Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topic is the projective space. Higher dimensional affine varieties $A \subset \mathbb{A}^n(\mathbb{C})$ are never compact in the euclidean topology. $\mathbb{P}^n(\mathbb{C})$ is a compactification.

1. $\mathbb{P}^n$.
2. Graded rings and the homogeneous coordinate ring of projective varieties
3. The projective closure

For affine zero-dimensional algebraic sets the number of solutions is a numerical invariant. Introducing projective algebraic sets will allow to generalise the number of points on one side and the degree of a hypersurface defined as the degree of the defining equation into a concept of a degree for arbitrary algebraic sets. This will the topic of the first lecture in the new year.

Perspective drawings

Two parallel lines in $\mathbb{A}^2$ do not intersect. However in perspective drawing they do intersect in a point in the horizon.

To put this into the right frame work, we define $\mathbb{P}^2(\mathbb{R})$ as the lines through the origin of $\mathbb{R}^3$. Then each point in the plane $\{z = 1\}$ gives a point of $\mathbb{P}^2(\mathbb{R})$ and in addition we have the horizon corresponding to one-dimensional subvector spaces of $\mathbb{R}^3$ contained in $\{z = 0\}$.

The projective space as a set

Definition. Let k be any field and W be a finite-dimensional k vector space. **The projective space of** W is

$$\mathbb{P}(W) = \{\text{1-dimensional subvector spaces of } W\}.$$

In particular

$$\mathbb{P}^n(k) = \mathbb{P}(K^{n+1}).$$

$\mathbb{P}^n$ refers to $\mathbb{P}^n(K)$ over an algebraic closed extension field K of k and we call $\mathbb{P}^n(k)$ also the set of k-rational points of $\mathbb{P}^n$.

A different way to define $\mathbb{P}^n$ is via an equivalence relation: Two points $a = (a_0, \ldots, a_n), b = (b_0, \ldots, b_n) \in K^{n+1} \setminus \{0\}$ are equivalent, i.e., $a \sim b$, iff $\exists \lambda \in K^*$ with $\lambda a = b$. Then

$$\mathbb{P}^n = (K^{n+1} \setminus \{0\})/\sim$$

identifies the equivalence class $[a]$ with the one-dimensional subspace spanned by a.

Homogeneous coordinates and projective algebraic sets

We refer to $[a_0 : a_1 : \ldots : a_n]$ as the **homogeneous coordinates of the point** $p = [a] \in \mathbb{P}^n$. Note that the ratios $a_i : a_j$ for $a_j \neq 0$ are well-defined.

Given a polynomial $f \in K[x_0, \ldots, x_n]$ the value $f(p)$ does not make sense. However for a **homogeneous polynomial** of degree d we have

$$f(\lambda a) = \lambda^d f(a).$$

Here f is called homogeneous if each term of f has the same total degree d. Thus

$$V(f) = \{p \in \mathbb{P}^n \mid f(p) = 0\}$$

where f is homogeneous is a well-defined subset of $\mathbb{P}^n$.

Definition. A **projective algebraic set** is a subset of the form

$$V(f_1, \ldots, f_r) = \bigcap V(f_i)$$

where the f_i are homogeneous of degree d_i. These sets form the closed sets of the Zariski topology of $\mathbb{P}^n$.

The standard atlas of $\mathbb{P}^n$.

The (Zariski) open subsets

$$U_i = \{[a_0 : \ldots : a_n] \in \mathbb{P}^n \mid a_i \neq 0\} = \mathbb{P}^n \setminus V(x_i)$$

cover $\mathbb{P}^n$ because each point in $\mathbb{P}^n$ has homogeneous coordinates $[a_0 : \ldots : a_n]$ with at least one $a_i \neq 0$. The maps

$$\varphi_i : U_i \to \mathbb{A}^n, [a_0 : \ldots : a_i : \ldots a_n] \mapsto (\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i})$$

are well-defined bijections. For example, the inverse of φ_0 is

$$\varphi_0^{-1} : \mathbb{A}^n \to U_0 \subset \mathbb{P}^n, (b_1, \ldots, b_n) \mapsto [1 : b_1 : \ldots : b_n]$$

More generally, φ_i^{-1} inserts 1 into the i-th position. The change of charts maps

$$\varphi_{ij} = \varphi_i \circ \varphi_j^{-1} : \varphi_j(U_i \cap U_j) \to \varphi_i(U_i \cap U_j)$$

are given by rational maps. For example

$$\varphi_{i0} : \mathbb{A}^n \dashrightarrow \mathbb{A}^n, (a_1, \ldots, a_n) \mapsto (\frac{1}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}).$$

$\mathbb{P}^n$ as a manifold.

The atlas

$$\mathcal{A} = \{(U_i, \varphi_i) \mid i = 0, \ldots, n\}$$

gives $\mathbb{P}^n(\mathbb{R})$ and $\mathbb{P}^n(\mathbb{C})$ the structure of a compact differentiable or compact complex manifold respectively, because rational functions are differentiable and holomorphic on their domain of definition.

$$\mathbb{P}^n(\mathbb{R}) = S^n / \sim$$

identifies antipodal points of the unit sphere $S^n \subset \mathbb{R}^{n+1}$. $\mathbb{P}^2(\mathbb{R})$ is a non-orientable surface which is the union of a Möbius strip M and a disc D glued along their common boundary $\partial M \cong \partial D = S^1$.

The Hopf fibration

$\mathbb{P}^n(\mathbb{C})$ with the euclidean topology is compact since the map from the unit sphere $S^{2n+1} \subset \mathbb{C}^{n+1} \setminus \{0\}$ to $\mathbb{P}^n(\mathbb{C})$ is continuous.

$$h : S^{2n+1} \to \mathbb{P}^n(\mathbb{C})$$

is called the **Hopf fibration**. The fibers of h are isomorphic to circles

$$S^1 = \{\lambda \in \mathbb{C} \mid |\lambda| = 1\}.$$

As a real manifold $\mathbb{P}^1(\mathbb{C}) \cong S^2$ since both spaces are one point compactifications of $U_0 \cong \mathbb{C} \cong \mathbb{R}^2$. Identifying S^3 with the one point compactification of $\mathbb{R}^3$ we see that of $\mathbb{R}^3$ is a disjoint union of linked circles and one line.

$\mathbb{P}^n$ as a compactification

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1} = \mathbb{A}^n \cup \mathbb{A}^{n-1} \cup \ldots \cup \mathbb{A}^0$$

where we identify $\mathbb{A}^n \cong U_0$ with a Zariski open subset via φ_0. For this reason we call $\mathbb{P}^{n-1} = V(x_{0)} \subset \mathbb{P}^n$ the **hyperplane at infinity**.

Let $A = V(f) \subset \mathbb{A}^n$ for $f \in K[x_1, \ldots, x_n]$ be a hypersurface. Then the Zariski closure $\overline{A} \subset \mathbb{P}^n$ is defined by $\overline{A} = V(f^h)$ where

$$f^h = x_0^{\deg f} f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \in K[x_0, \ldots, x_n]$$

denotes the **homogenisation of f.** Conversely for a homogeneous polynomial $f \in K[x_0, \ldots, x_n]$ we denote by

$$f^a = f(1, x_1, \ldots, x_n)$$

the corresponding affine polynomial. Clearly $(f^h)^a = f$. However

$$(f^a)^h = x_0^{\deg f - \deg f^a} f$$

coincides with f if and only if x_0 is not a factor of f.

A plane cubic curve in all three charts

Consider the curve $C = V(y^2z - x^3 - x^2z) \subset \mathbb{P}^2$ with homogeneous coordinates $[x : y : z]$.

$$y^2 = x^3 + x^2$$

in $U_2 = \{z = 1\}$

$$z = \frac{x^3}{1 - x^2}$$

in $U_1 = \{y = 1\}$

$$z = \frac{1}{y^2 - 1}$$

in $U_0 = \{x = 1\}$

Graded rings

Definition. A **graded ring** R is a ring together with a decomposition

$$R = \bigoplus_{d \in \mathbb{Z}} R_d$$

as abelian groups satisfying

$$R_d \cdot R_e \subset R_{d+e}$$

for the multiplication. An ideal J in a graded ring is called homogeneous if

$$J = \bigoplus_{d \in \mathbb{Z}} J_d \text{ with } J_d = J \cap R_d,$$

equivalently if J is generated by homogeneous elements. In that case

$$R/J = \bigoplus R_d/J_d$$

is again a graded ring.

Homogeneous coordinate ring

$S = K[x_0, \ldots, x_n]$ with

$$S_d = \{f \in S \mid f \text{ is homogeneous of degree } d\}$$

is a graded ring. We call this the **standard graded polynomial ring** in $n+1$ variables.

Definition. Let $A \subset \mathbb{P}^n$. Then

$$\mathrm{I}(A) = (\{f \in S_d \mid f(p) = 0 \; \forall p \in A\})$$

is called the **homogeneous ideal of** A and

$$S/\mathrm{I}(A) = \bigoplus_{d \geq 0} (S/\mathrm{I}(A))_d = \bigoplus_{d \geq 0} S_d/\mathrm{I}(A)_d$$

is called the **homogeneous coordinate ring** of A.

Conversely, for a homogeneous ideal $J \subset S$ we define

$$V(J) = \{p \in \mathbb{P}^n \mid f(p) = 0 \; \forall \text{ homogeneous } f \in J\}.$$

The algebra-geometry dictionary in the projective case

The correspondences

$$\{\text{subsets of } \mathbb{P}^n\} \leftrightarrow \{\text{homogeneous ideals of } S = K[x_0, \ldots, x_n]\}$$

$$A \mapsto \mathrm{I}(A), V(J) \leftarrow J$$

induce a bijection between

$$\{\text{algebraic subsets of } \mathbb{P}^n\} \leftrightarrow \{\text{homogeneous radical ideals of } S\}$$

and

$$\{\text{projective subvarieties of } \mathbb{P}^n\} \leftrightarrow \{\text{homogeneous prime ideals of } S\}.$$

The homogeneous maximal ideal $\mathfrak{m} = (x_0, \ldots, x_n)$ corresponds to the empty set $\emptyset$. For this reason $\mathfrak{m}$ is sometimes called the **irrelevant ideal**.

The projective Nullstellensatz

Proposition. *Let $J \subsetneq S$ be a homogeneous ideal of the standard graded polynomial ring $S = K[x_0, \ldots, x_n]$ over an algebraically closed field K. Then*

$$V(J) = \emptyset \subset \mathbb{P}^n \iff \mathrm{rad}(J) = (x_0, \ldots, x_n).$$

Proof. We denote by

$$C(J) = \{a \in \mathbb{A}^{n+1} \mid f(a) = 0 \; \forall f \in J\}$$

the zero loci of J in $\mathbb{A}^{n+1}$. This is a cone whose vertex is the origin $o = (0, \ldots, 0)$. $C(J) \neq \emptyset$ because J is a proper homogeneous ideal. If $C(J)$ contains a point $a = (a_0, \ldots, a_n)$ different from the origin then $[a_0 : \ldots : a_n] \in V(J) \subset \mathbb{P}^n$. Thus

$$\begin{aligned} V(J) = \emptyset &\iff C(J) = \{o\} \\ &\iff \mathrm{rad}(J) = \mathrm{I}(\{o\}) = (x_0, \ldots, x_n) \end{aligned}$$

by the Nullstellensatz for $\mathbb{A}^{n+1}$. □

The projective closure of the twisted cubic

Consider $A = V(y - x^2, z - xy) \subset \mathbb{A}^3$ the image of

$$\varphi : \mathbb{A}^1 \to \mathbb{A}^3, t \mapsto (t, t^2, t^3).$$

Using homogeneous coordinates $[w : x : y : z]$ on $\mathbb{P}^3$ we obtain by homogenizing both equations

$$(wy - x^2, wz - xy) = (wy - x^2, wz - xy, y^2 - xz) \cap (w, x).$$

The line $V(w, z) \cong \mathbb{P}^1$ is completely contained in the hyperplane at infinity $\mathbb{P}^2 = V(w)$. It does not belong to the projective closure

$$\overline{A} = V(wy - x^2, wz - xy, y^2 - xz)$$

of A in $\mathbb{P}^3$. $\overline{A}$ intersects the hyperplane at infinity in a single point:

$$\begin{aligned} V(wy - x^2, wz - xy, y^2 - xz, w) &= V(w, x^2, xy, y^2 - xz) \\ &= V(w, x, y) = \{[0 : 0 : 0 : 1]\end{aligned}$$

which is the limit of the points

$$[1 : t : t^2 : t^3] = [\frac{1}{t^3} : \frac{1}{t^2} : \frac{1}{t} : 1] \text{ for } t \to \infty.$$

Computation of the projective closure

Let $J \subset K[x_1, \ldots, x_n]$. Then

$$J^h = (\{f^h \mid f \in J\}) \subset K[x_0, \ldots, x_n]$$

is called the **homogenization** of J.

Algorithm.
Input. Generators $f_1, \ldots, f_r$ of an ideal $J \subset K[x_1, \ldots, x_n]$.
Output. Generators of $J^h \subset K[x_0, \ldots, x_n]$.

1. Choose a global monomial order $>$ in $K[x_1, \ldots, x_n]$ which refines the total degree, for example, $>_{\mathrm{rlex}}$.
2. Compute a Gröbner basis $f_1, \ldots f_{r'}$ of $(f_1, \ldots, f_r)$ with respect to this order.
3. Return $f_1^h, \ldots, f_{r'}^h$.

Correctness

Example. The computation

$x^2 - y$	$-y$	z
$xy - z$	x	$-y$
$y^2 - xz$	-1	x

shows that $x^2 - y, xy - z, y^2 - xz$ is a Gröbner basis. Thus $(y - x^2, z - xy)^h = (x^2 - wy, xy - wz, y^2 - xz)$.

Proof. Let $f_1, \ldots, f_{r'}$ be a Gröbner basis with respect to $>$ and $f \in J$ an arbitrary element. Consider the division expression

$$f = g_1 f_1 + \ldots + g_{r'} f_{r'}$$

for f. Since the lead terms $\mathrm{Lt}(g_i f_i)$ are disjoint and $>$ refines the total degree we have $d = \deg f \geq \deg(g_i f_i) = d_i$ and equality holds for at least one j. Thus

$$f^h = x_0^{d-d_0} g_0^h f_0^h + \ldots + x_0^{d-d_{r'}} g_{r'}^h f_{r'}^h$$

lies in $(f_1^h, \ldots, f_{r'}^h)$. □