INTERNATIONAL COMPUTER SCIENCE INSTITUTE

1947 Center St. • Suite 600 • Berkeley, California 94704-1198 • (510) 643-9153 • FAX (510) 643-7684

Aspects of Algebraic Geometry over Non Algebraically Closed Fields

Tomas Sander *

TR-96-055

December 1996

Abstract

In this paper we study algebraic-geometric properties of the set of K-rational points V_K of K-varieties V. We introduce an elementary class of fields $\mathcal{K}$ of char 0 for which we prove:

1. Algebraic-geometric data of V_K (e.g. the dimension of V_K) can be computed under natural assumptions on K,
2. Uniform Finiteness Theorems (of Bezout Theorem type) and other complexity results and bounds,
3. Algebraic-geometric concepts are definable by first order formulas in the language of rings.

The class $\mathcal{K}$ contains for example algebraically and real closed fields, Henselian fields (e.g. $\mathbb{Q}_p$ and power series fields), PAC-fields (i.e. pseudo algebraically closed fields), PRC-fields, PpC-fields (of characteristic 0). Further structural properties of $\mathcal{K}$ are studied.

*email: sander@icsi.berkeley.edu

Contents

0 Introduction

Algebraic Geometry is classically developed over algebraically closed fields. Effective Algebraic Geometry is a very lifely area of the subject where many exciting results have been derived during the last twenty years. And also Algebraic Geometry over non-algebraically closed fields is an area of growing interest, both from a theoretical and an effective point of view. Real Algebraic Geometry is one example for this. Another example is the study of the ($\mathbb{Q}$-)rational points of varieties which is one of the main topics of Arithmetic Geometry. In contrast to the situation over $\mathbb{R}$ and $\mathbb{C}$ many effective questions are still open (like, e.g., the existence of uniform bounds for the number of rational points on smooth curves in terms of the degree and the number of variables of the defining equations).

In this paper we are going to define a class $\mathcal{K}$ of fields, so far of char 0, "lying between" $\mathbb{Q}$ and algebraically closed fields. For this class we will give satisfactory solutions to the following problems for the K-rational points of K-varieties.

1. The computability of algebraic-geometric properties of V_K.
2. The first order definability of algebraic-geometric properties of V_K in the language of rings.
3. Bounds and Uniform Finiteness Theorems.

Some of the proofs in this paper are omitted and sometimes we sketch only briefly the ideas. Detailed versions of the proofs can be found in [Sa2]. The document [Sa2] can be downloaded via the WWW page
http://www.mathematik.uni-dortmund.de/lsvi/Sander.html

0.1 The K-Radical is the Central Tool

It turns out that the central tool to answer these questions is a "good control" over the K-Radical of an ideal $A \lhd K[X_1, \ldots, X_n]$ which describes the K-Zariski closure of the K-rational points $V_K(A)$ of $V(A)$:

$$\sqrt[K]{A} := I(V_K(A)) \lhd K[X_1, \ldots, X_n].$$

We have:

- The computability of the K-radical yields the computability of algebraic-geometric properties and objects of V_K.
- The first order definability of being K-radical yields the first order definability of algebraic-geometric properties of V_K.
- Degree bounds for the K-radical yield Bounds and Uniform Finiteness Theorems on V_K.

0.2 History

The general concept of K-radicals has been studied so far mainly in the context of "Nullstellensätze", for instance by Weispfenning, Lakshov, Adkins, Gianni, Tognoli et. al. (cf. [AdGiTo], [Lak], [We2]). This work seems to be the first systematic study of the K-radical from the point of view of its computation, i.e. the computation of a set of generators for $\sqrt[K]{A}$.
We know of two special cases in which there has been described an algorithm to compute the K-radical:

1. For algebraically closed fields K in 1926 by G. Herrmann (cf. [Her]).

2. For real closed fields in 1992 by E. Becker and R. Neuhaus (cf. [BeNe]).

Becker and Neuhaus in fact showed more: they described an intersting and involved algorithm to compute the τ-radical for a preordered field (K, τ).

0.3 To the Computability of the K-Radical

Algebraic Geometry over non algebraically closed fields deals with the study of the K-solutions of systems of algebraic equations. So it is necessary to assume something about the field K if one wants to get computational data about V_K. The minimal assumption one has to make here is the decidability of the existential theory of K (resp. the explicit computability of a K-solution of a system of equations). Else one does not even know whether V_K is empty or not and there is not much to say over V_K from a computational point of view.

We show at the end of Chapter 1 that computation of K-radicals can be primitive-recursively reduced to the solution of the following tasks:

1. Decide for a prime ideal P whether it is K-radical or not.
2. If P is not K-radical find a polynomial g that vanishes on $V_K(P)$, but not on $V_C(P)$.
3. Factorization of univariate polynomials in $K[X]$.

Two remarks:

Finding a computationally useful characterization of K-radical prime ideals in general seems to be impossible: we construct in Chapter 3 a field M such that the property of being K-radical can not be expressed by an elementary formula in the language of rings.

In the context of recursively presented fields, the tasks 1)-3) are indeed *subproblems* of the K-radical computation, i.e. the computability of K-radicals over K implies the solvability of 1)-3) for K.

0.4 Basic Algebraic-Geometric Objects and Data Related to V_K

We are mainly interested in fundamental properties of the K-rational points V_K of K-varieties V of the following type:

1. The dimension of V_K
2. The decomposition of V_K into its K-irreducible components
3. The singular locus of V_K
4. The K-Zariski-closure of the image of V_K under projections (Elimination Theory)
5. The Zariski-closure of the image of V_K under K-regular maps (the Implicitization Problem)
6. The projective closure of V_K.

0.5 The Class $\mathcal{K}$

So we want to find fields where the property of being K-radical of an ideal A can be related to some easy handable properties of $V_K(A)$. If P is a K-radical prime ideal $V(P)$ contains necessarily a regular K-rational point. It is natural now to study those fields where this property already *characterizes* the K-radical prime ideals. The following class of fields is introduced in Section 2 being the Main Definition of this work:

Definition 0.1

$$\mathcal{K} := \{K \mid \textit{char } K = 0, \forall n \in \mathbb{N}\, \forall P \lhd K[X_1, \ldots, X_n], P \textit{ prime: } \\ P \textit{ is } K\textit{-radical} \iff V(P) \textit{ contains a regular } K\textit{-rational point}\}$$

The first Main Theorem for $\mathcal{K}$ is that we can in fact compute for fields $K \in \mathcal{K}$ K-radicals only assuming that our minimal assumption of the solvability of systems of algebraic equations is met.

Main Theorem 1 (Computability of the K-Radical in $\mathcal{K}$) *In $\mathcal{K}$ there is an algorithm to compute the K-radical using only*

1. *Factorization in $K[X]$.*
2. *Decidability whether a system of algebraic equations with coefficients in K has a K-rational solution.*

The definition of $\mathcal{K}$ is general enough to cover fields playing a role in various areas of mathematics like Algebraic Number Theory, Galois Theory, Arithmetic of Fields, Real Algebraic Geometry (of Higher Level) and Valuation Theory. Fields of a "global character" do not belong to $\mathcal{K}$:

Fields in $\mathcal{K}$	Fields not in $\mathcal{K}$
$\mathbb{C}$, Algebraically closed fields	$\mathbb{Q}$
$\mathbb{R}$, Real closed fields	Number fields
$\mathbb{Q}_p$, p-adically closed fields	Function fields
PAC-, PRC-, PpC-fields	
Henselian fields, e.g.:	
Power series fields	
Real closed fields of higher level	

0.6 Structural Properties of $\mathcal{K}$

The main results are:

- Membership to $\mathcal{K}$ can be detected already by studying plane curves:

  A field K belongs to $\mathcal{K}$ if and only if for every irreducible plane K-curve C holds:

  If C contains a regular K-rational point, C contains infinitely many K-rational points.

- $\mathcal{K}$ is an elementary, inductive class in the language of rings.
- Closure properties: As an inductive, elementary class $\mathcal{K}$ is closed under ultraproducts and direct limits. Furthermore there is an "Algebraic Going Up Theorem": $\mathcal{K}$ is closed under algebraic extensions. Furthermore $\mathcal{K}$ is closed under a natural "Local Global Principle" with localities in $\mathcal{K}$. $\mathcal{K}$ is not closed under finite intersections.

- The theory of $\mathcal{K}$ is undecidable. The existential theory of $\mathcal{K}$ equals the existential theory of the Laurent series field $\mathbb{Q}((t))$.

0.7 Model Theoretic Aspects of Algebraic Geometry

By model theorists many decidability results for the theories of fields have been established. To make this fruitful for Algebraic Geometry over non algebraically fields the question comes up whether concepts of Algebraic Geometry are first order definable (in the language of rings). In the case of K-varieties (with points in an algebraically closed field) this is possible by (usually) quantifier free formulas. This is mainly known and reported in Section 3. Concerning K-rational points this is not the case in general: the field M of characteristic 0 we construct in Section 3 shows that there is an elementary class of fields s.t. e.g. the concept of being of dimension 0 is *not* elementary.

The outstanding importance of the K-radical occurs here as well: If the property of being K-radical is first order definable then this is also the case for the statements corresponding to our list of basic algebraic-geometric properties above, like "dim $V_K(A) = r$" or "Sing $V_K(A) = V_K(B)$" etc. Furthermore it turns out that if algebraic-geometric properties (including dimension) are first order definable for an elementary class at all one does not need arbitrary complicated formulas. Formulas which are low in the hierarchy of formulas do the job:

1. They can be chosen to be Π_3^0 (and also Σ_3^0) formulas.
2. For an inductive elementary class they can be taken as Boolean combinations of Σ_2^0 formulas.
3. For $\mathcal{K}$ they can be taken as Boolean combinations of Σ_1^0-formulas.

We derive the third result from the second Main Theorem for $\mathcal{K}$:

Main Theorem 2 (First Order Definability of being K-Radical in $\mathcal{K}$)
There is an existential formula φ such that for all fields $K \in \mathcal{K}$ and all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format holds:

$$A = \sqrt[K]{A} \iff K \models \varphi(A)$$

.

Another consequence of the Definability Theorem for $\mathcal{K}$ is a model theoretic proof for the existence of uniform bounds for generators of the K-radical. Such a proof seemed to be unknown even for the subclass of real closed fields.
The only fields (of char 0) we know of where the notion of dimension (and others) are elementary are fields in $\mathcal{K}$. So it would be interesting to know whether there exist fields not in $\mathcal{K}$ s.t. the dimension is first order definable.
We prove Nullstellensätze of the form introduced by McKenna for any complete, model complete theory (in the language of rings) containing the theory of $\mathcal{K}$. McKennas original proof for $\mathbb{Q}_p$ can be easily adapted to the situation of $\mathcal{K}$. We take it as another clue for the naturality of the class $\mathcal{K}$ that quite a few existing theorems and their proofs can be easily adapted to the situation of $\mathcal{K}$.

0.8 Complexity Theory and Uniform Finiteness Theorems

We say "deg $(A) \leq d$" if A can be generated by polynomials of degree $\leq d$. In Chapter 4 we prove the following degree bound for the K-radical of an ideal:

Main Theorem 3 (Degree Complexity Bound for the K-Radical in $\mathcal{K}$) *For all fields $K \in \mathcal{K}$ and all ideals $A \lhd K[X_1, \ldots, X_n]$ with deg $A \leq d$ holds:*

$$deg\ \sqrt[K]{A} \leq d^{2^{O(n^3)}}.$$

This degree bound is essentially of the same double exponential nature as the one derived by Krick and Logar for the usual radical and by Becker and Neuhaus for the real radical.

From the above Theorem we derive double exponential degree bounds on objects we associate to $V_K(A)$ like the K-irreducible components of $V_K(A)$, the singular locus of $V_K(A)$ or $\overline{\pi(V_K(A))}$.

With the help of this bound we prove Uniform Finiteness Theorems for $\mathcal{K}$. So the number of irreducible components of the K-rational points of a variety can be uniformly bounded in terms of the degree and the number of variables by a double exponential function. Consequently we get a Theorem similar to the Bezout Theorem:

Corollary 0.2 (Uniform Finiteness Theorem for $\mathcal{K}$) *Let $K \in \mathcal{K}$ and $A \lhd K[X_1, \ldots, X_n]$ with deg $A \leq d$ s.t. $\#V_K(A) < \infty$. Then $\#V_K(A) \leq d^{2^{O(n^3)}}$.*

Certainly one would like to have a single exponential bound (as one has for algebraically and real closed fields).

The double exponential increase in Main Theorem 3 is caused by currently double exponential bounds for the computation of the iterated singular loci "Sing V, Sing(Sing V) etc." of a complex variety V. If we were able to compute iterated singular loci set-theoretically with single exponential complexity bounds this would yield single exponential complexity bounds for most of the problems we consider. A positive answer this today open question - which is a question of Effective Algebraic Geometry over algebraically closed fields - would thus yield a qualitative breakthrough for Finiteness Theorems and Complexity Bounds in $\mathcal{K}$.

0.9 The Relative Situation $K \mid k$

Fields in $\mathcal{K}$ often arise as closures of fields k under a certain hull operation like the real closure of $\mathbb{Q}$ or a p-adic closure of $\mathbb{Q}$. Now it might be very time consuming or even impossible to code the field K over k (cf. [Ho], [Sa]). So as a step towards practical computations there is a need for an algorithm such that all computations are performed inside $k[X_1, \ldots, X_n]$. We show that - under a certain condition on k - $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ can be computed under avoiding computations in $K[X_1, \ldots, X_n]$:

Let $K \mid k$ be algebraic, $K \in \mathcal{K}$.
Let $A = (f_1, \ldots, f_m) \lhd K[X_1, \ldots, X_n]$, where $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. Then we are able to compute $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ if the following conditions are fulfilled:

1. The existential theory of K with parameters in k is decidable.
2. The univariate polynomial ring $k[X]$ allows effective factorization.

As an example where the additional assumption on facorization in $k[X]$ is really necessary we describe the following relative situation: k is an ordered field and K its real closure.

0.10 Galois Theoretic Results by F. Pop

Recently the class $\mathcal{K}$ has been introduced independently by F. Pop (Pop calls the fields in $\mathcal{K}$ "large fields" and has no restrictions on the characteristic, cf. [Po]). He discovered that the defining property of $\mathcal{K}$ is useful for problems arising from Galois Theory. Recall that one of the major unsolved problems in Galois Theory is the Inverse Galois Problem (for short: IGP) for $\mathbb{Q}$, i.e. the question whether every finite group can be realized as a Galois group over $\mathbb{Q}$. Hilbert had shown that a positive solution of IGP for $\mathbb{Q}(t)$ implies this for $\mathbb{Q}$ too. Now Pop has shown—among other results—the remarkable fact that for fields $K \in \mathcal{K}$ IGP has a positive answer for $K(t)$. If $K \in \mathcal{K}$ and if K is additionally Hilbertian then IGP has a positive answer for K. Thereby he generalizes results known e.g. for $\mathbb{R}(t), \mathbb{C}(t)$.
These Galois theoretic results are another indication for the usefulness and the conceptually unifying power of $\mathcal{K}$.

Ten open problems that occured during the study of $\mathcal{K}$, and the we consider to be interesting are listed in the appendix.

Acknowledgement I would like to thank E. Becker, V. Weispfenning, J. Schmid and R. Berr for many stimulating and helpful discussions related to this work.

1 The K-Radical

Notation
Convention 1: Throughout the following text we assume that all considered fields have characteristic 0 if not otherwise indicated.

Let K be a field of char 0. By C we denote its algebraic closure. A $K-$variety is the vanishing set

$$V(A) := \{x \in C^n \mid f(x) = 0 \; \forall f \in A\}$$

of an ideal $A \lhd K[X_1, \ldots, X_n]$ with points over the algebraic closure C of K. K is called a field of definition for V. The complements of these K-varieties in C^n form the open sets of the K-Zariski-Topology of C^n.
Convention 2: The topological concepts that we will use refer to the K-Zariski Topology unless otherwise mentioned. If it is clear to which base field K we refer we may drop the reference to K in the name of the concepts.

If M is any subset of C^n we denote by

$$I(M) := \{f \in K[X_1, \ldots, X_n] \mid f(x) = 0 \; \forall x \in M\}$$

the vanishing ideal of M. A K-variety V is called to be K-irreducible if it cannot be written as the union of two proper K-subvarieties. This is equivalent to say that $I(V)$ is a prime ideal of $K[X_1, \ldots, X_n]$. Every K-variety V possesses a unique irredundant decomposition $V = \bigcup V_i$ into irreducible K-varieties V_i. The V_i are called the K-irreducible components of V.
$K[V] := K[X_1, \ldots, X_n] \,/ I(V)$ denotes the coordinate ring of V. The elements of K[V] can be regarded as functions from V to C, the regular functions on V. A regular map from V to C^m is a map whose coordinate functions are regular functions. Two K-varieties are called isomorphic over K, if there are inverse regular maps defined over K from V to W and W to V. This is equivalent to the fact that the coordinate rings $K[V]$ and $K[W]$ are isomorphic as K-algebras.
Let V be an irreducible K-variety, $P = I(V)$. By $K(P) := K(V) :=$ quot$K[V]$ we denote the function field of V. As usual we call the elements of $K(V)$ K-rational functions on V. A K-rational map is a map whose coordinate functions are K-rational functions. Two K-varieties are called K-birationally isomorphic if there are inverse K-rational maps between them. This is equivalent to the fact that their function fields are isomorphic over K.
For $X \subset C^n$ we denote by $\overline{X}$ its closure in the K-Zariski topology. We have $\overline{X} = V(I(X))$.
Let $A \lhd K[X_0, \ldots, X_n]$ be a homogeneous ideal. Then we call its vanishing set in $\mathbb{P}^n$ a projective K-variety. These projective K-varieties define the closed sets of the projective K-Zariski topology on $\mathbb{P}^n$. The sets $U_i := \{X_i \neq 0\}$ define an open affine covering of $\mathbb{P}^n$: the U_i are homeomorphic to the affine space C^n with the (affine) K-Zariski topology by the map:
$\varphi_i : U_i \longrightarrow C^n$, $(x_0, \ldots, x_n) \longmapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$.
For a projective K-variety V those affine sets $U_i \cap V$, which are nonempty, are K-birationally equivalent to each other. We regard the affine space C^n as a subspace of $\mathbb{P}^n$ via φ_0^{-1}. The projective closure of an affine K-variety V is defined to be the closure of $\varphi_0^{-1}(V)$ in the projective K-Zariski topology.(The concept of K-varieties is developed e.g. in [Ku].)

1.1 Basic Problems of Effective Algebraic Geometry

We consider the following fundamental problems of computational geometry. For this let V be a K-variety. One might like to compute the following data of V:

1. The dimension of V,

2. The decomposition of V into its K-irreducible components,

3. The singular locus of V,

4. The Zariski-closure of $V \setminus W$, where W is another K-variety,

5. The K-Zariski-closure of the image of V under projections (elimination theory),

6. The Zariski-closure of the image of V under K-regular maps (the implicitization problem),

7. The projective closure of V.

Problems 1)-7) (and many more) are algorithmically solved for K-varieties. Our intention is to solve the corresponding problems for the K-rational points of varieties. To do that we introduce the concept of the K-radical.

1.2 The K-Radical

Let $V = V(A)$ be a variety. Then we denote by $V_K := V_K(A) := V(A) \cap K^n$ the set of K-rational points of A (resp. V). It is often necessary to solve the basic algebraic-geometric problems mentioned above for the K-rational points V_K of a variety. But the algorithms working over algebraically closed fields fail in general, when applied to a describing ideal for V_K. Even if this ideal is radical in the usual sense.
An easy example for this phenomenon is:
The dimension of $V_{\mathbb{R}}(X^2 + Y^2)$ is 0, but an algorithm working for algebraically closed fields would yield $\dim(X^2 + Y^2)$, which is 1.
The right concept to solve this tasks for non algebraically closed fields is the K-radical which we are going to define now:

Definition 1.1 (The K-Radical) *Let $A \lhd K[X_1, \ldots, X_n]$ be an ideal. Then we define the K-radical of A to be the vanishing ideal of the K-rational points of A:*

$$\sqrt[K]{A} := I(V_K(A)) \lhd K[X_1, \ldots, X_n].$$

A is called K-radical if $A = \sqrt[K]{A}$.

$\sqrt[K]{A}$ thus describes the K-Zariski closure of $V_K(A)$. The following properties of the K-radical are easy to verify:

Lemma 1.2 *Let $A, B \in K[X_1, \ldots, X_n]$. Then $\sqrt[K]{A \cap B} = \sqrt[K]{A} \cap \sqrt[K]{B}$.*

Proposition 1.3 *Let $A \lhd K[X_1, \ldots, X_n]$ be an ideal. Then the following statements are equivalent:*

1. *A is K-radical.*

2. *$V_K(A)$ is Zariski dense in $V(A)$ and A is a radical ideal.*

3. *A is the intersection of K-radical prime ideals.*

1.3 The Computational Solution of the Computational Problems for V_K

Note that a K-rational map of K-varieties $\varphi : V \longrightarrow W$ need not to be defined on the whole set V but only on K-Zariski dense open subset U of V. φ is called *dominant*, iff $\varphi(U)$ is Zariski dense in W. This property does not depend on the special choice of U.
The following immediate Lemma will be very helpful:

Lemma 1.4 *Let $\varphi : V \longrightarrow W$ be a dominant rational map and U be a Zariski dense open subset of V where φ is defined. Let X be any dense subset of V. Then $\varphi(U \cap X)$ is dense in W.*

Proof Easy.
Another preliminary Lemma we need is:

Lemma 1.5 *Let $X, V \subset C^n$, V a K-variety. Then $I(X \setminus V) = I(X) : I(V)$.*

Proof Easy.

Now we are able to answer the above problems for the K-rational points of a variety $V(A)$ provided we are able to compute K-radicals.

Ad 1 The dimension of $V_K(A)$ ist defined to be the dimension of the Zariski-closure of $V_K(A)$. $V_K(A)$ is described by $\sqrt[K]{A}$, and so we have $\dim V_K(A) = \dim \sqrt[K]{A}$.

Ad 2 Using the second assertion of Proposition 1.3 we see that the irreducible decomposition of $V_K(A)$ equals the usual irreducible decomposition of its Zariski-closure. So we compute the usual irreducible decomposition of $\sqrt[K]{A}$.

Ad 3 The singular locus of $V_K(A)$ is defined to consist of all the K-rational points of the singular locus of the Zariski-closure of $V_K(A)$. So one applies the usual algorithm to compute the singular locus to $\sqrt[K]{A}$.

Ad 4 If we want to compute the Zariski-closure of $V_K(A) \setminus V_K(B)$ Lemma 1.5 tells us that it can be described by the ideal quotient $\sqrt[K]{A} : \sqrt[K]{B}$.

Ad 5 To compute the Zariski closure of the projection $\overline{\pi(V_K(A)}$ we compute first the Zariski-closure $\overline{V_K(A)}$ by $\sqrt[K]{A}$. Because projections are continuous maps Lemma 1.4 yields now that $\overline{\pi(V_K(A)}$ equals $\overline{\pi(V_C(\sqrt[K]{A}))}$. We can compute the latter object by an usual algorithm.

Ad 6 Lemma 1.4 directly applies here again:
The Zariski-closure of $\varphi(V_K(A))$ equals the Zariski-closure of $\varphi(V_C(\sqrt[K]{A}))$.

Ad 7 $V_K(A)$ is dense in $V_C(\sqrt[K]{A})$ which again is dense in the projective closure W of $V_C(\sqrt[K]{A})$. So W is a projective variety containing $V_K(A)$ as a dense subset. So W_K is obviously the smallest set described by homogeneous equations containing $V_K(A)$. We can compute W by computing the projective closure of $\sqrt[K]{A}$ with an algorithm solving this task for algebraically closed fields.

By these considerations the computation of the K-radical turns out to be the central problem of effective algebraic geometry over non algebraically closed fields.

Remark At the first look it might seem unsatisfying that in studying projections and regular images of the K-rational points of a variety we get as results only the Zariski closures $\overline{\pi(V_K)}$ and not $\pi(V_K)$ itself. In the case of varieties over algebraically closed fields we are in principle able to compute $\pi(V_C)$ precisely (as a constructible set). But as long as we are working in the language of fields there is in general no precise description of $\pi(V_K)$ and the results we have are the best possible. The reason for this is that the only fields allowing quantifier elimination in the language of fields are algebraically closed fields as was shown by Macintyre, McKenna, van den Dries. (cf. [DrMaMc]).

Remark Another application of Lemma 1.4 and the computability of the real radical is the following: It is possible to decide for a given semi-algebraic set $S \subset R^n$ (for a real closed field R) whether S is a real algebraic variety. (A subset X of R^n is called a real algebraic variety iff there exists an R-variety V with $X = V_R$). To see this it is enough to notice that every semi-algebraic set $S \subset R^n$

can be (effectively) written as the projection of a real algebraic variety, i.e. there exists an R-variety $V \subset R^m, m \geq n$ such that $S = \pi(V_R)$ (cf. e.g. [BoCoRo]). The computability of the real radical yields that we can compute $W := \overline{\pi(V_R)}$ (applying item 5 of the list above). Obviously S is a real algebraic variety iff $S = W_R$. We can test whether the latter equation holds with an quantifier elimination algorithm for real closed fields.

Another nice consequence of Lemma 1.4 is the following

Proposition 1.6 *The property of an irreducible (affine or projective) K-variety V of containing a Zariski dense subset of K-rational points is a K-birational invariant of V. The following statements are equivalent:*

1. *V contains a dense subset of K-rational points.*
2. *Every model of $K(V)$ contains a dense subset of K-rational points.*

Proof Let V be an irreducible projective K-variety V s.t. w.l.o.g. $U_0 \cap V \neq \emptyset$. V contains a Zariski dense subset of K-rational points iff its affine part $\varphi_0(U_0 \cap V)$ (see subsection 1.1) has this property. So we can restrict the proof to affine varieties.
For this let W be a model of $K(V)$. Then there is a K-birational map $\psi : V \longrightarrow W$. Birational maps are especially dominant, so Lemma 1.4 proves the claim.

□

1.4 A Model Theoretic Characterization of K-Radical Prime Ideals

Proposition 1.6 suggests that there should be a characterization of K-radical prime ideals P using their function field $K(P)$.

Let $L \mid K$ be a field extension. K is said to be *existentially closed* in L if for every quantifier free formula φ in the language of rings $\mathcal{L} = (+, \cdot, 0, 1)$ with parameters in K and free variables $X_1, \ldots, X_n$ holds:

$$L \models \exists X_1, \ldots, X_n \, \varphi(X_1, \ldots, X_n) \Longrightarrow K \models \exists X_1, \ldots, X_n \, \varphi(X_1, \ldots, X_n)$$

We write $K \preceq_\exists L$.

Now we can prove:

Theorem 1.7 *Let $P \lhd K[X_1, \ldots, X_n]$ be a prime ideal. Then the following statements are equivalent:*

1. *P is K-radical*
2. *K is existentially closed in $K(P)$: $K \preceq_\exists K(P)$.*

Proof 1) $\Rightarrow$ 2)
This Theorem has been proved e.g. in [BeJa]. We liked to give a more geometric prove:

To prove $K \preceq_\exists K(P)$, we show that $K(P)$ can be embedded in an elementary extension of K. Because $I(V_K(P)) = P$, the system of sets

$$\{h \neq 0\} \cap V_K(P), \quad \text{for } h \notin P$$

has the Finite Intersection Property and so the system can be extended to an ultrafilter D on $V_K(P)$. For each $a \in V_K(P)$ let Q_a be the kernel of the evaluation map at a. We get a homomorphism

$$\varphi_a : K[X_1, \ldots X_n]/P \longrightarrow K[X_1, \ldots X_n]/Q_a$$

The maps $\varphi_a, a \in V_K(P)$ induce a ring homomorphism of the ultraproducts

$$\varphi : \prod\Big/_D K[X_1, \ldots X_n]/_P \longrightarrow \prod\Big/_D K[X_1, \ldots X_n]/Q_a := F$$

The first ultraproduct contains $K[X_1, \ldots, X_n]\ /P$ via the diagonal embedding d.

The ultrapower F is an elementary extension of K. $\varphi \circ d$ is injective, because any $I \in D$ is Zariski-dense in $V_C(P)$. So we can finally embed $K(P)$ into F.

□

1.5 What is Needed to Compute the K-Radical

To attack the problem of computing the K-radical we will reduce it in the following "Reduction-Algorithm" to some more tractable problems. The subproblems to which we reduce the K-radical computation can still be very difficult (or even unsolvable) in an algorithmical sense. But as we will see in Chapter 2 we can in fact treat these subproblems for a large class of fields in a satisfactory way. We mark the subproblems by (*) and collect them in the Theorem following the "Algorithm".

The Reduction–Algorithm

Input: $A \lhd K[X_1, \ldots, X_n]$
Output: $\sqrt[K]{A}$

Step 1 Compute $\sqrt{A}$.

Step 2 Compute the primary decomposition of $\sqrt{A} = \bigcap P_i$.

Step 3 Using Lemma 1.2 it suffices to compute the $\sqrt[K]{P_i}$'s:
(*) Decide whether P_i is K-radical.

If the answer is Yes, we have $\sqrt[K]{P_i} = P_i$.
(*) If the answer is No, find a polynomial $g \notin P_i$ with $g_{|V_K(P_i)} = 0$.
Go back to Step 1 where A is substituted by the ideal (P_i, g).

This "Algorithm" terminates because in the No-Case the dimension of the ideals considered decreases. More formally: the recursion depth of the algorithm is bounded by dim A.

Theorem 1.8 *The computation of K-radicals can be primitive-recursively reduced to the following tasks:*

1. *Decide for a prime ideal P whether it is K-radical or not.*
2. *If P is not K-radical find a polynomial g that vanishes on $V_K(P)$, but not on $V_C(P)$.*
3. *Factorization of univariate polynomials in $K[X]$.*

Proof The reduction process was described in the "Algorithm" above. Note that univariate factorization is needed to produce the primary decomposition of an ideal (cf. [BeWe], p.395).

□

Remark In the context of recursively presented fields, the tasks 1)-3) are indeed *subproblems* of the K-radical computation. We sketch now that the computability of K-radicals implies the solvability of 1)-3):

Ad 1 Compute $\sqrt[K]{P}$. Then P is K-radical iff $P = \sqrt[K]{P}$.

Ad 2 If P is not K-radical there is at least one of the generators of $\sqrt[K]{P}$ not contained in P.

Ad 3 We are able to check whether a univariate polynomial $f \in K[X]$ has a zero in K, because

$$\exists x \in K : f(x) = 0 \Longleftrightarrow \sqrt[K]{(f)} \neq K[X]$$

This decision allows to decide irreducibility of polynomials in $K[X]$. In the context of recursively presented fields this allows by a simple enumeration argument the construction of a factorization algorithm for $K[X]$ (cf. [MiRiRu], Theorem 1.8).

2 The Class of Fields $\mathcal{K}$

2.1 Definition of $\mathcal{K}$ and the Computation of K-Radicals in $\mathcal{K}$

Let $P \lhd K[X_1, \ldots, X_n]$ be a K-radical prime ideal, $V = V(P)$. Then V_K is Zariski-dense in V. So V_K is not contained in the singular locus of V, which is a proper subvariety of V. We have shown:

Proposition 2.1 *Let $P \lhd K[X_1, \ldots, X_n]$ be a K-radical prime ideal. Then $V_K(P)$ contains a regular point.*

We had seen in Theorem 1.8 that in order to determine the K-radical one needs a good characterization of K-radical prime ideals. To get such a characterization we demand now the converse of Proposition 2.1 . The following definition is the central definition of this work:

Definition 2.2

$$\mathcal{K} := \{K \mid \textit{ char } K = 0, \forall n \in \mathbb{N}\ \forall P \lhd K[X_1, \ldots, X_n], P \textit{ prime: } \\ P \textit{ is } K\textit{-radical} \iff V(P) \textit{ contains a regular } K\textit{-rational point}\}$$

For $K \in \mathcal{K}$ we are able to reduce the computation of the K-radical of an ideal to the computation of K-solutions of certain systems of algebraic equations with coefficients lying in K. Recall that the computation of the K-radical of an ideal $A \lhd K[X_1, \ldots, X_n]$ allows us directly to determine algebraic-geometric properties of $V_K(A)$.
The following main theorem will be the key to prove various properties for the K-rational points of a K-variety if $K \in \mathcal{K}$.

Theorem 2.3 *In $\mathcal{K}$ there is an algorithm to compute the K-radical using only*

1. *Decidability whether a system of algebraic equations with coefficients in K has a K-rational solution.*
2. *Factorization in $K[X]$.*

Proof In Theorem 1.8 we have reduced the computation of the K-radical to the following questions:

1. Decide for a prime ideal $P \lhd K[\ldots]$ whether it is K-radical or not.
2. If P is not K-radical, find polynomials not in P vanishing on $V_K(P)$.
3. Factorization of polynomials in $K[X]$.

Ad 1 Compute $d :=$dim P(cf. e.g. [KrWe]). $P = \sqrt[K]{P} \iff \exists x : x \in V_K(P) \wedge$ one of the $(n-d)$-minors of $\mathcal{J}(\mathcal{P})$ does not vanish at x. (Here $\mathcal{J}(\mathcal{P})$ denotes the Jacobian matrix of P.) The latter sentence can be decided using our first assumption.

Ad2 If $P \neq \sqrt[K]{P}$ then $V_K(P)$ does not contain a regular point, so $V_K(P) \subset \mathrm{Sing}(P)$. Because $\mathrm{Sing}(P)$ is a proper subvariety of $V_C(P)$, its describing equations, the $(n-d)$-minors of $\mathcal{J}(\mathcal{P})$ yield the desired additional polynomials.

Ad 3 This is assumed in our second assumption.

□

In the study of K-varieties it is convenient to sharpen the notion of irreducibility: a K-variety V (resp. its vanishing ideal $I(V) \lhd K[X_1, \ldots, X_n]$) is called *absolutely irreducible* (resp. *absolutely prime*) if V is irreducible regarded as a C-variety.

Lemma 2.4 *Let V be an irreducible K-variety containing a regular K-rational point. Then V is absolutely irreducible. If $P = I(V) \lhd K[X_1, \ldots, X_n]$, K is algebraically closed in $K(P)$.*

Proof The second assertion is a consequence of the first one (cf. [FrJa], Corollary 9.23). Assume the first assertion is not true, i.e. V splits over C into irreducible varieties V_i: $V = \bigcup V_i$. The absolute Galois group of K acts transitively on the set $\{V_1, \ldots, V_m\}$. If x is any K-rational point of V, x thus lies in all the V_i's and is thereby a singular point of V, a contradiction.

□

Luckily we do not have to verify the defining condition for $\mathcal{K}$ for all all prime ideals (resp. irreducible K-varieties) to prove that a field belongs to $\mathcal{K}$. The following Theorem shows that the membership to $\mathcal{K}$ can already be detected by studying plane K-curves. This will be an important tool to keep the proofs of Theorems about $\mathcal{K}$ transparent.

Theorem 2.5 (Plane Curve Condition) *A field K belongs to $\mathcal{K}$ if and only if for every plane irreducible K-curve C holds:*

$$Reg\ C_K \neq \emptyset \Rightarrow \#C_K = \infty.$$

In words:

> *If C contains a regular K-rational point, C contains infinitely many K-rational points.*

Proof "$\Longrightarrow$"
Because $K \in \mathcal{K}$, C contains a Zariski dense subset of K-rational points. The density forces C_K to be infinite.

"$\Longleftarrow$"
Let V be an irreducible variety containing a regular K-rational point x and let y be any point of V. We have to show that - assuming the Plane Curve Condition holds - $y \in \overline{V_K}$.
By Lemma 9.1 of [JaRa] we can draw a curve through x and y: there is an absolutely irreducible curve C defined over K such that:
1) $C \subset V$
2) $x, y \in C$
3) x is a regular point of C.
We show now that we can find a model E of C in the plane containing a regular K-rational point. Applying the Plane Curve Condition to E we get that E contains a Zariski dense subset of K-rational points. Because this property is a birational invariant of E (cf. Proposition 1.6) also $\overline{C_K} = C$. So $y \in \overline{C_K}$ and a forteriori $y \in \overline{V_K}$.
The construction of E:
Let E_1 be the projective closure of C. Then x is also a regular K-rational point of E_1.

Applying e.g. Hironokas Theorem on the resolution of singularities we can find a K-regular map $\varphi : E_2 \longrightarrow E_1$, where E_2 is a smooth projective K-curve. Furthermore φ posesses a K-rational inverse ψ defined at the regular points of E_1. Because x is regular $p := \psi(x)$ is a regular K-rational point of E_2.

We use in the following two standard theorems about the embeddings of smooth curves in the projective space (cf. e.g. [Ha]):

> If D is a smooth curve in $\mathbb{P}^n, n \geq 4$. Then a general projection centered at a point O (with coordinates in C) is an isomorphism.

If O is described by n linear forms $O = \{L_1 = 0, \ldots, L_n = 0\}$ then the projection $\pi : \mathbb{P}^n \setminus \{O\} \longrightarrow \mathbb{P}^{n-1}$ is given by by $\pi(z) = (L_1(z), \ldots, L_n(z))$. So we can choose O with coordinates in K such that $\pi(D)$ is a curve isomorphic to D described over K. Because π is defined

over K, K-rational points are mapped to K-rational points.
Applying this process several times to E_2 we end up with an K-isomorphic K-curve $E_3 \subset \mathbb{P}^3$ containing a regular K-rational point P.
We use now:

> If $D \subset \mathbb{P}^3$ is a smooth curve. Then a general projection of D to $\mathbb{P}^2$ centered at O (with coordinates in C) yields a curve having only nodes as singularities.

Now we want to exclude that P is mapped to a node. P is mapped under a projection centered at O to a node iff the line $\overline{PO}$ intersects the curve in an additional point. So we have to exclude that O is taken from the set collecting the secants of D through P. This collection can be described as the image of the morphism $D \setminus \{P\} \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3$ sending (Q,t) to the point (suitably parametrized) of the secant through P and Q. This image has at most dimension 2. So we can conclude:

> If $D \subset \mathbb{P}^3$ is a smooth curve containing a regular K-rational point P. Then a general projection of D to $\mathbb{P}^2$ centered at O (with coordinates in C) yields a curve having only nodes as singularities where the image of P is none of them.

So we can choose again a suitable O over K and by this find the curve E looked for above.

□

As a first application of the Plane Curve Condition we have

2.2 Model Theoretic Properties of $\mathcal{K}$

Theorem 2.6 *$\mathcal{K}$ is an elementary, inductive class in the language of rings.*

Proof First we take a set of axioms $\sum$ expressing the property of being a field of char 0. Now we axiomatize the Plane Curve Condition:
We express by the axiom A_{nd}, $n, d \in \mathbb{N}$ that every irreducible curve given by a polynomial $f(X,Y)$ of degree n having a regular K-rational point contains at least d K-rational points:

$$\mathbf{A_{nd}} : \forall f \in K[X,Y], \deg f = n :$$
$$\Big(\forall g, h \in K[X,Y], 1 \leq \deg g, \deg h \leq n-1, \text{ gilt:}$$
$$f \neq gh \implies \big[\exists x : x \in \mathrm{Reg}(V(f)) \Longrightarrow \exists x_1, \ldots x_d : \bigwedge_{1 \leq i < j \leq d} x_i \neq x_j \wedge f(x_i) = 0\big]\Big)$$

(If $f \in K[X,Y]$ is irreducible we can express "$x \in \mathrm{Reg}(V(f))$" by "$\frac{\partial f}{\partial X}(x) \neq 0 \ \vee \ \frac{\partial f}{\partial Y}(x) \neq 0$" .)
The collection of $\sum$ and the A_{nd}'s is an axiom scheme for the Plane Curve Condition.

The A_{nd} can be easily rewritten as universal existential sentences.

$$\forall f, \deg f = n, \ \forall x \ \exists g, h, 1 \leq \deg g, \deg h \leq n-1 \ \exists x_1, \ldots, x_d :$$
$$f = gh \vee \big[f(x) = 0 \Longrightarrow x \in \mathrm{Sing}V(f)\big] \ \vee \bigwedge_{1 \leq i < j \leq d} x_i \neq x_j \wedge f(x_i) = 0$$

Thus $\mathcal{K}$ is an inductive class.

□

Corollary 2.7 *Every ultraproduct of fields in $\mathcal{K}$ lies again in $\mathcal{K}$.*

2.3 Fields in $\mathcal{K}$

Fields that play a role in different mathematical disciplines like Algebraic Number Theory, Real Algebraic Geometry (of higher level), Galois Theory and Valuation Theory are in $\mathcal{K}$:

Theorem 2.8 *The following fields belong to $\mathcal{K}$:*

1. $\mathbb{C}$, *algebraically closed fields, pseudo-algebraically closed fields (PAC-Fields)*
2. $\mathbb{R}$, *real closed fields, pseudo-real closed fields (PRC-Fields), the field of totally real numbers*
3. $\mathbb{Q}_p$, *p-adically closed fields, pseudo-p-adically closed fields (PpC-Fields), the field of totally p-adic numbers.*
4. *(Non trivial) Henselian fields, (non trivial) valued fields fulfilling the implicit function theorem. As examples of Henselian fields there are:*

   Real closed fields of higher level and generalized real closed fields,

   Power series fields: $F((t))$, $F((\Gamma))$ (for an abelian ordered group Γ).

Global fields do not belong $\mathcal{K}$:

Theorem 2.9 $\mathbb{Q}$ *and finitely generated extension fields of $\mathbb{Q}$ do not belong to $\mathcal{K}$.*

Theorem 2.10 *Let K be a field. Then every finitely generated extension field of K of transcendence degree at least 1 does not belong to $\mathcal{K}$.*

Before we prove the theorems we need an auxiliary lemma:

Lemma 2.11 *Let V with $I(V) = P$ be an irreducible K-variety containing a regular K-rational point. Then there is a K-place $\lambda : K(P) \longrightarrow K \cup \infty$.*

Proof Let $\varphi : K[V] \longrightarrow K$ be the homomorphism gained by substituting in the regular K-rational point x. Then φ extends canonically to a homomorphism $\varphi : \mathcal{O}_x \longrightarrow K$, where $\mathcal{O}_x$ denotes the local ring of x. Because x is regular, $\mathcal{O}_x$ is a regular local noetherian ring. Now we can apply Lemma 1.4 of [Be2] which states that in this situation we can extend φ to a place $\lambda : \text{quot}\mathcal{O}_x \longrightarrow K \cup \infty$. Now $\text{quot}\mathcal{O}_x = K(P)$ and we are done.

□

Proof of Theorem 2.8

Ad 1 Claim: Algebraically closed fields are in $\mathcal{K}$:
Let K be an algebraically closed field. Then K is existentially closed in any extension field and so the defining condition of $\mathcal{K}$ automatically fulfilled.

Claim: PAC-fields are in $\mathcal{K}$:
PAC fields were introduced by Ax and were studied extensively by Fried and Jarden. They can be defined as follows:

Each non-empty absolutely irreducible variety defined over K has a K-rational point.

Following [FrJa], Prop. 10.1, PAC fields (of char 0) can be characterized as follows:

K is PAC iff for every absolutely irreducible variety V defined over K, V_K is Zariski dense in V.

Now let P be a prime ideal such that $V = V(P)$ contains a regular K-rational point . By Lemma 2.4 V is absolutely irreducible. Because K is PAC, V_K is Zariski dense in V and so P is a K-radical ideal.

Ad 2 It is wellknown that real closed fields fulfill the defining condition of $\mathcal{K}$ (cf. [BoCoRo], Proposition 3.3.15).

Claim: PRC fields are in $\mathcal{K}$:
PRC fields were introduced by Prestel in [Pr] and can be characterized as follows:

> *A field K is PRC iff K is existentially closed in every field extension L in which K is algebraically closed and to which all the orderings of K extend.*

Now let K be a PRC field and P be a prime ideal containing a regular K-rational point . Because of Lemma 2.4 K is algebraically closed in $K(P)$. Because of Lemma 2.11 there is a K-place $\lambda : K(P) \longrightarrow K \cup \infty$. If P is any ordering of K, $\lambda^{-1}(P)$ can be extended to an ordering of $K(P)$ containing P (cf. [Be2], proof of Theorem 1.3). So we know that any ordering of K extends to $K(P)$. Because K is PRC we can conclude that K is existentially closed in $K(P)$. This implies by Proposition 1.7 that P is K-radical.
The field of totally real numbers is PRC (cf [Po]).

Ad 3 $\mathbb{Q}_p$ is a p-adically closed field (cf. [PrRo]). p-adically closed fields are especially Henselian (cf. [PrRo], Theorem 3.1). That Henselian fields belong to $\mathcal{K}$ will be shown later on.
Claim: PpC fields belong to $\mathcal{K}$:
PpC fields can be characterized as follows (cf. [Gro], Proposition 4.04):

> *A formally p-adic field K is PpC iff K is existentially closed in each field extension L that fulfills the following conditions:*
> *1) K is algebraically closed in L*
> *2) all p-valuation rings of K can be extended to a p-valuation ring of L.*

The proof of membership to $\mathcal{K}$ can be done analogously to the proof for PRC-fields. Now let K be a PpC field and P be a prime ideal containing a regular K-rational point x. Because of Lemma 2.4 K is algebraically closed in $K(P)$ and $V = V(P)$ is an absolutely irreducible variety. Let O be a p-valuation ring of K. By Lemma 2.11 there is a K-place $\lambda : K(P) \longrightarrow K \cup \infty$. $\lambda^{-1}(O)$ is a p-valuation ring of $K(P)$ extending O (by [PrRo], Chapter 7 or an easy calculation). The proof can now becocompleted exactly as in the case of PRC-fields.
The field of totally p-adic numbers is PpC (cf. Po]).

Ad 4 Henselian fields fulfill the implicit function theorem for plane curves as follows immediately from a Theorem of Prestel and Ziegler ([PrZi], Theorem 7.4). We have:

> *In a Henselian field (K, τ) holds: Let $f \in K[X, Y]$ $a, b \in \mathcal{K}$ with $f(a, b) = 0$ and $\frac{df}{dy}(a, b) \neq 0$. Then there are $U, V \in \tau$ such that $\forall x \in a + U \ \exists!\ y \in b + V$ with $f(a, b) = 0$.*

Now we use the Plane Curve Condition. The non-triviality of the valuation assures that all (non-empty) open subsets $U \in \tau$ are infinite. It follows from the implicit function theorem for curves quoted above that C contains infinitely many K-rational points and we are done.
The class of fields fulfilling the implicit function theorem, the class of the so called t-Henselian fields introduced by Prestel and Ziegler in [PrZi], is strictly larger than the class of Henselian fields. Our argumentation above shows that even t-Henselian fields belong to $\mathcal{K}$.

Real closed fields of higher level were introduced by Becker in (cf. [Be1] for their definition). They are Henselian (cf. [Be1] Corollary 3.2). Generalized real closed fields introduced by Schwartz are also Henselian (cf. [Schw], [Ja]).

Power series fields $F((t))$ and more general $F((\Gamma))$ are Henselian (cf. e.g. [Kuh]).

□

Proof of Theorem 2.9
Let E be the elliptic curve given by the equation: $y^2 = x^3 - x$. E has rank 0 (cf. [SiTa], p.94). We have $E_{\mathbb{Q}} = \{(0,0),(1,0),(-1,0)\}$. E is smooth. So the Plane Curve Condition is violated and we get $\mathbb{Q} \notin \mathcal{K}$.
Using the Theorem of Faltings on the Mordell conjecture (cf. [Fa]) any smooth curve C of genus $g \geq 2$ defined over $\mathbb{Q}$ has only finitely many rational points over any given number field. This property of C implies by a Theorem of Lang (cf. [La2]) that C has only finitely many points over any finitely generated extension of $\mathbb{Q}$. So finitely generated extensions of $\mathbb{Q}$ violate the Plane Curve Condition for C.
At the end we describe a nice method to construct over any field K (hyperelliptic) curves of higher genus containing a K-rational point . For this let $a_1, \ldots, a_{2g+1}$ be distinct elements of K. Let C be the curve described by the equation: $Y^2 = \prod(X - a_i)$. Then C is smooth and has at least the $2g+1$ K-rational points $(a_i, 0)$.

□

Proof of Theorem 2.10
Let L be a finitely generated extension of K of transcendence degree at least 1. Let $t \in L$ be a transcendental element over K. By Lemma 3.9 there is a smooth $K(t)$-curve having at least one but only finitely many L-rational points. So the Plane Curve Condition is violated for L.

□

Corollary 2.12 *No rational function field belongs to $\mathcal{K}$.*

We have shown that the theory of $\mathcal{K}$ can be axiomatized by universal-existential sentences. This is in fact best possible:

Corollary 2.13 *Th($\mathcal{K}$) cannot be axiomatized by existential sentences. Th($\mathcal{K}$) cannot be axiomatized by universal sentences.*

Proof A theory can be axiomatized by universal axioms iff if it is preserved under submodels (cf. [ChKe], Theorem 5.2.4.). But a field $K \in \mathcal{K}$ contains the submodel $\mathbb{Q}$ which is not in $\mathcal{K}$.
A theory can be axiomatized by a set of existential sentences iff it is preserved under extensions (cf. [ChKe], Theorem 5.2.3). But for $K \in \mathcal{K}$, $K(t)$ does not belong to $\mathcal{K}$.

□

2.4 Closure Principles of $\mathcal{K}$

Because $\mathcal{K}$ is elementary $\mathcal{K}$ is closed under elementary equivalence and under taking ultraproducts. Because $\mathcal{K}$ is inductive it is closed under taking direct limits. We are going to analyse three further closure properties:

Theorem 2.14 (Algebraic Going Up) *Let $K \in \mathcal{K}$ and $L \mid K$ be an algebraic extension. Then $L \in \mathcal{K}$.*

Proof of Theorem 2.14
We first study the case of a finite extension $L \mid K$.
Let V be an irreducible L-variety containing a regular L-rational point. The technique of the Weill-descent (cf. e.g. [FrJa]) allows us to associate to V a suitable irreducible L-variety $\tilde{V}$ s.t.

1. $\pi(\tilde{V}) = V$, i.e. V is the image of $\tilde{V}$ under a projection.
2. $\tilde{V}$ contains a regular L-rational point x.
3. There is an L-isomorphism $\varphi : \tilde{V} \longrightarrow W$, where W is a K-variety.
4. $\varphi(\tilde{V}_L) = W_K$

To prove the Theorem we have to show that the L-rational points are dense in V. By 1) and the Lemma 1.4 it is sufficient to show that $\overline{\tilde{V}_L} = \tilde{V}$. This can be seen as follows: $\varphi(x)$ is a regular K-rational point of W. Because $K \in \mathcal{K}$ we have $\overline{W_K} = W$. 3), 4) and 1.4 imply now that $\tilde{V}_L$ is dense in $\tilde{V}$.
This result generalizes to infinite algebraic extensions because $\mathcal{K}$ is inductive and thus closed under taking direct limits of fields.

□

Theorem 2.15 *$\mathcal{K}$ is not closed under taking finite intersections. There are fields $K, L \in \mathcal{K}$, but $K \cap L \notin \mathcal{K}$.*

Proof We show that we can construct for every countable field F (which may be not in $\mathcal{K}$) two field extensions K, L of F with $K, L \in \mathcal{K}$ whose intersection equals F.
We first describe a method how to "increase" the set of rational points on a curve:

Let F be a field, $f \in F[X, Y]$ be an irreducible polynomial having a F-regular point. Then f has a "new" point in its function field $F(f)$, namely $(X, Y)/(f)$. We can regard $F(f)$ as an algebraic extension of $F(X)$. Because of Lemma 2.4 F is algebraically closed in $F(f)$ and f is an irreducible curve over $F(f)$.
Now we apply the same process to $F(f)$ and get a field $(F(f))(f)$ in which f has at least two more rational points. By repeating this process countably many times and taking the union of all these fields we end up with a field F_f in which f has infinitely many rational points. So we constructed a field in which the Plane Curve Condition is fulfilled for f. An iteration of this process yields a field extension $K \in \mathcal{K}$ of F.

Let us assume that the indeterminates we needed to produce the function fields (and thus K) were taken from the set $M := \{X_1, X_2, X_3, \ldots\}$. We repeat the same process now with a disjoint set of indeterminates $N := \{Y_1, Y_2, Y_3, \ldots\}$ and generate by this another field extension L of F which is again in $\mathcal{K}$. We regard K and L as subfields of the algebraic closure of $F(M, N)$.
Claim: $K \cap L = F$
Assume there were an $\alpha \notin F$ with $\alpha \in K \cap L$. Because F is algebraically closed in K, α is transcendental over F. Now choose finite subsets $\tilde{M} \subset M$ and $\tilde{N} \subset N$ such that α is algebraic over $F(\tilde{M})$ and $F(\tilde{N})$. (That $\tilde{M}$ and $\tilde{N}$ can be chosen finite follows easily by a nested induction on the building process of the field K (resp. L).) Because α is transcendental over F we can exchange α against an element of $\tilde{M}$ (resp. $\tilde{N}$) by maintaining the property of being an algebraically set independent over F. But now these sets have the element α in common contradicting the fact that the transcendence degree of $F(M, N) \mid F$ equals $\mid M \mid + \mid N \mid$. So the last claim is proved.

□

Remark The situation does not get better if one restricts oneselve to the intersection of an (infinite) descending sequence of fields in $\mathcal{K}$: Van den Dries and Smith (cf. [DrSm], Theorem 3) constructed

a descending chain $K_0 \supset K_1 \supset K_2 \supset \ldots$ of PAC-fields of char 0 (which are in $\mathcal{K}$), s.t. there intersection $\bigcap K_i$ equals $\mathbb{Q}$ which is not in $\mathcal{K}$.

Considering the Plane Curve Condition and the fact an algebraic extension of a field in $\mathcal{K}$ lies again in $\mathcal{K}$ we see that a field K in $\mathcal{K}$ has to have "many" points: If C is a curve over K, a regular K-rational point forces C to have infinitely many points with coordinates in K. So it would be interesting to know whether the following fields have "enough" points to belong to $\mathcal{K}$.

Open Problem 2.16 *Do $\mathbb{Q}_{ab}$, $\mathbb{Q}_{nil}$ and $\mathbb{Q}_{sol}$, the maximal abelian (resp. nilpotent, solvable) extensions of $\mathbb{Q}$ belong to $\mathcal{K}$?*

It was shown by Frey (cf. [Fr]) that $\mathbb{Q}_{ab}$ and $\mathbb{Q}_{nil}$ are not PAC. For $\mathbb{Q}_{sol}$ this question is open.

Open Problem 2.17 *Is $\mathcal{K}$ stable under "digging holes"? This means more precisely: Let $L \in \mathcal{K}$, $\alpha \in L \setminus \mathbb{Q}$ and let K be a maximal subfield of L not containing α. Does this imply $K \in \mathcal{K}$?*

This would imply that $\mathcal{K}$ has no minimal elements. The corresponding problem for PAC fields was posed by Macintyre and is still unsolved for PAC fields of char 0. For PAC fields of positive characteristic a negative answer to this question has been given by J. Koenigsmann (private communication). A special instance of this problem is the following one:

Open Problem 2.18 *Is there a "Finite Algebraic Going Down Theorem" for $\mathcal{K}$? More precisely: Let $L \in \mathcal{K}$ and $L = K(\alpha)$ be an algebraic extension. Does this imply $K \in \mathcal{K}$?*

Applying the Plane Curve Condition a positive answer to the last problem is equivalent to the following statement about curves:

> *If $L \mid K$ is a finite extension and if there is a plane K-curve having one but only finitely many regular K-rational points then there is a plane L-curve with this property.*

Proposition 2.19 *Let $L \in \mathcal{K}$ and let $K \preceq_\exists L$. Then $K \in \mathcal{K}$.*

Proof Let V be a K-variety. Because $K \preceq_\exists L$ we have $\#V_K = \#V_L$. Applying this to K-curves yields that the Plane Curve Condition is fulfilled for K.

□

As another closure principle we show that $\mathcal{K}$ is closed under a natural local-global-principle.

Definition 2.20 *Let K be a field with algebraic closure C. Let $\mathcal{M}$ be a set of fields $L_i \subset C, i \in I$ which all contain K. We call the L_i's localities. We say that K fulfills a* local-global-principle w.r.t to *M iff the following condition is fulfilled:*

> *For every smooth K-variety V holds:*
> $(\forall i \in I : V_{L_i} \neq \emptyset) \Longrightarrow V_K \neq \emptyset$

Proposition 2.21 *Let K be a field which satisfies a local-global principle where all the localities belong to $\mathcal{K}$. Then K itself belongs to $\mathcal{K}$.*

Proof We show that K fulfills the Plane Curve Condition. Assume this condition were violated. Then there is an irreducible K-curve C that contains a regular K-rational point s.t. $\#C_K < \infty$. By throwing away the singularities and the finitely many K-rational points using Rabinovich's trick we obtain a smooth K-curve E that is K-birational to C and that has no K-rational points. We get a contradiction because the local-global principle does not hold for E: Because $L_i \in \mathcal{K}$ and Reg $C_{L_i} \neq \emptyset$ we get $\#C_{L_i} = \infty$ and for E as a L_i-birational image of C we thus get $E_{L_i} \neq \emptyset$.

□

Remark The last Proposition is a slight generalization of an idea of Pop who proves an analogous result where the localities are assumed to be Henselian or real closed fields (cf. [Po]). He observed that the concepts of PAC, PRC, PpC-fields can be naturally presented in this frame (with suitably chosen sets of localities). This yields an alternative prove that the "pseudo classically closed fields" belong to $\mathcal{K}$. Refining the conditions on the set of localities Pop further proves that the field of totally real and totally p-adic numbers belong to $\mathcal{K}$.

To underline the importance of local-global principles we would like to note that Rumeleys local-global principle for algebraic diophantine equations was the breakthrough to give a positive answer to the solvability of Hilberts 10'th problem for the algebraic integers $\tilde{\mathbb{Z}}$ (cf. [Ru]). We hope that these ideas can be clarified and put together in the future to develop the theory of a class $\mathcal{R}$, the generalization of $\mathcal{K}$ to rings.

2.5 A Characterization of Fields in $\mathcal{K}$ using Laurent Series Fields

The following Theorem is due to F. Pop:

Theorem 2.22 *A field K belongs to $\mathcal{K}$ iff K is existentially closed in the Laurent series field $K((t))$.*

Proof $\Leftarrow$ was shown in Proposition 2.19. $\Rightarrow$: It is sufficient to show that K is existentially closed in every finitely generated subfield L of $K(t)^h$, the henselisation of $K(t)$ w.r.t. to the canonical valuation. Such a field L can be presented as a function field of a smooth K-curve having a (regular) K-rational point . So Theorem 1.7 yields: $K \preceq_\exists L$. The details: Let L be such a finitely generated extension of transcendence degree 1 over K. We may assume that L is generated by elements $x_1, \ldots, x_m$ of the valuation ring $\mathcal{O} = \{x \in K(t)^h \mid v(x) \geq 0\}$. Let $R := K[x_1, \ldots, x_m]$ be the affine K-algebra generated by these elements. The integral closure $\tilde{R}$ of R in L is generated by elements $y_1, \ldots, y_k \in \mathcal{O}$. Let C be the K-curve having the so presented $\tilde{R}$ as its coordinate ring. Because $\tilde{R}$ is integrally closed C is smooth. C contains the point $(y_1, \ldots y_k) \in \mathcal{O}^k \subset K[[t]]^k$. Specializing t to 0 gives us a K-rational point on C. This point is regular because C is smooth. This is what we had to show.

□

Remark One benefit we get from this Theorem is that it allows to transfer certain statements from the class of Laurent series fields to $\mathcal{K}$. As an application of this idea we will see in the next subsection how this helps to shed some light to the understanding of the existential theory of $\mathcal{K}$. Laurent series fields carry more structure: As Henselian valued fields, power series fields carry e.g. a natural topology and fulfill the for geometric reasoning very useful Implicit Function Theorem. We give an example of a transferable problem, a Bezout type Bound:

Open Problem 2.23 (Bezout Problem for $\mathcal{K}$) *Is the following true for all fields in $\mathcal{K}$? Let $A \lhd K[X_1, \ldots, X_n]$ be an ideal which can be generated by polynomials of degree $\leq d$ and let $\#V_K(A) < \infty$. Then $\#V_K(A) < d^{n^{O(1)}}$.*

For algebraically closed or real closed fields the answer is Yes by the well known Affine Bezout Theorem (cf. [He], [Sch]), resp. the Thom-Milnor Bounds (cf. [BoCoRo]). These geometric finiteness theorems are of fundamental importance for complexity theory over algebraically closed or real closed fields. This problem is transferable because we have for $K \in \mathcal{K}$ and a K-variety V: $\#V_K = \#V_{K((t))}$. In Section 4 we will show a weaker result: the bound on the right side of the above implication can be chosen to be of a double exponential type, more precisely it can be chosen to be $d^{2^{n^{O(1)}}}$.

2.6 Undecidability of the Theory of $\mathcal{K}$

Theorem 2.24 *The elementary theory of $\mathcal{K}$ is undecidable. Furthermore there is no decidable theory between $Th(\mathcal{F})$ and $Th(\mathcal{K})$, where $\mathcal{F}$ denotes the class of all fields.*

Proof Let $\mathcal{L}$ be the class of all PAC-fields of char 0. Then $\mathcal{L} \subset \mathcal{K} \subset \mathcal{F}$ and so $\mathrm{Th}(\mathcal{F}) \subset \mathrm{Th}(\mathcal{K}) \subset \mathrm{Th}(\mathcal{L})$. To prove the theorem it is sufficient to prove that there is no decidable theory between $\mathrm{Th}(\mathcal{L})$ and $\mathrm{Th}(\mathcal{F})$.

Undecidability results for the theory of PAC-Fields were proved by Ershov (cf. [Er]) and independently by Cherlin, van den Dries and Macintyre (cf. [ChDrMa]). Their ideas were refined by Fried and Jarden to show that an even stronger statement is true: The theory of perfect PAC fields and the theory of all fields are recursively inseparable. Some minor modifications of the latter proof yield that also the theory of $\mathcal{L}$ and $\mathcal{F}$ are recursively inseparable.

□

In contrast to the undecidability of the whole theory of PAC fields of char 0, the *existential theory* of PAC fields of char 0 is decidable (cf. [FrJa], Section 19.4). Let us now turn to this question for $\mathcal{K}$.

Proposition 2.25 *Let $\mathcal{P} := \{K((t)) \mid \ char(K) = 0\}$. Then we have:*
$$Th_\exists(\mathcal{K}) = Th_\exists(\mathcal{P}) = Th_\exists(\mathbb{Q}((t))).$$

Proof Power series fields belong to $\mathcal{K}$ (cf. Theorem 2.8). So we get: $\mathbb{Q}((t)) \subset \mathcal{P} \subset \mathcal{K}$. This induces the inverse inclusions for the corresponding existential theories: $\mathrm{Th}_\exists(\mathcal{K}) \subset \mathrm{Th}_\exists(\mathcal{P}) \subset \mathrm{Th}_\exists(\mathbb{Q}((t)))$. We prove now the remaining inclusions:
Ad $\mathrm{Th}_\exists(\mathcal{P}) \subset \mathrm{Th}_\exists(\mathcal{K})$: Let φ be an existential statement which holds in all fields of $\mathcal{P}$. We have to show that φ holds in all fields of $\mathcal{K}$. So let $K \in \mathcal{K}$. Then $K((t)) \in \mathcal{P}$ and thus $K((t)) \models \varphi$. Using the characterization of fields in $\mathcal{K}$ via Laurent series fields (cf. Theorem 2.22) we know that K is existentially closed in $K((t))$ and thus $K \models \varphi$.

Ad $\mathrm{Th}_\exists(\mathbb{Q}((t))) \subset \mathrm{Th}_\exists(\mathcal{P})$: Let φ be an existential statement s.t. $\mathbb{Q}((t)) \models \varphi$ and let $K((t)) \in \mathcal{P}$. Because K is of char 0, $\mathbb{Q}((t))$ embeds naturally in $K((t))$. So $K((t)) \models \varphi$.

□

Remark It was pointed out to me by Weispfenning that it follows from [We1] that the decidability of existential sentences over $\mathbb{Q}((t))$ can be recursively reduced to the decidability of existential sentences over $\mathbb{Q}$ (cf. [We1], Theorem 3.3 and Theorem 3.6, compare also [We3], Lemma 4.11). Thus we get that the decidability of the existential theory of $\mathbb{Q}$ yields the decidability of the existential theory of $\mathcal{K}$. Unluckily this does not answer whether $Th_\exists(\mathcal{K})$ is decidable because the decidability of the diophantine theory of $\mathbb{Q}$ is the biggest open problem in the area dealing with variations of Hilberts 10'th Problem (cf. [Ph] for a recent survey of results in this area). Anyhow it gives an indication that it will be hard to show the undecidability of $Th_\exists(\mathcal{K})$. So we still have the following

Open Problem 2.26 *Is the existential theory of $\mathcal{K}$ decidable?*

3 Model Theoretic Aspects of Algebraic Geometry

Notation We work in the following with first order formulas in the language of rings $\mathcal{L}(+,\cdot,0,1)$. Let K be a field. An ideal A in a polynomial ring over K is said to be given in (n,m,d)-format (or for short to be of (n,m,d)-format) if $A \lhd K[X_1,\ldots,X_n]$ and it is given as follows: $A=(f_1,\ldots,f_m)$, where $\deg f_i \leq d$. If φ is an elementary formula with free variables for the coefficients appearing in the generating system of an ideal A of (n,m,d)-format we denote loosely speaking by $\varphi(A)$ the formula that is obtained by substituting the free variables of φ by the coefficients appearing in the (given) generating set for A. In the notation of formulas φ expressing properties of ideals of (n,m,d)-format we usually drop the dependence on (n,m,d).

For a finite set $P \subset K[X_1,\ldots,X_n]$ we denote by $\deg P$ the maximal degree of a polynomial appearing in P. Let $A \lhd L[X_1,\ldots,X_n]$. By $\deg(A)$ we denote the minimum of all degrees $\deg P$ for all finite generating sets P of A. (This notion of degree has noting to do with the degree of the variety described by A.)

A well known fact which simplifies the work with ideals of certain formats is the following:

Lemma 3.1 *Let $A \lhd K[X_1,\ldots,X_n]$, $\deg A \leq d$. Then A can be represented as an ideal of (n,m,d)-format, where $m \leq (d+1)^n$.*

Remark The use of this Lemma will be: Suppose we want to show that there exists a bound (n,m,d) s.t. ideals of (n,m,d) format solve a task, we are interested in, it is sufficient to bound n and d. If we are working in a polynomial ring with a fixed number of variables it is sufficient to bound d.

3.1 First Order Definability of Algebraic-Geometric Properties of K-Varieties

The central goal of this whole section is to show that basic algebraic-geometric properties of the K-rational points of K-varieties for fields in $\mathcal{K}$ can be expressed by elementary formulas. We are mainly interested in the same kind of problems for varieties we studied in Section 1 from a computational point of view. As an intermediate step we report in this subsection that the corresponding properties of K-varieties and some ideal theoretic properties of ideals in polynomial rings can be expressed by elementary formulas. These will be the tools to construct formulas working for K-rational points. The results of this subsection - in which we deal with points in the algebraic closure - are well known or seem to be folklore. For the convenience of the reader we give at least some references. Proofs can usually be derived directly from the existing bounds of effective algebraic geometry and Gröbner base theory. Model theoretic proofs for the existence of many bounds have been given e.g. by A. Robinson and L. van den Dries. Let us first turn to some ideal theoretic properties.

Notation We explain the notation by an example. When we say that for ideals A, B, C, the property

$$\text{“}C = A \cap B\text{”}$$

can be expressed elementarily we mean that for all formats (n,m,d) there exists a first order formula φ s.t. for all fields K and all ideals A, B, C of (n,m,d)-format holds:

$$K \models \varphi(A,B,C) \text{ iff } C = A \cap B$$

Not to overload notation we drop the dependence of φ on the formats as was already mentioned. This notation can be adapted suitably to similar situations: certainly the statement

$$\text{“}f \in A\text{” is elementary}$$

means: For all formats (n,m,d) and natural numbers d' exists an elementary formula ψ (with free variables for the coefficients appearing in f and in the defining polynomials of A) s.t. for all fields

K and all ideals A of (n,m,d)-format and for all polynomials $f \in K[X_1,\ldots,X_n]$ with deg $f \leq d'$ holds:

$$K \models \psi(f,A) \text{ iff } f \in A.$$

If we use expressions like "$V(A)$" in our formulas it will become clear from the context to which field we refer: "$K \models V(A) = V(B)$" means:
"$\forall x \in K^n : x$ is a zero of $A \Leftrightarrow x$ is a zero of B".
"$C \models V(A) = V(B)$" means:
"$\forall x \in C^n : x$ is a zero of $A \Leftrightarrow x$ is a zero of B".
By Sing $V(A)$ (resp. Reg $V(A)$) we denote the singular (resp. regular) locus like they are build in the algebraically closed case

Proposition 3.2 *The following ideal theoretic statements are elementary. Furthermore the formulas expressing them can be chosen to be quantifier free:*

1. "$f \in A$"
2. "$A \subset B$"
3. "$A = B$"
4. *"A is absolutely prime", i.e the ideal generated by A in the ring* "$C[X_1,\ldots,X_n]$ *is irreducible.*
5. *"A is radical"*
6. "$B = \sqrt{A}$ "
7. "$C = A \cap B$"
8. "$C = A : B$"

Proof The proofs follow directly from the existence of bounds for the objects considered. These bounds were derived by algebraic and/or model theoretic methods (cf. e.g. [Se], [Dr1]).

Proposition 3.3 *Let* $A \lhd K[X_1,\ldots,X_n]$ *be an ideal of* (n,m,d)*-format.*

1. *deg* $\sqrt{A} \lhd K[X_1,\ldots,X_n] \leq d^{2^{O(n^2)}}$
2. *Then the number of its minimal prime divisors is bounded by* $d^{n^{O(1)}}$.
3. *For every minimal prime divisor* P_i *exists an ideal* $Q_i \lhd K[X_1,\ldots,X_n]$ *s.t.* $\sqrt{Q_i} = P_i$ *and deg* $Q_i \leq d^{n^{O(1)}}$.
4. *If* P *is a minimal prime divisor of* A*, then deg* $P \leq d^{2^{O(n^2)}}$.

Proof cf. [Chi], [Gr], [KrLo].

□

The last two Propositions allow us to use ideal theoretic notions in the construction of formulas. We further need:

Lemma 3.4 *Let* $A \lhd K[X_1,\ldots,X_n]$ *be an ideal of* (n,m,d)*-Format,* $V = V_C(A)$*. Then there exist ideals of degree*
$\leq d^{2^{O(n^2)}}$ *which describe the following* K*-varieties:*

1. *The singular locus of* V,

2. *The K-Zariski-closure of $V \setminus W$, where W is another K-variety given by an ideal of (n, m, d)-format,*

3. *The K-Zariski-closure of the image of V under projections,*

4. *The Zariski-closure of the image of V under a K-regular map φ, where φ is described by polynomials of degree $\leq d$,*

5. *The projective closure of V.*

Proof These bounds are well known. They follow for example easily from the double exponential bounds known on the degrees of Gröbner bases (cf. [Dub] and [Gi],[MöMo]). A model theoretic proof for the existence of bounds on the degree of Gröbner bases has been given in [We4].

□

Using these bounds we get immediately:

Proposition 3.5 *The following algebraic-geometric statements are elementary and can be expressed by quantifier free formulas:*

1. *"dim $V_C(A) = r$"*

2. *" Sing $V_C(A) = V_C(B)$"*

3. *"$\overline{V_C(A) \setminus V_C(B)} = V_C(C)$"*

4. *Let π denote the projection from C^n to the first k variables. Then we can express:*

   " $\overline{\pi(V_C(A))} = V_C(B)$"

5. *If $\alpha : C^n \longrightarrow C^{n'}$ is any K-regular map given by polynomials, whose degree is bounded by l we can express quantifier free (by including in φ free variables for the coefficients of α):*

   "$\overline{\alpha(V_C(A))} = V_C(B)$"

6. *Let $n' = n+1$ and consider only ideals B with a generating system of homogeneous polynomials. Then we can express quantifier free:*
   "The projective closure of $V_C(A)$ = The projective variety of B".

We do not claim that all basic concepts of algebraic geometry over algebraically closed fields can be expressed by elementary formulas. So let us turn now to another type of definability problem: Classifying algebraic varieties up to isomorphism is one of the *"guiding problems"* (Hartshorne [Ha],p.55) of algebraic geometry. So from a model theoretic and an effective point of view one fundamental question is whether the isomorphism problem for varieties is elementary and (or) decidable. An answer to these - today open - questions seems to be fundamental to clarify the model theoretic and effective content of algebraic geometry.

Open Problem 3.6 *Let K be a field and let A (resp. B) be ideals of (n, m, d)-format (resp. (n', m', d')-format). Is there an elementary formula φ s.t*

$$\varphi(A, B) \iff V_C(A) \text{ and } V_C(B) \text{ are } K\text{-isomorphic?}$$

It is easy to see that this question is equivalent to the existence of bounds for the polynomial describing the isomorphism between $V_C(A)$ and $V_C(B)$ (if there is any) in terms of (n, m, d) and (n', m', d').

Open Problem 3.7 *Let K be a field. Is there an algorithm deciding whether two K-varieties V and W are K-isomorphic (with an oracle allowing to perform certain computations in K)?*

The analogous, important problems concerning *birationality* and *unirationality* can be posed in a similar fashion.

3.2 First Order Definability of being K-Radical

We had already seen in Section 1 that the concept of the K-radical was fundamental to solve computational tasks for the K-rational points of varieties. Analogously we will see here that the first order definability of the K-radical turns out to be the key for the first order definability (in the language of rings) of algebraic-geometric properties of K-rational points of K-varieties.
Notation If we work over a class of fields $\mathcal{M}$ the statement that a property P of the K-rational points of a variety is elementary means: for all (n, m, d) exists a formula φ, s.t. for all fields $K \in \mathcal{M}$ and for all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format holds:

$$K \models \varphi(A) \text{ iff } V_K(A) \text{ has property } P.$$

Theorem 3.8 *Let $\mathcal{M}$ be an elementary class of fields. Then the following 4 statements are equivalent:*

1. *The property*

   "A is K-radical"

   is elementary.

2. *For all nonnegative integers r the property*

   " $dim V_K(A) = r$ "

   is elementary.

3. *There are uniform bounds for the degree of the generators for the K-radical of ideals in (n, m, d)-format for all $K \in \mathcal{M}$ and all $A \lhd K[X_1, \ldots, X_n]$ in terms of n and d.*

4. *The property*

   "A is K-radical"

   can be expressed by a $\forall\exists$-formula.

Proof 2) $\Rightarrow$ 1)
We had seen in Proposition 1.3 that A is K-radical iff A is radical and all minimal prime divisors P_i of A are K-radical. The number and the degrees of the minimal prime divisors of A can be bounded by a constant M according to proposition 3.3. The property of the P_i of being K-radical can be formulated by saying "dim $V_K(P)$ = dim P". Further it follows from Lemma 2.4 that K-radical prime ideals are absolutely prime. By using Proposition 3.2, 3.5 being K-radical can thus be expressed with the help of the dimension as follows:

$$\begin{aligned} & A \text{ is } K\text{-radical } \Leftrightarrow \\ K \quad \models \quad & \exists P_1, \ldots, P_M, \ \deg P_i's \leq M : \ \text{the } P_i's \text{ are absolutely prime} \\ & \wedge\, A = \bigcap P_i \wedge \ \dim P_i = \ \dim V(P_i), \ 1 \leq i \leq M. \end{aligned}$$

1) $\Rightarrow$3)
Assume there are no bounds. Then we can find a sequence of ideals $A_i = (f_1^i, \ldots, f_m^i) \lhd K[X_1, \ldots, X_n]$ with $\deg f_j^i \leq d$ such that $\deg \sqrt[K]{A_i}$ is a strictly increasing function of i. Let D be a nonprincipal ultrafilter on $\mathbb{N}$. Let $L := \prod K/D$ and consider the ideal $A := (F_1, \ldots, F_m) \lhd L[X_1, \ldots, X_n]$ (where $F_j := (\ldots, f_j^i, \ldots)$).
Now let $\sqrt[K]{A} = (G_1, \ldots, G_r)$. Because $L \in \mathcal{M}$ we get

$$L \models \varphi((G_1, \ldots, G_r)) \wedge V_K(A) = V_K((G_1, \ldots, G_m)).$$

After the theorem of Loś we have for infinitely many i's:

$$K \models \varphi((g_1^i, \ldots, g_r^i)) \wedge V_K(f_1^i, \ldots, f_m^i) = V_K(g_1^i, \ldots, g_r^i)$$

which states that $(g_1^i, \ldots, g_r^i) = \sqrt[K]{A_i}$. Because the degrees of the g_j^i's are uniformly bounded we get a contradiction to the choice of the A_i's.
3)$\Longrightarrow$4)
Let $r_0 := B(n, m, d)$ be the bound and let A_{r_0} be the formula:

$$\forall f, \deg f \leq r_0 : f_{|V(A)} = 0 \Longrightarrow f \in A.$$

Then we have for $K \in \mathcal{M}$:

$$A = \sqrt[K]{A} \iff K \models A_{r_0}(A).$$

A_{r_0} is equivalent to the universal existential formula:

$$\forall f, \deg f \leq r_0, \ \exists x : \ f \in A \vee [x \in V(A) \wedge f(x) \neq 0].$$

4) $\Longrightarrow$ 2)
Let A be of (n, m, d)-format. We know already 4) $\Longrightarrow$ 1) $\Longrightarrow$ 3). So there exist a bound $B(n, m, d)$ for the generators of the K-radical of ideals of (n, m, d)-format. Then we can express the property "dim $V_K(A) = r$" as follows:

$$\begin{aligned} &\exists \text{ ideal } B \text{ of } (n, (B+1)^n, B)\text{-format :} \\ &V(A) = V(B) \ \wedge \ B \text{ is } K\text{-radical } \ \wedge \ \ \dim B = r. \end{aligned}$$

From this we can construct an elementary formula by the previous subsection.

□

3.3 An Elementary Class of Fields where the Dimension is not First Order Definable

Lemma 3.9 *Let K be a field. Then there is a $K(t)$-curve C that is defined over $\mathbb{Q}(t)$ s.t.:*

1. *C is smooth,*
2. *C has a $\mathbb{Q}$-rational point,*
3. *C has has only finitely many L-rational points over any finitely generated field extension L of $K(t)$.*

Proof Let C be the $\mathbb{Q}(t)$ curve given by the equation:

$$Y^2 = X(X-1)(X-2)(X-3)(X-t)$$

1) and 2) are clear. Now let's prove condition 3): Manin has proved in [Ma] an analogue of Mordell's conjecture for function fields:

" Let K be a regular extension of the field k of characteristic 0 and let C be a curve of genus ≥ 2 defined over K. If there are infinitely many points on C rational over K, then it is birationally equivalent to a curve C_0 defined over k and all except possibly finitely many of the points correspond to points of C_0 defined over k."

Let $\tilde{K}$ be the algebraic closure of K. There is a $K(t)$-embedding of every finitely generated extension L of $K(t)$ in a finitely generated extension of $\tilde{K}(t)$. Therefor it is sufficient to prove condition 3) for finitely generated field extensions of $\tilde{K}(t)$. Now let L be a finitely generated extension of $\tilde{K}(t)$. Then L is a regular extension of $\tilde{K}$ of transcendence degree at least 1. To apply Manin's result we have to show that C is not birational to a $\tilde{K}$-curve. To prove this we use the fact every curve D of genus 2 is hyperelliptic. Its birationality class can be represented by a curve of type

$$Y^2 = (X - e_1)(X - e_2)\dots(X - e_6),$$

The e_i are pairwise different elements of the algebraic closure (cf. [HeLa], p. 485). Let D' be another curve of genus 2. Assume the birationality class of D' is given by the equation

$$Y^2 = (X - e'_1)(X - e'_2)\dots(X - e'_6).$$

Two curves given in such a way are birational iff $e_1, \dots e_6$, resp. $e'_1, \dots e'_6$ can be permuted in such a way that their cross ratio $(e_1 e_2 e_3 e_h), 4 \leq h \leq 6$ and $(e'_1 e'_2 e'_3 e'_h), 4 \leq h \leq 6$ coincide. (cf. [HeLa], p. 531). (For given distinct elements a, b, c, d their cross ratio $(abcd)$ is defined to be $\frac{d-a}{d-b}\frac{c-b}{c-a}$.) Let us apply this to our situation: C has genus 2 (cf. [HeLa]). The cross ratios of C contain an element of $\tilde{K}(t) \setminus \tilde{K}$. On the other hand we know that a $\tilde{K}$-curve is birational to a curve of the form above over $\tilde{K}$ and thus its cross ratios are elements of $\tilde{K}$. This implies that C is not birational to a $\tilde{K}$-curve.

□

Proposition 3.10 *There is a field M and a sequence of irreducible curves C^i defined over M with the following properties:*

1. *The C^i's are defined by polynomials of degree bounded by 6,*
2. *$\#C^i_M \geq i$,*
3. *$\#C^i_M < \infty$.*

Proof We work with the $\mathbb{Q}(t)$-curve C used in Lemma 3.9. C is given by an equation of the form $Y^2 = f(t, X)$. Let $\mathcal{T}$ be a transcendence basis of $\mathbb{C}$ over $\mathbb{Q}$. We pick a set $\mathcal{U} := \{t_1, t_2, t_3, \dots\} \subset \mathcal{T}$. For each $i \in \mathbb{N}$ pick now a set $\mathcal{V}^i := \{x^i_1, x^i_2, \dots, x^i_i\} \subset \mathcal{T}$. We may assume that the choices were made in such a way that all the picked elements are pairwise different. Now let C^i be the curve defined by the equation $Y^2 = f(t_i, X)$. Let $\mathcal{W}^i := \{\alpha^i_1, \dots, \alpha^i_i\}$ where α^i_j is a solution of the equation $Y^2 = f(t^i, x^i_j)$ in $\mathbb{C}$. Now let $M := \mathbb{Q}(\mathcal{U} \cup \bigcup(\mathcal{V}^i \cup \mathcal{W}^i)) \subset \mathbb{C}$.
Claim: M and the C^i's fulfill the conditions of the Proposition.
Properties 1) and 2) are clear by the construction. Now let's prove that a curve C^{i_0} has only finitely many M-rational points. To see this let $M^{i_0} := \mathbb{Q}(\mathcal{U} \setminus \{t_{i_0}\} \cup \bigcup_{i \neq i_0} \mathcal{V}^i \cup \mathcal{W}^i) \subset \mathbb{C}$. Picking new indeterminates $X_1, \dots X_{i_0}$ over $\mathbb{C}$ we can extend the inclusion map $i : M^{i_0} \hookrightarrow \mathbb{C}$ to a map $\varphi : M^{i_0}(t_{i_0}, x^{i_0}_1, \dots, x^{i_0}_{i_0}) \longrightarrow \mathbb{C}(t, X_1, \dots, X_{i_0}) =: L$ by sending t^{i_0} to t and $x^{i_0}_j$ to X_j. Let $\tilde{L}$ be the algebraic closure of L. $M \mid M^{i_0}(t_{i_0}, x^{i_0}_1, \dots, x^{i_0}_{i_0})$ is a finite extension. So we can extend φ to a map $\varphi : M \longrightarrow \tilde{L}$. Via φ the M-rational points of C^{i_0} are mapped to $\varphi(M)$-rational points of C. Now $\varphi(M)$ is contained in a finitely generated extension N of $\mathbb{C}(t)$. Hence by the previous Lemma C has only finitely many $\varphi(M)$-rational points and the claim is proved.

□

Corollary 3.11 *There is a field M s.t.*

1. *There are no bounds for the generators of the M-radical depending only on the number of variables and the degree of the defining polynomials.*
2. *Let $\mathcal{M}$ be the class of fields elementarily equivalent to M. Then the following properties are not elementary for $\mathcal{M}$:*
   - *"A is M-radical"*
   - *"dim $V_M(A) = 0$"*

Proof Let M be the field constructed in Proposition 3.10. Using the equivalences of Theorem 3.8 it is enough to show that there is a sequence of ideals $A_i \lhd M[X_1, X_2]$ generated by polynomials of bounded degree such that deg $\sqrt[M]{A_i}$ tends to infinity.
The curves C^i constructed in Proposition 3.10 can be defined by polynomials $f_i \lhd M[X_1, X_2]$ with deg $f_i \leq d$. Put $A_i = (f_i)$. Then $\sqrt[M]{A_i}$ is a zero-dimensional ideal having at least i points over $\overline{M}$, the algebraic closure of M. Now the Affine Bezout Theorem (cf. [He], [Sch]) implies that a zero-dimensional ideal generated by polynomials of degree $\leq D$ in $\overline{M}[X_1, X_2]$ can have at most D^2 points over $\overline{M}$. Thus deg $\sqrt[M]{A_i}$ has to tend to infinity.

□

Remark It would be nice to know whether there are "easier" fields s.t. there is family of curves defined by polynomials of bounded degree, s.t. the number rational points - although finite - tends to infinity. For example, is $\mathbb{Q}$ such a field? This question is open. The known bounds for the number of rational points on a curve given by Bombieri (cf. [Bo]) are not uniform in the degree but depend also on the heights of the coefficients appearing in the defining polynomials of the curve. It is not known whether this dependence is necessary. Currently it has been shown by Caporosa, Harris and Mazur (cf. [CaHaMa]) that the conjecture of Lang stating that a $\mathbb{Q}$-variety V of general type does not contain a Zariski dense subset of rational points implies the existence of uniform bounds for the number of rational points on a smooth curve.

3.4 First Order Definability of being K-Radical in $\mathcal{K}$

We had seen in Theorem 3.8 that - given a field K - if there are elementary formulas expressing the property of ideals of (n, m, d)-format of being K-radical there is already a $\forall\exists$- formula doing this. In $\mathcal{K}$ we can do even better and find an *existential formula* expressing this property. Furthermore we will see that there is an existential formula expressing this simultaneously for all $K \in \mathcal{K}$ and all ideals of (n, m, d)-format in $K[X_1, \ldots, X_n]$.

Theorem 3.12 *1. There is a bound $B(n, m, d)$ such that for all fields $K \in \mathcal{K}$ and all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format deg $\sqrt[K]{A} \leq B(n, m, d)$.*

2. *There is an existential formula φ such that for all fields $K \in \mathcal{K}$ and all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format holds:*

$$A = \sqrt[K]{A} \iff K \models \varphi(A)$$

.

Proof Ad 2 With the same arguments used in Theorem 3.8 2) $\Rightarrow$ 1) follows

$$\begin{aligned} A = \sqrt[K]{A} \iff & \\ K \models\ & \exists P_1, \ldots, P_M, \text{ deg } P_i's \leq M : A = \bigcap P_i \\ & \wedge P_1 \text{ is absolutely prime} \wedge \ldots \wedge P_M \text{ is absolutely prime} \\ & \wedge \text{ Reg}V(P_1) \neq \emptyset \wedge \ldots \wedge \text{ Reg}V(P_M) \neq \emptyset \end{aligned}$$

"Reg $V_K(P_i) \neq \emptyset$" can be expressed by an existential formula using the Jacobian criterion.

Ad 1 1) follows from 2) with Theorem 3.8.

□

Remark The Theorem above (more precisely: its proof) yields a model theoretic proof for the existence of degree bounds for the K-radical in $\mathcal{K}$ that depend only on the format of the ideals. We will see in the next subsection that the existence of bounds for the K-radical is the central key to prove the first order definability of algebraic-geometric properties. So far the only fields we know of having this good definability properties are fields in $\mathcal{K}$. So from the point of view of model theory it would be very interesting to have an answer to the following

Open Problem 3.13 *Are there fields K not in $\mathcal{K}$ s.t. the degrees of the generators of the K-radical can be bounded by a function depending only on (n, m, d)?. Do there exist fields K not in $\mathcal{K}$ s.t. the statement "$dim V_K(A) = r$", $r \in \mathbb{N}_0$ is elementary?*

3.5 First Order Definability of Algebraic-Geometric Properties of V_K

We will see in this subsection that for the elementary definability of basic algebraic-geometric properties of the K-rational points of K-varieties (which include dimension) it is sufficient that the notion of dimension (or equivalently the notion of being K-radical, as we already know) is elementarily definable. So we see that the first order definability of the dimension is of outstanding importance. Furthermore we get that if these basic properties (including dimension) are first order definable, then these properties can be expressed by formulas not too complicated. We will see that formulas which are low in the hierarchy of formulas, i.e. which have only a small number of alternations of quantifier blocks, will do the job.

Theorem 3.14 *Let $\mathcal{M}$ be an elementary class of fields s.t. the statement*

$$"A = \sqrt[K]{A}\ "$$

is elementary. Then the following properties are elementary and can be expressed by Π_3^0 and also by Σ_3^0-formulas.

1. *"dim $V_K(A) = r$"*
2. *" Sing $V_K(A) = V_K(B)$"*
3. *"$\overline{V_K(A) \setminus V_K(B)} = V_C(C)$"*
4. *Let π denote the projection from C^n onto the first $n-1$ variables and let $n' = n-1$:*

   " $\overline{\pi V_K(A)} = V_C(B)$"
5. *If $\alpha : C^n \longrightarrow C^{n'}$ is any K-rational map given by rational functions where the degree of the polynomials appearing in the enumerator and denominator are bounded by l we have (by including in φ free variables for the coefficients of α):*

   "$\overline{\alpha(V_K(A))} = V_C(B)$"
6. *Let $n' = n+1$ and consider only ideals B with a generating system of homogeneous polynomials:*

   " the projective closure of $V_K(A) =$ the projective variety of B"

Proof of Theorem 3.14 We choose 4) to give a detailed proof.
Let (n, m, d) be given. We had seen that the first order definability of being K-radical implies two facts (cf. Theorem 3.8):

1. There exists a bound $B := B(n, m, d)$ s. t. for an ideal A of (n, m, d)-format holds: deg $\sqrt[K]{A} \leq B(n, m, d)$.

2. The property of an ideal of being K-radical can be expressed by the $\forall\exists$-formula stating that all polynomials of degree $\leq B$ that vanish on $V_K(A)$ belong to A.

Let (n', m', d') be given and let ψ be a quantifier free formula expressing for K-varieties given by ideals C (resp. B) of $(n, (B+1)^n, B)$-format (resp. (n', m', d')-format) that "$\overline{\pi(V_C(C))} = V_C(B)$". Such a ψ exists using Proposition 3.5.

We had seen in Chapter 1 that we obtain $\overline{\pi(V_K(A))}$ as $\overline{\pi(V_C(\sqrt[K]{A})}$. So we can express for ideals A of (n, m, d)-format and ideals B of (n', m', d')-format the property:

$$\text{"}\overline{\pi(V_K(A))} = V_C(B)''$$

as follows:

$$\begin{aligned} &\exists \text{ an ideal } C \text{ of } (n, (B+1)^n, B)\text{-format s.t:} \\ &\big[\forall x\ x \in V_K(A) \iff x \in V_K(C)\big] \wedge C \text{ is } K\text{-radical} \\ &\wedge\ \psi(C, B) \end{aligned}$$

We sort the quantifiers:

$$\begin{aligned} &\exists C \text{ of } (n, (B+1)^n, B)\text{-format } \forall x\ \forall f \text{ of deg} \leq B\ \exists y : \\ &\big[x \in V_K(A) \iff x \in V_K(C)\big] \wedge \\ &\big[f \in C \vee [y \in V_K(C) \wedge f(y) \neq 0]\big] \wedge \psi(C, B) \end{aligned}$$

The latter formula is in fact a $\exists\forall\exists$-formula.

Now we construct a $\forall\exists\forall$-formula:

$$\begin{aligned} &\forall \text{ ideals } C \text{ of } (n, (B+1)^n, B)\text{-format holds:} \\ &\Big(\big[\forall x\ x \in V_K(A) \iff x \in V_K(C)\big] \wedge C \text{ is } K\text{-radical}\Big) \\ &\Longrightarrow \psi(C, B) \end{aligned}$$

Now choose Σ to be the Theory of K and apply Proposition 3.16. The others statements can be proved analogously by substituting the formula ψ above by the formula expressing the corresponding property for algebraically closed fields using Theorem 3.5.

□

Corollary 3.15 *Let $\mathcal{M}$ be an inductive, elementary class of fields. Assume furthermore that the property of being K-radical is elementary. Then the properties from Theorem 3.14 can be expressed by Boolean combinations of Σ_2^0-formulas.*

For the proof we need the following

Proposition 3.16 *Let $\mathcal{L}$ be a language, T a $\mathcal{L}$-theory, which is inductive or a Σ_n^0-theory. Let φ be a formula, s.t. φ is equivalent to a Π_{n+1}^0 and a Σ_{n+1}^0-Formel relative to T. If $n \geq 1$ then φ is equivalent to a Boolean combination of Σ_n^0- formulas relative to T.*

Proof Using the routine argument of introducing constants it is sufficient to prove the Theorem for sentences. The following Theorem is known (cf. [ChKe], Theorem 3.1.16):

> Let $\mathcal{L}$ be a language. Let φ be a sentence, such that φ is equivalent to a Π^0_{n+1} and to a Σ^0_{n+1}-sentence. If $n \geq 1$, φ is equivalent to a boolean combination of Σ^0_n-sentences.

The proof of this Theorem of Shoenfield in [ChKe] can be applied word by word to our situation if one studies only models of T instead of arbitrary $\mathcal{L}$-structures.

□

Proof of Corollary 3.15
Combine Theorem 3.14 with Proposition 3.16.

□

3.6 First Order Definability of Algebraic-Geometric Properties of V_K in $\mathcal{K}$

For $K \in \mathcal{K}$ these formulas can still be simplified:

Theorem 3.17 *Let $K \in \mathcal{K}$. Then the properties 1)-6) from Theorem 3.14 can be expressed by boolean combinations of $\exists$-formulas.*

Proof Again we study property 4).
By Proposition 3.16 it is sufficient to show that there is an $\exists\forall$- formula and a $\forall\exists$-formula expressing 4).
The reason for the simplification of the formulas is that in $\mathcal{K}$ the property of being K-radical can be already expressed by an existential formula. So as in the proof of Theorem 3.5 we can express the property

$$\overline{\pi(V_K(A))} = V_C(B)$$

as follows:

$$\begin{aligned} K \quad \models \quad & \exists \text{ an ideal } C \text{ of } (n, (B+1)^n, B)\text{-format, s. t.:} \\ & C \text{ is } K\text{-radical} \wedge \left[\forall x \ (x \in V(A) \iff x \in V(C))\right] \wedge \ \psi(C, B) \end{aligned}$$

This is obviously an $\exists\forall$-formula.
Now we construct an $\forall\exists$-formula expressing 4):

$$\begin{aligned} & \forall \text{ ideals } C \text{ of } (n, (B+1)^n, B)\text{-format:} \\ & \Big(\left[\forall x \ (x \in V(A) \iff x \in V(C))\right] \wedge C \text{ is } K\text{-radical}\Big) \Longrightarrow \psi(C, B). \end{aligned}$$

Because being K-radical can be expressed in $\mathcal{K}$ by an existential formula we see by sorting the quantifiers that this is in fact a $\forall\exists$-formula.
The other statements are again proved analogously by varying ψ.

□

3.7 $\mathcal{K}$-Nullstellensätze

McKenna introduced in his article *"Some diophantine Nullstellensätze"* [McK] a method to derive Nullstellensätze for *some* complete and model complete theories of fields. We show that such a Nullstellensatz can *always* be derived for *any* complete and model complete theory (in the language of rings $\mathcal{L}(+,\cdot,0,1)$ that contains Th($\mathcal{K}$). The proof follows closely the exposition in [McK] where he derives a Nullstellensatz for p-adically closed fields. The crucial point there, the topological completeness of $\mathbb{Q}_p$, can be substituted by the $\mathcal{K}$-property.

For this let T be a complete and model complete theory in the language of rings containing Th($\mathcal{K}$) different from ACF. We define the set Q^h to consist of all homogeneous forms in $\mathbb{Q}[Y_1, Y_2, Y_3, \ldots]$ having only the trivial zero in one model (and thus by completeness of T in all models) of T. By Q we denote the set of all dehomogenisations of elements of Q^h.

Theorem 3.18 *Let T be a complete, model complete theory, containing Th($\mathcal{K}$). Let Q be defined as above. Let K be a model of T, $A \lhd K[X_1, \ldots, X_n]$ Then*

$$\sqrt[K]{A} = \{f \in K[X_1, \ldots, X_n] \mid \exists m \in \mathbb{N}$$
$$\exists D(Y_1, \ldots, Y_s) \in Q\ \exists u_1, \ldots, u_s \in K(X_1, \ldots, X_n) \text{ with } f^m \cdot D(u_1, \ldots, u_s) \in A\}$$

Proof It is shown by McKenna in [McK], Theorem 2 that to get this Nullstellensatz we have to verify the following properties of the set Q:

1. Let $p \in Q$. Then neither p nor its homogenisation p^h have a zero in any model of T.
2. Q is closed under exchange of variables.
3. Q is multiplicatively closed.
4. Let K be a model of T, L a field extension of K. Then L can be embedded in a model of T iff no element of Q has a zero over L.

That the properties 1) to 3) are fulfilled is obvious by the construction of Q. Let's prove property 4):
The non-trivial direction is from right to left. So let L be an extension of K that cannot be embedded in a model of T. We have to construct a $p \in Q$ that has a zero over L but none over K. First Theorem 1 of [McK] yields that in this situation there is a polynomial q with coefficients in $\mathbb{Q}$ having no zero over K, but having a zero x over L. We study now the $\mathbb{Q}$-variety $V = V(q)$ with points in $\overline{L}$, the algebraic closure of L. We had already seen that the singular locus of a $\mathbb{Q}$-variety is again a $\mathbb{Q}$-variety. So by computing iterated singular loci of V: V, Sing(V), Sing(Sing(V)), ..., we can find a $\mathbb{Q}$-variety W_1 containing x as a *regular point*. Let W_2 be the $\mathbb{Q}$-irreducible component of W_1 containing x. Let W be the projective closure of W_2. By Hironakas Theorem on the resolution of singularities, we can find a $\mathbb{Q}$-regular map $\varphi : X \longrightarrow W$, where X is a smooth $\mathbb{Q}$-variety. Furthermore φ has a $\mathbb{Q}$-rational inverse ψ which is defined at the regular points of W. Because x is a regular point of W, X has the L-rational point $y := \psi(x)$.
Claim: X has no K-rational point .
Assume there were a K-rational point lying on X. This K-rational point had to be smooth. Because $K \in \mathcal{K}$, X contains a K-Zariski dense subset of K-rational point s and so does W as a K-birational image. So also the open subset W_2 (in the projective Zariski topology) of W contains a K-rational point . This is a contradiction and the claim is proved. Now let $X = V(f_1, \ldots, f_m)$ with homogeneous polynomials. By substituting the f_i by certain powers we might assume that they are all homogeneous of the same degree. By [McK], Lemma 4 there is a homogeneous polynomial N in $m' \geq m$ variables with coefficients in $\mathbb{Q}$ having only the trivial zero over K. Thus we put $q^h = N(f_1, \ldots, f_m, 0 \ldots, 0)$. If $y = (y_1, \ldots, y_k)$, let w.l.o.g. $y_1 \neq 0$. Thus by specializing the first variable of q^h to 1 we get a polynomial q in Q having a zero over L but none over K.

□

4 Complexity in $\mathcal{K}$

In this section we are going to derive degree complexity bounds for the K-radical for fields in $\mathcal{K}$. Our main interest is to bound the degrees of the K-radical $\sqrt[K]{A}$ for an ideal $A \lhd K[X_1, \ldots, X_n]$ in terms of n and deg A. This bound will allow us to derive complexity bounds for algebraic-geometric problems in $\mathcal{K}$. We will derive e.g. an upper bound for the number of K-rational points of a K-variety V_K (if $\#V_K < \infty$).

4.1 Complexity of the K-Radical in $\mathcal{K}$

To avoid case distinctions we assume throughout the whole chapter w.l.o.g. that $2 \leq d$ (every ideal of $(n, m, 1)$-format can also be regarded as an ideal of $(n, m, 2)$-format).

Theorem 4.1 *For all fields $K \in \mathcal{K}$ and all ideals $A \lhd K[X_1, \ldots, X_n]$ with deg $A \leq d$ holds:*

$$deg\ \sqrt[K]{A} \leq d^{2^{O(n^3)}}$$

We first describe an algorithm to compute the K-radical which is different from the one described in Theorem 2.3 but which is more convenient for complexity theoretic considerations.

We start with an ideal $A \lhd K[X_1, \ldots, X_n]$ with deg $A \leq d$.

The Algorithm

Input: $A \lhd K[X_1, \ldots, X_n]$
Output: $\sqrt[K]{A}$

Step 1 First compute a sequence of ideals describing the iterated singular loci of $V_C(A)$:

Put $A_0 := A$.

Compute A_1, a describing ideal of Sing $V_C(A_0)$.

Compute A_2, a describing ideal of Sing $V_C(A_1)$.

We continue our computation of iterated singular loci until we end up with an ideal A_k, s.t. Sing $V_C(A_k) = \emptyset$.

Step 2 Compute a list $\mathcal{M}$ of ideals describing all the K-irreducible components of all the $V_C(A_i), 0 \leq i \leq k$.

Step 3 Build up the list $\mathcal{L}$ that consists of all those ideals $Q \in \mathcal{M}$ s.t. $\overline{V_K(Q)} = V_C(Q)$.

Step 4 Compute B, the product ideal of all the ideals in $\mathcal{L}$.

Step 5 Compute $\sqrt{B}$. Then we have $\sqrt{B} = \sqrt[K]{A}$.

We first prove the correctness of this method:
Claim: $\sqrt{B} = \sqrt[K]{A}$
Let's first show that $V_K(B) = V_K(A)$:
Because for all the $Q \in \mathcal{L}$ holds that $V_K(Q) \subset V_K(A)$ we get: $V_K(B) \subset V_K(A)$. Let's prove the converse. Let $x \in V_K(A)$. Then there is an i_0, s.t. $x \in$ Reg $V_C(A_{i_0})$. So x is a regular point of one of the K-irreducible components, let's say $V_C(Q)$ of $V_C(A_{i_0})$. Because $K \in \mathcal{K}$, we get that $\overline{V_K(Q)} = V_C(Q)$ and thus Q occurs in the list $\mathcal{L}$. So $x \in V_K(B)$.

B describes the union of K-varieties containing K-Zariski dense subsets of K-rational points. So B itself has this property. Now $\sqrt{B}$ is a radical ideal containing $V_K(A)$ as a K-Zariski dense

subset and thus the K-radical of A. So the claim is proved.

Now we do the straightforward degree complexity analysis of our algorithm:
Applying iteratively Lemma 3.4 we get that deg $A_i \leq d^{2^{n^{3c}}}$ for a constant c. Using the single exponential bounds e.g. Giusti and Heintz give in [GiHe] for the number and degrees of describing ideals for the K-irreducible components of $V_C(A_i), 0 \leq i \leq k$ we get that both of these numbers are bounded by the function $d^{2^{en^3}}$ for a constant e. The degree of the product ideal of the ideals in $\mathcal{L}$ is now obviously bounded by $d^{2^{fn^3}}$ with a constant f. Applying now the degree bounds for the usual radical computation we see that the degree of $\sqrt[K]{A} = \sqrt{B}$ is bounded by $(d^{2^{en^3}})^{2^{cn^2}}$. This function is majorized by $d^{2^{gn^3}}$ for a constant g.

□

It is folklore - although we did not find an explicit reference for this in the literature - that the singular locus of a K-variety can be described single exponentially, i.e. if A is of (n, m, d)-format there is an ideal B of deg $\leq d^{n^{O(1)}}$ with $\mathrm{Sing}V_C(A) = V_C(B)$. Iterating this result we see that the iterated singular loci of $V_C(A)$ can be described by ideals, whose degree is bounded by $d^{2^{O(n^2)}}$. By inspection of the above algorithm one sees that the bounds for the K-radical can thereby be improved a little bit to be $d^{2^{O(n^2)}}$.

But it would be much more interesting to achieve a qualitative breakthrough in the nature of the complexity bounds for $\mathcal{K}$. As already the best known degree bounds for the usual radical, i.e. the C-radical for algebraically closed fields C, are of double exponential nature one can not expect that the degree bounds for the K-radical (for all $K \in \mathcal{K}$) get better than this. If there are single exponential degree bounds for the usual radical is an open difficult problem.

Another procedure seems to be more useful: instead of computing the K-Zariski closure of $\overline{V_K(A)}$ ideal theoretically, i.e. by computing a set of generators for $\sqrt[K]{A}$, one should try to compute $\overline{V_K(A)}$ set theoretically, i.e. compute an ideal B s.t. $\overline{V_K(A)} = V_C(B)$. It was mainly this set theoretical approach that made the single exponential bounds possible which were obtained in the last years in complex and real algebraic geometry. Let us first pose the problem properly:

Open Problem 4.2 *Is the following true? For all fields $K \in \mathcal{K}$ and all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format there is an ideal $B \lhd K[X_1, \ldots, X_n]$ with deg $B \leq (dm)^{n^{O(1)}}$ s.t. $\overline{V_K(A)} = V_C(B)$?*

Suppose the answer to this problem were Yes. Then one could conclude (using the Affine Bezout Theorem) that there is a single exponential Bezout type Bound for the number of K-rational points on a K-variety (cf. [He], [Sch], Corollary 4.5). And this is the typical situation. Recall that we noticed in Chapter 1 that algorithms solving algebraic geometric questions for the K-rational points of K-varieties can be constructed as follows: first one computes the K-Zariski closure of $V_K(A)$ and then one applies the algorithm solving this task for algebraically closed fields. As already mentioned the modern fast algorithms solve many tasks in the algebraically closed case with single exponential complexity bounds (like the computation of the projective closure (cf. e.g. [CaGaHe], [GiHe]) or the Zariski-closure of projections $\pi(V_K(A))$. So a lot of problems of effective algebraic geometry in $\mathcal{K}$ would drop into a single exponential complexity class, if the answer to the above problem were Yes. (Based on our double exponential degree bound on the K-radical we are going to derive in a subsequent section double exponential bounds on some algebraic-geometric problems in $\mathcal{K}$.)
Because the K-radical of A is the usual radical of an ideal describing $\overline{V_K(A)}$ we get the following relation between the problem sketched above and the complexity of the K-radical:

There is a single exponential degree bound for the K-radical in $\mathcal{K}$ if and only is the answer to the problem above is Yes and if there is a single exponential degree bound for the usual radical.

With regard to all these consequences the problem above turns out to be the central problem for complexity theory in $\mathcal{K}$. At least in the special case that K is a real closed field the answer to this problem is indeed Yes. This was shown 1995 in an interesting paper by Galligo and Vorobjov (cf. [GaVo]). Unluckily their proof makes heavy use of definability properties over real closed fields and of fast real quantifier elimination. So it can not be generalized to the general situation of $\mathcal{K}$.

The algorithm above clarifies what the current obstacle is for obtaining single-exponential descriptions of $\overline{V_K(A)}$: The double exponential bounds are caused by the currently double exponential bounds to compute iterated singular loci of K-varieties. All the other steps in the proved can be solved with single exponential degree bounds. This yields

Open Problem 4.3 *Is the following true? For all fields K and all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format there are ideals of deg $\leq (dm)^{n^{O(1)}}$ describing the iterated singular loci of $V_C(A)$.*

A positive answer to this problem yields a positive answer to the main problem of complexity theory in $\mathcal{K}$. It is interesting to note that this problem is a problem of classical effective algebraic geometry over algebraically closed fields. If one poses this problem in the context of real algebraic varieties it is intimately connected to finding a fast stratification of real varieties. Work in this direction is recently done e.g. by Gabrielov, Vorobjov and Rannou (cf. [GabVo], [Ra]).

4.2 Bounds for Algebraic Geometry in $\mathcal{K}$

Theorem 4.4 *Let $K \in \mathcal{K}$ and $A \lhd K[X_1, \ldots, X_n]$ be an ideal with deg $A \leq d$, $V = V_C(A)$. Then we have:*

The number and the degrees of the irreducible components of V_K is 1 bounded by $d^{2^{O(n^3)}}$.

Furthermore there exist ideals of degree $\leq d^{2^{O(n^3)}}$ describing the following K-varieties:

1. *The K-Zariski closure of the singular locus of V_K*
2. *The K-Zariski-closure of $V_K \setminus W_K$, where W is another K-variety given by an ideal of (n, m, d)-format*
3. *The K-Zariski-closure of the image of V_K under projections*
4. *The K-Zariski-closure of the image of V_K under a K-regular map φ, where φ is given by polynomials of degree $\leq d$*
5. *The projective closure of V_K.*

Proof Recall that we noticed in Chapter 1 how this objects can be computed: First compute the K-Zariski closure of V_K. Then apply the well known algorithms solving this tasks for K-varieties (with points in the algebraic closure of K).

The first step is realised by the K-radical computation which has a double exponential degree bound (cf. 4.1).

The algorithms working for K-varieties also have a double exponential complexity bound (cf Lemma 3.4). For the number and the degree of the minimal prime divisors this was stated in Proposition 3.3. For the singular locus and the other constructions this was proved in Lemma 3.4.

A combination of these two sources of complexity growth yields the result.

□

Corollary 4.5 (Uniform Finiteness-Theorem for $\mathcal{K}$) *Let* $K \in \mathcal{K}$, $A \lhd K[X_1, \ldots, X_n]$ *with* $\deg A \leq d$ *and* $\#V_K(A) < \infty$. *Then* $\#V_K(A) \leq d^{2^{O(n^3)}}$.

Proof Under the assumption of finiteness of $V_K(A)$ the points of $V_K(A)$ are exactly the irreducible components of $V_K(A)$. Now apply the first statement of Theorem 4.4. Another proof follows from an application of the Affine Bezout Theorem (cf. [He], [Sch]) to the 0-dimensional variety $V_C(\sqrt[K]{A})$ for which the K-points and the C-points coincide.

□

5 A Step Towards Practical Computations in $\mathcal{K}$

Fields $K \in \mathcal{K}$ often arise as closures of a given field k under a certain "hull-operation", like the real closure of an ordered field or the Henselian closure of a valued field. A frequently met situation is that the field k is effectively given and that there is a method to decide the existential theory of K with parameters in k. But unlike in the case where $K \in \mathcal{K}$ is an algebraically closed field the K-radical of an ideal $A \lhd K[X_1, \ldots, X_n]$ generated by polynomials from $k[X_1, \ldots, X_n]$ is not generated in general by polynomials in $k[X_1, \ldots, X_n]$. We give an example for this phenomenon:
Let $k = \mathbb{Q}$, let K be the real algebraic numbers and $A=(X^4 - 2)$. Now $\sqrt[K]{A} = (X^2 - 2\sqrt[4]{2} + \sqrt{2})$ can not be generated over $\mathbb{Q}[X_1, \ldots, X_n]$ because $X^4 - 2$ is irreducible over $\mathbb{Q}$.

Two possible ways out of this are:

1. Describe a coding of K over k.
2. Instead of computing $\sqrt[K]{A}$ compute $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$.

The (efficient) coding of the real closure of an ordered field (cf. e.g. [CoRo]) was an important step for the development of basic algorithms for real algebraic geometry like the production of a cylindric algebraic decomposition of a semialgebraic set (cf. [Co]) or fast real quantifier elimination (cf. [HeRoSo]). (For the coding of the real of an ordered field cf e.g. [CoRo].) Another major source for fields in $\mathcal{K}$ are Henselian fields. R. Smith has shown (cf. [Sm]) that every recursively presented valued field has a recursively presented Henselian closure. It will be an interesting future project to develop (efficient) codings of Henselian closures and to analyze decidability and solvability of systems of algebraic equations over Henselian fields from an algorithmic point of view. This analysis could be based on theoretical work in this direction by Weispfenning and Ziegler (cf. [We1], [Zi]). For $\mathbb{Q}_p$ first attempts have been made: It was shown by Dubhashi that the theory and so especially the for us important existential theory of $\mathbb{Q}_p$ can be decided in double exponential time (cf. [Du] for details). A coding for the algebraic part part of $\mathbb{Q}_p$ is given by Nerode (cf. [Ne]).

A principle drawback of the approach using codings is that such a coding might not always exist or that the arithmetic with the coding is very time consuming. That there is in general no primitive recursive coding even for the algebraic closure of a field was shown in [Ho], [Sa1]. So there is also a need for the second approach where we want to perform all computations inside $k[X_1, \ldots, X_n]$. To make the second approach work for $\mathcal{K}$ we have to formulate an additional computational assumption on k: $k[X]$ has to allow effective factorization. Let us first illustrate the usefulness of the second concept by the following

Proposition 5.1 *Let $K \mid k$ be an algebraic extension of fields. Let $A \lhd K[X_1, \ldots, X_n]$, $A = (f_1, \ldots, f_m)$, where $f_i \in k[X_1, \ldots, X_n], i = 1, \ldots, m$ and $V_K = V_K(A)$. Assume that we are able to compute $B := \sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ for ideals of this type. Then we are able to compute the following data:*

1. *dim V_K*
2. *The k-Zariski closure of V_K under projections*
3. *The k-Zariski closure of V_K under k-regular maps*
4. *The projective closure of V_K in the projective k-Zariski topology.*

For the proof of the Proposition we need the following immediate

Lemma 5.2 *Let $K \mid k$ be algebraic and $A \lhd K[X_1, \ldots, X_n]$. Then $V_C(\sqrt[K]{A} \cap k[X_1, \ldots, X_n])$ equals the k-Zariski closure of $V_K(A)$.*
Furthermore $\sqrt[K]{A} \cap k[X_1, \ldots, X_n] = \{f \in k[X_1, \ldots, X_n] \mid f_{|V_K(A)} = 0\}$, i.e. $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ is the vanishing ideal of $V_K(A)$ in $k[X_1, \ldots, X_n]$.

Proof The k-Zariski closure of $V_K(A)$ is described by the ideal $B \lhd k[X_1, \ldots, X_n]$ consisting of all polynomials vanishing on $V_K(A)$. $\sqrt[K]{A}$ consists of all polynomials in $K[X_1, \ldots, X_n]$ vanishing on $V_K(A)$. So $B = \sqrt[K]{A} \cap k[X_1, \ldots, X_n]$. The last assertion is clear because all polynomials in $k[X_1, \ldots, X_n]$ vanishing on $V_K(A)$ belong to $\sqrt[K]{A}$.

□

We will use the Lemma in the following way: $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ can be characterized as the ideal in $k[X_1, \ldots, X_n]$ which is radical and contains $V_K(A)$ as a k-dense subset.

Proof of Proposition 5.1

Ad 1 Let $R = k[X_1, \ldots, X_n]/B$ and $S = K[X_1, \ldots, X_n]/\sqrt[K]{A}$. Then R embeds naturally into S over k. Because $K \mid k$ is algebraic the extension $S \mid R$ is integral. So dim$R$ =dim$S$. Because dim V_K = dim S = dim B we can compute dim V_K by computing dim B.

Ad 2...4 $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ describes the k-Zariski closure of V_K. Applying Lemma 1.4 w.r.t. the k-Zariski topology in the same way we used it in Section 1, where we solved the computational problems for V_K, yields 2...4.

□

We show now - under a certain additional condition on k - how $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ can be computed under avoiding computations in $K[X_1, \ldots, X_n]$.

Theorem 5.3 *Let $K \mid k$ be algebraic, $K \in \mathcal{K}$. Let $A = (f_1, \ldots, f_m) \lhd K[X_1, \ldots, X_n]$, where $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. Then we are able to compute $\sqrt[K]{A} \cap k[X_1, \ldots, X_n]$ if the following conditions are fulfilled:*

1. *The existential theory of K with parameters in k is decidable.*
2. *The univariate polynomial ring $k[X]$ allows effective factorization.*

Remark The assumptions of the Theorem are met for example in the following relative situations:

1. $K = \mathbb{Q}_p^{alg}$, the algebraic part of $\mathbb{Q}_p$ and $k = \mathbb{Q}$.
   $\mathbb{Q}_p^{alg}$ belongs to $\mathcal{K}$ as a p-adically closed field. $\mathbb{Q}$ allows effective factorization. The existential theory of $\mathbb{Q}_p^{alg}$ with parameters in $\mathbb{Q}$ is decidable (cf. e.g. [PrRo]).
2. $K = \mathbb{R}^{alg}$, the real algebraic numbers and $k = \mathbb{Q}$. $\mathbb{Q}$ allows effective factorization. The existential theory of $\mathbb{R}^{alg}$ with parameters in $\mathbb{Q}$ is decidable (cf. e.g. [HeRoSo]).

Proof We first study the case of prime ideals $Q \lhd k[X_1, \ldots, X_n]$:

Claim 1: Let $Q \lhd k[X_1, \ldots, X_n]$ be a prime ideal. Then $V_K(Q)$ is k-Zariski dense in $V_C(Q)$ iff Reg$V_K(Q) \neq \emptyset$.
Let us first prove the direction "$\Longrightarrow$" by contraposition: If Reg $V_K(Q)$ is empty then $V_K(Q)$ is contained in the proper k-subvariety Sing $V_C(Q)$ and thus not k-Zariski dense in $V_C(Q)$, a contradiction.

Let us now prove the other direction where we assume that $V_K(Q)$ contains a regular point. Let $\bigcap P_i$ be the K-irreducible decomposition of the ideal generated by Q in $K[X_1,\ldots,X_n]$. It is well known that $V_C(P_i)$ is k-Zariski dense in $V_C(Q)$ for all i. By assumption there is at least one i s.t. $\mathrm{Reg}V_K(P_i) \neq \emptyset$. Because $K \in \mathcal{K}$, $V_K(P_i)$ is K-Zariski dense in $V_C(P_i)$ and so a forteriori k-Zariski dense in $V_C(P_i)$. By the transitivity of denseness we get that $V_K(P_i)$ is k-Zariski dense in $V_K(Q)$. This yields that the (possibly bigger) set $V_K(Q)$ is k-Zariski dense in $V_C(Q)$ and the claim is proved.
Claim 2: $A = B \cap C \Longrightarrow \sqrt[K]{A} \cap k[X_1,\ldots,X_n] = (\sqrt[K]{B} \cap k[X_1,\ldots,X_n]) \cap (\sqrt[K]{C} \cap k[X_1,\ldots,X_n])$
The proof is trivial using Lemma 1.2.

Now we are able to use mutatis mutandis the algorithm for the computation of the K-radical described in the section *Steps needed to compute the K-radical* and Theorem 2.3. (To simplify notation we write for an ideal $A \lhd k[X_1,\ldots,X_n]$ $\sqrt[K]{A}$ instead of $\sqrt[K]{K[X_1,\ldots,X_n]\cdot A}$.)

The Algorithm

Input: $A \lhd k[X_1,\ldots,X_n]$
Output: $\sqrt[K]{A} \cap k[X_1,\ldots,X_n]$

Step 1 Compute $\sqrt{A}$.

Step 2 Compute the primary decomposition of $\sqrt{A} = \bigcap P_i$ in $k[X_1,\ldots,X_n]$.

Step 3 By Claim 2 we know that

$$\sqrt[K]{A} \cap k[X_1,\ldots,X_n] = \bigcap (\sqrt[K]{P_i} \cap k[X_1,\ldots,X_n])$$

So it suffices to compute the $\sqrt[K]{P_i} \cap k[X_1,\ldots,X_n]$ for all i:
Decide now whether $V_K(P_i)$ is k-Zariski dense in $V_C(P_i)$ By Claim 1 this can be done by applying the Jacobian criterion to P_i. (Here we have check whether systems of equations where the equations are given by polynomials in $k[X_1,\ldots,X_n]$ possess a K-rational solution.)

If the answer is Yes, we have $\sqrt[K]{P_i} \cap k[X_1,\ldots,X_n] = P_i$.

If the answer is No, we know that $V_K(P_i) \subset \mathrm{Sing}\, V_C(P_i)$. So $\sqrt[K]{P_i} \cap k[X_1,\ldots,X_n] = \sqrt[K]{B} \cap k[X_1,\ldots,X_n]$, where B is an ideal generated by polynomials in $k[X_1,\ldots,X_n]$ which describes $\mathrm{Sing}V_C(P_i)$. In order to compute $\sqrt[K]{P_i} \cap k[X_1,\ldots,X_n]$ we now go back to Step 1 where A is substituted by the ideal B.

This algorithm terminates because in the No-case the dimension of the ideals considered decreases. More formally: the recursion depth of the algorithm is bounded by $\dim A$. Note that factorization of univariate polynomials in $k[X]$ enables us to produce the primary decomposition of $\sqrt{A} \lhd k[X_1,\ldots,X_n]$ needed in Step 2 (cf. [BeWe], p 395).

□

The assumption on effective factorization in $k[X]$ of the theorem is not always needed. As an example for this consider the following relative situation: Let k be an arbitrary field and let $K = C$ be the algebraic closure of k. Now for an ideal $A \lhd k[X_1,\ldots,X_n]$ the ideal $\sqrt[K]{A} \cap k[X_1,\ldots,X_n]$ is the usual radical of A considered as an ideal of $k[X_1,\ldots,X_n]$ which can be computed without any use of factorization in $k[X]$. On the other hand there are relative situations in which the assumption on factorization in $k[X]$ can not be removed:

Proposition 5.4 *Let k be an arbitrary ordered field which is effectively given and let $K = R$ be the real closure of k. Then the computability of $\sqrt[K]{A} \cap k[X_1,\ldots,X_n]$ for ideals $A \lhd K[X_1,\ldots,X_n], n \in \mathbb{N}$ which are generated by polynomials in $k[X_1,\ldots,X_n]$ implies the effectivity of factorization in $k[X]$.*

Proof Effective Factorization in $k[X]$ is equivalent to the decidability whether an element $f \in k[X]$ has a root in k, and if there is a root to compute one (cf. [MiRiRu], Theorem VII.1.8).

So let $f \in k[X]$ be given. Using Sturm's Algorithm we can check whether f has a root in R by calculations in $k[X]$ and sign tests of elements in k. If f does not posess a root in R, f has especially no root in k. So let us assume now that f possesses d roots in R. Using e.g. Thom's Lemma (cf. [CoRo]) we can encode effectively each of the d roots as a semialgebraic set, where the describing formulas involve only coefficients of k. For all these d roots we want to decide whether they belong to k. Let α be such a root of f defined as a semialgebraic set S. Like any given semi-algebraic set S can be effectively written as the projection of the real points of a variety V which is given by an ideal $A \lhd K[X_1, \ldots, X_n]$ generated by polynomials in $k[X_1, \ldots, X_n]$. Now assume we are able to compute $B = \sqrt[K]{A} \cap k[X_1, \ldots, X_n]$. Then we can compute the elimination ideal $B \cap k[X]$. This ideal describes the k-Zariski closure of $S = \{\alpha\}$ by Proposition 5.1. Obviously we have: $\alpha \in k$ iff B is generated by a polynomial of degree 1, i.e. iff $B = (X - a)$. If this is the case we can compute a by computing a monic generator of B and know $a = \alpha$.

□

A List of Open Problems

Open Problem 1 *(cf. 2.16) Do $\mathbb{Q}_{ab}$, $\mathbb{Q}_{nil}$ and $\mathbb{Q}_{sol}$, the maximal abelian (resp. nilpotent, solvable) extensions of $\mathbb{Q}$ belong to $\mathcal{K}$?*

Open Problem 2 *(cf. 2.17) Is $\mathcal{K}$ stable under "digging holes"? This means more precisely: Let $L \in \mathcal{K}$, $\alpha \in L \setminus \mathbb{Q}$ and let K be a maximal subfield of L not containing α. Does this imply $K \in \mathcal{K}$?*

Open Problem 3 *(cf. 2.18) Is there a "Finite Algebraic Going Down Theorem" for $\mathcal{K}$? More precisely: Let $L \in \mathcal{K}$ and $L = K(\alpha)$ be an algebraic extension. Does this imply $K \in \mathcal{K}$?*

Open Problem 4 (Bezout Problem for $\mathcal{K}$) *(cf. 2.23) Is the following true for all fields in $\mathcal{K}$? Let $A \lhd K[X_1, \ldots, X_n]$ be an ideal which can be generated by polynomials of degree $\leq d$ and let $\sharp V_K(A) < \infty$. Then $\sharp V_K(A) < d^{n^{O(1)}}$.*

Open Problem 5 *(cf. 2.26) Is the existential theory of $\mathcal{K}$ decidable?*

Open Problem 6 *(cf. 3.6) Let K be a field and let A(resp. B) be ideals of (n, m, d)-format (resp. (n', m', d')-format). Is there an elementary formula φ s.t*

$$K \models \varphi(A, B) \iff V_C(A) \text{ and } V_C(B) \text{ are } K\text{-isomorphic ?}$$

Open Problem 7 *(cf. 3.7) Let K be a field. Is there an algorithm deciding whether two K-varieties V and W are K-isomorphic (with an oracle allowing to perform certain computations in K)?*

Open Problem 8 *(cf. 3.13) Are there fields K not in $\mathcal{K}$s.t. the degrees of the generators of the K-radical can be bounded by a function depending only on (n, m, d)?. Do there exist fields K not in $\mathcal{K}$ s.t. the statement "$dim V_K(A) = r$", $r \in \mathbb{N}_0$ is elementary?*

Open Problem 9 *(cf. 4.2) Is the following true? For all fields $K \in \mathcal{K}$ and all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format there is an ideal $B \lhd K[X_1, \ldots, X_n]$ with deg $B \leq (dm)^{n^{O(1)}}$ s.t. $\overline{V_K(A)} = V_C(B)$?*

Open Problem 10 *(cf. 4.3) Is the following true? For all fields K and all ideals $A \lhd K[X_1, \ldots, X_n]$ of (n, m, d)-format there are ideals of deg $\leq (dm)^{n^{O(1)}}$ describing the iterated singular loci of $V_C(A)$.*

References

[AdGiTo] W.A. Adkins, P Gianni, A. Tognoli, *A Nullstellensatz for an algebraically non-closed field,* Bolletino U.M.I. (5) 15-B, 338-343 (1978)

[Be1] E.Becker, *Summen n-ter Potenzen in Körpern* , J. reine angew. Math. 307/308, 8-30 (1978)

[Be2] E. Becker, *Valuations and real places in the theory of formally real fields*, in Geometrie algebrique reelle et formes quadratiques, Proceedings, Lecture Notes in Mathematics, Springer-Verlag, 1982

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

[BeNe] E. Becker, R. Neuhaus, *Computation of real radicals of polynomial ideals* , in "Computational Algebraic geometry", Birkhäuser, 1993

[BeWe] Th. Becker, V. Weispfenning, *Gr "obner Bases*, Springer-Verlag, 1993

[Bo] E. Bombieri, *The Mordell conjecture revisited,* Ann. Sc. Norm. Super. Pisa, Ser. 17, No. 4, 615-640 (1990)

[BoCoRo] J. Bochnak, M. Coste, M-F. Roy, *Geometrie algebrique reelle* , Springer-Verlag, 1987

[CaHaMa] L. Caporaso, J. Harris, B. Mazur, *Uniformity of rational points,* to appear

[Ch] G. Cherlin, *Model theoretic algebra,* Lecture Notes in Mathematics, Springer Verlag, 1976

[ChDrMa] G. Cherlin, L. v.d.Dries, A. Macintyre *The elementary theory of regularly closed fields*, a manuscript

[Chi] A. L. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time,* J. Soviet Math. 34, 1838-1882

[ChKe] C.C. Chang, H.J. Keisler, *Model theory* , North Holland, 1973

[Co] G. E. Collins, *Quantifier elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition,* Lecture Notes in Computer Science 33, 134-183 (1975)

[CoLiO'S] D. Cox, J. Little, D. O'Shea *Ideals, varieties and algorithms*, Springer-Verlag, 1992

[CoRo] M. Coste, M.-F. Roy, *Thom's Lemma, the Coding of Real Algebraic Numbers and the Computation of the Topology of Semi-Algebraic Sets,* Journal of Symbolic Computation 5, 121-129 (1988)

[Dr1] L. van den Dries, *Model theory of fields,* Thesis, Utrecht, 1978

[Dr2] L. van den Dries, *Algorithms and bounds for polynomial rings,* in Logic Colloquium 78, North-Holland (1979)

[DrSch] L. van den Dries, K. Schmidt, *Bounds in the theory of polynomial rings over fields. A nonstandard approach,* Invent. math. 76, 77-91 (1984)

[DrMaMc] L. van den Dries, A. Macintyre, K. McKenna, *Elimination of quantifiers in algebraic structures,* Advances in Mathematics 47, 74-87 (1983)

[DrSm] L. v.d.Dries, R.L. Smith, *Decidable regularly closed fields of algebraic numbers,* Journal of Symbolic Logic 50, 468-475 (1985)

[Du] D.P. Dubhashi, *Quantifier elimination in p-adic fields*, The Computer Journal 36, 419-426 (1993)

[Dub] T. W. Dube, *Quantitative Analysis of Problems in Computer Algebra: Gröbner Bases and The Nullstellensatz,* New York University, Courant Institute of Mathematical Sciences (1989)

[ELTT] Ju.L. Ershov, I.A. Lavrov, A.D. Taimanov, M.A. Taitslin, *Elementary theories,* Russian Math. Surveys 20, 35-105 (1965)

[Er] Ju.L. Ershov, *Undecidability of regularly closed fields*, Algebra and Logic 20, 257-260 (1981)

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,* Invent. Math. 73, 349-366 (1983)

[Fr] G. Frey, *Pseudo algebraically closed fields with non-archimedian real valuations,* Journal of Algebra 26, 202-207 (1973)

[FrJa] M.D. Fried, M. Jarden, *Field arithmetic*, Springer-Verlag, 1986

[GaVo] A. Galligo, N. Vorobjov, *Complexity of finding irreducible components of a semialgebraic set*, Journal of Complexity 11, 174-193 (1995)

[Gi] M. Giusti, *Some effectivity problems in polynomial ideal theory* , in Proceedings Eurosam 84, Cambridge, England, July 1984, Springer Lecture Notes in Computer Science 174, 159-171

[GiHe] M. Giusti, J. Heintz, *Algorithmes - disons rapide - pour la decomposition d'une variete algebrique en composantes irreductibles et equidimensionelle,* in Effective Methods in Algebraic Geometry, MEGA 90, Birkhäuser, 1991

[Gr] D. Grigoriev, *Factorization of polynomials over finite fields and the solution of systems of algebraic equations,* J. Soviet. Math. 34, 1762-1803, (1986)

[Gro] C. Grob, *Die Entscheidbarkeit der Theorie der maximalen pseudo p-adisch abgeschlossenen Körper*, Dissertation, Konstanz, (1988)

[Ha] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977

[He] J. Heintz, *Definability and fast quantifier elimination over algebraically closed fields,* Theoret. Comput. Sci. 24 (1983), 239-277

[HeLa] K. Hensel, G. Landsberg, *Theorie der algebraischen Funktionen einer Variablen,* Chelsea Publishing Company, 1965

[Her] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale,* Math. Ann. 95, 736-788 (1926)

[HeRoSo] J. Heintz, M.-F. Roy, P. Solerno, *Sur la complexite du principe de Tarski-Seidenberg,* Bull. Soc. Math. France 118, 101-126 (1990)

[Ho] W. Hodges, *On the effectivity of some field constructions,* Proc. London Math. Soc. (3) 32, 133-162 (1976)

[Ja] B. Jacob, *The model theory of generalized real closed fields,* J. reine angew. Math. 323, 213-220 (1981)

[JaRa] M. Jarden, A. Razon, *Rumely's local global principle for algebraic PSC fields over rings* , preprint, (1994)

[Ke] H.J. Keisler, *Fundamentals of model theory*, in *Handbook of mathematical logic*, ed. J. Barwise, North-Holland, 1977

[KrLo] T. Krick, A. Logar, *An algorithm for the computation of the radical of an ideal in the ring of polynomials* , in Proceedings AAECC-9, New Orleans, LA, USA, October 1991, Springer Lecture Notes in Computer Science 539, 195-205

[KrWe] H. Kredel, V. Weispfenning, *Computing dimension and independent sets for polynomial ideals,* in Computational Aspects of Commutative Algebra, Academic Press, 1989

[Ku] E. Kunz, *Einführung in die kommutative Algebra und algebraische Geometrie,* Vieweg-Verlag (1979)

[Kuh] F.-V. Kuhlmann, *Valuation theory of fields, abelian groups and modules*, Habilitationsschrift, Heidelberg (1995)

[La1] S. Lang, *Algebra*, Addison Wesley, Reading, 1967

[La2] S. Lang, *Hyperbolic and diophantine analysis*, Bull. Amer. Math. Soc., 14 (1986), 159-205

[La3] S. Lang, *Introduction to Algebraic geometry,* Interscience Publishers, 1964

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

[Ma] Y. Manin, *Rational points on algebraic curves over function fields*, J. Sov. Math. 4, 1505-1507 (1963)

[McK] K. McKenna, *Some diophantine Nullstellensätze*, in Model theory of algebra and arithmetic, Proceedings, Lecture Notes in Mathematics, Springer-Verlag, 1980

[MiRiRu] R. Mines, F. Richman, W. Ruitenburg, *A course in constructive algebra,* Springer Verlag, 1988

[MöMo] H.M. Möller, F. Mora, *Upper and lower bounds for the degree of Gröbner bases* , in Proceedings Eurosam 84, Cambridge, England, July 1984, Springer Lecture Notes in Computer Science 174, 172-183

[Ne1] R. Neuhaus, *Berechnung reeller Radikale in Polynomringen* , Dissertation, Dortmund, 1993

[Ne2] R. Neuhaus, *Computation of real radicals of polynomial ideals, Part 2,* J. Pure Appl. Algebra, to appear

[Ner] A. Nerode, *A decision method for p-adic integral zeros of diophantine equations,* Bull. AMS 69, 513-517 (1963)

[Ph] Th. Pheidas, *Extensions of Hilbert's tenth problem,* J. Symb. Logic 59, 372-397 (1994)

[Po] F. Pop, *Embedding problems over large fields,* to appear in Annals of Math.

[Pr] A. Prestel, *Pseudo real closed fields*, in Set theory and model theory, Proceedings, Lecture Notes in Mathematics, Springer-Verlag, 1981

[PrRo] A. Prestel, P. Roquette, *Formally p-adic fields,* Springer-Verlag, 1984

[PrZi] A. Prestel, M. Ziegler, *Model theoretic methods in the theory of topological fields* J. reine angew. Math 299/300, 318-341 (1978)

[Ra] E. Rannou, *Complexite d'algorithmes des stratification,* Thesis, Rennes (1993)

[Ru] R. Rumeley, *Arithmetic over the ring of all algebraic integers,* J. reine angew. Math 368 (1986), 127-133

[Sa1] T. Sander *Existence and uniqueness of the real closure of an ordered field without Zorn's Lemma,* J. Pure Appl. Algebra 73, 165-180 (1991)

[Sa2] T. Sander, *Effektive algebraische Geometrie über nicht algebraisch abgeschlossenen Körpern*, Dissertation, Dortmund, 1996, available via
http://www.mathematik.uni-dortmund.de/lsvi/Sander.html

[Se] A. Seidenberg, *Constructions in Algebra,* Trans. AMS 197, 273-313 (1974)

[Sh] I.R Shafarevich, *Basic algebraic geometry,* Springer-Verlag, 1977

[SiTa] J. Silverman, J. Tate, *Rational points on elliptic curves*, Springer-Verlag, 1977

[Sm] R.L. Smith, *Effective valuation theory* in Aspects of effective algebra, Proceedings, Ed J. Crossley, Upside down a book company, 1981

[Sch] J. Schmid, *On the affine Bezout inequality,* Manuscripta math. 88, 225-232 (1995)

[Schw] N. Schwartz, *Chain signatures and real closures,* J. reine angew. Math 347, 1-20 (1984)

[We1] V. Weispfenning, *On the elementary theory of Hensel fields*, Ann. math. Logic 10 (1976) 59-93

[We2] V. Weispfenning, *Nullstellensätze - a model theoretic framework,* Zeitschr. f. math. Logik und Grundlagen d. Math. 23, 539-545 (1977)

[We3] V. Weispfenning, *Quantifier elimination and decision procedures for valued fields,* Proceedings Logic Coll. '83, Aachen, Lecture Notes in Mathematics 1103, Springer-Verlag 1983

[We4] V. Weispfenning, *Some bounds for the construction of Gröbner bases,* Proceedings AAECC-4, Lecture Notes in Computer Science, Springer-Verlag, 195-201 (1988)

[We5] V. Weispfenning, *Comprehensive Gröbner bases,* J. Symb. Comp. 14/1, 1-29 (1992)

[Zi] M. Ziegler, *Die elementare Theorie henselscher Körper,* Dissertation, Universität Köln (1972)