

18.705 Commutative Algebra

Lecture 5

Andrew V. Sutherland

Adapted from the [2018 lecture notes](#) of Jack Jeffries (§3.2-5)

September 24, 2026

Fibers of maps on spectra

Definition

Let $\varphi: R \rightarrow S$ be a ring map and $\mathfrak{p} \in \operatorname{Spec}(R)$. The **fiber ring** of φ over $\mathfrak{p}$ is $\kappa_{\varphi}(\mathfrak{p}) := \varphi(R \setminus \mathfrak{p})^{-1}(S/\varphi(\mathfrak{p})S)$, obtained by killing $\varphi(\mathfrak{p})$ and inverting $\varphi(R \setminus \mathfrak{p})$.

Proposition

$S \rightarrow \kappa_{\varphi}(\mathfrak{p})$ induces a homeomorphism from $\operatorname{Spec}(\kappa_{\varphi}(\mathfrak{p}))$ onto the fiber $(\varphi^*)^{-1}(\mathfrak{p})$.

Proof: $\operatorname{Spec}(S/\varphi(\mathfrak{p})S) \rightarrow \operatorname{Spec}(S)$ is a homeomorphism onto $\{\mathfrak{q} : \varphi^{-1}(\mathfrak{q}) \supseteq \mathfrak{p}\}$, and localizing at $\varphi(R \setminus \mathfrak{p})$ then picks out the $\mathfrak{q}$ with $\varphi^{-1}(\mathfrak{q}) \subseteq \mathfrak{p}$.

When $\varphi: R \rightarrow R$ is the identity map, the fiber ring $\kappa_{\varphi}(\mathfrak{p})$ is the fraction field of $R/\mathfrak{p}$; when $\mathfrak{p}$ is maximal we call $\kappa(\mathfrak{p}) := \kappa_{\varphi}(\mathfrak{p}) = R/\mathfrak{p}$ the **residue field** of R at $\mathfrak{p}$.

The “V-satz” and closed subsets of $\text{Spec}(R)$

Proposition

For $f \in R$ and $I \subseteq R$ an ideal, $f \in \mathfrak{p}$ for all $\mathfrak{p} \in V(I)$ iff $f \in \sqrt{I}$, and $\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$. In particular, the *nilradical* $\sqrt{(0)}$ of R is the intersection of all its primes.

Proof: $f \notin \sqrt{I}$ iff $I \cap \{1, f, f^2, \dots\} = \emptyset$ iff $IR_f \neq (1)$ iff $IR_f \subseteq \mathfrak{q}$ for some $\mathfrak{q} \in \text{Spec}(R_f)$ iff $I \subseteq \mathfrak{p}$ for some prime $\mathfrak{p}$ of R with $f \notin \mathfrak{p}$ (as $\text{Spec}(R_f) \simeq D(f)$).

$R_f \simeq R[y]/(fy - 1)$: this is the Rabinowitsch trick from the Strong Nullstellensatz!

Corollary

$I \mapsto V(I)$ and $Y \mapsto \bigcap_{\mathfrak{p} \in Y} \mathfrak{p}$ are inverse, inclusion-reversing bijections between radical ideals of R and closed subsets of $\text{Spec}(R)$; so $V(I) = V(J)$ iff $\sqrt{I} = \sqrt{J}$.

Proof: As for subvarieties of K^d : $\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}$ by the proposition, and $V(\bigcap_{\mathfrak{p} \in V(J)} \mathfrak{p}) = V(\sqrt{J}) = V(J)$.

Local rings

Definition

A ring R is **local** if it has exactly one maximal ideal $\mathfrak{m}$. We then write $(R, \mathfrak{m})$, or $(R, \mathfrak{m}, k)$, where $k := \kappa(\mathfrak{m}) = R/\mathfrak{m}$ is the **residue field**.

Lemma

R is local iff its nonunits form an ideal (which is then its maximal ideal $\mathfrak{m}$).

If $(R, \mathfrak{m})$ is local then $1 + \mathfrak{m} \subseteq R^\times$.

Proof: Proper ideals consist of nonunits; every nonunit lies in a maximal ideal. So if the nonunits form an ideal, it is the unique maximal ideal; and if R is local, the nonunits are exactly the elements of $\mathfrak{m}$. Finally, $x \in \mathfrak{m}$ implies $1 + x \notin \mathfrak{m}$.

Lemma

For every prime $\mathfrak{p}$ of R , the ring $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$ is local.

Proof: The primes of $R_{\mathfrak{p}}$ are the $\mathfrak{q}R_{\mathfrak{p}}$ with $\mathfrak{q} \subseteq \mathfrak{p}$, and $\mathfrak{p}R_{\mathfrak{p}}$ is the largest of them.

Examples of local rings

- $\mathbb{Z}/(p^n)$, with maximal ideal (p) .
- $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b\}$, with maximal ideal $p\mathbb{Z}_{(p)}$.
- $K[[x]]$: a power series is a unit iff its constant term is nonzero, so $\mathfrak{m} = (x)$.
Likewise $\mathbb{C}\{x\}$: if $f(0) \neq 0$ then $1/f$ is holomorphic near 0.
- $K[x_1, \dots, x_d]$ is not local (so many maximal ideals!), but $K[x_1, \dots, x_d]_{(x_1, \dots, x_d)}$ is: rational functions with denominator (in lowest terms) nonvanishing at 0.
- For $K = \overline{K}$, $X \subseteq K^d$ a subvariety, and $a \in X$: the **local ring of X at a** is $\mathcal{O}_{X,a} := K[X]_{\mathfrak{m}_a}$. Its radical ideals correspond to subvarieties of X every irreducible component of which contains a : only the geometry near a survives.

Non-examples: $\mathbb{Z}$, $K[x]$, and products of nonzero rings such as $\mathbb{Z}/(6) \simeq \mathbb{F}_2 \times \mathbb{F}_3$.

$\text{Max}(R)$ is uninteresting for a local ring, but $\text{Spec}(R)$ can be: e.g. $\text{Spec}(K[x, y]_{(x, y)})$ consists of (0) , (x, y) , and the (f) with $f \in K[x, y]$ irreducible and $f(0, 0) = 0$.

The characteristic of a local ring

Let $(R, \mathfrak{m}, k)$ be a local ring. Since k is a quotient of R , the kernel of $\mathbb{Z} \rightarrow k$ contains the kernel of $\mathbb{Z} \rightarrow R$: $\text{char}(k)$ divides $\text{char}(R)$ (with 0 a multiple of every integer).

If $\text{char}(k) = p$ then $\text{char}(R)$ is 0 or a power of p : if $\text{char}(R) = p^n c$ with $p \nmid c$, then $c \notin \mathfrak{m}$ (its image in k is nonzero), so c is a unit, and $p^n c = 0$ forces $p^n = 0$ in R .

Proposition

Let $(R, \mathfrak{m}, k)$ be a local ring. Then exactly one of the following holds:

1. $\text{char}(R) = \text{char}(k) = 0$: R has *equal characteristic zero* (e.g. $\mathbb{Q}[[x]]$);
2. $\text{char}(R) = 0$ and $\text{char}(k) = p$: R has *mixed characteristic* $(0, p)$ (e.g. $\mathbb{Z}_{(p)}$);
3. $\text{char}(R) = \text{char}(k) = p$: R has *equal characteristic* p (e.g. $\mathbb{F}_p[[x]]$);
4. $\text{char}(R) = p^n$ with $n > 1$ and $\text{char}(k) = p$ (e.g. $\mathbb{Z}/(p^n)$).

If R is reduced then one of the first three holds (p is a nonzero nilpotent in case 4).

Nakayama's Lemma (NAK)

Theorem (Nakayama's Lemma)

Let I be an ideal of R and M a finitely generated R -module with $IM = M$. Then $rM = 0$ for some $r \in 1 + I$, and $am = m$ for all $m \in M$ for some $a \in I$.

Proof: The determinant trick again; to the blackboard!

Finite generation is essential: $\mathbb{Q}$ is a $\mathbb{Z}_{(p)}$ -module with $p\mathbb{Q} = \mathbb{Q} \neq 0$.

On the blackboard: Nakayama's Lemma

Theorem (NAK). Let I be an ideal of R and M a finitely generated R -module with $IM = M$. Then there is $r \in 1 + I$ with $rM = 0$, and there is $a \in I$ with $am = m$ for all $m \in M$.

Proof. Let $m_1, \dots, m_s$ generate M . Since $M = IM$, each m_i is an I -linear combination of the generators:

$$m_i = \sum_{j=1}^s a_{ij} m_j \quad (a_{ij} \in I).$$

Let $A := (a_{ij}) \in I^{s \times s}$ and $v := (m_1, \dots, m_s)^T \in M^s$, so that $(I_s - A)v = 0$. Multiplying on the left by $\text{adj}(I_s - A)$ gives $\det(I_s - A)v = 0$ (the determinant trick), so $r := \det(I_s - A)$ kills every m_i , hence all of M . Expanding the determinant, every term other than the product of the diagonal entries $1 - a_{ii}$ lies in I , and that product is $\equiv 1 \pmod{I}$; so $r \equiv 1 \pmod{I}$, that is, $r \in 1 + I$.

For the second statement put $a := 1 - r \in I$; then $am = m - rm = m$ for all $m \in M$. □

Remark. Compare the proof that module-finite implies integral (Lecture 1): there the determinant trick was applied to the matrix of multiplication by r , here to the matrix expressing $M = IM$.

Presented on the blackboard; not part of the projected slides.

NAK for local rings

Proposition

Let $(R, \mathfrak{m}, k)$ be a local ring and M a finitely generated R -module.

- 1. If $M = \mathfrak{m}M$ then $M = 0$.*
- 2. $m_1, \dots, m_s \in M$ generate M iff their images span $M/\mathfrak{m}M$ over k .*

In particular, every generating set of M has at least $\dim_k(M/\mathfrak{m}M)$ elements.

Proof: (1) NAK gives $r \in 1 + \mathfrak{m}$ with $rM = 0$; but r is a unit, so $M = 0$.

(2) Let $N := \sum_i Rm_i$. Then $M/N = 0$ iff $M/N = \mathfrak{m}(M/N)$ (by (1))
iff $M = N + \mathfrak{m}M$ iff the images of the m_i span $M/\mathfrak{m}M$.

A **minimal generating set** of M is a set of elements of M whose images form a k -basis for $M/\mathfrak{m}M$. Every generating set contains a minimal one.

Example: the number of generators depends on the point

Let $I := (uy - vx, uz - wx, vz - wy) \subseteq R := K[u, v, w, x, y, z]$: the 2×2 minors of $\begin{pmatrix} u & v & w \\ x & y & z \end{pmatrix}$. For $K = \overline{K}$, $Z_K(I)$ is the set of 2×3 matrices of rank ≤ 1 .

- At the origin $\mathfrak{m} := (u, v, w, x, y, z)$, the three minors minimally generate $IR_{\mathfrak{m}}$: every element of $\mathfrak{m}I$ has all its terms of degree ≥ 3 , so a relation $a(uy - vx) + b(uz - wx) + c(vz - wy) \in \mathfrak{m}I$ has zero degree-2 part, which forces $a, b, c \in \mathfrak{m}$ since the minors are K -linearly independent. So $\mu(IR_{\mathfrak{m}}) = 3$.
- At the point $(1, 0, 0, 0, 0, 0)$, $\mathfrak{n} := (u - 1, v, w, x, y, z)$: u is a unit in $R_{\mathfrak{n}}$, and $uy - vx = u(y - \frac{v}{u}x)$, $uz - wx = u(z - \frac{w}{u}x)$, $vz - wy = v(z - \frac{w}{u}x) - w(y - \frac{v}{u}x)$, so $IR_{\mathfrak{n}} = (y - \frac{v}{u}x, z - \frac{w}{u}x)$ and $\mu(IR_{\mathfrak{n}}) = 2$ (check independence mod $\mathfrak{n}IR_{\mathfrak{n}}$).

Similarly $\mu(IR_{\mathfrak{p}}) = 2$ for the prime $\mathfrak{p} = (x, y, z)$, where u, v, w are all units.

The origin is the singular point of $Z_K(I)$, which has codimension 2 in K^6 .

Normal rings

Definition

A domain R is **normal** if it is integrally closed in its fraction field: every element of $\text{Frac}(R)$ that is integral over R lies in R . More generally, a ring is **normal** if it is integrally closed in its total ring of fractions (localization at nonzerodivisors).

Lemma

Every UFD is normal; e.g. $\mathbb{Z}$, $K[x_1, \dots, x_n]$, and every PID.

Proof: Let $a/b \in \text{Frac}(R)$ be integral over R , with $a, b \in R$ coprime.

Clearing denominators in $(a/b)^n + r_1(a/b)^{n-1} + \dots + r_n = 0$ gives $b \mid a^n$; an irreducible factor of b would divide a , so b is a unit and $a/b \in R$.

Example

$K[x^2, x^3] \subseteq K[x]$ is not normal: $x = x^3/x^2$ lies in its fraction field $K(x)$ and is a root of $t^2 - x^2$, but $x \notin K[x^2, x^3]$. (This is the cuspidal curve $y^2 = x^3$.)

Integral closures and rings of integers

Lemma

Let R be a domain with fraction field K , and $K \subseteq L$ a field extension. Then the integral closure S of R in L is normal.

Proof: Let $x \in \text{Frac}(S)$ satisfy $x^n + s_1x^{n-1} + \dots + s_n = 0$ with $s_i \in S$. Then x is integral over $R_0 := R[s_1, \dots, s_n]$, which is module-finite over R , so $R_0[x]$ is module-finite over R ; hence x is integral over R , i.e. $x \in S$.

The integral closure of a domain R in $\text{Frac}(R)$ is its **normalization** $\overline{R}$; it is normal.

Definition

Let K be a **number field** (a finite extension of $\mathbb{Q}$). Its **ring of integers** $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K ; it is a normal domain by the lemma.

E.g. $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-5}]$, and $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ are rings of integers, hence normal; but $\mathbb{Z}[\sqrt{-3}]$ is not normal: $\frac{1+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$ is a root of $t^2 - t + 1$.

Direct summands of normal rings

Lemma

Let $R \subseteq S$ be domains with S normal, and suppose R is a direct summand of S as an R -module, i.e. there is an R -linear $\pi: S \rightarrow R$ with $\pi|_R = \text{id}$. Then R is normal.

Proof: Let $a/b \in \text{Frac}(R)$ ($a, b \in R$) be integral over R , hence over S . As S is normal, $a/b = s$ for some $s \in S$, i.e. $a = bs$; applying π gives $a = \pi(a) = \pi(bs) = b\pi(s)$, so $a/b = \pi(s) \in R$.

Example

$R = K[x^2, xy, y^2] \subseteq K[x, y]$ is normal: R is the even-degree part of $K[x, y]$, and the odd-degree part is an R -submodule, so $K[x, y] = R \oplus (\text{odd part})$.

If a finite group G acts on a normal domain S by automorphisms and $|G| \in S^\times$, then S^G is a direct summand of S via the **Reynolds operator** $s \mapsto \frac{1}{|G|} \sum_{g \in G} g(s)$, so S^G is normal: e.g. invariant rings $K[x_1, \dots, x_n]^G$ with $\text{char } K \nmid |G|$.

More examples and non-examples

- The normalization of $K[x^2, x^3]$ is $K[x]$: normalization “resolves” the cusp.
- $R = K[x, y, z]/(x^2y - z^2)$ is a domain that is not normal: $(z/x)^2 = y$ in $\text{Frac}(R)$, so z/x is integral over R , but $z/x \notin R$ (check!).
Its normalization is $R[z/x] = K[x, z/x]$, a polynomial ring in two variables.
- $K[x^2, xy, y^2]$ is normal but not a UFD: $x^2 \cdot y^2 = (xy)^2$, where x^2, xy, y^2 are irreducible (degree 2 is minimal among nonunits) and pairwise non-associate.
- Every Veronese subring $K[x_1, \dots, x_n]^{(d)}$ (spanned by the monomials of degree divisible by d) is normal in any characteristic, by the same argument.

The trace

Definition

Let $K \subseteq L$ be a finite extension of fields. For $x \in L$, the **trace** $\text{Tr}_{L/K}(x) \in K$ is the trace of the K -linear map $L \rightarrow L$, $y \mapsto xy$ (computed in any K -basis of L).

Proposition

Let $K \subseteq L \subseteq M$ be finite extensions of fields.

1. $\text{Tr}_{L/K}: L \rightarrow K$ is K -linear, and $\text{Tr}_{L/K}(x) = [L : K] x$ for $x \in K$.
2. If $t^d + c_1 t^{d-1} + \cdots + c_d$ is the minimal polynomial of $x \in L$ over K , then $\text{Tr}_{K(x)/K}(x) = -c_1$.
3. $\text{Tr}_{M/K} = \text{Tr}_{L/K} \circ \text{Tr}_{M/L}$; in particular $\text{Tr}_{L/K}(x) = [L : K(x)] \text{Tr}_{K(x)/K}(x)$.
4. If L/K is separable, the pairing $(x, y) \mapsto \text{Tr}_{L/K}(xy)$ is nondegenerate: for every $0 \neq x \in L$ there is $y \in L$ with $\text{Tr}_{L/K}(xy) \neq 0$.

Proof: Exercise in field theory; for (2) use the basis $1, x, \dots, x^{d-1}$ of $K(x)$, and for (4) use separability (e.g. via the primitive element theorem).

Finiteness of the integral closure

Lemma

Let R be a normal domain with fraction field K , and let a be integral over R in some domain $S \supseteq R$. Then the minimal polynomial f of a over K has coefficients in R . In particular, if $a \in L$ for a finite extension L/K , then $\text{Tr}_{L/K}(a) \in R$.

Proof: Let $g \in R[t]$ be monic with $g(a) = 0$; then $f \mid g$ in $K[t]$, so the roots of f (in a splitting field) are roots of g , hence integral over R . The coefficients of f are polynomials in these roots, so they are integral over R and in K , hence in R . Finally, $\text{Tr}_{L/K}(a) = -[L : K(a)] \cdot c_1$, where c_1 is the second coefficient of f .

Theorem

Let R be a Noetherian normal domain with fraction field K , and let L/K be a finite separable extension. Then the integral closure of R in L is a finitely generated R -module, hence a Noetherian normal domain.

Proof: To the blackboard!

On the blackboard: finiteness of the integral closure

Theorem. Let R be a Noetherian normal domain with fraction field K , and L/K a finite separable extension of degree d . Then the integral closure S of R in L is a finitely generated R -module.

Proof. Step 1: L has a K -basis consisting of elements of S . Any $x \in L$ is algebraic over K , so after clearing denominators $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in R$ and $a_0 \neq 0$. Multiplying by a_0^{n-1} :

$$(a_0x)^n + a_1(a_0x)^{n-1} + a_2a_0(a_0x)^{n-2} + \cdots + a_na_0^{n-1} = 0,$$

so $a_0x \in S$. Rescaling a K -basis of L in this way yields a basis $s_1, \dots, s_d$ of L with all $s_i \in S$.

Step 2: For an R -submodule $M \subseteq L$ put $M^\vee := \{x \in L : \text{Tr}_{L/K}(xM) \subseteq R\}$; this is an R -submodule of L , and $M \subseteq N$ implies $N^\vee \subseteq M^\vee$. Let $B := \sum_i Rs_i$, a free R -module with basis $s_1, \dots, s_d$. Since L/K is separable the trace pairing $(x, y) \mapsto \text{Tr}_{L/K}(xy)$ is nondegenerate, so there is a dual basis $t_1, \dots, t_d$ of L with $\text{Tr}_{L/K}(s_i t_j) = \delta_{ij}$. Then $B^\vee = \sum_j Rt_j$ is free of rank d : writing $x \in L$ as $x = \sum_j k_j t_j$ with $k_j \in K$, we have $\text{Tr}_{L/K}(xs_i) = k_i$, so $x \in B^\vee$ if and only if every $k_i \in R$.

Step 3: $S \subseteq S^\vee$: for $s, s' \in S$ the product $ss' \in S$ is integral over R , so $\text{Tr}_{L/K}(ss') \in R$ by the lemma. Since $B \subseteq S$, also $S^\vee \subseteq B^\vee$. Hence

$$S \subseteq S^\vee \subseteq B^\vee \simeq R^d.$$

Step 4: $B^\vee$ is a finitely generated module over the Noetherian ring R , so its submodule S is finitely generated (Lecture 1). □

Remark. For $R = \mathbb{Z}$, $S = \mathcal{O}_K$: $S^\vee$ is the inverse different, and $[S^\vee : S] = |\text{disc}(K)|$ (18.785).

Presented on the blackboard; not part of the projected slides.