A

The System CASA

In this appendix, we briefly describe the mathematical software package CASA and we illustrate, by means of some examples, how some of the algorithms in the book can be carried out with this package. CASA has been developed by the computer algebra research group at the Research Institute for Symbolic Computation (RISC) of Johannes Kepler University in Linz, Austria. It can be freely downloaded at

`http://www.risc.uni-linz.ac.at/software`.

CASA or Computer Algebra Software for constructive Algebraic geometry is based on Maple, and it is designed for symbolic manipulation in algebraic geometry, mainly in projective algebraic geometry, over an algebraically closed field of characteristic zero. Essentially, the package provides some basic functions for the algebraic manipulation of geometric objects from the practical point of view. Many of the algorithms in CASA are now integrated into major computer algebra software such as Maple. A reference to CASA can be found in the example worksheet for the algebraic curves package of Maple 10.

The main data structure of CASA is that of an algebraic sets. In the following, we describe some of the functions of the package. For more details we refer to [GKW91], and [HHW03]. In CASA an algebraic set can be given implicitly, parametrically, by places or by projection. The system provides functions for computing with algebraic sets, as well as conversion algorithms between different representations. The functions of CASA can roughly be grouped as follows:

1. computations with ideals
2. determination of algebraic sets in different representations
3. conversion algorithms between representations
4. determination of linear systems of curves
5. intersection, union and difference of algebraic sets
6. computation of tangent spaces
7. computation of the dimension of algebraic sets
8. decomposition of an algebraic set on irreducible components

9. projection of algebraic sets onto hypersurfaces
10. computation of singularities and genus
11. algorithms of parametrization and implicitation
12. determination of Puiseux series
13. multivariate resultants and Dixon resultants
14. Gröbner bases for ideals and modules
15. Gröbner walk
16. computation of rational points
17. plotting of curves and surfaces
18. manipulation of offset curves
19. algorithms in algebraic coding theory

Let us illustrate the usability of CASA by means of some examples. First we read the package within the Maple session.

```
> with(casa);
```

```
           |__|
           |  |       Welcome to CASA 2.5 for Maple V.5
     |   /\|  |/\
    /=\__|  []  |
   /             \_    Copyright (C) 1990-2000 by Research Institute
   |               \   for Symbolic Computation (RISC-Linz), the
   \   CASA 2.5    |   University of Linz, A-4040 Linz, Austria.
    |              |
   _|     |||     |   For help type '?casa' or '?casa,<topic>'.
__/       |||     |_
```

[BCH2, BCHDecode, CyclicEncode, DivBasisL, GWalk, GoppaDecode, GoppaEncode, GoppaPrepareDu, GoppaPrepareSV, GoppaPrepareSa, GoppaPrimary, Groebnerbasis, InPolynomial, NormalPolynomial, OutPolynomial, PolynomialRoots, RPHcurve, SakataDecode, SubsPolynomial, _casaAlgebraicSet, adjointCurve, algset, casaAttributes, casaVariable, computeRadical, conic, decompose, delete, dimension, equalBaseSpaces, equalProjectivePoints, finiteCurve, finiteField, generators, genus, homogeneousForm, homogeneousPolynomial, homogenize, implDifference, implEmpty, implEqual, implIdealQuo, implIntersect, implOffset, implSubSet, implUnion, implUnionLCM, imult, independentVariables, init, isProjective, leadingForm, makeDivisor, mapOutPolynomial, mapSubsPolynomial, mgbasis, mgbasisx, mkAlgSet, mkImplAlgSet, mkParaAlgSet, mkPlacAlgSet, mkProjAlgSet, mnormalf, msolveGB, msolveSP, mvresultant, neighbGraph, neighborhoodTree, numberOfTerms, pacPlot, paraOffset, parameterList, passGenCurve, planecurve, plotAlgSet, pointInAlgSet, projPoint, properParametrization, properties, rationalPoint, realroot_a, realroot_sb, setPuiseuxExpansion, setRandomParameters, singLocus, singularities, ssiPlot,

subresultantChain, tangSpace, toAffine, toImpl, toPara, toPlac, toProj, toProjective, tsolve, variableDifferentFrom, variableList]

We start with a complex affine plane curve $\mathcal{C}$ of degree 15 defined by the polynomial:

$$f := -15\,x^5y^4 - 21\,y^2x^8 - 7\,y^2x^7 - 3\,y^3x^6 - 30\,x^2y^8 + 2\,y^4x^9 + 3\,y^6x^5 + 3\,y^5x - 5\,yx^8 + y^5x^8 - 11\,xy^{10} + 11\,x^6y^8 + y^2x^3 - 68\,y^5x^6 - y^8x^7 + 7\,y^4x^2 + 15\,x^{10}y^2 - 2\,y^6x^4 + 2\,y^9x^3 - 2\,x^7y - 22\,x^8y^4 - 11\,x^5y^5 + 5\,y^3x^3 - x^5y^2 - 106\,y^3x^8 + 5\,x^2y^7 - 165\,y^4x^7 + 3\,x^{10}y + 167\,y^7x^6 + x^{10} + 33\,y^5x^2 + 13\,y^6x + 12\,x^{10}y^3 + 21\,y^4x^3 + 76\,y^8x^5 - x^8 + 165\,y^6x^2 - 3\,x^5y^3 + 33\,y^6x^6 - 3\,y^8 + 15\,y^7x^5 - 5\,x^7y^5 + 106\,y^5x^3 + 22\,x^3y^6 - y^7 - y^7x^3 + 22\,x^7y^7 + 65\,y^3x^9 - 167\,y^9x - x^6y^2 - 15\,y^9 - 2\,y^7x^8 - y^3x^{11} - 33\,y^8x + 69\,y^7x + y^{10}x^2 - 13\,y^4x^6 + 30\,x^7y^6 - 33\,y^3x^7 - 22\,x^2y^9 - 65\,y^5x^4 - 76\,y^{10} + 2\,y^3x^2 + y^4x$$

We declare $\mathcal{C}$ to be the curve defined by f; i.e., we "make an implicitly defined algebraic set" from f and the variables x, y. For a detailed description of this command call help(casa,mkImplAlgSet).

```
> C:=mkImplAlgSet([f],[x,y]);
```

$$\begin{aligned}&\text{C} := \text{Implicit\_Algebraic\_Set}([\text{y}^{10}\,x^2 - y^7 - 3\,y^8 - y^7\,x^3 + 30\,x^7\,y^6 \\ &- y^3\,x^{11} - x^6\,y^2 - 33\,y^3\,x^7 - 22\,x^2\,y^9 - 3\,y^3\,x^6 - 65\,y^5\,x^4 - 7\,y^2\,x^7 \\ &+ 2\,y^3\,x^2 - 13\,y^4\,x^6 + 13\,y^6\,x - 22\,x^8\,y^4 - 2\,y^6\,x^4 - 5\,y\,x^8 + y^4\,x + 69\,y^7\,x \\ &- 15\,x^5\,y^4 - 21\,y^2\,x^8 - 76\,y^{10} - 33\,y^8\,x - 2\,y^7\,x^8 + 65\,y^3\,x^9 - 167\,y^9\,x \\ &+ 22\,x^7\,y^7 + 22\,x^3\,y^6 + 106\,y^5\,x^3 - 5\,x^7\,y^5 + 15\,y^7\,x^5 + 33\,y^6\,x^6 - 3\,x^5\,y^3 \\ &+ 76\,y^8\,x^5 + 21\,y^4\,x^3 + 33\,y^5\,x^2 + 12\,x^{10}\,y^3 + 3\,x^{10}\,y + 167\,y^7\,x^6 - 15\,y^9 \\ &- x^8 + y^5\,x^8 + x^{10} + y^2\,x^3 - y^8\,x^7 - 165\,y^4\,x^7 + 5\,x^2\,y^7 + 165\,y^6\,x^2 \\ &+ 5\,y^3\,x^3 - 106\,y^3\,x^8 - 11\,x\,y^{10} + 11\,x^6\,y^8 - 68\,y^5\,x^6 + 7\,y^4\,x^2 + 15\,x^{10}\,y^2 \\ &+ 2\,y^9\,x^3 - 2\,x^7\,y - 11\,x^5\,y^5 - x^5\,y^2 - 30\,x^2\,y^8 + 2\,y^4\,x^9 + 3\,y^6\,x^5 \\ &+ 3\,y^5\,x],\ [x,\ y])\end{aligned}$$

Let us compute the components of $\mathcal{C}$ (see Sect. 2.1).

```
> Components:=decompose(C);
```

$$\begin{aligned}&\text{Components} := \text{Implicit\_Algebraic\_Set}([\text{y}^2 - x^5],\ [x,\ y]), \\ &\text{Implicit\_Algebraic\_Set}([y^5 + 2\,y^4\,x - y^2\,x - 2\,y\,x^2 - x^3 + x^4],\ [x,\ y]), \\ &\text{Implicit\_Algebraic\_Set}([\text{y}^3\,x^2 - 11\,y^3\,x - 76\,y^3 - 15\,y^2 \\ &-3\,y - 1 - 15\,y^2\,x - 3\,y\,x - x],\ [x,\ y])\end{aligned}$$

So we see that $\mathcal{C}$ has three irreducible components, each of them of degree 5. Let us call them $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$, respectively. We give names to them in Maple

```
> for i from 1 to 3 do C[i]:=Components[i] od:
```

Now, we proceed to compute the genus of each component of $\mathcal{C}$ (see Sect. 3.3).

```
> for i from 1 to 3 do g[i]:=genus(C[i]) od;
```

$$g_1 := 3$$
$$g_2 := 0$$
$$g_3 := 0$$

We can ask for information on algebraic sets:

```
> properties(C[1]);
```

"The algebraic set is known to have the following properties:"

"It has genus 3"

"A neighborhood graph is: "

$$[[3,\ 0,\ 0,\ 1,\ \{y = y - x,\ x = x + y\},\ []]]$$

$$\text{Implicit\_Algebraic\_Set}([y^5 + 2\,y^4\,x - y^2\,x - 2\,y\,x^2 - x^3 + x^4],\ [x,\ y])$$

We determine the singularities of the curves. The singularities are given projectively with their multiplicities (see Sect. 2.1).

```
> singularities(C[1]);
```

$$\text{table}([3 = [[0,\ 0,\ 1]]])$$

```
> singularities(C[2]);
```

$$\text{table}([2 = [[\frac{40}{21}\,\text{RootOf}(5\,\_Z^2 + 4\,\_Z + 89) - \frac{5}{21},\ -\frac{5}{21} - \frac{2}{21}\,\text{RootOf}(5\,\_Z^2 + 4\,\_Z + 89),\ 1],\ [0,\ 1,\ 0]],\ 3 = [[1,\ 0,\ 0]]])$$

```
> singularities(C[3]);
```

$$\text{table}([2 = [[0,\ 0,\ 1]],\ 3 = [[0,\ 1,\ 0]]])$$

$\mathcal{C}_1$ has one triple point. $\mathcal{C}_2$ has three double points, two of them in an algebraic extension of degree 2 (each of them depending on one root of the polynomial $5x^2 + 4x + 89$), and one triple point. $\mathcal{C}_3$ has one double point and one triple point. Thus, genus($\mathcal{C}_1$) = 3, and genus($\mathcal{C}_2$) = 0. However, in the case of $\mathcal{C}_3$ there must be infinitely near singularities. Let us compute the neighborhood graph for $\mathcal{C}_3$ (see Sect. 3.2).

```
> neighbGraph(C[3]);
```

$[[2,\ 0,\ 0,\ 1,\ \{x = x + y,\ y = y - x\},\ [[2,\ 1,\ 1,\ 0,\ \{\},\ []]]],$
$[3,\ -1, 1, 0,\ \{x = x + y,\ y = y - x\},\ [[2,\ 2,\ 1,\ 0,\ \{x = x + 2\,y,\ y = y - 2\,x\},\ []]]]$

In the blow-up, every singularity has an infinitely near double point. Note that we also get information on the necessary linear changes for the blowing up (compare Sect. 3.2).

Since the curves $\mathcal{C}_2$ and $\mathcal{C}_3$ have genus zero, we may determine rational parametrizations of these curves (see Sect. 4.8). In addition, these parametrizations can be obtained over the original ground field if possible (with the optional argument: OPTIMAL), or otherwise over an algebraic extension field of degree 2 (see Sect. 5.3).

```
> P[2]:=toPara(C[2],t,["optimal"]);
```

$$P_2 := \text{Parametric\_Algebraic\_Set}([-t^3 + 3\,t^2 - 3\,t,\ -\frac{t-1}{-4 + t^2 - t}],\ [t])$$

```
> P[3]:=toPara(C[3],t);
```

$$P_3 := \text{Parametric\_Algebraic\_Set}([\frac{1}{t^2},\ -\frac{1}{t^5}],\ [t])$$

Since the curve $\mathcal{C}_1$ has positive genus, we deduce that it is not rational. However, we may compute a local parametrization with center, for instance, at $(0, 0)$ (see Sect. 2.5).

```
> properties(toPlac(C[1]));
```

"The algebraic set is known to have the following properties:"

"There are at least 3 terms to show in the Puiseux expansion"

$$\text{Places\_Algebraic\_Set}([[x^2,\ -x^2 - x^3 - \frac{1}{2}\,x^5 - \frac{3}{2}\,x^6 - \frac{7}{8}\,x^7 + x^8 - \frac{3}{16}\,x^9 + \text{O}(x^{10})],\ [x^3,\ x + \frac{1}{3}\,x^5 - \frac{2}{3}\,x^7 - \frac{1}{3}\,x^8 + x^9 + \text{O}(x^{10})]],\ [x])$$

Now, we can implicitize the rational parametrizations given by P_2 and P_3 (see Sect. 4.5).

```
> toImpl(P[3]);toImpl(P[2]);
```

$$\text{Implicit\_Algebraic\_Set}([x^5 - y^2],\ [x,\ y])$$

$$\text{Implicit\_Algebraic\_Set}([y^3\,x^2 - 11\,y^3\,x - 76\,y^3 - 15\,y^2 - 3\,y - 1 - 15\,y^2\,x - 3\,y\,x - x],\ [x,\ y])$$

We may determine a reparametrization of the curve $\mathcal{C}_2$ by performing a substitution of the parameter in the algebraic set P_2 in parametric representation.

```
> RP[2]:=mkAlgSet(P[2],[t=t^2-2]);
```

$$RP_2 := \text{Parametric\_Algebraic\_Set}([-t^6 + 9\,t^4 - 27\,t^2 + 26, -\frac{t^2-3}{t^4 - 5\,t^2 + 2}],\ [t])$$

Observe that now, the parametrization RP_2 of the curve $\mathcal{C}_2$ is not proper. However, from the parametrization RP_2, we may determine a new proper parametrization of $\mathcal{C}_2$ (see Sect. 6.1).

```
> properParametrization(RP[2]) ;
```

$$[\frac{-26 + 51\,t - 33\,t^2 + 7\,t^3}{-1 + t^3 - 3\,t^2 + 3\,t}, -\frac{2\,t^2 - 5\,t + 3}{2\,t^2 - t - 2}]$$

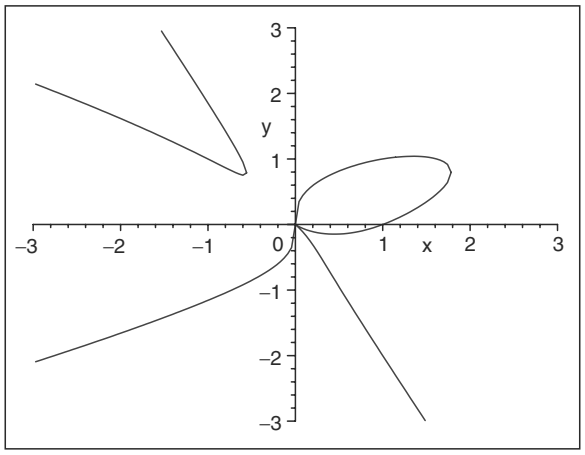
CASA can also plot the following types of algebraic sets: planar curves represented implicitly, in parametric form or by places, space curves represented implicitly, in parametric form, in projected form or by places, surfaces represented implicitly or in parametric form. Let us plot the plane curves $\mathcal{C}_1, \mathcal{C}_2$, and $\mathcal{C}_3$.

```
> plotAlgSet(C[1],x=-3..3,y=-3..3,numpoints=200,thickness=5,
color=blue);
```

Time for isolating critical points : , .047

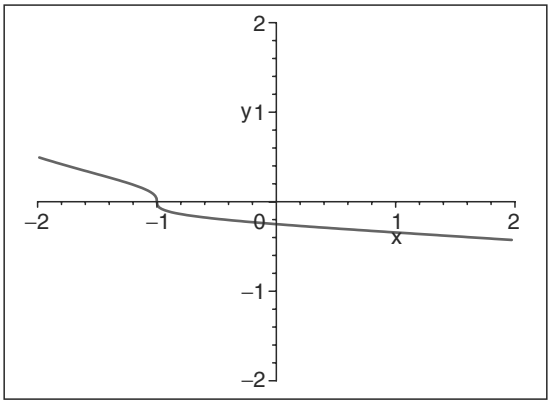
Time for finding intermediate points : , 1.156

Time for others : , .0



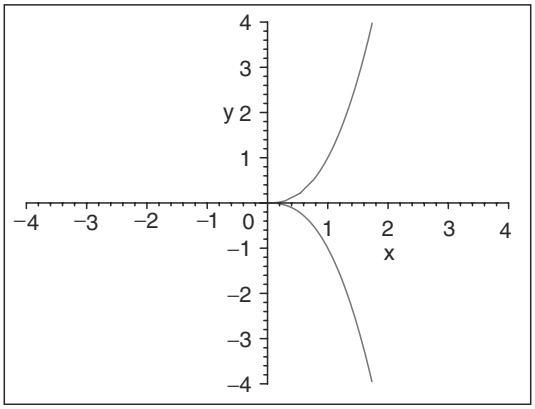
```
> plotAlgSet(C[2],x=-2..2,y=-2..2,numpoints=200,thickness=5,
color=red);
```

Time for isolating critical points : , .016
Time for finding intermediate points : , 2.703
Time for others : , .032




```
> plotAlgSet(C[3],x=-4..4,y=-4..4,numpoints=200,thickness=5);
```

Time for isolating critical points : , .031
Time for finding intermediate points : , .532
Time for others : , .015



Let us also plot the whole composite curve $\mathcal{C}$.

```
> plotAlgSet(C,x=-2..2,y=-2..2,numpoints=200, thickness=5,
color=pink)
```

Time for isolating critical points : , .012

Time for finding intermediate points : , 0.516

Time for others : , .0

Time for isolating critical points : , .031

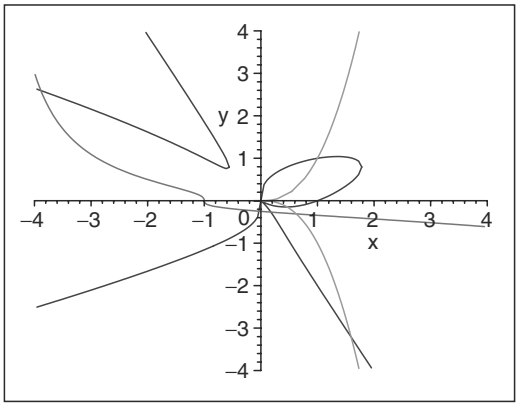
Time for finding intermediate points : , 2.375

Time for others : , .031

Time for isolating critical points : , .047

Time for finding intermediate points : , 1.500

Time for others : , .0



Finally, for computing the intersection multiplicity of two plane curves at an intersection point (see Sect. 2.3), we may use the command IMULT:

```
> imult(C[1],C[3],[0,0]);
```

B

Algebraic Preliminaries

For a thorough introduction to algebra we refer the reader to any of a great number of classical textbooks, e.g., [BiM79], [Lan84], [ZaS58] or [VaW70]. We denote the set of natural numbers (including 0) by $\mathbb{N}$, the integers by $\mathbb{Z}$, the rational numbers by $\mathbb{Q}$, the real numbers by $\mathbb{R}$, and the complex numbers by $\mathbb{C}$.

B.1 Basic Ring and Field Theory

A *semigroup* $(S, \circ)$ is a set S together with an associative binary operation $\circ$ on S. A semigroup is *commutative* iff the operation $\circ$ is commutative. A *monoid* $(S, \circ, e)$ is a semigroup with an identity element e; that is $e \circ x = x \circ e = x$, for all $x \in S$. A monoid is *commutative* iff the operation $\circ$ is commutative. For a monoid S, we denote by S^* the set $S \setminus \{e\}$. A *group* $(G, \circ, \diamond, e)$ is a monoid $(G, \circ, e)$ together with a unitary inverse operation $\diamond$; that is, $x \circ (\diamond x) = (\diamond x) \circ x = e$, for all $x \in G$. G is *commutative* or *abelian group* iff the operation $\circ$ is commutative.

A *ring* $(R, +, \cdot, 0)$ is an abelian group $(R, +, 0)$, and a semigroup $(R, \cdot)$ satisfying the laws of distributivity $x \cdot (y + z) = x \cdot y + x \cdot z$, and $(x + y) \cdot z = x \cdot z + y \cdot z$. A *commutative ring* is one in which the operation $\cdot$ is commutative. A *ring with identity* is a ring R together with an element 1 $(\neq 0)$, such that $(R, \cdot, 1)$ is a monoid. If R is a ring (with identity or not), by R^* we denote the set $R \setminus \{0\}$. Unless stated otherwise, we will always use the symbols $+, -, \cdot, 0, 1$ for the operations of a ring. We call these operations *addition*, *subtraction*, *multiplication*, *zero*, and *one*. The *subtraction* operation is defined as $x - y := x + (-y)$, for $x, y \in R$.

The *characteristic* of a commutative ring with identity R, char*(R)*, is the least positive integer m such that $\underbrace{1 + \cdots + 1}_{m \text{ times}} = 0$. $\text{char}(R) = 0$ if no such m exists.

Let $(R, +, \cdot, 0)$ and $(\widetilde{R}, \widetilde{+}, \widetilde{\cdot}, \widetilde{0})$ be rings. A *ring homomorphism* h is a function from R to $\widetilde{R}$ satisfying the conditions

$$h(r+s) = h(r)\widetilde{+}h(s), \quad h(r \cdot s) = h(r)\widetilde{\cdot}h(s).$$

Furthermore, if R and $\widetilde{R}$ are rings with identities 1 and $\widetilde{1}$, respectively, and h is not the zero-homomorphism, then $h(1) = \widetilde{1}$. Moreover, if h is one-to-one and onto then h is called an *isomorphism from R to $\widetilde{R}$*. In this case, we say that R and $\widetilde{R}$ are *isomorphic*, and we write $R \cong \widetilde{R}$.

A nonzero element a of R is a *zero divisor* iff for some nonzero $b \in R$, we have that $a \cdot b = 0$. An *integral domain* or a *domain* D is a commutative ring with identity having no zero divisors.

A *field* $(K, +, \cdot, 0, 1)$ is a commutative ring with identity $(K, +, \cdot, 0, 1)$, and simultaneously a group $(K^\star, \cdot, 1)$. If all the operations on K are computable, we call K a *computable field*.

Let D be an integral domain. The *quotient field* $Q(D)$ of D is defined as

$$Q(D) = \{\frac{a}{b} \mid a, b \in D,\ b \neq 0\}/\sim,$$

where $\frac{a}{b} \sim \frac{c}{d}$ if and only if $ad = bc$. The operations $+, -, \cdot, ^{-1}$, can be defined on representatives of the elements of $Q(D)$ as:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad -\frac{a}{b} = \frac{-a}{b}, \qquad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

$Q(D)$ is the smallest field containing D.

Let $(R, +, \cdot, 0, 1)$ be a commutative ring with identity. A nonempty subset I of R is an *ideal* in R iff $a + b \in I$, and $a \cdot c \in I$ for all $a, b \in I$, and $c \in R$. Moreover we say that I is a *proper ideal* iff $\{0\} \neq I \neq R$. I is a *maximal ideal* if it is not contained in a bigger proper ideal. I is a *prime ideal* iff $a \cdot b \in I$ implies that $a \in I$ or $b \in I$. I is a *primary ideal* if $a \cdot b \in I$ implies that $a \in I$ or $b^n \in I$ for some $n \in \mathbb{N}$. I is a *radical ideal* iff $a^n \in I$ for some $n \in \mathbb{N}$ implies that $a \in I$. Moreover, the *radical* of the ideal I is the ideal $\{a \mid a^n \in I \text{ for some } n \in \mathbb{N}\}$, and we denote it by $\sqrt{I}$ or radical(I). A set $B \subseteq R$ *generates the ideal* I or B is a *generating set* or a *basis for* I iff

$$I = \{\sum_{i=1}^{n} r_i b_i \mid n \in \mathbb{N}^\star,\ r_i \in R,\ b_i \in B\}.$$

In this case, we say that the ideal I is *generated* by B, and we denote this by $I = \langle B \rangle$. Furthermore, we say that the ideal I is *finitely generated* if it has a finite generating set. If the cardinality of the generating set is 1, we say that I is a *principal ideal*.

An ideal I in R generates a *congruence relation*, $\equiv_I$ on R by $a \equiv_I b$ or $a \equiv b \bmod I$ iff $a - b \in I$. In this case we say that a *is congruent to* b *modulo* I. Observe that the factor ring R/I consisting of the congruence

classes w.r.t. $\equiv_I$ inherits the operations of R in a natural way. If R is a commutative ring with identity 1 and I is a prime ideal of R, then R/I is an integral domain. If I is maximal, then R/I is a field.

In the following considerations, we take nonzero elements of a commutative ring R with identity 1. Invertible elements of R are called *units*. If $a = b \cdot u$ for a unit u, then a and b are called *associated*. b *divides* a iff $a = b \cdot c$ for some $c \in R$. If c divides $a - b$ we say that a is *congruent* to b modulo c, and we write this as $a \equiv_c b$ or $a \equiv b \bmod c$ or $a \equiv b \bmod < c >$. The congruence modulo c is an equivalence relation.

An element a of R is *irreducible* iff every b dividing a is either a unit or associated to a. An element a of R is *prime* iff a is not a unit, and whenever a divides a product $b \cdot c$, then a divides either b or c; i.e. if $< a >$ is a proper prime ideal. In general prime and irreducible elements can be different; for instance, 6 has two different factorizations into irreducibles in $\mathbb{Z}[\sqrt{-5}]$, and none of these factors is prime.

A *principal ideal domain* D is a domain in which every ideal is principal. An integral domain D is a *unique factorization domain* iff every nonunit of D is a finite product of irreducible factors and every such factorization is unique up to reordering and unit factors. In a unique factorization domain prime and irreducible elements are the same. An element a is *squarefree* iff every nonunit factor of a occurs with multiplicity exactly 1 in a.

Let D be an integral domain, and let $a, b \in D$ such that at least one of them is not zero. We say that $d \in D$ is a *greatest common divisor (gcd)* of a and b iff (i.) d divides both a and b, and (ii.) if c is a common divisor of a and b then, c divides d. In a unique factorization domain the gcd always exists, and it is determined up to associates. Moreover, if R is a principal ideal domain, the greatest common divisor $d \in R$, can be written as a linear combination $d = s \cdot a + t \cdot b$, for some $s, t \in R$. This equation is called the *Bézout equality*, and s, t are the *Bézout cofactors*. If $\gcd(a, b) = 1$, we say that a and b are *relatively prime*.

In $\mathbb{Z}$ we have the well known *Euclidean Algorithm* for computing a gcd. In general, an integral domain D in which we can execute the Euclidean algorithm, i.e., we have division with quotient and remainder such that the remainder is less than the divisor, is called a *Euclidean Domain*. More precisely, a Euclidean domain D is an integral domain together with a degree function $\deg : D^\star \to \mathbb{N}$, such that

1. $\deg(a \cdot b) \geq \deg(a)$ for all $a, b \in D^\star$,
2. (division property) for all $a, b \in D$, $b \neq 0$, there exists a *quotient* q and a *remainder* r in D such that $a = q \cdot b + r$ and $r = 0$ or $\deg(r) < \deg(b)$.

Every Euclidean domain is a principal ideal domain and every principal ideal domain is a unique factorization domain. However, the reverse implications do not hold in general.

In a Euclidean Domain, the Euclidean algorithm can be adapted such that the Bézout cofactors are also computed. Usually, this extension is called the extended Euclidean algorithm.

B.2 Polynomials and Power Series

Let R be a ring. A *(univariate) polynomial over* R is a mapping $p : \mathbb{N} \longrightarrow R$, $n \longmapsto p_n$, such that $p_n = 0$ nearly everywhere, i.e., for all but finitely many values of n. If $n_1 < n_2 < \cdots < n_r$ are the nonnegative integers for which p yields a nonzero result, then we usually write

$$p = p(x) = \sum_{i=1}^{r} p_{n_i} x^{n_i}.$$

p_j is the *coefficient* of x^j in the polynomial p, and we denote it by $\mathrm{coeff}(p, j)$. If p is the zero mapping, we say that p is the zero polynomial. The set of all polynomials over R together with the usual addition and multiplication of polynomials form a ring over R, which is denoted by $R[x]$. The *degree* of a nonzero polynomial p, $\mathrm{degree}(p)$, is the maximal $n \in \mathbb{N}$ such that $p_n \neq 0$. We say that the degree of the zero polynomial is -1. The *leading term* of a nonzero polynomial p is $x^{\mathrm{degree}(p)}$, denoted by $\mathrm{lt}(p)$. The *leading coefficient* of a nonzero polynomial p is the coefficient of $\mathrm{lt}(p)$, denoted by $\mathrm{lc}(p)$. For the zero polynomial the leading coefficient and the leading term are undefined. A polynomial p is *monic* iff $\mathrm{lc}(p) = 1$.

If R is an integral domain, then also the ring of polynomials $R[x]$ over R is an integral domain. Furthermore, if R is a unique factorization domain, then also the ring of polynomials $R[x]$ over R is a unique factorization domain.

An *n-variate polynomial over* R is a mapping $p : \mathbb{N}^n \longrightarrow R$, $(i_1, \ldots, i_n) \longmapsto p_{i_1,\ldots,i_n}$, such that $p_{i_1,\ldots,i_n} = 0$ nearly everywhere. We usually write

$$p = p(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} p_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

The set of all n-variate polynomials over R together with the usual addition and multiplication of polynomials form a ring over R, which is denoted by $R[x_1, \ldots, x_n]$. The n-variate polynomial ring can be viewed as built up successively from R by adjoining one polynomial variable at a time. In fact, $R[x_1, \ldots, x_n]$ is isomorphic to $(R[x_1, \ldots, x_{n-1}])[x_n]$. The *total degree* of an n-variate polynomial p is defined as the maximal $\sum_{j=1}^{n} i_j$ such that $p_{i_1,\ldots,i_n} \neq 0$. We denote this total degree by $\mathrm{degree}(p)$. In addition, we write $\mathrm{coeff}(p, x_n, j)$ for the coefficient of x_n^j in the polynomial p, where p is considered in $(R[x_1, \ldots, x_{n-1}])[x_n]$. The *degree in the variable* x_n of

$$p = p(x_1, \ldots, x_n) = \sum_{i=0}^{m} p_i(x_1, \ldots, x_{n-1}) x_n^i \in (R[x_1, \ldots, x_{n-1}])[x_n]^\star$$

is m if $p_m \neq 0$, and we denote this by $\deg_{x_n}(p)$. By reordering the set of variables we get $\deg_{x_i}(p)$ for all $1 \leq i \leq n$. In a similar way, we get $\mathrm{lt}_{x_i}(p)$ and $\mathrm{lc}_{x_i}(p)$. If all the terms occurring (with nonzero coefficient) in the polynomial p have the same (total) degree, then p is call a *form* or a *homogeneous polynomial*.

An n-variate polynomial $p(x_1, \ldots, x_n)$ of total degree d can be written as

$$p(x_1, \ldots, x_n) = p_d(x_1, \ldots, x_n) + p_{d-1}(x_1, \ldots, x_n) + \cdots + p_0(x_1, \ldots, x_n),$$

where $p_i(x_1, \ldots, x_n)$ are forms of degree i, respectively (i.e., all the terms occurring in p_i are of the same degree and it is i). The homogenization $p^\star(x_1, \ldots, x_n, x_{n+1})$ of the polynomial $p(x_1, \ldots, x_n)$ is given as

$$p^\star(x_1, \ldots, x_n, x_{n+1}) =$$

$$p_d(x_1, \ldots, x_n) + p_{d-1}(x_1, \ldots, x_n)x_{n+1} + \ldots + p_0(x_1, \ldots, x_n)x_{n+1}^d.$$

The polynomial $p^\star(x_1, \ldots, x_n, x_{n+1})$ is homogeneous. For all $\alpha \in K^\star$, where K is a field, we have that $p^\star(a_1, \ldots, a_n, a_{n+1}) = 0$ if and only if it holds that $p^\star(\alpha\, a_1, \ldots, \alpha\, a_n, \alpha\, a_{n+1}) = 0$. Furthermore $p(a_1, \ldots, a_n) = 0$ if and only if $p^\star(a_1, \ldots, a_n, 1) = 0$. In addition, $p^\star(a_1, a_2, \ldots, a_n, 0) = p_d(a_1, \ldots, a_n) = 0$ means that there is a zero $(a_1, a_2, \ldots, a_n, 0)$ of $p^\star$ at infinity in the direction $(a_1, \ldots, a_n)$. By adding these points at infinity to affine space we get the corresponding projective space.

For homogeneous polynomials, we have the following well known *Euler's Formula*: let $F(x_1, \ldots, x_r)$ be an homogeneous polynomial of degree d. Then,

$$\sum_{i=1}^{r} x_i \cdot \frac{\partial F}{\partial x_i} = d \cdot F.$$

Let K, L be fields such that $K \subset L$. Let $\alpha \in L$ such that $f(\alpha) = 0$ for some irreducible $f \in K[x]$. Then, α is called *algebraic* over K of degree $\deg(f)$. If α is not algebraic over K, the we say that α is *transcendental* over K. The polynomial f is determined up to a constant and it is called the *minimal polynomial* of α over K. In addition, by $K(\alpha)$ we denote the smallest field containing K and α. $K(\alpha)$ is called a *(simple) algebraic extension field* of K. For representing the elements in the algebraic extension field $K(\alpha)$ of K, we use the isomorphism $K(\alpha) \cong K[x]/\langle f(x)\rangle$, where $\langle f(x)\rangle$ denotes the ideal generated by $f(x)$ in $K[x]$. Every polynomial can be reduced modulo $f(x)$ to some $r(x)$, with $\deg(r) < \deg(f)$. On the other hand, two different polynomials $r(x), s(x)$ with $\deg(r), \deg(s) < \deg(f)$ cannot be congruent modulo $f(x)$, since otherwise $r - s$, a nonzero polynomial of degree less than $\deg(f)$, would be a multiple of f. Thus, every element $a \in K(\alpha)$ has a unique representation

$$a = \underbrace{a_{m-1}x^{m-1} + \ldots + a_1 x + a_0}_{a(x)} + \langle f(x)\rangle, \quad a_i \in K.$$

We call $a(x)$ the *normal representation* of a. Observe that from this unique normal representation we can immediately deduce that $K(\alpha)$ is a vector space over K of dimension $\deg(f)$, and $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis of this vector space.

The field $\overline{K}$ is called the *algebraic closure* of K if $\overline{K}$ is algebraic over K and every polynomial $f(x) \in K$ has a root over $\overline{K}$, so that $\overline{K}$ can be said to contain all the elements that are algebraic over K. We say that K is algebraically closed if $K = \overline{K}$.

Let K be a field, and let $\overline{K}$ be the algebraic closure of K. A polynomial $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is *irreducible* over K if and only if every $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ dividing f is either a unit or an associate of f. Moreover, if $f(x_1, \ldots, x_n)$ has no nontrivial factor in $\overline{K}[x_1, \ldots, x_n]$, then $f(x_1, \ldots, x_n)$ is called *absolutely irreducible*. A factorization over $\overline{K}$ is called an *absolute factorization*.

Let I be an ideal. A univariate polynomial $p(x)$ over I is *primitive* if and only if there is no prime in I which divides all the coefficients in $p(x)$. Every polynomial $q(x) \in I[x]$ can be decomposed uniquely, up to multiplication by units, as

$$q(x) = \mathrm{cont}(q) \cdot \mathrm{pp}(q),$$

where $\mathrm{cont}(q) \in I$, and $\mathrm{pp}(q)$ is the primitive polynomial in $I[x]$. We call $\mathrm{cont}(q)$ the *content* of $q(x)$, and $\mathrm{pp}(q)$ the *primitive part* of $q(x)$.

If K is a field, then $K[x]$ is a Euclidean domain, so $h = \gcd(f, g)$, for $f, g \in K[x]$ can be computed by means of the Euclidean Algorithm.

A polynomial $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is *squarefree* if and only if every nontrivial factor $q(x_1, \ldots, x_n)$ of p (i.e, q not associated to p and not a constant) occurs with multiplicity exactly 1 in p. There is a simple criterion for deciding squarefreeness (see for instance [Win96], pp.101). More precisely, let $q(x)$ be a nonzero polynomial in $K[x]$, where $\mathrm{char}(K)$ is either zero or prime. Then, $q(x)$ is squarefree if and only if $\gcd(q(x), q'(x)) = 1$ ($q'(x)$ is the derivative of $q(x)$). The problem of squarefree factorization of $q(x) \in K[x]$ consists of determining the squarefree pairwise relatively prime polynomials $q_1(x), \ldots, q_s(x)$ such that

$$q(x) = \prod_{i=1}^{s} q_i(x)^{e_i},$$

where $e_i \in \mathbb{N}$. The representation of $q(x)$ as above is called the *squarefree factorization of* $q(x)$. For a thorough introduction to factorization of polynomials we refer the reader to Chapter 5 in [Win96].

Let K be a field. A *power series* $A(x)$ over K is a mapping $A : \mathbb{N} \longrightarrow K$. Usually we write a power series as $A(x) = \sum_{i=0}^{\infty} a_i x^i$, where a_i is the image of i under the mapping A.

The set of all power series over K form a commutative ring with 1 and we denote this ring by $K[[x]]$. The *order* of the power series A is the smallest i such that $a_i \neq 0$.

Taylor's Theorem *Let D be a unique factorization domain of characteristic zero, and let $f(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$. Let $p = (a_1, \ldots, a_n)$, $a_i \in D$, and $h = (h_1, \ldots, h_n) = (x_1 - a_1, \ldots, x_n - a_n)$. Then,*

$$f(x_1, \ldots, x_n) = f(p) + \sum_{i_1=1}^{n} \frac{\partial f(p)}{\partial x_{i_1}} h_{i_1} + \frac{1}{2!} \sum_{i_1, i_2=1}^{n} \frac{\partial^2 f(p)}{\partial x_{i_1} \partial x_{i_2}} h_{i_1} h_{i_2} + \cdots +$$

$$\frac{1}{k!} \sum_{i_1, \ldots, i_k=1}^{n} \frac{\partial^k f(p)}{\partial x_{i_1} \ldots \partial x_{i_k}} h_{i_1} \cdots h_{i_k} + \cdots .$$

We call this expression the *Taylor expansion of the polynomial f at p.*

Taylor's Theorem for univariate analytic functions: *Let $f(z)$ be a complex analytic function in an open disk centered at z_0 and radius r. Then, for $|z - z_0| < r$, the power series $\sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n$ converges to $f(z)$.*

Implicit Mapping Theorem (see [Gun90]): *Let F be an holomorphic mapping from an open neighborhood of a point $A \in \mathbb{C}^n$ into $\mathbb{C}^m$ for some $m \leq n$, such that $F(A) = 0$ and $\operatorname{rank}(J''_F(A)) = m$, where $J_F(A) = (J'_F(A), J''_F(A))$ is the Jacobian matrix of F at A, and $J'_F(A)$ is an $m \times (n - m)$ matrix, and $J''_F(A)$ is an $m \times m$ matrix. Then, for some open polydisc $U(A, R) = U(A', R') \times U(A'', R'') \subset \mathbb{C}^{n-m} \times \mathbb{C}^m = \mathbb{C}^n$, there exists an holomorphic mapping $G : U(A', R') \to U(A'', R'')$ such that $G(A') = A''$, and $F(Z) = 0$ for some point $Z = (Z', Z'') \in U(A, R)$, precisely when $Z'' = G(Z')$.*

B.3 Polynomial Ideals and Elimination Theory

Let R be a commutative ring with identity 1 and $R[x_1, \ldots, x_n]$ the polynomial ring in n indeterminates over R. A commutative ring with identity R is called a *Noetherian ring* if and only if the *basis condition* holds in R, i.e., every ideal in R is finitely generated.

A commutative ring with identity R is Noetherian if and only if there are no infinitely ascending chains of ideals in R. I.e., if $I_1 \subseteq I_2 \subseteq \ldots \subseteq R$, then there is an index k such that $I_k = I_{k+1} = \cdots$.

Hilbert's Basis Theorem: *If R is a Noetherian ring then also the ring of polynomials $R[x]$ is Noetherian.*

Hilbert's basis theorem implies that the multivariate polynomial ring $K[x_1, \ldots, x_n]$ over a field K is Noetherian. So every ideal $I \in K[x_1, \ldots, x_n]$ has a finite basis, and if we are able to effectively compute with finite bases then we are dealing with all the ideals in $K[x_1, \ldots, x_n]$.

B.3.1 Gröbner Bases

The method of Gröbner bases was introduced by Buchberger in [Buc65], where he also developed an algorithm for computing it. Gröbner bases are

very special and useful bases for polynomial ideals. The Buchberger algorithm for constructing Gröbner bases is at the same time a generalization of the Euclidean Algorithm and of Gauss' triangularization algorithm for linear systems. Intuitively speaking, Gröbner bases can be motivated from different points of view. The first one is based on the theory of polynomials ideals, and the second one focuses on the application to the solution of systems of algebraic equations. In both cases, the difficulty of the problem comes from the need to generalize the Euclidean division to the non-Euclidean domain $K[x_1, \ldots, x_n]$, where K is a field.

Ideal theoretically the goal is to decide the "main problem in ideal theory", namely the question whether a polynomial $f \in K[x_1, \ldots, x_n]$ is contained in a given ideal I of the ring $R = K[x_1, \ldots, x_n]$. Observe that if R is univariate, then R is a Euclidean domain. Therefore, I is a principal ideal, and it can be expressed as $I = \langle g(x) \rangle$. So $f \in I$ if and only if f is a multiple of g if and only if the remainder of f on division by g is 0. In the multivariate case a Gröbner basis for the ideal I admits a generalization of the division algorithm such that $f \in I$ if and only if the remainder of f on division by the Gröbner basis is 0.

The Buchberger algorithm for computing a Gröbner basis for an ideal I can also be considered as a generalization of Gaussian elimination to the multivariate case. Given a system of algebraic, i.e., polynomial, equations

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, m,$$

where $f_i \in K[x_1, \ldots, x_n]$, we observe that the solutions of these equations over the algebraic closure of K remain unchanged when we replace the f_i by g_j, where $\{g_j | 1 \leq j \leq k\}$ is another basis for the ideal generated by $\{f_i | 1 \leq i \leq m\}$. If we determine a Gröbner basis w.r.t a lexicographic ordering of the terms, then we get a triangular basis comparable to a triangular system of linear equations. This property is expressed in the following theorem.

Theorem (elimination property of Gröbner bases): *Let G be a Gröbner basis for the ideal I in $K[x_1, \ldots, x_n]$ w.r.t. the lexicographic ordering $x_1 < x_2 < \cdots < x_n$. Then for every $i \in \{1, \ldots, n\}$ the ideal $I \cap K[x_1, \ldots, x_i]$ is generated by $G \cap K[x_1, \ldots, x_i]$.*

Any Gröbner basis allows to decide the solvability of the corresponding system of algebraic equations, simply by checking whether the Gröbner basis contains a constant. We can also read off whether the system has finitely or infinitely many solutions.

For a thorough introduction to Gröbner bases we refer the reader to [AdL94], [BeW93], [BCL83], [CLO97] or [Win96].

B.3.2 Resultants

Let D be a unique factorization domain, and let $f(x), g(x) \in D[x]$ be the polynomials

$$f(x) = a_n x^n + \cdots + a_0, \quad a_n \neq 0, \qquad g(x) = b_m x^m + \cdots + b_0, \quad b_m \neq 0.$$

The *resultant*, $\mathrm{res}_x(f,g)$, of the univariate polynomials $f(x), g(x)$ over D is the determinant of the Sylvester matrix of f and g, consisting of shifted lines of coefficients of f and g. More precisely, $\mathrm{res}_x(f,g) = \det(\mathrm{Syl}_x(f,g))$, where

$$\mathrm{Syl}_x(f,g) = \begin{pmatrix} a_n & \dots & a_0 & & \\ & a_n & \dots & a_0 & \\ & \ddots & \ddots & \ddots & \\ & & a_n & \dots & a_0 \\ b_m & \dots & b_0 & & \\ & b_m & \dots & b_0 & \\ & \ddots & \ddots & \ddots & \\ & & b_m & \dots & b_0 \end{pmatrix}.$$

$\mathrm{Syl}_x(f,g)$ contains m rows of coefficients of f, and n rows of coefficients of g.

Resultants have important properties (see [BrK86], [CLO98], [VaW70]). Some of the more important ones are the following:

1. $\mathrm{res}_x(f,g) = 0$ if and only if f and g have a common root.
2. $\mathrm{res}_x(f,g) = (-1)^{mn}\mathrm{res}_x(g,f)$.
3. Let α_i, $i = 1,\dots,n$, be the roots of f, and let β_i, $i = 1,\dots,m$, be the roots of g. Then

$$\mathrm{res}_x(f,g) = \mathrm{lc}(f)^m \mathrm{lc}(g)^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j), \text{ and } \mathrm{res}_x(f,g) = \mathrm{lc}(f)^m \prod_{j=1}^{n} g(\alpha_j).$$

4. There exist polynomials $a(x)$ and $b(x)$ over D such that $af + bg = \mathrm{res}_x(f,g)$.

The notion of resultant of two univariate polynomials can be generalized to multivariate polynomials. Let K be an algebraically closed field, and let $f(x_1,\dots,x_n)$, $g(x_1,\dots,x_n) \in K[x_1,\dots,x_n]$. We view the polynomials f and g as elements of $K[x_1,\dots,x_{n-1}][x_n]$ where the coefficients are in $K[x_1,\dots,x_{n-1}]$, and the main variable is x_n. So we may determine $R(x_1,\dots,x_{n-1}) := \mathrm{res}_{x_n}(f,g) \in K[x_1,\dots,x_{n-1}]$, and we have the following important property (see [Mis93]): if $(a_1,\dots,a_n) \in K^n$ is a common root of f and g, then $R(a_1,\dots,a_{n-1}) = 0$. Conversely, if $R(a_1,\dots,a_{n-1}) = 0$, then one of the following holds:

1. $\mathrm{lc}_{x_n}(f)(a_1,\dots,a_{n-1}) = \mathrm{lc}_{x_n}(g)(a_1,\dots,a_{n-1}) = 0$,
2. $f(a_1,\dots,a_{n-1},x_n) = 0$ or $g(a_1,\dots,a_{n-1},x_n) = 0$,
3. for some $a_n \in K$, $(a_1,\dots,a_n)$ is a common root of f and g

For a thorough introduction to resultants we refer the reader to [BrK86], [CLO98] or [Mis93].

B.4 Algebraic Sets

For any field K, the *n-dimensional affine space* over K is defined as

$$\mathbb{A}^n(K) := K^n = \{(a_1, \ldots, a_n) \mid a_i \in K\} \ .$$

$\mathbb{A}^2(K)$ is the affine plane over K. The *n-dimensional projective space* over K is defined as

$$\mathbb{P}^n(K) := \{(a_1 : \cdots : a_{n+1}) \mid (a_1, \ldots, a_{n+1}) \in K^{n+1} \setminus \{(0, \ldots, 0)\}\} \ ,$$

where $(a_1 : \cdots : a_{n+1}) = \{(\alpha a_1, \ldots, \alpha a_{n+1}) \mid \alpha \in K^\star\}$. So a point in $\mathbb{P}^n(K)$ has many representations as an $(n+1)$-tuple, since $(a_1 : \cdots : a_{n+1})$ and $(\alpha a_1 : \cdots : \alpha a_{n+1})$, for any $\alpha \in K^\star$, denote the same projective point P. $(a_1 : \ldots : a_{n+1})$ are *homogeneous coordinates* for P. $\mathbb{P}^2(K)$ is the projective plane over K.

For any ideal I in $K[x_1, \ldots, x_n]$ we denote by $V(I)$ the set of all the points in $\mathbb{A}^n(\overline{K})$, the n-dimensional affine space over the algebraic closure of K, which are common zeros of all the polynomials in I. Such sets $V(I)$ are called *algebraic sets*. In commutative algebra and algebraic geometry there is a 1–1 correspondence between radical polynomial ideals and algebraic sets, the zeros of such ideals over the algebraic closure of the field of coefficients. *Hilbert's Nullstellensatz* relates the radical of an ideal I to the set of common roots $V(I)$ of the polynomials contained in I. More precisely, the radical of I consists of exactly those polynomials in $K[x_1, \ldots, x_n]$ which vanish on all the common roots of I.

On the other hand, for any subset V of $\mathbb{A}^n(\overline{K})$ we denote by $I(V)$ the ideal of all the polynomials vanishing at V. Then for radical ideals I and algebraic sets $V(\cdot)$ and $I(\cdot)$ are inverses of each other, i.e., $V(I(V)) = V$ and $I(V(I)) = I$. This correspondence extends to operations on ideals and algebraic sets (see, for instance [CLO97], Chap. 4).

An algebraic set V is called *irreducible* if it cannot be expressed as a union of two algebraic sets, both of them different from V. In fact, V is irreducible if and only if $I(V)$ is a prime ideal. Irreducible algebraic sets are called *algebraic varieties*. In general, an algebraic set can be written uniquely as the finite union of algebraic varieties. These notions can be extended analogously to projective space.

The intersection of two algebraic sets is an algebraic set defined by the union of the two ideals. In fact, the intersection of an arbitrary number of algebraic sets is again an algebraic set. However, in general, only finite unions of algebraic sets are algebraic. The empty set is the algebraic set generated by any nonzero constant polynomial, for example 1, and the whole affine space is the algebraic set generated by the zero polynomial. Consequently, the algebraic sets are the closed sets in a topology, called the *Zariski topology*. In the Zariski topology, any two nonempty open sets have a nonempty intersection.

References

[Abh66] Abhyankar, S.S.: Resolution of Singularities of Embedded Algebraic Surfaces. Academic Press (1966)

[AbB87a] Abhyankar, S.S., Bajaj, C.L.: Automatic Parametrization of Rational Curves and Surfaces I: Conics and Conicoids. Computer Aided Geometric Design; **19**, no. 1: 11–14 (1987)

[AbB87b] Abhyankar, S.S., Bajaj, C.L.: Automatic Parametrization of Rational Curves and Surfaces II: Cubics and Cubicoids. Computer Aided Geometric Design; **19**, no. 9: 499–502 (1987)

[AbB88] Abhyankar, S.S., Bajaj, C.L.: Automatic Parametrization of Rational Curves and Surfaces III: Algebraic Plane Curves. Computer Aided Geometric Design; **5**, 390–321 (1988)

[AbB89] Abhyankar, S. S., Bajaj, C. L.: Automatic Rational Parametrization of Curves and Surfaces IV: Algebraic Space Curves. Transactions on Graphics; **8**, no. 4, 325–334 (1989)

[AdL94] Adams, W.W., Loustaunau, P.: An Introduction to Gröbner Bases. AMS, Providence, RI, Graduate studies in Mathematics; **3** (1994)

[ASS07] Alcázar, J.G., Schicho, J., Sendra, J.R.: A Delineability-based Method for Computing Critical Sets of Algebraic Surfaces. Journal of Symbolic Computation; **42**, no. 6, 678–691 (2007)

[AlS07] Alcázar, J.G., Sendra, J.R.: Local Shape of Offsets to Algebraic Curves. Journal of Symbolic Computation; **42**, no. 3, 338–351 (2007)

[AGR95] Alonso, C., Gutierrez, J., Recio, T.: Reconsidering Algorithms for Real Parametric Curves. Journal of Applicable Algebra in Engineering, Communication and Computing; **6**, 345-352 (1995)

[AnR06] Andradas, C., Recio, T.: Plotting missing points and branches of real parametric curves. Applicable Algebra in Engineering, Communication and Computing; **18(1-2)**, 107–126 (2007)

[ARS97] Andradas, C., Recio, T., Sendra, J. R.: A Relatively Optimal Rational Space Curves Reparametrization Algorithm through Canonical Divisors. Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, Kchlin W. (ed.); 349–356. ACM Press, New York (1997)

[ARS99] Andradas, C., Recio, T., Sendra, J. R.: Base Field Restriction Techniques for Parametric Curves. Proceedings of the 1999 International Symposium

on Symbolic and Algebraic Computation, Dooley S. (ed.); 17–22. ACM Press, New York (1999)

[ARS04] Andradas, C., Recio, T., Sendra, J. R.: La Variedad de Weil para Variedades Unirracionales. Book in honor of Prof. Outerelo. Editorial de la Universidad Complutense de Madrid; 33–51 (2004)

[ACFG05] Aroca, J.M., Cano, J., Feng, R., Gao, X.S.: Algebraic General Solutions of Algebraic Ordinary Differential Equations. Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation. Gutierrez J. (ed.); 29–36. ACM Press, New York (2005)

[ASS97] Arrondo, E., Sendra, J., Sendra, J.R.: Parametric Generalized Offsets to Hypersurfaces. Journal of Symbolic Computation; **23**, 267–285 (1997)

[ASS99] Arrondo, E., Sendra, J., Sendra, J.R.: Genus Formula for Generalized Offset Curves. Journal of Pure and Aplied Algebra; **136**, Issue 3, 199–209 (1999)

[BaN82] Back, J., Newman, D.J.: Complex Analysis Undergraduate Text in Mathematics. Springer-Verlag. New York (1982)

[Baj94] Bajaj, C. (ed.): Algebraic Geometry and Its Applications. Springer-Verlag, Berlin Heidelberg New York (1994)

[BaR95] Bajaj, C.L., Royappa, A.V.: Finite Representation of Real Parametric Curves and Surfaces. International Journal on Computational Geometry and Applications; **5**, no. 3, 313–326 (1995)

[BLM97] Bajaj, C., Lee, H., Merkert, R., Pascucci, V.: NURBS based B-rep Models from Macromolecules and their Properties. In Proceedings of Fourth Symposium on Solid Modeling and Applications. Atlanta,Georgia, 1997. C. Hoffmann and W. Bronsvort(ed.); 217–228. ACM Press (1997)

[BPR03] Basu, S., Pollack, R., Roy, M-F.: Algorithms in Real Algebraic Geometry. Springer-Verlag Heidelberg; Series: Algorithms and Computation in Mathematics (2003)

[BeW93] Becker, T., Weispfenning, V.: Gröbner Bases - A Computational Approach to Commutative Algebra. Springer-Verlag, Berlin, Graduate texts in Mathematics (1993)

[BiH96] Bilu, Y., Hanrot, G.: Solving the Thue Equations of High Degree. Journal of Number Theory; **60(2)**, 373–392 (1996)

[BiM79] Birkhoff, G., MacLane, S.: Algebra. 2nd Edition. Macmillan, New York (1979)

[BSS99] Blake, I., Seroussi, G., Smart, N.: Elliptic Curves in Cryptography. Cambridge Univ. Press. (1999)

[BrK86] Brieskorn, E., Knörrer, H.: Plane Algebraic Curves. Birkhäuser, Basel (1986)

[Buc65] Buchberger, B.: Ein Algorithmus Zum Baseselemente de Restklassenringen nach einen nulldimensionen Polynomideal. Ph. D. Thesis Math Ins., Univ of Innsbruk, Austria (1965)

[BCL83] Buchberger, B., Collins, G.E., Loos, R.: Computer Algebra, Symbolic and Algebraic Computation. 2nd ed., Springer-Verlag, Wien New York (1983)

[Buc01] Buchmann, J.A.: Introduction to Cryptography. Springer-Verlag (2001)

[BCD03] Busé, L., Cox, D., D'Andrea, C.: Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points. Journal of Algebra and Applications; **2**, 189–214 (2003)

[BuD06] Busé, L., D'Andrea, C.: A Matrix-Based Approach to Properness and Inversion Problems for Rational Surfaces. Applicable Algebra in Engineering, Communication and Computing; **17**, no. 6, 393–407 (2006)

[CaM91] Canny, J. F., Manocha, D.: Rational Curves with Polynomial Parametrizations. Computer Aided Design; **23**, no. 9: 645–652 (1991)
[Coh00] Cohen, H.: A Course in Computational Number Theory. GTM 138, Springer Verlag (2000)
[CLO97] Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer-Verlag, New York (1997)
[CLO98] Cox, D.A., Little, J., O'Shea, D.: Using Algebraic Geometry. Graduate Texts in Mathematics, 185. Springer–Verlag (1998)
[CoS97b] Cox, D.A., Sturmfels, B. (eds.): Applications of Computational Algebraic Geometry. Proceedings of Symposia in Applied Mathematics; **53**, AMS, Providence (1997)
[CrR03] Cremona, J.C., Rusin, D.: Efficient Solutions of Rational Conics. Math. of Computation; **72**, 1417–1441 (2003)
[ChG92a] Chionh, E.-W., Goldman, R.N.: Using multivariate resultants to find the implicit equation of a rational surface. The Visual Computer; **8**, 171–180 (1992)
[ChG92b] Chionh, E. W., Goldman, R. N.: Degree, Multiplicity and Inversion Formulas for Rational Surfaces Using u-Resultants. Computer Aided Geometric Design; **9**, no. 2, 93–109 (1992)
[CGS06] Chionh, E. W., Gao, X.S., Shen, L.Y.: Inherently improper surface parametric supports. Computer Aided Geometric Design; **23**, no. 8: 629–639 (2006)
[ChG91] Chou, S. C., Gao, X. S.: On the Normal Parametrization of Curves and Surfaces. International Journal on Computational Geometry and Applications; **1**, no. 2: 125–136 (1991)
[Duv87] Duval, D.: Diverses questions relatives au calcul formel avec des nombres algébriques (Some Questions Concerning Algebraic Numbers in Symbolic Computation). PhD Thesis, Institut Fourier, Grenoble, France (1987)
[Duv89] Duval, D.: Rational Puiseux Expansion. Compositio Mathematica; **70**, 119–154 (1989)
[Far93] Farin, G.: Curves and Surfaces for Computer Aided Geometric Design. A Practical Guide (Second Edition), Academic Press (1993)
[FHK02] Farin, G., Hoschek, J., Kim, M.–S.: Handbook of Computer Aided Geometric Design. North–Holland (2002)
[FaN90a] Farouki, R. T., Neff, C.A.: Analytic Properties of Plane Offset Curves. Computer Aided Geometric Design; **7**, 83–99 (1990)
[FaN90b] Farouki, R. T., Neff, C.A.: Algebraic Properties of Plane Offset Curves. Computer Aided Geometric Design; **7**, 100–127 (1990)
[FaS90] Farouki, R., Sakkalis, T.: Singular Points on Algebra Curves. Journal of Symbolic Computation; **9/4**, 405–421 (1990)
[FeG04] Feng, R., Gao, X.-S.: Rational General Solutions of Algebraic Ordinary Differential Equations. Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, Gutierrez J. (ed.); 155–162. ACM Press, New York (2004)
[For92] Forsman, K.: On rational state space realizations. In M. Fliess, editor. Proceeding NOLCOS'92: 197–202. Bordeaux. IFAC (1992)
[Ful89] Fulton, W.: Algebraic Curves – An Introduction to Algebraic Geometry. Addison-Wesley, Redwood City CA (1989)

[GKW91] Gebauer, R., Kalkbrener, M., Wall, B., Winkler, F.: CASA: A Computer Algebra Package for Constructive Algebraic Geometry. Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, Watt S.M (ed.); 403–410. ACM Press (1991)

[GCL92] Geddes, K.O., Czapor, S. R., Labahn, G.: Algorithms for Computer Algebra. Kluwer Academic Publishers, Boston (1992)

[GSA84] Goldman, R. N., Sederberg, T. W., Anderson, D. C.: Vector Elimination: A Technique for the Implicitization, Inversion, and a Intersection of Planar Parametric Rational Polynomial Curves. Computer Aided Design; **1**, 337–356 (1984)

[Gon97] González-Vega, L.: Implicitization of Parametric Curves and Surfaces. Journal of Symbolic Computation; **23**, 137–152 (1997)

[Gop77] Goppa, V.D.: Codes associated with divisors. Problems of Information Transmission; **12**, n.1, 22–27 (1977)

[Gop81] Goppa, V.D.: Codes on algebraic curves. Soviet Math. Dokl. (translation); 207–214 (1981)

[GMS02] Götz, R.M., Maymeskul, V., Saff, E.B.: Asymptotic Distribution of Nodes for Near-Optimal Polynomial Interpolation on Certain Curves in $\mathbb{R}^2$. Constr. Approx; **18**, 255–283 (2002)

[GuR65] Gunning, R. C., Rossi, H.: Analytic Functions of Several Complex Variables. Prentice–Hall, Inc., N.J (1965)

[Gun90] Gunning, R. C.: Introduction to Holomorphic Functions of Several Variables. CRC Press (1990)

[GuR92] Gutierrez, J., Recio, T.: Rational Function Decomposition and Gröbner Basis in the Parameterization of a Plane Curve. LATIN 92, LNCS 583; 231–246. Springer Verlag (1992)

[GRS02] Gutierrez, J., Rubio, R., Schicho, J.: Polynomial Parametrization of Curves whithout Affine Singularities. Computer Aided Geometric Design; **19**, 223–234 (2002)

[GRY02] Gutierrez, J., Rubio, R., Yu, J-T.: D-Resultant for Rational Functions. Proceedings of the American Mathematical Society; **130 (8)**, 2237–2246 (2002)

[Har95] Harris, J.: Algebraic Geometry. A First Course. Springer-Verlag (1995)

[Har01] Hartmann, E.: Parametric G^n-Blending of Curves and Surfaces. Visual Computer; **17**, 1–13 (2001)

[HHW03] Hemmecke, R., Hillgarter, E., Winkler, F.: The CASA system, in Handbook of Computer Algebra: Foundations, Applications, Systems. J. Grabmeier, E. Kaltofen, V. Weispfenning (eds.) Springer-Verlag (2003)

[HiH90] Hilbert, D., Hurwitz, A.: Über die Diophantischen Gleichungen vom Geschlecht Null. Acta math; **14**, 217–224 (1890)

[HiW98] Hillgarter, E., Winkler, F.: Points on Algebraic Curves and the Parametrization Problem. Automated Deduction in Geometry. Lecture Notes in Artif. Intell. 1360: 185–203. D. Wang (ed.). Springer Verlag Berlin Heidelberg (1998)

[Hof93] Hoffmann, C. M.: Geometric and Solid Modeling. Morgan Kaufmann Publ., Inc (1993)

[HSW97] Hoffmann, C.M., Sendra, J.R., Winkler, F. (eds.): Parametric Algebraic Curves and Applications. Special Issue on Parametric Curves and Applications of the Journal of Symbolic Computation; **23/2&3** (1997)

[HoL93] Hoschek, J., Lasser, D.: Fundamentals of Computer Aided Geometric Design. A.K. Peters, Ltd. Natick, MA, USA (1993)

[IrR82] Ireland, K., Rosen, M.: A classical introduction to modern number theory. Springer Verlag (1982)

[Jac74] Jacobson, N.: Basic Algebra I. Freeman, San Francisco (1974)
[Jac80] Jacobson, N.: Basic Algebra II. Freeman, San Francisco (1980)
[Joh98] Johnson, J.R.: Algorithms for Real Root Isolation. Quantifier Elimination and Cylindrical Algebraic Decomposition. Text and Monographs in Symbolic Computation. Springer Verlag: 269–289 (1998)
[Kiy93] Kiyosi, I. (ed.): Encyclopedic Dictionary of Mathematics. Vol. 1. Mathematical Society of Japan (1993)
[Kob98] Koblitz, N.: Algebraic Aspects of Cryptography. Springer-Verlag Berlin (1998)
[Kob02] Koblitz, N.: Good and bad uses of elliptic curves in cryptography. Moscow Math. J; **2**, n.4: 693–715 (2002)
[Kot04] Kotsireas I. S.: Panorama of Methods for Exact Implicitization of Algebraic Curves and Surfaces. Geometric Computation. Falai Chen and Dongming Wang (eds.). Lecture Notes Series on Computing; **11**, Chapter 4, World Scientific Publishing Co., Singapore (2004)
[Krä81] Krätzel, E.: Zahlentheorie. VEB Dt. Verlag der Wissenschaften (1981)
[Lan84] Lang, S.: Algebra. 2nd Edition. Addison-Wesley, Reading M.A. (1984)
[LiV00] Li, H., Van Oystaeyen, F.: A Primer of Algebraic Geometry. Marcel Dekker, New York – Basel (2000)
[LiN94] Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge, UK (1994)
[Lü95] Lü, W.: Offset-Rational Parametric Plane Curves. Computer Aided Geometric Design; **12**, 601–617 (1995)
[MPL96] Mignotte, M., Pethö, A., Lemmermeyer, F.: On the Family of Thue Equations $x^3-(n-1)x^2y-(n+2)xy^2-y^3=k$. Acta Arithm., LXXVI.3; 245–296 (1996)
[Mir99] Miranda, R.: Linear Systems of Plane Curves. Notices of AMS; **46**, no. 2: 192–201 (1999)
[Mis93] Mishra, B.: Algorithmic Algebra. Springer Verlag (1993)
[Noe83] Noether, M.: Rationale Ausführung der Operationen in der Theorie der Algebraischen Funktionen. Math. Ann; **23**, 311–358 (1883)
[Orz81] Orzech, G., Orzech, M.: Plane Algebraic Curves. An Introduction Via Valuations. Marcel Dekker, New York (1981)
[PeD06] Pérez–Díaz, S.: On the Problem of Proper Reparametrization for Rational Curves and Surfaces. Computer Aided Geometric Design; **23/4**, 307–323 (2006)
[PDS01] Pérez–Díaz, S., Sendra, J.R.: Parametric G^1-Blending of Several Surfaces. Computer Algebra in Scientific Computing CASC' 01. Lectures Notes in Computer Science. Springer Verlag, XII; 445–461 (2001)
[PDSS02] Perez-Díaz, S., Schicho, J., Sendra, J.R.: Properness and Inversion of Rational Parametrizations of Surfaces. Applicable Algebra in Engineering Communication and Computing; **13**, 29–51 (2002)
[PDS03] Pérez–Díaz, S., Sendra, J.R.: Computing All Parametric Solutions for Blending Surfaces. Journal of Symbolic Computation; **26/6**, 925–964 (2003)
[PDS04] Perez-Díaz, S., Sendra, J.R.: Computation of the Degree of Rational Surface Parametrizations. Journal of Pure and Applied Algebra; **193(1-3)**, 99–121 (2004)
[PDS05] Pérez–Díaz, S., Sendra, J.R.: Partial Degree Formulae for Rational Algebraic Surfaces. Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, Kauers M. (ed.); 301–308. ACM Press, New York (2005)

[PeP98a] Peternell, M., Pottmann, H.: Applications of Laguerre Geometric in CAGD. Computer Aided Geometric Design; **15**, 165–186 (1998)
[PeP98b] Peternell, M., Pottmann, H.: A Laguerre Geometric Approach to Rational Offsets. Computer Aided Geometric Design; **15**, 223–249 (1998)
[Pot95] Pottmann, H.: Rational Curves and Surfaces with Rational Offsets. Computer Aided Geometric Design; **12**, 175–192 (1995)
[PoW97] Pottman, H., Wallner, J.: Rational Blending Surfaces Between Quadrics. Computer Aided Geometric Design; **14**, 407–419 (1997)
[PoV00] Poulakis, D., Voskos, E.: On the Practical Solutions of Genus Zero Diophantine Equations. Journal of Symbolic Computation; **30**, 573–582 (2000)
[PoV02] Poulakis, D., Voskos, E.: Solving Genus Zero Diophantine Equations with at Most Two Infinity Valuations. Journal of Symbolic Computation; **33**, 479–491 (2002)
[Pre98] Pretzel, O.: Codes and Algebraic Curves. Oxford Univ. Press (1998)
[ReS97a] Recio, T., Sendra, J.R.: Real Reparametrizations of Real Curves. Journal of Symbolic Computation; **23**, 241–254 (1997)
[ReS97b] Recio, T., Sendra, J.R.: A Really Elementary Proof of Real Lüroth Theorem. Revista Matematica de la Universidad Complutense de Madrid; **10**, 283–291 (1997)
[RSV04] Recio, T., Sendra, J.R., Villarino, C.: From hypercircles to units. Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, Gutierrez J. (ed.); 258–265. ACM Press, New York (2004)
[Ros88] Rose, H.E.: A Course in Number Theory. Oxford Science Publications (1988)
[Rud66] Rudin, W.: Real and Complex Analysis. McGraw-Hill (1966)
[SSeS05] San Segundo, F., Sendra, J.R.: Degree Formulae for Offset Curves. Journal of Pure and Applied Algebra; **195(3)**, 301–335 (2005)
[Sch92] Schicho, J.: On the choice of pencils in the parametrization of curves. Journal of Symbolic Computation; **14**, 557–576 (1992)
[Sch98a] Schicho, J.: Rational Parametrization of Surfaces. Journal of Symbolic Computation; **26**, 1–9 (1998)
[Sch98b] Schicho, J.: Inversion of Birational Maps with Gröbner Bases. Gröbner Bases and Applications; 495–503. B. Buchberger, F. Winkler (eds.). Cambridge Univ. Press (1998)
[ScS07] Schicho, J., Sendra, J.R., (Guest editors): Special Issue of the Applicable Algebra in Engineering, Communication and Computing on Algebraic Curves; **18**, (2007).
[Sed86] Sederberg, T.W.: Improperly parametrized rational curves. Computer Aided Geometric Design; **3**, 67–75 (1986)
[Sed98] Sederberg, T. W.: Applications to Computer Aided Geometric Design. Applications of Computational Algebraic Geometry, Proceedings of Symposia in Applied Mathematics; **53**, 67–89. AMS (1998)
[SGD97] Sederberg, T.W., Goldman, R., Du, H.: Impliciticing Rational Curves by the Method of Moving Algebraic Curves. Journal of Symbolic Computation; **23**, 153–176 (1997)
[Sen02] Sendra, J. R.: Normal Parametrizations of Algebraic Plane Curves. Journal of Symbolic Computation; **33**, 863–885 (2002)

[Sen04] Sendra, J. R.: Rational Curves and Surfaces: Algorithms and Some Applications. Geometric Computation. F. Chen and D. Wang (eds.) Lecture Notes on Computing; **11**, Chapter 3, 63–125, World Scientific Publishing Co., Singapure (2004).

[SeS99] Sendra, J., Sendra, J.R.: Algebraic Analysis of Offsets to Hypersurfaces. Mathematische Zeitschrift; **234**, 697–719 (1999)

[SeS00] Sendra, J., Sendra, J.R.: Rationality Analysis and Direct Parametrization of Generalized Offsets to Quadrics. Applicable Algebra in Engineering, Communication and Computing; **11**, no. 2, 111–139 (2000)

[SeV01] Sendra, J. R., Villarino, C.: Optimal Reparametrization of Polynomial Algebraic Curves. International Journal of Computational Geometry and Applications; **11**, no. 4, 439–453 (2001)

[SeV02] Sendra, J. R., Villarino C.: Algebraically Optimal Reparametrizations of Quasi-Polynomial Algebraic Curves. Journal of Algebra and Its Applications; **1**, no. 1, 51–74 (2002)

[SeW89] Sendra, J.R., Winkler, F.: A Symbolic Algorithm for the Rational Parametrizatioin of Algebraic Plane Curves. Techn. Rep. RISC 89–41, RISC-Linz, J. Kepler Univ. Linz, Austria (1989)

[SeW91] Sendra, J.R., Winkler, F.: Symbolic Parametrization of Curves. Journal of Symbolic Computation; **12**, 607–631 (1991)

[SeW97] Sendra, J.R., Winkler, F.: Parametrization of Algebraic Curves over Optimal Field Extensions. Journal of Symbolic Computation; **23**, 191–207 (1997)

[SeW99] Sendra, J. R., Winkler, F.: Algorithms for Rational Real Algebraic Curves. Fundamenta Informaticae; **39**, no. 1–2, 211–228 (1999)

[SeW01a] Sendra, J.R., Winkler, F.: Tracing Index of Rational Curve Parametrizations. Computer Aided Geometric Design; **18**, 771–795 (2001)

[SeW01b] Sendra, J. R., Winkler, F.: Computation of the Degree of a Rational Map between Curves. Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation, Mourrain B. (ed.): 317–322. ACM Press, New York (2001)

[Sha94] Shafarevich, I.R.: Basic Algebraic Geometry I and II. Springer-Verlag, Berlin New York (1994)

[Sta00] Stadelmeyer, P.: On the Computational Complexity of Resolving Curve Singularities and Related Problems. Ph.D. thesis, RISC-Linz, J. Kepler Univ. Linz, Austria, Techn. Rep. RISC 00–31 (2000)

[TzW89] Tzanakis, N., de Weger, B.M.M.: On the Practical Solution of the Thue Equation. Journal of Number Theory; **31(2)**, 99–132 (1989)

[VaW70] van der Waerden, B.L.: Algebra I and II. Springer-Verlag, New York (1970)

[VaH94] van Hoeij, M.: Computing Parametrizations of Rational Algebraic Curves. Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation, von zur Gathen J. (ed.); 187–190. ACM Press, New York (1994)

[VaH97] van Hoeij, M.: Rational parametrization of curves using canonical divisors. Journal of Symbolic Computation; **23**, 209–227 (1997)

[vGG99] von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, New York (1999)

[Wal50] Walker, R.J.: Algebraic Curves. Princeton Univ. Press (1950)

[Win96] Winkler, F.: Polynomial Algorithms in Computer Algebra. Springer-Verlag, Wien New York (1996)

[Zar39] Zariski, O.: The reduction of singularities of algebraic surfaces. Annals of Mathematics; **40**, 639–689 (1939)

[ZaS58] Zariski, O., Samuel, P.: Commutative Algebra I, II. Springer-Verlag, New York Heidelberg Berlin (1958)

[Zip91] Zippel, R.: Rational Function Decomposition. Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, Watt S.M (ed.): 1–6. ACM Press, New York (1991)

Index

Table of Algorithms