friends for proof-reading my Diplomarbeit for finding mistakes and helping me with my LaTeX-code. Here I especially thank my best friend Johannes Kloos. I thank you for your aid and your diligence. You are a really good friend.

1 Real radicals, definition and properties

1.1 Motivation

Among the foundation of algebraic geometry there is Hilbert's Nullstellensatz. It gives rise to the correspondence between algebraic sets over algebraically closed fields L and ideals of some affine algebras of subfields of L. Therefore we have to define some machinery in algebraic geometry.

Definition 1.1
Let K be a field, $I \trianglelefteq L[x_1, \ldots, x_n]$ be an ideal. For any extension field L of K we define:

- $V_L(I) := \{\underline{a} \in L^n \ : \ f(\underline{a}) = 0 \ \forall f \in I\}$, *these sets are called K-varieties in L^n.*
- *For any $X \subset L^n$ let $I_K(X) := \{f \in K[x_1, \ldots, x_n] \ : \ f_{|X} = 0\}$ be the ideal of X.*

As usual $\overline{K}$ will denote the algebraic closure of the field K.

Now the geometric Nullstellensatz, which can be found in any textbook on algebraic geometry (e.g. see [GP02], p. 217 Theorem 3.5.2), is:

Theorem 1.2 (Hilbert's Nullstellensatz)
Let K be any field and $\overline{K}$ its algebraic closure, $I \trianglelefteq K[x_1, \ldots, x_n]$ an ideal. Then

$$I_K(V_{\overline{K}}(I)) = \sqrt{I}$$

In a beginners' course on algebraic geometry, one always deals with complex algebraic geometry, i.e. all fields which occur are subfields of the complex numbers $\mathbb{C}$. As $\mathbb{C}$ is algebraically closed, we know that for any subfield $K \subset \mathbb{C}$ its algebraic closure is a subfield of $\mathbb{C}$. If we now choose any ideal $I \trianglelefteq K[x_1, \ldots, x_n]$, we will always consider $V_{\mathbb{C}}(I)$. In this case we have a special form for Hilbert's Nullstellensatz.

Theorem 1.3 (Special form of Hilbert's Nullstellensatz)
Let $K \subset \mathbb{C}$ be any subfield of $\mathbb{C}$. For any ideal $I \trianglelefteq K[x_1, \ldots, x_n]$. Then:

$$I_K(V_{\mathbb{C}}(I)) = \sqrt{I}$$

Example 1.4

1. *Let $K = \mathbb{C}$ and $I = \langle x^2 + y^2 + 1, x^2 - 1\rangle$. Then*

   - $V_{\mathbb{C}}(I) = \{(1, \sqrt{2}i); (1, -\sqrt{2}i); (-1, \sqrt{2}i), (-1, -\sqrt{2}i)\}$
   - $I_{\mathbb{C}}(V_{\mathbb{C}}(I)) = \langle x^2 - 1, y^2 + 2\rangle$

2. *Now let $K = \mathbb{Q}$ and I be the same ideal as before. Let us now consider $V_{\mathbb{R}}(I)$: Since $x^2 + y^2 + 1 = 0$ has no real solutions, we conclude $V_{\mathbb{R}}(I) = \varnothing$ and therefore $I_{\mathbb{Q}}(V_{\mathbb{R}}(I)) = \mathbb{Q}[x, y]$.*

The following sections deal with the behavior of the I_K and $V_{\mathbb{R}}$ functors over subfields of $\mathbb{R}$. From now on, if not denoted otherwise, K is a subfield of the real numbers $\mathbb{R}$ which contains $\mathbb{Q}$.

1.2 The real radical

Definition 1.5 (Real radical)
Let A be an affine K-algebra, $I \trianglelefteq A$ any ideal. We define the real radical of I to be

$$\sqrt[re]{I} := \langle f \in A : \exists r, m \in \mathbb{N} : f^{2r} + \sum_{i=1}^{m} k_i g_i^2 \in I,\ k_i \in K_{\geq 0}, g_i \in A\rangle$$

I is called ***real*** *iff $\sqrt[re]{I} = I$.*

Example 1.6

1. *Let $K = \mathbb{Q}$ and $I = \langle x^2 + y^2 + 1, x^2 - 1\rangle$ from Example 1.4. Now $1 \in \sqrt[re]{I}$, because $1 + (x^2 + y^2) \in I$. Hence $\sqrt[re]{I} = \mathbb{Q}[x, y]$. We conclude:*

   $$I_K(V_{\mathbb{R}}(I)) = \mathbb{Q}[x, y] = \sqrt[re]{I}$$

2. *$K = \mathbb{Q},\ I = \langle xy^2 + 1, x - 1\rangle$. In this case*

   - $1 + y^2 = xy^2 + 1 - y^2(x - 1) \in I \Rightarrow 1 \in \sqrt[re]{I} \Rightarrow \sqrt[re]{I} = \mathbb{Q}[x, y]$
   - $V_{\mathbb{R}}(I) = \varnothing$, *because $x = 1$ yields $y^2 + 1 = 0$*

And again: $I_K(V_{\mathbb{R}}(I)) = \sqrt[re]{I}$

3. $K = \mathbb{Q}(\sqrt{2}),\ I = \langle x^2 - 3\rangle$. *We have:*

   - $V_{\mathbb{R}}(I) = \{\sqrt{3}, -\sqrt{3}\}$
   - $I_{\mathbb{Q}(\sqrt{2})}(V_{\mathbb{R}}(I)) = I$

   Claim: *I is real*
   Proof
   Let $f \in \sqrt[re]{I}$. Then there is an $r \in \mathbb{N}$ and a $t = \sum_{i=1}^{m} k_i g_i^2 \in I$ where $k_i \in \mathbb{Q}(\sqrt{2})_{\geq 0}, g_i \in \mathbb{Q}(\sqrt{2})[x]$ s.t. $f^{2r} + t \in I$. So $(f^{2r} + t)(\sqrt{3}) = 0 \overset{t(\sqrt{3})\geq 0}{\Longrightarrow} f^{2r}(\sqrt{3}) = 0 = f(\sqrt{3}) \overset{f\in\mathbb{Q}(\sqrt{2})[x]}{\Longrightarrow} f \in I$ ∎

   Again we observe $I_K(V_{\mathbb{R}}(I)) = \sqrt[re]{I}$.

Indeed the following special result holds. Krivine proved it in the 60s, for detailed information see appendix chapter B. (This theorem is a special form of the Real Nullstellensatz. (cf. Theorem B.14))

Theorem 1.7 (Special Real Nullstellensatz)
Let $J \trianglelefteq K[x_1, \ldots, x_n]$, then:

$$I_K(V_{\mathbb{R}}(J)) = \sqrt[re]{J}$$

In the next section, we will see that real radicals in Real Algebraic Geometry are of the same importance as radicals in Complex Algebraic Geometry.

Before going on, we state the following short lemma about the properties of real radicals:

Lemma 1.8
Let $I, J \trianglelefteq K[x_1, \ldots, x_n]$ be ideals, then:

i. $\sqrt[re]{I}$ *is a radical ideal*

ii. $\sqrt[re]{I}$ *is a real ideal*

iii. $\sqrt[re]{I \cap J} = \sqrt[re]{I} \cap \sqrt[re]{J}$

iv. *Let $S \subset K[x_1, \ldots, x_n]$ be multiplicatively closed, s.th. $1 \in S$ and $0 \notin S$, then taking the real radical commutes with localization, i.e.:*

$$\sqrt[re]{I_S} = (\sqrt[re]{I})_S$$

PROOF
The properties i.-iii. are clear from the definition of the real radical or from the Real Nullstellensatz. For Property iv. see Theorem B.4. ∎

1.3 Associated primes of real radical ideals

The primary decomposition of a real ideal I provides information on the structure of the irreducible components of the variety $V_K(I)$. So recalling further properties about the primary decomposition will help us to study our varieties in a better way.

Lemma 1.9
Let $I \trianglelefteq K[x_1, \ldots, x_n]$ be a real ideal. Then every minimal prime of I is real.

PROOF
See Lemma B.5. ∎

As a corollary to this lemma we get:

Corollary 1.10
Let $I \trianglelefteq K[x_1, \ldots, x_n]$ be any ideal. Let $\Gamma(I) := \{M \lhd \cdot K[x_1, \ldots, x_n] : M \supset I$ and real$\}$ and $\Delta(I) := \{P \trianglelefteq K[x_1, \ldots, x_n] : P$ is prime, real and contains $I\}$. Then the following equations hold:

i. $\sqrt[re]{I} = \bigcap_{P \in \Delta(I)} = \bigcap_{P \in Min(\sqrt[re]{I})} P$

ii. $\sqrt[re]{I} = \bigcap_{M \in \Gamma(I)} M$

PROOF
To i: $\sqrt[re]{I}$ is real and radical, thus all minimal prime ideals of $\sqrt[re]{I}$ are real by Lemma 1.9. Now the statement follows immediately from the fact that $I \subset P$ implies $\sqrt[re]{I} \subset \sqrt[re]{P}$ for all prime ideals $P \supset I$. So:

$$\sqrt[re]{I} \overset{\sqrt[re]{I} \text{ is radical}}{=} \bigcap_{P \in Min(\sqrt[re]{I})} P \overset{1.9}{=} \bigcap_{P \in \Delta(I)} P$$

To ii: We prove the result by contradiction. Let

$$\mathsf{R} = \{I \trianglelefteq K[x_1, \ldots, x_n] : \sqrt[re]{I} \neq \bigcap_{M \in \Gamma(I)} M\}.$$

Our claim is that $\mathsf{R} = \varnothing$.
ASSUME $\mathsf{R} \neq \varnothing$:
R is partially ordered by inclusion and $K[x_1, \ldots, x_n]$ is noetherian, so there exists a $G \in \mathsf{R}$ maximal w.r.t. inclusion. Now we have the following situation:

- $\sqrt[re]{G} \supset G$ and $\sqrt[re]{\sqrt[re]{G}} = \sqrt[re]{G}$, but as G is maximal w.r.t. inclusion G is real.

- G is neither a maximal ideal nor the whole polynomial ring, as for maximal ideals and the whole ring, the assertion trivially holds.

Let g be a polynomial which is not in G. Then the chain $G, G : g, G : g^2, \ldots$ gets stationary as $K[x_1, \ldots, x_n]$ is noetherian. So there exists an m such that $G : g^m = G : g^l$ for all $l \geq m$. Set $f = g^m$, then:

i. $G : f = G : f^2$,

ii. $G = \langle G, f \rangle \cap G : f$, by Lemma 1.4.10 on page 25 in [dJP00].

iii. G is a proper subideal of $\langle G, f \rangle$ and $G : f$.

Hence $\langle G, f \rangle$ and $G : f$ satisfy the assertion, i.e:

$$\sqrt[re]{\langle G, f \rangle} = \bigcap_{M \in \Gamma(\langle G, f \rangle)} M \tag{1.1}$$

$$\sqrt[re]{G : f} = \bigcap_{M \in \Gamma(G:f)} \bar{M} \tag{1.2}$$

Thus, we have:

$$\begin{aligned} G = \sqrt[re]{G} &= \sqrt[re]{\langle G, f \rangle} \cap \sqrt[re]{G : f} \\ &= \Big(\bigcap_{M \in \Gamma(\langle G, f \rangle)} M \Big) \cap \Big(\bigcap_{\bar{M} \in \Gamma(G:f)} \bar{M} \Big) \\ &= \bigcap_{M \in (\Gamma(\langle G, f \rangle) \cap \Gamma(G:f))} M \\ &= \bigcap_{M \in \Gamma(G)} M \end{aligned}$$

This contradicts $G \in \mathsf{R}$, implying $\mathsf{R} = \varnothing$ ∎

The following example shows that $\sqrt[re]{I} \neq \bigcap_{P \in \mathrm{Min}(I) \text{ and real}} P$.

Example 1.11
Let $I = \langle x^2 + y^2 \rangle \trianglelefteq \mathbb{Q}[x, y]$. Then the only real point of I is $(0, 0)$, hence $\sqrt[re]{I} = \langle x, y \rangle$. Now I is prime and the primary decomposition of I is $I = P$. As I is not real we conclude that $\sqrt[re]{I} \neq \bigcap_{P \in \mathrm{Min}(I) \text{ and real}} P$.

We conclude, from the second part of the previous corollary, that this does not happen if I has dimension 0, as every maximal ideal containing a zero-dimensional ideal I is already minimal. So if I is any zero-dimensional ideal, then $\sqrt[re]{I} = \bigcap_{P \in \mathrm{Min}(I) \text{ and real}} P$.

In the next two chapters we restrict ourselves to the special case of univariate polynomials. The second chapter deals with univariate polynomials f over the field $\mathbb{Q}$ and the third chapter will deal with univariate polynomials over the transcendent extension fields $\mathbb{Q}(y_1, y_2, \ldots, y_m)$. After these chapters we obtain via reduction to the univariate case an algorithm to compute the real radical of a zero-dimensional ideal I over the (transcendent) field extension $\mathbb{Q}(y_1, y_2, \ldots, y_m)$.

To conclude this chapter we use the notion of the real radical to explain how our well-known 1:1 correspondences from algebraic geometry can be translated to Real Algebraic Geometry.

1.3.1 One-to-one correspondences in real algebraic geometry

Let K be any subfield of $\mathbb{R}$, then:

$$\begin{aligned}
\text{real radical ideals in } K[x_1, \ldots, x_n] &\overset{1:1}{\longleftrightarrow} K\text{-varieties in } \mathbb{R}^n \\
\text{real prime ideals in } K[x_1, \ldots, x_n] &\overset{1:1}{\longleftrightarrow} \text{irreducible } K\text{-varieties in } \mathbb{R}^n \\
\text{real maximal ideals in } K[x_1, \ldots, x_n] &\overset{1:1}{\longleftrightarrow} \text{irreducible } K\text{-varieties of dimension 0 in } \mathbb{R}^n
\end{aligned}$$

So every correspondence over $\mathbb{C}$ occurs in a natural way by means of real radicals in real algebraic geometry. Let us consider an example:

Example 1.12
Let $K = \mathbb{Q}$ and let $I = \langle x^8 + x^6 + 4x^5 + 4x^3 + 4x^2 + 4 \rangle$. Applying the primary decomposition in Singular, we get:

```
> ring r=0,x,dp;
> ideal I=x8+x6+4x5+4x3+4x2+4;
> LIB "primdec.lib";
> primdecGTZ(I);
[1]:
   [1]:
      _[1]=x6+4x3+4
   [2]:
```

```
      _[1]=x3+2
[2]:
   [1]:
      _[1]=x2+1
   [2]:
      _[1]=x2+1
```

So the associated prime ideals are $P_1 = \langle x^3 + 2\rangle$ *and* $P_2 = \langle x^2 + 1\rangle$. $\sqrt{I} = P_1 \cap P_2$. *Now we want to determine whether the* P_i *are real.*

- P_2 *is obviously not real, since* $1 \in \sqrt[re]{P_2}$, *so* $\sqrt[re]{P_2} = \mathbb{Q}[x]$.
- $V_{\mathbb{R}}(P_1) = \{-\sqrt[3]{2}\}$ *and* $x^3 + 2 \in \mathbb{Q}[x]$ *is the minimal polynomial of* $-\sqrt[3]{2}$ *in* $\mathbb{Q}[x]$. *Hence* $I_{\mathbb{Q}}(-\sqrt[3]{2}) = \langle x^3 + 2\rangle$ *and therefore* P_1 *is real.*

We conclude $\sqrt[re]{I} = P_1 = \langle x^3 + 2\rangle$.

2 Special univariate case

To obtain an algorithm for the zero-dimensional case, we first consider the univariate case, i.e. ideals in the principal ideal domain $K[x]$. I shall recall some theorems, like unique factorization, the fundamental theorem of algebra and Sturm's theorem to count the number of all distinct real roots of a polynomial $f \in K[x]$.

Theorem 2.1 (Unique factorization (cf. [vzGG99]))
Let $f \in K[x]$ be a polynomial with $\deg f \geq 1$. *Then there exist (up to permutation and multiplication with units) unique non-associated irreducible polynomials $p_1, \ldots, p_r \in K[x]$, $m_1, \ldots m_r \in \mathbb{N}$ and a unit ε, such that*

$$f = \varepsilon p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}.$$

As a direct consequence every irreducible polynomial is prime and has no root in K. Moreover every irreducible polynomial p is the minimal polynomial of an algebraic extension of K.
Let us consider the real zero-set of a polynomial $f \in K[x]$.
As there exists no formula to solve the polynomial equation $f = 0$ using only roots and arithmetic operations if $\deg f \geq 5$, we aren't able to compute the roots without using numerical methods.

But as we will see soon, we are only interested in their existence. To solve the problem of the existence of real roots see [BPR03] Chapter 10 and [BCR98] Chapter 1.2. Here I only state some theorems without proving everything.

Definition 2.2
Let $p \in K[x]$ be an irreducible polynomial. We call p ***real*** *if p has a real root $\alpha \in \mathbb{R}$. Then p is the minimal polynomial of this root α.*

If we now compute the real radical of $\langle f \rangle \trianglelefteq K[x]$, we know that factorizing f corresponds to the primary decomposition. So if

$$f = \varepsilon p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$$

then the $\langle p_i \rangle$, for all $i = 1, \ldots, r$ are precisely the minimal primes of $\langle f \rangle$. Such a minimal prime is real iff $V_{\mathbb{R}}(p_i) \neq \varnothing$, i.e. if p has a real root. So $\langle p_i \rangle$ is real iff p_i is real.

Hence the real radical of $\langle f \rangle$ is:

$$\sqrt[re]{\langle f \rangle} = \langle \prod_{p_i \text{ real}} p_i \rangle.$$

This leads us directly to the demand of a criterion to know whether an irreducible polynomial p is real or not.
We have two cases:
If the degree of p is odd the fundamental theorem of algebra over $\mathbb{R}$ tells that p has a real root. But if the degree of p is even, we can't be sure if p has a real root. In this case we use the theorem of Sturm, which counts the number of all distinct real roots of a non–constant polynomial $f \in K[x]$ in an interval $[a, b]$, where $a < b$. As Sturm's theorem is algorithmically very inefficient, we will also use the property that every polynomial over $\mathbb{R}$ is a continuous map. Thus if $f(a) \cdot f(b) \leq 0$ we know that $0 \in f[a, b]$, so f has a real root.
To state Sturm's theorem we first define the notion of a Sturm Sequence. (cf [Coh93])

2.1 Sturm sequences and Sturm's theorem

Definition 2.3 (Sturm sequence)
Let $f \in \mathbb{R}[x]$ be any polynomial and f' its formal derivative. Then the Sturm sequence $(f_0, f_1, \ldots, f_r)$ with $f_0 = f, f_1 = f'$ is defined recursively by

$$\begin{aligned} f_0 &= q_1 f_1 - f_2 \\ f_1 &= q_2 f_2 - f_3 \\ &\vdots \\ f_{r-2} &= q_{r-1} f_{r-1} - f_r \\ f_{r-1} &= q_r f_r \end{aligned}$$

with $r \geq 1$ and $f_0, \ldots, f_r, q_i, \ldots q_r \in \mathbb{R}[x]$ and $\deg f_i < \deg f_{i-1}$, which determines r and the f_i, q_j uniquely.

Note that changing the minus on the right hand side to a plus leads to the well-known version of the Euclidean algorithm.

In particular $f_r = \gcd(f, f')$. This difference is essential for Sturm's theorem.

Notation 2.4
Let $(c_o, c_1, \ldots c_r) \in \mathbb{R}^{r+1}$ be any $(r+1)$-sequence, then:

1. $\mathrm{Var}(c_o, c_1, \ldots c_r)$ *is the number of sign changes of* $(c_o, c_1, \ldots c_r) \in \mathbb{R}^{r+1}$ *after cancelling all zeros in the sequence. We set* $\mathrm{Var}(0, 0, \ldots, 0) := -1$.

2. *For any $t \in \mathbb{R}$ we set $v_f(t) := \mathrm{Var}(f_0(t), f_1(t), \ldots, f_r(t))$, where $(f_0, f_1, \ldots, f_r)$ is the Sturm sequence of f. If there is no confusion about f we simply write $v(t)$ instead of $v_f(t)$.*

Theorem 2.5 (Sturm 1829)
Let $f \in \mathbb{R}[x]$ be a non-constant polynomial and $a, b \in \mathbb{R}$, s.t. $a < b$ and $f(a) \cdot f(b) \neq 0$. Then the number of all distinct roots in the interval (a, b) is $v(a) - v(b)$.

To get a more detailed information in which interval the real roots lie, I state the following short lemma:

Lemma 2.6
Let $f(x) = a_0 t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n \in \mathbb{R}[x]$ a polynomial of degree n. Then all real roots of f are in $[-M, M]$, where

$$M := \max\{1, \frac{|a_1| + \ldots + |a_n|}{|a_0|}\}$$

This M is is called the Cauchy bound $C(f)$ of f.

Proof
Let us first assume, without loss of generality, that $a_0 = 1$. For any root $\alpha \in \mathbb{R}^*$ of f, i.e. with $f(\alpha) = 0$ we have:

$$\alpha = -(a_1 + a_2\alpha^{-1} + .. + a_n\alpha^{1-n})$$

Thus

$$|\alpha| = |a_1 + a_2\alpha^{-1} + .. + a_n\alpha^{1-n}| \leq |a_1| + |a_2| \cdot |\alpha|^{-1} + \ldots + |a_n| \cdot |\alpha|^{1-n}.$$

Hence $|\alpha| \leq 1$ or $|\alpha| \leq |a_1| + \ldots + |a_n|$. ∎

With this interval we conclude the following corollary:

Corollary 2.7
Let f and M be defined a above, then the number of all distinct real root of f is $v(-M-1) - v(M+1)$.

Let us see some arguments to implement the algorithm only over $\mathbb{Q}$.

The Singular representation of $\mathbb{Q}(\sqrt{2})[x]$ is:

```
> ring r=(0,a),x,dp;
> minpoly=a2-2;
```

But the minimal polynomial $a^2 - 2$ has 2 roots in $\mathbb{Q}(\sqrt{2})$, namely $\sqrt{2}$ and $-\sqrt{2}$. In this simple case Singular can't be sure whether a is the positive or the negative root of 2.
As another example consider $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. The minimal polynomial of $\sqrt{2}+\sqrt{3}$ is $a^4 - 10a^2 + 1$. Its roots are $\sqrt{2}+\sqrt{3}; \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3}, -\sqrt{2}+\sqrt{3}$. If we now present this field in Singular, we have the sign problem once more.

How can we possibly decide whether an element of $\mathbb{Q}(a)$ is positive if we do not even know whether a is positive?

The statement whether for example x^2+a is real depends on which a we have chosen.

An idea to get rid of this problem could be giving a floating point approximation of which root we choose. But if we come back to the example with $\sqrt{2} = 1,414213562...$ Every approximation would yield numerical mistakes for example:

$$\text{Is } 1,4142135621 - \sqrt{2} \text{ positive or negative?}$$

This mistakes would be fatal for the computation of the real radical.

In $\mathbb{R}$ the factorization isn't implemented. Here again the reasons are numerical mistakes. Because of all these problems, I decided to implement the algorithm only over the ground field $\mathbb{Q}$.

Let us view an example for the computation with Sturm Sequences and the Sturm theorem [1]:

Example 2.8

```
> LIB "rootsur.lib";//LIB for counting roots
// ** loaded /usr/share/Singular/LIB/rootsur.lib (1.75,2005/10/28)
> ring r=0,x,dp;
> poly f=x10+9x9+x8+27x6+x2+1;
> sturmseq(f);
[1]:
   x10+9x9+x8+27x6+x2+1
[2]:
   x9+81/10x8+4/5x7+81/5x5+1/5x
[3]:
   x8+72/709x7-1080/709x6+1458/709x5-80/709x2+18/709x-100/709
[4]:
```

[1] To get rid of the problem that the coefficients grow higher and higher the command STURMSEQ divides every polynomial bye the absolute value of its leading coefficient. So all leading coefficients in our computation are 1 or -1.

```
   -x7-509085/75956x6+6237/37978x5-1418/18989x3-44091/75956x2
   -102/1117x-56709/75956
[5]:
   -x6-293058/12923783x5+607648/348942141x4+79172/38771349x3-
   29517859/348942141x2+35700/12923783x-38954237/348942141
[6]:
   -x5+162370773/3727998286x4+22101077/1863999143x3+
    216017847/3727998286x2-55440544/9319995715x+27145044/9319995715
[7]:
   x4+1645949589660/377458982597x3+11974361093723/1887294912985x2-
   35388752256/1887294912985x+16234786802188/1887294912985
[8]:
   x3+98742954999870/45465619987631x2-30711339770675/45465619987631x+
   268106006636523/90931239975262
[9]:
   -x2+9058629616172377/13791803211944376x-
   58833564722327827/62063114453749692
[10]:
   -x-1005382139360615355 8/8827044072076166007
[11]:
   1
> sturm(f,-40,40);
2
//The polynomial has 2 distinct real roots
> factorize(f,2);
[1]:
   _[1]=x10+9x9+x8+27x6+x2+1
[2]:
   1
//The polynomial is irreducible and thus real
```

In addition to Sturm's theorem the sign rules of Descartes are of some importance to solve the root counting problem. So at the end of this section, I state this important theorem.

Theorem 2.9 (Descartes (cf. [Bro96], Theorem 2.33))
Let $f = f_n x^n + f_{n-1}x^{n-1} + \ldots f_1 x + f_0 \in \mathbb{R}[x]$ and let $pos(f)$ be the number of all positive roots of f counted with multiplicity. Let

$$\mathrm{Var}(f) := \mathrm{Var}(f_n, f_{n-1}, \ldots, f_0)$$

then:

- $\mathrm{Var}(f) \geq pos(f)$

- $\mathrm{Var}(f) - pos(f)$ *is even.*

2.2 The procedure `RealPoly`

I shortly describe a procedure to test whether a univariate irreducible monic polynomial is real over $\mathbb{Q}$ or not.

Definition 2.10 (Length of a polynomial)
Let $f = x^n + f_1 x^{n-1} + \ldots + f_{n-1}x + f_n$ be any polynomial in $K[x]$, then we define the length of f to be

$$length(f) := 1 + |f_1| + \ldots + |f_n|.$$

So $length(f) \geq M + 1$, where $M = \max\{1, |f_2| + \ldots + |f_n|\}$ as defined in Lemma 2.6, i.e. every real root of f is in $[-length(f), length(f)]$.

The following Singular procedure computes the length of an arbitrary polynomial f.

```
static proc length(poly f)
"USAGE:     length(f); poly f;
RETURN:    sum of the absolute value of all coefficients of an
           irreducible polynomial f
EXAMPLE:   example length; shows no example"

{
 number erg,buffer;
 f=simplify(f,1);//wlog f is monic
 int n=size(f);
 for (int i=1;i<=n;i=i+1){
   buffer= leadcoef(f[i]);
   erg=erg + absValue(buffer);
 }

 return(erg);
}
```

We can test now whether a univariate polynomial is real or not.

From the fundamental theorem of algebra, we conclude that every polynomial f of odd degree has a real root. So the only case in which we use Sturm's Theorem is if the degree of f is even.

Now a polynomial is real if the number of real roots is not equal to zero. So in the case of an irreducible polynomial f of even degree we count the real roots. Obviously we get the following procedure:

```
static proc is_real(poly f)
"USAGE:     is_real(f); a univariate irreducible polynomial f;
RETURN:    1: if f is real
           0: is f is not real
EXAMPLE:   example is_real; shows an example"

{
  int d,anz;
  if (isuniv(f)==0) {return(0);};//f has to be univariate
  d=deg(f) mod 2;
  if (d==1)
  {
     return(1);//because of fundamental theorem of algebra
  }
  else
  {
   f=simplify(f,1);//wlog we can assume that f is monic
   number a=leadcoef(sign(leadcoef(subst(f,isuni(f),-length(f)))));
   number b=leadcoef(sign(leadcoef(subst(f,isuni(f),length(f)))));
   if
   (a*b!=1)
   //polynomials are continuous so the image is an interval
   //refers to analysis
   {
      return(1);
   }
   else
   {
      anz=sturm(f,-length(f),length(f));
      if (anz==0) {return(0);}
      else {return(1);};
   }
  };
}
example
{ "EXAMPLE:"; echo = 2;
   ring r1 = 0,x,dp;
   poly f=x2+1;
   is_real(f);
```

```
}
```

As the univariate case is essential for an algorithm in the zero-dimensional case, I state the resulting procedure to compute the real part of a polynomial $f \in \mathbb{Q}[x]$ in some arbitrary variable x.

```
proc RealPoly(poly f)
"USAGE:    RealPoly(f); poly f;
RETURN:    poly f, where f is the real part of the input f
EXAMPLE:   example RealPoly; shows an example"
{
 if (f==1) {return(f);};
 ideal j=factorize(f,1);//for getting the square-free factorization
 poly erg=1;
 for (int i=1;i<=size(j);i=i+1)
 {
  if (is_real(j[i])==1) {erg=erg*j[i];};
  //we only need real primes
 }
 return(erg);
}
example
{ "EXAMPLE:"; echo = 2;
   ring r1 = 0,x,dp;
   poly f=x5+16x2+x+1;
   RealPoly(f);
   RealPoly(f*(x4+2));
}
```

3 The general univariate case

The aim of this chapter is to extend the theory given in Chapter 2 and to give an algorithm to compute the real radical of a polynomial f in $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$, where $y_1, y_2, \ldots, y_m$ are parameters so that $\mathbb{Q}(y_1, y_2, \ldots, y_m)$ is a transcendent extension of the rational numbers.

In the first section we explain an algorithm to find an isolating set for any univariate polynomial $f \in \mathbb{R}[x]$. This can be simply understood as a finite set $\Gamma \subset \mathbb{Q}$ which separates the real roots of f. As a reference for this section see [BPR03] Chapter 10.2. In particular, the theory of Bernstein coefficients is introduced. The next section uses the algorithm to find an isolating set and states an algorithm to decide whether a multivariate polynomial is positive semi-definite or not. Here I refer to the article of Zeng& Zeng (see [GX04]). The chapter is concluded in the last subsection, where we extend the `RealPoly` algorithm of Chapter 2.

During the computation of the real part of an arbitrary multivariate polynomial the following special form of Lemma 4.1 in [BN98] is of great importance:

Lemma 3.1
Let $p \in \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$, where $m \in \mathbb{N}_0$ and $\deg_x p > 0$ be an irreducible polynomial. Then the following conditions are equivalent:

(a) $\langle p \rangle \cdot \mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ is real

(b) $\langle p \rangle \cdot \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ is real

(c) p is indefinite over $\mathbb{R}$, i.e. there are points $\underline{a}, \underline{b} \in \mathbb{R}^{m+1}$ satisfying $p(\underline{a}) \cdot p(\underline{b}) < 0$

Proof
$(a) \implies (b)$ Let $f \in \sqrt[re]{\langle p \rangle \cdot \mathbb{Q}[y_1, y_2, \ldots, y_m, x]}$ be an arbitrary polynomial. We have to show that $f \in \langle p \rangle \cdot \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$.
As $f \in \sqrt[re]{\langle p \rangle \cdot \mathbb{Q}[y_1, y_2, \ldots, y_m, x]}$ we get after localization that

$$f \in \sqrt[re]{\langle p \rangle \cdot \mathbb{Q}(y_1, y_2, \ldots, y_m)[x]} = \langle p \rangle \cdot \mathbb{Q}(y_1, y_2, \ldots, y_m)[x],$$

i.e. p divides f in $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ $(*)$.

Our aim is to show that p also divides f in $\mathbb{Q}[y_1, y_2, \ldots, y_m, x]$.
Applying pseudo-division with remainder to f and p in $(\mathbb{Q}[y_1, y_2, \ldots, y_m])[x]$ (see [vzGG99], Chapter 6.12) implies that there exists an $\alpha \in \mathbb{Q}[y_1, y_2, \ldots, y_m]$ s.t. there are unique polynomials $q, r \in (\mathbb{Q}[y_1, y_2, \ldots, y_m])[x] = \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ with:

$$\alpha \cdot f = q \cdot p + r \quad \text{and} \deg_x r < deg_x p.$$

As this equality also holds in $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ and $\alpha \in \mathbb{Q}[y_1, y_2, \ldots, y_m]$ is a unit in $\mathbb{Q}(y_1, y_2, \ldots, y_m)$, we conclude from $(*)$ that $r = 0$ in $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ and thus $r = 0$ in $\mathbb{Q}[y_1, y_2, \ldots, y_m, x]$, i.e. $p | \alpha \cdot f$ in $\mathbb{Q}[y_1, y_2, \ldots, y_m, x]$.

p is prime in $\mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ and of positive degree in x, hence p doesn't divide α, so p divides f. Thus $f \in \langle p \rangle \cdot \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ and $\langle p \rangle \cdot \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ is real.

$(b) \implies (a)$ This is clear from Lemma 1.8.

$(b) \iff (c)$ For this equivalence see Remark B.11. ∎

According to this lemma we get the following corollary.

Corollary 3.2
If there exists an algorithm to decide whether a polynomial $f \in \mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ is indefinite, it is possible to compute real radicals in the principal ideal domain $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$.

PROOF
This is simply analogous to Chapter 2, which is the special case that $m = 0$.
So let $F := \mathbb{Q}(y_1, y_2, \ldots, y_m)$ and $I \trianglelefteq F[x]$ an arbitrary ideal. Then there exists an $f \in F[x]$ s.t. $I = \langle f \rangle$. The algorithm is as follows:

1. Factorize f in $F[x]$, i.e. $f = \varepsilon \cdot p_1^{a_1} \cdots p_r^{a_r}$.

2. Decide for every p_i if it is real via the decision of indefiniteness over $\mathbb{Q}[y_1, y_2, \ldots, y_m, x]$

3. Now $\sqrt[re]{\langle f \rangle} = \langle \prod_{p_i \text{ is real}} p_i \rangle$ ∎

In the rest of this chapter, I describe a solution to decide the problem of indefiniteness of a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$. This algorithm will act via reduction of variables in each step. Therefore we will need some machinery for the univariate case, i.e. a polynomial in $\mathbb{Q}[x]$.

In the univariate case there are two problems:
We have to decide whether a univariate polynomial is indefinite and to obtain an algorithm to find an isolating set for a polynomial $f \in \mathbb{Q}[x]$.

3.1 How to compute an isolating set of a univariate polynomial $f \in \mathbb{Q}[x]$

The main ideas of this subsection can be found in the book by M.-F.Roy, R.Pollack and S.Basu (see [BPR03], Chapter 10.2).

First we define isolating sets:

Definition 3.3 (Isolating set)
Let $f \in \mathbb{Q}[x] \setminus \{0\}$ be a polynomial. Then a finite set $\Gamma := \{a_1, \ldots, a_m\} \subset \mathbb{Q}$ is called an isolating set of f if

1. *for every $a \in \Gamma$: $f(a) \neq 0$.*

2. *Assume that $a_1 \leq a_2 \leq \ldots \leq a_m$. Then f has a most one zero in every (a_i, a_{i+1}) and for every zero α of f there is an i such that $\alpha \in (a_i, a_{i+1})$.*

3. *An isolating set is called minimal if $|\Gamma|$ is minimal, i.e. if $|\Gamma| = \mathrm{num}(f) + 1$ where $\mathrm{num}(f)$ is the number of all distinct real roots of f.*

If $\deg f = 0$, then we set $\Gamma = \{0\}$

Remark 3.4
Property 3 tells that every real root α of f is isolated by exactly 2 points a_i, a_{i+1}, such that the interval (a_i, a_{i+1}) does only contain α as real root of f.

3.1.1 Bernstein polynomials and coefficients

Notation 3.5
The **Bernstein polynomials** *of degree n with respect to the basis (l, r) are*

$$Bern_{n,i}(l,r) = \binom{n}{i} \frac{(x-l)^i \cdot (r-x)^{n-i}}{(r-l)^n},$$

for $i = 0, \ldots, p$.

Remark 3.6
Note that $Bern_{n.i}(l,r) = (-1)^n Bern_{n,n-i}(r,l)$ and that

$$\begin{aligned} Bern_{n,i}(l,r) &= \frac{x-l}{r-l} \cdot \frac{n}{i} Bern_{n-1,i-1}(l,r) \\ &= \frac{r-x}{r-l} \cdot \frac{n}{n-i} Bern_{n-1,i}(l,r). \end{aligned}$$

Let us consider some machinery to prove that the Bernstein polynomials form a basis of polynomials of degree $\leq n$:

All the three transformations I shall introduce are linear automorphisms from the vector space of polynomials of degree at most d.

- **Reciprocal polynomial in degree** p:

$$Rec_n(f(x)) := x^n \cdot f(\frac{1}{x}).$$

  The non-zero roots of f are the inverses of the non-zero roots of $Rec(f)$.

- **Contraction by ratio** λ: for every non-zero λ let:

$$Co_\lambda(f(x)) = f(\lambda \cdot x).$$

  The roots of $Co_\lambda(f)$ are of the form $\frac{a}{\lambda}$ where a is a zero of f.

- **Translation by** c: for every c let

$$T_c(f(x)) = f(x - c).$$

  The roots of $T_c(f(x))$ are of the form $a + c$ where a is a root of f.

The following proposition gives an idea how to compute the Bernstein coefficients of an arbitrary polynomial of degree at most n. It also tell us that the set

$$\{Bern_{n,i}(l, r) \ : \ i = 0, \ldots, n\}$$

forms a basis of polynomials of degree at most n for every l, r.

Proposition 3.7
Let $f = \sum_{i=0}^{n} b_i Bern_{d,i}(l, r) \in \mathbb{R}[x]$ *be of degree* $\leq n$.
Let $T_{-1}(Rec_d(Co_{r-l}(T_{-l}(f)))) = \sum_{i=0}^{n} c_i x^i$. *Then* $\binom{n}{i} b_i = c_{n-i}$

Proof
As all these transformations are additive, since they are automorphisms, we prove this for an arbitrary $Bern_{n,i}(l, r) = \binom{n}{i} \cdot \frac{(x-l)^i \cdot (r-x)^{n-i}}{(r-l)^n}$. It is:

$$
\begin{aligned}
&T_{-1}(Rec_d(Co_{r-l}(T_{-l}(b_i\binom{n}{i}\cdot\frac{(x-l)^i\cdot(r-x)^{d-i}}{(r-l)^n})))) = \\
&T_{-1}(Rec_d(Co_{r-l}(b_i\binom{n}{i}\frac{x^i\cdot((r-l-x))^{n-i}}{(r-l)^n}))) = \\
&T_{-1}(Rec_d(b_i\binom{n}{i}\frac{((r-l)x)^i\cdot((r-l)\cdot(1-x))^{n-i}}{(r-l)^n})) = \\
&T_{-1}(Rec_d(b_i\binom{n}{i}x^i\cdot(1-x)^{n-i})) = \\
&T_{-1}(b_i\binom{n}{i}\frac{1}{x}^i\cdot(\frac{x-1}{x})^{n-i}\cdot x^n) = \\
&T_{-1}(b_i\binom{n}{i}(x-1)^{n-i}) = b_i\binom{n}{i}x^{n-i}
\end{aligned}
$$

■

Hence, using Proposition 3.7, it is possible to compute the Bernstein coefficients for every polynomial.

Let us consider an example of degree 3.

Example 3.8
Let $f = (x-1)\cdot(x+1)\cdot(x+2) = x^3+2x^2-x-2$, *then* $\text{length}(f) = 6$. *The Bernstein polynomials in the basis* $(-6,6)$ *are:*

- $Bern_{3,0}(-6,6) = \frac{(x+6)^0\cdot(6-x)^3}{(6-(-6))^3} = -\frac{1}{1728}x^3 + \frac{1}{96}x^2 - \frac{1}{16}x + \frac{1}{8}$
- $Bern_{3,1}(-6,6) = \frac{(x+6)^1\cdot(6-x)^2}{(6-(-6))^3} = \frac{1}{576}x^3 - \frac{1}{96}x^2 - \frac{1}{16}x + \frac{3}{8}$
- $Bern_{3,2}(-6,6) = \frac{(x+6)^2\cdot(6-x)^1}{(6-(-6))^3} = -\frac{1}{576}x^3 - \frac{1}{96}x^2 + \frac{1}{16}x + \frac{3}{8}$
- $Bern_{3,3}(-6,6) = \frac{(x+6)^3\cdot(6-x)^0}{(6-(-6))^3} = \frac{1}{1728}x^3 + \frac{1}{96}x^2 + \frac{1}{16}x + \frac{1}{8}$

Let us now compute the Bernstein coefficients of f *according to Proposition 3.7.*

Step 1: $f_1 := T_{-6}(f) = f(x-6) = x^3 - 16x^2 + 83x - 140$

Step 2: $f_2 := C_{6-(-6)}(f_1) = C_{12}(f_1) = f_1(12x) = 1728x^3 - 2304x^2 + 996x - 140$

Step 3: $f_3 := Rec_3(f_2) = -140x^3 + 996x^2 - 2304x + 1728$

Step 4: $f_4 := T_{-1}(f_3) = f_3(x+1) = -140x^3 + 576x^2 - 732x + 280$

Step 5: The Bernstein coefficients are

a) $b_0 = \frac{-140}{\binom{3}{0}} = -140$

b) $b_1 = \frac{576}{\binom{3}{1}} = 192$

c) $b_2 = \frac{-732}{\binom{3}{2}} = -244$

d) $b_3 = \frac{280}{\binom{3}{3}} = 280$

The correctness of the result can be tested easily by direct computation, e.g. using Singular.

Remark 3.9
The list $b = b_0, \ldots, b_n$ *of coefficients of* f *in the Bernstein basis of* (l, r) *gives the value of* f *at* l *(resp.* r*), which is equal to* b_0 *(resp.* b_n*). Moreover:*
The sign of f *at the right of* l *(resp.left of* r*) is given by the first (resp. last) non-zero element of the list* b*.*

As in Chapter 2, let $\mathrm{Var}(b)$ denote the number of sign variations of $b = (b_0, \ldots b_m)$. Note that, if $\mathrm{Var}(b) = 0$, where b is the list of Bernstein coefficients of a polynomial f in (l, r), the sign of f on (l, r) is the sign of any non-zero element of b, since the Bernstein polynomials for l, r are positive on (l, r). Thus f has no root in (l, r). More generally, the following holds:

Proposition 3.10
Let $f \in \mathbb{R}[x]$ *be of degree* n *and let* $b = b_0, \ldots, b_n$ *be the list of the Bernstein coefficients of* f *in* (l, r)*. Let* $\mathrm{num}(f, (l, r))$ *be the number of roots of* f *in* (l, r) *counted with multiplicities. Then*

- $\mathrm{Var}(b) \geq \mathrm{num}(f, (l, r))$
- $\mathrm{Var}(b) - \mathrm{num}(f, (l, r))$ *is even*

Proof
The claim follows immediately from Descartes' law of signs (Theorem 2.9), using Proposition 3.7. Indeed, the image of (l, r) under translation by $-l$ followed by contraction of ratio $r - l$ is $(0, 1)$. The image of $(0, 1)$ under the inversion $z \mapsto \frac{1}{z}$ is $(1, +\infty)$. Finally, translating by -1 gives $(0, +\infty)$. ∎

As a direct consequence of this proposition we get the following corollary.

Corollary 3.11
Let the notations be as above. If $\mathrm{Var}(b) = 1$ *then* f *has exactly one root in* (l, r).

The proof of the following proposition can be found in [BPR03], p. 370 Prop. 10.41.

Proposition 3.12
Let b, b' *and* b'' *be the lists of coefficients of* f *in the Bernstein basis of* $(l, r), (l, m)$ *and* (m, r). *If* $l < m < r$, *then*

$$\mathrm{Var}(b') + \mathrm{Var}(b'') \leq \mathrm{Var}(b).$$

Moreover, if m *is not a root of* f, $\mathrm{Var}(b) - \mathrm{Var}(b') - \mathrm{Var}(b'')$ *is even.*

As an improvement over Sturm's sequences, there exists a combinatorial algorithm to compute the lists b' and b'' for a given list b for the Bernstein basis of (l, r) with a given m. This makes the Bernstein coefficients easier to handle in computations.

I first state the algorithm and prove the correctness afterwards.

Algorithm 3.1 (Bernstein Coefficients)
proc *Bernsteincoef(l,r,m)*

INPUT : *a list* $b = b_0, \ldots, b_n$ *representing a polynomial* f *of degree at most* n *in the Bernstein basis of* (l, r) *and* $m \in \mathbb{Q}$

OUTPUT: *a list* b' *representing* f *in the Bernstein basis* (l, m) *and a list* b'' *representing* f *in the Bernstein basis of* (m, r)

BEGIN

Define $\alpha = \frac{r-m}{r-l}, \beta = \frac{m-l}{r-l}$

Initialize: $b_j^{(0)} = b_j, j = 0, \ldots, n$

For ($i = 1$ *to* n)

{

For ($j = 1$ *to* $n - i$)

{

$b_j^{(i)} := \alpha b_j^{(i-1)} + \beta b_{j+1}^{(i-1)};$

}

}

OUTPUT:

$b' := b_0^{(0)}, \ldots, b_0^{(j)}, \ldots, b_0^{(n)}$

$b'' := b_0^{(n)}, \ldots, b_j^{(n-j)}, \ldots, b_n^{(0)}$

END

The algorithm can be visualized with the following triangle:

$$\begin{array}{ccccccccccccc}
b_0^{(0)} & & \cdots & & \cdots & & \cdots & & \cdots & & b_n^{(0)} \\
& b_0^{(1)} & & \cdots & & \cdots & & \cdots & & b_{n-1}^{(1)} & \\
& & \ddots & & \cdots & & \cdots & & \iddots & & \\
& & & b_0^{(i)} & & \cdots & & b_{n-i}^{(i)} & & & \\
& & & & b_0^{(n-1)} & & b_1^{(n-1)} & & & & \\
& & & & & b_0^{(n)} & & & & &
\end{array}$$

with $b_j^{(i)} := \alpha b_j^{(i-1)} + \beta b_{j+1}^{(i-1)}, \alpha = \frac{r-m}{r-l}, \beta = \frac{m-l}{r-l}$.

The coefficients of f in the Bernstein basis of (l, r) appear in the top side of the triangle and the coefficients of f in the Bernstein basis (l, m) and (m, r) appear in the two other sides of the triangle. Note that $b_0^{(n)} = f(m)$
Before giving a detailed proof for the correctness we consider an example for a univariate polynomial in degree 3.

Example 3.13
Let $f = x^3 + 2x^2 - x - 2$ be the polynomial of Example 3.8. Then
$b = Bern(f, -6, 6) = (-140, 192, -244, 280)$

1. case: $m = 0$

$Bern_{3,i}(-6, 0) = \binom{3}{i} \frac{(x+6)^i \cdot (0-x)^{3-i}}{6^3}$

$Bern_{3,i}(0, 6) = \binom{3}{i} \frac{x^i \cdot (6-x)^{3-i}}{6^3}$

The computed α and β are:

- $\alpha = \frac{6-0}{6-(-6)} = \frac{1}{2}$

- $\beta = \frac{0-(-6)}{6-(-6)} = \frac{1}{2}$

The output of the algorithm visualized in the triangle is:

$$\begin{array}{ccccccc} -140 & & 192 & & -244 & & 280 \\ & 26 & & -26 & & 18 & \\ & & 0 & & -4 & & \\ & & & -2 & & & \end{array}$$

So the lists b' and b'' are:

$$b' = (-140.26, 0, -2)$$
$$b'' = (-2, -4, 18, 280)$$

2. case: $m = 3$

$Bern_{3,i}(-6, 3) = \binom{3}{i} \frac{(x+6)^i \cdot (3-x)^{3-i}}{6^3}$

$Bern_{3,i}(3, 6) = \binom{3}{i} \frac{(x-3)^i \cdot (6-x)^{3-i}}{6^3}$

The computed α and β are:

- $\alpha = \frac{6-3}{6-(-6)} = \frac{1}{4}$
- $\beta = \frac{3-(-6)}{6-(-6)} = \frac{3}{4}$

The output of the algorithm visualized in the triangle is:

$$\begin{array}{ccccccc} -140 & & 192 & & -244 & & 280 \\ & 109 & & -135 & & 149 & \\ & & -74 & & 78 & & \\ & & & 40 & & & \end{array}$$

So the lists b' and b'' are:

$$b' = (-140, 109, -74, 40)$$
$$b'' = (40, 78, 149, 280)$$

The following corollary demonstrates the correctness of Algorithm 3.1.

Corollary 3.14
The lists b' and b'' determined in Algorithm 3.1 are the correct Bernstein coefficients in the basis (l, m) resp. (m, r)

PROOF
First of all it is easy to verify by a simple induction on i that

$$b_j^{(i)} = \sum_{l=0}^{i} \binom{i}{l} \alpha^l \beta^{i-l} b_{j+l}^{(0)}. \quad (*)$$

Note that for the basis (l, m)

$$\frac{x-l}{r-l} = \beta \frac{x-l}{m-l}$$
$$\frac{r-x}{r-l} = \alpha \frac{x-l}{m-l} + \frac{m-x}{m-l}.$$

Thus

$$\left(\frac{x-l}{r-l}\right)^i = \beta^i \left(\frac{x-l}{m-l}\right)^i$$
$$\left(\frac{r-x}{r-l}\right)^{n-i} = \sum_{k=0}^{n-i} \binom{n-i}{k} \alpha^k \left(\frac{x-l}{m-l}\right)^k \left(\frac{m-x}{m-l}\right)^{n-i-k}.$$

It follows that

$$Bern_{n,j}(l,r) = \binom{n}{j} \frac{(x-l)^j (r-x)^{n-j}}{(r-l)^n}$$
$$= \binom{n}{j} \sum_{i=j}^{n} \binom{n-j}{i-j} \alpha^{i-j} \beta^j \left(\frac{x-l}{m-l}\right)^i \left(\frac{m-x}{m-l}\right)^{n-i}.$$

Since

$$\binom{n}{j}\binom{n-j}{i-j} = \binom{i}{j}\binom{n}{i}$$
$$Bern_{n,j}(l,r) = \sum_{i=j}^{n} \binom{i}{j} \alpha^{i-j} \beta^j \binom{n}{i} (\frac{x-l}{m-l})^i (\frac{m-x}{m-l})^{n-i}.$$

Finally

$$Bern_{n,j}(l,r) = \sum_{i=j}^{n} \binom{i}{j} \alpha^{i-j} \beta^i Bern_{n,i}(l,m). \quad (**)$$

Now

$$\sum_{j=0}^{n} b_j^{(0)} Bern_{n,j}(l,r)$$
$$\overset{(**)}{=} \sum_{j=0}^{n} b_j^{(0)} \left(\sum_{i=j}^{n} \binom{i}{j} \alpha^{i-j} \beta^i Bern_{n,i}(l,m) \right)$$
$$\underset{\text{indices}}{\overset{\text{modify}}{=}} \sum_{i=0}^{n} \left(\sum_{j=0}^{i} \binom{i}{j} \alpha^j \beta^{i-j} b_j^{(0)} \right) Bern_{n,i}(l,m) \overset{(*)}{=} \sum_{i=0}^{n} b_0^{(i)} Bern_{n,i}(l,m)$$

For the basis (m, r) the proof is done in an analogous way. ∎

3.1.2 A procedure to isolate real roots

To isolate real roots we use the theory of Bernstein coefficients which was introduced in the previous subsection.
The main idea of the algorithm is to shorten the intervals (a, b) with the aid of the Bernstein coefficients such that these intervals contain exactly one zero of the given polynomial f.

Algorithm 3.2 (Real root Isolation)
proc *isolset(f)*

INPUT : *a polynomial* $f \in \mathbb{Q}[x]$

OUTPUT: *a set L of intervals (a,b) s.t. f has exactly one zero in* (a, b)

BEGIN

Set $g =$ `RealPoly`(f)

Compute $M = length(g)$ *as in Chapter 2 [note that all real roots of f are in* $(-M, M)$*]*

Compute $b(g, -M, M)$*, the Bernstein coefficients in the basis* $-M, M$ *as explained in Proposition 3.7*

Initialize: $POS = \{b(g, l, r)\}$ *and L the empty list*

While $POS \neq \varnothing$

Remove an element $b(g, l, r)$ *from POS*

if $\mathrm{Var}(b(g, l, r)) = 1$*, then* $L := L \cup \{(l, r)\}$

if $\mathrm{Var}(b(g, l, r)) > 1$

Compute $b(g, l, m)$ *and* $b(g, m, r)$ *as described in Algorithm 3.1 for* $m = \frac{l+r}{2}$

If $g(m) = 0$ *then*

Compute via division by 10 an ε, starting with $\varepsilon = 0.1$ s.t. $sturm(g, m-\varepsilon, m+\varepsilon) = 1$[1]

$L := L \cup \{(m-\varepsilon, m+\varepsilon)\}$

Compute $b(g, l, m-\varepsilon)$ and $b(g, m+\varepsilon, r)$ with the aid of Algorithm 3.1

$POS := POS \cup \{b(g, l, m-\varepsilon), b(g, m+\varepsilon, r)\}$

else $POS := POS \cup \{b(g, l, m), b(g, m, r)\}$

END

As an example for the computation of this algorithm see the following:

Example 3.15
Let us again consider $f = x^3 + 2x^2 - x - 2$ from the examples 3.8 and 3.13. The first 2 steps are clear:

1. $length(f) = 1 + 2 + 1 + 2 = 6$
2. $POS = \{b(f, -6, 6)\} = \{(-140, 192, -244.280)\}$
3. *Delete* $(-140, 192, -244, 280)$ *from* POS.
4. $\mathrm{Var}(-140, 192, -244, 280) = 2 \neq 1$ *hence*

$$POS = \{b(f, -6, 0), b(f, 0, 6)\} \overset{Ex.\ 3.13}{=} \{(-140, 26, 0, -2), (-2, -4, 18, 280)\}$$
$$L = \varnothing$$

5. *Delete* $(-140, 26, 0, -2)$ *from* POS.
6. $\mathrm{Var}(-140, 26, 0, -2) = 2$ *hence*

$$POS := POS \cup \{b(f, -6, -3), b(f, -3.0)\}$$
$$\overset{Ex.\ 3.13}{=} \{(-140, -57, -22, -8), (-8, 6, -1, -2), (-2, -4, 18, 280)\}$$
$$L = \varnothing$$

[1] In all my tests this path of the algorithm wasn't touched, as almost all polynomials have integral or irrational zeros. This was the reason why I didn't start with 2^n such that $2^n > length(f)$, as in [BPR03], in the computations.

7. *Delete* $(-140, -57, -22, -8)$ *from* POS.

8. $\mathrm{Var}(-140, -57, -22, -8) = 0 < 2$

9. *Delete* $(-8, 6, -1, -2)$ *from* POS.

10. $\mathrm{Var}(-8, 6, -1, -2) = 3 > 1$ *hence*

$$\begin{aligned} POS :&= POS \cup \{b(f, -3, -\frac{3}{2}), b(f, -\frac{3}{2}.0)\} \\ &= \{(-8, 1, \frac{7}{4}, \frac{9}{8}), (\frac{9}{8}, \frac{1}{2}, -\frac{3}{2}, -2), (-2, -4, 18, 280)\} \\ L &= \varnothing \end{aligned}$$

11. *Delete* $(-8, 1, \frac{7}{4}, \frac{9}{8})$ *from* POS.

12. $\mathrm{Var}(-8, 1, \frac{7}{4}, \frac{9}{8}) = 1$ *hence*

$$\begin{aligned} POS &:= POS \cup \{b(f, -3, -\frac{3}{2}), b(f, -\frac{3}{2}.0)\} = \{(\frac{9}{8}, \frac{1}{2}, -\frac{3}{2}, -2), (-2, -4, 18, 280)\} \\ L &:= L \cup \{(-3, -\frac{3}{2})\} = \{(-3, -\frac{3}{2})\} \end{aligned}$$

13. *Delete* $(\frac{9}{8}, \frac{1}{2}, -\frac{3}{2}, -2)$ *from* POS.

14. $\mathrm{Var}(\frac{9}{8}, \frac{1}{2}, -\frac{3}{2}, -2) = 1$ *hence*

$$\begin{aligned} POS &:= \{(-2, -4, 18, 280)\} \\ L &:= L \cup \{(-\frac{3}{2}, 0)\} = \{(-3, -\frac{3}{2}), (-\frac{3}{2}, 0)\} \end{aligned}$$

15. *Delete* $(-2, -4, 18, 280)$ *from* POS.

16. $\mathrm{Var}(-2, -4, 18, 280) = 1$ *hence*

$$\begin{aligned} POS &= \varnothing \\ L &:= L \cup \{(0, 6)\} = \{(-3, -\frac{3}{2}), (-\frac{3}{2}, 0), (0, 6)\} \end{aligned}$$

Proposition 3.16
Algorithm 3.2 terminates and the list L is the correct output

Proof
The termination of the algorithm follows from Proposition 3.12, as $\mathrm{Var}(b(g, -M, M))$ is a finite natural number. Since g and f have the same real roots, the correctness follows from Proposition 3.12 and Corollary 3.11. ∎

Now it is not complicated to get an isolating set for f from the given list L.

Corollary 3.17
To get an isolating set for the polynomial f we compute the list L from Algorithm 3.2 sort it by magnitude and delete all duplicates.

Proof
Clear, since every interval in L contains exactly one root of f. ∎

3.2 An algorithm for the decision problem

In this section I give an algorithm to solve the decision problem of positive semi-definiteness. The whole algorithm is explained in detail in the article of Zeng & Zeng (see [GX04]). The most important theorem for the algorithm is:

Theorem 3.18
Let f be a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ with $n \geq 2$. Then a non-zero univariate polynomial $p \in \mathbb{Q}[x_n]$ can be computed effectively such that for every isolating set Γ of p, $f(x_1, \ldots, x_n) \geq 0$ in $\mathbb{R}^n$ iff $f(x_1, \ldots, x_{n-1}, a) \geq 0$ for every $a \in \Gamma$.

According this theorem, the algorithm to decide whether a polynomial is positive semi-definite, i.e. not negative on $\mathbb{R}^n$, is a recursion in the number of variables n. This recursion is simply done via the computation of a **new** polynomial $p \in \mathbb{Q}[x_n]$ and one of its isolating sets Γ.
Thus let me first of all state the conditions for a univariate polynomial to be positive semi-definite.

Proposition 3.19
Let $f \in \mathbb{R}[x]$ be a polynomial and g the polynomial obtained by deleting even factors in the decomposition of f into irreducible factors. Then the following results are equivalent:

1. *f is indefinite on $\mathbb{R}$*
2. *f has a root of odd multiplicity in $\mathbb{R}$*
3. *g has a root α in $\mathbb{R}$*

i.e. if the leading coefficient of f is positive and g has no real root, then f is positive semi-definite.

PROOF

$1 \implies 3$: Set $h = \frac{f}{g}$. Then h is the square of a polynomial $\overline{h}$, hence h is positive semi-definite. As f is indefinite there exists $a, b \in \mathbb{R}$ such that $f(a) \cdot f(b) < 0$. Let wlog $a < b$. Now $h(a)$ and $h(b)$ are both non-negative. Thus we get that $g(a) \cdot g(b) < 0$, as g is continuous, g has a zero in $(a, b) \subset \mathbb{R}$.

$3 \implies 2$: As every root of g has an odd multiplicity, the root α of g has odd multiplicity, too. Now it does not matter whether α is a zero of h, as this zero would only count in an even multiplicity as $h = \overline{h}^2$. Hence α is a zero of f with odd multiplicity.

$2 \implies 1$: Is clear as f is continuous and α is a root of odd multiplicity. Hence there exists an interval $[a, b]$ in which f has a sign change, i.e. f is indefinite. ∎

3.2.1 How to find the polynomial p in $\mathbb{Q}[x_n]$

This subsection only describes the main definitions and some shorter proofs on how to find the polynomial p from Theorem 3.18. From now on let the ordering of $\mathbb{Q}[x_1, \ldots, x_n]$ be a lexicographical ordering, such that $x_1 < x_2 < \ldots < x_n$.

Definition 3.20 (leading variable and the pseudo-coefficient)
Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$. The leading variable of f (short $lvar(f)$) is the largest variable in f, i.e. if

$$f = a_s(x_1, \ldots, x_{k-1})x_k^s + a_{s-1}(x_1, \ldots, x_{k-1})x_k^{s-1} + \ldots + a_0(x_1, \ldots, x_{k-1}),$$

$a_s \in \mathbb{Q}[x_1, \ldots, x_{k-1}] \setminus \{0\}$, for a $k \leq n$, then $lvar(f) = x_k$ and the pseudo leading coefficient of f is $ini(f) = a_s(x_1, \ldots, x_{k-1})$.

Definition 3.21 (Pseudo-remainder)
Let $f, g \in \mathbb{Q}[x_1, \ldots, x_n]$ such that $lvar(g) \leq lvar(f) = x_k$. The unique remainder $prem(g, f)$ obtained by pseudo-division of f by g in $(\mathbb{Q}[x_1, \ldots, x_{k-1}])[x_k]$ is called the pseudo remainder of f and g. A polynomial g is called reduced w.r.t. f if $prem(g, f) = g$.

Remark 3.22
Note that $\deg_{lvar(f)}(prem(g, f)) < \deg_{lvar(f)}(f)$.

Definition 3.23 (Triangular sets)
a) A set $T = \{f_1, ..., f_r\} \subset \mathbb{Q}[x_1, \ldots, x_n]$ is called triangular if $lvar(f_1) < ... < lvar(f_r)$. Moreover, let $U \subset T$. Then (T, U) is called a triangular system if T is a triangular set such that $ini(T)$ does not vanish on $V(T) \setminus V(U) (=: V(T \setminus U))$.

b) T is called irreducible if for every i there are no d_i,f_i',f_i'' such that

$$lvar(d_i) < lvar(f_i) = lvar(f_i') = lvar(f_i''),$$

$$0 \notin prem(\{d_i, ini(f_i'), ini(f_i'')\}, \{f_1, ..., f_{i-1}\}),$$

$$prem(d_i f_i - f_i' f_i'', \{f_1, ..., f_{i-1}\}) = 0.$$

Furthermore, (T, U) is called irreducible if T is irreducible.

The main result is the following theorem:

Theorem 3.24
Let $G = \{g_1, ..., g_s\} \subset \mathbb{Q}[x_1, \ldots, x_n]$, then there are irreducible triangular sets $T_1, ..., T_l$ such that $V(G) = \bigcup_{i=1}^{l}(V(T_i \setminus I_i))$ where $I_i = \{ini(f) \mid f \in T_i\}$. Such a set $\{T_1, ..., T_l\}$ is called an irreducible characteristic series of the ideal $\langle G \rangle$.

The characteristic series of an ideal I can be computed in Singular by the command `char_series`.

Example 3.25
1.
```
ring R= 0,(x,y,z,u),dp;
    ideal i=-3zu+y2-2x+2,
            -3x2u-4yz-6xz+2y2+3xy,
            -3z2u-xu+y2z+y;
    print(char_series(i));
==> _[1,1],3x2z-y2+2yz,3x2u-3xy-2y2+2yu,
==> x,     -y+2z,      -2y2+3yu-4
```

The method to compute the characteristic sets of an ideal I is called Wu's Method or the Wu-Ritt algorithm in many books or articles on Computer Algebra.
To finish, I only state the algorithm for the decision problem and give examples for binary polynomials. For the detailed proofs see [GX04].

Algorithm 3.3 (Decision for semi-definiteness)
proc *decision(f)*
INPUT : $f \in \mathbb{Q}[x_1, \ldots, x_n]$ *a multivariate polynomial with positive leading coefficient*
OUTPUT: *1, if f is positive semi-definite else 0*
BEGIN
If (n=1) decide by Proposition 3.19 whether f is positive semi-definite.
Return 1 if it is and 0 else.
IF (n>1)

Compute the characteristic sets $C_1, \ldots, C_r$ *of*
$I = \langle f + t, \frac{\partial f}{\partial x_i} : i = 1, \ldots, n-1 \rangle$
in $\mathbb{Q}[t, x_1, \ldots, x_n]$ *w.r.t. the lexicographical ordering* $t < x_n < \{x_1, \ldots, x_{n-1}\}$ *with the aid of* `char_series`.
The first polynomial f_i *in every* C_i *is in* $\mathbb{Q}[t, x_n]$. *Set* $\Phi = \prod_{i=1}^{r} f_i$.
$e(x_n) :=$ `RealPoly`$(\Phi(0, x_n))$, *i.e.* e *is the real part of the trailing coefficient of* Φ *in* $(\mathbb{Q}[x_n])[t]$
For every tuple $(j_1, \ldots, j_k)$ *of integers with* $1 \leq j_1 < \ldots < j_k \leq n-1$ *compute the characteristic sets* $D_1, \ldots, D_{m(j_1,\ldots,j_k)}$ *for*
$I(j_1, \ldots, j_k) := \langle f + t, \frac{\partial f}{\partial x_i} : i \in \{1, \ldots, n-1\} \setminus \{j_1, \ldots, j_k\} \rangle$.
The first polynomial f_i *in every* D_i *is in* $\mathbb{Q}[t, x_{j_1}, \ldots, x_{j_k}, x_n]$. *Set*
$\Phi_{j_1,\ldots,j_k} = \prod_{i=1}^{m(j_1,\ldots,j_k)} f_i$.
Let $u_{j_1,\ldots,j_k}(t, x_n)$ *be the leading coefficient of* $\Phi_{j_1,\ldots,j_k}$ *in* $\mathbb{Q}(t, x_n)[x_{j_1}, \ldots, x_{j_k}]$ *w.r.t. the elimination ordering* $x_{j_1} < \ldots < x_{j_k}$.
Set $e_{j_1,\ldots,j_k} :=$ `RealPoly`$(u_{j_1,\ldots,j_k}(0, x_n))$.
Set $p := e \cdot \prod_{\lambda \subset \{1,2,\ldots,n-1\}} e_\lambda$
Determine an isolating set Γ *of* p *by the aid of Algorithm 3.2*
Test for every $a \in \Gamma$ *if* $f_a := f(x_1, \ldots, x_{n-1}, a)$ *is positive semi-definite by recursion.*
If every such f_a *is positive semi-definite use Theorem 3.18 and return 1 else return 0.*
END

Now let us consider some examples.

Example 3.26
Let $f = 2x^6 + 3x^4y^2 + y^6 + x^2y^2 - 6y + 5$.

Step 1: a) $I := \langle t + 2x^6 + 3x^4y^2 + y^6 + x^2y^2 - 6y + 5, 12y^2x^3 + 12x^5 + 2y^2x \rangle$
Singular computes the following characteristic sets
$C_1 = \{216y^{12} - 108y^{10} - 9y^8 + 324ty^6 - 1944y^7 + 1628y^6 - 108ty^4 + 648y^5 - 540y^4 + 108t^2 - 1296ty + 3888y^2 + 1080t - 6480y + 2700, -6y^6 + 6y^4x^2 + y^4 - 4y^2x^2 - 6t + 36y - 30\}$,
$C_2 = \{81t^2 + 846t + 265, 486ty + 4383t - 23760y + 20945, 3x^2 + 1\}$,
$C_3 = \{y^6 + t - 6y + 5, x\}$

b) $\Phi :=$
$17496t^2y^{18} + 182736ty^{18} - 8748t^2y^{16} + 57240y^{18} - 91368ty^{16} - 729t^2y^{14}$
$- 28620y^{16} + 43740t^3y^{12} - 262440t^2y^{13} - 7614ty^{14} + 676188t^2y^{12}$
$- 2741040ty^{13} - 2385y^{14} - 17496t^3y^{10} + 104976t^2y^{11} + 2434068ty^{12}$
$- 858600y^{13} - 270216t^2y^{10} + 1096416ty^{11} + 717620y^{12} - 729t^3y^8$
$+ 4374t^2y^9 - 970920ty^{10} + 343440y^{11} + 34992t^4y^6 - 419904t^3y^7$
$+ 1248453t^2y^8 + 45684ty^9 - 286200y^{10} + 716040t^3y^6 - 6489072t^2y^7$
$+ 13116537ty^8 + 14310y^9 - 8748t^4y^4 + 104976t^3y^5 + 4339080t^2y^6$
$- 23342688ty^7 + 4109355y^8 - 178848t^3y^4 + 1621296t^2y^5 + 7028312ty^6$

$$
\begin{aligned}
&- 6881520y^7 - 1161000t^2y^4 + 5825520ty^5 + 1842280y^6 + 8748t^5 \\
&- 157464t^4y + 944784t^3y^2 - 1889568t^2y^3 - 2570400ty^4 + 1717200y^5 \\
&+ 222588t^4 - 3219264t^3y + 14591664t^2y^2 - 19735488ty^3 - 715500y^4 \\
&+ 2055240t^3 - 20898000t^2y + 52429680ty^2 - 6181920y^3 + 8375400t^2 \\
&- 46267200ty + 15454800y^2 + 13567500t - 12879000y + 3577500
\end{aligned}
$$

c) $e :=$`RealPoly`$(57240y^{18} - 28620y^{16} - 2385y^{14} - 858600y^{13} + 717620y^{12}$
$+ 343440y^{11} - 286200y^{10} + 14310y^9 + 4109355y^8 - 6881520y^7$
$+ 1842280y^6 + 1717200y^5 - 715500y^4 - 6181920y^3 + 15454800y^2$
$- 12879000y + 3577500)$
$=216y^{13} - 216y^{12} - 108y^{11} + 108y^{10} - 9y^9 - 1935y^8 + 3572y^7 - 980y^6$
$- 1188y^5 + 540y^4 + 3888y^3 - 10368y^2 + 9180y - 2700$

Step 2: As $x = x_1, y = x_2$ *the only tuple* $(j_1, \ldots, j_k)$ *is* (1) *so we have to compute the characteristic sets of* $Jac = \langle t + 2x^6 + 3x^4y^2 + y^6 + x^2y^2 - 6y + 5\rangle$ *w.r.t. the ordering* $t < y < x$.

a) Singular computes the characteristic sets:
$D_1 = \{t + 2x^6 + 3x^4y^2 + y^6 + x^2y^2 - 6y + 5\}$

b) $\Phi_1 = t + 2x^6 + 3x^4y^2 + y^6 + x^2y^2 - 6y + 5$

c) $u_1 = 2$ *is the leading coefficient of* $y^6 + 3y^2x^4 + 2x^6 + y^2x^2 + t - 6y + 5$ *in* $\mathbb{Q}(t, y)[x]$

d) $e_{(1)} = 1$

Step 3: $p := e \cdot e_1 = 216y^{13} - 216y^{12} - 108y^{11} + 108y^{10} - 9y^9 - 1935y^8 + 3572y^7 - 980y^6 - 1188y^5 + 540y^4 + 3888y^3 - 10368y^2 + 9180y - 2700$

Step 4: The isolating set computed by the algorithm isolset, which I implemented in Singular, is:

$$\Gamma = \left\{\frac{547}{864}, \frac{547}{576}, \frac{7111}{6912}, \frac{3829}{3456}\right\}$$

Step 5:

- $f_1 := f(x, \frac{547}{864}) = 2x^6 + \frac{299209}{248832}x^4 + \frac{299209}{746496}x^2 + \frac{526552254943631641}{415989582513831936}$
  f_1 *is prime and has no real root. Hence it is positive semi-definite.*

- $f_2 := f(x, \frac{547}{576}) = 2x^6 + \frac{299209}{110592}x^4 + \frac{299209}{331776}x^2 + \frac{1298833469905177}{36520347436056576}$
  f_2 *is prime and has no real root. Hence it is positive semi-definite.*

- $f_3 := f(x, \frac{7111}{6912}) = 2x^6 + \frac{50566321}{15925248}x^4 + \frac{50566321}{47775744}x^2 + \frac{1409036562626545309969}{109049173118505959030784}$
  f_3 is prime and has no real root. Hence it is positive semi-definite.

- $f_4 := f(x, \frac{3829}{3456}) = 2x^6 + \frac{14661241}{3981312}x^4 + \frac{14661241}{11943936}x^2 + \frac{344180307451240679977}{1703893329976655609856}$
  f_4 is prime and has no real root. Hence it is positive semi-definite.

Now we change f to $2x^6 - 3x^4y^2 + y^6 + x^2y^2 - 6y + 5$, i.e. replace $+3x^4y^2$ by $-3x^4y^2$. Our next example will show that this polynomial is indefinite.

Example 3.27

Step 1. a) $I := \langle t + y^6 - 3y^2x^4 + y^2x^2 - 6y + 2x^6 + 5, -12y^2x^3 + 2y^2x + 12x^5\rangle$
Singular computes the following characteristic series:
$C_1 = \{108t^2 + 108ty^6 + 108ty^4 - 1296ty + 1080t + 108y^{10} - 9y^8 - 648y^7 + 548y^6 - 648y^5 + 540y^4 + 3888y^2 - 6480y + 2700, -6t - 6y^6 + 6y^4x^2 - y^4 - 4y^2x^2 + 36y - 30, 0\}$,
$C_2 = \{729t^2 + 7830t + 3529, 21870ty + 118773t - 595188y + 550375, 3x^2 - 1\}$,
$C_3 = \{t + y^6 - 6y + 5, x, 0\}$

b) $\Phi :=$
$78732t^5 + 157464t^4y^6 + 78732t^4y^4 - 1417176t^4y + 2026620t^4$
$+ 78732t^3y^{12} + 157464t^3y^{10} - 6561t^3y^8 - 1889568t^3y^7 + 3271752t^3y^6$
$- 944784t^3y^5 + 1632960t^3y^4 + 8503056t^3y^2 - 29393280t^3y + 18970632t^3$
$+ 78732t^2y^{16} - 6561t^2y^{14} - 472392t^2y^{13} + 1245132t^2y^{12} - 944784t^2y^{11}$
$+ 2478600t^2y^{10} + 39366t^2y^9 + 5565429t^2y^8 - 29778192t^2y^7$
$+ 24537816t^2y^6 - 14871600t^2y^5 + 10805832t^2y^4 - 17006112t^2y^3$
$+ 133844400t^2y^2 - 194504976t^2y + 78981480t^2 + 845640ty^{16} - 70470ty^{14}$
$- 5073840ty^{13} + 4671972ty^{12} - 10147680ty^{11} + 9218664ty^{10} + 422820ty^9$
$+ 60501969ty^8 - 110999808ty^7 + 80689112ty^6 - 55311984ty^5$
$+ 24952320ty^4 - 182658240ty^3 + 497807856ty^2 - 449141760ty$
$+ 134289900t + 381132y^{16} - 31761y^{14} - 2286792y^{13} + 1933892y^{12}$
$- 4573584y^{11} + 3811320y^{10} + 190566y^9 + 27282699y^8 - 45905232y^7$
$+ 32918512y^6 - 22867920y^5 + 9528300y^4 - 82324512y^3 + 205811280y^2$
$- 171509400y + 47641500$

c) $e :=$`RealPoly`$(381132y^{16} - 31761y^{14} - 2286792y^{13} + 1933892y^{12} - 4573584y^{11}$
$+ 3811320y^{10} + 190566y^9 + 27282699y^8 - 45905232y^7 + 32918512y^6$
$- 22867920y^5 + 9528300y^4 - 82324512y^3 + 205811280y^2$
$- 171509400y + 47641500)$
$= 108y^{11} - 108y^{10} - 9y^9 - 639y^8 + 1196y^7 - 1196y^6 + 1188y^5 - 540y^4$
$+ 3888y^3 - 10368y^2 + 9180y - 2700$

Step 2. *As* $x = x_1, y = x_2$ *the only tuple* $(j_1, \ldots, j_k)$ *is* (1) *so we have to compute the characteristic sets of* $Jac = \langle t + 2x^6 - 3x^4y^2 + y^6 + x^2y^2 - 6y + 5\rangle$ *w.r.t. the ordering* $t < y < x$.

a) *Singular computes the following characteristic sets:*
$D_1 = \{t + y^6 - 3y2x4 + y^2x^2 - 6y + 2x^6 + 5\}$

b) $\Phi_1 = t + y^6 - 3y^2x^4 + y^2x^2 - 6y + 2x^6 + 5$

c) $u_1 = 2$ *is the leading coefficient of* $y^6 - 3y^2x^4 + 2x^6 + y^2x^2 + t - 6y + 5$ *in* $\mathbb{Q}(t, y)[x]$

d) $e_{(1)} = 1$

Step 3. $p := e \cdot e_1 = 108y^{11} - 108y^{10} - 9y^9 - 639y^8 + 1196y^7 - 1196y^6 + 1188y^5 - 540y^4 + 3888y^3 - 10368y^2 + 9180y - 2700$

Step 4. *The isolating set of* p *computed by* `isolset` *is:*

$$\Gamma = \left\{\frac{1945}{2304}, \frac{13615}{13824}, \frac{1945}{1728}, \frac{1945}{864}\right\}$$

Step 5.

- $f_1 := f(x, \frac{1945}{2304}) = 2x^6 - \frac{3783025}{1769472}x^4 + \frac{3783025}{5308416}x^2 + \frac{44401163709486387025}{149587343098087735296}$
  f_1 *is prime and has no real root, thus* f_1 *is positive semi-definite.*

- $f_2 = f(x, \frac{13615}{13824}) = 2x^6 - \frac{185368225}{63700992}x^4 + \frac{185368225}{191102976}x^2 + \frac{23451757301096416126945}{69791470795843813779701 76}$
  f_2 *is prime but it has 4 real roots of odd multiplicity and hence it is indefinite. The command* `solve` *computes all roots of the polynomial* $f_2 \in \mathbb{Q}[x]$ *in* $\mathbb{C}$

```
>poly f=2x6-185368225/63700992x4+185368225/191102976x2
+23451757301096416126945/69791470795843813779701 76;
> LIB "solve.lib";
> solve(f);
[1]:
   -0.96619394
[2]:
   -0.72448954
[3]:
   0.72448954
[4]:
   0.96619394
[5]:
```

```
   (-i*0.058556498)
[6]:
   (i*0.058556498)
```

As we found an indefinite polynomial we could stop our example and conclude that the polynomial is indefinite.

3.3 The generalized procedure RealPoly

Let me first recall the algorithm for the real polynomial of a univariate polynomial which I introduced in Chapter 2.

```
proc RealPoly(poly f)
"USAGE:    RealPoly(f); poly f;
RETURN:    poly f, where f is the real part of the input f
EXAMPLE:   example RealPoly; shows an example"
{
 if (f==1) {return(f);};
 ideal j=factorize(f,1);//for getting the square-free factorization
 poly erg=1;
 for (int i=1;i<=size(j);i=i+1)
 {
  if (is_real(j[i])==1) {erg=erg*j[i];};
  //we only need real primes
 }
 return(erg);
}
```

This algorithm can simply be extended to polynomials over $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x]$ with the aid of Lemma 3.1 and the resulting Corollary 3.2. The only procedure we have to extend is the auxiliary procedure `is_real`. It decides for a prime polynomial whether it is real or not.

The algorithm for the decision problem that I mentioned in the last subsection decides when a polynomial is positive semi-definite or not. The prime polynomials which we get in the factorization of a polynomial always have a positive leading coefficient. Hence they aren't negative semi-definite. So if these polynomials are not positive semi-definite, then they are indefinite and thus real. For a prime polynomial p `is_real(p)`

is 1 iff `decision(p)` is 0. So $1 -$ `decision` is the result for the answer of the question, if a prime polynomial is real.

To get faster computations we only use the decision algorithm if there exists no ring variable in $\mathbb{Q}[y_1, y_2, \ldots, y_m, x]$ such that the degree of p in this variable is odd. This is just a simple consequence of the fundamental theorem of algebra. Let's fix it as a lemma:

Lemma 3.28
Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be a polynomial. If there exists a variable x_i such that the degree of f in x_i ($\deg_{x_i} f$) is odd then f is indefinite over $\mathbb{R}$.

Proof
Without loss of generality, let $\deg_{x_n} f = k$ and k odd. Written in $\mathbb{Q}(x_1, \ldots, x_{n-1})[x_n]$ f has the form

$$f = f_k(x_1, \ldots, x_{n-1})x_n^k + \ldots + f_1(x_1, \ldots, x_{n-1})x_n + f_0(x_1, \ldots, x_{n-1})$$

for a non-zero polynomial $f_k \in \mathbb{Q}[x_1, \ldots, x_{n-1}]$. Let $(a_1, \ldots, a_{n-1}) \in \mathbb{R}^{n-1}$ be a point s.t. $f_k(a_1, \ldots, a_{n-1}) \neq 0$.

Now $f(a_1, \ldots, a_{n-1}, x_n)$ is a univariate polynomial of odd degree in $\mathbb{R}[x_n]$. But these polynomials are indefinite as they have a zero by the fundamental theorem of algebra.■

This leads us directly to the extension of the `is_real` procedure for the case that f is not univariate. This short extension is:

```
if (isuniv(f)==0)
  {
   for (i=1;i<=nvars(r);i++)
   {
     d=size(coeffs(f,var(i)))+1;
     if ((d mod 2)==1)
     {
       return(1);
     }
   }
   d=1-decision(f);
   return(d);
  }
```

To finish this chapter we consider some examples.

Example 3.29

1. $f = 2x^6 + 3x^4y^2 + y^6 + x^2y^2 - 6y + 5$ *from Example 3.26 is prime and positive semi-definite, thus the* `RealPoly` *of* f *is 1.*

2. $f = 2x^6 - 3x^4y^2 + y^6 + x^2y^2 - 6y + 5$ *from Example 3.27 is prime and indefinite, thus the* `RealPoly` *of* f *is* f *itself.*

3. *Let*

$$\begin{aligned} f =& x^8y^2z^4 - 2x^7y^3z^2 + x6y^4z^4 + x^6y^4 + x^6y^2z^4 + 2x^6yz^5 - 2x^5y^5z^2 - \\ & 2x^5y^3z^2 - 4x^5y^2z^3 + x^4y^6 + x^4y^4 + 2x^4y^3z^5 + 2x^4y^3z + 2x^4yz^5 + x4z^6 - \\ & 4x^3y^4z^3 - 4x^3y^2z^3 - 2x^3yz^4 + 2x^2y^5z + 2x^2y^3z + x^2y^2z^6 + x^2y^2z^2 + \\ & x^2z^6 - 2xy^3z^4 - 2xyz^4 + y^4z^2 + y^2z^2 \in \mathbb{Q}[x, y, z]. \end{aligned}$$

   Factorizing yields that

$$f = (x^2y + z)^2 \cdot (xz^2 - y)^2 \cdot (x^2 + y^2 + 1) = p_1^2 \cdot p_2^2 \cdot p_3.$$

   From lemma 3.28 we know that p_1 *and* p_2 *are real. As* x^2+y^2+1 *is positive semi-definite the real polynomial computed from* f *is* $g = p_1 \cdot p_2 = x^3yz^2 - x^2y^2 + xz^3 - yz$

4 The zero-dimensional case

The aim of this Chapter is to introduce an algorithm to compute the real radical of a zero-dimensional ideal I in the $\mathbb{Q}$-algebra $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x_1, \ldots, x_n]$. Thus I preparatorilly recall the concept of an ideal being in general position.
Applying this notion, there is a natural reduction from the zero-dimensional case to the univariate case.
This section will only be short without proofs. I only cite the definition and a useful theorem. For more information see the book by Greuel and Pfister ([GP02] Chapter 4.2 on primary decomposition).

4.1 General position and the theory of primary decomposition

Definition 4.1

(a) A maximal ideal $M \lhd \cdot K[x_1, \ldots, x_n]$ is called in general position w.r.t. the lexicographical ordering with $x_1 > x_2 > \ldots > x_n$ if there exist polynomials $g_1, g_2, \ldots, g_n \in K[x_n]$ with

$$M = \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n) \rangle.$$

(b) A zero-dimensional ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ is called in general position w.r.t. the lexicographical ordering with $x_1 > x_2 > \ldots > x_n$, if all associated primes $P_1, \ldots P_k$ are in general position and if

$$P_i \cap K[x_n] \neq P_j \cap K[x_n]$$

for all $i \neq j$.

The following theorem guarantees the existence of a coordinate change into general position for an arbitrary zero-dimensional ideal in $K[x_1, \ldots, x_n]$

Proposition 4.2
Let K be a field of characteristic 0, and let $I \lhd K[x_1, \ldots, x_n]$ be a zero-dimensional ideal. Then there exists a non-empty, Zariski open subset $U \subset K^{n-1}$ such that for all $a = (a_1, \ldots, a_{n-1}) \in U$, the coordinate change $\varphi_a : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ defined by

- $\varphi_a(x_i) = x_i$ *for* $i < n$, *and*
- $\varphi_a(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i$

has the property that $\varphi_a(I)$ is in general position with respect to the lexicographical ordering.

The most important proposition of the theory of primary decomposition which explains the need for the notion of general position is the following:

Proposition 4.3
Let $I \lhd K[x_1, \ldots, x_n]$ be a zero-dimensional ideal. Let $\langle g \rangle = I \cap K[x_n]$, $g = g_1^{v_1} \cdots g_s^{v_s}$, g_i monic and prime with $g_i \neq g_j$ for $i \neq j$. Then

1. $I = \bigcap_{i=1}^{s} \langle I, g_i^{v_i} \rangle$.

If I is in general position w.r.t. the lexicographical ordering with $x_1 > x_2 > \ldots x_n$, then

2. $\langle I, g_i^{v_i} \rangle$ is primary for all i.

So the idea of primary decomposition is:

1. use a coordinate change $\varphi_a : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ to get into general position
2. get the primary decomposition of $\varphi_a(I)$ from Proposition 4.3
3. invert the coordinate change to get the primary decomposition of our original I.

4.2 The theory of zero-dimensional radical computation

To explain the main idea used in the algorithm for the zero-dimensional real radical via reduction to the univariate case consider the following example. For the rest of this chapter let $F := \mathbb{Q}(y_1, y_2, \ldots, y_m)$ as in Chapter 3.

Example 4.4
Let $I = \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\rangle \trianglelefteq F[x_1, \ldots, x_n]$ be given. If $\overline{g_n}$ is the real part of g_n obtained by the procedure `RealPoly` from the last two chapters then the real radical of I is:

$$\sqrt[re]{I} = \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), \overline{g_n}(x_n)\rangle$$

Proof
Let $g_n = \prod_{i=1}^{r} p_i^{\alpha_i}$ be the factorization of g_n in $F[x_n]$. Then every ideal $\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle$ is maximal because of the isomorphism

$$F[x_1, \ldots, x_n]/\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle \cong F[x_n]/\langle p_i\rangle.$$

As p_i is prime we conclude that $F[x_1, \ldots, x_n]/\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle$ is a field.
Now $\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle$ is real iff p_i is real because $F[x_n]/\langle p_i\rangle$ is real iff p_i is real by Proposition B.7. Hence

$$\begin{aligned}
\sqrt[re]{I} &\overset{cor.B.6}{=} \bigcap_{M \in \mathrm{Min}(I) \text{ real}} M \\
&= \bigcap_{p_i \text{ is real}} \langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle \\
&= \langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, \prod_{p_i \text{ is real}} p_i\rangle \\
&= \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), \overline{g_n}(x_n)\rangle
\end{aligned}$$

■

The main theorem for the zero-dimensional computation in the article of Becker and Neuhaus is the Shape lemma which gives a detailed information on the shape of the reduced Groebner basis of a radical ideal satisfying the property of being in general position in some kind of way. So that we can obtain the position of an ideal given in the example above.

Lemma 4.5 (Shape)
Let I be a zero-dimensional radical ideal in $F[x_1, \ldots, x_n]$ with all d roots in $\overline{F}^n$ having distinct x_n coordinates. Then the reduced Groebner basis of I in the lexicographical ordering has the shape

$$G = \{x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_{n-1}), g_n(x_n)\},$$

where g_n is a square-free polynomial of degree d and the g_i $i < n$ are polynomials of degree $d - 1$.

Proof
First of all we will see that there exist $g_1, \ldots, g_{n-1} \in F[x_n]$ of degree $d - 1$ and a square-free $g_n \in F[x_n]$ of degree d such that

$$I = \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\rangle.$$

Afterwards I show that $G = \{x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\}$ is a reduced Groebner basis.

Step 1: Existence of $g_1, \ldots, g_n$:
From Hilbert's Nullstellensatz we know that $I_F(V_{\overline{F}}(I)) = \sqrt{I} = I$ and $V_{\overline{F}}(I)$ is finite. Let $a_1, \ldots, a_d$ be the d distinct x_n coordinates, i.e. the projection of $V_{\overline{F}}(I)$ to the x_n-axis, in $\overline{F}$.

Set $g_n = (x_n - a_1) \cdot (x_n - a_2) \cdots (x_n - a_d)$ and let $\langle r\rangle = I \cap F[x_n] \trianglelefteq F[x_n]$. Wlog we can assume, that r is monic.

Claim: $r = g_n$ and hence $g_n \in F[x_n]$

Proof:
Using Hilbert's Nullstellensatz over $\overline{F}$ we get:

$$\begin{aligned}\langle r\rangle &= I_{\overline{F}}(V_{\overline{F}}(r)) = I_{\overline{F}}(\{a_1, a_2, \ldots, a_d\}) \\ &= \langle (x_n - a_1) \cdot (x_n - a_2) \cdots (x_n - a_d)\rangle = \langle g_n\rangle.\end{aligned}$$

Hence g_n and r are associated in $\overline{F}[x_n]$. As both are monic, $r = g_n$ in $\overline{F}[x_n]$, i.e. they are equal in $F[x_n]$ too.

From the assumption, we know that all roots of I have distinct x_n coordinates so we take for each x_j with $j < n$ the unique x_j coordinates $b_{ij} \in \overline{F}$ for all a_i. Via Lagrange interpolation we can get polynomials g_j of degree $d-1$ satisfying the following conditions:

$$\begin{aligned} g_j(a_i) &= b_{ij} \ \forall i, j \text{ with } j < n \\ g_j = g_{j_{d-1}} x_n^{d-1} + g_{j_{d-2}} x_n^{d-2} + \ldots g_{j_1} x_n + g_{j_0} &\in \overline{F}[x_n].\end{aligned}$$

Recall that these g_j have the form

$$g_j(x_n) = \sum_{i=1}^{d} b_{ij} \cdot \prod_{r \neq i} \frac{x_n - a_r}{a_i - a_r}.$$

Hence the radical ideal $\overline{I} = \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n) \rangle$ defines the zero-set of I in $\overline{F}$ by definition. If we can show now that every g_j is already in $F[x_n]$ we have $I = \overline{I} \trianglelefteq F[x_1, \ldots, x_n]$ which we assumed.

Let $j < n$ be arbitrary and $\langle r_j \rangle := I \cap F[x_j] = \overline{I} \cap F[x_j]$ the univariate part of I in the variable x_i. Now r_j has the form $r_j = r_{j_d} x_j^d + \ldots r_{j_1} x_j + r_{j_0}$.
Using the form of $\overline{I}$ and the elimination property we know that there exists a polynomial $k \in F[x_n]$ such that

$$r_j(g_j) = k \cdot g_n$$

If we now compare the coefficients of g_i inductively in some way, we get that they are all in F. [1]

Thus $g_j \in F[x_n]$ and $I = \overline{I}$

Step 2: Reduced Groebner basis:
This is much easier than the first statement. From the form of I it is clear that $L(I) = \langle x_1, \ldots, x_{n-1}, x_n^d \rangle$, because all g_j have a degree less than d. So G is a Groebner basis by the product criterion. Also all leading monomials of G are co-prime and thus interreduced. So the Groebner basis G is reduced. ∎

A naive idea for an algorithm could be:

1. Compute the radical $\sqrt{I}$ of the given ideal I.

2. Test if $\sqrt{I}$ fulfills the shape condition with respect to one variable x_i and compute a reduced Groebner basis of $\sqrt[re]{I}$ w.r.t. a lexicographical ordering with lowest variable x_i. If not use a random change into general position until this condition is fulfilled.

3. Compute the real radical of $\sqrt{I}$ as described in Example 4.4 and undo the coordinate change.

[1] It would take too much time to do this in detail and as this theorem is not important for practical computations because there is a more useful generalization for maximal ideals in the next subsection. I have just sketched that the g_i are in $F[x_n]$.

As a coordinate change into general position causes a growth of coefficients and terms which slows the Groebner bases computations down it is important to avoid this change as often as possible. Therefore I give some heuristics, i.e. some kinds of special cases in which we do not have to apply a random coordinate change.
The idea for the algorithm due to Becker and Neuhaus ([BN98]) has been presented in Example 4.4 and Lemma 4.5. In the rest of the chapter, I will present my own algorithm.

As in Singular the primary decomposition of zero-dimensional ideal is vary efficient in the average case we can use this algorithm as a black box. The main idea of the primary decomposition due to Gianni/Trager/Zacharias (the command is `primdecGTZ`) was presented in the prior section. Hence we can assume the maximality of all ideals we are dealing with. The next section presents some heuristics which I found by testing the property of being real for maximal ideals (short realness).

4.3 How to decide whether a maximal ideal is real

For a maximal ideal there are only two possibilities – either it is real or its real radical is the whole ring. This is the reason why getting criteria for maximal ideals is not difficult. The main idea of this section is to find an heuristic which fulfills the following criteria:

1. Its costs have to be lower in the average case than the costs that a random coordinate change would cost.

2. The decision of realness must be an easy test, i.e. it shouldn't cost too many operations.

3. Our heuristic must cancel out maximal ideals M which are not real as early as possible in the computations.

Here are some properties of maximal ideals that I found during the work on my Diplomarbeit. For the definition of orderings and real closed I refer to the Appendix Chapter A.

One obvious property of real maximal ideals is the following corollary.

Corollary 4.6
Let $M \lhd \cdot F[x_1, \ldots, x_n]$ be maximal and $f_1, \ldots, f_n$ be the univariate polynomials such that $\langle f_i \rangle = M \cap F[x_i]$. If M is real then every f_i is real too.

PROOF
First of all, we prove that every f_i is prime: As $f_i \in M$, one irreducible factor of f_i is in M. Suppose now that f_i is not prime in $F[x_i]$. Then $f_i = gh$, where $1 < \deg g, \deg h < \deg f$. As every maximal ideal is prime we obtain $g \in M$ or $h \in M$. Let wlog $g \in M$. But then $\langle f_i \rangle \subsetneq \langle g \rangle \subseteq M \cap F[x_i]$ which is a contradiction.

If now one of the f_i is not real the its real part is 1. Hence $1 \in \sqrt[re]{\langle f_i \rangle} = \sqrt[re]{M \cap F[x_i]} \overset{L.1.8}{=} \sqrt[re]{M} \cap F[x_i]$, so $1 \in \sqrt[re]{M}$ and thus M is not real. ∎

Another simple remark is:

Remark 4.7
If $M = \langle f_1, \dots f_n \rangle \lhd \cdot \mathbb{Q}[x_1, \dots, x_n]$ is a maximal ideal with every $f_i \in \mathbb{Q}[x_i]$ is real, then M is real.

PROOF
This is clear as every f_i has a zero a_i in the common real closed field $\mathbb{R}$. Thus $(a_1, \dots, a_n) \in \mathbb{R}^n$ is in the real zeros of M. ∎

Note that this simple remark for the rational numbers is not true for an arbitrary real field F. This remains only true if F is an ordered field. The problem for arbitrary real fields is the following:
A polynomial $f_i \in F[x_i]$ is real iff there there exist orderings $\alpha_1, \dots, \alpha_r$ and the corresponding real closures $R_{\alpha_1}, \dots, R_{\alpha_r}$ such that f_i has zeros in every R_{α_i}.
But these orderings α_i could occur in a way that there exists no common real closed ground field R_α and no corresponding ordering α of F such that the polynomials f_i all have a root in R_α, which would yield that M is real. The following counter-example for arbitrary real fields clarifies the problem:

Example 4.8
Let $M = \langle x^2 + 1 + t, y^2 - t \rangle \lhd \cdot \mathbb{Q}(t)[x, y]$. Then $m_1 = x^2 + 1 + t$ is real in every real closed extension R_α of $\mathbb{Q}(t)$ which admits an ordering α in which $t < -1$ (note that we conclude that m_1 is real as it is indefinite over $\mathbb{R}$), $m_2 = y^2 - t$ is real in every real closed extension R_β which admits an ordering β satisfying $t > 0$. Both types of orderings, the α– and β-orderings, contradict each other.
In fact M is not real as

$$1^2 + x^2 + y^2 = m_1 + m_2 \in M$$

and hence $1 \in \sqrt[re]{M}$.

Analogous to the Shape Lemma, there holds a stronger property for maximal ideals that can be tested very easily:

Proposition 4.9
Let $M \lhd \cdot F[x_1, \ldots, x_n]$ be a maximal ideal and $G = \{g_1, \ldots, g_n\}$ the reduced Groebner basis of M with respect to any lexicographical ordering with smallest variable x_i. If G has the following properties:

- *$g_1 \in F[x_i]$[2] and g_1 is real.*
- *every g_i for $i = 2, \ldots, n$ has odd degree in its leading variable (see Definition 3.20).*

Then the maximal ideal M is real.

Proof
Assume for simplicity that $G = \{g_1, \ldots, g_n\}$ is a Groebner basis satisfying the properties above w.r.t. the ordering $x_1 < x_2 < \ldots < x_n$.
As $g_1 \in F[x_1]$ is real there exists a real closed field $R \supset F$ such that g_1 has a zero $\alpha_1 \in R$. Now $g_2(x_2, \alpha_1) \in R[x_2]$ has odd degree and thus has a zero α_2 in R by the fundamental theorem of algebra. By the same reason $g_3(x_3, \alpha_2, \alpha_1) \in R[x_3]$ has a zero $\alpha_3 \in R$. Inductively there exists an $\alpha \in V_{R^n}(M)$.
Thus $V_R(M) \neq \varnothing$ and hence, by the definition of the real zero-set of M, $V_{re}(M) \neq \varnothing$ (see Definition B.13). Now by the Real Nullstellensatz (cf. Theorem B.14) $\sqrt[re]{M} = I_F(V_R(M)) = I_F(\alpha) \subset M$. As M is maximal and $V_{re})M =\neq \varnothing$ we conclude the realness M. ∎

As a last condition to test the realness of M is:

Lemma 4.10
Let $M = \langle m_1, \ldots, m_n \rangle$ be a maximal ideal in $F[x_1, \ldots, x_n]$ written as a reduced lexicographical Groebner basis w.r.t to the ordering $x_1 < x_2 < \ldots < x_n$. IF M is real, every generator m_i is real.

Proof
Assume contrary: Thus let i be the smallest index such that m_i is not real. As M is a lexicographical Groebner basis we get the following cases:

Case 1: $i = 1$ then $m_1 \in F[x_1]$ and has no real root. So

$$\langle 1 \rangle = \sqrt[re]{m_1} \subset \sqrt[re]{\langle m_1, \ldots, m_n \rangle} = \sqrt[re]{M}.$$

Thus M is not real which is a contradiction.

Case 2: $i > 0$. Let R be an arbitrary real closure of (F, α) w.r.t. an ordering α of F such that $a = (a_1, \ldots, a_n) \in R^n$ is a real point of M (i.e. $a \in V_{re}(M)$). Then we have the following situation:

[2] G is a triangular set as it is a reduced lexicographical Groebner basis, wlog we can assume that the univariate polynomial in smallest variable in G is g_1.

- $M' := \langle m_1, \ldots, m_i \rangle = M \cap F[x_1, \ldots, x_i] \lhd \cdot F[x_1, \ldots x_i]$ is real since $(a_1, \ldots, a_i) \in V_R(M') \subset V_{re}(M')$.

- $M'' := \langle m_1, \ldots, m_{i-1} \rangle = M \cap F[x_1, \ldots, x_{i-1}] \lhd \cdot F[x_1, \ldots x_{i-1}]$ is real since $(a_1, \ldots, a_{i-1}) \in V_R(M'') \subset V_{re}(M'')$.

As M' is real, the ordering α of F can be extended in $k(M) = F[x_1, \ldots, x_n]/M$, i.e. $k(M)$ is a formally real field (see Proposition B.7). From the first isomorphism theorem, we get:

$$\begin{aligned} F[x_1, \ldots, x_i]/M' &\cong (F[x_1, \ldots, x_{i-1}, x_i]/M'')/(M'/M'') \\ &= ((F[x_1, \ldots, x_{i-1}]/M'')[x_i])/((\langle m_i \rangle + M'')/M''). \end{aligned}$$

Now as $(a_1, \ldots, a_{i-1})$ is a (real) root of the maximal M'' we get that

$$F[x_1, \ldots, x_{i-1}]/M'' \cong F(a_1, \ldots, a_{i-1})$$

which is ordered by $F(a_1, \ldots, a_{i-1}) \cap R^2$. Hence

$$k(M) \cong F(a_1, \ldots, a_{i-1})[x_i]/\langle m_i(a_1, \ldots, a_{i-1}, x_i) \rangle$$

and $k(M)$ is real. Thus the ordering $F(a_1, \ldots, a_{i-1}) \cap R^2$ can be extended to $F(a_1, \ldots, a_{i-1}, a_i) \cap R^2$ (as a_i is a real root of $m_i(a_1, \ldots, a_{i-1}, x_i)$ by the definition of a). But then $m_i(a_1, \ldots, a_{i-1}, x_i)$ is indefinite over R by the sign change criterion (Theorem B.10) and thus $m_i(x_1, \ldots, x_i)$ is indefinite over R, too. Now we get from Remark B.12 that m_i is real which contradicts the assumption. ∎

Lemma 4.10 is no equivalence as we can see in the following example:

Example 4.11
Let $M = \langle x^3 - 2, y^2 + x^2 - x \rangle \lhd \cdot \mathbb{Q}[x, y]$. Now $x^3 - 2$ is real since $\sqrt[3]{3}$ is in $\mathbb{R}$ and $y^2 + x^2 - x$ is real by Lemma 3.1 as it is indefinite-
But M is not real as $y^2 + \sqrt[3]{2}^2 - \sqrt[3]{2}$ has no real root since $\sqrt[3]{2}^2 - \sqrt[3]{2} > 0$.

The last corollary is useful to test the realness of prime polynomials $f \in F[x_1, \ldots, x_n]$.

Corollary 4.12
Let $f \in \mathbb{Q}[y_1, y_2, \ldots, y_m, x_1, \ldots, x_n]$ be an irreducible polynomial. Then f is real considered as polynomial in $F[x_1, \ldots, x_n]$ iff f considered as a polynomial in $\mathbb{Q}[y_1, y_2, \ldots, y_m, x_1, \ldots, x_n]$ is real.

Proof
⇒: As $\langle f \rangle F[x_1, \ldots, x_n]$ is real in $F[x_1, \ldots, x_n]$, there exists an x_i such that $\deg_{x_i} f > 0$. Without loss of generality let x_n be this x_i. By Lemma 1.8 we conclude that $\langle f \rangle F(x_1, \ldots, x_{n-1})[x_n] = \langle f \rangle \mathbb{Q}(y_1, y_2, \ldots, y_m, x_1, \ldots, x_{n-1})[x_n]$ is real. Thus by Lemma 3.1 $\langle f \rangle \mathbb{Q}[y_1, y_2, \ldots, y_m, x_1, \ldots, x_n]$ is real and hence f is real considered over $\mathbb{Q}[x_1, \ldots, x_n, y_1, y_2, \ldots, y_m]$.

$\Leftarrow$: This is clear as reality commutes with localization (see Lemma 1.8). ∎

Combining all these conditions yields a good heuristic to decide the property of being real for maximal ideals M. Let us first consider a large example in which it was possible to avoid the change into general position completely.

Example 4.13
Let

$$I = \langle (y^3+3y^2+y+1)(y^2+4y+4)(x^2+1),\\ (x^2+y)(x^2-y^2)(x^2+2xy+y2)(y^2+y+1)\rangle \trianglelefteq \mathbb{Q}[x,y]$$

The primary decomposition of I yields 10 maximal ideals.

1. $M_1 = \langle y^2+1, x-y\rangle$ *which is not real as* y^2+1 *is not real. Hence it does not satisfy the conditions in Proposition 4.9 and Corollary 4.6..*

2. $M_2 = \langle y-1, x^2+1\rangle$ *does not satisfy the corollary 4.6 and is thus not real.*

3. $M_3 = \langle y^2+y+1, x^2+1\rangle$ *does not satisfy Corollary 4.6 and is thus not real.*

4. $M_4 = \langle y^2+1, x+y\rangle$ *does not satisfy Corollary 4.6 and is thus not real.*

5. $M_5 = \langle y+2, x-2\rangle$ *is real by Proposition 4.9 or Remark 4.7.*

6. $M_6 = \langle y+2, x^2-2\rangle$ *is real by Proposition 4.9 for the ordering* $x < y$ *with the reduced Groebner basis* $G = \{x^2-2, y+2\}$.

7. $M_7 = \langle y+2, x+2\rangle$ *is real by Proposition 4.9 or Remark 4.7.*

8. $M_8 = \langle y^3+3y^2+y+1, x+y\rangle$ *is real by Proposition 4.9 w.r.t. the ordering* $y < x$ *under which* M *is a reduced Groebner bases.*

9. $M_9 = \langle y^3+3y^2+y+1, x^2+y\rangle$. *Here it is not obvious to see if* M_9 *is real or not. So we have to compute the Groebner bases w.r.t. both orderings* $x < y$ *and* $y < x$.
   The Groebner basis w.r.t. to the lexicographical ordering $x < y$ *of* M_9 *is*

   $$G_M = \langle x^6-3x^4+x^2-1, y+x^2\rangle.$$

   First we have to test if $x^6-3x^4+x^2-1$ *is real. We know that* $x^6-3x^4+x^2-1$ *is prime and after applying the* `RealPoly` *Procedure introduced in the last two chapters we get that* $x^6-3x^4+x^2-1$ *is real. Now we know that* M_9 *is real by Proposition 4.9 w.r.t. to the ordering* $x < y$.

10. $M_{10} = \langle y^3 + 3y^2 + y + 1, x - y \rangle$ *is real by Proposition 4.9.*

So the real radical of I *is*

$$\begin{aligned} \sqrt[re]{I} &= M_5 \cap M_6 \cap M_7 \cap M_8 \cap M_9 \cap M_{10} \\ &= \langle y^4 + 5y^3 + 7y^2 + 3y + 2, x^4 - x^2y^2 + x^2y - y^3 \rangle \end{aligned}$$

In the next subsection I describe a procedure using the criteria introduced above.

After giving this procedure it is easy to describe the algorithm for the zero-dimensional case using a coordinate change into general position.

4.3.1 The procedure `prepare_max`

The procedure `prepare_max` which uses the properties I found, acts in the following way:
It gets as input a maximal ideal M and returns a list $erg = \overline{M}, j$, where

$$\overline{M} = \begin{cases} \sqrt[re]{M} & \text{if } j = 1, \text{ the change into general position can be avoided} \\ M & \text{if } j = 0, \text{ the change into general position cannot be avoided} \end{cases}$$

I explain my algorithm in pseudo-code. The proof of the correctness of this algorithm follows from the criteria I explained above. In the algorithm itself there is no need to check Corollary 4.6 explicitly. This criterion is checked implicitly in the check of Proposition 4.9 as we will see.

The procedure `prepare_max` is written as follows:

Algorithm 4.1 (An heuristic to check if a coordinate change can be avoided)
proc *prepare_ max(M)*

INPUT : *a maximal ideal* $M \lhd \cdot F[x_1, \ldots, x_n]$

OUTPUT: *a list* $erg = (\overline{M}, j)$ *s.t.:*

$$\overline{M} = \begin{cases} \sqrt[re]{M} & \text{if } j = 1, \text{ the change into general position can be avoided} \\ M & \text{if } j = 0, \text{ the change into general position can}'\text{t be avoided} \end{cases}$$

BEGIN

Initialize $P := \{\lambda : \lambda \text{ is a permutation of the variables } \{x_1, \ldots, x_n\}\}$

while $(P \neq \varnothing)$ *do* {

Choose a $\lambda = (x_{j_1}, x_{j_2}, \ldots, x_{j_n}) \in P$

$P := P \setminus \{\lambda\}$

Compute the lexicographical Groebner basis $M_\lambda = \{f_1, f_2, \ldots, f_n\}$ *of* M *w.r.t. the ordering* $x_{j_1} < x_{j_2} < \ldots < x_{j_n}$. *Now* f_1 *is univariate in the variable* x_{j_1}.

Let $\overline{f_1} :=$ `RealPoly`(f_1) *the real part of* f_1. *As* f_i *is prime there are two possibilities* $\overline{f_1} = 1$ *or* $\overline{f_1} = f_1$.

if $(\overline{f_1} = 1)$

{

$erg := \langle 1 \rangle, 1$

$return(erg)$;

}

According to Proposition 4.9 search the first position $k \geq 2$ *such that* m_k *has even degree in* x_{j_k}. *Set* $k = n + 1$ *if there exists none.*[2]

if $(k > n)$

{

$erg := M, 1$; *(Correctness is clear from Prop. 4.9)*

$return(erg)$;

}

According to Lemma 4.10 search from. position $(k+1)$ *in* M_λ, *the first non-real generator* m_i.

If there exists a position $i \leq n$ *set* $erg = \langle 1 \rangle, 1$ *and return* erg.

}

[2]This is done via my auxiliary procedure `search_first`.

If F is non parametric, i.e. $F = \mathbb{Q}$ and every generator of M is univariate use Remark 4.7 and return $erg := M, 1$.

$erg := M, 0;$

$return(erg);$

END

4.3.2 A short overview on coordinate changes into general position

If an ideal fails this test, i.e. the result of $prepare\_max(M)$ is $erg = M, 0$ we have to apply a coordinate change into general position.
As this is crucial for the performance of the implemented algorithm, but not in the central scope of my Diplomarbeit, it seems advisable to use the already well-optimized coordinate change implemented in the primdec.lib.
The method I implemented is called `GeneralPos`. It gets a list of maximal ideals which failed the test `prepare_max` as input and returns the intersection of all real maximal ideals of this input.
The main idea of the coordinate change is to avoid the situation that our change is completely randomized. `GeneralPos` is written in a recursion such that if the depth of the recursion tree (in Singular this is called the voice) is higher then a defined constant we apply a completely random change.
The idea of the not completely random change is to construct a polynomial *randp* to change the last variable. This change is just a little change, i.e. the coefficients of it are not too large. As an example, in $F[x, y, z]$ for $F = \mathbb{Q}$ we could change the last variable z to $z+3x+y$ and not to $z+1001x+199y$ or something like that. If $F = \mathbb{Q}(s)$ we could change z to $z + 2x + 4y + s + 5s^2$ or something else. In the general case this small variation of the last coordinate will suffice to test again with `prepare_max` if the maximals ideals are real.
Let us consider an example. An ideal in which we have to apply a coordinate change into general position was presented in Example 4.8. Lets have a look at this.

Example 4.14
Let $M = \langle x^2 + 1 + t, y^2 - t\rangle \lhd \cdot\mathbb{Q}(t)[x, y]$. Choosing the coordinate change

$$\begin{aligned} \varphi : \mathbb{Q}(t)[x, y] &\to \mathbb{Q}(t)[x, y] \\ x &\mapsto x \\ y &\mapsto y + x + t \end{aligned}$$

we get:

$$\begin{aligned}\varphi(M) &= \langle x^2+1+t, (y+x+t)^2-t\rangle \\ &= \langle x^2+1+t, x^2+2xy+2tx+y^2+2ty+t^2-t\rangle\end{aligned}$$

Its lexicographical Groebner basis w.r.t. the ordering $y < x$ is:

$$\begin{aligned}G_\varphi = \{&y^4+4ty^3+(6t^2+t)y^2+(4t^3+4t)y+(t^4+6t^2+4t+1),\\ &(-4t-2)x-y^3+(-3t)y^2+(-3t^2-2t-3)y+(-t^3-2t^2-3t)\}.\end{aligned}$$

Now $y^4+4ty^3+(6t^2+2)y^2+(4t^3+4t)y+(t^4+6t^2+4t+1)$ is not real in $\mathbb{Q}(t)[y]$ as $y^4+4ty^3+(6t^2+2)y^2+(4t^3+4t)y+(t^4+6t^2+4t+1)$ is positive semi-definite (which we conclude from the decision method presented in Chapter 3). Hence as in Example 4.8 we get that M is not real.

In all my tests it didn't happen often that I had to change into general position for the test of being real. In fact the only examples I found in which there is a need to apply this change are ideals over transcendent extensions of $\mathbb{Q}$ which are of the form in Example 4.8, i.e. every generator is univariate and real. For these cases I have not yet found any property to check realness by the aid of Singular without applying this change. A simple example for an ideal in which this change yields the reality of a maximal ideal is the following:

Example 4.15
Let $M = \langle x^2+1-t, y^2-t\rangle \lhd \cdot\mathbb{Q}(t)[x,y]$. Here the same coordinate change as in the example above yields:

$$\begin{aligned}\varphi(M) &= \langle x^2+1-t, (y+x+t)^2-t\rangle \\ &= \langle x^2+1-t, x^2+2xy+2tx+y^2+2ty+t^2-t\rangle\end{aligned}$$

Here the Groebner basis w.r.t. the lexicographical ordering $y < x$ is:

$$\begin{aligned}G_\varphi = \{&y^4+4ty^3+(6t^2-4t+2)y^2+(4t^3-8t^2+4t)y+(t^4-4t^3+2t^2+1),\\ &2x+y^3+3ty^2+(3t^2-4t+3)y+(t^3-4t^2+3t)\}.\end{aligned}$$

Now $y^4+4ty^3+(6t^2-4t+2)y^2+(4t^3-8t^2+4t)y+(t^4-4t^3+2t^2+1)$ is real as it is indefinite and the degree of $2x+y^3+3ty^2+(3t^2-4t+3)y+(t^3-4t^2+3t)$ in x is odd. Hence $\varphi(M)$ is real by Proposition 4.9, thus M is real. In fact M is α-real in every ordering α of $\mathbb{Q}(t)$ satisfying the condition $t \geq 1$.

To finish this subsection let me explain the idea of the algorithm `GeneralPos` in pseudo code. Note that this is just a simplification and the complete algorithm is more complicated.

Algorithm 4.2 (Coordinate change into general position)
proc *GeneralPos(NonPrep)*

INPUT : *A set* $NonPrep := \{M_1, \ldots, M_l\}$ *of maximal ideals in* $F[x_1, \ldots, x_n]$

OUTPUT: *The intersection ideal* $J := \cap \sqrt[re]{M_i}$ *bye the aid of a coordinate change.*

BEGIN

if (the voice of the procedure is less then 10)

{

Initialize a randomized polynomial

$$randp := \begin{cases} x_n + \sum_{i=1}^{n-1} a_i x_i & a_i \in \{0, 1, \ldots, 5\} \text{ randomized and } F = \mathbb{Q} \\ x_n + \sum_{i=1}^{n-1} a_i x_i + b_1 y_1 + b_2 y_1^2 & a_i, b_j \in \{0, 1, \ldots, 5\} \text{ randomized and } F = \mathbb{Q}(y_1, y_2, \ldots, y_m) \end{cases}$$

}

else

{

$randp := randomLast(100)$; [3]

}

Define the map φ *as follows:*

$$\varphi(x_i) := \begin{cases} x_i & \text{if } i < n \\ randp & \text{if } i = n \end{cases}$$

By the definition of randp the inverse map is defined as follows:

$$\varphi^{-1}(x_i) := \begin{cases} x_i & \text{if } i < n \\ 2x_n - randp & \text{if } i = n \end{cases}$$

while $NonPrep \neq \varnothing$ *do*

[3]Where **randomLast** randomizes a polynomial $x_n + \sum_{i=1}^{n-1} a_i x_i$, where the a_i are integers between 0 and 100.

{

Choose an $M \in NonPrep$*;*

$NonPrep := NonPrep \setminus \{M\}$*;*

Initialize $Prep := \varnothing$ *and* $StillNonPrep = \varnothing$*;*

if ($prepare\_max(\varphi(M)) = \overline{M}, 1$ *and* $\overline{M} \neq \langle 1 \rangle$*)*

{

$Prep := Prep \cup \{M\}$*;*

}

else

{

$StillNonPrep := SillNonPrep \cup \{\varphi(M)\}$*;*

}

}

$Prepared := \bigcap_{M \in Prep} M$*;*

if ($StillNonPrep = \varnothing$*)*

{

$J := Prepared$*;*

}

else

{

$J := Prepared \cap (\varphi^{-1}(GeneralPos(StillNonPrep)))$*;*

}

return(J);

END

As an example for this algorithm we could take as input the ideal of Example 4.14 and 4.15, i.e. let $NonPrep := \{M_1, M_2\}$, where $M_1 = \langle x^2+1+t, y^2-t\rangle$ and $M_2 = \langle x^2+1-t, y^2-t\rangle$. With the coordinate change φ of the previous two examples ($\varphi(x) = y, \varphi(y) = y+x+t$) we get that the resulting ideal J is M_2.

4.4 An algorithm to compute the zero-dimensional radical

From the explanation in the last section, it is not difficult to get an algorithm which computes the real radical of a zero-dimensional ideal J in $F[x_1, \ldots, x_n]$.

Before explaining the algorithm, we want to simplify the input as much as possible. For example the following remark is very useful.

Remark 4.16
Let $I = \langle f_1, f_2, \ldots, f_r\rangle \trianglelefteq F[x_1, \ldots, x_n]$ be a zero-dimensional ideal. For every generator with the prime factorization $f_i = \prod_{j=1}^{l} p_j^{\alpha_j}$, set:

$$g_j := \prod_{j=1}^{l} \overline{p_j},$$

where

$$\overline{p_j} = \begin{cases} p_j & \text{if } p_j \text{ is not univariate} \\ \texttt{RealPoly}(p_j) & \text{if } p_j \text{ is univariate} \end{cases}.$$

Then $I \subseteq \langle g_1, \ldots, g_n\rangle \subseteq \sqrt[re]{I}$.

Proof
The first inclusion is clear as every generator f_i of I is divisible by the corresponding g_i hence in the ideal $\langle g_1, \ldots, g_n\rangle$. For the second inclusion we have to show that every g_i is in $\sqrt[re]{I}$. Therefor we show that $g_i \in \sqrt[re]{\langle f_i\rangle}$ which is a subideal of $\sqrt[re]{I}$.
Let $h_i := \frac{\overline{f_i}}{g_i}$, where $\overline{f_i}$ is the square-free part of f_i. Then every h_i is the product of non-real univariate factors q_j and hence $\sqrt[re]{\langle h\rangle} = \langle 1\rangle$. Now

$$\begin{aligned} g_i \in \langle f_i\rangle \subseteq \sqrt[re]{\langle f_i\rangle} \\ = \sqrt[re]{\langle g_i \cdot h_i\rangle} \overset{Lemma\ 1.8}{=} \sqrt[re]{\langle g_i\rangle} \cap \sqrt[re]{\langle h_i\rangle} \\ = \sqrt[re]{\langle g_i\rangle} \cap \langle 1\rangle = \sqrt[re]{\langle g_i\rangle} \end{aligned}$$

■

From this remark we get a procedure to simplify every generator of the ideal I. Now the algorithm for the zero-dimensional computation is the following:

Algorithm 4.3
proc *RealZero(I)*

INPUT : *a zero-dimensional ideal* $I \trianglelefteq F[x_1, \ldots, x_n]$

OUTPUT: *an ideal* $\overline{J}$ *s.th.* $\overline{J} = \sqrt[re]{I}$

Simplify the ideal $I = \langle f_1, \ldots, f_r \rangle$ *to* $J = \langle g_1, \ldots, g_r \rangle$ *as described in Remark 4.16,*[4]

Compute the associated primes of $Max := \mathrm{Min}(I)$ *with* `primdecGTZ` *or* `primdecSY`.
(This depends on which algorithm is faster.[4]*).*

Initialize $Prep := \varnothing$ *and* $NonPrep := \varnothing$

while $Max \neq \varnothing$ *do*

{

Choose an $M \in Max$

$Max := Max \setminus \{M\}$

Compute $erg = \overline{M}, j$ *with Algorithm 4.1.*

If $j = 1$ *and* $\overline{M} \neq \langle 1 \rangle$

{

$Prep := Prep \cup \{\overline{M}\}$

}

else

{

$NonPrep := NonPrep \cup \{\overline{M}\}$

[4]These operations are applied with a timer by the aid of the `watchdog` command. watchdog(command, timer) returns the result of the command if the time for the command finishes before the timer.

}

$Prepared := \bigcap_{\overline{M} \in Prep} \overline{M}$:

$NonPrepared := GeneralPos(NonPrep)$;[5]

According to Lemma 1.8 we get that

$$\overset{re}{\sqrt{I}} = \overset{re}{\sqrt{J}} = Prepared \cap NonPrepared =: \overline{J}.$$

$return(\overline{J})$;

To finish this chapter I give an example in which every path of Algorithm 4.3 is taken.

Example 4.17
Let

$$\begin{aligned} I = \langle & (x^2y^3 - tx^2y + y^6 - y^5 - ty^4 + t^2 + 1) \cdot (y^3 - t^2y^2 + (-t^3 + t^2 - t)y + t^3), \\ & (-2t)x^4 - 4tx^2 + (-t+1)y^6 + (-t^2+t)y^5 + (t^2-t)y^4 + (-t^4+t^3)y^2 + \\ & (t^4 - t^3)y + (t^5 - t^4 + 2t^3 - 2t), y^7 + t^2y^4 - t^2y^3 - t^4, (-t)x^2y^2 + t^2x^2 - \\ & y^6 - ty^5 + ty^4 + (-t^3 + t^2 - t)y^2 + t^3y + (t^4 - t^3 + t^2)\rangle. \end{aligned}$$

Then every generator of I is simplified in the sense of Remark 4.16.

1. *The primary decomposition of I provides 4 minimal primes which are*

   - $M_1 = \langle x^2 + 1 - t, y^3 + t^2 \rangle$
   - $M_2 = \langle x^2 + t^2 + 1, y^2 + t \rangle$
   - $M_3 = \langle x^2 + 1 - t, y^2 - t \rangle$
   - $M_4 = \langle x^2 + 1 + t, y^2 - t \rangle$

   We set $Max := \{M_1, M_2, M_3, M_4\}$.

2. $Prep := \varnothing$ *and* $NonPrep := \varnothing$

3. *As Max is not empty choose $M_1 \in Max$ and set*

$$Max := Max \setminus \{M_1\} = \{M_2, M_3, M_4\}.$$

[5]The idea of this approach was explained with 2 examples in the previous subsection.

4. *prepare_max*$(M_1) = M_1, 1$ *because of Proposition 4.9. Hence set:*

$$Prep := Prep \cup \{M_1\} = \{M_1\}$$
$$NonPrep := NonPrep = \varnothing$$

5. *As* Max *is not empty choose* $M_2 \in Max$ *and set*

$$Max := Max \setminus \{M_2\} = \{M_3, M_4\}.$$

6. *prepare_max*$(M_2) = \langle 1 \rangle, 1$ *by Lemma 3.2 w.r.t. the lexicographical ordering* $y < x$. *Hence set:*

$$Prep := Prep = \{M_1\}$$
$$NonPrep := NonPrep = \varnothing$$

7. *As* Max *is not empty choose* $M_3 \in Max$ *and set*

$$Max := Max \setminus \{M_3\} = \{M_4\}.$$

8. *prepare_max*$(M_3) = M_3, 0$. *Hence we have to apply a coordinate change and set:*

$$Prep := Prep = \{M_1\}$$
$$NonPrep := NonPrep \cup \{M_3\} = \{M_3\}$$

9. *As* Max *is not empty choose* $M_4 \in Max$ *and set*

$$Max := Max \setminus \{M_4\}.$$

10. *prepare_max*$(M_4) = M_4, 0$. *Hence we have to apply a coordinate change and set:*

$$Prep := Prep = \{M_1\}$$
$$NonPrep := NonPrep \cup \{M_4\} = \{M_3, M_4\}$$

11. *Now* Max *is empty and we set* $Prep = \{M_1\}$.

12. *From the examples 4.14 and 4.15 we conclude with the coordinate change* φ *satisfying* $\varphi(x) = x, \varphi(y) = y + x + t$ *that* M_3 *is real and* M_4 *is not real. Hence*

$$NonPrep = \{M_3\}$$

13. Set

$$\begin{aligned}\overline{J} &= Prep \cap NonPrep = M_1 \cap M_3 \\ &= \langle y^5 - ty^3 + t^2y^2 - t^3, x^2 + (-t+1)\rangle\end{aligned}$$

Hence the real radical of I is

$$\overline{J} = \langle y^5 - ty^3 + t^2y^2 - t^3, x^2 + (-t+1)\rangle.$$

In the next chapter I explain the algorithm for the higher dimensional case, i.e. for arbitrary polynomial ideals $J \trianglelefteq F[x_1, \ldots, x_n]$. This approach will act via a reduction to the zero-dimensional case and localization on every subset of the variables $\{x_1, \ldots, x_n\}$.

5 An algorithm to compute the real radical of an arbitrary polynomial ideal

We are now able to compute the real radical of zero-dimensional ideals over the $\mathbb{Q}$-algebra $\mathbb{Q}(y_1, y_2, \ldots, y_m)[x_1, \ldots, x_n]$. To obtain an algorithm for the higher dimensional case we use a reduction to the zero dimensional case.
As we will see soon, taking all isolated real points of an ideal yields a zero dimensional ideal I_{Iso}. For this ideal we compute the zero-dimensional radical as described in the previous chapter.
This chapter uses the definitions, propositions. theorems and lemmas of the appendix. For detailed information see [BN98] Chapter 3 and 4.

As in the previous chapter, let $F := \mathbb{Q}(y_1, y_2, \ldots, y_m)$ for the whole chapter.

Since -1 is no sum of squares in F, we conclude that F is a formally real field with the pre-ordering $re = \sum F^2$. Hence every ordering $\alpha \in X(F)$ of F extends re. For every ordering $\alpha \in X(F)$ let R_α denote the unique real closure of (F, α).

5.1 Isolated real points

We consider a real closed field R_α with its order topology and R_α^n with the product topology of this order topology. This can be understood as a generalization of the Euclidean topology in $\mathbb{R}$ to arbitrary real closed fields. We can define the isolated real points of an ideal $I \in F[x_1, \ldots, x_n]$ as follows:

Definition 5.1
Let I be an ideal in $F[x_1, \ldots, x_n]$, then

a) a point $x \in V_{\overline{F}}(I)$ is called **real isolated point** *of I if it is isolated in some space $V_{R_\alpha}(I) \subseteq R_\alpha^n$ for a suitable R_α w.r.t. the induced topology.*

b) The set of all isolated points will be denoted by $V_{Iso}(I)$.

c) Finally, we define $I_{Iso} := I_F(V_{Iso}(I))$ which is the ideal describing the F-Zariski closure of $V_{Iso}(I)$.

It is now easy to verify by the general Real Nullstellensatz see Theorem B.14 that I_{Iso} is real.

The importance of I_{Iso} in connection with the computation of real radicals can be seen in the following proposition.

Proposition 5.2
Let $I \trianglelefteq F[x_1, \ldots, x_n]$ be an ideal. Then I_{Iso} is contained in any zero-dimensional component of $\sqrt[re]{I}$, i.e. every zero-dimensional component of $\sqrt[re]{I}$ consists only of isolated points.

PROOF
Let M be a zero-dimensional component of I. Then M is real by Proposition B.7.

Let $a \in V_{re}(M)$ be an arbitrary point. Then a refers, by the Real Nullstellensatz (Theorem B.14 and Remark B.15), to a real closed field $R \supseteq F$ and a maximal ideal $\overline{M} = I_R(a) \lhd \cdot R[x_1, \ldots, x_n]$. Hence a is the only zero of $\overline{M}$ in R^n.

Let us first of all see that $\overline{M}$ is a zero-dimensional component of $\sqrt[re]{I \cdot R}$.
Assume contrary:

Then we would find a further real prime $\overline{P}$ between $\sqrt[re]{I \cdot R}$ and $\overline{M}$. But then

$$\sqrt[re]{I} \subseteq \overline{P} \cap F[x_1, \ldots, x_n] =: P \subseteq M.$$

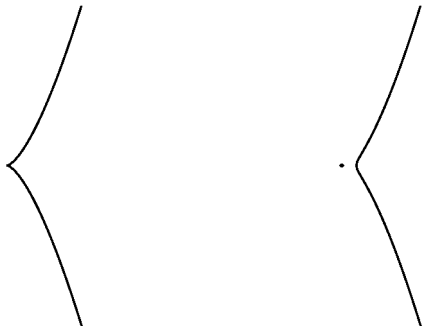
As M is a minimal prime of $\sqrt[re]{I}$ we get $M = P$. But now $R : F$ is an algebraic extension (see definition of the real closure), hence $R[x_1, \ldots, x_n] : F[x_1, \ldots, x_n]$ is an integral extension and thus $\overline{P} = \overline{M}$ by the Lying Over theorem.

As a component of $\sqrt[re]{I \cdot R}$ the maximal ideal $\overline{M}$ occurs in the primary decomposition of $\sqrt[re]{I \cdot R}$, e.g. $\sqrt[re]{I \cdot R} = (\bigcap_i \overline{P_i}) \cap \overline{M}$.

Now we can choose an $f \in (\bigcap_i \overline{P_i}) \setminus \overline{M}$. Then $V_R(I) \cap \{f \neq 0\} = \{x\}$ and thus x is isolated in $V_R(I)$ w.r.t. Zariski topology. But as Zariski open subsets are much bigger then the open set in the 'Euclidean' topology of R^n we get that x is isolated in sense of Definition 5.1. Applying the I_F-functor, we get

$$I_{Iso} = I_F(V_{Iso}(I)) \subseteq I_F(x) \subseteq M.$$ ∎

Of course it may happen that an ideal I has more real isolated points than its real radical has zero-dimensional components. Let us consider for example an ideal $I \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$.



(a) The cusp $y^2 - x^3$ (b) Our P_1

Figure 5.1: Some varieties

Note first that $\mathbb{Q}$ is an ordered field with unique real closure $\mathbb{R}_{alg} = \mathbb{R} \cap \overline{\mathbb{Q}}$ (see Lemma B.2). Hence every isolated point of I is isolated in $\mathbb{R}_{alg}$. By the Tarski-Seidenberg principle we can even say that each of this isolated points is isolated in $\mathbb{R}$ and we don't have to worry about orderings. Now the example is:

Example 5.3
Consider the ideal I in primary decomposition

$$I = \langle y^2 - x^2 \cdot (x-1) \rangle \cap \langle x+1, y \rangle$$

where $P_1 := \langle y^2 - x^2 \cdot (x-1) \rangle$ is the prime ideal resulting from the cuspidial curve $y^2 - x^3$ by changing one linear factor x to $x-1$. The consequence of this change is that P_1 has an isolated point $(0,0) \in \mathbb{R}^2$. You can see this in figure 5.1. As I is the union of the components P_1 and $P_2 = \langle x+1, y \rangle$ the isolated points are $V_{Iso}(J) = \{(-1,0), (0,0)\}$ and $I_{Iso} = \langle x+1, y \rangle \cap \langle x, y \rangle$. But the only zero-dimensional component of $\sqrt[re]{I}$ is P_2.

5.1.1 Singular points

Let us recall the definition of singular points and the singular locus.

Definition 5.4 (see. [GP02] Definition A.8.7)
Let X be a variety and $p \in X$. Then p is called a **singular** *point of X, or X is called singular at p, if the local ring $\mathcal{O}_{X,p}$ is not a regular local ring. Otherwise p is called a* **regular**, *or* **non-singular** *point of X. X is called regular or* **smooth** *if it is regular at each point p of X.*

Comparing this definition with the Corollary 5.6.14 from the computer algebra book by Greuel and Pfister ([GP02]) yields the well-known Jacobian criterion.

Theorem 5.5 (Jacobian criterion)
Let $X \subseteq \overline{K}^n$ be a variety and $I_K(X) = \langle f_1, \ldots, f_r \rangle$ then a point $p \in X$ is **regular** *iff the rank of the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}(p)\right)_{i.j}$ is $n - \dim \mathcal{O}_{X,p}$. If X is equi-dimensional then a point p is singular iff*

$$\operatorname{rk}\left(\frac{\partial f_i}{\partial x_i}(p)\right)_{i.j} < n - \dim X.$$

From this definition we are now able to define the singular locus of an ideal.

Definition 5.6 (Singular locus)
Let $I \trianglelefteq K[x_1, \ldots, x_n]$ be an arbitrary ideal. As usual let

$$V_{Sing}(I) := \{\underline{x} \in \overline{K} \ : \ V_{\overline{K}}(I) \text{ is singular at } \underline{x}\}.$$

The the ideal describing the Singular locus of I is $I_{Sing} := I_F(V_{Sing}(I))$.

After recalling singular points we follow the article of Becker and Neuhaus (cf [BN98] Chapter 3). To prove the main theorem for real isolated points, namely that I_{Iso} is a zero-dimensional ideal, we show the following proposition:

Proposition 5.7
Let $I \trianglelefteq F[x_1, \ldots, x_n]$ and R a real closed intermediate field of the extension $\overline{F} : F$. Moreover let Q be a minimal prime of the extension ideal $I \cdot \overline{F}$ of positive dimension. Let $x \in V_{\overline{F}}(Q)$. be any point. If x is regular in $V_{\overline{F}}(I)$, then it is not isolated in $V_R(I)$.

To prove this we need the following auxiliary lemma.

Lemma 5.8
Let R be a real closed field with algebraic closure $\overline{R} = R(\sqrt{-1})$ and Q any prime ideal in $\overline{R}[x_1, \ldots, x_n]$. Then $P := Q \cap R[x_1, \ldots, x_n]$ is a prime ideal and for the conjugation $\sigma \in \operatorname{Aut}(\overline{R} : R)$ holds that $P \cdot \overline{R} = Q \cap \sigma(Q)$.

The idea of the proof is to show the equality of the resulting varieties using Hilbert's Nullstellensatz. Note that both $P \cdot \overline{R}$ and $Q \cap \sigma(Q)$ are already radical in $\overline{R}[x_1, \ldots, x_n]$.

Using this lemma we prove the proposition.

Proof
Without loss of generality we can assume that $d = \dim P \in \{1, \ldots, n-1\}$. Let $\sigma \in Aut(\overline{F} : F)$ denote the conjugation. As $x \in V_{\overline{F}}(I) \cap R^n$ we know that $x = \sigma(x) \in V_{\overline{F}}(\sigma(Q))$ where $\sigma(Q)$ is a minimal prime of $\sigma(I \cdot \overline{F}) = I \cdot \overline{F}$.

If $Q \neq \sigma(Q)$, then x would be a zero of two distinct irreducible components of $V_{\overline{F}}(I)$ and thus be a singular point. This is a contradiction to the assumption and hence $Q = \sigma(Q)$. By Lemma 5.8 we get that since $P = Q \cap R[x_1, \ldots, x_n]$, $P \cdot \overline{F} = Q = \sigma(Q)$. Note that $\dim P = \dim Q = d$.
Now let $\{f_1, \ldots, f_r\}$ be a set of generators of P. Then

$$Q = P \cdot \overline{F} = \langle f_1, \ldots, f_r \rangle \overline{F}[x_1, \ldots, x_n]$$

and because of the regularity of $x \in V_{\overline{F}}(I)$ we get via the Jacobian Criterion (Theorem 5.5) that the rank of the Jacobian matrix $(\frac{\partial f_i}{\partial x_j})_{i=1,\ldots,r;j=1,\ldots,n}$ is $n-d$. This fact implies that x is a regular point of P and thus $P = \sqrt[re]{P}$ and P is real. (cf. [BCR98] Proposition 3.3.15)

According to [[BCR98], Proposition 3.3.7] there exist $n-d$ polynomials $g_1, \ldots, g_{n-d} \in P$ as well as a neighborhood U of x in R^n such that

$$V_R(g_1, \ldots, g_{n-d}) \cap U = V_R \cap U$$

and

$$\operatorname{rk} \left(\frac{\partial g_i}{\partial x_j} \right)_{i,j} = n - d.$$

Now the theorem of implicit functions (see e.g. [[BCR98], Corollary 2.9.6]) yields that x is not isolated in $V_R(g_1, \ldots, g_{n-d}) \cap U \subset V_R(I)$. Thus it is not isolated in $V_R(I)$. ∎

From Proposition 5.8 we conclude that $V_{Iso}(I) \subseteq V_{Sing}(I)$, the set of all singular points of the ideal I. Now $V_{Sing}(I)$ is closed and every component of dimension greater than 0 of $V_{Sing}(I)$ has no isolated points. Thus we conclude that $V_{Iso}(I)$ has a dimension less then a equal zero and hence I_{Iso} equals either the unit ideal or has dimension zero. Let's fix this fact in the following remark:

Remark 5.9
Let $I \trianglelefteq \mathbb{Q}(y_1, y_2, \ldots, y_m)[x_1, \ldots, x_n]$. Then $\dim I_{Iso} \leq 0$, i.e. $I_{Iso} = \bigcap_{i=1}^{r} M_i$ for some maximal ideals $M_1, \ldots, M_r$.

The importance of I_{Iso} in connection with the computation of $\sqrt[re]{I}$ relies on the fact that (according to Proposition 5.2) any zero-dimensional component M of $\sqrt[re]{I}$ occurs among the M_i, i.e. every zero-dimensional component of $\sqrt[re]{I}$ consists only of isolated points.

5.1.2 The procedure `zeroreduct`

As we saw in Example 5.3 it may happen that some real isolated points do not refer to any zero-dimensional component of $\sqrt[re]{I}$. Due to this fact we do not know how to

compute $V_{Iso}(I)$ from the given input I. We will see that it suffices to compute an ideal J of dimension at most zero satisfying $I \subseteq J \subseteq I_{Iso}$. This section describes an algorithm how to compute J.

Therefore let I be a radical ideal in $F[x_1, \ldots, x_n]$ and $I^{(d)} = \langle f_1, \ldots, f_r \rangle$ for $d \in \{0, \ldots, n-1\}$ its d-dimensional part, i.e. the intersection of all d-dimensional minimal primes of I. As $I^{(d)}$ is equi-dimensional the Jacobian criterion yields that

$$V_{Sing}(I^{(d)}) = V_{\overline{F}}(Jac(I^{(d)}, n-d)) \text{ and}$$
$$I^{(d)}_{Sing} = \sqrt{Jac(I^{(d)}, n-d)}$$

where $Jac(I^{(d)}, n-d)$ is the ideal generated by $I^{(d)}$ and all $(n-d) \times (n-d)$-minors of the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_i}\right)_{i,j}$ in $F[x_1, \ldots, x_n]$. Note that by Krull's principal ideal theorem (see e.g. [GP02] Theorem 5.6.8), $n - d \leq r$ holds. Iterating the following corollary it is possible to compute the desired ideal J.

Corollary 5.10
Let $I \trianglelefteq F[x_1, \ldots, x_n]$ be a radical ideal of dimension $d \in \{1, \ldots, n-1\}$ and $I = \bigcap_{e=0}^{d} I^{(e)}$ its equi-dimensional decomposition. Then the ideal $J := (\bigcap_{e=0}^{d-1} I^{(e)}) \cap I^{(d)}_{Sing}$ has the following properties:

(a) $I \subset J$ and $\dim J < d$

(b) $V_{Iso}(I) \subset V_{Iso}(J)$

(c) $J_{Iso} \subset I_{Iso}$

Proof
Ad (a): From [Har77] Theorem 5.3 we conclude that $V_{Sing}(I^{(d)})$ is a proper closed subset of $V(I^{(d)})$. As this theorem also holds for every irreducible component of $V(I^{(d)})$ we conclude that $\dim V_{Sing}(I^{(d)}) < d$, thus $\dim J < d$. The inclusion $I \subset J$ is clear.

Ad (b):

$$\begin{aligned}
\text{Let } x \in V_{Iso}(I) & \\
&\subseteq (\bigcup_{e=0}^{d-1} V_{\overline{F}}(I^{(e)})) \cup V_{Iso}(I^{(d)}) \\
&\overset{5.7}{\subseteq} (\bigcup_{e=0}^{d-1} V_{\overline{F}}(I^{(e)})) \cup V_{Sing}(I^{(d)}) \\
&= V_{\overline{F}}((\bigcap_{e=0}^{d-1} I^{(e)}) \cap I^{(d)}_{Sing}) \\
&= V_{\overline{F}}(J).
\end{aligned}$$

The fact that x is isolated in $V_R(I)$ yields that x is isolated in $V_R(J)$ as $V_R(J) \subset V_R(I)$ by the Real Nullstellensatz B.14.

Ad (c): Clear from the Real Nullstellensatz. ∎

Iterating Corollary 5.10 we get the following corollary.

Corollary 5.11
Let $I \trianglelefteq F[x_1, \ldots, x_n]$. Then there exists an algorithm to compute an ideal J such that $\dim J \leq 0$ *and* $I \subseteq J \subseteq I_{Iso}$.

Before I state the algorithm let me remark two important things: First, if I is already of dimension less than equal or zero every point of I is isolated, hence $I = I_{Iso}$. The second thing is that computing the radical of I may cost a lot of time. This is why I iterate Corollary 5.10 for the ideal I and not for $\sqrt{I}$.
As Hilbert's Nullstellensatz describes the variety of an ideal to be the same as for its radical we know that $V_{Sing}(I) = V_{Sing}(\sqrt{I})$. For the problem of the equi-dimensional decomposition we get the same phenomenon, i.e. $\sqrt{I^{(e)}} = (\sqrt{I})^{(e)}$ for every equi-dimensional part and hence $V_{Sing}(I^{(e)}) = V_{Sing}((\sqrt{I})^{(e)})$ for every e. The only time we have to compute radicals is to compute $I^{(d)}_{Sing}$, which is by definition a radical ideal.

To finish this proof let me state the procedure `zeroreduct` to get this ideal.

```
static proc zeroreduct(ideal i)
"USAGE:zeroreduct(i), i an arbitrary ideal
RETURN: an ideal j of dimension <=0 s.th. i is contained in
        j and j is contained in i_{Iso} which is the Zariski closure
        of all real isolated points of i
"
```

```
{
 list equi;
 int d,n,di;
 n=nvars(basering);
 def r=basering;

 //change ring to get faster Groebner bases computation for dimensions

 string rneu="ring neu=("+charstr(r)+"),("+varstr(r)+"),dp;";
 execute(rneu);
 ideal i=imap(r,i);

 i=Groebner(i);
 while (dim(i)> 0)
 {
   equi=equidim(i);
   d=size(equi);
   di=dim(equi[d]);

   //to compute the singular locus
   //of the top dimensional part
   equi[d]=radical(equi[d]);

   equi[d]=equi[d],minor(jacob(equi[d]),n-di);
   equi[d]=radical(equi[d]);
   i=intersect(equi[1..d]);
   i=Groebner(i);
 }

 setring r;
 i=imap(neu,i);
 i=timeStd(i,301);
 return(i);
}
```

To finish this subsection, let us consider 2 examples:

Example 5.12

1. *Let* $I = \langle y^2 - x^2 \cdot (x-1) \rangle \cap \langle x+1, y \rangle$ *from Example 5.3. Then* I *is already equidimensionally decomposed with* $I^{(1)} = \langle y^2 - x^2 \cdot (x-1) \rangle$ *and* $I^{(0)} = \langle x+1, y \rangle$. $I^{(1)}_{Sing} = \langle y^2 - x^2 \cdot (x-1), 2y, -3x^2 + 2x \rangle = \langle x, y \rangle$ *which has dimension 0. Hence*

$$J = I^{(1)}_{Sing} \cap I^{(0)} = \langle x, y \rangle \cap \langle x+1, y \rangle$$

which was just I_{Iso} *by Example 5.3.*

2. *As a simple example to see that the zero-dimensional part of the singular locus of an ideal can be larger than the locus of isolated points we could consider the cuspidial curve* $y^2 - x^3 = 0$. *Here the procedure zeroreduct acts in the same way as in the example above and we get* $J = \langle x, y\rangle$ *but* $(0,0)$ *is no isolated point in the cusp as this curve contains no isolated points.*

5.2 The theory of higher dimensional computation

The main theorem for the higher dimensional computation, adapted from [BN98] Theorem 4.5., is:

Theorem 5.13
Let $I \trianglelefteq F[x_1, \ldots, x_n]$. *For any* $S \subsetneq \{x_1, \ldots, x_n\}$ *let* $J^{(S)}$ *denote an ideal of the quotient ring* $F[x_1, \ldots, x_n] \cdot F(S)$ *satisfying* $\dim J^{(S)} \leq 0$ *and* $I \cdot F(S) \subseteq J^{(S)} \subseteq (I \cdot F(S))_{Iso}$. *Then*

$$\sqrt[re]{I} = \bigcap_{S \subsetneq \{x_1,\ldots,x_n\}} (\sqrt[re]{J^{(S)}} \cap F[x_1, \ldots, x_n])$$

Proof
$\subseteq$ For any subset $S \subsetneq \{x_1, \ldots, x_n\}$ we have

$$\begin{aligned}\sqrt[re]{I} &\subseteq (\sqrt[re]{I} \cdot F(S)) \cap F[x_1, \ldots, x_n]) \\ &= \sqrt[re]{I \cdot F(S)} \cap F[x_1, \ldots, x_n] \\ &\subseteq \sqrt[re]{J^{(S)}} \cap F[x_1, \ldots, x_n]\end{aligned}$$

$\supseteq$ $\sqrt[re]{I}$ is a radical ideal. So it suffices to prove that $\bigcap_{S \subsetneq \{x_1,\ldots,x_n\}} (\sqrt[re]{J^{(S)}} \cap F[x_1, \ldots, x_n])$ is contained in any minimal prime P of $\sqrt[re]{I}$.:
Let S_0 be a maximal subset of $\{x_1, \ldots, x_n\}$ independent modulo P (see [GP02] Definition 3.5.3) and $T := K[S_0] \backslash \{0\}$. Then P_T is a zero-dimensional component of $(\sqrt[re]{I})_T = \sqrt[re]{I_T}$. Thus we conclude using Proposition 5.2 (which says that every real zero-dimensional component of I_T contains $(I_T)_{Iso}$) that

$$\begin{aligned}\bigcap_{S \subset \{x_1,\ldots,x_n\}} (\sqrt[re]{J^{(S)}} \cap F[x_1, \ldots, x_n]) &\subseteq \sqrt[re]{J^{(S_0)}} \cap F[x_1, \ldots, x_n] \\ &\subseteq \sqrt[re]{(I_T)_{Iso}} \cap F[x_1, \ldots, x_n] \\ &\subseteq \sqrt[re]{P_T} \cap F[x_1, \ldots, x_n] = \sqrt[re]{P_T^c} = P_T^c = P \blacksquare\end{aligned}$$

To compute the real radical of an arbitrary dimensional ideal we have to solve the following problem:
Given a zero-dimensional radical ideal $\overline{J}$ in $F(z_1,\ldots,z_r)[x_1,\ldots,x_n]$, compute the intersection ideal $J := J^c = \overline{J} \cap F[x_1,\ldots,x_n]$. We name this problem **special radical contraction problem** as $\overline{J} = J \cdot F(z_1,\ldots,z_r)[x_1,\ldots,x_n]$ is just the extension of J. Hence our aim is to compute $\overline{J}^c$.

5.2.1 A solution to the special radical contraction problem

Let $\overline{J} = \langle f_1,\ldots,f_k\rangle \trianglelefteq F(z_1,\ldots,z_r)[x_1,\ldots,x_n]$ be a zero- dimensional radical ideal. We can assume without loss of generality (via multiplication with suitable polynomials $h \in F[z_1,\ldots,z_r]$) that every $f_i \in (F[z_1,\ldots,z_r])[x_1,\ldots,x_n]$ and has content 1.
The following proposition gives my solution to the contraction problem.

Proposition 5.14
Let $\overline{J} \trianglelefteq F(z_1,\ldots,z_r)[x_1,\ldots,x_n]$ be given as above and let

$$K := \langle f_1,\ldots f_k\rangle \trianglelefteq F[z_1,\ldots,z_r,x_1,\ldots,x_n]$$

be the ideal generated by the f_i considered as polynomials in $F[z_1,\ldots,z_r,x_1,\ldots,x_n]$. Then:

a) If K is a prime ideal, then $K = J := \overline{J} \cap F[z_1,\ldots,z_r,x_1,\ldots,x_n]$.

b) Let $K = \bigcap_{i=1}^{l} Q_i$ be the minimal primary decomposition of K. Let

$$\Gamma := \{Q_i : Q_i \cdot F(z_1,\ldots,z_r)[x_1,\ldots,x_n] \neq F(z_1,\ldots,z_r)[x_1,\ldots,x_n]\}.$$

Then

$$\begin{aligned} K' :&= \overline{J} \cap F[z_1,\ldots,z_r,x_1,\ldots,x_n] \\ &= \bigcap_{Q_i \in \Gamma} Q_i. = J \end{aligned}$$

Proof
Ad a) $K \subset J = \overline{J} \cap F[z_1,\ldots,z_r,x_1,\ldots,x_n]$ is clear. Now let $f \in J$, then $f \in \overline{J}$ considered as polynomial over $F(z_1,\ldots,z_r)[x_1,\ldots,x_n]$. Hence there exists a $F(z_1,\ldots,z_r)$-linear combination of the f_i to get our f, say

$$f = \sum_{i=1}^{k} a_i f_i \ (*),$$

where every $a_i \in F(z_1, \ldots z_r)[x_1, \ldots, x_n]$. Multiplying all denominators we get a polynomial $g \in F[z_1, \ldots, z_r]$ such that $g \cdot a_i \in F[z_1, \ldots, z_r, x_1, \ldots, x_n]$ for every i. Thus the equality $(*)$ changes to:

$$g \cdot f = \sum_{i=1}^{k} (g \cdot a_i) f_i \ (**).$$

From $(**)$ we conclude that $g \cdot f \in K$, but then $g \in K$ or $f \in K$.r
Assume $g \in K$. Then $g \in \overline{J}$ but g is a unit in $F(z_1, \ldots, z_r)$. Thus $1 \in \overline{J}$ which is a contradiction to the assumption. So we finally get the desired $J \subset K$.

Ad b) Again $K' \subset J$ is clear. Now let $f \in J$. As

$$\overline{J} = J \cdot F(z_1, \ldots, z_r)[x_1, \ldots, x_n] \neq F(z_1, \ldots, z_r)[x_1, \ldots, x_n]$$

we conclude that f is no polynomial in $F[z_1, \ldots, z_r]$. Since $\overline{J}$ is radical we see that every primary component Q_i satisfying

$$Q_i \cdot F(z_1, \ldots, z_r)[x_1, \ldots, x_n] \neq F(z_1, \ldots, z_r)[x_1, \ldots, x_n]$$

is already prime. Now

$$\begin{aligned}
f \in J &= \overline{J} \cap F[z_1, \ldots, z_r, x_1, \ldots, x_n] \\
&= (K \cdot F(z_1, \ldots, z_r)[x_1, \ldots, x_n]) \cap F[z_1, \ldots, z_n, x_1, \ldots, x_n] \\
&= [(\bigcap_{i=1}^{l} Q_i) F(z_1, \ldots, z_r)[x_1, \ldots, x_n]] \cap F[z_1, \ldots . z_r, x_1, \ldots, x_n] \\
&\subseteq [\bigcap_{i=1}^{l} (Q_i \cdot F(z_1, \ldots, z_r)[x_1, \ldots, x_n])] \cap F[z_1, \ldots, z_r, x_1, \ldots, x_n] \\
&= [\bigcap_{Q_i \in \Gamma} Q_i \cdot F(z_1, \ldots, z_r)[x_1, \ldots, x_n]] \cap F[z_1, \ldots, z_r, x_1, \ldots, x_n] \\
&= \bigcap_{Q_i \in \Gamma} (Q_i \cdot F(z_1, \ldots, z_r)[x_1, \ldots, x_n] \cap F[z_1, \ldots, z_r, x_1, \ldots, x_n]) \\
&\overset{a)}{=} \bigcap_{Q_i \in \Gamma} Q_i = K'
\end{aligned}$$

Hence $J \subseteq K'$ and we conclude that $J = K'$ ∎

Proposition 5.14 describes in detail an algorithm to intersect the zero-dimensional real radical of $J^{(S)}$ with the ground ring $F[x_1, \ldots, x_n]$.
I implemented this procedure in Singular and named it `contnonloc` for the contraction of J^e to the non-local ground ring $F[x_1, \ldots, x_n]$. It gets as input 3 parameters:

- the ideal $J \lhd F[z_1, \ldots, z_r, x_1, \ldots, x_n]$ described above,
- a string of parameters which consists of all the z_i and
- a string of variables which are all the x_i.

Then it computes the primary decomposition of the ideal K and computes the desired $J = K'$ using Proposition 5.14 b).
Finally, let us consider two examples:

Example 5.15
a) Let $\overline{J} = \langle y^2 - x^3 \rangle \trianglelefteq Q(x)[y]$. As $y^2 - x^3 \in \mathbb{Q}[x, y]$ is prime, we get by Proposition 5.14 a) that $J = \langle y^2 - x^3 \rangle$.

b) Let $\overline{J} = \langle x^3z^2 + z, x^2y + z \rangle \trianglelefteq \mathbb{Q}(x)[y, z]$ be given. We want to compute J. Set $K = \langle x^3z^2 + x^2y, x^2y + z \rangle$. Then $K = Q_1 \cap Q_2 \cap Q_3$ where

- *$Q_1 = \langle y^3 + z^5, xz^2 - y, xy^2 - z^3, x^2y + z, x^3z + 1 \rangle = P_1$ is prime and in Γ.*
- *$Q_2 = \langle y, z \rangle = P_2$ is prime and in Γ-*
- *$Q_3 = \langle x^2, z \rangle$ where its minimal prime $P_3 = \langle x, z \rangle$ is not in Γ.*

By the aid of Proposition 5.14 we get that $J = K' = P_1 \cap P_2$. Hence

$$J := \overline{J} \cap \mathbb{Q}[x, y, z] = \langle y^3 + z^5, xz^2 - y, xy^2 + z^3, z^2y + z \rangle.$$

5.2.2 The algorithm to compute the real radical of polynomial ideals I over $\mathbb{Q}(x_1, \ldots, x_n)$

With all the machinery prepared in the last chapters and sections, we are now able to compute the real radical of an arbitrary polynomial ideal $J \trianglelefteq F[x_1, \ldots, x_n]$.
The idea how to compute this was presented in Theorem 5.13. What we should do again is to simplify the input using Remark 4.16. This simplification removes some non-real zero-dimensional components . All other simplifications are hidden in the child algorithms `zeroreduct, RealZero, contnonloc`.
To describe an algorithm we need a procedure to compute the power set of $\{1, \ldots, n\}$. Recall that this has the cardinality 2^n. If we now write every number r between 0 and $2^n - 1$ in its binary representation, this r refers bijective to exactly one subset $\{j_1, \ldots, j_k\}$ by the equality

$$r = \sum_{i=1}^{k} 2^{j_i - 1}.$$

Note that the sum of nothing is 0.

Example 5.16
Enumerate every subset of $\{1,2,3\}$. *There are 8 subsets: As an example the number 5 is* 2^0+2^2, *hence* $j_1=1$ *and* $j_2=3$. *Thus 5 refers to* $\{1,3\}$. *0 always refers to the empty set.*

In Singular I describe all my sets as lists. To avoid the problem with the empty list I decided only to compute every non-empty subset. On these subsets we can localize as described in Theorem 5.13.
Obviously we obtain the following procedure:

```
static proc subset(int n)
"USAGE :subset(n); n>=1 in Z
RETURN :l a list of all non-empty subsets of {1,..,n}
EXAMPLE:subset(n) shows an example;
"
{
 list l,buffer;
 int i,j,binzahl;
 if (n<=0)
 {
   return(l);
 }
 int grenze=int(exp(2,n))-1;//computes 2^n-1
 for (i=1;i<=grenze;i++)
 {
  binzahl=i;
  for (j=1;j<=n;j++)
  {
   if ((binzahl mod 2)==1)
   {
     buffer=buffer+list(j);
   }
   binzahl=binzahl div 2;
  }
  l[i]=buffer;
  buffer=list();
 }
 return(l);
}
example
{ "EXAMPLE:"; echo = 2;
```

```
  subset(3);
  subset(4);
}
```

Now with all these procedures it is not difficult to write the final algorithm and to finish my Diplomarbeit. Here I state my final procedure in pseudo-code. In Singular it has the tag `real`:

Algorithm 5.1
proc $real(I)$

INPUT : an ideal $I \trianglelefteq \mathbb{Q}[x_1, \ldots, x_n]$

OUTPUT: an ideal J *with* $J = \sqrt[re]{I}$

Compute the subsets S_I *of* $\{x_1, \ldots, x_n\}$.

Compute the zero-dimensional ideals $J^{(S_i)} \trianglelefteq \mathbb{Q}(S_i)[\{x_1, \ldots, x_n\} \setminus S_i]$ *for every* i *using the procedure* ***zeroreduct****.*

Compute the real radicals $\sqrt[re]{J^{(S_i)}}$ *of the* $J^{(S_i)}$ *as described in Chapter 4.*

Use the procedure `contnonloc` *and set*

$$J := \bigcap_{S \subsetneq \{x_1,\ldots,x_n\}} (\sqrt[re]{J^{(S)}} \cap F[x_1, \ldots, x_n]).$$

Considering Theorem 5.13 return J.

To conclude this chapter let us consider 2 examples:

Example 5.17

1. *Let* $I = \langle y^2 - x^2 \cdot (x-1)\rangle \cap \langle x+1, y\rangle \trianglelefteq \mathbb{Q}[x, y]$ *from example 5.3. Then* $I^{(1)} = \langle y^2 - x^2 \cdot (x-1)\rangle$ *and* $I^{(0)} = \langle x+1, y\rangle$ *are both real, hence* I *is real. Let us compute the real radical with the aid of Proposition 5.13.*
   The subsets are $S_0 = \varnothing, S_1 = \{x\}, S_2 = \{y\}$.

   a) $I \cdot \mathbb{Q}(S_0) = I$ *and the zero reduction of* I *is* $J^{(S_0)} = \langle x, y\rangle \cap \langle x+1, y\rangle$ *as we computed in Example 5.12.1.* $J^{(S_0)}$ *is already real.*

   b) $I \cdot \mathbb{Q}(S_1) = I \cdot \mathbb{Q}[x] = \langle y^2 - x^2 \cdot (x-1)\rangle \cap \langle x+1, y\rangle = \langle y^2 - x^2 \cdot (x-1)\rangle \trianglelefteq \mathbb{Q}(x)[y]$. $I \cdot \mathbb{Q}(x)$ *is already zero-dimensional. Thus we only have to compute its real radical. As* $y^2 - x^2 \cdot (x-1)$ *is indefinite by Lemma 3.28 we conclude that*

$$J^{(S_1)} = \langle y^2 - x^2 \cdot (x-1)\rangle \in \mathbb{Q}(x)[y_1, y_2, \ldots, y_m]$$

is real and thus $\langle y^2 - x^2 \cdot (x-1)\rangle \in \mathbb{Q}[x,y]$ *is real as it is prime (see Proposition 5.14).*

c) See b).

Hence $\sqrt[re]{I} = (\langle x, y\rangle \cap \langle x+1, y\rangle) \cap \langle y^2 - x^2 \cdot (-1)\rangle = I$

2. *Let*

$$I = \langle x^6y^2z^4 - 2x^5y^3z^2 + x^4y^4 + 2x^4z^5 - 4x^3y^2z^3 + 2x^2y^3z + x^2z^6 - 2xyz^4 + y^2z^2\rangle$$

Now there are seven subsets on which we can localize. They are: $S_0 = \varnothing, S_1 = \{x\}, S_2 = \{y\}, S_3 = \{x,y\}, S_4 = \{z\}, S_5 = \{x,z\}, S_6 = \{y,z\}$.

a) $J^{(S_0)} = \texttt{zeroreduct}(I) = \langle 1\rangle \trianglelefteq \mathbb{Q}[x,y,z]$. *Hence*

$$(\sqrt[re]{J^{(S_0)}}) \cap \mathbb{Q}[x,y,z] = \langle 1\rangle$$

b) $J^{(S_1)} = \langle x^3z^2 + z, x^2y + z\rangle \lhd \mathbb{Q}(x)[y,z]$ *which is already real. From Example 5.15 b) we get that*

$$J_1 := (\sqrt[re]{J^{(S_1)}}) \cap \mathbb{Q}[x,y,z] = \langle y^3 + z^5, xz^2 - y, xy^2 + z^3.x^2y + z\rangle.$$

I only state the last 5 ideals.

c) $J_2 := (\sqrt[re]{J^{(S_2)}}) \cap \mathbb{Q}[x,y,z] = \langle xz^2 - y, xy^2 + z^3, x^2y + z, x^3z + 1, z^5 + y^3\rangle$

d) $J_3 := (\sqrt[re]{J^{(S_3)}}) \cap \mathbb{Q}[x,y,z] = \langle x^3yz^2 - x^2y^2 + xz^3 - yz\rangle$

e) $(\sqrt[re]{J^{(S_4)}}) \cap \mathbb{Q}[x,y,z] = J_2$

f) $(\sqrt[re]{J^{(S_5)}}) \cap \mathbb{Q}[x,y,z] = (\sqrt[re]{J^{(S_6)}}) \cap \mathbb{Q}[x,y,z] = J_3$

Finally we get that

$$\begin{aligned}\sqrt[re]{I} &= J_1 \cap J_2 \cap J_3 = J_3 \\ &= \langle x^3yz^2 - x^2y^2 + xz^3 - yz\rangle.\end{aligned}$$

A General concepts and basic definitions of real algebra

To explain an algorithm in $\mathbb{Q}(y_1, y_2, \ldots, y_m)$ we need some more information about real algebra, real fields and τ-real ideals. For more details see [KS89] and [BCR98].

A.1 Ordered fields and their real closures

A.1.1 Orderings and pre-orderings of fields

From now on let K denote an arbitrary field, i.e. K need not necessarily be a subfield of $\mathbb{R}$.

Definition A.1
An ordering of K is a subset $\tau \subset K$ with

(1) $\tau + \tau \subseteq \tau$ *and* $\tau \cdot \tau \subseteq \tau$

(2) $\tau \cap (-\tau) = \{0\}$

(3) $\tau \cup (-\tau) = K$.

The pair (K, τ) is called an ordered field.

Notation A.2

1. *If* (1) *and* (3) *are assumed, then* (2) *is equivalent to*

   (2') $-1 \notin \tau$.

2. *If τ is an ordering of K. Then the convention $a \leq b \iff b - a \in \tau$ gives a total ordering on K with*

   (i) $a \leq b \implies a + c \leq b + c$ *and*

(ii) $a \leq b,\ c \geq 0 \implies ac \leq bc\ \forall a, b, c \in K$

Conversely every total ordering $\leq$ *which satisfies* (i) *and* (ii) *defines an ordering* τ *via its positive hull*

$$\tau := \{a \in K\ :\ a \geq 0\}.$$

As these constructions are inverse to each other. We call total orderings satisfying (i) *and* (ii) *simply orderings, too.*

Definition A.3
A pre-ordering of K *is a subset* $\sigma \subset K$*, with*

(1) $\sigma + \sigma \subset \sigma$ *and* $\sigma \cdot \sigma \subset \sigma$

(2) $\sigma \cap (-\sigma) = \{0\}$

(4) $K^2 \subseteq \sigma$*, i.e.* $a^2 \in \sigma$ *for all* $a \in K$

Remark A.4

1. *Again assuming* (1) *and* (4) *property* (2) *is equivalent to*

   (2') $-1 \notin \sigma$

2. *Every ordering is a pre-ordering, since* (3) *implies* (4).

3. *If* σ *is a pre-ordering of* K*, then* $a \leq b \iff b - a \in \sigma$ $(a, b \in K)$ *defines a partial ordering which is compatible with the field axioms.*

4. *Let* $\Sigma = \{\sigma_\alpha\ :\ \alpha \in I\}$ *be a non-empty family of pre-orderings of* K*. Then*

   i. $\bigcap\limits_\alpha \sigma_\alpha$ *is a pre-ordering.*

   ii. *If additionally* Σ *satisfies the condition that there exists* $\forall \alpha, \beta \in I$ *a* $\gamma \in I$ *s.th.* $\sigma_\alpha \cup \sigma_\beta \subset \sigma_\gamma$ *then* $\bigcup\limits_\alpha \sigma_\alpha$ *is a pre-ordering.*

In particular, if K has a pre-ordering, then there exists a minimal one. This is denoted by $re := \sum K^2$, with $\sum K^2 := \{a_1^2 + a_2^2 + \ldots + a_n^2\ :\ n \in \mathbb{N},\ a_1, a_2, \ldots, a_n \in K\}$.
It's clear that $\sum K^2 \subseteq \sigma$ for every pre-ordering σ of K, but $\sum K^2$ is a pre-ordering iff $-1 \notin \sum K^2$.

Definition A.5
The field K *is called* **formally real** *if* -1 *is no sum of squares, i.e. if* $-1 \notin \sum K^2$.

We see that every field K admits a pre-ordering iff K is formally real.
In this case $\sum K^2$ is its minimal pre-ordering. Note that every formally real field has characteristic 0. If char $K = p$ we would have $-1 = (p-1) \cdot 1^2$. So it is not possible to order finite fields.

Let us see that every pre-ordering is the intersection of several orderings.

Lemma A.6
Let σ be a pre-ordering of K and let $a \in K \setminus \sigma$. Then

1. *$\sigma[a] := \sigma - a\sigma = \{b - ac \ : \ b, c \in \sigma\}$ is a pre-ordering of K,*

2. *there exists an ordering τ of K such that $\sigma \subset \tau$.*

Proof
Ad 1. The properties (1) and (4) are clear for $\sigma[a]$. Let us show (2′):
Suppose $-1 \in \sigma[a]$, i.e. $-1 = b - ac$ with $b, c \in \sigma$. Then $c \neq 0$ and $a = c^{-2} \cdot c \cdot (1 + b) \in \sigma$, which is a contradiction.

Ad 2. Let $M_\sigma := \{\sigma' : \sigma' \text{ is a preordering, } \sigma \subset \sigma'\}$. M_σ is partially ordered by inclusion and $\sigma \in M_\sigma$ so by Zorn's Lemma and Remark A.4 3. there exits a maximal pre-ordering $\tau \in M$. This τ has to be an ordering of K, because if $a \notin \tau$, then $\tau[a] = \tau$ due to the maximality of τ, so $-a \in \tau$. ∎

Theorem A.7
Every pre-ordering σ is the intersection of orderings of K.

Proof
$\sigma \subseteq \bigcap\{\tau : \tau \text{ is an ordering of } K \text{ and } \sigma \subset \tau\}$ is trivial. Let $a \in K \setminus \sigma$ be arbitrary, then $\sigma[a]$ is a pre-ordering by the previous lemma. Hence there exists an ordering τ with $\sigma \subset \sigma[a] \subset \tau$. Since $-a \in \tau$ and $a \neq 0$, it follows that $a \notin \tau$. Thus

$$\sigma = \bigcap\{\tau : \tau \text{ is an ordering of } K \text{ and } \sigma \subset \tau\}$$

∎

Definition A.8
For any formally real field K the set of all orderings is denoted by $X(K)$.

Corollary A.9
K has an ordering iff K is formally real.

Corollary A.10 (E. Artin)
Let char $K \neq 2$ and $a \in K$. a is non-negative w.r.t. every ordering of K iff a is the sum of squares in K.

PROOF
If K is formally real, then $\sum K^2$ is a pre-ordering of K. Here theorem A.7 leads to the assertion. If K is not formally real, then $\sum K^2 = K$ as for every $a \in K$

$$a = (\frac{a+1}{2})^2 + (-1) \cdot (\frac{a-1}{2})^2.$$

■

Example A.11

1. *The field of real numbers and hence every subfield has only the ordering which was introduced in school.*

2. *Let $\mathbb{Q}(t)$ be the function field in one variable over $\mathbb{Q}$, $\vartheta \in \mathbb{R}$ a transcendent number over $\mathbb{Q}$. Then $f(\vartheta)$ is a well-defined real number for every $f \in \mathbb{Q}(t)$ and the subset*

$$\tau := \{f \in \mathbb{Q}(t) \ : \ f(\vartheta) \geq 0\}$$

is an ordering of $\mathbb{Q}(t)$. This ordering is induced by the field embedding

$$\begin{aligned} \mathbb{Q}(t) &\hookrightarrow \mathbb{R} \\ f &\mapsto f(\vartheta) \end{aligned}$$

3. *Let $(F, \leq)$ be an ordered field, $F(t)$ the rational function field in one variable over F. For every $a \in F$ we define*

$$\begin{aligned} P_{a,+} &:= \{0\} \cup \{(t-a)^r \cdot f(t) \ : \ r \in \mathbb{Z}, f \in F(t) \text{ with } f(a) \neq \infty \text{ and } f(a) > 0\} \\ P_{a,-} &:= \{0\} \cup \{(a-t)^r \cdot f(t) \ : \ r \in \mathbb{Z}, f \in F(t) \text{ with } f(a) \neq \infty \text{ and } f(a) > 0\} \end{aligned}$$

which are both orderings of $F(t)$. Both orderings extend the ordering $\leq$ of F.

Notation A.12
Let (K, τ) be an ordered field, we define:

1. *$sign_\tau : K \to \{-1, 0, 1\}$ with $sign_\tau(0) = 0$ and if $a \neq 0$ $sign_\tau(a) = 1$ if $a \in \tau$, else $sign_\tau(a) = -1$*

2. *The absolute value $|\cdot|_\tau$ w.r.t. τ is defined as $|a|_\tau = a \cdot sign_\tau(a)$.*

3. *The generalized intervals $[a, b]_\tau, [a, b[_\tau .]a, b]_\tau,]a, b[_\tau$ are defined in the obvious way.*

4. *∞ and $-\infty$ are clear from definition of τ, too.*

A.2 Real closed fields and the real closure

A.2.1 Real closed fields

Definition A.13
A **real closed field** *R is a formally real field with the following properties*

(i) *R^2 is the unique ordering of R*

(ii) *every polynomial $F \in R[x]$ of odd degree has a root in R*

Note, that (ii) is a generalization of the fundamental theorem of algebra over $\mathbb{R}$ and that $\mathbb{R}$ is real closed.
We can imagine real closed fields as $\mathbb{R}$-like fields. These fields have common properties with the real numbers. Let me state some basic theorems about real closed fields and their properties:

Theorem A.14
A formally real field R is real closed iff $R[i] = R[t]/\langle t^2+1\rangle$ is algebraically closed.

Proof
$\Rightarrow$ The same proof as for $\mathbb{C} = \mathbb{R}[i]$ is the algebraic closure of $\mathbb{R}$

$\Leftarrow$ The only thing we have to show is that R^2 is an ordering of R.

To (1) Let $a^2, b^2 \in R^2$, then $(ab)^2 = a^2 \cdot b^2 \in R^2$. As $R[i]$ is the algebraic closure of R, there exist $c, d \in R$ such that $a+ib = (c+id)^2$ (clearly $a-ib = \overline{a+ib} = (c-id)^2$), but then $a^2+b^2 = (c^2+d^2)^2 \in R^2$.

To (2') As R is not algebraically closed and $R[i]$ is its algebraic closure, $-1 \notin R^2$.

To (4) Let $a \in R$. Then $x^2 - a$ has a root $c + id \in R[i]$. Then

$$a = (c+id)^2 = (c^2 - d^2) + 2icd,$$

hence $cd = 0$.

Let $a \neq 0$. The case $c = 0$ yields that $a \in -R^2$ and $a = -d^2 \notin R^2$, the case $d = 0$ that $a = c^2 \in R^2$, but not in $-R^2$. So $R = R^2 \cup (-R^2)$. ∎

Another property of real closed fields is that ring endomorphisms $\varphi : R \to R$ don't change the ordering.

Theorem A.15
Let R be a real closed field.

a) For every (ring) endomorphism $\varphi : R \to R$, $a \leq b \implies \varphi(a) \leq \varphi(b)$ for all $a, b \in R$

b) If $K \lhd R$ is a subfield and $R : K$ is algebraic, then the identity map is the only K-automorphism of R.

Proof
Ad a) follows directly from $R^2 = \{a \in R : a \geq 0\}$.

Ad b) Let $\varphi \in Aut_K(R)$ and $a \in R$. As $[R : K]$ is algebraic, $\{\varphi^n(a) : n \in \mathbb{N}\}$ is a finite set. Suppose $\varphi(a) \neq a$, wlog $a < \varphi(a)$, then a) would inductively yield $a < \varphi(a) < \varphi^2(a) < \cdots$, which is a contradiction. ∎

Theorem A.16 (Sturm's Theorem)
Let R be a real closed field and $f \in R[x]$. Let $a, b \in R$ be such that $a < b$ and neither a nor b are roots of f. Then the number of roots of F in the interval $[a, b]$ is equal to $v_f(a) - v_f(b)$.

We can choose the same constant M for a polynomial as in Chapter 2 for the univariate case for of polynomials $f \in \mathbb{Q}[x]$.

A.2.2 The Real Closure

Definition A.17
An algebraic extension R of an pre-ordered field (F, σ) is called a **real closure** *of F if R is real closed and its unique ordering extends the pre-ordering of F, i.e. $\sigma \subseteq R^2 \cap F$.*

A very useful theorem which is hard to proof is the existence of a unique real closure for ordered fields.

Theorem A.18
Every ordered field (K, τ) admits a unique real closure R_τ.

Definition A.19
Let R be a real closed field. If ϵ is a variable, one denotes by $R\langle\epsilon\rangle$ the field of Puisseux series in ϵ with coefficients in R. Its elements are the series of the form

$$\sum_{i \geq i_0,\ i \in \mathbb{Z}} a_i \epsilon^{\frac{i}{q}}$$

with $i_0 \in \mathbb{Z}, a_i \in R, q \in \mathbb{N} \setminus \{0\}$. .

The field $R\langle\epsilon\rangle$ is real closed and its positive elements are Puisseux series $\sum_{i=k}^{+\infty} a_i \epsilon^{\frac{i}{q}}$ with $a_k > 0$, i.e. a series is positive iff the lowest degree leading term is positive in R.

Example A.20

1. *The field of real algebraic numbers* $\mathbb{R}_{alg} = \overline{\mathbb{Q}} \cap \mathbb{R}$ *is the real closure of* $\mathbb{Q}$.

2. *Consider the field* $\mathbb{R}(t)$ *with the ordering* $\tau = P_{0,+}$ *(i.e.* $t > 0$ *and* $b \geq t$ *for all* $b \in \mathbb{R}$*, hence a polynomial* $f(t) = \frac{g(t)}{h(t)}$ *is non-negative if* $h(0) \neq 0$ *and* $g(0) \cdot h(0) \geq 0$*). So the ordering of* $\mathbb{R}\langle t\rangle$ *extends the ordering of* $\mathbb{R}(t)$ *and in fact, the field of Puisseux series* $\mathbb{R} < t >$ *is the real closure of* $\mathbb{R}(t)$

To finish this chapter I state one of the most important theorem on real closed fields, the so called **Tarski-Seidenberg principle**. It tells us that if for any closed field R a statement is true, it remains true in every real closed extension R' of R. (see [BPR03] Theorem 2.80)

Theorem A.21 (Tarski-Seidenberg principle)
Suppose that R' *is a real closed field containing the real closed field* R*. If* Φ *is a sentence in the language of ordered fields over* R *(i.e. a statement over* R *using the* $>, <, =, \text{sign}$ *tags). Then* Φ *is true in* R *iff it is true in* R'*.*

If we use this theorem, we can see e.g. that for the ordered field $\mathbb{Q}$ and its real closure $\mathbb{R}_{alg}$, which are contained in $\mathbb{R}$, every statement we have done over $\mathbb{R}_{alg}$ is true over $\mathbb{R}$.

This is the reason why every definition or theorem in my Diplomarbeit is written over $\mathbb{R}$ and not over $\mathbb{R}_{alg}$. Especially, this was very useful for the definition of being positive semi-definite or indefinite (see Lemma 3.1).

B τ-real ideals and the real radical

In this section, I define τ-radicals for pre-orderings σ of real fields K.

Definition B.1 (τ-radicals and the real radical)
Let K be a formally real field and τ a pre-ordering of K. For any K-algebra A, we define the τ-radical of an ideal $I \trianglelefteq A$ by

$$\sqrt[\tau]{I} = \{f \in A \ : \ f^{2r} + \sum_{i=1}^{m} a_i g_i^2 \in I \text{ with } r, m \in \mathbb{N}, g_i \in A \text{ and } a_i \in \tau \ \forall i\}.$$

An ideal I with the property $I = \sqrt[\tau]{I}$ is called τ-real.
If $\tau = \sum K^2 =: re$, then $\sqrt[re]{I}$ is called the real radical of I.

From this definition it is not clear that $\sqrt[\tau]{I}$ is an ideal. The only thing which is not obvious is that $\sqrt[\tau]{I}$ additive. Therefore let f and g be in $\sqrt[\tau]{I}$. We have to show that $f + g \in \sqrt[\tau]{I}$.

Proof
As $f, g \in \sqrt[\tau]{I}$ there exist $m, n \in \mathbb{N}$ and polynomials

$$a_1, \ldots, a_l, b_1, \ldots, b_r \in A,$$
$$l_1, \ldots, l_r, k_1, \ldots, k_r \in \tau$$

such that

$$f^{2m} + \sum_{i=1}^{l} l_i a_i^2 \in I$$
$$g^{2n} + \sum_{i=1}^{r} k_i b_i^2 \in I$$

Let wlog $m \geq n$. Set $\lambda = \sum_{i=1}^{l} l_i a_i^2$ and $\mu = g^{2(m-n)}(\sum_{i=1}^{r} k_i b_i^2)$ then:

$$f^{2m} + \lambda \in I \text{ and } g^{2m} + \mu \in I.$$

Now let us consider the sum $(f+g)^{4m}+(f-g)^{4m}$. By the aid of the binomial theorem we get:

$$\begin{aligned}(f+g)^{4m}+(f-g)^{2m} &= (\sum_{i=1}^{4m}\binom{4m}{i}f^i g^{4m-i})+(\sum_{i=1}^{4m}\binom{4m}{i}f^i(-g)^{4m-i}) \\ &= (\sum_{i=1}^{2m}\binom{4m}{2i}f^{2i}g^{2(2m-i)})\end{aligned}$$

Now set u as follows

$$u=\sum_{i=1}^{m} f^{2i}\cdot g^{2(m-i)}\mu+\sum_{i=1}^{2m}\lambda\cdot f^{2(i-m)}\cdot g^{2(2m-i)}$$

Hence u is the positive sum of squares and by the definition of u we conclude that

$$(f+g)^{4m}+(f-g)^{4m}+u\in I$$

and hence $f+g\in\sqrt[\tau]{I}$. So $\sqrt[\tau]{I}=\langle f\in A\ :\ f^{2r}+\sum_{i=1}^{m}a_i g_i^2\in I$ with $r,m\in\mathbb{N}, g_i\in A$ and $a_i\in\tau\ \forall i\rangle$ ∎

To see that this definition does not differ from the definition given in Chapter 1 for $K=\mathbb{Q}$ we prove the following lemma:

Lemma B.2
Let $K=\mathbb{Q}$, $re=\sum K^2=K_{\geq 0}$ is an ordering of K.

Proof
$\sum\mathbb{Q}^2\subseteq\mathbb{Q}_{\geq 0}$ is clear.

Let $\frac{p}{q}\in\mathbb{Q}_{>0}$. Then

$$\frac{p}{q}=\frac{pq}{q^2}=\sum_{i=1}^{pq}(\frac{1}{q})^2\in\sum\mathbb{Q}^2.$$

∎

Hence $\mathbb{Q}$ has a unique real closure and this closure is $\mathbb{R}_{alg}:=\overline{\mathbb{Q}}\cap\mathbb{R}$, so we get the following corollary.

Corollary B.3
For every algebraic extension K of $\mathbb{Q}$ which is in $\mathbb{R}$ there exists only one possible ordering, i.e. $\sum K^2=K_{\geq 0}$.

B.1 Some properties of the $\sqrt[\tau]{}$-functor

The $\sqrt[\tau]{}$-functor has the following properties (cf. [BN98] Chapter 2).

Theorem B.4
Let (K,τ) be a pre-ordered field, I, J ideals in some K-algebra A and S a multiplicative closed subset of A satisfying $1 \in S$ and $0 \notin S$. Then we have:

(a) $\sqrt[\tau]{I \cap J} = \sqrt[\tau]{I} \cap \sqrt[\tau]{J}$

(b) $\sqrt[\tau]{I_S} = (\sqrt[\tau]{I})_S$

Here $\sqrt[\tau]{I_S}$ denotes the τ-radical of the extension ideal I_S of I in the quotient ring A_S which naturally is a k-algebra.

As localization is a fundamental concept to compute real radicals, we state similarly to Chapter 1 the following properties:

Lemma B.5
Let (K,τ) be a pre-ordered field and I a τ-real ideal of some K-algebra A. Then all minimal primes of I are τ-real as well.

Proof
Let $P \in \operatorname{Min}(I)$ and $f \in \sqrt[re]{P}$ arbitrary. We want to show that $f \in P$.
From Lemma B.4, we conclude that

$$\sqrt[re]{I_P} = (\sqrt[re]{I})_P = I_P = P \cdot K[x_1,\ldots,x_n]_P \trianglelefteq K[x_1,\ldots,x_n]_P.$$

Now $f \in \sqrt[re]{P}$ yields that $f^{2r} + s \in P$ for suitable $r \in \mathbb{N}$ and $s \in \sum \tau A^2$, i.e. we have $f^{2r} + s \in P = I_P \cap A$. Hence there exists a $t \notin P$ s.t.

$$t(f^{2r}+s) \in I \implies (tf)^{2r} + t^{2r}s \in I \implies tf \in \sqrt[re]{I} = I \subset P \overset{t \notin P}{\implies} f \in P \qquad \blacksquare$$

Corollary B.6
Let (K,τ) be a pre-ordered field and I an ideal of some K-algebra A. Then $\sqrt[\tau]{I} = \bigcap P$, where P ranges over all τ-real primes containing I.

Proof
The τ-real ideal $\sqrt[\tau]{I}$ is radical and thus the intersection of its minimal primes. These are τ-real by Lemma B.5. $\blacksquare$

Proposition B.7
Let (K,τ) be a pre-ordered fields and P a prime ideal of some K-algebra A. Then the following statements are equivalent:

(a) P is τ-real

(b) There is some $\alpha \in X(K)$ satisfying $\alpha \supseteq \tau$ which can be extended to an ordering $\overline{\alpha}$ of the function field $k(P) := Q(A/P)$.

(c) There is some $\alpha \in X(K)$ satisfying $\alpha \supseteq \tau$ such that P is α-real.

Moreover if A is an affine K-algebra and P a maximal ideal of A then the statements $(a) - (c)$ are equivalent to:

(d) There is some $\alpha \in X(K)$ satisfying $\alpha \supseteq \tau$ such that $k(P)$ can be embedded into some real closed field containing the real closure of (K, τ).

PROOF
$(a) \Rightarrow (b)$: Let $\overline{\tau}$ denote the quadratic semi-ring defined by

$$\overline{\tau} := \{\sum_{i=1}^{m} s_i a_i^2 \in k(P) : m \in \mathbb{N}_0 \text{ and } s_1, \ldots, s_m \in \tau, a_1, \ldots, a_m \in k(P)\}.$$

CLAIM: P is τ-real iff $\overline{\tau}$ is a pre-ordering of $k(P)$.

PROOF
$\Rightarrow$: Suppose $\overline{\tau}$ is no pre-ordering in $k(P)$, i.e. $-1 \in \overline{\tau}$. Hence

$$-1 = \sum_{i=1}^{m} s_i (\frac{f_i}{g_i})^2 \qquad \text{where } a_i = \frac{f_i}{g_i} \in k(P), \text{ i.e. } g_i \notin P.$$

$$\Rightarrow -(\prod_{i=1}^{m} g_i)^2 = \sum_{i=1}^{m} (s_i \prod_{j \neq i} g_j^2) \cdot f_i^2$$

$$\Rightarrow (\prod_{i=1}^{m} g_i)^2 + \sum_{i=1}^{m} (s_i \prod_{j \neq i} g_j^2) \cdot f_i^2 = 0 \in P$$

$$\Rightarrow \prod_{i=1}^{m} g_i \in \sqrt[\tau]{P}$$

But none of the g_i is in P, hence there product isn't in P as P is prime. Thus $\sqrt[\tau]{P} \neq P$.

$\Leftarrow$ Suppose that P is not τ-real. Then there exists an $f \notin P$ s.t.

$$f^{2r} + \sum_{i=1}^{m} s_i a_i^2 \in P$$

for suitable $m \in \mathbb{N}_0$, $s_1, \ldots, s_m \in \tau$ and $a_1, \ldots, a_m \in A$.

But then

$$-1 = \sum_{i=1}^{m} \underbrace{s_i}_{\in\tau} \underbrace{(\frac{a_i}{f^r})^2}_{\in k(P)} \in \overline{\tau}.$$

Hence $\overline{\tau}$ is no pre-ordering. ∎

Now by choosing an ordering $\overline{\alpha} \in X(k(P))$ extending $\overline{\tau}$ we obtain via the projection $\alpha = \overline{\alpha} \cap k$ an element of $X(k)$ as required in (b).

$(b) \Rightarrow (c)$: Let $f \in \sqrt[\tau]{P}$, i.e. there exist suitable $m, r \in N, s_1, \ldots, s_m \in \tau, a_1, \ldots, a_m \in A$ such that $f^{2r} + \sum_{i=1}^{m} s_i a_i^2 \in P$.

Now taking residues modulo P yields the equation $\overline{f}^{2r} + \sum_{i=1}^{m} s_i \overline{a_i}^2 = 0$ in the ordered field $(k(P), \overline{\alpha})$ from which we conclude that $\overline{f} = 0$ in $k(P)$. Hence $f \in P$

$(c) \Rightarrow (a)$ This assertion follows immediately by the following inclusion chain

$$P \subset \sqrt[\tau]{P} \subset \sqrt[\alpha]{P} = P.$$

Hence $\sqrt[\tau]{P} = P$.

Finally let me remark that in the case of an affine k-algebra A for any maximal ideal P of A, the function field $k(P) = A/P$ is a finite (algebraic) extension of k. ∎

To finish this subsection we cite some important facts:

Proposition B.8
Let (K, τ) be a pre-ordered field and I an ideal of some affine K-algebra A. Then $\sqrt[\tau]{I} = \bigcap M$, where M ranges over all τ-real maximal ideals of A containing I.

Remark B.9
For the special case of $(K, \tau) = (\mathbb{Q}, \geq)$ and $A = \mathbb{Q}(y_1, y_2, \ldots, y_m)[x_1, \ldots, x_n]$ this proposition is the same as Corollary 1.10 from Chapter 1.

The well-known **sign change criterion** from D.Dubois and G. Elfroymson (see [KS89] Chapter 2 § 12 Theorem 4) is:

Theorem B.10
Let (K, τ) be an ordered field with its unique real closure R and $f \in K[x_1, \ldots, x_n]$ be an irreducible polynomial. Then the following are equivalent:

(a) The ordering τ can be extended to an ordering $\overline{\alpha}$ over the function field $k(f) = Q(K[x_1, \ldots, x_n]/\langle f \rangle)$.

(b) f is indefinite over R, i.e. the exists $a, b \in R^n$ such that $f(a) \cdot f(b) < 0$.

This leads us directly to the following remark about the situation over $\mathbb{Q}$.

Remark B.11
Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be an irreducible polynomial. Then f is real (i.e. $\langle f \rangle$ is real) iff f is indefinite over $\mathbb{R}_{alg}$ and thus by Theorem A.21 indefinite over $\mathbb{R}$.

PROOF
f is real iff the ordering $re = \mathbb{Q}_{\geq}$ can be extended in $Q(\mathbb{Q}[x_1, \ldots, x_n]/\langle f \rangle)$ by Proposition B.7. By the sign change criterion this can be extended iff f is indefinite over $\mathbb{R}_{alg}$. ∎

As a another remark for polynomials over $Q(y_1, y_2, \ldots, y_m)$ we get:

Remark B.12
Let $f \in \mathbb{Q}(y_1, y_2, \ldots, y_m)[x_1, \ldots, x_n]$ be an irreducible polynomial. Then f is not real iff for every ordering α of $\mathbb{Q}(y_1, y_2, \ldots, y_m)$ and every corresponding real closure R_α f is not indefinite (i.e. positive semi-definite) over R_α.

PROOF
Let $F := \mathbb{Q}(y_1, y_2, \ldots, y_m)$.
Suppose the contrary. Therefore let me first of all remark that since f is irreducible the ideal $\langle f \rangle$ is a prime ideal. Let now $\alpha \in X(F)$ be an ordering such that f is indefinite over R_α. This ordering α of F can be extended to an ordering $\overline{\alpha}$ in $k(f) = F[x_1, \ldots, x_n]/\langle f \rangle$.by Proposition B.7 b) this is equivalent to the statements that $\langle f \rangle$ is real. Thus f is real. ∎

B.1.1 The Real Nullstellensatz

We now state the Real Nullstellensatz which was proved by Krivine in the 60s. We first define the set of real points. For more detailed information see [KS89] or ([BN98] Definition 2.7 and Theorem 2.8)

Definition B.13
Let (K, τ) be a pre-ordered field and $I \trianglelefteq K[x_1, \ldots, x_n]$. For a ordering $\alpha \supseteq \tau$ let R_α denote the unique real closure of (K, α). Then we define the set of all τ-real point V_τ as follows:

$$V_\tau(I) = \cup_{\alpha \supseteq \tau} V_{R_\alpha}(I).$$

Especially the set of all real points is denoted by $V_{re}(I)$.

A generalization of Theorem 1.7 which was introduced in Chapter 1 is the general Real Nullstellensatz:

Theorem B.14 (The general real Nullstellensatz)
Let (K,τ) be a pre-ordered field and $I \trianglelefteq K[x_1,\dots,x_n]$ be an ideal. The we have

$$I_K(V_\tau(I)) = \sqrt[\tau]{I}$$

.

Proof

$\supseteq$: Let $f \in \sqrt[\tau]{I}$. We have to show that f vanishes at $V_\tau(I)$. From the definition of $V_\tau(I)$ we get that

$$V_\tau(I) = \cup_{\alpha\supseteq\tau} V_{R_\alpha}(I).$$

As $f \in \sqrt[\tau]{I}$ we know that there exists an $m \in \mathbb{N}$ and polynomials $g_1,\dots g_r \in K[x_1,\dots,x_n]$, $k_1,\dots l_r \in \tau$ such that $f^{2m} + \sum_{i=1}^{r} k_i g_i^2 \in I$. For an arbitrary real closed field R_α let x be an arbitrary zero of I. Thus

$$\begin{aligned}
(f^{2m} + \sum_{i=1}^{r} k_i g_i^2)(x) = 0 &\implies f^{2m}(x) + \sum_{i=1}^{r} k_i g_i^2(x) = 0 \\
&\implies \underbrace{f^{2m}(x)}_{\in\alpha \text{ i.e. } \geq 0} + \underbrace{\sum_{i=1}^{r} k_i g_i^2(x)}_{\in\alpha \text{ i.e. } \geq 0} = 0 \\
&\implies f^{2m}(x) = 0 \overset{R_\alpha \text{ is a field}}{\implies} f(x) = 0
\end{aligned}$$

Hence f vanishes at x.

$\subseteq$: Let $f \in K[x_1,\dots,x_n] \setminus \sqrt[\tau]{I}$. We have to show that there exists an $x \in V_\tau(I)$ such that $f(x) \neq 0$, i.e. there exists a real closed field R which contains the point x. As $f \notin \sqrt[\tau]{I}$ there exists (by Proposition B.8) a τ-real maximal ideal such that $I \subseteq M$ but $f \notin M$. Let $k(M)$ be the function field $K[x_1,\dots,x_n]/M$. This field can can embedded into some real closure R of (K,α) such that $\alpha \subseteq \tau$ by Proposition B.7 (d). Now, let $\overline{\varphi} : K[x_1,\dots,x_n] \mapsto k[x_1,\dots,x_n]/M = k(M)$ denote the canonical endomorphism. Then the point $x := (\overline{x_1},\dots,\overline{x_n}) \in k(M)^n \subseteq R^n$ has the demanded properties, i.e. $f(x) \neq 0$. ∎

The following lemma is useful for the computation in real closed fields. Note that it is a kind of specialization of the Weak Nullstellensatz over algebraically closed fields.

Lemma B.15
Let R be any real closed field and $M \lhd \cdot R[x_1,\dots,x_n]$ be a maximal ideal. Then we have the following 2 cases.

i. M is not real, so $V_R(M) = \varnothing$.

ii. M is real and $V_R(M)$ consists of only one point.

PROOF
As M is a maximal ideal $R' := R[x_1, \ldots, x_n]/M$ is a field extension. As R is real closed, we know that $\overline{R} = R(i)$ and $[\overline{R} : R] = 2$. So we have the following 2 cases.

$[R' : R] = 1$ Then $R' = R$ and every zero of M is real thus M is real.
Let $a = (a_1, a_2, \ldots, a_n) \in R^n$ so $a \in V_R(M)$.
Now $I_R(a) = \langle x_1 - a_1, x_2, \ldots, x_n - a_n \rangle$ is a maximal ideal contains M as $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle = I_R(a) \subset I_R(V_R(M)) = M$. Thus $M = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. And hence $V_R(M) = \{a\}$ is exactly one point.

$[R' : R] = 2$ Then $R' = \overline{R}$ and $\overline{R}$ is not real thus M is not real by Proposition B.7. Hence by the real Nullstellensatz (Theorem B.14) $V_R(M) = \varnothing$. ∎

Bibliography

[BCR98] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.

[BN98] E. Becker and R. Neuhaus. On the computation of the real radical. *Journal of Pure and Applied Algebra*, 124:261–280, 1998.

[BPR03] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2003.

[Bro96] Fabrizio Broglia, editor. *Lectures in real geometry*, volume 23 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1996. Papers from the Winter School held at the Universidad Complutense de Madrid, Madrid, January 3–7, 1994.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[dJP00] Theo de Jong and Gerhard Pfister. *Local analytic geometry*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 2000. Basic theory and applications.

[GP02] Gert-Martin Greuel and Gerhard Pfister. *A* **Singular** *introduction to commutative algebra*. Springer-Verlag, Berlin, 2002. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh, and UNIX).

[GX04] Zeng Guangxing and Zeng Xiaoning. An effective decision method for semidefinite polynomials. *J. Symb. Comput.*, 37(1):83–99, 2004.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[KS89] Manfred Knebusch and Claus Scheiderer. *Einführung in die reelle Algebra*, volume 63 of *Vieweg Studium: Aufbaukurs Mathematik [Vieweg Studies: Mathematics Course]*. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[vzGG99] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.