Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

1. Discrete valuation rings
2. Dynamical intersection numbers
3. A bounds on the number of singular points of plane curves
4. Rational curves
5. The geometric genus

Discrete valuation

Definition. Let L be a field. A **discrete valuation** on L is a surjective map

$$v : L \setminus \{0\} \to \mathbb{Z}$$

such that for all $a, b \in L \setminus \{0\}$

1. $v(ab) = v(a) + v(b)$,
2. $v(a+b) \geq \min\{v(a), v(b)\}$.

Note that the first condition says that $(L \setminus \{0\}, \cdot) \to (\mathbb{Z}, +)$ is a group homomorphism. In particular $v(1) = 0$. By convention $v(0) = \infty$. The set

$$R = \{a \in L \mid v(a) \geq 0\}$$

is a subring of L, which is called the **valuation ring** of v. The subset of non-units in R

$$\mathfrak{m} = \{a \in L \mid v(a) > 0\}$$

is an ideal. Hence $(R, \mathfrak{m})$ is a local ring.

Discrete valuation rings

Definition. A **discrete valuation ring** (DVR) R is an integral domain such that R is the valuation ring of a valuation v on its quotient field $L = Q(R)$.

Example. The formal power series ring $R = K[[t]]$ in one variable over a field K is a DVR. Indeed, the quotient field of R is

$$L = K((t)) = \{\sum_{n=N}^{\infty} a_n t^n \mid N \in \mathbb{Z}\}$$

the ring of formal Laurent series, and

$$v(\sum a_n t^n) = \min\{n \mid a_n \neq 0\}$$

for a non-zero Laurent series defines a valuation on L with valuation ring $K[[t]]$. Following the notion for power series in one complex variable, we say that $f \in K[[t]]$ has a **zero of order** n if $v(f) = n$ and $f \in K((t))$ with $n = v(f) < 0$ is said to have **pole of order** $-n$.

Characterization of DVR's

Proposition. *Let R be a ring. TFAE:*

1) *R is a DVR.*
2) *R is a noetherian regular local ring of Krull dimension 1.*

Proof. $1) \Rightarrow 2)$: Suppose R is a DVR. Let $t \in R$ be an element with $v(t) = 1$. Then any element $f \in R$ with $v(f) = n$ is of the form $f = ut^n$ with u a unit in R. In particular, t is a generator of $\mathfrak{m}$ and the only proper ideals $I \neq 0$ are of the form $I = (t^n) = \mathfrak{m}^n$ with $n = \min\{v(f) \mid f \in I\}$. Hence $(0) \subsetneq \mathfrak{m}$ is the only chain of prime ideals in R and R is PID. So R is noetherian and a regular local ring of Krull dimension 1, because $\mathfrak{m}$ is generated by a single element, i.e., $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional by Nakayama's Lemma.

$2 \Rightarrow 1$

Conversely, let R be a noetherian regular local ring of Krull dimension 1. By Nakayama's Lemma the maximal ideal $\mathfrak{m}$ is a principal ideal, say $\mathfrak{m} = (t)$. Hence the powers $\mathfrak{m}^k = (t^k)$ are principal ideals as well. Let $f \in R$ be a non-zero element. Since $\bigcap_{k=1}^{\infty} \mathfrak{m}^k = (0)$ by Krull's intersection theorem

$$n = \max\{k \mid f \in \mathfrak{m}^k\}$$

is the maximum of finitely many integers and $f = ut^n$ for a unit $u \in R$. We set $v(f) = n$. Then $v(f_1 f_2) = v(f_1) + v(f_2)$. In particular R is a domain. We extend v to a map

$$v : Q(R) \setminus \{0\} \to \mathbb{Z} \quad \text{by} \quad v(\frac{f_1}{f_2}) = v(f_1) - v(f_2).$$

Then v is discrete valuation on $Q(R)$ and R is its valuation ring. $\square$

Smooth points of curves

Corollary. *Let $p \in C$ be a smooth point of an irreducible curve. Then $\mathcal{O}_{C,p}$ is a DVR.* □

Remark. We denote the valuation of $K(C)$ corresponding to $\mathcal{O}_{C,p}$ with v_p. In case of a smooth projective curve C one can show that

$$p \mapsto v_p$$

induces a bijection between the points of C and the valuations of the function field $v : K(C) \setminus \{0\} \to \mathbb{Z}$ with $v(a) = 0$ for all $a \in K \setminus \{0\}$.

Proposition. *Let C be a smooth quasi projective curve and $\varphi' : C \dashrightarrow \mathbb{P}^n$ a rational map. Then φ' extends to a morphism*

$$\varphi : C \to \mathbb{P}^n.$$

Proof

Suppose that φ' is given by a tuple $f_0, \ldots, f_n$ of rational functions. There are two reasons why $[f_0(p) : \ldots : f_n(p)]$ might be not defined in $p \in C$. One of the rational functions might have a pole at p or all rational functions might vanish at p.
Taking $k = \min\{v_p(f_j) \mid j = 0, \ldots, n\}$ and $t \in \mathfrak{m}_{C,p} \subset \mathcal{O}_{C,p}$ a generator we see that $[t^{-k} f_0 : \ldots : t^{-k} f_n]$ is defined at $p \in C$ and coincides φ' where t has no zeroes or poles. $\square$

Remark. The proposition is not true for a higher dimension source: The morphism

$$\mathbb{A}^2 \setminus \{o\} \to \mathbb{P}^1, p \mapsto [x(p) : y(p)]$$

has no extension to $\mathbb{A}^2$. Instead the closure of the graph is the blow-up of $o \in \mathbb{A}^2$.

Projectivity of the Hilbert schemes

Remark. The proposition above explains why the fact that the Hilbert scheme $\mathrm{Hilb}_{p(t)}(\mathbb{P}^n)$ is projective is so nice. Let $o \in C$ be a smooth point on a quasi-projective curve. Then every family $X' \subset C \setminus \{o\} \times \mathbb{P}^n$ of subschemes X'_q with Hilbert polynomial $p(t)$ can be extended to a family

$$X \subset C \times \mathbb{P}^n$$

where the fibers X_o has Hilbert polynomial $p(t)$ as well. Indeed the family X' corresponds to a rational map $C \dashrightarrow \mathrm{Hilb}_{p(t)}(\mathbb{P}^n) \subset \mathbb{P}^N$ which extends to a morphism. Loosely speaking

$$\lim_{q \to o} X_q = X_o \in \mathrm{Hilb}_{p(t)}(\mathbb{P}^n)$$

exists along curves.

Degree of a morphism $f : C \to \mathbb{P}^1$

Let $C \subset \mathbb{P}^n$ be a smooth projective curve $f \in K(C)$ a non-constant rational function. By the proposition above the rational map

$$C \dashrightarrow \mathbb{P}^1, p \mapsto [1 : f(p)]$$

extends to a morphism $f : C \to \mathbb{P}^1$, which we denote by the same letter.

Definition. The **degree** of f is

$$\deg f = \sum_{p \in C : v_p(f) > 0} v_p(f)$$

the number of preimage points of $[1 : 0]$ counted with multiplicities.

Proposition. *Counted with multiplicities each fiber $f^{-1}(\lambda)$ of $\lambda \in \mathbb{P}^1$ has precisely $\deg f$ many points.*

Proof

Since rational function are given by quotients of homogeneous polynomials of the same degree on the ambient $\mathbb{P}^n$ the number of poles $\sum_{p \in C : v_p(f) < 0} -v_p(f)$ coincides with the number zeroes by Bézout's theorem. To see that the number of preimage points of $\lambda \in \mathbb{A}^1 = K$ coincides with $\deg f$, we note that f and $f - \lambda$ have the same poles. □

Remark. One can show that $\deg f$ also coincides with the degree of the field extension $[K(C) : K(f)]$. Note that $K(f) \cong K(\mathbb{P}^1)$.

More generally for a morphism $\varphi : C \to E$ between smooth projective curves the **degree** can be defined as

$$\deg \varphi = [K(C) : K(E)]$$

and this number coincides with the number of preimage points of any point $p \in E$ counted with multiplicities.

Dynamical intersection numbers

We assume that $K = \mathbb{C}$. Let $f \in K[x, y, z]$ a square free polynomial of degree d and $g \in K[x, y, z]$ a homogeneous polynomial of degree e which as no common factor with f. Then

$$d \cdot e = \sum_{p \in V(f,g)} i(f, g; p)$$

by Bézout's theorem. We will show that the intersection multiplicities can be interpreted dynamically.

As an application of Bertini's theorem we see that there exists a homogeneous polynomial g_1 of degree e such that $C = V(f)$ and $D = V(g_1)$ intersect transversally in $d \cdot e$ distinct points.

Indeed, consider the e-uple embedding

$$\rho_{2,e} : \mathbb{P}^2 \to \mathbb{P}^{\binom{e+2}{2}-1}$$

Curves of degree e in $\mathbb{P}^2$ correspond to hyperplanes H in $\mathbb{P}^{\binom{e+2}{2}-1}$ and a general hyperplane H_1 intersects every component of $\rho_{2,e}(C)$ transversally in smooth points of $\rho_{2,e}(C)$.

Dynamical intersection numbers, 2

Let g_1 be the polynomial corresponding to the equation of H_1 and consider the pencil of curves of degree e

$$D = V(t_0 g + t_1 g_1) \in \mathbb{P}^1 \times \mathbb{P}^2$$

All but finitely many fibers D_λ over $\lambda \in \mathbb{P}^1$ intersect C in $d \cdot e$ distinct points. Consider now the curve

$$X' = D \cap (\mathbb{P}^1 \times C)$$

and the union X of components which dominate $\mathbb{P}^1$. Let $\sigma : Y \to X$ be a birational morphism from a smooth projective curve and let Y_0 the preimage of $[1:0] \in \mathbb{P}^1$ under $f = \pi_1 \circ \sigma$ where π_1 denotes the projection onto the first factor of $\mathbb{P}^1 \times \mathbb{P}^2$. Each point of Y_0 maps to a point of $V(f, g)$ under π_2.

Dynamical intersection numbers, 3

Let $q \in Y_0$ be a point and $s \in \mathfrak{m}_{Y,q} \subset \mathcal{O}_{Y,q}$ a local generator. The rational function $t = t_1/t_0 \in \mathcal{O}_{\mathbb{P}^1,[1:0]}$ pullsback to $f = us^r$ with $r = v_q(f)$ and $u \in \mathcal{O}_{Y,q}$ a unit. For point λ with $|\lambda|$ small there are the precisely r preimage points in the holomorphic chart defined by s with absolute value approximately $(\frac{|\lambda|}{|u(0)|})^{1/r}$. For $\lambda \to 0$ the images of these points in C approach the image of $p \in C \cap D_0$ of q.

Let $p_1, \ldots, p_k$ denote the distinct points of $C \cap V(g)$. Let q_{ij} for $j = 1, \ldots d_i$ denote the distinct preimages of p_i in Y and r_{ij} denote the ramification numbers as above. Then precisely $\sum_{j=1}^{d_i} r_{ij}$ images of the points in the fiber $f^{-1}(\lambda)$ approach p_i for $\lambda \to 0$.

Dynamical intersection numbers, 4

Thus we must have

$$i(f, g; p_i) = \sum_{j=1}^{d_i} r_{ij}.$$

This identity fits with the fact that $\sum_{i=1}^{k} \sum_{j=1}^{d_i} r_{ij} = d \cdot e$ counts the number of points in the fibers of $Y \to \mathbb{P}^1$.
To prove this identity one can use that $i(f, g; p_i)$ can also be computed as the multiplicity of the resultant $\mathrm{Res}_x(f, g) \in K[y, z]$ at the point $[b_i : c_i]$ for $p_i = [a_i : b_i : c_i]$, if our coordinate system is chosen general enough. For example the $[b_i : c_i]$'s should be pairwise distinct. The resultant $\mathrm{Res}_x(f, g_\lambda)$ has precisely $\sum_{j=1}^{d_i} r_{ij}$ zeroes counted with multiplicities which approach $[b_i : c_i]$ for $\lambda \to 0$. $\square$

A bound on the number of singular points

Theorem. 1) *Let* $C \subset \mathbb{P}^2$ *be a plane curve of degree* d. *Let* $r_p = \mathrm{mult}(C;p)$ *denote the multiplicity of* C *at* p. *Then*

$$\sum_{p \in C} \binom{r_p}{2} \leq \binom{d}{2}.$$

2) *If* C *is irreducible then*

$$\sum_{p \in C} \binom{r_p}{2} \leq \binom{d-1}{2}.$$

Remark. Both bounds are sharp: A general union of d lines has $\binom{d}{2}$ double points. The image of $\mathbb{P}^1$ under a general morphism defined by forms of degree d has $\binom{d-1}{2}$ double points.

Proof of the bounds

Let $\mathrm{I}(C) = (f)$. Then f is square free and $C_{sing} = V(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z})$ is a finite set. In general coordinates f and $\frac{\partial f}{\partial x}$ have no common factor. If $p \in C$ is a point of multiplicity r_p then $\frac{\partial f}{\partial x}$ has multiplicty $\geq r_p - 1$ at p. Thus by Bézout and the bound on intersection multiplicities we have

$$\sum_{p \in C} r_p(r_p - 1) \leq d(d-1).$$

For the second case we may assume $d \geq 2$. Let $p_1, \ldots, p_s$ denote the singular points of C, and let $r_1, \ldots, r_s$ denote their multiplicity. The vector space

$$L(d-1; (r_1 - 1)p_1, \ldots, (r_s - 1)p_s)$$

has dimension $\geq \binom{d+1}{2} - \sum_{i=1}^{s} \binom{r_i}{2}$ which is at least d by the first bound.

Proof of the bounds continued

In particular $t = \binom{d+1}{2} - \sum_{i=1}^{s} \binom{r_i}{2} - 1 \geq 1$. Choose t further points $q_1, \ldots, q_t$ on C. Then

$$L(d-1; (r_1 - 1)p_1, \ldots, (r_s - 1)p_s, q_1, \ldots, q_t)$$

contains a non-zero element g. f and g have no common factor, because f is irreducible and $\deg g < d$. So they intersect only in finitely many points and Bézout gives

$$d(d-1) \geq \sum_{i=1}^{s} r_i(r_i - 1) + t.$$

Since $t = \binom{d+1}{2} - \sum_{i=1}^{s} \binom{r_i}{2} - 1 \geq 1$ this inequality is equivalent to the assertion:

$$d(d-1) - \frac{(d+1)d}{2} + 1 = \frac{1}{2}(d^2 - 3d + 2).$$

$\square$

Rational curves

Theorem. *Let $C \subset \mathbb{P}^2$ be a irreducible plane curve of degree d with points of multiplicity r_p. If*

$$\sum_{p \in C} \binom{r_p}{2} = \binom{d-1}{2}$$

then there exists a birational map $\mathbb{P}^1 \to C$.

Proof. With notation of the proof above we consider now only $t-1$ additional $q_1, \dots, q_{t-1}$. Then

$$\mathbb{P}(L(d-1; (r_1-1)p_1, \dots, (r_s-1)p_s, q_1, \dots, q_{t-1}) \cong \mathbb{P}^1$$

is pencil. The dimension cannot be larger, because otherwise we could find a curve in the which passes through 2 further point, too many for Bézout. So for every point $q \in C \setminus \{p_1, \dots, p_s, q_1, \dots, q_{t-1}\}$ there is a unique curve D in the pencil which passes through q. This defines a birational map $C \dashrightarrow \mathbb{P}^1$ whose inverse extends to a birational morphism $\mathbb{P}^1 \to C$. $\square$

Rational curves

Remark. The equality above is sufficient but not necessary for rationality.

Example. The curve $V(z^2y^3 - x^5)$ is rational but has only two singular point of multiplicity 2 and 3. So

$$\binom{4}{2} > \binom{2}{2} + \binom{3}{2}.$$

Note that in the blow-up of the affine curve $z^2 - x^5$ we get another double point $u^2 - x^3$ in the chart $(x, z) = (x, ux)$. Over the triple point $y^3 - x^5$ we find a further double point $w^3 - x^2$ under the transformation $(x, y) = (x, wx)$

Taking these singular points into account we get equality

$$6 = 1 + 3 + 1 + 1.$$

Infinitesimal near points

Let $X_2 \to X_1 \to \mathbb{P}^2$ be the blow-up of a point p followed by a blow-up of a point q on the exceptional $E_1 \subset X_1$. Then we call a points $p_1 \in E_1$ an **infinitesimal near points** to p of first order and the points $p_2 \in E_2$ in the exceptional curve of $X_2 \to X_1$ infinitesimal near points of p of second order.

So we have an infinite tree of infinitesimal near points to every point $p \in \mathbb{P}^2$.

Theorem. *Let $C \subset \mathbb{P}^2$ be an irreducible curves of degree d. Then*

$$\binom{d-1}{2} \geq \sum_p \binom{r_p}{2}$$

where the sum runs over all points of $\mathbb{P}^2$ including infinitesimal near points, and r_p denotes the multiplicity of the strict transfom at p. Equality holds if and only if C is birational to $\mathbb{P}^1$.

The genus and its toplogical interpretation

Definition. The difference $g = \binom{d-1}{2} - \sum_p \binom{r_p}{2}$ as above is called the geometric **genus** of the plane curve C.
If C is a smooth projective curve then the **genus** g **of** C is defined as the genus of a birational plane model of C.

A smooth projective curve C over the complex numbers $\mathbb{C}$ is also a Riemann surface. As differential manifold this a compact orientable surface S. Their differentiable classification depend only on the integer g. It is a handle body with g handles.

The number g can also be recovered from any triangulation of S. If we have a triangulation with c_0 vertices c_1 edges and c_2 faces of S then the topological Euler characteristic is

$$\chi(S) = c_0 - c_1 + c_2 = 2 - 2g.$$

The Hilbert polynomial of a smooth projective curve

The genus g of a smooth projective curve can also be computed from the Hilbert polynomial.

Theorem. *The Hilbert polynomial of a smooth projective curve* $C \subset \mathbb{P}^n$ *of degree* d *has the form*

$$p(t) = dt + 1 - g.$$

Corollary. *The constant term of the Hilbert polynomial* $p(t)$ *of a smooth projective curve* C *does not depend on the embedding* $C \hookrightarrow \mathbb{P}^n$.