Algebraic Geometry, Lecture 17

Frank-Olaf Schreyer

Saarland University, Perugia 2021

Overview

Mora's division theorem

The proof of Grauert's division theorem does not yield an algorithm because the iteration usually does not terminate. For ideals of $K[x_1,\dots,x_n]_{(x_1,\dots,x_n)} \subset K[[x_1,\dots,x_n]]$ their exists an algorithm to compute a Gröbner basis. Without loss of generality we may assume that an ideal $I \subset K[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$ is generated elements of $K[x_1,\dots,x_n]$, since the denominators are units in $K[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$.

Theorem. *Let $>$ be a local monomial order and let $f_1,\dots,f_r \in K[x_1,\dots,x_n]$. For every further element $g \in K[x_1,\dots,x_n]$ there exists an element $u \in K[x_1,\dots,x_n]$ with $u(0)=1$, elements $g_1,\dots,g_r \in K[x_1,\dots,x_n]$ and a remainder $h \in K[x_1,\dots,x_n]$ such that the following holds:*

1) $ug = g_1f_1 + \ldots + g_rf_r + h$.

2a) $\mathrm{Lt}(g) \geq \mathrm{Lt}(g_if_i)$ *whenever both sides are non-zero.*

2b) *If $h \neq 0$, then $\mathrm{Lt}(h)$ is not divisible by any $\mathrm{Lt}(f_i)$.*

Mora's algorithm

Definition. Let $>$ be a monomial order. The **ecart** of a non-zero element $f \in K[x_1, \ldots, x_n]$ is

$$\mathrm{ecart}(f) = \deg f - \deg \mathrm{Lt}(f).$$

Algorithm.

Input. A local monomial order $>$, polynomials $f_1, \ldots, f_r$ and g

Output. A remainder h of a Mora division of g by $f_1, \ldots, f_r$.

1. Set $h := g$ and $D := \{f_1, \ldots, f_r\}$.
2. **while** $(h \neq 0$ **and** $D(h) := \{f \in D \mid \mathrm{Lt}(f) \text{ divides } \mathrm{Lt}(h)\} \neq \emptyset)$ **do**
   - Choose $f \in D(h)$ with $\mathrm{ecart}(f)$ minimal.
   - **if** $\mathrm{ecart}(f) > \mathrm{ecart}(h)$ **then** $D := D \cup \{f\}$.
   - $h := h - \frac{\mathrm{Lt}(h)}{\mathrm{Lt}(f)} f$.
3. return h.

Termination of Mora's algorithm

We write h_k and D_k for the value of h and D after k iterations of the while loop. Let x_0 be a further variable. After k iterations the while loop continues iff $\mathrm{Lt}(h_k) \in (\{\mathrm{Lt}(f) \mid f \in D_k\} \subset K[x_1, \ldots, x_n]$ and h_k is added to D_k iff

$x_0^{\mathrm{ecart}(h_k)} \mathrm{Lt}(h_k) \notin I_k := (\{x_0^{\mathrm{ecart}(f)} \mathrm{Lt}(f) \mid f \in D_k\}) \subset K[x_0, x_1, \ldots, x_n]$.

Since the chain of monomial ideals

$$I_0 \subset I_1 \subset \ldots \subset I_k \subset \ldots \subset K[x_0, \ldots, x_n]$$

becomes stationary, there exists an N such that

$$D_N = D_{N+1} = D_{N+2} = \ldots$$

no longer increases.

After this point we homogenize h_N and the elements of D_N with x_0.

Termination of Mora's algorithm continued

$$f^h = x_0^{\deg f} f(x_1/x_0, \ldots, x_n/x_0)$$

has lead term $\mathrm{Lt}(f^h) = x_0^{\mathrm{ecart}(f)}\,\mathrm{Lt}(f)$ with respect to the monomial order $>_g$ on $K[x_0, \ldots, x_n]$ defined by

$$\begin{aligned} x_0^a x^\alpha >_g x_0^b x^\beta \Leftrightarrow\ & \deg x_0^a x^\alpha > \deg x_0^b x^\beta \text{ or} \\ & \deg x_0^a x^\alpha = \deg x_0^b x^\beta \text{ and } x^\alpha > x^\beta. \end{aligned}$$

Since D_N does not change after this point, we get a sequence

$$(h_k^h)_{k \geq N}$$

of homogeneous elements of the same degree with lead terms

$$\mathrm{Lt}(h_N^h) = x_0^{\mathrm{ecart}(h_N)}\,\mathrm{Lt}(h_N) >_g \mathrm{Lt}(h_{N+1}^h) >_g \ldots.$$

After finitely many further steps the algorithm stops with an $h_M = 0$ or an h_M with $\mathrm{Lt}(h_M) \notin (\{\mathrm{Lt}(f) \mid f \in D_N\})$, since there are only finitely many monomials in $K[x_0, \ldots, x_n]$ of the same degree.

Correctness of the output.

Recursively, starting with $u_0 = 1$, $g_i^{(0)} = 0$ and $h_0 = g$ suppose that we already have expressions

$$u_\ell g = g_1^{(\ell)} f_1 + \ldots + g_r^{(\ell)} f_r + h_\ell \quad \text{with } u_\ell(0) = 1$$

for $\ell = 0, \ldots, k-1$. Then, if the test condition for the k-th iteration of the while loop is fulfilled, choose a polynomial $f = f^{(k)}$ as in the algorithm and set

$$h_k = h_{k-1} - m_k f^{(k)} \text{ where } m_k = \frac{\mathrm{Lt}(h_{k-1})}{\mathrm{Lt}(f^{(k)})}.$$

There are two possibilities

(a) $f^{(k)}$ is one of $f_1, \ldots, f_r$ or

(b) $f^{(k)}$ is one of $h_1, \ldots, h_{k-1}$.

Thus substituting $h_{k-1} = h_k + m_k f^{(k)}$ into the expression for $u_{k-1}g$ we obtain the desired expression for $u_k g$ with

(a) $u_k = u_{k-1}$ and $g_j^{(k)} = g_j^{(k-1)} + m_k$ if $f^{(k)} = f_j$ or

(b) $u_k = u_{k-1} + m_k u_\ell$ for some ℓ and $g_j^{(k)} = g_j^{(k-1)} + m_k g_j^{(\ell)}$ $\forall j$

Correctness of the output continued

In both cases we have $u_k(0) = u_{k-1}(0) = 1$. In case (b) this follows from

$$\mathrm{Lt}(h_\ell) > \mathrm{Lt}(h_k) = \mathrm{Lt}(m_k h_\ell) = m_k \, \mathrm{Lt}(h_\ell).$$

Hence $1 > m_k$ and $u_k(0) = u_{k-1}(0) + 0u_\ell(0) = 1$.

The final expression satisfies condition 2a) because the lead terms of the h_k decrease in each round of the while loop. Finally, condition 2b) is satisfied due to the stopping condition of the while loop. $\square$

Example. Consider $g = x$ and $f_1 = x - x^2$ in $K[x]$. Mora division proceeds as follows:

$$h_0 = x, D_0 = \{x - x^2\}, 1 \cdot g = 0 \cdot f_1 + x,$$
$$f^{(1)} = x - x^2, m_1 = 1, D_1 = \{x - x^2, x\}, 1 \cdot g = 1 \cdot f_1 + x^2,$$
$$f^{(2)} = x, m_2 = x, D_2 = D_1, (1 - x) \cdot g = 1 \cdot f_1 + 0.$$

Differentiation

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

Definition. For $f = \sum_{n\in\mathbb{N}} a_n x^n$ 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 polynomial,*
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:

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

Differentiation and gradient

3) and 4) are clear from the formula because $(x^{np})' = npx^{np-1} = 0$ in case of char $K = p > 0$, while $(x^m)' = mx^{m-1} \neq 0$ if $p \not| m$. $\square$

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 $f \in K[x_1, \dots, x_n]$. We define the **differential of** f **at a point** $p = (a_1, \dots, a_n) \in \mathbb{A}^n$ 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 $\mathrm{I}(H) = (f)$ 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 $A \subset \mathbb{A}^n$ be an algebraic set. 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

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

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.

Implicit function theorem

Remark. 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 $(\frac{\partial f_i}{\partial x_j}(p))$, 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:

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 of the Jacobian criterium

Proof. We have

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

The first inequality is true by the definition of T_pA. 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 state below. $\square$

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*

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

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

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

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

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

from the principal ideal theorem. □

Regular local rings

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

The K-vector space $\mathfrak{m}_{A,p}/m^2_{A,p}$ 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 $(\mathfrak{m}_{A,p}/\mathfrak{m}^2_{A,p})^* \cong T_p(A)$ 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 $(f) = (f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n})$ holds iff $\frac{\partial f}{\partial x_1} = 0, \dots, \frac{\partial f}{\partial x_n} = 0$ since the partial derivative $\frac{\partial f}{\partial x_i}$ has smaller degree in x_i than f. Thus $(f) = (f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n})$ implies that char $K = p$ and $f \in K[x_1^p, \dots, x_n^p]$. 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.* $\square$

Generic smoothness

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

Proof. One can show that every variety is birational to a hypersurface H. In case of char $K = 0$ this follows from the existence of a primitive element 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. □

The tangent cone

At a singular point of an algebraic set $p \in A \subset \mathbb{A}^n$ the tangent space T_pA is only a very rough approximation of A near p.
The tangent cone, as defined below, is a better approximation. We assume that $p = o \in \mathbb{A}^n$ is the origin.
Then for $I = \mathrm{I}(A) \subset K[x_1, \ldots, x_n]$ the **ideal of initial forms** of I is

$$J = (\{f_m \mid f_m \text{ is the smallest degree part of an equation } f = f_m + ... + f_d \in I\}).$$

$V(J)$ is called the **tangent cone** of A at p.
The ring $K[x_1, \ldots, x_n]/J$ is isomorphic to the associated graded ring

$$gr_{\mathfrak{m}} R = R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \ldots = \bigoplus_{k=0}^{\infty} \mathfrak{m}^k/\mathfrak{m}^{k+1}.$$

of $R = \mathcal{O}_{A,o}$ with respect to the maximal ideal $\mathfrak{m} = \mathfrak{m}_{A,o}$.

Mora's tangent cone algorithm

Algorithm.
Input. Generators of the ideal I of an affine algebraic set $A \subset \mathbb{A}^n$.
Output. Generators of the ideal of initial forms of I at o.

1. Choose a local monomial order $>$ which refines the degree:

$$\deg x^\alpha < \deg x^\beta \implies x^\alpha > x^\beta.$$

2. Compute a Gröbner basis G of I using Mora's algorithm.
3. Return the initial forms f_m of all $f = f_m + \ldots + f_d \in G$.

Hierachy of approximations

Let $R = \mathcal{O}_{A,p}$ be the local ring of an algebraic set. We have introduced the $\mathfrak{m} = \mathfrak{m}_{A,p}$-adic completion $\widehat{\mathcal{O}}_{A,p}$, the associated graded ring $gr_{\mathfrak{m}}R$ and the Zariski tangent space $T_pA = (\mathfrak{m}/\mathfrak{m}^2)^*$.

For two local rings $\mathcal{O}_{A,p}$ and $\mathcal{O}_{B,q}$ we have the following implications:

$$\begin{aligned}
\mathcal{O}_{A,p} \cong \mathcal{O}_{B,q} &\implies \widehat{\mathcal{O}}_{A,p} \cong \widehat{\mathcal{O}}_{B,q}, \\
\widehat{\mathcal{O}}_{A,p} \cong \widehat{\mathcal{O}}_{B,q} &\implies gr_{\mathfrak{m}_{A,p}}\mathcal{O}_{A,p} \cong gr_{\mathfrak{m}_{B,q}}\mathcal{O}_{B,q}, \\
gr_{\mathfrak{m}_{A,p}}\mathcal{O}_{A,p} \cong gr_{\mathfrak{m}_{B,q}}\mathcal{O}_{B,q} &\implies T_pA \cong T_qB.
\end{aligned}$$

In general none of these implications is an equivalence.

Analytically isomorphic local rings

Example. Consider $A = V(y^2 - x^2 - x^3)$ and $B = V(y^2 - x^2)$ at the origin o for $K = \mathbb{C}$.

$$\widehat{\mathcal{O}}_{A,o} \cong \widehat{\mathcal{O}}_{B,o}$$

via the ring homomorphism induced by the substitution

$$\mathbb{C}[[x,y]] \to \mathbb{C}[[x,y]], (x,y) \mapsto (x, y\sqrt{1+x}).$$

Indeed

$$\sqrt{1+x} = 1 + \frac{x}{2} - \frac{x^2}{4} + \ldots = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} x^k \in \mathbb{C}[[x]]$$

and its square $1 + x$ are units.

Definition. If $\widehat{\mathcal{O}}_{A,p} \cong \widehat{\mathcal{O}}_{B,q}$, then (A,p) and (B,q) are called **analytically isomorphic**.

Appendix: Discrete valuation rings

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 a 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 $a \in K \setminus \{0\}$.