Radicals of binomial ideals

Eberhard Becker, Rudolf Grobe and Michael Niermann*
Universität Dortmund
FB Mathematik
Lehrstuhl VI
44221 Dortmund
Fed. Rep. of Germany

September 16, 1996

*the authors acknowledge support from the Deutsche Forschungsgemeinschaft

Introduction

Polynomial ideals allowing a set of generators consisting of binomials are called binomial ideals.They form a distinguished class of ideals,both from a theoretical and algorithmical point of view.In the introduction of their paper [EiSt] Eisenbud and Sturmfels present a very interesting survey of the ubiquity of binomial ideals.Their paper is most relevant for our work.Their results suggested to study radicals of binomial ideals in a quite general context.The usual notion of the radical of an ideal is closely related to algebraic geometry over algebraically closed fields.There are good reasons to sudy zeros of an ideal $\mathfrak{a}$ in other extension fields L of the base field K.The vanishing ideal of the set of the $L-$rational points of $\mathfrak{a}$ is called the *$L-$radical* of $\mathfrak{a}$. Varying the field L in special classes of field extensions gives rise to variants of the notion of an $L-$radical.Notably,the real radicals of real algebraic geometry deserve special attention. In this paper we study quite general radicals of polynomial ideals and focus on two main problems:

- Is the radical of a binomial ideal still a binomial ideal?
- Are there special algorithms to compute the radical of a binomial ideal?

Section 1 presents the basic results about binomial ideals we are going to use.We first list various statements of the Eisenbud-Sturmfels paper [EiSt].Besides that we prove a Bezout-type bound for the cardinality of the set of $L-$rational points of a binomial ideal provided this set is finite.Special attention is given to that part of field theory that is associated with binomial ideals.Roughly speaking,we have to study *Kummer theory* without roots of unities.Results of M.Kneser concerning this topic are influential at many places of this paper.

In the subsequent section we study radicals of ideals from an axiomatic point of view.We introduce what we call a *radical operation* which assigns to an ideal of a $K-$algebra another ideal of the same algebra subject to some natural axioms.We have two reasons to present this axiomatic approach. First of all,the instances of radicals of ideals mentioned above ask for a unified treatment.Secondly,starting with these axioms it can be clarified why or why not radicals of binomial ideals are again binomial ideals.

This will be made apparent in the third section where we show that the radicals of the special ideals

$$(X_1^{f_1} - a_1, \dots, X_r^{f_r} - a_r) \lhd K[X_1, \dots, X_s]$$

decide whether the radical of an arbitary binomial ideal is a binomial ideal.In addition, the method of the proof suggests an algorithm to compute the radical even if it is not a binomial ideal.The essential additional idea we follow is the suggestion from [EiSt] to decompose the affine variety of $\mathfrak{a}$ into cells and to study the cells via Laurent polynomial rings.

In section 4 we use the reduction to the special ideals just mentioned to characterize the field extensions $L|K$ such that the $L-$radicals of arbitrary binomial ideals over K are again binomial ideals.This is true in interesting cases as

i) $L = K$,

ii) $L = K_{sep}$,the separable closure,

iii) $L = R$,a real closure.

If K is not perfect there are binomial ideals with a non-binomial (usual) radical.In addition,the various radicals occuring in real algebraic geometry are also studied in detail.

The concluding section 5 is devoted to deriving various algorithms to study the following problems:

- Determine *dim* and irreducible components
- Decide the existence of points
- Find cardinalities if the set of $L-$points is finite
- Compute radicals

It is our aim to design algorithms which benefit from the special structure of binomial ideals.Again,the decomposition into cells is the basic idea to start with.

List of contents

1 Binomial ideals and radical extensions

2 Radicals of ideals

3 Radicals of binomial ideals

4 $L-$radicals and $\tau-$radicals

5 Algorithms

1 Binomial ideals and radical extensions

In this section we present the notions and basic results we are going to use. Let K be a field and $K[\underline{X}] = K[X_1, \ldots, X_n]$ be the polynomial ring in n variables over K. Any product $t = \prod_{i=1}^{n} X_i^{r_i}$, $r_i \in \mathbb{N} \cup \{0\}$ is referred to as a *term*. Elements at, $a \in K$, t a term are called *monomials*, and *binomials* are the differences of two monomials, one of which may be zero.

Let $\Delta \subseteq \{1, \ldots, n\}$. We say a term (resp. binomial) is built over Δ if only variables X_i with $i \in \Delta$ occur in the presentation of the term (resp. binomial).

An ideal $\mathfrak{a} \lhd K[\underline{X}]$ is said to be a *binomial ideal* or just *binomial* if it can be generated by a set of binomials. Clearly, this generating set can be chosen to be finite. An algorithm to detect whether a given ideal is binomial is based on the following characterization, cf. [EiSt], prop. 1.1:

1.1 Proposition

The following statements are equivalent

i) $\mathfrak{a}$ is binomial,

ii) for some term order the reduced Gröbner basis of $\mathfrak{a}$ consists of binomials,

iii) for every term order the reduced Gröbner basis of $\mathfrak{a}$ consists of binomials.

As immediate consequences we get [EiSt], (1.2), (1.3):

1.2

i) if $L|K$ is an extension field then $\mathfrak{a}$ is binomial iff $\mathfrak{a}\, L[\underline{X}]$ is binomial,

ii) if $\mathfrak{a}$ is binomial then every elimination ideal $\mathfrak{a} \cap K[X_1, \ldots, X_n]$ is again a binomial ideal.

iii) if $\mathfrak{a}$, $\mathfrak{a}'$ are binomial ideals and $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$ ideals in $K[\underline{X}]$ generated by monomials then

$$(\mathfrak{a} + \mathfrak{a}') \cap (\mathfrak{a} + \mathfrak{b}_1) \cap \ldots \cap (\mathfrak{a} + \mathfrak{b}_s)$$

is a binomial ideal. If $\mathfrak{a}' = 0$ then this intersection equals $\mathfrak{a} + \mathfrak{b}$ where $\mathfrak{b}$ is generated by monomials.

Note that the intersection of binomial ideals is rarely binomial.

If A, B are two K–algebras we denote the set of K–algebra homomorphisms $A \to B$ by $\mathrm{Hom}_K(A, B)$. If L is any extension field of K then the set of L points of $\mathfrak{a}$

$$V_L(\mathfrak{a}) = \{x \in L^n | f(x) = 0 \text{ for every } f \in \mathfrak{a}\}$$

is canonically bijective to $\mathrm{Hom}_K\left({K[\underline{X}]}/{\mathfrak{a}}, L\right)$. If $L = \overline{K}$, the algebraic closure of K, we set $V(\mathfrak{a}) = V_{\overline{K}}(\mathfrak{a})$. As proposed by Eisenbud–Sturmfels the affine variety $V(\mathfrak{a})$ is decomposed into *cells* $V^\Delta(\mathfrak{a})$, $\Delta \subseteq \{1, \ldots, n\}$. Setting $(K^\times)^\Delta = \{(x_1, \ldots, x_n) \in K^n | x_i \neq 0 \text{ for } i \in \Delta, \, x_i = 0 \text{ for } i \neq \Delta\}$
we define

$$V^\Delta(\mathfrak{a}) = (K^\times)^\Delta \cap V(\mathfrak{a}).$$

Clearly,

$$V(\mathfrak{a}) = \bigcup_{\Delta \subseteq \{1,\ldots,n\}} V^\Delta(\mathfrak{a}).$$

We just write $V^\Delta = V^\Delta(\mathfrak{a})$ if no confusion is to be expected. Let now $\mathfrak{a}$ be a binomial ideal generated by a set of binomials $\{b_1, \ldots, b_s\}$. We want to analyze the non–emptiness of a cell $V^\Delta(\mathfrak{a}) = V^\Delta$, $\Delta \subseteq \{1, \ldots, n\}$. Let $\pi_\Delta : K[\underline{X}] \to K[X_i | i \in \Delta]$ be the K–algebra homomorphism defined by

$$\begin{array}{ll} X_i \mapsto X_i & \text{if } i \in \Delta, \\ X_i \mapsto 0 & \text{if } i \notin \Delta. \end{array}$$

Set $\mathfrak{a}_\Delta = \pi_\Delta(\mathfrak{a})$ and $\mathfrak{a}_\Delta^\pm = \mathfrak{a}_\Delta \, K[X_i, X_i^{-1} | i \in \Delta]$ the extended ideal in the Laurent polynomial ring. Further write

$$A_\Delta := {K[X_i, X_i^{-1} | i \in \Delta]}/{\mathfrak{a}_\Delta^\pm}.$$

We then find that, in a canonical way,

1.3

$$V^\Delta \simeq \mathrm{Hom}_K(A_\Delta, \overline{K})$$

Everything can be read off any fixed set of generators $b_1, \ldots, b_s$ of $\mathfrak{a}$. There are three types of generators among the b_i's:

1) b_i is built over Δ,

2) $b_i = ax_jt - a'x_{j'}t'$ where $a, a' \in K, j, j' \notin \Delta$, t, t' terms,

3) $b_i = at - a'x_jt'$ where $a \in K^\times$, $a' \in K$, $j \notin \Delta$, t a term built over Δ, t' any term.

We first conclude:

1.4

Assume $V^\Delta \neq 0$ then

i) none of $b_1, \dots, b_s$ is of type 3).

ii) $\mathfrak{a}_\Delta$ is generated by the generators of type 1).

iii) $\mathfrak{a} + \sum\limits_{i \notin \Delta} (X_i) = \mathfrak{a}_\Delta K[\underline{X}] + \sum\limits_{i \notin \Delta} (X_i)$.

The natural projection $\overline{K}^n \xrightarrow{p} \overline{K}^\Delta$ induces a regular map $V(\mathfrak{a}) \xrightarrow{p} V(\mathfrak{a}_\Delta)$ if there are no generators of type 3). We get

1.5

If $V^\Delta \neq 0$ then:

i) the mapping $p : V(\mathfrak{a}) \to V(\mathfrak{a}_\Delta)$ is surjective and admits the section $s : V(\mathfrak{a}_\Delta) \to V(\mathfrak{a})$,

$$\begin{array}{l} s((x_i)_{i \in \Delta}) = (y_1, \dots, y_n) \text{ where} \\ y_i = x_i \text{ if } i \in \Delta, y_i = 0 \text{ if } i \notin \Delta, \end{array}$$

ii) the fibers of p are described by binomial ideals.

Proof: i) follows from the fact that generators of type 3) are missing.
ii) Obvious.

■

Non-empty cells for distinct sets Δ and Δ' of indices are not unrelated. Theorem (4.1) of [EiSt] is a very interesting complete result. We only need a trivial part of it.

Assume $\Delta' \subseteq \Delta \subseteq \{1, \dots, n\}$. We will use the projection

$$\overline{p} : \left\{ \begin{array}{ccc} (K^\times)^\Delta & \to & (K^\times)^{\Delta'} \\ (x_1, \dots, x_n) & \mapsto & (y_1, \dots, y_n) \end{array} \right.$$

where $y_i = x_i$ if $i \in \Delta'$ and $y_i = 0$ for $i \notin \Delta'$. Applying (1.4), i) by replacing $\{1, 2, \dots, n\}$ by Δ and the Δ of (1.4) by Δ' we readily derive:

1.6

If $\Delta' \subseteq \Delta$ and $V^{\Delta'}$, $V^{\Delta} \neq \emptyset$ then

$$\overline{p}(V^{\Delta}) \subseteq V^{\Delta'}.$$

The final analysis of V^{Δ} depends on the structure of the ideal $\mathfrak{a}_{\Delta}^{\pm} \lhd K[X_i, X_i^{-1} | i \in \Delta]$. We may set $\Delta = \{1, \ldots, n\}$ and write $K[\underline{X}^{\pm}] := K[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}]$. The Laurent polynomial ring is isomorphic to the group algebra $K[\mathbf{Z}^n]$ and admits the basis $\{\underline{X}^{\underline{m}} | \underline{m} \in \mathbf{Z}^n\}$ with $\underline{m} = (m_1, \ldots, m_n)$, $\underline{X}^{\underline{m}} = \prod\limits_{1}^{n} X_i^{m_i}$. These elements are units. An ideal $\mathfrak{a} \lhd K[\underline{X}^{\pm}]$ is called *binomial* or a *binomial ideal* if it can be generated by a set of elements of the type $\underline{X}^{\underline{m}} - a$, $a \in K$.

Note that *the binomial ideals of $K[\underline{X}^{\pm}]$ are just the extensions $\mathfrak{b}^{\pm}$ of binomial ideals $\mathfrak{b}$ of $K[\underline{X}]$*. In fact, $\mathfrak{b}^{\pm}$ is generated by binomials $a_i \underline{X}^{\underline{m}_i - \underline{r}_i} - b_i$. Conversely, if $\mathfrak{a}$ is generated by the elements $\{X^{\underline{m}_i} - a_i\}_{i \in I}$ then $\mathfrak{a} = \mathfrak{b}^{\pm}$ where $\mathfrak{b} = (\underline{X}^{\underline{m}_i^+} - a_i \underline{X}^{m_i^-} | i \in I)$, $\underline{m}^+ = (\ldots, \sup(m_i, 0), \ldots)$, $\underline{m}^- = (-\underline{m})^+$, $\underline{m} = \underline{m}^+ - \underline{m}^-$.

Let $\mathfrak{a}$ be a binomial ideal in $K[\underline{X}^{\pm}]$, $\mathfrak{a} \neq K[\underline{X}^{\pm}]$. Then necessarily $a \neq 0$ if $\underline{X}^{\underline{m}} - a \in \mathfrak{a}$. Now let $\mathfrak{a}$ be generated by $\underline{X}^{\underline{m}_i} - a_i, i = 1, \ldots, k$ where $\underline{m_i} \in \mathbf{Z}^n$. $a_i \in K^{\times}$. Let $L =< \underline{m_1}, \ldots, \underline{m_k} >$ be the sublattice of $\mathbf{Z}^n$ generated by $\underline{m_1}. \ldots, \underline{m_k}$. The assignment

$$\underline{m_i} \mapsto a_i$$

can be extended to a <u>character</u> $\rho : L \rightarrow K^{\times}$, i.e. a homomorphism $(L. +) \rightarrow (K^{\times}, \cdot)$. To see this we need the following rules (where $\underline{m}. \underline{m'} \in \mathbf{Z}^n. a, a' \in K^{\times}$):

$$\underline{X}^{\underline{m}} \equiv a \bmod \mathfrak{a} \quad \Rightarrow \quad \underline{X}^{-\underline{m}} \equiv a^{-1} \bmod \mathfrak{a} \qquad (1)$$

$$\underline{X}^{\underline{m}} \equiv a \bmod \mathfrak{a}, \underline{X}^{\underline{m'}} \equiv a' \bmod \mathfrak{a} \quad \Rightarrow \quad \underline{X}^{\underline{m} + \underline{m'}} \equiv aa' \bmod \mathfrak{a} \qquad (2)$$

The first one is obtained by multiplying the original congruence with $a^{-1} \underline{X}^{-\underline{m}}$. The second one follows from the identity

$$\underline{X}^{\underline{m} + \underline{n}} - ab = \underline{X}^{\underline{n}}(\underline{X}^{\underline{m}} - a) + a(\underline{X}^{\underline{n}} - b). \qquad (3)$$

Next let $\underline{m} = \sum_{i=1}^k \lambda_i \underline{m_i} = \sum_{i=1}^k \mu_i \underline{m_i} \in L$ where $\lambda_i, \mu_i \in \mathbf{Z}$. ¿From (1) and (2) we get

$$\underline{X}^{\underline{m}} - \prod_{i=1}^{k} a_i{}^{\lambda_i}, \underline{X}^{\underline{m}} - \prod_{i=1}^{k} a_i{}^{\mu_i} \in \mathfrak{a}.$$

Since $\mathfrak{a} \neq K[\underline{X}^{\pm}]$ we conclude $\prod_{i=1}^k a_i{}^{\lambda_i} = \prod_{i=1}^k a_i{}^{\mu_i}$. Therefore we can define

$$\rho\left(\sum_{i=1}^{k}\lambda_i\underline{m_i}\right) := \prod_{i=1}^{k} a_i{}^{\lambda_i}. \tag{4}$$

The pair (L,ρ) defines a binomial ideal $\neq K[\underline{X}^{\pm}]$:

$$I(L,\rho) := (\underline{X}^{\underline{m}} - \rho(\underline{m}) | \underline{m} \in L)$$

and the above considerations have shown

$$\mathfrak{a} = (\underline{X}^{\underline{m_1}} - a_1, \dots, \underline{X}^{\underline{m_k}} - a_k) = I(L,\rho) \text{ where} \tag{5}$$

$$L = < \underline{m_1}, \dots, \underline{m_k} >, \rho \text{ as in (4).}$$

(provided $\mathfrak{a} \neq K[\underline{X}^{\pm}]$). We have

$$I(L,\rho) \cap K[X_1,\dots,X_n] = (\{\underline{X}^{\underline{m}^+} - \rho(m)\underline{X}^{\underline{m}^-} \big| m \in L\}) \tag{6}$$

cf. [EiSt], Cor 2.5.

We need further basic results about binomial ideals in $K[\underline{X}^{\pm}]$ already proved in [EiSt]. In particular, we need that (L,ρ) is uniquely determined by $\mathfrak{a}$.

We will apply the elementary divisor theorem to get this and other facts. Every lattice automorphism $\varphi : \mathbf{Z}^n \to \mathbf{Z}^n$ gives rise to a K-algebra automorphism

$$\hat{\varphi} : K[\underline{X}^{\pm}] \to K[\underline{X}^{\pm}], \underline{X}^{\underline{m}} \mapsto X^{\varphi(\underline{m})}.$$

We will use appropriate automorphisms to normalize binomial ideals and note first

$$\hat{\varphi}\left(I(L,\rho)\right) = I(\varphi(L), \rho\circ\varphi^{-1}). \tag{7}$$

Given any sublattice $L \subseteq \mathbf{Z}^n$, the elementary divisor theorem provides a basis $\underline{v_1}, \dots, \underline{v_n}$ of $\mathbf{Z}^n$ and the elementary divisors $r_1, \dots, r_d \in \mathbb{N}$ such that

$$\begin{array}{ll} \text{i)} & r_1 | r_2 | \cdots | r_d, \\ \text{ii)} & r_1\underline{v_1}, \dots, r_d\underline{v_d} \text{ is a } \mathbf{Z}\text{-basis of } L. \end{array} \tag{8}$$

¿From the computational point of view we want to stress that finding $\underline{v_1}, \dots, \underline{v_n}$ and $r_1, \dots, r_d$ can be achieved by doing Euclidean algorithm finitely often. In fact, represent a set of generators of L as the columns of a matrix A. Then finding $\underline{v_1}, \dots, \underline{v_n}$ and $r_1, \dots, r_d$ amounts to computing unimodular matrices U, V satisfying

$$V^{-1}AU = \begin{pmatrix} r_1 & & \\ & \ddots & 0 \\ & & r_d \end{pmatrix}, r_1|r_2|\cdots|r_d. \tag{9}$$

Any existence proof based on the Euclidean algorithm provides a way to compute all data, cf. [vdW] e.g. . In our present situation, the condition i) in (8) is not needed. Hence, in computing U, V we can stop once a diagonal matrix $V^{-1}AU$ is obtained.

Suppose unimodular matrices U, V have been found satisfying

$$V^{-1}AU = \begin{pmatrix} r_1 & & \\ & \ddots & 0 \\ & & r_d \end{pmatrix}$$

where we do not assume $r_1|r_2|\cdots|r_d$. The columns $\underline{v_1}, \ldots, \underline{v_n}$ of V form a $\mathbf{Z}$-basis of $\mathbf{Z}^n$ and $r_1\underline{v_1}, \ldots, r_d\underline{v_d}$ a $\mathbf{Z}$-basis of L. Let

$$\mathrm{Sat}(L) = \{\underline{w} \in \mathbf{Z}^n | \exists k \in \mathbf{Z}\backslash\{0\} : k\underline{w} \in L\}$$

be the saturated hull of L, [EiSt]. Then $\mathrm{Sat}(L) =< \underline{v_1}, \ldots, \underline{v_d} >$ and $[\mathrm{Sat}(L) : L] = r_1 r_2 \cdots r_d$. In the case $d = n$, i.e. $\mathrm{Sat}(L) = \mathbf{Z}^n$, we see that $\prod_{i=1}^n r_i$ is the volume of a fundamental domain of L.

Assume that $\underline{v_1}, \ldots, \underline{v_n}, r_1, \ldots, r_d$ as in (8) have been computed. V^{-1} induces the automorphism $\varphi : \mathbf{Z}^n \longrightarrow \mathbf{Z}^n, \underline{v_i} \mapsto \underline{e_i}$ where $\underline{e_i}$ denotes the i-th standard basis vector $(0, \ldots, 0, 1, 0, \ldots, 0)$ (1 at the i-th slot). Then $\varphi(L) =< r_1\underline{e_1}, \ldots, r_d\underline{e_d} >$ and we get

$$\hat{\varphi}(I(L, \rho)) = ({X_1}^{r_1} - \rho(r_1\underline{v_1}), \ldots, {X_d}^{r_d} - \rho(r_d\underline{v_d})), \tag{10}$$

$$K[\underline{X}^{\pm}]\big/_{\mathfrak{a}} \simeq K[\underline{X}^{\pm}]\big/_{\hat{\varphi}(\mathfrak{a})} \xrightarrow{\sim}$$

$$\left(K[X_1, \ldots, X_d]\big/_{({X_1}^{r_1} - \rho(r_1\underline{v_1}), \ldots, {X_d}^{r_d} - \rho(r_d\underline{v_d}))} \right) \left[{X_{d+1}}^{\pm 1}, \ldots, {X_n}^{\pm 1} \right]. \tag{11}$$

1.7 Proposition

Assume $\mathfrak{a} = I(L, \rho)$, *then*

i) $\dim \mathfrak{a} = n - \dim_{\mathbf{Z}} L$,

ii) $L = \{\underline{m} \in \mathbf{Z}^n | \exists a \in K^\times : \underline{X}^{\underline{m}} - a \in \mathfrak{a}\}$.

Proof:

i) follows from (11).

ii) It is enough to show that $\underline{m} \in L$ if $\underline{X}^{\underline{m}} \equiv a \bmod \mathfrak{a}$ for some $a \in K^\times$. Assume $\underline{X}^{\underline{m}} - a \in \mathfrak{a}$. Then $\underline{X}^{\varphi(\underline{m})} - a \in \hat{\varphi}\left(I(L,\rho)\right)$. Using $X_i^{r_i} - a_i \in \hat{\varphi}(\mathfrak{a})$ for $i = 1, \ldots, d$ we find

$$\underline{X}^{\varphi(\underline{m})} \equiv a' X_1{}^{s_1} \cdots X_d{}^{s_d} X_{d+1}{}^{s_{d+1}} \cdots X_n{}^{s_n} \bmod \mathfrak{a}$$

where $a' \in K^\times$, $0 \leq s_i < r_i$ for $i = 1, \ldots, d$. Set $\mathfrak{b} = (\hat{\varphi}(\mathfrak{a}), X_{d+1} - 1, \ldots, X_n - 1)$. Then $X_1{}^{r_1} X_2{}^{r_2} \cdots X_d{}^{r_d} - a'' \in \mathfrak{b}$ where $a'' = aa'^{-1} \in K^\times$. From

$$K[\underline{X}^\pm]\big/_{\mathfrak{b}} \xrightarrow{\sim} K[X_1, \ldots, X_d]\big/_{(X_1{}^{r_1} - a_1, \ldots, X_d{}^{r_d} - a_d)}$$

and a Gröbner basis argument we conclude $s_1 = \cdots = s_d = 0$, i.e. $\varphi(\underline{m}) \in \rho(L)$, $\underline{m} \in L$.

■

¿From (10) we get a parametrization of the algebraic set $V(\mathfrak{a})$:

$$V(\mathfrak{a}) = \{(x_1, \ldots, x_n) \in \overline{K}^{\times^n} | f(x) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

The automorphism φ induces a rational isomorphism

$$\overline{\varphi} : \overline{K}^{\times^n} \to \overline{K}^{\times^n}, (x_1, \ldots, x_n) \mapsto \left(\underline{x}^{\varphi(\underline{e_1})}, \ldots, \underline{x}^{\varphi(\underline{e_n})}\right)$$

satisfying

$$\overline{\varphi}(\underline{x}^{\underline{v_1}}, \ldots, \underline{x}^{\underline{v_n}}) = (x_1, \ldots, x_n), \overline{\varphi}\left(V\left(\hat{\varphi}(\mathfrak{a})\right)\right) = V(\mathfrak{a}) \qquad (12)$$

Hence

$$V(\mathfrak{a}) = \bigcup_{\substack{(a_1, \ldots, a_d) \in \overline{K}^d \\ a_i{}^{r_i} = \rho(r_i \underline{v_i})}} \overline{\varphi}\left((a_1, \ldots, a_d) \times \overline{K^\times}^{n-d}\right)$$

and we can state

1.8 Proposition *$V(\mathfrak{a})$ decomposes over $\overline{K}$ into rational irreducible components of dimension $n - d$, $d = \dim L$. If $\mathrm{char} K = 0$ or $\mathrm{char} K \not| r_d$ then the number of irreducible components is $r_1 r_2 \cdots r_d$.*

Let us return to a binomial $\mathfrak{a} \lhd K[X_1,\dots,X_n]$. Then $V^\Delta(\mathfrak{a}) \neq \emptyset$ if and only if we have $\mathfrak{a}^{\pm}_{\Delta} \neq K[X_i, X_i^{-1} | i \in \Delta]$. Each non–empty cell is therefore characterized by a lattice $L^\Delta \subseteq \mathbb{Z}^\Delta$ and a character $\rho^\Delta : L^\Delta \to K^\times$. Thus we find a list of data $(L^\Delta, \rho^\Delta)_\Delta$ where Δ runs through the subsets of $\{1,\dots,n\}$ satisfying $V^\Delta(\mathfrak{a}) \neq \emptyset$.

This list contains a great amount of information, in particular, the algorithms in §5 will make use of it. In this section we will use it to derive a Bezout–type result for binomial ideals and to describe Spec A with $A = K[X_1,\dots,X_n]/_{\mathfrak{a}}$ and $\dim \mathfrak{a}$.

1.9 Proposition

Let K be an infinite field, $\mathfrak{a} \lhd K[X_1,\dots,X_n]$ a binomial ideal generated by binomials of degree at most d. Assume that $V_K(\mathfrak{a})$ is a finite set. Then

i) $\#V_K(\mathfrak{a}) \leq d^n$,

ii) $\#V_K(\mathfrak{a}) \leq 3^n$, if K is a real field.

Proof: We start with the decomposition $V_K(\mathfrak{a}) = \bigcup V_K^\Delta(\mathfrak{a})$ where Δ runs through the subsets of $\{1,\dots,n\}$. Suppose that $V_K^\Delta(\mathfrak{a}) = V^\Delta(\mathfrak{a}) \cap V_K(\mathfrak{a})$ is not empty. For the sake of simplicity, set $\Delta = \{1,\dots,s\}$. ¿From (10) we take that $V^\Delta(\mathfrak{a})$ is described by a set of equation

$$X_1^{f_1} = a_1, \dots, X_r^{f_r} = a_r, r \leq s.$$

Since $V_K^\Delta(\mathfrak{a})$ is finite and non–empty we get $r = s$, i.e. $\mathfrak{a}^{\pm}_{\Delta}$ is 0–dimensional. In addition, if K is a real field, we find $\#V_K^\Delta \leq 2^s$ since the only roots of unities in K are ±1. This leads to

$$\#V_K(\mathfrak{a}) \leq \sum_{s=0}^{n} \binom{n}{s} 2^s = 3^n$$

if K is real. This bound in fact appears, take $K = \mathbb{R}$, $\mathfrak{a} = (X_1^{k_1}(X^{2l_1} - 1), \dots, X_n^{k_n}(X_n^{2l_n} - 1))$, $k_i, l_i \geq 1$.

To prove i) we consider the case $V_K(\mathfrak{a}) \neq \{(0,\dots,0)\}$ and choose Δ, say $\Delta = \{1,\dots,r\}$, minimal among the non-empty sets $\Delta' \subseteq \{1,\dots,n\}$ with non–empty $V_K^{\Delta'}(\mathfrak{a})$. We will apply the projection maps in (1.5) and (1.6): $p : V(\mathfrak{a}) \to V(\mathfrak{a}_\Delta)$ and $\overline{p} : V^{\Delta'} \to V^{\Delta''}$ whenever both cells are non–empty.

We claim that $V(\mathfrak{a}_\Delta)$ is finite, i.e. $\mathfrak{a}_\Delta$ is 0–dimensional. In fact, $V(\mathfrak{a}_\Delta) = \bigcup_{\Delta' \subseteq \Delta} V^{\Delta'}(\mathfrak{a})$. Suppose $\emptyset \subsetneq \Delta' \subsetneq \Delta$ and $V^{\Delta'} \neq \emptyset$. The projection $\overline{p} : V^\Delta \to V^{\Delta'}$ clearly maps V_K^Δ into $V_K^{\Delta'}$. By assumption, $V_K^{\Delta'} = \emptyset$ showing $V^{\Delta'} = \emptyset$. Hence $V(\mathfrak{a}_\Delta) \subseteq \{0,\dots,0\} \cup V^\Delta$ and the latter set is finite.

The mapping p induces a surjection $\widetilde{p} : V_K(\mathfrak{a}) \to V_K(\mathfrak{a}_\Delta)$. Given $x = (x_1,\dots,x_n) \in V_K(\mathfrak{a})$ we denote by $\mathfrak{b} \lhd K[X_{r+1},\dots,X_n]$ the binomial ideal obtained by inserting $x_1, \ldots, x_r$ for $X_1, \ldots, X_r$ in the given set of binomial generators. Then

$$\tilde{p}^{-1}(\tilde{p}(x)) = \{(x_1, \ldots, x_r, y_{r+1}, \ldots, y_n) \in K^n | (y_{r+1}, \ldots, y_n) \in V_K(\mathfrak{b})\}.$$

The zero-dimensional ideal $\mathfrak{a}_\Delta \lhd K[X_1, \ldots, X_r]$ is generated by binomials of degree at most d, hence $\#V_K(\mathfrak{a}_\Delta) \leq d^r$. Since $r \geq 1$ and for each $x \in V_K(\mathfrak{a})$ the ideal $\mathfrak{b} \lhd K[X_{r+1}, \ldots, X_n]$ is generated by binomials of degree at most d we apply induction to get $\#V_K(\mathfrak{b}) \leq d^{n-r}$. Putting both bounds together the claim follows once we have settled the beginning of the induction, i.e. $n = 1$. In this case, let $\mathfrak{a} = (b_1, \ldots, b_r) \lhd K[X]$. Then $\mathfrak{a} = (b)$, $b = gcd(b_1, \ldots, b_r)$ and the results follows.

■

Now consider any $\Delta \subseteq \{1, \ldots, n\}$ and any prime ideal $\mathfrak{q} \lhd K[X_i, X_i^{-1} | i \in \Delta]$ which contains $\mathfrak{a}_\Delta^\pm$. Set

1.10

$$\mathfrak{p} := \pi_\Delta{}^{-1} \left(\mathfrak{q} \cap K[X_i | i \in \Delta]\right)$$

then $\mathfrak{p}$ is a prime ideal of $K[\underline{X}]$ containing $\mathfrak{a}$. ¿From $\mathfrak{p}$ the data Δ and $\mathfrak{q}$ can be recovered: $\Delta = \{i | X_i \notin \mathfrak{p}\}, \mathfrak{q} = \pi_\Delta(\mathfrak{p})^\pm$.

Conversely, if $\mathfrak{p}$ is a given prime ideal of $K[\underline{X}]$, $\mathfrak{a} \subseteq \mathfrak{p}$ then define Δ and $\mathfrak{q}$ as above. Then $\mathfrak{q}$ is a prime ideal in the Laurent polynomial ring and $\mathfrak{p}$ and $(\Delta, \mathfrak{q})$ are linked by (1.10). We summarize

1.11 Proposition .

i) The assignment $(\Delta, \mathfrak{q}) \mapsto \mathfrak{p}$ *from above is a bijection between* $\bigcup_{\Delta : V^\Delta \neq \emptyset}$ *Spec* A_Δ *and Spec* A.

ii) $\dim \mathfrak{a} = \max\{|\Delta| - \dim L^\Delta | V^\Delta \neq \emptyset\}$.

Proof: i) Proved above. ii) apply i) and (1.7).

■

The final topic of this section is the class of 0–dimensional binomial ideals $\mathfrak{a}$. More precisely we are interested in the residue fields of maximal ideals in $A = K[X_1, \ldots, X_n]/_{\mathfrak{a}}$. They turn out to be radical extensions of K and the properties of such extensions are vital for our main results. The radical extensions encountered here are of the type $L = K(\sqrt[r_1]{a_1}, \ldots, \sqrt[r_n]{a_n})$ where the radicands $a_i \in K$, $i = 1, \ldots, n$ and where we denote by $\sqrt[e]{a}$ <u>any</u> of the solutions of $X^e = a$ in the algebraic closure $\overline{K}$ of K.

1.12 Proposition

Let $\mathfrak{a}$ be a zero-dimensional binomial ideal and $\mathfrak{m}$ a maximal ideal of $K[\underline{X}]$, $\mathfrak{a} \subseteq \mathfrak{m}$. Then $K[X_1, \ldots, X_n]/_{\mathfrak{m}} = K(\sqrt[r_1]{a_1}, \ldots, \sqrt[r_n]{a_n})$ for suitable $a_i \in K$, $r_i \in \mathbb{N}$ and roots $\sqrt[r_i]{a_i}$ $(i = 1, \ldots, n)$.

Proof: Using (1.11) and (11) we may assume $\mathfrak{a} = (X_1^{r_1} - a_1, \ldots, X_d^{r_d} - a_d) \lhd K[X_1, \ldots, X_d]$ for some $d \leq n$ and $a_1, \ldots, a_d \in K^\times$. Now the claim follows.

■

In the situation of §4 we will deal with radical extensions $F|K$ contained in a given extension field $L \supseteq K$. Separability and degree of $F|K$ have to be studied. We first show

1.13 Proposition

Let $L|K$ be a field extension. The following statements are equivalent:

i) char $K = 0$ or char $K = p$ and $K \cap L^p = K^p$,

ii) every radical extension of K in L is a separable extension.

Proof: i) $\Rightarrow$ ii) Set $x_i = \sqrt[r_i]{a_i}$, $r_i = p^n f_i$, $p \nmid f_i$. Then $a_i \in K \cap L^{p^n} = K^{p^n}$, $a_i = b_i^{p^n}$ for some $b_i \in K$ and $x_i^{f_i} = b_i$. Hence, every x_i is separable over K. ii) $\Rightarrow$ i) Let char $K = p$ and assume $a \in (K \cap L^p) \backslash K^p$. Then $K(\sqrt[p]{a}) \subseteq L$ and $\sqrt[p]{a}$ is not separable over K.

■

The question of the degree of radical extensions has been dealt with in several papers. See [Kn] but also [H1], [H2]. In [Kn] M. Kneser proves a Kummer theory type result without assuming roots of unities in K. We follow his approach. If F is any field we set

$$\begin{aligned} \mu(d, F) &= \{\zeta \in F | \zeta^d = 1\}, \\ \mu(p^\infty, F) &= \bigcup_k \mu(p^k, F), \\ \mu(F) &= \bigcup_d \mu(d, F). \end{aligned}$$

If $F = K(\sqrt[r_1]{a_1}, \ldots, \sqrt[r_n]{a_n})$, we denote by

$$< K^\times, \sqrt[r_1]{a_1}, \ldots, \sqrt[r_n]{a_n} >$$

the subgroup of $F^\times$ generated by $K^\times \cup \{\sqrt[r_1]{a_1}, \ldots, \sqrt[r_n]{a_n}\}$.

This subgroup contains $K^\times$, its factor group modulo $K^\times$ is finite and it generates F as a field extension of K. More generally, we consider a subgroup $C < \overline{K}^\times$ and the field extension $K(C)$ where we assume

$$C/_{K^\times} \text{ is finite.}$$

A set of coset representatives of $C/_{K^\times}$ is a K–basis of $K(C)$. Hence

$$[K(C) : K] \leq [C : K^\times]. \tag{13}$$

1.14 Proposition

If $K(C)|K$ is a separable extension then the following statements are equivalent:

i) $[K(C) : K] = [C : K^\times]$,

ii) *a) for every prime number p we have $\mu(p, \overline{K}) \cap C \subseteq K$,*
b) if $1 + \sqrt{-1} \in C$ then $\sqrt{-1} \in K$.

In the proof Kneser uses the following splitting property. Retain the hypothesis on C and consider a group D satisfying $K^\times < D < C^\times$.

1.15

The following statements are equivalent:

i) $[K(C) : K] = [C : K^\times]$,

ii) a) $[K(D) : K] = [D : K^\times]$,
b) $C \cap K(D)^\times = D$,
c) $[K(C) : K(D)] = [C : D]$.

The proof follows from (13) and this chain of inequalities:

$$\begin{gathered}[C : K^\times] = [K(C) : K] = [K(C) : K(D)][K(D) : K] \leq \\ [K(D)^\times C : K(D)^\times][D : K^\times] = [C : C \cap K(D)^\times][D : K^\times] \leq \\ [C : D][D : K^\times] = [C : K^\times].\end{gathered}$$

■

Maximal ideals of $K[X_1,\dots,X_n]$ are exactly the vanishing ideals of $x = (x_1,\dots,x_n) \in \overline{K}^n$, i.e.

$$\mathfrak{m}_x = \ker(K[X_1,\dots,X_n] \to K(x_1,\dots,x_n)) \text{ where } X_i \mapsto x_i, i = 1,\dots,n.$$

If $x_1 = \dots = x_r = 0$, $\mathfrak{m}' = \ker(K[X_{r+1},\dots,X_n] \to K(x_{r+1},\dots,x_n))$ then $\mathfrak{m}_x = (X_1,\dots,X_r) + \mathfrak{m}'K[X_1,\dots,X_n]$. Hence, in characterizing binomial maximal ideals we may restrict attention to points $x \in (\overline{K}^\times)^n$. x is called separable if $K(x_1,\dots,x_n)$ is a separable field extension.

1.16 Theorem

Let $x \in (\overline{K}^\times)^n$ be a separable point. Then the following statements are equivalent:

i) $\mathfrak{m}_x$ is a binomial ideal,

ii) $[K(x_1,\dots,x_n) : K] = [< K^\times, x_1,\dots,x_n >: K^\times]$.

If $\mathfrak{m}_x$ is binomial then a set of generators is given as follows:

$$X_i^{f_i} - c_i \prod_{j=1}^{i-1} X_j^{r_{ij}}, i = 1,\dots,n,$$

where $c_i \in K^\times$, $f_i = [< K^\times, x_1,\dots,x_i >:< K^\times, x_1,\dots,x_{i-1} >]$ and $x_i^{f_i} = c_i \prod_{j=1}^{i-1} x_j^{r_{ij}}$.

Proof: i) $\Rightarrow$ ii) Set $\mathfrak{m} = \mathfrak{m}_x$. Then the extension ideal $\mathfrak{m}^\pm \lhd K[\underline{X}^\pm]$ is binomial. Hence $\mathfrak{m}^\pm = I(L,\rho)$ where $L = \{\underline{m} | x^{\underline{m}} \in K^\times\}$, $\rho(\underline{m}) = x^{\underline{m}}$ according to (1.7). In addition, $\dim L = n - \dim \mathfrak{m}^\pm = n$. Hence, for each i we find $x_i^{r_i} \in K^\times$ for some $r_i \in \mathbb{N}$. Consequently, $C :=< K^\times, x_1,\dots,x_n >$ has a finite factor group $C/_{K^\times}$ and the character $\rho : \mathbf{Z}^n \to K^\times, \underline{m} \mapsto x^{\underline{m}}$ induces a isomorphism $\mathbf{Z}^n/_L \xrightarrow{\sim} C/_{K^\times}$. The order of the generators $\overline{x}_i = x_i K^\times$ of $C/_{K^\times}$ are prime to the characteristic p of K in case char $K > 0$. In fact, if $x_i^{ps} \in K^\times$ then $x_i^s \in K^\times$ since $K(x_i)/K$ is a separable extension. Thus, if $p =$ char $K > 0$ then $p \not| [\mathbf{Z}^n : L]$. We have $[\mathbf{Z}^n : L] = \mathrm{Hom}_K \left(K[\underline{X}^\pm]/_{I(L,\rho)}, \overline{K} \right) = \# V(I(L,\rho))$. On the other hand

$$V(\mathfrak{m}^\pm) = V(\mathfrak{m}) = \{ y \in K^n | y \text{ conjugate to } x \}.$$

This means $\# V(\mathfrak{m}^\pm) = [K(x_1,\dots,x_n) : K]$ since $K(x_1,\dots,x_n)/K$ is supposed to be separable. Now $[K(x_1,\dots,x_n) : K] = [C : K^\times]$ is proved.
ii) $\Rightarrow$ i) Let us first exploit (1.15). Choose $\gamma \in C$. Then $[K(D)(\gamma) : K(D)] =$

$[< D,\gamma >: D]$, by applying (1.15) first to $< D,\gamma >$ and C and next to $D, < D,\gamma >$. Let $s =$ order of γ mod D. We deduce $\mathrm{Irr}(x, K(D)) = X^s - x^s$. In the situation of our theorem we find

$$\mathrm{Irr}\,(x_i, K(x_1,\ldots,x_{i-1})) = X^{f_i} - c_i \prod_{j=1}^{n} x_j^{r_{ij}}.$$

In particular, $[K(x_1,\ldots,x_n) : K] = f_1 f_2 \ldots f_n$. Let $\mathfrak{a}$ be defined by the polynomials $X_i^{f_i} - c_i \prod\limits_{j=1}^{n} X_j^{r_{ij}}$. Since $\mathfrak{a} \subseteq \mathfrak{m}$ there is an epimorphism $K[X_1,\ldots,X_n]/_{\mathfrak{a}} \twoheadrightarrow K(x_1,\ldots,x_n)$. A Gröbner basis argument shows that $K[X_1,\ldots,X_n]/_{\mathfrak{a}}$ has dimension $f_1 \ldots f_n$, and the epimorphism has to bijective entailing $\mathfrak{a} = \mathfrak{m}$.

■

We want to emphasize that Kneser's result (1.14) provides an easy criterion for checking the equality $[K(C) : K] = [C : K^\times]$.

Separable extensions $K(C)/K$ satisfying this equality allow a strong going–down theorem for binomial ideals which will be used in §4.

1.17 Proposition

Let $K(C)$ be a finite separable field extension of K satisfying $[K(C) : K] = [C : K^\times]$. Let $\mathfrak{b} \lhd K(C)[X_1,\ldots,X_n]$ be a binomial ideal generated by binomials of the type $\underline{X}^{\underline{m}} - c\underline{X}^{\underline{n}}$ with $c \in C \cup \{0\}$. Then

$$\mathfrak{b} \cap K[X_1,\ldots,X_n]$$

is a binomial ideal.

Proof: We have a presentation $K[T_1,\ldots,T_r] \twoheadrightarrow K(C)$, $T_i \mapsto x_i$ with a binomial kernel $\mathfrak{m}$, where $C =< K^\times, x_1,\ldots,x_r >$. If $b = X^{\underline{m}} - cX^{\underline{n}}$ is one of the generators then, by assumption, $c = a\prod\limits_{1}^{r} x_i^{s_i}$, $a \in K$. We assign to b the binomial $\widetilde{b} = X^{\underline{m}} - a\prod T_i^{s_i} \cdot X^{\underline{n}} \in K[T_1,\ldots,T_r,X_1,\ldots,X_n]$. Let $\mathfrak{a} \lhd K[T_1,\ldots,X_n]$ be generated by $\mathfrak{m}$ and all the binomials $\widetilde{b}$ obtained in this way. It is a general fact in ideal theory that $\mathfrak{b} \cap K[X_1,\ldots,X_n] = \mathfrak{a} \cap K[X_1,\ldots,X_n]$. In our present situation, $\mathfrak{b} \cap K[X_1,\ldots,X_n]$ turns out to be an elimination ideal of a binomial ideal, hence is binomial by (1.2), i).

■

2 Radicals of ideals

In this section we introduce various notions of radicals of ideals which naturally appears when algebraic geometry is studied over non–algebraically closed fields. We end up with an axiomatic framework for radical operations. Any such operation assigns an ideal $\mathfrak{a}^*$ to a given ideal $\mathfrak{a}$ subject to certain conditions. The axioms we list seems quite natural. Radical operations studied by Laksov [La1], [La2] and others fit into this framework. In addition, we will characterize those radical operations for which $\mathfrak{a}^*$ is a binomial ideal whenever $\mathfrak{a}$ is of such type, see §3.

Let K denote a field with algebraic closure $\overline{K}$, A an affine K-algebra and $L|K$ any extension. We are interested in the set of all $\overline{K}$-geometric points $V = \mathrm{Hom}_K(A, \overline{K})$ and its set of L-geometric points $V_L = \mathrm{Hom}_K(A, L)$.

In the natural way, A gives rise to rings of functions on V with values in $\overline{K}$ and on V_L with values in L, respectively. Next let $\mathfrak{a}$ be an ideal of A. We set

$$V_L(\mathfrak{a}) = \{x \in V_L | f(x) = 0 \text{ for all } f \in \mathfrak{a}\}, V(\mathfrak{a}) = V_{\overline{K}}(\mathfrak{a})$$

In a natural way,

$$V_L(\mathfrak{a}) = \mathrm{Hom}_K\left({}^{A}\!/\!_{\mathfrak{a}}, L\right).$$

In addition we denote by

$$\sqrt[L]{\mathfrak{a}} = \{f \in A | f = 0 \text{ on } V_L(\mathfrak{a})\}$$

the vanishing ideal of $V_L(\mathfrak{a})$ in A and say that

$$\sqrt[L]{\mathfrak{a}} \text{ is the } L\text{-}radical \text{ } of \text{ } \mathfrak{a}.$$

Now let K be a real(=formally real) field. Then there are field extensions of special interest. The *real closures* of K are the maximal real algebraic extensions of K. If R is a real closure of K then, by the Artin–Schreier theory [BCR], Chap. 1,

2.1

i) R^2 is the unique order of R,

ii) $R \neq \overline{K}$, $R(\sqrt{-1}) = \overline{K}$.

Hence, a real closure R of K induces an order $\alpha := R^2 \cap K$ on K. The Artin–Schreier theory states

2.2

i) every order α on K is induced by a real closure,

ii) two real closures of K are K–conjugate if and only if they induce the same order on K.

If the order α of K is given then a real closure R inducing α is called a *real closure of* α and denoted by R_α. ¿From (2.2) we get that R_α is unique up to conjugacy over K.

The *residue field* $k(x)$ of a point $x \in V(\mathfrak{a})$ is the algebraic extension field $x({}^{A}\!/_{\mathfrak{a}})$ of K. x is called *real* if $k(x)$ is real which is equivalent to requiring $k(x)$ to be contained in some real closure R of K. Hence, the set of real points

$$V_{re}(\mathfrak{a}) = \{x \in V(\mathfrak{a}) | x \text{ real}\}$$

satisfies

$$V_{re}(\mathfrak{a}) = \bigcup V_R(\mathfrak{a}), R \text{ the real closures of } K.$$

The sets $V_{re}(\mathfrak{a})$ and $V_R(\mathfrak{a})$ are the two extremes when considering real points. There is need to consider intermediate cases as can be seen in §4 e.g. To this end we make use of the notion of a preorder τ of K. By definition, cf. [BCR], chap. 1, τ is any subset of K satisfying $\tau + \tau \subseteq \tau, \tau \cdot \tau \subseteq \tau, K^2 \subseteq \tau, -1 \not\in \tau$.

The smallest preorder of a real field is the set of all sums of squares :

$$\sum K^2 := \left\{ \sum_1^r x_i^2 | r \in \mathbb{N}, x_i \in K \right\},$$

the maximal ones are exactly the orders α of K. By the Artin–Schreier theory we have the intersection theorem

$$\tau = \bigcap \alpha, \alpha \text{ order of } K \text{ such that } \tau \subseteq \alpha.$$

We then introduce the *set of* τ*–points*

$$V_\tau(\mathfrak{a}) = \bigcup V_R(\mathfrak{a}), R \text{ the real closures of } K \text{ inducing orders } \alpha \supseteq \tau.$$

If $\tau = \sum K^2$ then $V_\tau(\mathfrak{a}) = V_{re}(\mathfrak{a})$. If $\tau = \alpha$ an order of K and R_α a *fixed* real closure of α then $V_\alpha(\mathfrak{a}) = \{x \in V(\mathfrak{a}) | x \text{ conjugate to a point in } V_{R_\alpha}(\mathfrak{a})\}$.

In general, $V_\tau(\mathfrak{a}) = \bigcup V_\alpha(\mathfrak{a})$ where α ranges over all orders $\alpha \supseteq \tau$. Finally, we define the τ*–radical* $\sqrt[\tau]{\mathfrak{a}}$ of $\mathfrak{a}$ to be the *vanishing ideal* of $V_\tau(\mathfrak{a})$ in A. We have

2.3

i) $\sqrt[\tau]{\mathfrak{a}} = \bigcap\limits_{\alpha \supseteq \tau} \sqrt[\alpha]{\mathfrak{a}}$,

ii) $\sqrt[\alpha]{\mathfrak{a}} = \sqrt[R_\alpha]{\mathfrak{a}}$, R_α any fixed real closures of α.

The first statement follows from the definition, the second one from the description of $V_\alpha(\mathfrak{a})$.

To cover the cases of the various radicals considered so far we introduce the following setting:

Ω an extension field (not necessarily algebraically closed),

$\mathcal{L}$ a family of extension fields of K in Ω.

Then we set

$$V_{\mathcal{L}}(\mathfrak{a}) = \bigcup_{L \in \mathcal{L}} V_L(\mathfrak{a}),$$

$$\sqrt[\mathcal{L}]{\mathfrak{a}} = \text{ vanishing ideal of } V_{\mathcal{L}}(\mathfrak{a}) = \bigcap_{L \in \mathcal{L}} \sqrt[L]{\mathfrak{a}}$$

and call $\sqrt[\mathcal{L}]{\mathfrak{a}}$ the *$\mathcal{L}$–radical* of $\mathfrak{a}$.

In [La1], p. 78. Def. 2 or [La2], p. 324 Laksov introduce a certain radical of an ideal relative to a field extension K a field k denoted by $\sqrt[K]{\mathfrak{a}}$. We do not follow this notation but write $La - \sqrt[K]{\mathfrak{a}}$ for this *Laksov–radical.* Back in our situation we get for any extension field $L|K$

$$La - \sqrt[L]{\mathfrak{a}} \subseteq \sqrt[L]{\mathfrak{a}}.$$

In general, these two radicals differ. However, if L contains $\overline{K}$ or there exist for each $n \in \mathbb{N}$ a polynomial $p_n(X_1, \ldots, X_n)$ such that $V_L(p_n) = \emptyset$ then Laksov's investigations apply to yield

$$La - \sqrt[L]{\mathfrak{a}} = \sqrt[L]{\mathfrak{a}}.$$

In some sense this means that $\sqrt[L]{\mathfrak{a}}$ has found an equational description. For real base fields very distinguished description have been deduced, e.g.

$$\sqrt[\tau]{\mathfrak{a}} = \{f \in A | f^{2N} + \sum_1^s u_i g_i^2 \in \mathfrak{a} \text{ for some } N, s \in \mathbb{N}, u_i \in \tau, g_i \in A\}.$$

This follows from the Artin–Lang homomorphism theorem, cf. [BN], [BCR] but also [BJ] where general results about the K–radical are proved.

$\mathcal{L}$ radicals and Laksov's radical are the prototypes for the general radical operations we are now going to introduce. Let $\mathcal{C}$ be a class of K–algebras closed under forming homomorphic images and quotient rings A_s, $A \in \mathcal{C}$, $s \in A$. A *radical operation* in $\mathcal{C}$ assigns to each algebra A and an ideal $\mathfrak{a} \lhd A$ an ideal $\mathfrak{a}^* \lhd A$ subject to the following

2.4

I) $\mathfrak{a} \subseteq \mathfrak{a}^*$, $(\mathfrak{a}^*)^* = \mathfrak{a}^*$,

II) $\mathfrak{a}^* = \sqrt{\mathfrak{a}^*}$,

III) $(\mathfrak{a} \cap \mathfrak{b})^* = \mathfrak{a}^* \cap \mathfrak{b}^*$,

IV) if $\mathfrak{a}, \mathfrak{b} \lhd A$, $\mathfrak{a} \subseteq \mathfrak{b}$ then $\left({}^{\mathfrak{b}}\!/_{\mathfrak{a}}\right)^* = {}^{\mathfrak{b}^*}\!/_{\mathfrak{a}}$,

V) if $\varphi : A \to B$ is an algebra homomorphism and $\mathfrak{b} \lhd B$ then $(\varphi^{-1}(\mathfrak{b}))^* \subseteq \varphi^{-1}(\mathfrak{b}^*)$,

VI) $(\mathfrak{a}A_s)^* = \mathfrak{a}^* A_s$ for every $\mathfrak{a} \lhd A$, $s \in A$.

We call $\mathfrak{a}^*$ the *$*$-radical* of $\mathfrak{a}$.An ideal $\mathfrak{a}$ satisfying $\mathfrak{a} = \mathfrak{a}^*$ is called *$*$-radical.*

2.5 Proposition

In the class of affine K–algebras the assignments $\mathfrak{a} \mapsto \sqrt[\mathcal{L}]{\mathfrak{a}}$ and $\mathfrak{a} \mapsto La - \sqrt[L]{\mathfrak{a}}$ are radical operations.

Proof:

In the case of $La - \sqrt[L]{\mathfrak{a}}$ the proof can be found in [La1]. We have $\sqrt[\mathcal{L}]{\mathfrak{a}} = \bigcap\limits_{L \in \mathcal{L}} \sqrt[L]{\mathfrak{a}}$. That $\mathfrak{a} \mapsto \sqrt[L]{\mathfrak{a}}$ defines a radical operation is readily checked. The general case follows from the observation that every family of radical operations $\{\mathfrak{a} \mapsto \mathfrak{a}^{*_i}\}_{i \in I}$ gives rise a new radical operation by setting $\mathfrak{a}^* := \bigcap\limits_{i} \mathfrak{a}^{*_i}$.

■

Some radical operations allow a stronger version of VI, namely

$$(\mathfrak{a}A_S)^* = \mathfrak{a}^* A_S$$

for an arbitrary multiplicative semigroup. Examples are $\sqrt[L]{\mathfrak{a}}$, $La - \sqrt[L]{\mathfrak{a}}$ and $\sqrt[T]{\mathfrak{a}}$. Also some satisfy a further axiom

VII) $(\mathfrak{a}A[T])^* = \mathfrak{a}^* A[T]$.

Examples are: $La - \sqrt[L]{\mathfrak{a}}$ if L is infinite, $\sqrt[\mathcal{L}]{\mathfrak{a}}$ if there is no finite bound for the cardinalities of the fields L in $\mathcal{L}$. Hence, $\sqrt{\mathfrak{a}}$, $\sqrt[\tau]{\mathfrak{a}}$ are instances.

A further remark is of interest.If A is noetherian then every minimal prime ideal $\mathfrak{p}$ of $\mathfrak{a}^*$ stisfies $\mathfrak{p} = \mathfrak{p}^*$ as follows from I,III.Hence in this case the $*$-radical is the intersection of $*$-radical prime ideals.

The following result is of great importance for the computation of $*$–radicals of binomial ideals. In the case of a quotient ring A_S with canonical mapping $i : A \longrightarrow A_S, a \mapsto \frac{a}{1}$ and $\mathfrak{a} \lhd A_S$ we write, as usual, $\mathfrak{a} \cap A$ to denote $i^{-1}(\mathfrak{a}) \lhd A$.

2.6 Proposition

Let $s_1, \ldots, s_r \in A$ and $s = s_1 s_2 \ldots s_r$. Then for every radical operation we have

$$\mathfrak{a}^* = [(\mathfrak{a}A_s)^* \cap A] \cap \bigcap_{i=1}^{r} (\mathfrak{a}, s_i)^*.$$

Proof:

Every radical ideal $\mathfrak{b}$ satisfies the identity

$$\mathfrak{b} = (\mathfrak{b}A_s \cap A) \cap \bigcap_i (\mathfrak{b}, s_i).$$

This applies to $\mathfrak{b} = \mathfrak{a}^*$. Since $(\mathfrak{a}A_S)^* = \mathfrak{a}^* A_S$ we get

$$\mathfrak{a}^* = ((\mathfrak{a}A_s)^* \cap A) \cap \bigcap (\mathfrak{a}^*, s_i).$$

Now using I, III we derive

$$\mathfrak{a}^* = \mathfrak{a}^{**} = ((\mathfrak{a}A_s)^* \cap A)^* \cap \bigcap_i (\mathfrak{a}^*, s_i)^*.$$

¿From I, V we deduce $i^{-1}(\mathfrak{a}A_s)^* = [i^{-1}(\mathfrak{a}A_s)]^*$. Using I we find $\mathfrak{a}^* \subseteq (\mathfrak{a}, s_i)^*$ and finally $(\mathfrak{a}^*, s_i)^* = (\mathfrak{a}, s_i)^*$.

■

The last proof essentially used that the $*$–radical is a radical ideal. Much more is true. The decomposition in turn implies that $\mathfrak{a}^*$ is a radical ideal. More precisely, assume the properties I, VI and that $\mathfrak{a}^*$ admits the decomposition of (2.6). We then deduce that $\mathfrak{a}^* = \sqrt{\mathfrak{a}^*}$. In fact, let $s^n \in \mathfrak{a}^*$. Then $(\mathfrak{a}A_s)^* = \mathfrak{a}^* A_s = A_s$. Hence, $\mathfrak{a}^* = (\mathfrak{a}, s)^*$ implying $s \in \mathfrak{a}^*$.

An algebra is said to be $*$–reduced if $(0)^* = 0$. In this terminology, $\mathfrak{a}^*$ is the smallest of the ideals $\mathfrak{b} \supseteq \mathfrak{a}$ such that ${}^{A}\!/_{\mathfrak{b}}$ is $*$–reduced. Axiom V means that pre images of $*$–radical ideals are $*$–radical. It is also equivalent to the "continuity" condition: $\varphi(\mathfrak{a}^*) \subseteq [\varphi(\mathfrak{a})]^*$. Hence, isomorphisms $A \underset{\sim}{\xrightarrow{\varphi}} B$ are compatible with forming the $*$–radical: $\varphi(\mathfrak{a})^* = \varphi(\mathfrak{a}^*)$. Now IV can be generalized as follows: if $\varphi : A \twoheadrightarrow B$ is an epimorphism and $\ker \varphi \subseteq \mathfrak{a}$ then $\varphi(\mathfrak{a}^*) = (\varphi(\mathfrak{a}))^*$.

3 Radicals of binomial ideals

In this section we show that the computation of the $*$–radical of a binomial ideal can be reduced to the determination of the $*$–radicals of ideals of the type $(X_1^{f_1} - a_1, \dots, X_r^{f_r} - a_r) \lhd K[X_1, \dots, X_s], r \leq s, a_i \in K^\times$. If the radical operation even satisfies the axiom VII $-(\mathfrak{a}A[T])^* = \mathfrak{a}^*A[T]^*-$
the $*$–radicals of such ideals with $r = s$ suffice. As a first consequence we get a general characterization of radical operations for which $\mathfrak{a}^*$ is a binomial ideal whenever $\mathfrak{a}$ is binomial. In the subsequent section this general statement will be made more explicit for L–radicals and τ–radicals. We also derive the fact that the cells $V^\Delta(\mathfrak{a})$ and the $*$–radicals of $\mathfrak{a}_\Delta^\pm$ completely determine $\mathfrak{a}^*$. This leads to the algorithms in §5 the basic principles of which are already explained at the end of this section.

3.1 Theorem

Let $\mathfrak{a} \mapsto \mathfrak{a}^*$ be a radical operation on the class of affine K–algebras. Then the following statements are equivalent:

i) for every binomial ideal $\mathfrak{a} \lhd K[X_1, \dots, X_n]$, $n \in \mathbb{N}$ the $*$–radical $\mathfrak{a}^*$ is again binomial,

ii) the $*$–radical is binomial for all ideals of the type

$$a_{r,s} = (X_1^{f_1} - a_1, \dots, X_r^{f_r} - a_r) \lhd K[X_1, \dots, X_s]$$

where $r \leq s$, $a_i \in K^\times$.

If the radical operation additionally satisfies axiom VII, then it is sufficient in ii) to consider the zero–dimensional ideals $a_{r,r}$.

The proof proceeds in various steps. Of course, i) $\Rightarrow$ ii). So let us *assume the hypothesis in ii).* We draw several consequences.

I) $\mathfrak{a} \lhd K[X_1]$, $\mathfrak{a}$ binomial then $\mathfrak{a}^*$ binomial.

Proof: $\mathfrak{a}$ is a principal ideal. Its generator form a Gröbner basis , hence has to be a binomial $X^k(X^l - a)$, $a \in K$ (we set $X = X_1$). If $a = 0$ then $(X^{k+l})^* = \left(\sqrt{(X^{k+l})}\right)^* = (X)^*$. Thus $(X^{k+1})^* = (1)$ or $(X^{k+l})^* = (X)$. If $a \neq 0$ then $(X^k(X^l - a))^* = [(X^k) \cap (X^l - a)]^* = (X^k)^* \cap (X^l - a)^*$ which turns out to binomial.

■

II) $\mathfrak{a} \lhd K[\underline{X}]$, a binomial ideal, $\Delta \subseteq \{1,\dots,n\}$ then

$$\mathfrak{b}_\Delta := (\mathfrak{a}_\Delta K[X_i, X_i^{-1}|i \in \Delta])^* \cap K[X_i|i \in \Delta]$$

and $\pi_\Delta^{-1}(\mathfrak{b}_\Delta)$ are binomial ideals.

Proof: Since $\pi_\Delta^{-1}(\mathfrak{b}_\Delta) = \mathfrak{b}_\Delta K[\underline{X}] + \sum\limits_{i \notin \Delta}(X_i)$ the second claim follows from the first. We may assume $\Delta = \{1,\dots,s\}$. Then

$$\mathfrak{a}_\Delta^\pm = \pi_\Delta(\mathfrak{a})K[X_1,\dots,X_s]_{X_1\dots X_s}$$

Since $\pi_\Delta(\mathfrak{a})$ is binomial ideal we see that set $\mathfrak{c} := \mathfrak{a}_\Delta^\pm$ is a binomial ideal in $K[\underline{K}^\pm]$. Once $\mathfrak{c}^*$ turns out to be binomial we conclude by (6) that $\mathfrak{b}_\Delta$ is a binomial ideal. We choose an automorphism φ (as in §1) of $K[\underline{X}^\pm]$ to transform $\mathfrak{c}$ into an ideal

$$\mathfrak{c}_1 = (X_1^{f_1} - a_1, \dots, X_r^{f_r} - a_r) \lhd K[X_1,\dots,X_s]_{X_1\dots X_s}.$$

Because of $\mathfrak{c}^* = \varphi(\mathfrak{c})^* = \varphi(\mathfrak{c}^*)$ and the fact that binomiality is preserved under φ^{-1} we can restrict attention to $\mathfrak{c}_1$. Clearly, $\mathfrak{c}_1 = \mathfrak{a}_{r,s}K[\underline{X}]_{X_1\dots X_s}$ with $\mathfrak{a}_{r,s}$ as above. Then $\mathfrak{c}_1^* = \mathfrak{a}_{r,s}^*K[\underline{X}]_{X_1\dots X_s}$ and the claim follows from the hypothesis.

■

III) $\mathfrak{a}$ binomial ideal, M a set of monomials then there is a further set of monomials M_1 such that

$$(\mathfrak{a} + (M))^* = \mathfrak{a}^* + (M) + (M_1).$$

The proof makes use of the following facts. Let $\Delta \subseteq \{1,\dots,n\}$, $\mathfrak{a}$ a binomial ideal in $K[X_1,\dots,X_n]$. Then we have

3.2

i) $\left(\mathfrak{a} + \sum\limits_{i \notin \Delta}(X_i)\right)^* = (\pi_\Delta(\mathfrak{a}))^*K[\underline{X}] + \sum\limits_{i \notin \Delta}(X_i),$

ii) $\pi_\Delta(\mathfrak{a}) = (\mathfrak{a} \cap K[X_i|i \in \Delta]) + (M')$ for some set M' of monomials.

Indeed, i) is a consequence of axiom IV for radical operations. The statement ii) follows from a discussion of three possible types of binomial generators of $\mathfrak{a}$, cf. §1.

Proof of III): The claim is correct for $n = 1$ or $M = \emptyset$. Now assume $n \geq 2$ and $M \neq \emptyset$. In view of $(\mathfrak{a} + (M))^* = (\mathfrak{a}^* + (M))^*$ we may assume that $\mathfrak{a}$ is $*$–radical. To make use of an inductive procedure we apply the decomposition of $*$–radicals (2.6) with $r = n$, $f_i = X_i$. Since every monomial in M becomes a unit in $K[\underline{X}^{\pm}]$ we get the decomposition

$$(\mathfrak{a} + (M))^* = \bigcap_{i=1}^{n} (\mathfrak{a} + (M) + (X_i))^*.$$

Applying (3.2) we find, setting $S_i = K[X_j | j \neq i]$:

$$(\mathfrak{a} + (M) + (X_i))^* = [(\mathfrak{a} \cap S_i) + (M') + (M'')]^* K[\underline{X}] + (X_i).$$

The continuity of the radical operation entails that $\mathfrak{a} \cap S_i$ is $*$–radical. Hence, by induction on n:

$$\begin{aligned} (\mathfrak{a} + (M) + (X_i))^* &= (\mathfrak{a} \cap S_i + (M') + (M'') + (M_i''))K[\underline{X}] + (X_i) \\ &= \mathfrak{a} + (M) + (M_i'') + (X_i). \end{aligned}$$

We find that the hypothesis (1.2), iv) is fulfilled hence our claim follows.

■

We are prepared to prove (3.1). Using (2.6) we start with the decomposition

$$\mathfrak{a}^* = [(\mathfrak{a}K[\underline{X}^{\pm}])^* \cap K[\underline{X}]] \cap \bigcap_{i=1}^{n} (\mathfrak{a}, X_i)^*.$$

¿From II we know that $(\mathfrak{a}^{\pm})^* \cap K[\underline{X}]$ is a binomial ideal containing $\mathfrak{a}$. To apply (1.2), iii) directly we should have $(\mathfrak{a}, X_i)^* = \mathfrak{a} + (M_i)$, M_i a set of monomials. However, we compute (using $S_i = K[X_j | j \neq i]$):

$$(\mathfrak{a}, X_i)^* = [(\mathfrak{a} \cap S_i)^* + (M) + (M')]K[\underline{X}] + (X_i).$$

Hence, if $\mathfrak{a} \cap S_i$ is not $*$–radical we cannot expect $(\mathfrak{a}, X_i)^*$ to be of the required type. To put ourselves into the situation that $\mathfrak{a} \cap S_i$ are $*$–radical for every $i = 1, \ldots, n$ we modify $\mathfrak{a}$ without changing the $*$–radical and binomiality. Set

$$\mathfrak{a}_0 = \mathfrak{a}, \mathfrak{a}_{i+1} = \mathfrak{a}_i + \sum_{j=1}^{n} (\mathfrak{a}_i \cap S_j)^* K[\underline{X}].$$

Then

1) each $\mathfrak{a}_i$ is a binomial ideal,

2) $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{a}^*$, hence $\mathfrak{a}_i^* = \mathfrak{a}^*$.

In fact, let $\mathfrak{a}_i$ already satisfy 1), 2). Then the elimination ideal $\mathfrak{a}_i \cap S_j$ is binomial, hence by induction, $(\mathfrak{a}_i \cap S_j)^*$ is a binomial ideal yielding 1) for $\mathfrak{a}_{i+1}$. The continuity of radical operations shows $(\mathfrak{a}_i \cap S_j)^* \subseteq \mathfrak{a}_i^*$, and 2) is proved for $\mathfrak{a}_{i+1}$.

By noetherian induction there is i such that $\mathfrak{a}_i = \mathfrak{a}_{i+1}$ enforcing $(\mathfrak{a}_i \cap S_j)^* = \mathfrak{a}_i \cap S_j$ for every j. Now pass from $\mathfrak{a}$ to $\mathfrak{b} := \mathfrak{a}_i$. Then

$$\mathfrak{a}^* = \mathfrak{b}^* = [(\mathfrak{b}K[X^{\pm}])^* \cap K[X]] \cap \bigcap (\mathfrak{b}, X_i)^*,$$

and now we have $(\mathfrak{b}, X_i)^* = \mathfrak{b} + (M_i') + (X_i)$ for every i. The proof of the equivalence of i) and ii) is complete.

In the radical operation satisfies axiom VII then we get
$(\mathfrak{a}_{r,s})^* = (\mathfrak{a}_{r,r}K[X_1, \ldots, X_r][X_{r+1}, \ldots, X_s])^* = \mathfrak{a}_{r,r}^* K[X_1, \ldots, X_s]$.

■

The method of the last proof suggests an algorithm to compute the $*$-radical even if $\mathfrak{a}^*$ is non binomial. The decomposition

$$\mathfrak{a}^* = [(\mathfrak{a}K[\underline{X}^{\pm}])^* \cap K[\underline{X}]] \cap \bigcap_{i=1}^{n} (\mathfrak{a}, X_i)^*$$

together with the reduction formula (3.2) leads to the following formula

$$\mathfrak{a}^* = \bigcap_{\Delta \subseteq \{1,\ldots,n\}} \pi_\Delta^{-1} \left(\left(\mathfrak{a}_\Delta^{\pm} \right)^* \cap K[X_i | i \in \Delta] \right)$$

Of course,only those subsets with $V^\Delta(\mathfrak{a}) \neq \emptyset$ need to be considered.This formula propose the following basic algorithm.

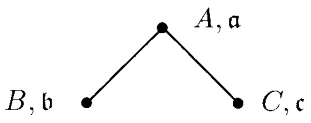
1st step: determine all non empty cells,

2nd step: compute for each non-empty cell the $*$-radical $(\mathfrak{a}_\Delta^{\pm})^*$,

3rd step: compute contraction and intersection of ideals by Gröbner basis techniques

At this moment, the use of (possibly very expensive) Gröbner basis methods cannot be avoided. There are ways to reduce the number of cells to be considered. Details will follow in §5, here we only outline the basic idea.

We built up a binary tree each node of which stands for an affine K–algebra A together with an ideal $\mathfrak{a}$ of it. The branching at a node runs as follows:



(14)

where for some $s \in A$:

$$B = A_s, \mathfrak{b} = \mathfrak{a}A_s$$

$$C = {}^{A}\!\Big/_{(s)}, \mathfrak{c} = {}^{\mathfrak{a}+(s)}\!\Big/_{(s)}.$$

For every radical operation we deduce

$$\mathfrak{a}^* = (\mathfrak{b}^* \cap A) \cap \pi^{-1}(\mathfrak{c}^*)$$

with $\pi : A \to C$ the canonical epimorphism.

The root of our tree will be the polynomial ring $K[X_1, \ldots, X_n]$ and the ideal $\mathfrak{a}$, the terminal nodes (= leaves) the affine algebras $K[X_i, X_i^{-1}|i \in \Delta]$, $\Delta \subseteq \{1, \ldots, n\}$ and the ideals $\mathfrak{a}^{\pm}_{\Delta} = \pi_{\Delta} K[X_i, X_i^{-1}|i \in \Delta]$. The tree then allows to transfer back information from the leaves to the root, this means from the algebras $K[X_k, X_i^{-1}|i \in \Delta]$ and ideals $\mathfrak{a}^{\pm}_{\Delta}$ back to $K[X_1, \ldots, X_n]$ and $\mathfrak{a}$.

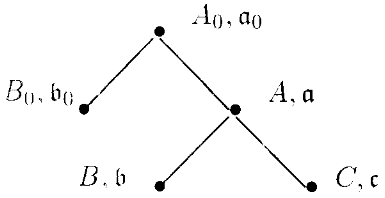
To present the tree we parametrize the nodes by a pair (Γ, Λ) of subsets of $\{1, \ldots, n\}$ subject to the condition $\Gamma \cap \Lambda = \emptyset$. The algebra at the node (Γ, Λ) is

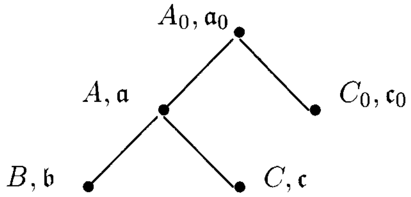
$$A_{\Gamma,\Lambda} = K[X_i, X_i^{-1}|i \in \Gamma][X_j|j \in \Lambda]$$

and the ideal

$$\mathfrak{a}_{\Gamma,\Lambda} = \pi_{\Gamma\cup\Lambda}(\mathfrak{a})A_{\Gamma,\Lambda}.$$

The root belongs to $(\emptyset, \{1, \ldots, n\})$. If $\Lambda = \emptyset$ we have reached a leaf. If $\Lambda \neq \emptyset$ we choose $i \in \Lambda$ and pass to the nodes $(\Gamma \cup \{i\}, \Lambda \backslash \{i\})$ and $(\Gamma, \Lambda \backslash \{i\})$. Using the general notation from above we have $A = C[X_i]$, $B = C[X_i, X_i^{-1}]$ and $\pi^{-1}(\mathfrak{c}^*) = \mathfrak{c}^* A + (X_i)$. This tree can be built for any ideal $\mathfrak{a} \lhd K[X_1, \ldots, X_n]$. But in general it seems of little importance since we will have to consider all the 2^n leaves. In the case of binomial ideals however the combinatorial structure of a set of binomial generators allow to discard several nodes right from the beginning. Again, details will be presented in §5. Here, we give the basic principle. Let us consider two situations:





as in (14).

Assume first $\mathfrak{a}^* = A$ then $\mathfrak{b}^* = (\mathfrak{a}B)^* = \mathfrak{a}^*B = B$ and $\mathfrak{c}^* = \left(\mathfrak{a} + (s)/_{(s)}\right)^* = (\mathfrak{a} + (s))^*/_{(s)} = C$. Furthermore $\mathfrak{a}_0^* = (\mathfrak{b}_0^* \cap A_0) \cap \pi^{-1}(\mathfrak{a}^*) = \mathfrak{b}_0^* \cap A_0$ or $\mathfrak{a}_0^* = \pi^{-1}(\mathfrak{c}_0^*)$. Hence, if there is an a–priori knowledge that $\mathfrak{a}^* = A$ the node $(A, \mathfrak{a})$ and its successors can be discarded.

Next let us assume $\mathfrak{a} = \mathfrak{c}C[X_i]$ and that the radical operation satisfies axiom VII. Then $\mathfrak{a}^* = \mathfrak{c}^*C[X_i], \mathfrak{b}^* = \mathfrak{c}^*C[X_i, X_i^{-1}]$ and $\mathfrak{b}^* \cap A = \mathfrak{a}^*$. Thus,either the node $(B, \mathfrak{b})$ or the node $(C, \mathfrak{c})$ can be deleted.

4 L–radicals and τ–radicals

In this section we characterize the field extensions $L|K$ and the preorders τ of K such that for every binomial ideal the corresponding radicals are again binomial ideals. To treat special cases we need the following fact.

4.1 Lemma

Let $f_1(T), \ldots, f_n(T) \in K[T]$ be polynomials with no multiple roots. Then every ideal $\mathfrak{a} \lhd K[X_1, \ldots, X_n]$ with $(f_1(X_1), \ldots, f_n(X_n)) \subseteq \mathfrak{a}$ is a radical ideal.

Proof: $A := K[\underline{X}]/(f_1(X_1), \ldots, f_n(X_n))$ is a finite–dimensional separable algebra, hence a product of finitely many fields. Now $K[\underline{X}]/_{\mathfrak{a}}$ is a factor algebra of A, thus a product of fields itself. This means that $\mathfrak{a}$ is radical.

■

4.2 Proposition

Let L be a finite field, $\#L = q$, and $\mathfrak{a} \lhd K[\underline{X}]$ an arbitrary ideal. Then

$$\sqrt[L]{\mathfrak{a}} = (\mathfrak{a}, X_1^q - X_1, \ldots, X_n^q - X_n).$$

If $\mathfrak{a}$ is binomial the same is true for $\sqrt[L]{\mathfrak{a}}$.

Proof: Set $\mathfrak{b} = (\mathfrak{a}, X_1^q - X_1, \dots, X_n^q - X_n)$. Then clearly, $\mathfrak{b} \subseteq \sqrt[L]{\mathfrak{a}}$ and $V(\mathfrak{b}) = V_L(\mathfrak{a})$. By definition, $\sqrt[L]{\mathfrak{a}} =$ vanishing ideal of $V_L(\mathfrak{a})$. So it remains to show that $\mathfrak{b}$ is a radical ideal. But this follows from (4.1). The final claim is obvious.

■

We now consider the L–radical of an ideal $\mathfrak{a} = (X_1^{r_1} - a_1, \dots, X_n^{r_n} - a_n) \lhd K[X_1, \dots, X_n]$ where $a_1, \dots, a_n \in K^\times$. Set

$$e_i = \#\mu(r_i, L), i = 1, \dots, n \tag{15}$$

Then $e_i | r_i$, $p \not| e_i$ if char $K = p > 0$, and

$$\mu(e_i) := \mu(e_i, \overline{K}) = \mu(r_i, L). \tag{16}$$

Let $V_L(\mathfrak{a}) \neq \emptyset$. pick any $(x_1, \dots, x_n) \in V_L(\mathfrak{a})$. Then

$$V_L(\mathfrak{a}) = \{(x_1\zeta_1, \dots, x_n\zeta_n) | \zeta_i^{e_i} = 1 \text{ for } i = 1, \dots, n\} \tag{17}$$

since $\mu(r_i, L) = \mu(e_i)$. We further obtain

$$V(\sqrt[L]{\mathfrak{a}}) = \{x \in \overline{K}^n | x \text{ conjugate to some } y \in V_L(\mathfrak{a})\}. \tag{18}$$

We first consider a simple case.

4.3

Assume $V_K(\mathfrak{a}) \neq \emptyset$. Choose any $(x_1, \dots, x_n) \in V_K(\mathfrak{a})$. Then $\sqrt[L]{\mathfrak{a}} = (X_1^{e_1} - x_1^{e_1}, \dots, X_n^{e_n} - x_n^{e_n})$.

Proof: Both ideals have the same set of zeros in $\overline{K}^n$, and both are radical ideals, use (4.1).

■

4.4 Theorem *cf. [EiSt]*

The K–radical of every binomial ideal is a binomial ideal.

Proof: If K is finite, (4.2) gives the result. If K is infinite, in view of (3.1), we have to prove the claim for ideals $\mathfrak{a} = (X_1^{r_1} - a_1, \dots, X_n^{r_n} - a_n) \lhd K[X_1, \dots, X_n]$, $a_1, \dots, a_n \in K^\times$. But this is (4.3) or $V_K(\mathfrak{a}) = \emptyset$, $\sqrt[K]{\mathfrak{a}} = (1)$.
■

In general, L–radicals of binomial ideals need not be binomial again. We deduce a first necessary condition.

4.5

If $\sqrt[L]{\mathfrak{a}}$ is binomial for every binomial ideal then either char $K = 0$ or char $K = p$ and $K \cap L^p = K^p$.

Proof: Assume char $K = p > 0$ and let $a \in (K \cap L^p)\backslash K^p$. Then consider $\mathfrak{a} = (X^p - a, Y^p - (1+a))$. These generators from a Gröbner basis of $\mathfrak{a}$. Consequently, $X - Y + 1$ does not lie in $\mathfrak{a}$. However, $(X-Y+1)^p = (X^p - a) - (Y^p - (1+a)) \in \mathfrak{a}$ hence $X - Y + 1 \in \sqrt[L]{\mathfrak{a}}\backslash\mathfrak{a}$. We find $(X^p - a, X - Y + 1) = \sqrt[L]{\mathfrak{a}}$. Since the two given generators form a reduced Gröbner basis the L–radical is not a binomial ideal.

■

Note that the condition "$K \cap L^p = K^p$" is satisfied trivially if $K = L$ or if $L|K$ is a separable algebraic field extension.

We return to the study of the L–radical of an ideal $\mathfrak{a} = (X_1^{r_1} - a_1, \dots, X_n^{r_n} - a_n) \lhd K[X_1, \dots, X_n]$ where $a_1, \dots, a_n \in K^\times$ and the convention (15) is retained. In this situation we prove

4.6 Proposition

Assume char $K = 0$ or char $K = p > 0$ and $K \cap L^p = K^p$. Let $(x_1, \dots, x_n) \in V_L(\mathfrak{a})$. The following statements are equivalent:

i) $\sqrt[L]{\mathfrak{a}}$ is a binomial ideal,

ii) $[K(x_1^{e_1}, \dots, x_n^{e_n}) : K] = [< K^\times, x_1^{e_1}, \dots, x_n^{e_n} >: K^\times]$.

If $\sqrt[L]{(X_1^{r_1} - a_1, \dots, X^{r_n} - a_n)}$ is binomial a set of generators is given as follows:

$$X_i^{e_i f_i} - c_i \prod_{j=1}^{i-1} X_j^{e_j r_{ij}}, i = 1, \dots, n$$

where $c_i \in K^\times, f_i = [< K^\times, x_1^{e_1}, \dots, x_i^{e_i} >:< K^\times, x_1^{e_1}, \dots, x_{i-1}^{e_{i-1}} >]$ and $x_i^{e_i f_i} = c_i \prod\limits_{j=1}^{i-1} x_j^{e_j r_{ij}}$.

Proof: ¿From $V_L(\mathfrak{a}) \subseteq (K^\times)^n$ we deduce $\sqrt[L]{\mathfrak{a}} = \sqrt[L]{\mathfrak{a}^\pm} \cap K[\underline{X}]$. Hence, $\sqrt[L]{\mathfrak{a}}$ is binomial iff $\sqrt[L]{\mathfrak{a}^\pm}$ is of this type. The binomial ideals in $K[\underline{X}^\pm]$ are of the type $I(G, \rho)$, G a sublattice of $\mathbf{Z}^n$ and $\rho : G \to K^\times$ a character. To characterize the ideals $I(G, \rho) \subseteq \sqrt[L]{\mathfrak{a}^\pm}$ we have to consider the group $L^\times/_{K^\times}$. If $x \in L^\times$ we set $\overline{x} = xK^\times \in L^\times/_{K^\times}$.

Set

$$G := \left\{ (e_1 s_1, \ldots, e_i s_i, \ldots, e_n s_n) \in \mathbb{Z}^n | \prod_{i=1}^{n} (\overline{x}_i^{e_i})^{s_i} = 1 \right\}.$$

G is a lattice of finite index. We set

$$U =< K^\times, x_1^{e_1}, \ldots, x_n^{e_n} >$$

and define the character

$$\rho : \mathbb{Z}^n \to L^\times, \underline{m} = (m_1, \ldots, m_n) \mapsto \prod_1^n x_i^{m_i}.$$

Then $\rho(e_1\mathbb{Z} \times \ldots \times e_n\mathbb{Z}) = U$, $G = (e_1\mathbb{Z} \times \ldots \times e_n\mathbb{Z}) \cap \rho^{-1}(K^\times)$, hence $[\mathbb{Z}^n : G] = e_1 e_2 \ldots e_n [U : K^\times]$.

We now claim:

$$I(G', \rho') \subseteq \sqrt[L]{\mathfrak{a}^\pm} \Leftrightarrow G' \subseteq G, \rho' = \rho/_{G'}. \tag{19}$$

Proof of (19): We know $V_L(\mathfrak{a}^\pm)$ from (22). "$\Leftarrow$ We find $(\underline{X}^{\underline{m}} - \rho(\underline{m}))(x_1\zeta_1, \ldots, x_n\zeta_n) = (\prod (x_i^{e_i})^{s_i}) - \rho(e_1 s_1, \ldots, e_n s_n) = 0$ "$\Rightarrow$. If $\underline{X}^{\underline{m}} - \rho'(\underline{m}) \in \sqrt[L]{\mathfrak{a}^\pm}$ then for every choice of $\zeta_i \in \mu(e_i), i = 1, \ldots, n$ we must have $\prod_1^n (x_i\zeta_i)^{m_i} = \rho'(\underline{m})$ entailing $\zeta_i^{m_i} = 1$ for $i = 1, \ldots, n$. This implies $m_i = e_i s_i$ and $\rho'(\underline{m}) = \rho(\underline{m})$. (19) is proved.

Hence. $I(G, \rho)$ is the largest binomial ideal contained in $\sqrt[L]{\mathfrak{a}^\pm}$. To study when $I(G, \rho) = \sqrt[L]{\mathfrak{a}^\pm}$ we first note that $I(G, \rho)$ is a radical ideal. In fact, from §1, (11) we know

$$K[\underline{X}^\pm]\big/_{I(G, \rho)} \simeq K[X_1, \ldots, X_n]\big/_{(X_1^{f_1} - b_1, \ldots, X_n^{f_n} - b_n)} =: A$$

with $f_1 \ldots f_n = [\mathbb{Z}^n : G] = e_1 \ldots e_n [U : K^\times]$. If char $K = 0$, A is a reduced algebra by (4.1). If char $K = p > 0$, then we first recall that $p \not| e_i$ for $i = 1, \ldots, n$. Using the assumption that $K \cap L^p = K^p$ we deduce that $U/_{K^\times}$ has no p-torsion. This means that no f_i is divisible by p, hence A is reduced by (4.1).

We now prove i) $\Rightarrow$ ii). Then $\#V(I(G, \rho)) = \#V(\sqrt[L]{\mathfrak{a}^\pm})$. Using the structure of $K[X^\pm]\big/_{I(G.\rho)}$ we find

$$\#V(I(G, \rho)) = [\mathbb{Z}^n : G] = e_1 \ldots e_n [U : K^\times].$$

Set $F = K(x_1^e, \ldots, x_n^{e_n})$. We prove: $\#V(\sqrt[L]{\mathfrak{a}^\pm}) \leq e_1 \ldots e_n [F : K]$. In fact, let $\beta := (\beta_1, \ldots, \beta_n)$ be conjugate to a point $(x_1', \ldots, x_n') \in V_L(\mathfrak{a}^\pm)$. Then there is $\varphi \in \mathrm{Aut}(\overline{K}|K)$ and there are $\zeta_i \in \mu(e_i), i = 1, \ldots, n$ such that $\varphi(x_i\zeta_i) = \beta_i$. We find $\varphi(x_i^{e_i}) = \beta_i^{e_i}$. Thus β induces a homomorphism $\varphi_\beta : F \to \overline{K}$, $x_i^{e_i} \mapsto \beta_i^{e_i}$. There are at most $[F : K]$ such homomorphisms. If $\varphi_\beta = \varphi_\gamma$ then $\beta_i^{e_i} = \gamma_i^{e_i}$, hence $\beta_i = \gamma_i\zeta_i$, $\zeta_i \in \mu(e_i)$ for $i = 1, \ldots, n$. This proves the claim for $\#V(\sqrt[L]{\mathfrak{a}^\pm})$. Hence $[U : K^\times] \leq [F : K]$, showing equality by §1, (13).

ii) $\Rightarrow$ i) $F = K(x_1^{e_1}, \ldots, x_n^{e_n})$ is a separable extension satisfying the hypothesis of (1.17). We have $\sqrt[L]{\mathfrak{a}} = \sqrt[L]{\mathfrak{a} \otimes F} \cap K[\underline{X}]$. Clearly

$$\mathfrak{a}' := (X_1^{e_1} - x_1^{e_1}, \ldots, X_n^{e_n} - x_n^{e_n} \subseteq \mathfrak{b} := \sqrt[L]{\mathfrak{a} \otimes F}$$

. The reduced algebra $F[\underline{X}]/_{\mathfrak{a}'}$ has dimension $\#V_L(\mathfrak{a} \otimes F) = \#V_L(\mathfrak{a}) = e_1 \ldots e_n$ which is also the dimension of $F[\underline{X}]/_{\mathfrak{b}}$. Hence, the canonical epimorphism $F[\underline{X}]/_{\mathfrak{a}'} \twoheadrightarrow F[X]/_{\mathfrak{b}}$ is an isomorphism yielding $\mathfrak{a}' = \mathfrak{b}$. Now (1.17) completes the proof.

To deduce that the given polynomials form a set of generators the proof of the corresponding claim of (1.16) can be adopted. This time we use that

$$\dim_K {K[X]}/_{\sqrt[L]{\mathfrak{a}}} = \#V(\sqrt[L]{\mathfrak{a}}) = e_1 \ldots e_n[< K^\times, x_1^{e_1}, \ldots, x_n^{e_n} >: K^\times]$$

.

■

This last proposition allows a characterization of the extensions $L|K$ such that the $L-$radical of any binomial ideal in $K[X_1, \ldots, X_n]$ is again a binomial ideal To prepare this theorem we first derive necessary conditions.
Let $\#\mu(r, L) = e$ and let l be a prime number dividing $\frac{r}{e}$ and $l \neq char K$. Then $\mu(e, L) = \mu(el, L)$,hence

$$\#\mu(l^\infty, L) = l^k \text{ where } l^k \text{ is the largest power of } l \text{ dividing } e$$

In a first case, let l be odd and ζ be a primitive $l-$th root of unity.Assume

$$L^{l^k} \cap < K^\times, \zeta > \nsubseteq K$$

Then $x^{l^k} = a\zeta$ where $a \in K^\times, \zeta \notin K$. By the previous proposition, we get that

$$\sqrt[L]{\left(X^{l^{k+1}} - a^l\right)}$$

is not a binomial ideal.
In the second case let $l = 2$ and set $i = \sqrt{-1}$.Assume that

$$L^{2^k} \cap < K^\times, 1 + i > \nsubseteq K$$

Then $x^{2^k} = a(1 + i)$ where $a \in K^\times, i \notin K$.From (4.6), we find that

$$\sqrt[L]{\left(X^{2^{k+2}} + 4a^4\right)}$$

is not a binomial ideal.

4.7 Theorem

Let $L|K$ be any field extension. The following statements are equivalent:

i) the $L-$radical of every binomial ideal is a binomial ideal,

ii) 1) either $char(K) = 0$ or $char(K) = p$ and $L^p \cap K = K^p$,

2) for all odd primes l such that $1 < \#\mu(l^\infty, L) = l^k < \infty$ we have

$$L^{l^k} \cap < K^\times, \zeta > \subseteq K$$

where ζ is a primitive $l-$th root of unity,

3) if $4 \leq \#\mu(2^\infty, L) = 2^k < \infty$ then $L^{2^k} \cap < K^\times, 1 + \sqrt{-1} > \subseteq K$

If 1) holds and either a) $L = K$ or b) $\mu(L) = \mu(\overline{K})$ or c) $\mu(L) = \mu(K)$ the $L-$radical of a binomial ideal is binomial. The (usual) radical of every binomial ideal is binomial if and only if K is a perfect field.

Proof: That the conditions in ii) are necessary was shown above,use also (4.5).Now we show that they are sufficient. We have to verify the condition ii) of (4.6). In view of assumption 2) we may assume that, if $charK = p > 0$,p does not divide any of the r_i. Using the notation used there set $C :=< K^\times, x_1^{e_1}, \ldots, x_n^{e_n} >$. We let ζ be a primitive $l-$th root of unity,l odd.We want to apply (1.14),i.e we have to show that $\zeta \in K$ if $\zeta \in C$ is assumed. If for all i we have $e_i = r_i$ then $C = K^\times$.Next assume that some $e_i < r_i$ and that $\zeta \in C$. Since $(x_j^{e_j})^{r_j/e_j} \in K^\times$ and there is only need to consider the $l-$primary part of $C/K^\times$ we can restrict attention to those $i-$'s such that $l|(r_i/e_i)$. As said above $l \neq charK$.Furthermore,from the arguments before(4.7) we derive $l^k|e_i$.Now the assumption 2) yields that $\zeta \in K$.The corresponding test for the element $1 + \sqrt{-1}$ is seen to positive in the same way.Thus the equality in ii) of (4.6) holds and the equivalence of i) and ii) is proved. The remaining statements readily follow.

■

A prominent example for case b) is $L = K_{sep}$, the separable closure of K, and examples for case c) are provided by the real closures R of a real field since $\mu(R) = \mu(K) = \{\pm 1\}$. To see field extensions L such that not every L-radical of a binomial ideal is binomial we can take the following examples.

I) $K = \mathbb{Q}$ p an odd prime number, $a \in \mathbb{Q} \backslash \mathbb{Q}^p$, ζ a p–th root of unity, $\zeta \neq 1$. $L = \mathbb{Q}(\sqrt[p]{a\zeta})$, $\mathfrak{a} = (X^{p^2} - a^p)$, and

$$\sqrt[L]{\mathfrak{a}} = \left((X^{p^2} - a^p)/(X^p - a)\right).$$

II) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[4]{1+i})$, $\mathfrak{a} = (X^{16}+4)$. Then
$\sqrt[L]{(X^{16}+4)} = (X^8 - 2X^4 + 2)$.

We now turn to the consideration of τ–radicals, τ a preorder of K. In particular, K is assumed to be **real** throughout the rest of this section. Recall from §2 that $V_\tau(\mathfrak{a}) = \bigcup V_R(\mathfrak{a})$, where R ranges over the real closures of K inducing an order $\alpha \supseteq \tau$, i.e. $\tau \subseteq R^2$. $\sqrt[\tau]{\mathfrak{a}}$ is the vanishing ideal of $V_\tau(\mathfrak{a})$:

$$\sqrt[\tau]{\mathfrak{a}} = \bigcap \sqrt[\alpha]{\mathfrak{a}}$$

where α ranges over the orders containing τ. We first deal with special cases.

4.8 Proposition

If α is an order of K, $\mathfrak{a} \lhd K[\underline{X}]$ a binomial ideal then $\sqrt[\alpha]{\mathfrak{a}}$ is a binomial ideal.

Proof: In (2.3) we showed $\sqrt[\alpha]{\mathfrak{a}} = \sqrt[R]{\mathfrak{a}}$, R a real closure of α. As already remarked, $L = R$ satisfies the condition c) of 4.7 .

■

We first treat univariate ideals.

Let $a \in K^\times$. One readily checks that there is a unique largest divisor $d|n$ such that $a \in (K^\times)^d$. Assume $a = b^d$. If d is odd b is uniquely determined since K is real, otherwise up to a factor -1.

4.9 Proposition

Let $n \in \mathbb{N}$, $a \in K^\times$, $V_\tau(X^n - a) \neq \emptyset$ and d the maximal divisor of n such that $a \in K^d$. Then for some $b \in K$ such that $a = b^d$ we get

$$\sqrt[\tau]{(X^n - a)} = \begin{cases} \left(X^{\frac{n}{d}} - b\right) & \textit{if } d \textit{ is odd,} \\ \left.\begin{matrix} \left(X^{\frac{n}{d}} - b\right) \\ \left(X^{2\frac{n}{d}} - b^2\right) \end{matrix}\right\} & \textit{if } d \textit{ is even.} \end{cases}$$

If d is odd then $X^{\frac{n}{d}} - b$ is irreducible over K, if d is even both polynomials $X^{\frac{n}{d}} \pm b$ are irreducible over K.

Proof: Let $V_\tau(X^n - a) = \{x_1, \ldots, x_r\}$. Clearly,
$\sqrt[\tau]{(X^n - a)} = \bigcap\limits_i (Irr(x_i, K))$. Let x be one of the roots. Since $K(x)$ is a real field and $x^n \in K^\times$ Kneser's result (1.14) applies and states $[K(x) : K] =$ ord of $xK^\times$ in $K(x)^\times/_{K^\times} =: s$. Then $\mathrm{Irr}(x, K) = X^s - x^s$. We deduce $a = (x^s)^{\frac{n}{s}} \in K^{\frac{n}{s}}$, hence $\frac{n}{s}\big|d$, i.e. $\frac{n}{d}\big|s$. Now, $x^n = a = b^d$, $d|n$ implies

$x^{\frac{n}{d}} = \pm b$ since $K(x)$ is a real field. This means $s|\frac{n}{d}$, altogether $s = \frac{n}{d}$ and $\mathrm{Irr}(x, K) = X^{\frac{n}{d}} - b$ if d is odd, $\mathrm{Irr}(x, K) = X^{\frac{n}{d}} \pm b$ otherwise. In the case of d being odd we deduce $\sqrt[\tau]{(X^n - a)} = \left(X^{\frac{n}{d}} - b\right)$. Otherwise, d, hence n, is even. Suppose both polynomials $X^{\frac{n}{d}} \pm b$ occur as $\mathrm{Irr}(x_i, K)$. Then $\sqrt[\tau]{(X^n - a)} = \left(X^{2\frac{n}{d}} - b^2\right)$. Then let only $X^{\frac{n}{d}} - b$ occur for the x_i's. We find $\sqrt[\tau]{(X^n - a)} = X^{\frac{n}{d}} - b$. Finally assume that $X^{\frac{n}{d}} + b$ were reducible. By the theory of the pure equation, cf. [L] e.g. either $-b \in K^p$ for some $p|\frac{n}{d}$ or $4|\frac{n}{d}$ and $-b = -4c^4$ for some $c \in K$. Having that d is even we find $a \in K^{pd}$ or $a \in K^{2d}$: both are contradictions.

■

The τ-radicals of bivariate binomial ideals are no longer binomial ideals in general. The study of the bivariate case already discloses the properties of the preorder τ to guarantee binomial τ–radicals. We need certain notions and techniques of the theory of real fields, consult [Lam] or [KnS].

Let τ be a preorder of K. Each order $\alpha \supseteq \tau$ gives rise to the subgroup $\alpha^* := \alpha\backslash\{0\} < K^\times$. α^* is even closed under addition. Clearly, a subgroup $U < K^\times$ which is closed under addition cannot contain -1. A preorder τ is called a *fan* if every subgroup $U < K^\times$ not containing -1 is of the form $U = \alpha^*$ for some order $\alpha \supseteq \tau$.

Fans can be characterized in various ways. They have proved to be of great importance in the theory of real fields and real algebraic geometry, cf. [ABrR]. They are intimately related to the valuation theory of the field, a fact that will be used later. To introduce a further characterization we set

$$\tau[a] = \{t_1 + t_2 a | t_1, t_2 \in \tau\}.$$

This set $\tau[a]$ is a preorder iff $-1 \notin \tau[a]$ iff $a \notin -\tau$. In this case, $\tau[a]$ is the preorder generated by τ and a and we have

$$\tau[a] = \bigcap_{\tau \subseteq \alpha, a \in \alpha} \alpha.$$

Obviously, $\tau \cup \tau a \subseteq \tau[a]$. In [Lam], §5 we find the following statements:

4.10

i) τ is a fan iff $\tau[a] = \tau \cup \tau a$ for every $a \in K\backslash(-\tau)$,

ii) every order α and the intersection of two orders $\tau = \alpha \cap \beta$ are fans, the socalled trivial fans,

iii) if τ, σ are preorders of K, $\tau \subseteq \sigma$ and τ a fan then σ is a fan.

We can now state

4.11 Theorem

The following statements are equivalent:

i) the τ–radical of every binomial ideal is a binomial ideal,

ii) τ is a fan.

The proof proceeds in various steps. We first show the easier implication i) $\Rightarrow$ ii). To this end we consider the binomial ideal $\mathfrak{a} = (X^4 - a^2, Y^4 - b^2)$ in $K[X, Y]$ where $a, b \neq 0$. We claim:

$$\text{if } \sqrt[\tau]{\mathfrak{a}} \text{ is a binomial ideal} \neq 1 \text{ then } \#V_\tau(\mathfrak{a}) \text{ divides } 16.$$

Assume $\sqrt[\tau]{\mathfrak{a}}$ binomial then $(\sqrt[\tau]{\mathfrak{a}})^\pm = \sqrt[\tau]{\mathfrak{a}^\pm} = I(L, \rho)$, $V(\sqrt[\tau]{\mathfrak{a}}) = V(\sqrt[\tau]{\mathfrak{a}^\pm})$ and $\#V(\sqrt[\tau]{\mathfrak{a}}) = [\mathbf{Z}^n : L]$. ¿From $4\mathbf{Z}^2 \subseteq L$ we find $[\mathbf{Z}^n : L] | 16$. On the other hand, $V_\tau(\mathfrak{a})$ is closed under conjugation over K. Hence, $V(\sqrt[\tau]{\mathfrak{a}}) = V_\tau(\mathfrak{a})$.

Next assume that τ is not a fan. By definition, there is $a \in K^\times \backslash (-\tau)$ such that $\tau \cup \tau a \subsetneqq \tau[a]$. Choose $b \in \tau[a] \backslash (\tau \cup \tau a)$. We claim: $b \notin \tau[-a]$, $b \notin -\tau[-a]$. Otherwise, in the first case, $b = t_1 - t_2 a$, $t_i \in \tau$ and $b = t_3 + t_4 a$. We obtain $b(t_2 + t_4) = t_4 t_1 + t_2 t_3$, thus $b \in \tau$: a contradiction. In a similiar way we show $b \notin -\tau[-a]$. As a consequence we find orders $\alpha, \beta, \gamma \supseteq \tau$ satisfying

$$a, b \in \alpha; -a, b \in \beta; -a, -b \in \gamma.$$

¿From $b \in \tau[a]$ we deduce that there is no order $\delta \supseteq \tau$ with $a, -b \in \delta$.

For this choice of a, b we will conclude that $\#V_\tau(\mathfrak{a}) = 12$. In fact, in any real closure R of K $\mathfrak{a}$ has exactly 4 solutions if not $V_R(\mathfrak{a}) = \emptyset$. In $R_\alpha \cup R_\beta \cup R_\gamma$ we find 12 solutions. The remaining 4 zeros of $\mathfrak{a}$ in $\overline{K}$, namely $(\pm\sqrt{a}, \pm\sqrt{-b})$, cannot lie in a real closure R_δ of an order $\delta \supseteq \tau$ since this would imply $a, -b \in \delta$. Thus, i) $\Rightarrow$ ii) is proved.

To derive the implication ii) $\Rightarrow$ i) it is sufficient to study the τ–radicals of zero–dimensional ideals

$$\mathfrak{a} = (X_1^{r_1} - a_1, \ldots, X_n^{r_n} - a_n) \lhd K[X_1, \ldots, X_n], a_i \in K^\times.$$

We will show by induction on the number n and for fixed n on $r := r_1 \cdot \ldots \cdot r_n$ that for every real field K, every fan τ in K and every ideal of this type the τ–radical is again a binomial ideal. To get to smaller values of r we will have to pass from τ to other fans τ'. In particular, τ' may be an extension of τ to an extension field, i.e. $\tau' \cap K = \tau$. Therefore we need results about the extension of fans to extension fields. This is usually done by using Bröcker's trivialization theorem for fans [Lam], §12 or [ABrR], chapt. VI),1 which reduces the problem mainly to valuation theory. For more details we refer to the literature cited already and [B], ch. IV, §2 where extension theorems are proved.

4.12 Proposition

Let p be a prime number, $a \in K$, $F = K(\sqrt[p]{a})$ a real field and $\tau \subseteq K$ a fan. In case $p = 2$ assume $a \in \tau$. Define $\tau' \subseteq F$ as follows: $\tau' = \bigcap \alpha'$, where α' ranges over all orders of F satisfying $\alpha' \cap K \supseteq \tau$, and, in addition, if $p = 2$: $\sqrt{a} \in \alpha'$. Then τ' is a fan satisfying $\tau' \cap K = \tau$.

Proof: First consider $p \neq 2$. Then $F|K$ has odd degree and [B], ch. IV, §2, p. 145 applies to show the existence of a fan $\tau' \subseteq F$ such that $\tau' \cap K = \tau$. Given $\alpha \supseteq \tau$ then $-1 \notin \alpha \cdot \tau'$. Hence $\alpha\tau' \subseteq \alpha'$ for some order α' of F. The extensions of α correspond, by Artin–Schreier theory, to the K-embeddings $F \to R$. But $X^p - a$ has a unique root in R. This means every $\alpha \supseteq \tau$ has a unique extension in F. As seen, it must contain τ' and τ' has the description as given. To treat the case $p = 2$ we take a valuation ring W of K that trivializes τ. W has at least one extension and at most two extensions. All the extending valuation rings have a real residue field. Following the pattern of the proof of [B], ch. IV, §2, Lemma 4 and distinguishing cases according the values of the ramification index and residue degree the proof can be completed.

■

We are prepared to start the proof of the implication ii) ⇒ i). We study $\mathfrak{a} = (X_1^{r_1} - a_1, \dots, X_n^{r_n} - a_n)$, and proceed by induction as described above.

<u>**1st case:**</u> Some *odd* prime number p divides some r_i, say $p|r_1$. We may assume there is $x = (x_1, \dots, x_n) \in V_\tau(\mathfrak{a})$. The field $K(x_1)$ is real and we have $\left(x_1^{r_1/p}\right)^p = a_1$. If $a_1 \in K^p$ then we apply (4.9) to replace the ideal $X_1^{r_1} - a_1$ by $\sqrt[\tau]{(X_1^{r_1} - a_1)} = (X^{s_1} - b_1)$ with $s_1 < r_1$. This substitution does not change $\sqrt[\tau]{\mathfrak{a}}$. Now induction yields the claim in this case. Next assume $a_1 \notin K^p$. Then set $z_1 = x_1^{r_1/p}$ and $F = K(z_1) \subseteq K(x_1)$. The polynomial $X^p - a_1$ is irreducible with z_1 as one of its root. According to (4.12) we extend τ to the fan τ'. ¿From $\tau' \cap K = \tau$ we infer

$$V_{\tau'}(\mathfrak{a} \otimes F) \subseteq V_\tau(\mathfrak{a}). \tag{20}$$

We further prove:

$$\text{every } y \in V_\tau(\mathfrak{a}) \text{ is } K\text{–conjugate to some } y' \in V_{\tau'}(\mathfrak{a} \otimes F). \tag{21}$$

Then, as an immediate consequence we deduce

$$\sqrt[\tau]{\mathfrak{a}} = K[\underline{X}] \cap \sqrt[\tau']{\mathfrak{a} \otimes F}. \tag{22}$$

To prove (21) pick any $y = (y_1, \dots, y_n) \in V_\tau(\mathfrak{a})$. Then $\left(y_1^{r_1/p}\right)^p = a$. Thus there is an automorphism $\varphi \in \operatorname{Aut}(\overline{K}|K)$ such that $\varphi\left(y_1^{r_1/p}\right) = z_1$. Assume

$K(y_1, \dots, y_n) \subseteq R_\alpha$, $\alpha \supseteq \tau$. Then $K(\varphi(y_1), \dots, \varphi(y_n)) \subseteq R'_\alpha$ R'_α induces α' on F. We find $\alpha' \cap K = \alpha$, hence $\tau' \subseteq \alpha'$. This means $\varphi(y) \in V_{\tau'}(\mathfrak{a} \otimes F)$. The binomial ideal $\mathfrak{a} \otimes F$ has now the feature to contain the binomial $X_1^{r_1} - a_1$ with $p|r_1$ and $a_1 \in F^p$. This is the first case we dealt with. Consequently, by induction, $\sqrt[\tau']{\mathfrak{a} \otimes F}$ is a binomial ideal. Since $F = K(z_1)$ and $[F : K] = [< K^\times, z_1 >: K^\times]$ we will use §1 (1.17) to conclude that $\sqrt[\tau]{\mathfrak{a}}$ is a radical ideal. To apply this result special binomial generators are needed for $\sqrt[\tau]{\mathfrak{a} \otimes F}$. In this situation and others to follow we are given $x = (x_1, \dots, x_r) \in V_\tau(\mathfrak{a})$, $C =< K^\times, x_1, \dots, x_r >$ and $F = K(D)$, $K^\times < D < C$. Suppose

$$\underline{X}^{\underline{m}} - a\underline{X}^{\underline{m}}, a \in K(D^\times)$$

lies in $\sqrt[\tau]{\mathfrak{a} \otimes F}$. Then, $\prod x_i^{m_i} = a \prod x_i^{n_i}$, i.e. $a \in K(D)^\times \cap C = D$ by §1, (1.15). This means §1, (1.17) can be applied.

__2nd case:__ Now all exponents r_i are powers of 2. ¿From (4.9) we know

$$\sqrt[\tau]{(X_i^{r_i} - a_i)} = \begin{cases} X_i^{s_i} - a_i, & \text{irreducible, } s_i|r_i \\ X_i^{2s_i} - a_i^2, & X^{s_i} \pm a_i \text{ irreducible }, 2s_i|r_i \end{cases}$$

Since $\sqrt[\tau]{\mathfrak{a}} = \sqrt[\tau]{\sum_1^n \sqrt[\tau]{(X_i^{r_i} - a_i)}}$ we may assume

$$\mathfrak{a} = \left(X_1^{r_1} - a_1, \dots, X_k^{r_k} - a_k, X_{k+1}^{2r_{k+1}} - a_{k+1}^2, \dots, X_n^{2r_n} - a_n^2\right)$$

where $X^{r_i} - a_i$ is irreducible for $i \leq k$ and both $X^{r_i} \pm a_i$ are irreducible for $i > k$.

If some $r_i = 1$ for $i \leq k$ then induction on the number of variables applies. Let be $r_i = 2$ or some $s_j = 1$ for some $i \leq k$ or $j > k$ say $r_1 = 2$, $k \geq 1$ as the first case. If $K(x_1, \dots, x_n) \subseteq R_\alpha$ for $(x_1, \dots, x_n) \in V_\tau(\mathfrak{a})$ then $a_1 = x_1^2 \in R_\alpha^2 \cap K \subseteq \alpha$. Hence

$$V_\tau(\mathfrak{a}) = V_{\tau[a_1]}(\mathfrak{a}).$$

Now, $\tau[a_1]$ is a fan again. Thus we may assume $a_1 \in \tau$. Setting

$$\mathfrak{a}' = (X_2^{r_2} - a_2, \dots, X_n^{2r_n} - a_n) \lhd K[X_2, \dots, X_n]$$

we find $V_\tau(\mathfrak{a}) = \{(\pm\sqrt{a_1})\} \times V_\tau(\mathfrak{a}')$. Using this we derive $\sqrt[\tau]{\mathfrak{a}} = (X_1^2 - a_1, \sqrt[\tau]{\mathfrak{a}'})$. Induction on the number of variables yields binomiality for $\sqrt[\tau]{\mathfrak{a}}$. The case $s_j = 1$ is done in the same way.

Thus we may assume $4|r_i$ for $i \leq k$ and $2|s_j$ for $j > k$. The case of $k = 0$ will be dealt with in the third case. Assume $k \geq 1$. Note that $X_1^{r_1} - a_1$ is irreducible over K. Fix $(y_1, \dots, y_n) \in V_\tau(\mathfrak{a})$ and set $L = K(y_1)$. L is a real field. If $x \in V_\tau(\mathfrak{a})$ then $x_1^{r_1} = a_1$ as well and there is $\varphi \in \operatorname{Aut}(\overline{K}|K)$ with $\varphi(x_1) = y_1$. Hence it is enough to consider points $x \in V_\tau(\mathfrak{a})$ with $x_1 \in L$.

Then $x_1^{r_1} = y_1^{r_1} = a_1$, $x \in L$ implies $x_1 = \pm y_1$ and $x_1^{\frac{r_1}{2}} = y_1^{\frac{r_1}{2}} =: z_1$. We have $z_1^2 = a_1$. Extend τ to the fan τ' of $F := K(z_1)$ which contains z_1. Since z_1 is a square in L we find that $x \in V_{\tau'}(\mathfrak{a} \otimes F)$. This implies $\sqrt[\tau]{\mathfrak{a}} = K[\underline{X}] \cap \sqrt[\tau']{\mathfrak{a} \otimes F}$. In F we have $X_1^{r_1} - a_1 = \left(X_1^{\frac{r_1}{2}} - z_1\right)\left(X_1^{\frac{r_1}{2}} + z_1\right)$. We find that $w_1^{\frac{r_1}{2}} = z_1$ for every $(w_1 \ldots, w_n) \in V_{\tau'}(\mathfrak{a} \otimes F)$. Thus $X_1^{r_1} - a_1$ can be modified to $X_1^{\frac{r_1}{2}} - z_1$. Induction on the product of the degrees proves the claim for $\sqrt[\tau]{\mathfrak{a}}$. It remains the

<u>**3rd case:**</u> $\mathfrak{a} = (X_1^{4r_1} - a_1^2, \ldots, X_n^{4r_n} - a_n^2)$ where all r_i powers of 2.We do not assume the polynomials $X_i^{2r_i} \pm a_i$ to be irreducible. Consider any $(x_1, \ldots, x_n) \in V_\tau(\mathfrak{a})$. Then $F := K(x_1, \ldots, x_n)$ is a real field. Now Kneser's criterion (1.14) applies to yield

$$[F : K] = [< K^\times, x_1, \ldots, x_r >: K^\times] \leq \prod_1^n (2r_i)$$

since for each $i = 1, \ldots, n$ the fact $x_i^{2r_i} = \pm a_i$ implies $\mathrm{ord}(\overline{x}_i) | 2r_i$, $\overline{x}_i = x_i K^\times \in F^\times /_{K^\times}$. Furthermore, we find $\epsilon_i = \pm 1$ such that $x_i^{2r_i} = \epsilon_i a_i$. If $K(x_1, \ldots, x_n) \subseteq R_\alpha$ for some $\alpha \supseteq \tau$ we then obtain $\epsilon_1 a_1, \ldots, \epsilon_n a_n \in \alpha$.

For any given $\epsilon \in \{\pm 1\}^n$ set

$$H_\epsilon := \{\alpha \supseteq \tau | \epsilon_i a_i \in \alpha, i = 1, \ldots, n\}.$$

As just shown, every $x \in V_\tau(\mathfrak{a})$ gives rise to some $H_\epsilon \neq \emptyset$. Conversely, if $H_\epsilon \neq \emptyset$ and $\alpha \in H_\epsilon$ then choose a real closure R_α. In R_α the equations $X_i^{2r_i} = \epsilon_i a_i$ are solvable, and we find a point $x = (x_1, \ldots, x_n) \in R^n$, $x \in V_\tau(\mathfrak{a})$ inducing H_ϵ. Points inducing distincts sets H_ϵ, H_η are clearly not conjugate.

Assume first $H_\epsilon \neq \emptyset$ for every ϵ. We claim: $[K(x_1, \ldots, x_n) : K] = \prod_1^n (2r_i)$ for every $x \in V_\tau(\mathfrak{a})$. As a consequence we get: $\#V_\tau(\mathfrak{a}) \geq 2^n \cdot \prod_1^n (2r_i) = \#V(\mathfrak{a})$, whence $V_\tau(\mathfrak{a}) = V(\mathfrak{a})$. Since $\mathfrak{a}$ is a radical ideal the statement $\sqrt[\tau]{\mathfrak{a}} = \mathfrak{a}$ follows. To prove the claim concerning the field degree assume the contrary. Then the field degree is strictly less than $\prod(2r_i)$ and from Kneser's result, stated above, we find a certain relation

$$c = \prod_1^n x_i^{l_i} \text{ where } c \in K^\times, 0 \leq l_i < 2r_i$$

and not all $l_i = 0$. If $l_i \neq 0$ consider $t_i = \frac{2r_i}{gcd(2r_i, l_i)}$ and let t_1 be maximal among the 2–powers t_i. We find $2|t_1$. Then

$$c^{t_1} = \prod_1^n (\epsilon_i a_i)^{s_i} \text{ where } s_i = \frac{l_i}{gcd(2r_i, l_i)} \cdot \frac{t_1}{t_i}.$$

At least s_1 is odd, also $c^{t_1} \in (K^\times)^2$. That means there are a_i, ϵ_i, say for $i = 1, \dots, k$, such that $\prod_1^k(\epsilon_i a_i) \in (K^\times)^2$. But then $H_\eta = \emptyset$ for $\eta = (-\epsilon_1, \epsilon_2, \dots, \epsilon_k, 1, \dots, 1)$: a contradiction.

We are now left with the case that some $H_\epsilon = \emptyset$. Since τ is a fan this is equivalent to a relation

$$-1 = t \cdot (\epsilon_1 a_1) \dots (\epsilon_s a_s), s \geq 1, t \in \tau$$

(renumbered if necessary). We consider the variables $X_1, \dots, X_s$. The ideal $\mathfrak{a}$ contains

$$\prod_1^s X_i^{4r_i} - \prod_1^s a_i^2 = \left(\prod_1^s X^{2r_i} - \prod_1^s \epsilon_i a_i\right)\left(\prod_1^s X^{2r_i} + \prod_1^s \epsilon_i a_i\right).$$

The first factor on the right hand side never vanishes on $V_\tau(\mathfrak{a})$, hence can be deleted. We find $V_\tau(\mathfrak{a}) = V_\tau(\mathfrak{b})$ with $\mathfrak{b}$ generated by

$$\prod_1^s X^{2r_i} + \prod_1^s \epsilon_i a_i, X_2^{4r_2} - a_2^2, \dots, X_n^{4r_n} - a_n^2.$$

To $\mathfrak{b}$ we can apply the induction on the product of the degrees. In fact, $V_\tau(\mathfrak{b}) = V_\tau(\mathfrak{b}^\pm)$ hence $\sqrt[\tau]{\mathfrak{b}} = \sqrt[\tau]{\mathfrak{b}^\pm} \cap K[\underline{X}]$. $\mathfrak{b}^\pm$ is associated to a lattice L of index $2r_1 \cdot 4r_2 \cdot \dots \cdot 4r_n =: s$. Diagonalizing L we end up with a system

$$X_1^{s_1} = b_1, \dots, X_n^{s_n} = b_n, \ \prod s_i = s < \prod(4r_i),$$

Hence, we conclude that $\sqrt[\tau]{\mathfrak{b}}$ is a binomial ideal and the proof is complete.

■

We finally comment on possible generalizations of the last theorem. This means we are given a preorder τ not necessarily a fan and ask for special binomial ideals $\mathfrak{a}$ such that $\sqrt[\tau]{\mathfrak{a}}$ is still binomial. By a careful reading and adjusting some arguments one can prove

i) $\sqrt[\tau]{(X_1^{r_1} - a_1, \dots, X_n^{r_n} - a_n)}$ is binomial if either all r_i are odd or all $r_i \leq 2$.

The property of a fan was only needed to deal with generators of the type $X_i^{4r_i} - a^2$.

As demonstrated in §3 the computation of $\sqrt[\tau]{\mathfrak{a}}$ actually depends on the computation of $\sqrt[\tau]{\mathfrak{a}_\Delta^\pm}$ for all non–empty cells $V^\Delta(\mathfrak{a})$. The ideals $\mathfrak{a}_\Delta^\pm$ can be transformed into ideals of the type $(X_1^{r_1} - a_1, \dots, X_n^{r_n} - a_n)$. Therefore if we only meet ideals as in i) above the binomiality of $\sqrt[\tau]{\mathfrak{a}}$ results. Hence, we conclude that if for all non–empty cells $V^{\Delta}(\mathfrak{a})$ the group $\mathrm{Sat}(L_{\Delta})/_{L_{\Delta}}$ is either of odd order or of exponent 2 then $\sqrt[\tau]{\mathfrak{a}}$ is a binomial ideal for every preorder τ.

The following statements can be found in [Lam] e.g. Most of the preorders are not fans. If τ is an order or $\tau = \alpha \cap \beta$, α, β orders of K then τ is a fan, a socalled trivial fan. By means of valuation rings non–trivial fans can be constructed as follows: if W is a valuation ring of K with residue field k and $\overline{\tau} \subseteq k$ a fan then

$$\tau = K^{2} \cdot \{\epsilon \in W^{*} | \overline{\epsilon} \in \overline{\tau}\}$$

is a fan in K, the *pullback of* τ. By Bröcker's trivialization theorem every fan is the pullback of a trivial fan. In the iterated power series field $K = \mathbb{R}((X_1))((X_2))\ldots((X_n))$ the smallest preorder $\tau = \sum K^2$ is a fan. On the other hand fans in algebraic extensions of $\mathbb{Q}$ are trivial. If $K|\mathbb{R}$ is a real function field of transcendence degree d then a fan $\tau \in K$ has index

$$[K^{\times} : \tau^{\times}] \leq 2^{d}$$

and there are fans with index 2^d.

5 Algorithms

Let $\mathfrak{a}$ be a binomial ideal and K an infinite field.We want to solve the following problems.

A) determine $\dim \mathfrak{a}$ and the irreducible components of $V(\mathfrak{a})$,

B) decide whether $V_L(\mathfrak{a})$ or $V_\tau(\mathfrak{a}) \neq \emptyset$,

C) if $V_L(\mathfrak{a})$ is non-empty and finite determine its cardinality,

D) compute *-radicals of $\mathfrak{a}$.

There are well known algorithms to solve these tasks for general ideals.However in our context of binomial ideals we will design algorithms which take into account the distinguished structure of these ideals. Our algorithms consist of three main steps.We first decompose $V(\mathfrak{a})$ into cells and pass from the polynomial ring to some Laurent polynomial rings as described in the first section. In the second step we treat the corresponding questions for each of the relevant cells.Then we put together these informations to solve the original problem in $K[\underline{X}]$.

The first step could be performed by writing down for each $\Delta \subseteq \{1, \dots, n\}$ the ideal

$$\mathfrak{a}^{\pm}_{\Delta} = \pi_\Delta(\mathfrak{a}) \cdot K[X_i^{\pm} | i \in \Delta]$$

But more care allows us to skip many empty cells and detect some trivial cells in advance just by looking at the combinatorial structure of the generators of $\mathfrak{a}$, and furthermore to carry out all the intersections in the third step in such a way that all intermediate results are still binomial.

There are two possibilities listed as 1) and 2) below to discard cells.Let $\mathfrak{a}$ be generated by a set B of binomials $b_1, \dots, b_s$.Then the ideal

$$\mathfrak{a}_\Delta \triangleleft K[X_i | i \in \Delta]$$

is generated by $\pi_\Delta(B)$ which is obtained from B by setting the variables $X_j, j \notin \Delta$ in the binomials $b_1, \dots, b_s$ to 0.

1) If $\pi_\Delta(B)$ contains a monomial $\neq 0$ then $\mathfrak{a}^{\pm}_{\Delta} = (1)$,

2) There is $\Delta' \subseteq \Delta$ such that each $\pi_\Delta(B)$ contains only binomials built over Δ'. Then

   i) $V(\mathfrak{a}_\Delta) = V(\mathfrak{a}_{\Delta'}) \times K^{\Delta \setminus \Delta'}$,

ii) $V^{\Delta'}(\mathfrak{a}) \subseteq \overline{V^{\Delta}(\mathfrak{a})}$ (Zariski closure),

iii) $p : V_L^{\Delta}(\mathfrak{a}) \longrightarrow V_L^{\Delta'}(\mathfrak{a})$ and $p : V_\tau^{\Delta}(\mathfrak{a}) \longrightarrow V_\tau^{\Delta'}(\mathfrak{a})$ are surjective

Proof: 1) Clear 2)There are no constraints for the variables X_j, $j \in \Delta \backslash \Delta'$.Hence i) follows.To derive the two other statements we may take $\Delta' = \{1, \ldots, r\} \subseteq \Delta = \{1, \ldots, s\}$.From i) we conclude

$$V^{\Delta}(\mathfrak{a}) = \{(x_1, \ldots, x_s, 0, \ldots, 0) \big| (x_1, \ldots, x_r, 0, \ldots, 0) \in V^{\Delta'}(\mathfrak{a}), x_{r+1}, \ldots, x_s \in \overline{K}^{\times}\}$$

This identity implies the remaining claims. ■

The following algorithm makes use of the observations 1) and 2).

5.1 Algorithm

Input: $\mathfrak{a} = (f_1, \ldots, f_r) \lhd K[\underline{X}]$ binomial.

We construct a tree consisting of nodes N with two sons and three entries: $B(N)$ a list of binomials and $\Gamma(N), \Lambda(N) \subseteq \{1, \ldots, n\}$.

Initialization: T a tree consisting of one node R with either $B(R) = (f_1, \ldots, f_r), \Gamma(R) = \emptyset, \Lambda(R) = \{1, \ldots, n\}$ or NIL if $B(R)$ contains a constant $\neq 0$.

```
WHILE there exists a leaf $N \neq$ NIL DO
   IF there exists a $i \in \Lambda(N)$ such that

            $X_i$ occurs in $B(N)$ choose one of these $X_i$          (23)

      THEN
         CREATE(left_son($N$),right_son($N$))
         $B$(left_son($N$)):=$B(N)$
         $\Gamma$(left_son($N$)):=$\Gamma(N) \cup \{i\}$
         $\Lambda$(left_son($N$)):=$\Lambda(N)\backslash\{i\}$
         $B$(right_son($N$)):=obtained from $B(N)$ by setting $X_i$ to 0
            IF $B$(right_son($N$)) contains a monomial $\neq 0$ built over
            $\Gamma(N)$
            THEN right_son($N$):= NIL
            ELSE
            $\Gamma$(right_son($N$)):=$\Gamma(N)$
            $\Lambda$(right_son($N$)):=$\Lambda(N)\backslash\{i\}$
     ELSE left_son($N$):=right_son($N$):= NIL
DELETE all nodes NIL
```

Output: A empty tree or a tree with root R such that at each node N

$$\pi_{\Gamma(N) \cup \Lambda(N)}(\mathfrak{a}) \text{ is generated by } B(N),$$

.

The leaves (=terminal nodes) of this tree play a fundamental role.We form the list

$$\mathcal{T} = \{\Gamma(N) \cup \Lambda(N) | \text{ N a leave}\}$$

Claim: The list $\mathcal{T}$ satisfies

I)

$$V(\mathfrak{a}) = \bigcup_{\Delta\in\mathcal{T}} \overline{V^{\Delta}(\mathfrak{a})}\ , \quad dim(\mathfrak{a}) = max\{dimV^{\Delta}(\mathfrak{a})|\Delta \in \mathcal{T}\},$$

II)

$V_L(\mathfrak{a}) \neq \emptyset$ (resp. $V_T(\mathfrak{a}) \neq \emptyset$) if and only if $V_L{}^{\Delta}(\mathfrak{a})$ (resp.$V_T^{\Delta}(\mathfrak{a}) \neq \emptyset$) for some $\Delta \in \mathcal{T}$,

III) if $V_L(\mathfrak{a}) \neq \emptyset$ and finite then

$$V_L(\mathfrak{a}) = \bigcup_{\Delta\in\mathcal{T}} V_L^{\Delta}(\mathfrak{a}),$$

IV)

$$\mathfrak{a}^* = \bigcap_{\Delta\in\mathcal{T}} \pi_{\Delta}^{-1}((\mathfrak{a}_{\Delta}^{\pm})^* \cap K[X_i|i \in \Delta])$$

if the radical operation satisfies axiom VII.

Proof: We first compare this tree to the following one denoted by T.That one consists of nodes (Γ, Λ) where $\Gamma, \Lambda \subseteq \{1, \dots, n\}$. It has the root $(\emptyset, \{1, \dots, n\})$ and the branching rule :while $\Lambda \neq \emptyset$ choose $i \in \Lambda$ and set left son $=(\Gamma \cup \{i\}, \Lambda\backslash\{i\})$, right son$=(\Gamma, \Lambda\backslash\{i\})$.The leaves of this tree are the pairs $(\Delta, \emptyset)$,$\Delta \subseteq \{1, \dots, n\}$).If (Γ', Λ') is a successor of (Γ, Λ) then $\Gamma \subseteq \Gamma' \subseteq \Gamma \cup \Lambda$.The tree of (5.1) is obtained from this one by deleting a node and its subtree of successors according to the rules semantically described in 1) and 2). Now pick any $\Delta \subseteq \{1, \dots, n\}$.Assume

$$\mathfrak{a}_{\Delta}^{\pm} \neq (1) \text{ and } \Delta \notin \mathcal{T}$$

Then some predecessor (Γ, Λ) of Δ in $\mathcal{T}$ must have led to NIL either by rule 1) or rule 2).If 1) applies then $B(N)$ contains a monomial $\neq 0$ built over $\Gamma(N)$.From $\Gamma(N) \subseteq \Delta$ we get that $\mathfrak{a}_{\Delta}$ contains this monomial,hence $\mathfrak{a}_{\Delta}^{\pm} = (1)$: a contradiction. Thus rule 2) must have been applied.This means that the binomials in $B(N)$ are completely built over $\Gamma(N)$, hence over

$$\Delta \subseteq \Gamma(N) \cup \Lambda(N) = :\tilde{\Delta} \in \mathcal{T}$$

Using the statements in 2) we find

$$V^{\Delta}(\mathfrak{a}) \subseteq \overline{V^{\tilde{\Delta}}(\mathfrak{a})}$$

This proves I).In the same way II) follows. To deduce III) we observe that if $V_L^{\Delta}(\mathfrak{a}) \neq \emptyset$ then $\Delta \in \mathcal{T}$. Otherwise the relation between $V^{\Delta}(\mathfrak{a})$ and $V^{\tilde{\Delta}}(\mathfrak{a})$

as given in the proof of statement 2) above would lead to an infinite set $V_L(\mathfrak{a})$.To derive IV) we recall the formula

$$\mathfrak{a}^* = \bigcap_{\Delta} \pi_{\Delta}^{-1}((\mathfrak{a}_{\Delta}^{\pm})^* \cap K[X_i|i \in \Delta])$$

Pick any $\Delta \subsetneq \{1,\dots,n\}$which is not in$\mathcal{T}$ and assume $\mathfrak{a}_{\Delta}^{\pm} \neq (1)$.The arguments above have shown the existence of $\tilde{\Delta} \supseteq \Delta$, $\tilde{\Delta} \in \mathcal{T}$ such that

$$\mathfrak{a}_{\tilde{\Delta}} = \mathfrak{a}_{\Delta} K[X_i|i \in \Delta]$$

Set $S_{\bar{\Delta}} = K[X_i|i \in \bar{\Delta}]$ for any $\bar{\Delta} \subseteq \{,\dots,n\}$.We will prove

$$(\mathfrak{a}_{\tilde{\Delta}}^{\pm})^* \cap S_{\tilde{\Delta}} = \left((\mathfrak{a}_{\Delta}^{\pm})^* \cap S_{\Delta}\right) S_{\tilde{\Delta}}$$

This implies

$$\pi_{\tilde{\Delta}}^{-1}((\mathfrak{a}_{\tilde{\Delta}}^{\pm})^* \cap S_{\tilde{\Delta}}) \subsetneq \pi_{\Delta}^{-1}((\mathfrak{a}_{\Delta}^{\pm})^* \cap S_{\Delta})$$

and IV) is proved. To prove the identity we simplify the notation :$\tilde{\Delta} = \{1,\dots,n\}$, $\Delta = \{1,\dots,r\}$, $\mathfrak{a} = \mathfrak{a}_{\Delta}$, $\mathfrak{b} = \mathfrak{a}_{\tilde{\Delta}}$. The properties of the radical operations yield

$$(\mathfrak{b}^{\pm})^* = (\mathfrak{b}^*)^{\pm} = (\mathfrak{a}^* K[X_1,\dots,X_n])^{\pm} = (\mathfrak{a}^* S_{\Delta})^{\pm} \cdot K[\underline{X}^{\pm}]$$
$$= (\mathfrak{a}^{\pm})^* K[\underline{X}^{\pm}] = ((\mathfrak{a}^{\pm})^* \cap S_{\Delta}) K[\underline{X}^{\pm}]$$

from which the claimed identity follows.

■

The statements I) - IV) means that only cells $V^{\Delta}(\mathfrak{a})$ with $\Delta \in \mathcal{T}$ need to be considered to solve our initial problems A) - D). Litterally, the determinations of the irreducible components of $V(\mathfrak{a})$ have not been mentioned. But I) implies that $V(\mathfrak{a})$ is the union of the Zariski closures of the irreducibles components of the sets $V^{\Delta}(\mathfrak{a})$, $\Delta \in \mathcal{T}$. Thus the components of $V(\mathfrak{a})$ can be obtained as the maximal sets among those irreducible sets. Two final remarks are in order

i) ¿From IV) we obtain

$$V(\mathfrak{a}^*) = \bigcup_{\Delta \in \mathcal{T}} V(\pi_{\Delta}^{-1}((\mathfrak{a}_{\Delta}^{\pm})^* \cap S_{\Delta}))$$

This shows

$$dim(\mathfrak{a}^*) = max_{\Delta \in \mathcal{T}}\{dim(\mathfrak{a}_{\Delta}^{\pm})^*\}$$

and that the irreducible components can be obtained from the closures of the irreducible components of $V((\mathfrak{a}_{\Delta}^{\pm})^*)$.

ii) Neither the value of the exponents nor the coefficients play a role in these combinatorical considerations.

Example: Let $f_1 := X_1X_3 + X_2X_4, f_2 := X_1X_2 + X_1X_4$, $f_3 := cX_2 + X_1X_3X_4, c \neq 0$, $\mathfrak{a} = (f_1, f_2, f_3) \triangleleft \mathbb{Q}[X_1, X_2, X_3, X_4]$. The resulting tree has just three nodes N_1, N_2, N_3, which can't be replaced by NIL .

$N1: \; B(N_1) = \{0\}, \Gamma(N_1) = \emptyset, \Lambda(N_1) = \{3, 4\}$,

$N2: \; B(N_2) = \{0\}, \Gamma(N_2) = \{1\}, \Lambda(N_2) = \emptyset$ and

$N3: \; B(N_3) = \{f_1, f_2, f_3\}, \Gamma(N_3) = \{1, 2, 3, 4\}, \Lambda(N_3) = \emptyset$.

We stop at N_1 because (23) doesn't apply. This means that the cells corresponding to $\Delta = \emptyset, \{3\}, \{4\}, \{3, 4\}$ are described by the same equations. In this case we have the zero ideal. N_2 gives us the zero ideal for $\Delta = \{1\}$,and the only non-trivial node is N_3 with the ideal $\mathfrak{a}_{\{1,2,3,4\}} = (f_1, f_2, f_3)$.

In the second step of our algorithms we have to deal with individual cells $V^{\Delta}(\mathfrak{a})$. We first decide whether the cell is empty over $\overline{K}$,i.e. whether $\mathfrak{a}_{\Delta}^{\pm} = (1)$.This amounts to showing that certain systems

$$\underline{X}^{\underline{v_1}} = b_1, \ldots, \underline{X}^{\underline{v_r}} = b_r$$

have no solutions over $\overline{K}^{\times}$.In dealing with such systems it is appropriate to regard $\overline{K}^{\times}$ as a $\mathbf{Z}$ - module and let $A \in M_{r,n}(\mathbf{Z})$ induce the mapping

$$A : (\overline{K}^{\times})^n \longrightarrow (\overline{K}^{\times})^r \, , (x_1, \ldots, n)^t \mapsto (y_1, \ldots, r)^t \text{ where}$$

$$y_i = \prod_j x_j^{a_{ij}} \, , A = (a_{ij})$$

Then clearly $A(Bx) = (AB)x$. A system of equations $Ax = b$ can be manipulated as usual.In particular,given $U \in GL_r(\mathbf{Z})$, $V \in GL_n(\mathbf{Z})$, we can pass to the equivalent system

$$(UAV)y = Ub \text{ where } y = V^{-1}x$$

5.2 Lemma *Let $\mathfrak{b} \triangleleft K[\underline{X}^{\pm}]$ be generated by $\underline{X}^{\underline{v_1}} - b_1, \ldots, \underline{X}^{\underline{v_r}} - b_r$, $A \in M_{r,n}(\mathbf{Z})$ the matrix with the rows $\underline{v_1}, \ldots, \underline{v_r}$. Further let $U \in GL_r(\mathbf{Z})$, $V \in GL_n(\mathbf{Z})$ such that*

$$U \cdot A \cdot V = \begin{pmatrix} a_{11} & \cdots & a_{1s} & \cdots & a_{1n} \\ & \ddots & \vdots & & \vdots \\ & & a_{ss} & \cdots & a_{sn} \\ & & 0 & & \\ & & & & \end{pmatrix} , \; a_{ii} \neq 0 \text{ for } i = 1, \ldots, s \, .$$

Then setting

$$(c_1, \ldots, c_r)^t = U \cdot (b_1, \ldots, b_r)^t$$

we find

$$\mathfrak{b} = K[\underline{X}^{\pm}] \Leftrightarrow \exists s < t \leq n : c_t \neq 1$$

.

Proof: The system $(UAV)y = Ub$ is solvable over $\overline{K}^{\times}$ iff $c_{s+1} = \ldots = c_n = 1$. ■

In practice we pass from the extended matrix $(A|b)$ with $b = (b_1, \ldots, b_r)^t$ to the matrix $(UAV|Ub)$. Very often V is just a permutation matrix and need not be considered.

Example: We continue with the previous example and the cell associated to $\Delta \subseteq \{1, 2, 3, 4\}$.Then

$$(A|b) = \left(\begin{array}{cccc|c} 1 & -1 & 1 & -1 & 1 \\ 0 & 1 & 0 & -1 & 1 \\ 1 & -1 & 1 & 1 & c \end{array}\right)$$

which can be transformed into

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & -2 & 1 \\ 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 2 & c \end{array}\right)$$

Therefore $\mathfrak{a}_{\Delta}^{\pm} \neq (1)$.

So far we have found all cells $V^{\Delta}(\mathfrak{a})$, $\Delta \in \mathcal{T}$ that are not empty.Clearly only those play a role.We are now ready to solve the problems A) - D).

Problem A)

We have

$$dim V^{\Delta}(\mathfrak{a}) = \#\Delta \; - \; dim\, L^{\Delta} \text{ if } \mathfrak{a}_{\Delta}^{\pm} \neq (1)$$

The dimension of $L^{\Delta} =< \underline{v_1}, \ldots, \underline{v_r} >$ equals the rank of the matrix A with columns $\underline{v_1}, \ldots, \underline{v_r}$ and can be read off after putting A into trigonal shape.If unimodular matrices U, V are chosen such that UAV is a diagonal matrix then the irreducible components can be described.Details are given in section 1. In the example above we find $dim(\mathfrak{a}) = 2$ and the four irreducible components

$$\{X_1 = X_2 = 0\}, \{X_2 = X_3 = X_4 = 0\} \text{ and } \{X_1X_3 = c, X_2 = X_4, X_4 = \pm\sqrt{c}\}$$

Problem B)

In order to find $L-$points in $V^{\Delta}(\mathfrak{a})$ we put the describing matrix of the lattice L^{Δ} into diagonal form,i.e. we have to consider the solvability of the system

$$X_1^{f_1} = b_1, \ldots, X_d^{f_d} = b_d$$

Hence,if the field L allows a decision procedure for equations of the type $X^f = b$ we can decide whether $V_L(\mathfrak{a}) \neq \emptyset$. In the case of a real closed field $L = R$ the decision procedure is as simple as this:

- f odd : $X^f = b$ is solvable in R,
- f even :$X^f = b$ is solvable in R iff $b \geq 0$.

In a real closed field the diagonalization of the matrix A is not needed. Assume $\mathfrak{a}^{\pm}_{\Delta} \neq (1)$ and let $A \in M_{r,n}(\mathbf{Z})$ describe the lattice L^{Δ}.Further set $b_i = (-1)^{\epsilon_i}|b_i|$ and consider the extended matrix

$$\left(\begin{array}{c|c} & \epsilon_1 \\ A & \vdots \\ & \epsilon_r \end{array} \right) = (A|\epsilon)$$

If B is an integral matrix let $\overline{B}$ the reduction mod 2.We prove

i)
$$V_R^{\Delta}(\mathfrak{a}) \neq \emptyset \Longleftrightarrow \mathrm{rg}_{\mathbb{F}_2}(\overline{A}) = \mathrm{rg}_{\mathbb{F}_2}(\overline{A}|\overline{\epsilon})$$

ii) if $V_R^{\Delta}(\mathfrak{a}) \neq \emptyset$ and $\mathrm{rg}_{\mathbb{F}_2}(\overline{A}) + s = \mathrm{rg}(A)$ then $\sqrt[R]{\mathfrak{a}^{\pm}_{\Delta}}$ has 2^s minimal prime ideals.

Proof: We resume the arguments of the first section.Choose unimodular matrices U, V such that

$$UAV = \begin{pmatrix} f_1 & & & & & \\ & \ddots & & & & \\ & & f_k & & & 0 \\ & & & 2f_{k+1} & & \\ & & & & \ddots & \\ & & & & & 2f_{k+s} \\ & 0 & & & & \end{pmatrix}$$

where $f_1, \dots, f_k$ are odd and $f_i \neq 0$.
Since $\mathfrak{a}^{\pm}_{\Delta} \neq (1)$ we find $Ub = (c_1, \dots, c_{k+s}, 1, \dots, 1)^t$. Setting $U\epsilon = (\eta_1, \dots, \eta_r)^t$ this means $c_i = (-1)^{\eta_i}|c_i|, i = 1, \dots, r$ and

$$\eta_i \equiv 0 \bmod 2, |c_i| = 1 \text{ if } i > k+s$$

Then $UAVy = Ub$ is solvable over R iff

$$\eta_{k+1} = \dots = \eta_{k+s} \equiv 0 \bmod 2$$

Now rg $(\overline{A})$ = rg $(\overline{UAV}) = k$ and $\mathrm{rg}(\overline{A}|\overline{\epsilon})$ =rg $(\overline{UAV}|\overline{U\epsilon}) = k+1$ iff some $\eta_i \not\equiv 0 \bmod 2$ for $k < i \leq k+s$. Thus i) is proved. After the normalization of section 1 we see that $\sqrt[R]{\mathfrak{a}^{\pm}_{\Delta}}$ is generated by $X_1 - a_1, \dots, X_k - a_k$, $X_{k+1}^2 - a_{k+1}, \dots, X_{k+s}^2 - a_s$. This shows that there are 2^s minimal prime ideals. Obviously $s =$ rg $A-$ $\mathrm{rg}_{\mathbb{F}_2}\overline{A}$. ■

In our example we find $\mathrm{rg}\overline{A} = 2, \mathrm{rg}(\overline{A}|\overline{\epsilon}) = 2$ iff $c > 0$. Hence $V_{\mathbb{R}}(\mathfrak{a}) \neq \emptyset$ iff $c > 0$. In that case $\sqrt{\mathfrak{a}} = \sqrt[R]{\mathfrak{a}}$.

Problem C

We have to consider only cells with $\dim \mathfrak{a}_\Delta^\pm = 0$, i.e. $\dim L^\Delta = \#\Delta$. After diagonalizing L^Δ we have to count the number of zeros of a system

$$X_1^{f_1} = a_1, \ldots, X_n^{f_n} = a_n$$

in L. This number is given by the number of roots of unities in L. If $L = \overline{K}$ then $\#V_L^\Delta(\mathfrak{a}) = [\mathbf{Z}^{|\Delta|} : L^\Delta]$ or the p-free part of it if $\mathrm{char} K = p > 0$. If $L = R$ a real closed field then $\#V_R^\Delta(\mathfrak{a}) = 2^s$,
$s = \mathrm{rg}\ A - \mathrm{rg}_{\mathbb{F}_2} \overline{A}$.

Problem D

After diagonalizing L^Δ and considering only the essential variables we have to calculate

$$(X_1^{f_1} - a_1, \ldots, X_n^{f_n} - a_n)^*.$$

Once this is done we know $(\mathfrak{a}_\Delta^\pm)^*$. Now, the intersection $(\mathfrak{a}_\Delta^\pm)^* \cap S_\Delta$ can be done by Gröbner basis methods since this ideal can be understood as an elimination ideal, cf [EiSt] e.g. . Then we know $\pi_\Delta^{-1}((\mathfrak{a}_\Delta^\pm)^* \cap S_\Delta)$ and finally, again using Gröbner basis techniques, $\mathfrak{a}^*$ results as the intersections of these ideals for $\Delta \in \mathcal{T}, \mathfrak{a}_\Delta^\pm \neq (1)$.

This procedure applies to all *-radicals even if they are not binomial ideals. If however the *-radicals of every binomial ideal is again binomial then it seems worthwhile to trace back the tree of (5.1). In fact, at each non-terminal node we pass from an algebra A and an ideal $\mathfrak{a}$ to the two algebras $A[X_k^{-1}]$ and $A/(X_k)$ and the ideals $\mathfrak{b} = \mathfrak{a}A[X_k^{-1}]$ and $\mathfrak{c} = (\mathfrak{a} + (X_k))/(X_k)$. The decomposition law (2.6) yields

$$\mathfrak{a}^* = (\mathfrak{b}^* \cap A) \cap \pi^{-1}(\pi(\mathfrak{a})^*).$$

Thus in the case of binomial ideals all intermediate results are still binomial ideals.

References

[ABrR] C. Andradas, L. Bröcker, J. Ruiz *Constructible sets in real algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd. , Springer–Verlag 1996

[B] E. Becker *Hereditarily–pythagorean fields and orderings of higher level*, Monografias de Matemática 29, (1978), IMPA, Rio de Janeiro

[BJ] E. Becker, B. Jacob *Rational points on algebraic varieties over a generalized real closed field: a model theoretic approach*, J. reine angew. Math. 357 (1985), 77–95

[BN] E. Becker, R. Neuhaus *Computation of real radicals of polynomial ideals*, in: Computational Algebraic Geometry, ed. F. Eysette, A. Galligo, Progress in Mathematics, vol. 109, Boston 1993 ,1 - 20.

[BCR] J. Bochnak, M. Coste, M.F. Roy *Géométrie algébrique réelle*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Folge 3, Band 12, Springer-Verlag 1987

[Co] H. Cohen *A Course in Computational Number Theory*, Berlin 1993

[EiSt] D. Eisenbud, B. Sturmfels *Binomial ideals* Duke Math. J., to appear

[H1] F. Halter–Koch *Über Radikalerweiterungen*, Acta Arith. 26 (1980), 43–58

[H2] F. Halter–Koch *Körper, über denen alle algebraischen Erweiterungen der Kummerschen Theorie genügen*, J. Algebra 64 (1980), 391–398.

[Kn] M. Kneser *Lineare Abhängigkeit von Wurzeln*, Acta Arith. 26 (1974). 307–308

[KnS] M. Knebusch, C. Scheiderer *Einführung in die reelle Algebra*, Vieweg–Verlag 1989

[L] S. Lang *Algebra*, 1965

[La1] D. Laksov *Generalized radicals of ideals in algebras*, Rend. del Sem. Mat. Università e Politecnio Torino 1986, 77–89

[La2] D. Laksov *Radicals and Hilbert Nullstellensatz for not necessarily algebraically closed fields*, L'Enseignement Mathématique 33 (1987), 323–338

[Lam] T. Y. Lam *Orderings, valuations and quadratic forms*, CBMS Notes, 1983

[vdW] B.L. van der Waerden *Algebra, 2.Teil*, Berlin 1967