Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today we will talk about smooth points and prove the theorem of Bertini.

1. Smooth points and the Zariski tangent space.
2. Bertini's theorem and the geometric interpretation of the degree
3. The dual variety

Differentation

Let K be arbitrary field. Differentiation in $K[x]$ can be defined without analysis.

Definition. For $f = \sum_{n\in\mathbb{N}} x^n$ we define the derivative

$$f' = \sum_{n\in\mathbb{N}} n a_n x^{n-1}.$$

The usual differentiation rules hold with one exception if $\operatorname{char} K = p > 0$:

Proposition. *Let $f, g \in K[x]$ be polynomials. Then*

1) $(f+g)' = f' + g'$,
2) $(fg)' = f'g + fg'$,
3) *If* $\operatorname{char} K = 0$ *then* $f' = 0$ *iff* $f = a_0$ *is a constant polynolmial,*
4) *If* $\operatorname{char} K = p > 0$ *then* $f' = 0 \iff f \in K[x^p]$.

Proof. 1) is clear. By 1) it suffices to prove 2) for monomials:

$$\begin{aligned}(x^{n+m})' &= (n+m)x^{n+m-1} = nx^{n-1}x^m + mx^n x^{m-1} \\ &= (x^n)'x^m + x^n(x^m)'.\end{aligned}$$

Differentation and gradient

3) and 4) are clear from the formula because $(x^{np})' = npx^{np-1} = 0$ in case of char $K = p > 0$. □

Remark. In case of a finite field or an algebraically closed field of char $K = p$ we have

$$f \in K[x^p] \iff f = g^p \text{ for some } g \in K[x]$$

because the map $K \to K, a \mapsto a^p$ is surjective.

For multivariate polynomials $f \in K[x_1, \ldots, x_n]$ partial derivatives $\frac{\partial f}{\partial x_i}$ are defined analogously. The gradient

$$(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$$

of f is identically zero in char $K = p$ iff $f \in K[x_1^p, \ldots, x_n^p]$.

Differential and tangent space

Definition. Let $f \in K[x_1, \ldots, x_n]$. We define the **differential of** f **at a point** $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ as

$$d_p f = \sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(p)(x_i - a_i).$$

In other words $d_p f$ is the linear part in the Taylor expansion

$$f = f(p) + d_p f + \text{ terms of degree } \geq 2 \text{ in the } x - a_i$$

of f.

For a hypersurface $H \subset \mathbb{A}^n$ with $\mathrm{I}(A) = (f)$ we define the **tangent space** of H at a point $p \in H$ as the linear subspace

$$T_p H = V(d_p f).$$

The tangent space of an algebraic set

Definition. Let $A \subset \mathbb{A}^n$. The tangent space of A at a point $p \in A$ is defined by

$$T_p(A) = V(\{d_p f \mid f \in \mathrm{I}(A)\}).$$

The local dimension of A at p is defined as

$$\dim_p A = \{\dim C \mid \text{ is an irreducible component of } A \text{ passing through } p\}$$

A is **smooth** at p if $\dim T_p A = \dim_p A$.

Proposition. *Let $A \subset \mathbb{A}^n$ be an algebraic set and let $f_1, \ldots, f_r \in \mathrm{I}(A)$ polynomials vanishing on A. Then*

$$n - \operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(p)\right) \geq \dim_p A$$

and A is smooth at p if equality holds.

If $i_1 < \ldots < i_k$, $j_1 < \ldots < j_k$ correspond to the indices of a maximal size non-vanishing minor of the jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}(p)\right)$ then in case of $K = \mathbb{R}$ or $\mathbb{C}$ the implicit function theorem says that one can solve the system of equations $f_{i_1} = \ldots = f_{i_k} = 0$ locally:

Jacobian criterium

One can express $x_{j_1}, \ldots, x_{j_k}$ as differentiable or holomorphic functions of the $x_j's$ with $j \notin \{j_1, \ldots, j_k\}$ respectively and every solution of $f_{i_1} = \ldots = f_{i_k} = 0$ near p arises as a point on the corresponding graph.

Proof. We have

$$n - \text{rank}(\frac{\partial f_i}{\partial x_j}(p)) \geq \dim T_p A \geq \dim_p A$$

The first inequality is true by the definition of $T_p A$. It could be strict since we did not assumed that $f_1, \ldots, f_r$ generate $\mathrm{I}(A)$. The second inequality holds in a much more general setting, which we briefly discuss below. □

Krull dimension and height

Definition. Let R be a commutative ring. A **chain of prime ideals** in R of **length** c is a chain with strict inclusions

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_c.$$

The **Krull dimension** of R is

$$\dim R = \sup\{c \mid \exists \text{ chain of prime ideals in } R \text{ of length } c\}$$

The **height** of a prime ideal $\mathfrak{q} \subset R$ is

$$\text{height}(\mathfrak{q}) = \sup\{c \mid \exists \text{ chain of prime of length } c \text{ with } \mathfrak{p}_c = \mathfrak{q}\}.$$

The **height** of an arbitrary ideal $I \subset R$ is

$$\text{height}(I) = \min\{\text{height}(\mathfrak{q}) \mid \mathfrak{q} \text{ is a prime ideal with } I \subset \mathfrak{q}\}.$$

Remark. Notice for prime ideals $\mathfrak{p} \subset R$:

$$\dim R \geq \dim R/\mathfrak{p} + \text{height}(\mathfrak{p})$$

and

$$\text{height}(\mathfrak{p}) = \dim R_{\mathfrak{p}}.$$

Krull dimension of $K[x_1, \ldots, x_n]$

Proposition. $\dim K[x_1, \ldots, x_n] = n$.

Proof. $(0) \subsetneq (x_1) \subsetneq \ldots \subsetneq (x_1, \ldots, x_k) \subsetneq \ldots \subsetneq (x_1, \ldots, x_n)$ is a chain of prime ideals of length n. Thus $\dim K[x_1, \ldots, x_n] \geq n$. To see equality we note that we obtained

$$\mathfrak{p} \subset \mathfrak{q} \text{ and } \dim V(\mathfrak{p}) = \dim V(\mathfrak{q}) \implies \mathfrak{p} = \mathfrak{q}$$

from the lying over theorem. Thus any chain prime ideals can have length at most $n = \dim \mathbb{A}^n$. □

Corollary. $\dim K[A] = \dim A$ *holds for algebraic subsets* $A \subset \mathbb{A}^n$.

More efforts are needed to prove that any maximal chain of prime ideals in $K[x_1, \ldots, x_n]$, i.e., a chain which cannot be made longer by inserting a prime ideal, has length precisely n. The key is the so called refined version of the Noether normalisation. As a corollary we obtain for varieties

Theorem. *Every maximal chain of prime ideals in the coordinate ring of affine variety* $K[C]$ *has length* $\dim C$.

Dimension of the local ring

Corollary. *Let $A \subset \mathbb{A}^n$ be an algebraic set. Then*

$$\dim A_p = \dim \mathcal{O}_{A,p}.$$

Proof. Prime ideals in $\mathcal{O}_{A,p}$ correspond to prime ideals on $K[A]$ contained in the maximal ideal $\mathfrak{m}_A$ corresponding to p. Hence a maximal chain in $\mathcal{O}_{A,p}$ correspond to a chain

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_c$$

in $K[x_1, \ldots, x_n]$ with $\mathrm{I}(A) \subset \mathfrak{p}_0$ a minimal prime of $\mathrm{I}(A)$ and $\mathfrak{p}_c = \mathfrak{m} = \mathrm{I}(p)$. So $C = V(\mathfrak{p}_0)$ is an irreducible component of A passing through p and the chain above corresponds to the chain

$$(0) \subsetneq \mathfrak{p}_1/\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{m}/\mathfrak{p}_0$$

in $K[C]$ which has length $\dim K[C] = \dim C$ by the theorem. □

Krull's principal ideal theorem

Theorem. *Let R be a noetherian ring. Every minimal prime $\mathfrak{p}$ of a principal ideal $(f) \subset R$ has height*

$$\operatorname{height}(\mathfrak{p}) \leq 1.$$

Equality holds if f is a non-zero divisor. More generally, if $\mathfrak{p}$ is a minimal prime of an ideal $(f_1, \ldots, f_c) \subset R$ generated by c elements, then

$$\operatorname{height}(\mathfrak{p}) \leq c.$$

Corollary. *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring. Then*

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 \geq \dim R.$$

Proof. By Nakayama's Lemma $\mathfrak{m}$ is generated by $c = \dim_k \mathfrak{m}/\mathfrak{m}^2$ elements. Since $\mathfrak{m}$ is the unique maximal ideal of R we obtain

$$\dim R = \operatorname{height}(\mathfrak{m}) \leq c$$

from the principal ideal theorem. □

Regular local rings

Definition. A **regular local** ring is noetherian local ring $(R, \mathfrak{m}, k)$ with $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim R$.

Proposition. *A point $p \in A$ of an algebraic set $A \subset \mathbb{A}^n$ is a smooth point of A iff $\mathcal{O}_{A,p}$ is a regular local ring.*

Proof. Since $n - \mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2$ is the codimension of $T_p(A)$ we have $\dim T_p A = \dim A_p$ iff $\mathcal{O}_{A,p}$ is a regular local ring. □

The K-vector space $\mathfrak{m}_{A,p}/m_{a,p}^2$ can be interpreted as the vector space of linear functions on $T_p(A)$ regarded as a K-vector space with origin p. Thus the dual vector space $(\mathfrak{m}_{A,p}/\mathfrak{m}_A^2)^* \cong T_p(A)$ is called the **Zariski tangent space** of A at p. Points $p \in A$ where A is not smooth are called **singular points of** A.

Example. Let $H \subset \mathbb{A}^n$ be a hypersurface and $(f) = \mathrm{I}(A)$ be its ideal in $K[x_1, \ldots, x_n]$. Then the set of singular points is

$$H_{sing} = V(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}).$$

Singular points

Notice that $(f) = (f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$ holds iff $\frac{\partial f}{\partial x_1} = 0, \ldots, \frac{\partial f}{\partial x_n} = 0$ since the partial derivative $\frac{\partial f}{\partial x_i}$ has smaller degree in x_i than f. Thus $(f) = (f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$ implies that $\operatorname{char} K = p$ and $f \in K[x_1^p, \ldots, x_n^p]$. For K algebraically closed this gives $f = g^p$ contradicting that f is square free. Thus we have

Proposition. *The set of smooth points of a reduced hypersurface $H \subset \mathbb{A}^n$ is a Zariski open dense subset of H.*

Theorem. *Let $A \subset \mathbb{A}^n$ be a affine variety. Then the set smooth points of A is a Zariski open dense subset of A.*

Singular points

Proof. One can show that every variety is birational to a hypersurface H. In case of $\operatorname{char} K = 0$ this follows from the existence of a primitive elements for the field extensions $K(x_{n-d+1}, \ldots, x_n) \subset K(A)$ where $A \to \mathbb{A}^d$ is a suitable linear projection. In positive characteristic the construction of the birational morphism is more complicated.
For points p in the open set $U \subset A$, which is isomorphic an open set of H we have

$$\mathcal{O}_{A,p} \cong \mathcal{O}_{H,p}$$

and the result follows from the proposition. □

In case of projective varieties $X \subset \mathbb{P}^n$ one defines singular points the same way. The **embedded tangent space** $T_p(X)$ is defined as the projective closure of $T_p(X \cap U_i) \subset U_i \cong \mathbb{A}^n$ in $\mathbb{P}^n$.
Notice that $T_p(X) \cong \mathbb{P}^d$ is a linear subspace of dimension $d = \dim X$ at smooth points p of X.

The dual projective space

Definition. Let $\mathbb{P}^n$ be a projective space. Then the projective space of hyperplanes $H \subset \mathbb{P}^n$ is a called the **dual projective space**

$$\check{\mathbb{P}}^n = \{H \subset \mathbb{P}^n \mid H \text{ is a hyperplane}\}.$$

Remark. For a point $p \in \mathbb{P}^n$ the space of hyperplanes passing through p

$$H_p = \{H \in \check{\mathbb{P}} \mid p \in H\} \subset \check{\mathbb{P}}^n$$

is a hyperplane in $\check{\mathbb{P}}^n$ and any hyperplane in $\check{\mathbb{P}}^n$ arizes this way: The subvariety

$$\mathbb{F} = V(a_0x_0 + \ldots + a_nx_n) \subset \mathbb{P}^n \times \check{\mathbb{P}}^n$$

can be interpreted in two way

$$\mathbb{F} = \{(p, H) \in \mathbb{P}^n \times \check{\mathbb{P}}^n \mid p \in H\} = \{(p, H) \in \mathbb{P}^n \times \check{\mathbb{P}}^n \mid H \in H_p\}$$

The fibers of the projection $\mathbb{F} \to \check{\mathbb{P}}^n$ onto the second factor are hyperplanes in $\mathbb{P}^n$ and the fibers of the projection to the first factor $\mathbb{F} \to \mathbb{P}^n$ are hyperplanes in $\check{\mathbb{P}}^n$.

Bertini's theorem

Theorem. *Let $X \subset \mathbb{P}^n$ be a projective variety of dimension d. Let X_{sing} denote its set of singular points. There exists an non-empty open subset $U \subset \check{\mathbb{P}}^n$ of hyperplanes such that $X \cap H$ is smooth outside $X_{sing} \cap H$ for every $H \in U$.* In particular if X is smooth then $X \cap H$ is smooth as well for all $H \in U$.

Proof. Consider the open set $X^* = X \setminus X_{sing}$ of smooth point of X and the variety

$$\begin{array}{ccc} D^* = \{(p, H) \in X^* \times \check{\mathbb{P}}^n \mid T_p X \subset H\} & \longrightarrow & \check{\mathbb{P}}^n \\ \Big\downarrow{\scriptstyle \pi_1} & & \\ X^* & & \end{array}.$$

with its two projections. A point $(p, H) \in D^*$ is pair such that $X \cap H$ is singular in p.

Proof of Bertini's theorem

The fiber of $\pi_1 : D^* \to X^*$ over a point $p \in X^*$ is a projective space of dimension $n - d - 1$

$$\{H \subset \mathbb{P}^n \mid H \supset T_p(X)\} \cong \mathbb{P}^{n-d-1}$$

because H is contained in the fiber iff H is defined by a linear combination of the $n - d$ equations of $T_pX \cong \mathbb{P}^d \subset \mathbb{P}^n$.
Thus $\dim D^* = d + n - d - 1 = n - 1$. We take

$$D = \overline{D^*} \subset X \times \check{\mathbb{P}}^n \subset \mathbb{P}^n \times \check{\mathbb{P}}^n.$$

Then $\dim D = \dim D^*$ and the projection $\pi_2(D) \subset \check{\mathbb{P}}^n$ is a Zariski closed subset of dimension

$$\dim \pi_2(D) \leq \dim D = n - 1$$

and $U = \check{\mathbb{P}}^n \setminus \pi_2(D)$ is the desired open subset. □

Geometric interpretation of the degree

Theorem. *Let $X \subset \mathbb{P}^n$ be a projective variety of dimension d. Then a general linear subspace $\mathbb{P}^{n-d}$ intersects X in $\deg X$ many distinct points transversally.*

Proof. Let $H \subset \mathbb{P}^n$ be a general hyperplane. In particular H does not contain any component of X_{sing}. Let $C_1 \cup \ldots \cup C_r = X \cap H$ be the irreducible components. Then

$$\deg X = \sum_{j=1}^{r} i(X, H; C_j) \deg C_j$$

holds by Bézout's theorem. By Bertini's theorem the intersection is smooth. In particular the intersection is transversal at smooth points of each C_j and the intersection multiplicity is 1. The result follows now by induction. A general complimentary $\mathbb{P}^{n-d}$ is the intersection of d general hyperplanes $H_1 \cap \ldots \cap H_d$ such that H_i intersects each component of $X \cap H_1 \cap \ldots \cap H_{i-1}$ transversally. $\square$

The dual variety

Remark. Actually the intersection $X \cap H$ is irreducible and $X \cap \mathbb{P}^{n-d+1}$ is an irreducible smooth curve.

Definition. $\check{X} = \pi_2(D)$ is called the **dual variety** of X.

For $C \subset \mathbb{P}^2$ an irreducible curve which is not a line, the dual variety is again a curve $\check{C} \subset \check{\mathbb{P}}^2$.

Theorem. *Let $C \subset \mathbb{P}^2$ be irreducible curve over a field of characteristic 0. Then the double dual curve*

$$\check{\check{C}} = C$$

gives the original curve back.

Theorem of Brianchon

Theorem. *The three diagonals of a hexagon which is circumscribed around a conic intersect in a point*

This theorem follows via duality from Pascal's theorem.

Plücker's research