# Algebraic Geometry, Lecture 16

Frank-Olaf Schreyer

Saarland University, Perugia 2021

# Overview

1. Local rings and the Lemma of Nakayama,
2. Completions and the ring of formal power series,
3. Grauert division and the Weierstraß preparation theorem,
4. A lower bound on intersection multiplicities.

# Local rings

**Definition.** A **local ring** is a ring $R$ which has a unique maximal ideal $\mathfrak{m}$. The field $k = R/\mathfrak{m}$ is called the **residue field** of the local ring. We write $(R, \mathfrak{m})$ or even $(R, \mathfrak{m}, k)$ if we want to specify the notation for the maximal ideal and residue field of a local ring.

**Examples**

1. Let $R$ be a ring and $\mathfrak{p}$ a prime ideal. Then the localization
$$R_{\mathfrak{p}} = \{\frac{g}{h} \mid h \notin \mathfrak{p}\}$$
is a local ring with maximal ideal
$$\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}} = \{\frac{g}{h} \mid g \in \mathfrak{p}, h \notin \mathfrak{p}\}$$
and residue field
$$R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong Q(R/\mathfrak{p})$$
the quotient field of the integral domain $R/\mathfrak{p}$.
2. $\mathcal{O}_{\mathbb{A}^n,o} = K[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$ has a residue field isomorphic to $K$.

In general the residue field $R/\mathfrak{m}$ is not a subring of $R$.

# Lemma of Nakayama

A local noetherian ring $(R, \mathfrak{m})$ is easier to handle than general rings since every element $f \notin \mathfrak{m}$ is a unit in $R$

**Lemma.** *Let $(R, \mathfrak{m})$ be a local noetherian ring and let $N \subset M$ be a submodule of a finitely generated $R$-module $M$. Then*

$$N + \mathfrak{m}M = M \text{ iff } N = M.$$

**Proof.** By replacing $M$ by $M/N$ we reduce to the case $N = 0$. So we have to prove $\mathfrak{m}M = M \implies M = 0$. The other direction is trivial. Let $m_1, \dots, m_r$ be generators of $M$. Since $\mathfrak{m}M = M$ we find expressions

$$m_i = \sum_{j=1}^{r} g_{ij} m_j \text{ with } g_{ij} \in \mathfrak{m}.$$

In matrix notation

$$(E - B) \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = 0 \text{ with } B = (g_{ij}).$$

# Proof of Nakayama's Lemma continued

Multiplying the matrix equation with the cofactor matrix of $E - B$ yields $\det(E - B)m_i = 0$ for all $i$. Since $\det(E - B) \equiv 1 \mod \mathfrak{m}$ the determinant is a unit. Hence $m_i = 0$ for all $i$ and $M = 0$. $\square$

**Corollary.** *Let $(R, \mathfrak{m}, k)$ be a local ring and let $m_1, \ldots, m_r \in M$ be elements of a finitely generated $R$-module $M$. Then $m_1, \ldots, m_r$ generate $M$ iff $\overline{m}_1, \ldots, \overline{m}_r$ span the $k$-vector space $M/\mathfrak{m}M$.*

**Proof.** We consider the submodule $N = Rm_1 + \ldots + Rm_r \subset M$.

$$N + \mathfrak{m}M = M$$

holds iff $\overline{m}_1, \ldots, \overline{m}_r \in M/\mathfrak{m}M$ generate $M/\mathfrak{m}M$. Since $M/\mathfrak{m}M$ is a $k = R/\mathfrak{m}$-vector space, the result follows. In particular, any **minimal set of generators** has precisely $\dim_k M/\mathfrak{m}M$ elements. $\square$

# Krull' intersection theorem

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

$$\bigcap_{i=1}^{\infty} \mathfrak{m}^i = (0).$$

**Proof.** Consider the subring

$$S = R[\mathfrak{m}t] = R \oplus \mathfrak{m}t \oplus \mathfrak{m}^2 t^2 \oplus \ldots \subset R[t].$$

Since $\mathfrak{m}$ is finitely generated ideal in $R$, $S$ is a finitely generated $R$-algebra, hence noetherian as well. Consider now $J = \bigcap_{i=1}^{\infty} \mathfrak{m}^i$ and the ideal

$$J \oplus Jt \oplus Jt^2 \oplus \ldots \subset S$$

is generated by finitely many homogeneous elements. Let $r$ be the maximal degree of a generator. Then

$$\mathfrak{m}tJt^r = Jt^{r+1}$$

Thus $\mathfrak{m}J = J$ and $J = 0$ follows from Nakayma's Lemma. $\square$

# Formal power series

We want to compute in $\mathcal{O}_{\mathbb{A}^n,o} = K[x_1,\ldots,x_n]_{(x_1,\ldots,x_n)}$. As a first step we regard $\mathcal{O}_{\mathbb{A}^n,o}$ as a subring of the formal power series ring

$$K[[x_1,\ldots,x_n]] = \{f = \sum_{\alpha\in\mathbb{N}^n} f_\alpha x^\alpha\}.$$

The product $f = \sum_{\alpha\in\mathbb{N}^n} f_\alpha x^\alpha$ of two elements $g = \sum_{\beta\in\mathbb{N}^n} g_\beta x^\beta$ and $h = \sum_{\gamma\in\mathbb{N}^n} g_\gamma x^\gamma \in K[[x_1,\ldots,x_n]]$ is well-defined since the sum

$$f_\alpha = \sum_{\beta+\gamma=\alpha} g_\beta h_\gamma$$

is finite.

Every fraction $f \in \mathcal{O}_{\mathbb{A}^n,o}$ may be written in the form $f = \frac{g}{1-h}$ with $h \in (x_1,\ldots,x_n)$. We embed

$$\mathcal{O}_{\mathbb{A}^n,o} \hookrightarrow K[[x_1,\ldots,x_n]], \frac{g}{1-h} \mapsto g\sum_{k=0}^{\infty} h^k$$

To make sense out of the infinite sum $\sum_{k=0}^{\infty} h^k \in K[[x_1,\ldots,x_n]]$ we need a bit of topology.

# The $\mathfrak{m}$-adic topology

**Definition.** Let $R$ be a ring and $\mathfrak{m} \subset R$ an ideal. We define a system of open neighbarhoods of $0 \in R$ as the subsets $\mathfrak{m}^k \subset R$. A sequence of $(a_n)$ of elements of $R$ **converges in the $\mathfrak{m}$-adic topology** to an element $a \in R$ if

$$\forall k \in \mathbb{N} \; \exists n_0 \in \mathbb{N} \text{ such that } a_n - a \in \mathfrak{m}^k \; \forall n \geq n_0 \text{ holds.}$$

A sequence $(a_n)$ is a **Cauchy sequence** with respect to the $\mathfrak{m}$-adic topology if

$$\forall k \in \mathbb{N} \; \exists n_0 \in \mathbb{N} \text{ such that } a_m - a_n \in \mathfrak{m}^k \; \forall m, n \geq n_0 \text{ holds.}$$

$R$ is **Hausdorff** with respect to the $\mathfrak{m}$-adic topology if $\cap_{k=1}^{\infty} \mathfrak{m}^k = 0$. $R$ is **complete** with respect to the $\mathfrak{m}$-adic topology, if $R$ is Hausdorff and every Cauchy sequence converges.

# Completions

**Definition.** For a ring $R$ and the $\mathfrak{m}$-adic topology the quotient ring

$$\hat{R} = \{\text{Cauchy sequence}\}/\{\text{zero sequences}\}$$

is called the $\mathfrak{m}$-**adic completion**. This is a ring since the set of zero-sequences is an ideal in the term wise defined ring of Cauchy sequences. The map

$$R \to \hat{R},\ a \mapsto [\text{constant sequence } (a)]$$

is a ring homomorphism, which is injective if and only if $\bigcap_{k=1}^{\infty} \mathfrak{m}^k = 0$. $\hat{R}$ is always complete with respect to the $\hat{\mathfrak{m}} = \mathfrak{m}\hat{R}$-adic topolology.

Thus we may regard $K[[x_1, \dots, x_n]]$ as the completion of the polynomial ring $K[x_1, \dots, x_n]$ with respect to the $(x_1, \dots, x_n)$-adic topology and

$$f = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha = \lim_{d \to \infty} \sum_{\alpha : |\alpha| \le d} f_\alpha x^\alpha.$$

$R = K[[x_1, \ldots, x_n]]$ is a local ring. Its maximal ideal is $\mathfrak{m} = (x_1, \ldots, x_n)$. Indeed every element $u \notin \mathfrak{m}$ has the form $u = \lambda(1 - h)$ with $h \in \mathfrak{m}$ and $\lambda \in K^*$ and

$$u^{-1} = \lambda^{-1} \sum_{k=0}^{\infty} h^k$$

since this series converges by the following proposition.

**Proposition.** *Let $(h_k)$ be a sequence of power series. Then $\sum_{k=0}^{\infty} h_k$ converges iff the sequence $(h_k)$ is a $\mathfrak{m}$-adic zero sequence.* □

Thus every $u \notin \mathfrak{m}$ is a unit.

Formal power series cannot be evaluated at points $p \neq 0$. For the origin the value $f(0) \in K \cong K[[x_1, \ldots, x_n]]/\mathfrak{m}$ is given by the constant term.

# Lead terms of power series

**Definition.** Let $>$ be a **local monomial order** on $K[x_1, \dots, x_n]$, i.e., $1 > x_i\ \forall i$. The lead term of a non-zero power series $f = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha$ with respect to $>$ is the term

$$\mathrm{Lt}(f) = f_\beta x^\beta$$

where $x^\beta = \max\{x^\alpha \mid f_\alpha \neq 0\}$. This well defined because $x^\beta$ is one of the finitely many generators of the monomial ideal $(\{x^\alpha \mid f_\alpha \neq 0\}) \subset K[x_1, \dots, x_n]$ since $>$ is a local monomial order. We set $Lt(0) = 0$.

# Grauert division

Let $P = K[[x_1, \ldots, x_n]]$ denote the power series ring.

**Theorem.** *Let $>$ be a local monomial order, and let $f_1, \ldots, f_r \in P$ be non-zero power series. For every $f \in P$ there exists unique power series $g_1, \ldots, g_r \in P$ and a remainder $h \in P$ such that the following holds:*

1) $f = g_1 f_1 + \ldots + g_r f_r + h$ *and*

2a) *No term of $g_i Lt(f_i)$ is divisible by $\mathrm{Lt}(f_j)$ for for $j < i$.*

2b) *No term of $h$ is divisible by an $\mathrm{Lt}(f_i)$.*

**Proof.** Uniqueness follows as before because all non-zero lead terms $\mathrm{Lt}(g_i f_i) = \mathrm{Lt}(g_i)\,\mathrm{Lt}(f_i)$ and $\mathrm{Lt}(h)$ have different monomial parts. For the existence, we note that the result is trivially true in case $f_1, \ldots, f_r$ are monomials. Thus there exists a unique expression

$$f = f^{(0)} = g_1^{(0)}\,\mathrm{Lt}(f_1) + \ldots + g_r^{(0)}\,\mathrm{Lt}(f_r) + h^{(0)}$$

satisfying condition 2a) and 2b).

# Proof of the Grauert division theorem continued

Define

$$f^{(1)} = f^{(0)} - (g_1^{(0)} f_1 + \ldots + g_r^{(0)} f_r + h^{(0)}).$$

and write similarly

$$f^{(1)} = g_1^{(1)} \operatorname{Lt}(f_1) + \ldots + g_r^{(1)} \operatorname{Lt}(f_r) + h^{(1)}.$$

Iterating we obtain sequences $(f^{(k)}), (g_1^{(k)}), \ldots, (g_r^{(k)})$ and $(h^{(k)})$ of power series. Define

$$g_i = \sum_{k=0}^{\infty} g_i^{(k)} \text{ and } h = \sum_{k=0}^{\infty} h^{(k)}.$$

and the existence follows if we can prove that the sequences are zero sequences in the $\mathfrak{m}$-adic topology. It suffices to proof that $(f^{(k)})$ is a $\mathfrak{m}$-adic zero sequence.

# Proof of the Grauert division theorem continued

Clearly we have

$$\mathrm{Lt}(f^{(0)}) > \mathrm{Lt}(f^{(1)}) > \ldots > \mathrm{Lt}(f^{(k)}) > \ldots$$

This does not implies that $f^{(k)}$ is a $\mathfrak{m}$-adic zero sequence. However in case that $>$ is a weight order $>_w$ with strictly negative weights $(w_1, \ldots, w_n)$ then $\lim_{k\to\infty} \mathrm{Lt}(f^{(k)}) = 0$ implies $\lim_{k\to\infty} f^{(k)} = 0$.

To complete the proof we observe that the procedure only depends on knowing the lead terms $\mathrm{Lt}(f_i)$ and use the following fact:
**Claim.** *There exists a weight order $>_w$ with strictly negative weights such* $\mathrm{Lt}_{>_w}(f_i) = \mathrm{Lt}_{>}(f_i)$ *coincides for the finitely many power series $f_1, \ldots, f_r$.*

We leave the proof of this claim as an exercise. $\square$
**Remark.** In case of $K = \mathbb{C}$ perturbing the local order to a weight order is also a key to the Theorem of Grauert, which says that if $f_1, \ldots, f_r \in \mathbb{C}[[x_1, \ldots, x_n]]$ and $f$ are convergent power series then $g_1, \ldots, g_r$ and $h$ are convergent series as well.

# Lead ideal and Gröbner basis in case of $K[[x_1, \dots, x_n]]$

**Definition.** Let $I \subset K[[x_1, \dots, x_n]]$ be an ideal. Then

$$\mathrm{Lt}(I) = (\{\mathrm{Lt}(f) \mid f \in I\})$$

is called the **lead ideal** of $I$. $\mathrm{Lt}(I)$ is finitely generated, since it is a monomial ideal.

**Corollary.** *If $f_1, \dots, f_r \in I \subset K[[x_1, \dots, x_n]]$ are elements such that $(\mathrm{Lt}(f_1), \dots, \mathrm{Lt}(f_r)) = \mathrm{Lt}(I)$ then $I = (f_1, \dots, f_r)$. In particular $K[[x_1, \dots, x_n]]$ is noetherian.* $\square$

**Corollary.** *The monomials $x^\alpha \notin \mathrm{Lt}(I)$ represent a linearly independent elements of $K[[x_1, \dots, x_n]]/I$, which are dense in the $\mathfrak{m}$-adic topology. If $\dim_K K[[x_1, \dots, x_n]]/I < \infty$ then these elements represent a basis.* $\square$

The definition of a Gröbner basis and a version of Buchberger's criterium work as before.

# The Weierstraß preparation theorem

**Definition.** A power series $f \in K[[x_1, \ldots, x_n]]$ is called $x_1$-**general**, if $f(x_1, 0, \ldots, 0) \in K[[x_1]]$ is non-zero.

**Example.** Let $>$ be a local monomial order. If $f \in K[[x_1, \ldots, x_n]]$ is a power series with $\mathrm{Lt}(f) = ax_1^m$, then $f$ is $x_1$-general. Conversely, for a $x_1$-general power series $f$ there exists a local monomial order such that $\mathrm{Lt}(f) = ax_1^m$.

**Theorem.** *Let $f \in K[[x_1, \ldots, x_n]]$ be a $x_1$-general power series. Then there exists a unit $u \in K[[x_1, \ldots, x_n]]$ and a monic polynomial $p \in K[[x_2, \ldots, x_n]][x_1] \subset K[[x_1, \ldots, x_n]]$ such that*

$$f = up.$$

**Remark.** The original Weierstraß preparation theorem is the case when $K = \mathbb{C}$ and when $f$ is a convergent power series. In that case $u$ and the coefficients of $p$ are convergent power series as well.

# Proof of the Weiserstraß preparation theorem

**Proof.** Let $>$ be a local monomial order such that $\mathrm{Lt}(f) = ax_1^m$ Grauert division of $x_1^m$ by $f$ yields an expression

$$x_1^m = gf + r$$

where $r \in K[[x_2, \dots, x_n]][x_1]$ is a polynomial of degree $< m$ in $x_1$. Since $x_1^m = \mathrm{Lt}(gf) = \mathrm{Lt}(g)\,\mathrm{Lt}(f)$ we have $\mathrm{Lt}(g) = a^{-1} \in K$. Hence $g$ is a unit in $K[[x_1, \dots, x_n]]$ and

$$f = u(x_1^m - r) \quad \text{with } u = g^{-1}$$

is the desired expression. □

**Corollary.** *Let $I = (f) \subsetneq K[[x_1, \dots, x_n]]$ a non-zero ideal. Then after a linear change of coordinates,*

$$K[[x_2, \dots, x_n]] \subset K[[x_1, \dots, x_n]]/(f)$$

*is an integral ring extension.*

**Corollary.** $\dim K[[x_1, \dots, x_n]] = n$.

# A lower bound on intersection multiplicities

**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*

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

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

**Proof.** We choose the local monomial order defined by

$$\begin{aligned} x^\alpha > x^\beta \Leftrightarrow \deg x^\alpha &< \deg x^\beta \text{ or} \\ \deg x^\alpha &= \deg x^\beta \text{ and } x^\alpha >_{\mathrm{rlex}} x^\beta. \end{aligned}$$

Let $\operatorname{mult}_o(f) = m \leq \operatorname{mult}_o(g) = n$. So $f = f_m + \ldots + f_d$ and $g = g_n + \ldots + g_e$. We first assume that $V(f)$ and $V(g)$ have no common factor. Then after a linear change of coordinates and adjusting of the leading coefficient we may assume that $\operatorname{Lt}(f) = x^m$ and after we replace $g$ by an $g_1 = \lambda(g - hf)$ with $\lambda \in K^*$ that $\operatorname{Lt}(g_1) = x^{a_1} y^{b_1}$ with $a_1 + b_1 = n$ and $a_1 < m$.

Taking the remainder of $x^{n-a_1}g - y^{b_1}f$ leads to a new Gröbner basis element $g_2$ with lead term $\mathrm{Lt}(g_2) = x^{a_2}y^{b_2}$ with $a_2 < a_1$ whose degree is $a_2 + b_2 \geq m + b_1$.

After finitely many steps our stair must reach the $y$-axes with a monomial $y^{b_r}$.

If $f_m$ and $g_n$ have no common factor then the new lead terms always have degree $a_{k+1} + b_{k+1} = a_{k-1} + b_k$, i.e., lie on the corresponding diagonal. An elementary argument shows that the area under the stair has size $m \cdot n$.

Thus $i(f, g; o) = m \cdot n$ in this case.

An elementary argument shows that the area under the stair has size $m \cdot n$.

Thus $i(f, g; o) = m \cdot n$ in this case.

On the other hand if $f_m$ and $g_n$ have a common factor then the stair for $f_m$ and $g_n$ ends before it reaches the $y$-axes. Hence the stair for $f$ and $g$ which reaches the $y$-axes has a strictly larger area. $\square$