Introduction to the Basics of Algebraic Geometry, Computational Tools and Geometric Applications

Janko Böhm
University of Saarland

17.05.2004

Abstract

This is the manuscript for a talk given in a seminar on computer aided geometric design at the University of Saarland. The aim of the talk was to introduce the basic concepts of algebraic geometry, the computational tools, i.e. resultants and Groebner bases, and their geometric applications.

Contents

1 Overview

The main topics:

- Basics of Algebra and Geometry

  Affine varieties

  Varieties defined by ideals

  Hilbert Basis Theorem

  The ideal of a variety

  Nullstellensatz

  Projection and elimination

  Some remarks on projective geometry

- Computational Tools

  Resultants

  Groebner bases

- Geometric Applications

  Implicitation and birational geometry computations

  Intersection computations

  The genus of a curve

  Parametrization of curves and surfaces

2 Basics of algebra and geometry

2.1 Affine varieties

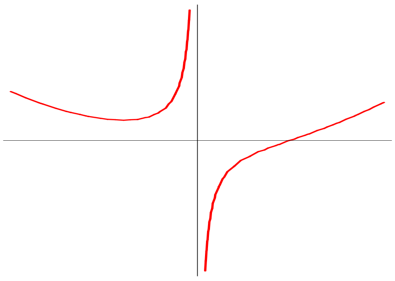
Let k be a field.

Definition 1 *An affine variety is the common zero locus of polynomials* $f_1, ..., f_r \in k[x_1, ..., x_n]$

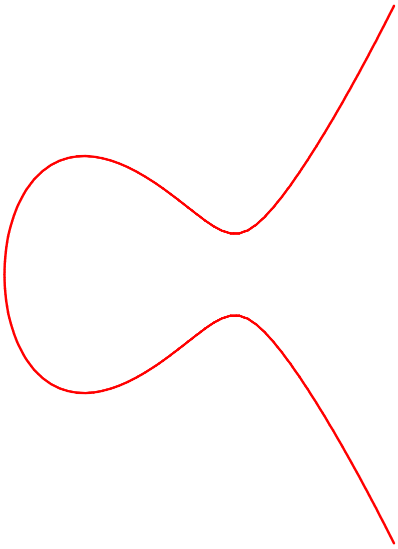
$$V(f_1, ..., f_r) = \{f_1 = 0, ..., f_r = 0\}$$

Example 2 - $V(1) = \emptyset$

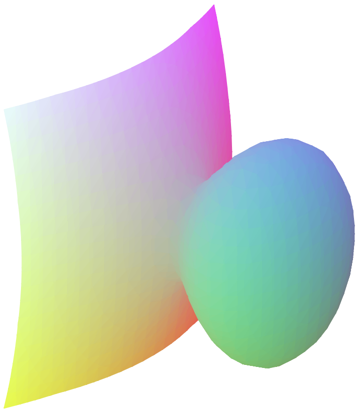
- $V(0) = k^n$
- *Linear Algebra: For linear* f_i *this is the solution space of an inhomogeneous system of linear equations. Here we know, how to decide if* $V(f_1, ..., f_r)$ *is empty and describe* $V(f_1, ..., f_r)$ *by a parametrization applying Gauss algorithm.*
- *The graph of a function: For example the graph of* $y(x) = \frac{x^3-1}{x}$*:*

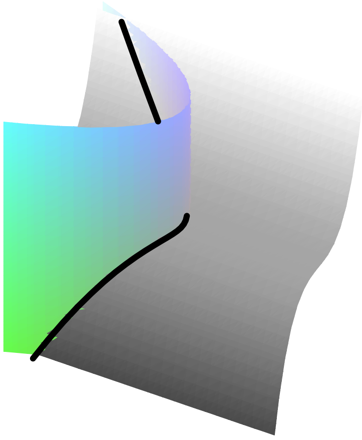
  is $V(xy - x^3 + 1)$.
- *Plane curve: Consider* $V(f)$ *for one equation in the plane, e.g.* $f = y^2 - x^3 - x^2 + 2x - 1$*:*

- *Surfaces in* k^3*: Consider* $V(g)$ *for one equation in* 3*-space (an algebraic* *set with 1 equation is called a hypersurface), e.g.* $g = f - z + z^2$.



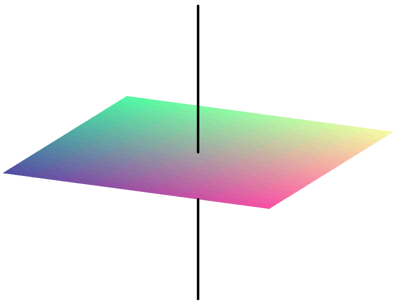
- *Twisted cubic: Consider the curve* $C = V(y - x^2, z - x^3) \subset k^3$ *given by 2 equations in 3-space.*



- *There are also strange examples, e.g.*

$$V(xz, yz) = V(z) \cup V(x, y)$$

decomposes into the $x - y$*-plane* $V(z)$ *and the* z*-axis* $V(x, y)$



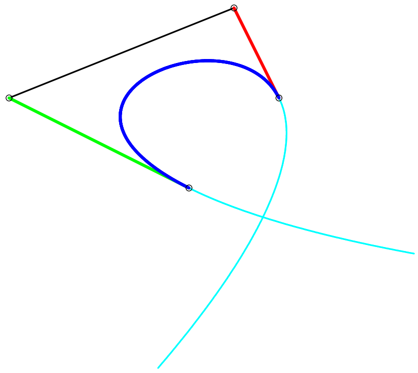
Varieties, which do not admit a further decomposition are called irreducible, otherwise reducible.

Example 3 *Consider the following sets given by parametrizations:*

- *Bezier spline: The curve $C \subset k^2$ parametrized by*

$$X(t) = x_0(1-t)^3 + 3x_1t(1-t)^2 + 3x_2t^2(1-t) + x_3t^3$$
$$Y(t) = y_0(1-t)^3 + 3y_1t(1-t)^2 + 3y_2t^2(1-t) + y_3t^3$$

with $t \in k$ goes through the points $(x_0, y_0), (x_3, y_3) \in k^2$ and the tangent lines at these points go through (x_1, y_1) resp. (x_2, y_2)

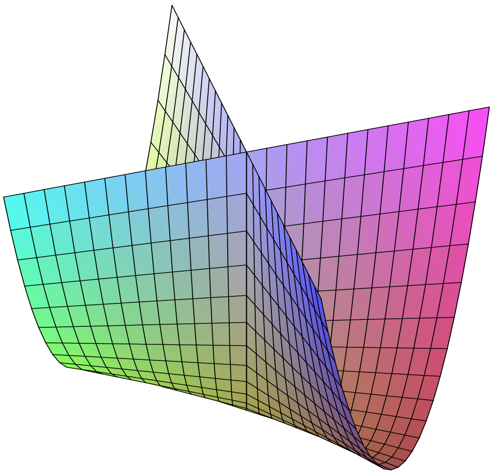


See for example the standard vector graphics programs.

- *Whitney umbrella: The surface $S \subset k^3$ given by the parametrization*

$$X(s,t) = s \cdot t$$
$$Y(s,t) = s$$
$$Z(s,t) = t^2$$

with $(s,t) \in k^2$.



C and S are also varieties. To see this, we have to describe them by implicit equations, i.e. as $V\left(f_1,...,f_r\right)$. Techniques to do this will be one of the topics. The implicit description would allow us for example to check easily, if a given point lies on the variety.

2.2 Varieties defined by ideals

First recall, that an ideal $I \subset R$ inside a ring R is an additive subgroup of R s.t. R-multiples of elements in I again lie inside of I.

An important observation is, that the common zeroset of polynomials $f_1,...,f_r$ only depends on the ideal $I = \langle f_1,...,f_r\rangle \subset k\left[x_1,...,x_n\right]$ generated by $f_1,...,f_r$. The reason is, that if $f_1\left(p\right) = 0,...,f_r\left(p\right) = 0$ any polynomial linear combination also vanishes in p:

$$\sum_{i=1}^{r} s_i\left(p\right)\overbrace{f_i\left(p\right)}^{=0} = 0$$

for all $s_i \in k\left[x_1,...,x_n\right]$. Hence any different set of generators of I gives the same zeroset and we should define:

Definition 4 *For an ideal $I \subset k\left[x_1,...,x_n\right]$ we define*

$$V\left(I\right) = \left\{x \in k^n \mid f\left(x\right) = 0 \forall f \in I\right\}$$

Example 5 *Consider $I = \langle f_1, f_2\rangle$ with*

$$\begin{aligned} f_1 &= 2x^2 - 3y^2 + 10 \\ f_2 &= 3x^2 - y^2 + 1 \end{aligned}$$

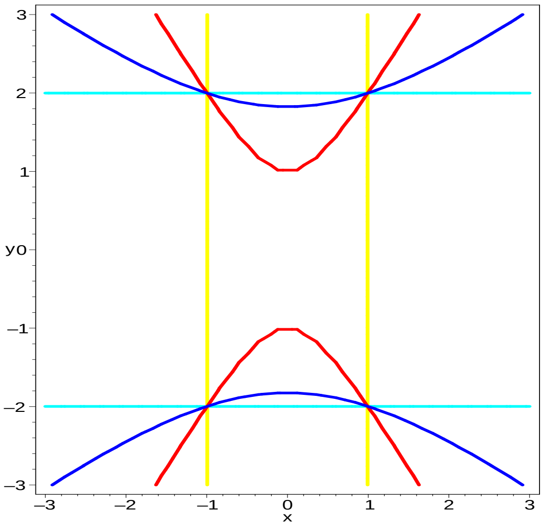
Gaussian elimination applied to the linear system of equations

$$\begin{aligned} 2X - 3Y + 10 &= 0 \\ 3X - Y + 1 &= 0 \end{aligned}$$

shows that

$$I = \left\langle x^2 - 1, y^2 - 4\right\rangle$$

hence $V(I) = \{(1,2), (-1,2), (1,-2), (-1,-2)\}$ *consists of* 4 *points.*



The definition of $V(I)$ naturally raises the question, whether any ideal in $k[x_1, ..., x_n]$ has a finite set of generators, hence any $V(I) = V(f_1, ..., f_r)$ with some $f_1, ..., f_r \in k[x_1, ..., x_n]$. This is answered by the Hilbert Basis Theorem:

2.3 Hilbert Basis Theorem

In $k[x]$ (principal ideal domain) every ideal has a **single generator**, which one can find by successively using the Euclidian algorithm to compute the gcd. What about polynomials in several variables?

Definition 6 *A ring R is called **Noetherian**, if **every ideal is finitely generated** or equivalently if R contains no infinitely properly ascending chain of ideals*

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq ...$$

(Exercise: recall the proof of the equivalence from your algebra lecture). You can imagine the analogous definition for modules.

Theorem 7 (Hilbert Basis Theorem) *If R is Noetherian then so is $R[x]$.*

We skip the

Proof. Let $I \subset R[x]$ an ideal. The set of lead coefficients of I generate an ideal $L \subset R$ which is finitely generated by some $g_1, ..., g_r \in R$ since R is Noetherian. By definition for each g_i there is an $m_i \in \mathbb{N}_0$ s.t.

$$I \ni f_i = g_i x^{m_i} + \text{lower order terms}$$

and let $J = \langle f_1, ..., f_r \rangle \subset R[x]$ and $m = \max\{m_1, ..., m_r\}$. Modulo the generators of J we can reduce the degree of elements of I to degree $< m$. The R-module M generated by $1, x, ..., x^{m-1}$ is finitely generated hence also $M \cap I$ is finitely generated by some $h_1, ..., h_l \in R[x]$ and $I = \langle f_1, ..., f_r, h_1, ..., h_l \rangle$.

2.4 The ideal of a variety

Given an ideal I, we formed the set of common zeros $V(I)$ of the elements of I. Conversely given some set $S \subset k^n$, we can consider the set of **polynomials** $I(S)$ **vanishing on** S, which is indeed an ideal (exercise: prove this).

Definition 8 *For $S \subset k^n$ let $I(S) = \{f \in k[x_1, ..., x_n] \mid f(x) = 0 \forall x \in S\}$.*

Obviously it holds, that

Remark 9 $J_1 \subset J_2 \Rightarrow V(J_2) \subset V(J_1)$
$S_1 \subset S_2 \Rightarrow I(S_2) \subset I(S_1)$

So one can start to study a given variety by studying the hypersurfaces, in which it is contained $V(J) \subset V(f)$ e.g. the twisted cubic lies inside $V(y - x^2)$ and $V(z - x^3)$. By the above correspondence this naturally leads to the **ideal membership problem**: Given an ideal $J \subset R$ check, if a given $f \in R$ lies inside J. For $k[x]$ this is solved by the division with remainder with respect to the single generator of J (found by the Euclidian algorithm).

How do the two processes forming $I(S)$ and $V(J)$ relate to each other? One could expect, that $J = I(V(J))$ for any ideal J, but this is not true: Consider for example the ideal $J = \langle x^2 \rangle \subset k[x]$, where $V(J) = \{0\} \subset k$, so $I(V(J)) = \langle x \rangle$. At least we can note, that if $f \in J$ and $p \in V(J)$, then $f(p) = 0$ so $f \in I(V(J))$, i.e.

Remark 10 *For every ideal J*

$$J \subset I(V(J))$$

What about the relation the other way around? Since every polynomial in $I(S)$ is vanishing on S, we note:

Remark 11 *For any set $S \subset k^n$*

$$S \subset V(I(S))$$

If $S = V(J)$ we can get the other inclusion by applying V to $J \subset I(V(J))$, hence

Remark 12 *If S is a variety i.e. $S = V(J)$ for some ideal J, then $S = V(I(S))$.*

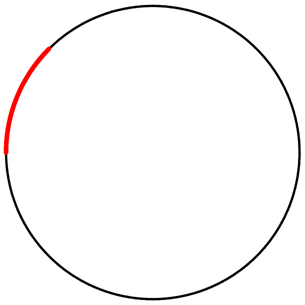
By playing with V and I you can easily check:

Remark 13 *$V(I(S))$ is the smallest variety containing S.*

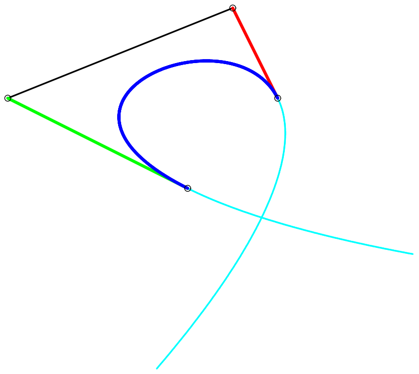
(If S is any set and $V(J)$ some variety with $S \subset V(J) \subset V(I(S))$ then $I(V(J)) \subset I(S)$ so $V(I(S)) \subset V(I(V(J))) = V(J) \subset V(I(S))$ so $V(I(S)) = V(J)$).

Example 14 *Take $S = \{(x,0) \in \mathbb{R}^2 \mid 0 < x < 1\}$. Then $I(S) = \langle y \rangle$ and $V(I(S))$ is the whole x-axis.*

For a small part S of a circle $V(I(S))$ gives the whole circle



The blue + cyan part is $V(I(S))$ for the blue Bezier spline S:



If you know about topology, then note, that we can consider $V(I(S))$ as the closure of S in a suitable topology, the **Zariski topology**. You can imagine, that as the closed sets we should take the affine varieties. To check, that this indeed defines an topology one has to check that $\emptyset, k^n$ are affine varieties and finite unions and infinite intersections of varieties are again varieties. So you should prove the following remark (and also keep in mind that the polynomial ring is Noetherian):

Given two ideals J_1 and J_2 we can form the sum $J_1 + J_2$, product $J_1 \cdot J_2$ and intersection $J_1 \cap J_2$, where

$$J_1 + J_2 = \{f_1 + f_2 \mid f_i \in J_i\} \quad J_1 \cdot J_2 = \langle f_1 \cdot f_2 \mid f_i \in J_i \rangle$$

Remark 15 *The vanishing loci are*

$$\begin{aligned} V(J_1 + J_2) &= V(J_1) \cap V(J_2) \\ V(J_1 \cdot J_2) &= V(J_1 \cap J_2) = V(J_1) \cup V(J_2) \end{aligned}$$

so unions and intersections of varieties are again varieties.

(Exercise: prove this).

Example 16 *With* $J_1 = \langle y - x^2 \rangle$ *and* $J_2 = \langle z - x^3 \rangle$ *the twisted cubic given by* $J_1 + J_2$ *is the intersection of* $V(J_1)$, $V(J_2)$.

Definition 17 $\mathbb{A}^n(k)$ *is* k^n *together with the Zariski topology.*

Working with affine varieties, it is natural to ask, what kind of maps we should consider between them. The good maps with respect to the Zariski topology are the ones (locally) given by polynomials. Given a variety $S \subset k^n$ any polynomial function on k^n induces a polynomial function on X and two such functions f_1, f_2 are identical, iff $f_1 - f_2 \in I(S)$ so the **polynomial functions** on S are the elements of the **coordinate ring**

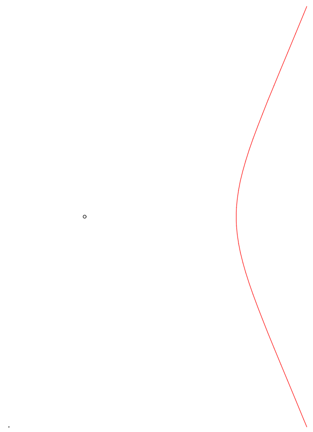
$$k[x_1, ..., x_n] / I(S)$$

Example 18 *Consider the map (parametrization)*

$$\begin{aligned} \varphi : \quad & \mathbb{A}^1(\mathbb{R}) \to \mathbb{A}^2(\mathbb{R}) \\ & t \mapsto (t^2 + 1, t^3 + t) \end{aligned}$$

and let $C = image(\varphi)$.*Then* $I(C) = \langle y^2 - x^3 - x^2 \rangle$ *(you can easily check the inclusion* $\supset$ *by substituting the parametrization into the equation). We observe, that* $(0,0) \in V(I(C))$ *but* $(0,0) \notin C$. *Actually one can prove, that*

$$\overline{C} = V(I(C)) = C \cup \{(0,0)\}$$



2.5 The Nullstellensatz

If $1 \in J$ then $V(J) = \emptyset$ (In $k[x]$ we can check $1 \in J$ easily by computing the single generator of J). What about the converse? In general this is false, e.g. consider $V(x^2+1) \subset \mathbb{A}^1(\mathbb{R})$, but if k is algebraically closed, then it is true (since any polynomial decomposes in linear factors). It turns out to be true also in polynomial rings with more than one variable:

Theorem 19 (Week Nullstellensatz) *For $J \subset k[x_1, ..., x_n]$ an ideal it holds: If $k = \overline{k}$ and $V(J) = \emptyset$ then $1 \in J$.*

(Without proof). This says, that any system of equations generating an ideal strictly smaller that $k[x_1, ..., x_n]$ has a common zero. So you can consider it as the fundamental theorem of algebra in several variables.

Definition 20 *For an ideal J the radical ideal is*

$$\sqrt{J} = \{f \in R \mid \exists n : f^n \in J\}$$

Example 21 $\sqrt{\langle x^2(x-1)\rangle} = \langle x(x-1)\rangle$. *So think of the radical as making multiple zeros to zeros of order* 1.

Remark 22 $\sqrt{J} \subset I(V(J))$ *and* $V(J) = V\left(\sqrt{J}\right)$.

Proof. If $f \in \sqrt{J}$ i.e. $f^m \in J$ so $f^m(p) = 0$ $\forall p \in V(J)$, hence $f(p) = 0$ $\forall p \in V(J)$, i.e. $f \in I(V(J))$.

If we apply V to the inclusion $\sqrt{J} \subset I(V(J))$ we get $V(J) = V(I(V(J))) \subset V\left(\sqrt{J}\right)$.

For the other inclusion apply V to $J \subset \sqrt{J}$ and get $V\left(\sqrt{J}\right) \subset V(J)$.

Theorem 23 (Strong Nullstellensatz) *For $J \subset k[x_1, ..., x_n]$ it holds: If $k = \overline{k}$ then*

$$I(V(J)) = \sqrt{J}$$

We skip the

Proof. (Trick of Rabinovich) Take generators of J

$$J = \langle f_1, ..., f_s \rangle$$

and let $f \in I(V(J))$. Then for $L = \langle J, yf - 1 \rangle \subset k[x_1, ..., x_n, y]$ we have $V(L) = \emptyset$ (since for all $p \in V(J)$ we get $yf(p) - 1 = -1 \neq 0$), hence by the weak Nullstellensatz there are a_i and b, such that

$$\sum_i a_i f_i + b(1 - yf) = 1$$

in particular for $y = \frac{1}{f}$ and multiplying by a high enough power of f we get $f^m \in J$.

2.6 Projection and elimination

In linear algebra Gauss algorithm parametrizes the solution space of a linear system of equations by a coordinate space. This can be viewed as the projection of the solution space. Solving nonlinear systems of equations we also can apply projection.

For any ideal $I \subset R = k[x_1, ..., x_n]$ we consider the elimination ideal

$$I_m = I \cap k[x_{m+1}, ..., x_n]$$

and the projection

$$\begin{array}{ll} \pi_m : & \mathbb{A}^n(k) \to \mathbb{A}^{n-m}(k) \\ & \pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n) \end{array}$$

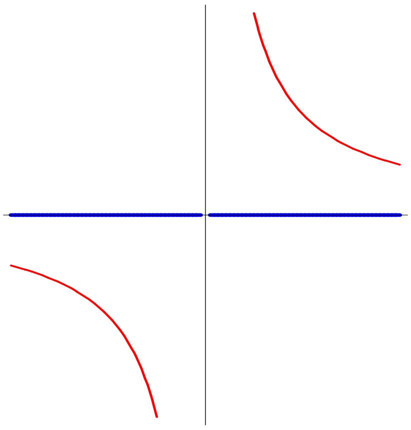
Example 24 *Consider*

$$\begin{array}{l} I = \left\langle x^2 - 1, y^2 - 4 \right\rangle \\ S = V(I) = \{(1,2), (-1,2), (1,-2), (-1,-2)\} \end{array}$$

then $\pi_1(S) = \{-2, 2\}$ and $I_1 = \langle y^2 - 4 \rangle$.

So what do you think is the relation between them?

Example 25 *If S is some variety, then in general the projection is not a variety, e.g. for the hyperbola $S = V(xy - 1)$ we have $\pi_1(S) = \mathbb{A}^1(k) \setminus \{0\}$*



hence the right question is, how to describe the Zariski closure of the projection:

Theorem 26 *If $k = \overline{k}$ then*

$$\overline{\pi_m(V(I))} = V(I_m)$$

Proof. For any $(a_{m+1}, ..., a_n) = \pi_m(a_1, ..., a_n) \in \pi_m(V(I))$ we observe that

$$0 = f(a_1, ..., a_n) = f(a_{m+1}, ..., a_n) \text{ for all } f \in I_m$$

(since $f \in I$), hence $\pi_m(V(I)) \subset V(I_m)$. $V(I_m)$ being closed, this also holds for the closure.

Any $g \in I(\pi_m(V(I))) \subset k[x_{m+1}, ..., x_n]$ can be considered as an element of $k[x_1, ..., x_n]$ and vanishes on $V(I)$ so by the Nullstellensatz $\exists m : g^m \in I$, but then $g^m \in I \cap k[x_{m+1}, ..., x_n] = I_m$ i.e. $I(\pi_m(V(I))) \subset \sqrt{I_m} = I(V(I_m))$ hence applying V

$$V(I_m) = V(I(V(I_m))) \subset V(I(\pi_m(V(I)))) = \overline{\pi_m(V(I))}$$

We will see soon, how to compute I_m.

2.7 Some remarks on projective geometry

2.7.1 Projective space and projective varieties

In affine space $\mathbb{A}^2(k)$ we expect two lines to meet in one point, but there are special pairs of lines, for which this does not hold, namely two parallel lines. We fix this problem by the following:

We define the projective n-space $\mathbb{P}^n(k)$ over k as

$$\mathbb{P}^n(k) = \mathbb{A}^{n+1}(k) / \sim$$

with $(a_0, ..., a_n) \sim (b_0, ..., b_n) \Leftrightarrow \exists \lambda \in k^*$ with $(a_0, ..., a_n) = \lambda (b_0, ..., b_n)$ and denote the equivalence classes by $(a_0 : ... : a_n)$. So we identify all points lying on the same line through $(0, ..., 0)$.

Example 27 *We can think of $\mathbb{P}^2(\mathbb{R})$ as the half sphere with opposite points on the boundary identified. We observe, that $\mathbb{P}^2(\mathbb{R}) = \mathbb{A}^2(\mathbb{R}) \cup \mathbb{P}^1(\mathbb{R})$ is the union of $\mathbb{A}^2(\mathbb{R})$ with the line at infinity $\mathbb{P}^1(\mathbb{R})$ by stereographic projection.*

So how to define varieties in projective space? All points on lines through the origin of $\mathbb{A}^{n+1}(k)$ are identified, so we have to define varieties by polynomials, which satisfy

$$f(p) = 0 \Rightarrow f(\lambda p) = 0 \text{ for all } \lambda$$

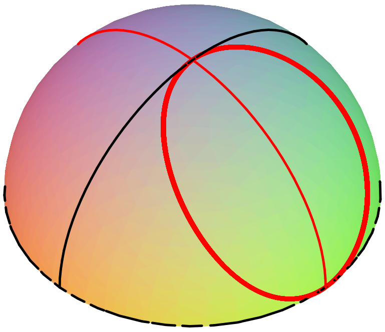
If k is infinite, this is equivalent to f being homogeneous, i.e. all monomials in f have the same degree. For example $x^2y + xy^2$ is homogeneous, but $x^2y + xy$ is not. In terms of ideals we should consider homogeneous ideals, i.e. ideals which have homogenous generators. One of the reasons, why considering projective space is:

2.7.2 The Theorem of Bezout

Theorem 28 *If k is algebraically closed and $f, g \in k[x, y, z]$ are homogeneous of degrees d and e with no common factor, then the curves $C_1 = V(f)$ and $C_2 = V(g)$ intersect in $d \cdot e$ points, counted with multiplicity.*

Example 29 *The lines $L_1 = V(x)$ and $L_2 = V(x - z)$ in $\mathbb{P}^2$ meet at the point $(0 : 1 : 0)$ since $x = 0$ and $z = 0$.*

The line $L_1 = V(x)$ and the parabola $C = V(yz - x^2)$ meet at $(0:0:1)$ and $(0:1:0)$.



The line $L_2 = V(y)$ and the parabola C meet in $(0:0:1)$ with multiplicity 2, as the parabola is tangent to L_2.

3 Computational tools

Working with varieties, the two key computational tools are resultants (fast, applicable in special situations) and Groebner bases (the universal tool).

3.1 Resultants

Resultants are used to solve systems of polynomial equations and determine, whether or not a solution exists. They produce elements in the elimination ideals. We first give some results in $K[x]$, keeping in mind, that we can take $K = k(x_2, ..., x_n)$ as the field .

Given $f, g \in K[x]$ of positive degree $l = \deg f$ and $m = \deg g$, write $f = \sum_{i=0}^{l} f_{l-i} x^i$ and $g = \sum_{i=0}^{m} g_{m-i} x^i$. If f and g have a common factor h of nonzero degree i.e. $f = f_1 h$ and $g = g_1 h$ then with $A = g_1$ and $B = -f_1$ we get

$$Af + Bg = 0 \text{ with } \deg A \leq m - 1 \text{ and } \deg B \leq l - 1$$

Conversely given this, assume $B \neq 0$ and f and g do not have a common factor of positive degree. The extended Euclidian algorithm gives $a, b \in K[x]$ with $af + bg = 1$ so

$$B = Baf + Bbg = (Ba - bA) f$$

i.e. $\deg B \geq l$ a contradiction. So we proved:

Proposition 30 *For $f, g \in K[x]$ of positive degree $\deg f = l$ and $\deg g = m$ it is equivalent:*

1. *f and g have a common factor of positive degree.*

2. *There are $0 \neq A, B \in K[x]$ with $Af + Bg = 0$ with $\deg A \leq m - 1$ and $\deg B \leq l - 1$.*

The equation $Af + Bg = 0$ is equivalent to the linear system of equations in the coefficients of $A = \sum_{i=0}^{m-1} a_{m-i-1} x^i$ and $B = \sum_{i=0}^{l-1} b_{l-i-1} x^i$

$$\operatorname{Syl}(f, g, x) \cdot \begin{pmatrix} a_0 \\ \vdots \\ b_{l-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

with some matrix $\operatorname{Syl}(f, g, x)$ called the Sylvester matrix

$$\operatorname{Syl}(f, g, x) = \begin{pmatrix} f_0 & & & g_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ f_l & & f_0 & g_m & & g_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & f_l & & & g_m \end{pmatrix}$$

e.g. the coefficient of the lead term x^{l+m-1} is given by $f_0 a_0 + g_0 b_0$ and the constant coefficient is given by $f_l a_{m-1} + g_m b_{l-1}$.

So defining the Sylvester resultant $\operatorname{Res}(f, g, x) = \det \operatorname{Syl}(f, g, x)$ we get:

Proposition 31 *For $f, g \in K[x]$ of positive degree $\deg f = l$ and $\deg g = m$ it is equivalent:*

1. *f and g have a common factor of positive degree.*

2. *There are $0 \neq A, B \in K[x]$ with $Af + Bg = 0$ with $\deg A \leq m - 1$ and $\deg B \leq l - 1$.*

3. $\operatorname{Res}(f, g, x) = 0$.

Furthermore there are $A, B \in K[x]$ polynomial expressions in the coefficients of f and g with $Af + Bg = \operatorname{Res}(f, g, x)$.

For the second part we modify the right hand side of linear system of equations in the proof $2 \Leftrightarrow 3$.

Given $f, g \in k[x_1, ..., x_n]$ of positive degree in x_1, we can compute the resultant $\operatorname{Res}(f, g, x_1) \in k[x_2, ..., x_n]$ by computing in $k(x_2, ..., x_n)[x_1]$ and noting, that we do not have to invert coefficients in the course of the computation.

Proposition 32 *For $f, g \in R = k[x_1, ..., x_n]$ and $I = \langle f, g \rangle$, we get*

1. $\operatorname{Res}(f, g, x_1) \in I_1 = I \cap k[x_2, ..., x_n]$ *is in the first elimination ideal.*
2. $\operatorname{Res}(f, g, x_1) = 0 \Leftrightarrow f$ *and g have a common factor of positive degree.*

Proof.

1. We can write $\operatorname{Res}(f, g, x_1) = Af + Bg$ with $A, B \in R$ and $\operatorname{Res}(f, g, x_1)$ is an integer polynomial in the coefficients of f, g with respect to x_1.
2. We note by above Proposition and Gauss theorem

$$\begin{aligned}&\operatorname{Res}(f, g, x_1) = 0\\ &\Leftrightarrow f, g \text{ have common factor of positive degree in } k(x_2, ..., x_n)[x_1]\\ &\Leftrightarrow f, g \text{ have common factor of positive degree in } k[x_2, ..., x_n][x_1]\end{aligned}$$

Example 33 *Consider $I = \langle f_1, f_2 \rangle$ with*

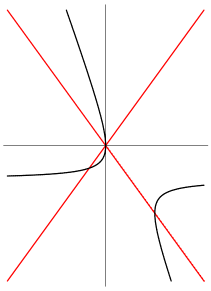
$$\begin{aligned}f_1 &= x + 2xy + y^2\\ f_2 &= x^2 - y^2\end{aligned}$$

so

$$\operatorname{Res}(f_1, f_2, y) = \det \operatorname{Syl}(f_1, f_2, y) = \det \begin{pmatrix} 1 & 0 & -1 & 0 \\ 2x & 1 & 0 & -1 \\ x & 2x & x^2 & 0 \\ 0 & x & 0 & x^2 \end{pmatrix} = -x^2(x-1)(3x+1)$$

i.e. the x-coordinates of the solutions have to satisfy this equation. Inserting $x_1 = 0$, $x_2 = 1$ and $x_3 = -\frac{1}{3}$ in f_2 gives $y_1 = 0$, $y_2 = \pm 1$ and $y_3 = \pm\frac{1}{3}$. Checking these tuples with f_1 gives the solutions

$$(x, y) = (0, 0), (1, -1), \left(-\frac{1}{3}, -\frac{1}{3}\right)$$



3.2 Groebner bases

Now we will consider the algorithm, which allows us to do the computations in polynomial rings, e.g. treat the ideal membership problem. In the case of $k[x]$ we can find the generator of an ideal applying the Euclidian algorithm and check ideal membership using division with remainder. Here we sucessively divide by the lead term of generator. The lead term is given by ordering the monomials with respect to the degree.

Example 34 *Test if* $V(x^2+x+1) \subset V(x^4+x^2+1)$*:*

$$\begin{array}{ll} (x^4+x^2+1) : (x^2+x+1) & = x^2 - x + 1 \\ x^4+x^3+x^2 & \\ \hline \quad -x^3+1 & \\ \quad -x^3-x^2-x & \\ \hline \qquad\quad x^2+x+1 & \end{array}$$

so the remainder is zero, hence the answer is yes.

In the multivariate case we do not know, how to find the lead term (e.g. consider $xy^2 + x^2y$) to do a division algorithm and then the analogue of the Euclidian algorithm. So we need:

Definition 35 (monomial order) *To any monomial* $x^\alpha = x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$ *we can associate the exponent vector* $\alpha = (\alpha_1, ..., \alpha_n)$*. A monomial order is a total ordering* $>$ *on the set of exponent vectors (here total means: for any* 2 *elements it holds* $\alpha < \beta$, $\alpha = \beta$ *or* $\alpha > \beta$*) with the following properties:*

1. *Multiplication of monomials is respected i.e. for all* γ *we have* $\alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$*.*
2. *Any nonempty set has a smallest element.*

There are various monomial orders. Here we will only consider

Example 36 (Lexicographic order) $\alpha > \beta \Leftrightarrow$ *the leftmost nonzero entry of* $\alpha - \beta$ *is positive.*

For example in $k[x, y, z]$

$$\begin{aligned} x = (1,0,0) > y &= (0,1,0) > z = (0,0,1) \\ xy^2 &= (1,2,0) > (0,3,4) = y^3z^4 \\ x^3y^2z^4 &= (3,2,4) > (3,2,1) = x^3y^2z \end{aligned}$$

With respect to a given monomial ordering, for any polynomial f we denote by $in(f)$ the largest monomial appearing in f and by $lt(f)$ the corresponding term in f (i.e. the product of $in(f)$ by its coefficient).

Algorithm 37 (Division with remainder) *Given $f \in R = k[x_0, ..., x_n]$ and $g_1, ..., g_m \in R$ we can write*

$$f = \sum a_i g_i + r$$

where no monomial of r is divisible by any $in(g_i)$ by the following algorithm:

```
a=(0..0);remainder=0;

while f!=0 do (
    if exist i with in(g#i) divides in(f) then (
        c=lt(f)/lt(g#i);
        a#i=a#i+c;f=f-c*g#i;
    ) else (
        remainder=remainder+lt(f);
        f=f-lt(f);
    );
);
```

The process terminates, since in every step the initial term decreases and this has to stop, since every set of monomials has a smallest element. Note, that in general in any step we have different possible choices of i such that $in(f_i)$ divides the initial term, hence the output is not unique.

Example 38 *Using lex divide $x^2y + xy^2 + y^2$ by $xy - 1$ and $y^2 - 1$.*

$$\begin{array}{ll}
\boxed{x^2y} + xy^2 + y^2 = & x(xy-1) + y(xy-1) + x + 1(y^2-1) + y + 1 \\
x^2y - x & \\
\cline{1-1}
\boxed{xy^2} + x + y^2 & \\
xy^2 - y & \\
\cline{1-1}
\boxed{x} + y^2 + y & \\
\cline{1-1}
y^2 + y & \\
y^2 - 1 & \\
\cline{1-1}
y + 1 &
\end{array}$$

Note, that unlike in the one variable case, we have to put terms into the remainder also in the intermediate steps.

Using lex we divide $x^2 - y^2$ by $x^2 + y$ and $xy + x$:

$$\begin{array}{ll}
\boxed{x^2} - y^2 = & 1(x^2+y) + (-y^2 - y) \\
x^2 + y & \\
\cline{1-1}
-y^2 - y &
\end{array}$$

This seems to be nonsense, as

$$x^2 - y^2 = -y\left(x^2+y\right) + x\left(xy+x\right)$$

so $x^2 - y^2 \in \langle x^2+y, xy+x\rangle$ and the division algorithm does not return 0. The problem lies in the fact, that in this equation the two lead terms cancel. So we can repair the situation by adding all polynomials to the list of divisors, which we can build by cancelling lead terms between divisors. This leads to the notion of a Groebner basis of an ideal:

Definition 39 *$g_1, ..., g_r \in I$ are called a Groebner basis of I if $in\left(g_1\right), ..., in\left(g_r\right)$ generate the ideal generated by all initial monomials of elements in I.*

Remark 40 (Ideal membership) *If $g_1, ..., g_r$ is a Groebner basis of I then $f \in I$ iff division by $g_1, ..., g_r$ gives 0.*

Proof. If $f \in I$ then division with remainder gives

$$f = \sum a_i g_i + r$$

where no monomial of r is divisible by any $in\left(g_i\right)$. Since $r \in I$ and $g_1, ..., g_r$ is a Groebner basis $in\left(r\right) \in \langle in\left(g_1\right), ..., in\left(g_r\right)\rangle$ so there is an i such that $in\left(g_i\right) \mid in\left(r\right)$ hence $r = 0$.

In the example a Groebner basis of $I = \langle x^2+y, xy+x\rangle$ is given by

$$G = \left\{y^2+y, x^2+y, xy+x\right\}$$

Since we can obtain x^2-y^2 by cancelling lead terms and division of x^2-y^2 by x^2+y and $xy+x$ yields $-y^2-y$, this element has to be contained in the Groebner basis. We need a criterion telling us, at which point we have reached a Groebner basis:

Given two polynomials the syzygy pair cancels the lead terms:

Definition 41 (Syzygy polynomial) *For $f, g \in R$ the syzygy polynomial is*

$$S\left(f,g\right) = \frac{\operatorname{lcm}\left(in\left(f\right), in\left(g\right)\right)}{lt\left(f\right)} f - \frac{\operatorname{lcm}\left(in\left(f\right), in\left(g\right)\right)}{lt\left(g\right)} g$$

Theorem 42 *$g_1, ..., g_r \in I$ are a Groebner basis iff $S\left(g_i, g_j\right)$ divided by $g_1, ..., g_r$ is zero for all i, j.*

Proof. $\Rightarrow$: $S(g_i, g_j) \in I$ so see the remark on the ideal membership question.

$\Leftarrow$: Let $f \in I$. Since all syzygy polynomials reduce to 0 modulo $g_1, ..., g_r$ we can write

$$f = \sum_i a_i g_i$$

We have to show, that $in(f) \in \langle in(g_1), ..., in(g_r)\rangle$. If $in(f) = in(a_i g_i)$ then this is the case, otherwise in the sum $\sum_i a_i g_i$ some lead terms cancel. In this case by assumtion we can replace any syzygy pair in the sum by an R-combination of $g_1, ..., g_r$.

Exercise: Use the theorem to check in the above example, that G is indeed a Groebner basis.

Algorithm 43 (Buchberger) *By the above theorem the following algorithm computes a Groebner basis:*

```
G={g1,...,gr};
repeat (
    G'=G;
    for all tuples p,q in G do (
        S=divide(S(p,q),G);
        if S!=0 then G=append(G,S);
    );
) until G'==G;
```

By Noetherian property of R the algorithm terminates.

Example 44 *In $k[t, z, y, x]$ with respect to the lexicographic order $t > z > y > x$ we compute a Groebner basis of*

$$I = \left\langle t^2 - x, t^3 - y, t^4 - z\right\rangle$$

In each step the first column denotes the coefficients of the syzygy polynomial and the second the division with remainder:

	↱	$-tx + y$	↱	$-t^2x + z$	↱	$-ty + z$	↱	$t^3y - zx$
$t^2 - x$	t		t^2	x				ty
$t^3 - y$	1				t			
$t^4 - z$			1		1		x	
$-tx + y$		1					$-t^3$	$-y$
$z - x^2$				1		1		$-x$
$-ty + x^2$						1		
$y^2 - x^3$								1

You can check as an exercise, that all other syzygy polynomials reduce to 0.

Hence a Groebner basis of I *is given by* $y^2-x^3, z-x^2, tx-y, ty-x^2, t^2-x$.

Note, that we can do not need t^3-y *and* t^4-z*, since they appear in a syzygy polynomial with coefficient* 1 *and by this get a Groebner basis, which is minimal with respect to the following notation:*

Definition 45 *A Groebner basis* $g_1,...,g_r$ *is called minimal, if removing a generator from* $\langle in(g_1), ..., in(g_r)\rangle$ *gives a strictly smaller ideal.*

4 Geometric Applications

4.1 Implicitation and birational geometry computations

Computing I_m with Groebner bases:

Theorem 46 *If* $G=\{g_1,...,g_r\}$ *is a Groebner basis of* $I\subset R$ *with respect to lex, then*

$$G_m := G\cap k[x_{m+1},...,x_n]$$

is a Groebner basis of $I_m\subset k[x_{m+1},...,x_n]$ *with respect to lex.*

Proof. We first show $I_m=\langle G_m\rangle$:

Obviously $G_m\subset I_m$. On the other hand take $f\in I_m\subset I$ and do division with remainder by $g_1,...,g_r$. In the first step

$$f=a_{j1}g_{j_1}+r_1$$

with $in(g_{j_1}) \mid in(f)$ so $in(g_{j_1})\in k[x_{m+1},...,x_n]$. Any term containing $x_1,...,x_m$ would be bigger than $in(g_{j_1})$ in *lex* ordering, so $g_{j_1}\in k[x_{m+1},...,x_n]\cap I=I_m$. As a consequence $r_1\in I_m$ so inductively we get

$$f=a_{j1}g_{j_1}+...+a_{j_s}g_{j_s}$$

with $g_{j_i}\in I_m$ and the remainder being 0 because $f\in I$ and $(g_1,...,g_r)$ is a Groebner basis of I. So we proved that $f\in\langle G_m\rangle$.

We skip the proof that G_m is a Groebner basis.

Projection allows us to describe the image of polynomial maps. This is the key computational ingredient of the large area of birational geometry (where more generally the maps are given by rational functions):

Example 47 *Consider the curve* $C=\varphi(\mathbb{A}^1(k))$ *with*

$$\begin{array}{rl}\varphi: & \mathbb{A}^1(k)\to\mathbb{A}^3(k)\\ & t\mapsto(t^2,t^3,t^4)\end{array}$$

The graph $\Gamma(\varphi)$ of φ has projections to the source and target of φ

$$\begin{tikzcd}
& \Gamma(\varphi) \arrow[dl] \arrow[dr, "\pi_1"] & = \{(t, \varphi(t)) \mid t \in \mathbb{A}^1(k)\} \subset \mathbb{A}^1(k) \times \mathbb{A}^3(k) \\
\mathbb{A}^1(k) \arrow[rr, "\varphi"'] & & \mathbb{A}^3(k)
\end{tikzcd}$$

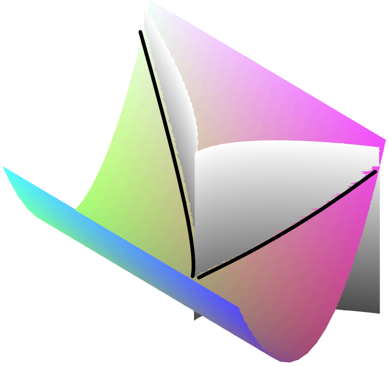
and $image(\varphi) = \pi_1(\Gamma(\varphi))$. So in order to get the image of φ we have to compute the first elimination ideal of

$$I(\Gamma(\varphi)) = \left\langle x - t^2, y - t^3, z - t^4 \right\rangle$$

By the above example a Groebner basis of $I(\Gamma(\varphi))$ in $k[t, z, y, x]$ with respect to $t > z > y > x$ is given by $y^2 - x^3, z - x^2, tx - y, ty - x^2, t^2 - x$, hence

$$\overline{image(\varphi)} = V\left(y^2 - x^3, z - x^2\right)$$

(Note that in this case $image(\varphi)$ is closed, in general this is not true).



This is the key computational ingredient of the large area of birational geometry, where more generally the maps are given by rational functions, think for example of the parametrization of the circle.

Proposition 48 *Suppose $k = \overline{k}$ and we are given a rational map*

$$\begin{array}{rl} \varphi: & \mathbb{A}^m(k) \backslash Z \to \mathbb{A}^n(k) \\ & t = (t_1, .., t_m) \mapsto \left(\frac{f_1(t)}{g_1(t)}, ..., \frac{f_n(t)}{g_n(t)}\right) \end{array}$$

with $f_i, g_i \in k[t_1, .., t_m]$ and $Z = V(g)$, $g = g_1 \cdot ... \cdot g_n$ the zeros of the denominators. Then

$$\overline{image(\varphi)} = V(I_{m+1})$$

with

$$I = \langle g_1 x_1 - f_1, ..., g_n x_n - f_n, 1 - gs \rangle \subset k[s, t_1, .., t_m, x_1, ..., x_n]$$

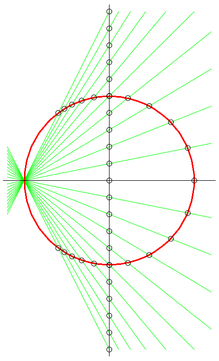
Note, that this stays true for any infinite field.

We skip the proof, as the idea is simple: To describe the graph, we multiply the equations $x_i = \frac{f_i(t)}{g_i(t)}$ by the denominator and add an additional variable s and the equation $1 - gs$ to remove the solutions (x, t) with some $g_i(x) = 0$.

Example 49 *Consider the parametriziaton of the circle:*

$$\varphi : \mathbb{A}^1(k) \backslash Z \to \mathbb{A}^2(k), t \mapsto (x(t), y(t))$$
$$x(t) = \frac{1-t^2}{t^2+1}, \; y(t) = \frac{2t}{t^2+1}$$

with $Z = V(t^2+1)$, given by the second intersection point of the line $y = t(x+1)$ with the circle:



A Groebner basis of $I = \left\langle (t^2+1)x - (1-t^2), (t^2+1)y - 2t, 1 - (t^2+1)^2 s \right\rangle$ with respect to lex $s > t > x > y$ is given by

$$\left\{ x^2 + y^2 - 1, ty + x - 1, tx + t - y, s - \frac{1}{2}x - \frac{1}{2} \right\}$$

and hence $I_2 = \langle x^2 + y^2 - 1 \rangle$. What kind of information gives the second or third equation?

The following proposition describes the relationship between resultants and rational implicitation:

Proposition 50 *Let $k = \overline{k}$. Given $f, g \in k[t, x_1, ..., x_n]$*

$$f_1 = a_w t^w + .. + a_0$$
$$f_2 = b_l t^l + .. + b_0 \text{ with } a_i, b_i \in k[x_1, ..., x_n]$$

for any zero $c = (c_1, ..., c_n)$ of $\operatorname{Res}(f_1, f_2, t)$ with $a_w(c) \neq 0$ and $b_l(c) \neq 0$, there is a t_0 with $f_1(t_0, c) = 0$ and $f_2(t_0, c) = 0$.

Proof. If $a_w(c) \neq 0$ and $b_l(c) \neq 0$ then

$$0 = \operatorname{Res}(f_1, f_2, t)(c) = \operatorname{Res}(f_1(t, c), f_2(t, c), t)$$

hence $f_1(t, c)$ and $f_2(t, c)$ have a common factor, so a common zero.

Explore this in the example of the circle:

Example 51 *Computing the resultant of* $f_1 = (t^2+1)x - (1-t^2)$, $f_2 = (t^2+1)y - 2t$, *we get*

$$\operatorname{Res}(f_1, f_2, t) = \det \begin{pmatrix} x+1 & 0 & y & 0 \\ 0 & x+1 & -2 & y \\ x-1 & 0 & y & -2 \\ 0 & x-1 & 0 & y \end{pmatrix} = 4x^2 + 4y^2 - 4 \in I_2$$

The proposition tells us, that any $c \in \mathbb{A}^2(k)$ *with* $\operatorname{Res}(f_1, f_2, t)(c) = 0$ *is a point in the image of the parametrization* φ *or is a root of*

$$a_2 = x + 1 \text{ or } b_2 = y$$

i.e. $c \in \{(-1, 0), (1, 0)\}$, *so*

$$V(\operatorname{Res}(f_1, f_2, t)) = image(\varphi) \cup \{(-1, 0)\} = \overline{image(\varphi)}$$

The point $(-1, 0)$ *is called a base point (i.e. a common zero) of the linear system* $l_t = \{y - t(x+1)\}$ *used to parametrize the circle.*

References

[1] Cox, Little, O´Shea: Ideals, Varieties, and Algorithms. UTM, Springer (1996).

[2] Decker, Schreyer: Varieties, Groebner Bases, and Algebraic Curves. Manuscript.

[3] Schenck: Computational Algebraic Geometry. LMSST 58, Cambridge University Press (2003).