Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topics are Bézout's theorem, intersection multiplicities of plane curves and multiplicity of plane curves.

1. Rational functions and regular functions on projective varieties
2. Intersection multiplicities
3. Multiplicity of points on plane curves
4. Bézout's theorem

Rational functions on projective varieties

Definition. Let $X \subset \mathbb{P}^n$ be a projective variety, i.e., an irreducible algebraic set. Let $\mathrm{I}(X) \subset S = K[x_0, \ldots, x_n]$ denote its homogeneous ideal and $S_X = S/\mathrm{I}(X)$ its homogeneous coordinate ring. Then

$$K(X) = \{f = \frac{g}{h} \mid g \in S_X, h \in S_X \setminus \{0\} \text{ and } \deg g = \deg h\} \subset Q(S_X)$$

is called the **rational function field** of X. Notice that since $\deg f = \deg g$ the fraction $f = \frac{g}{h}$ defines a well-defined function

$$X \setminus V(h) \to K, p = (a_0 : \ldots : a_n) \mapsto \frac{f(a)}{g(a)}.$$

$f \in K(X)$ is defined at $p \in X$ if f has a representative $\frac{g}{h}$ with $h(p) \neq 0$. We define the local ring of X at p by

$$\mathcal{O}_{X,p} = \{f \in K(X) \mid f = \frac{g}{h} \text{ with } h(p) \neq 0\}.$$

Comparison with the affine notion

Proposition. *Let $U_i \cong \mathbb{A}^n$ be an affine chart which intersects X. Then*

$$K(X \cap U_i) \cong K(X)$$

via dehomogenisation and homogenisation.

Proof. In case $i = 0$ we have

$$f(x_0, \ldots, x_n) = \frac{g(x_0, \ldots, x_n)}{h(x_0, \ldots, x_n)} \mapsto f^a = \frac{g(1, x_1, \ldots, x_n)}{h(1, x_1, \ldots, x_n)}$$

and conversely

$$f = \frac{g(x_1, \ldots, x_n)}{h(x_1, \ldots, x_n)} \mapsto f^h = \frac{x_0^{\deg g + \deg h} g(x_1/x_0, \ldots, x_n/x_0)}{x_0^{\deg g + \deg h} h(x_1/x_0, \ldots, x_n/x_0)}.$$

Hence $(f^h)^a = f$ is clear, and $(f^a)^h = f$ holds because a possible common x_0 factors in the nominator and the denominator cancels. □

Intersection multiplicities for plane curves

Let $C = V(f)$ and $H = V(g) \subset \mathbb{P}^2$ be two plane algebraic curves without a common component. For $p \in C \cap H$ we define the **intersection multiplicity of** C **and** H **at** p by

$$i(C, H; p) = i(f, g; p) = \dim_K \mathcal{O}_{\mathbb{P}^2,p}/(f, h)\mathcal{O}_{\mathbb{P}^2,p},$$

i.e., as the K vector space dimension of the quotient of the local ring by the ideal generated by f, g.

Example. Consider the plane affine curves define by $f = y$, $g = y - x^n$. The intersection number at the origin is

$$\begin{aligned} i(f, g; o) = \dim_K K[x, y]_{(x,y)}/(f, g) &= \dim_K K[x, y]_{(x,y)}/(y, x^n) \\ = \dim_K (K[x, y]/(y, x^n))_{(x,y)} &= \dim_K K[x, y]/(y, x^n) = n. \end{aligned}$$

Further examples

Example 2. For $f = y^2 - x^3$ and $g = x^2 - y^3$ we obtain

$$\begin{aligned} \mathcal{O}_{\mathbb{A}^2,o}/(f,g) &\cong \mathcal{O}_{\mathbb{A}^2,o}/(y^2 - x^3, x^2 - yx^3) \\ &\cong \mathcal{O}_{\mathbb{A}^2,o}/(y^2 - x^3, x^2(1 - yx)) \\ &\cong \mathcal{O}_{\mathbb{A}^2,o}/(y^2 - x^3, x^2) \\ &\cong \mathcal{O}_{\mathbb{A}^2,o}/(y^2, x^2) = K[x,y]/(y^2, x^2) \end{aligned}$$

Hence $i(f,g;o) = 4$.

Further examples

Example 3. For $f = y^2 - x^3$ and $g = y^2 - 2x^3$ we obtain

$$\begin{aligned}\mathcal{O}_{\mathbb{A}^2,o}/(f,g) &\cong \mathcal{O}_{\mathbb{A}^2,o}/(y^2 - x^3, y^2 - 2x^3) \\ &\cong \mathcal{O}_{\mathbb{A}^2,o}/(y^2, x^3)\end{aligned}$$

Hence $i(f,g;o) = 6$. This makes a lot of sense because it we perturb g a little bit $g_t = y^2 - 2(x-2t)^2(x-t)$ then $V(f,g_t)$ has six intersection points which approach the origin o for $t \to 0$.

Ordinary m-fold points and tangent lines

Definition. Let $p \in V(f) \subset \mathbb{P}^2$ be a point. After a change of coordinates we may assume that p corresponds to the origin $o \in \mathbb{A}^2 \cong U_0 \subset \mathbb{P}^2$. Suppose

$$f^a = f_m + \ldots + f_d \text{ with } f_j \in K[x,y]_j,$$

i.e. with f_j homogeneous of degree j and f_m in not the zero polynomial. Then we say that f has **multiplicity** m at p,

$$\operatorname{mult}_p(f) = m.$$

If f_m factors into linear forms ℓ_k:

$$f_m = \prod_{k=1}^{m} \ell_k.$$

We call the lines $L_k = V(\ell_k)$ the **tangent lines** of $V(f)$ at p. If they are pairwise distinct, we call p an **ordinary** m**-fold point** of $V(f)$.

Double points and smooth points

Example. The curve $V(y^2 - x^2 - x^3)$ has an ordinary double point at o with tangent lines $L_1 = V(y - x)$ and $L_2 = V(y + x)$.

$V(y^2 - x^3)$ is a curve with a non-ordinary double point.

Remark. Suppose $K = \mathbb{C}$. If $\mathrm{mult}_p(f) = 1$ then locally in the euclidean topology of $\mathbb{A}^2(\mathbb{C}) = \mathbb{C}^2$ the zero loci coincides with the graph of an holomorphic function by the implicit function theorem.

Definition. If $\mathrm{mult}_p(f) = 1$ then $p \in C = V(f)$ is called a **smooth point** of C. Otherwise p is called a **singular point** of C.

Bézout's theorem for plane curves

Theorem. *Let $C = V(f)$ and $H = V(g) \subset \mathbb{P}^2$ be two plane curves of degree d and e. Counted with multiplicities C and D intersect in precisely $d \cdot e$ points:*

$$\sum_{p \in C \cap H} i(C, H; p) = d \cdot e.$$

Remark. If $p \notin C \cap H$, then $i(C, H; p) = 0$ because either f or g gives a unit in $\mathcal{O}_{\mathbb{P}^2, p}$.

If $i(C, H; p) = 1$, then we say C and H intersect **transversally** at p. In that case both C and H are smooth at p and have different tangent lines, because $\dim K[x, y]_1 = 2$.

Examples

Example 2. For $f = y^2 - x^3$ and $g = x^2 - y^3$ we have intersection multiplicity 4 at $o \in \mathbb{A}^2 \cong U_2 = \{z \neq 0\} \subset \mathbb{P}^2$. One further intersection point is $p = (1:1:1) \in U_2$. So there should be

$$4 = 3 \cdot 3 - 4 - 1$$

further intersection points. Indeed these are the points with coordinates $(\zeta^2 : \zeta^3 : 1)$, where ζ is any of the four non-trivial fifth root unity in $K = \mathbb{C}$.

Example 3. For $f = y^2 - x^3$ and $g = y^2 - 2x^3$ we obtain intersection multiplicity 6 at $o \in \mathbb{A}^2 \subset \mathbb{P}^2$. So we are missing 3 intersection points. They lie on the line at infinity: In the chart $U_1 = \{y \neq 0\}$ we have the equations $z - x^3, z - 2x^3$, and the intersection multiplicity at $p = (0:1:0)$ is 3.

A lower bound on the intersection multiplicity

Theorem. *Let $f, g \in K[x, y]$ be polynomials without a common factor which vanish at the origin $o \in \mathbb{A}^2$. Then*

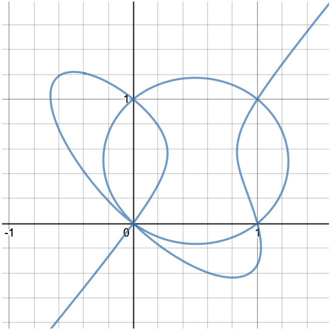
$$i(f, g; o) \geq \mathrm{mult}_o(f)\,\mathrm{mult}_o(g)$$

and equality holds if and only if $V(f)$ and $V(g)$ have no common tangent line at o.

We will prove this with a Gröber basis computation in local rings in one of the next lectures.

An application

Consider the plane curve C defined by
$f = -3\,x^5 - 2\,x^4y - 3\,x^3y^2 + x\,y^4 + 3\,y^5 + 6\,x^4 + 7\,x^3y + 3\,x^2y^2 - 2\,x\,y^3 - 6\,y^4 - 3\,x^3 - 5\,x^2y + x\,y^2 + 3\,y^3.$



$V(f)$ has a triple point at the origin and double points at the points with coordinates $(0, 1), (1, 0), (1, 1)$.

The application continued

Consider now the pencil of conics through these four point

$$D_t = V(t(x^2 - x) + y^2 - y).$$

The curve D_t intersects C with intersection multiplicity 3 at the origin and intersection multiplicity 2 at the double points.
Thus by Bézout

$$2 \cdot 5 - 3 - 2 - 2 - 2 = 1,$$

there remains one moving intersection point $p(t)$. Computing the coordinates of this point gives a rational parametrization of C.
The final result is $p(t) = (x(t), y(t))$ with

$$x(t) = \frac{-3\,t^5 - 8\,t^4 + 17\,t^3 + 9\,t^2 - 24\,t + 9}{9\,t^5 + t^4 - 6\,t^3 + 3\,t^2 - 14\,t + 9}$$

and

$$y(t) = \frac{-3\,t^5 - 8\,t^4 + 17\,t^3 + 9\,t^2 - 24\,t + 9}{9\,t^5 + t^4 - 6\,t^3 + 3\,t^2 - 14\,t + 9}.$$

.

A more general version of Bézout's theorem

Theorem. *Let* $X \subset \mathbb{P}^n$ *be a projective variety and* $H = V(g)$ *a hypersurface of degree e which does not contain* X. *Let* $Z_1, \ldots, Z_r$ *be the irreducible components of* $X \cap H$. *Then*

$$\deg X \cdot \deg H = \sum_{i=1}^{r} i(X, H; Z_i) \deg Z_i.$$

We will see how to define the **intersection multiplicty** $i(X, H; Z_i)$ of X and H **along** Z_i in the course of the proof.

The proof is build upon the computation of the Hilbert polynomial of the S/J for $J = \mathrm{I}(X) + (g)$ in two ways.

First computation of $p_{S/J}(t)$

Since X is a variety, $\mathrm{I}(X)$ is a prime ideal and since $g \notin \mathrm{I}(X)$, it is a non-zero-divisor in $S_X = S/\mathrm{I}(X)$. Hence

$$0 \longleftarrow S/J \longleftarrow S_X \xleftarrow{g} S_X(-e) \longleftarrow 0$$

is a short exact sequence. Since

$$p_X(t) = p_{S_X}(t) = \deg X \frac{t^r}{r!} + \text{ lower terms}$$

where $r = \dim X$, we obtain

$$\begin{aligned} p_{S/J}(t) &= p_X(t) - p_X(t-e) \\ &= \deg X \frac{ret^{r-1}}{r!} + \text{ lower terms} \\ &= \deg X \deg H \frac{t^{r-1}}{(r-1)!} + \text{ lower terms.} \end{aligned}$$

Hence $\dim V(J) = r - 1$ and $\deg J = \deg X \cdot \deg H$.

Associated primes of graded modules

For the second computation we consider the filtration of the S-module $M = S/J$ by quotients of prime ideals. Since M is graded all associated primes are graded as well.

We start by proving that a non-zero graded module M have at least one homogeneous associated prime.
Let $m \in M_d$ be a non-zero homogeneous element of degree d. Then the ideal $\operatorname{ann}(m)$ is homogeneous as well, and the map

$$S(-d) \to M, f \mapsto fm$$

induces an inclusion $S/\operatorname{ann}(m)(-d) \hookrightarrow M$. A maximal element in the set

$$\mathcal{M} = \{\operatorname{ann}(m) \mid m \in M \setminus \{0\} \mid m \text{ is homogeneous}\}$$

is a prime ideal. Since S is noetherian $\mathcal{M}$ contains a maximal element. Hence M has a homogeneous associated prime.

Associated primes of graded modules

Proposition. *Let M be a finitely generated graded S-module . Then M has a filtration*

$$0 = M_0 \subset M_1 \subset \ldots \subset M_N = M$$

with quotients

$$M_i/M_{i-1} \cong S/\mathfrak{p}_i(-d_i)$$

for homogeneous prime ideals $\mathfrak{p}_i$ and integers d_i.

Proof. We take $M_1 = Sm_1$ for $m_1 \in M_{d_1}$ is a homogeneous element whose annihilator a prime $\mathfrak{p}_1$. If $M_{k-1} \subset M$ is already constructed and $M_{k-1} \neq M$, we consider an associated prime $\mathfrak{p}_k = \operatorname{ann}(\overline{m}_k)$ of an homogeneous elemet $\overline{m}_k \in M/M_{k-1}$ and take M_k as the preimage of $S/\mathfrak{p}_k(-d_k) \hookrightarrow M/M_{k-1}$ in M. This process stops with an $M_N = M$ since M is noetherian. □

Corollary. *The associated primes of a finitely generated graded S-module are homogeneous.*

Proof. $\operatorname{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_N\}$. □

Second computation of $p_{S/J}(t)$

Consider $M = S/J$ and a filtration

$$0 = M_0 \subset M_1 \subset \ldots \subset M_N = M$$

with quotients

$$M_i/M_{i-1} \cong S/\mathfrak{p}_i(-d_i)$$

for homogeneous prime ideals $\mathfrak{p}_i$ and integers d_i. The HIlbert functions and Hilbert polynomials are additive in short exact sequences:

Proposition. *If*

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of graded S-modules, then

$$h_M = h_{M'} + h_{M''}$$

□

Hence we obtain

$$p_M(t) = \sum_{j=1}^{N} p_{S/\mathfrak{p}_k}(t - d_k).$$

Proof of Bézout's theorem

Comparing both formulas we obtain $\dim V(\mathfrak{p}_k) \leq r-1$ for all $\mathfrak{p}_k$ since $p_M(t)$ has degree $r-1$. Only those with equality contribute to the leading coefficient. The minimal associated primes correspond to the irreducible components Z_j of $X \cap H$.
Thus

$$\deg X \cdot \deg H = \sum_{Z_j \text{ with } \dim Z_j = r-1} i(X, H; Z_j) \deg Z_j.$$

if we define

$$i(X, H; Z_j) = |\{k \mid \mathfrak{p}_k = \mathrm{I}(Z_j)\}|.$$

Actually $\dim Z_j = r-1$ holds for every component of $X \cap H$. This follows from Krull's principal ideal theorem. □