

18.705 Commutative Algebra

Lecture 3

Andrew V. Sutherland

Adapted from the [2018 lecture notes](#) of Jack Jeffries (§2.2-2.3)

September 17, 2026

In previous lectures...

Theorem (Hilbert Basis Theorem)

If A is a Noetherian ring then so are $A[x_1, \dots, x_n]$ and $A[[x_1, \dots, x_n]]$.

Corollary (Weak Nullstellensatz)

*If R is a finitely generated K -algebra and $\mathfrak{m} \in \text{Max}(R)$, then $[R/\mathfrak{m} : K] < \infty$.
In particular, if $K = \overline{K}$ then $R/\mathfrak{m} = K$, so $a \mapsto \mathfrak{m}_a$ and $a \mapsto \mathfrak{m}_a/I$ give bijections $K^d \rightarrow \text{Max}(K[x_1, \dots, x_d])$ and $Z_K(I) \rightarrow \text{Max}(K[x_1, \dots, x_d]/I)$.*

Theorem (Medium Nullstellensatz)

Let $K = \overline{K}$ and $I \subseteq K[x_1, \dots, x_d]$ an ideal. Then $Z_K(I) = \emptyset \Leftrightarrow I = (1)$.

Corollary

If a system of polynomial equations over a field K has a solution in some nonzero K -algebra, then it has a solution in $\overline{K}$.

The Strong Nullstellensatz

Inequations: $f(a) \neq 0$ if and only if $yf(a) = 1$ has a solution $y \in K$.

So $f_1 = \cdots = f_m = 0$, $g_1 \neq 0, \dots, g_n \neq 0$ has a solution in K^d if and only if $f_1 = \cdots = f_m = 0$, $yg_1 \cdots g_n = 1$ has a solution in K^{d+1} .

Theorem (Strong Nullstellensatz)

Let $K = \overline{K}$, let $I \subseteq K[x] := K[x_1, \dots, x_d]$ be an ideal, and let $f \in K[x]$. Then f vanishes on $Z_K(I)$ if and only if $f^n \in I$ for some $n \geq 1$.

Proof: If $f^n \in I$ and $a \in Z_K(I)$ then $f(a)^n = 0$, so $f(a) = 0$.

For the converse, to the blackboard!

Hilbert proved the Nullstellensatz (“theorem of zeros”) in 1893, three years after the Basis Theorem; both arose from his work on invariant theory.

On the blackboard: proof of the Strong Nullstellensatz

Theorem. Let $K = \overline{K}$, let I be an ideal of $K[x] := K[x_1, \dots, x_d]$, and let $f \in K[x]$. If f vanishes on $Z_K(I)$ then $f^n \in I$ for some $n \geq 1$.

Proof. We may assume $f \neq 0$. Let y be a new variable and consider the ideal $I' := IK[x, y] + (yf - 1)$ of $K[x, y]$. A point $(a, b) \in Z_K(I')$ would satisfy $a \in Z_K(I)$ and $bf(a) = 1$, contradicting $f(a) = 0$. So $Z_K(I') = \emptyset$, and $I' = (1)$ by the Medium Nullstellensatz. Writing $I = (g_1, \dots, g_m)$ (Hilbert Basis Theorem), we have

$$1 = r_0(x, y) (yf(x) - 1) + r_1(x, y) g_1(x) + \dots + r_m(x, y) g_m(x)$$

for some $r_i \in K[x, y]$. Now apply the $K[x]$ -algebra homomorphism $K[x, y] \rightarrow K(x)$ that sends $y \mapsto 1/f$: the first term vanishes, leaving

$$1 = r_1(x, 1/f) g_1(x) + \dots + r_m(x, 1/f) g_m(x) \quad \text{in } K(x).$$

Let n be at least the y -degree of every r_i , so that $s_i := f^n r_i(x, 1/f) \in K[x]$. Multiplying through by f^n gives $f^n = s_1 g_1 + \dots + s_m g_m \in I$. $\square$

Remark. The variable y encodes $f \neq 0$ as the equation $yf = 1$; this is the “Rabinowitsch trick”.

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

Radical ideals

Definition

The **radical** of an ideal I of a ring R is $\sqrt{I} := \{f \in R : f^n \in I \text{ for some } n \geq 1\}$, and I is a **radical ideal** if $\sqrt{I} = I$. Prime ideals are radical, and so is $\sqrt{I}$ for any ideal I .

$\sqrt{I}$ is an ideal: if $f^m, g^n \in I$ then $(rf)^m = r^m f^m \in I$, and every term of the binomial expansion of $(f + g)^{m+n-1}$ is divisible by f^m or g^n .

Lemma

R/I is **reduced** (has no nonzero nilpotents) if and only if I is radical.

Proof: The image of f in R/I is a nonzero nilpotent if and only if $f \in \sqrt{I} \setminus I$.

For $X \subseteq K^d$ let $I(X) := \{f \in K[x_1, \dots, x_d] : f(a) = 0 \text{ for all } a \in X\}$, a radical ideal. The Strong Nullstellensatz says exactly that $I(Z_K(J)) = \sqrt{J}$ for every ideal $J \subseteq K[x_1, \dots, x_d]$ (when $K = \overline{K}$).

The ideal–variety correspondence

Corollary

Let $K = \overline{K}$. Then Z_K and I are mutually inverse, inclusion-reversing bijections

$$\{\text{radical ideals } J \subseteq K[x_1, \dots, x_d]\} \longleftrightarrow \{\text{subvarieties } X \subseteq K^d\}.$$

In particular, $Z_K(I) = Z_K(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Proof: $I(Z_K(J)) = \sqrt{J} = J$ for radical J (Strong NSS), and for $X = Z_K(J)$ we have $Z_K(I(X)) = Z_K(\sqrt{J}) = Z_K(J) = X$, since $f(a)^n = 0 \Leftrightarrow f(a) = 0$.

This answers our question: over $K = \overline{K}$, a system of polynomial equations is determined by its solution set up to taking the radical of the ideal it generates.

Definition

Let $K = \overline{K}$ and let $X \subseteq K^d$ be a subvariety. The **coordinate ring** of X is $K[X] := K[x_1, \dots, x_d]/I(X)$, the ring of polynomial functions on X .

Coordinate rings

Let $K = \overline{K}$. Every reduced finitely generated K -algebra is a coordinate ring:
 $K[x_1, \dots, x_d]/J \simeq K[Z_K(J)]$ for J radical. What are the equations of $K[x]^G$?

Example (the Veronese ring $K[x^2, xy, y^2] = K[x, y]^{\mu_2}$; $K = \overline{K}$, $\text{char } K \neq 2$)

Let $R = K[x^2, xy, y^2]$ and $J := \ker(K[u, v, w] \rightarrow R)$, where $u, v, w \mapsto x^2, xy, y^2$.
 $v^2 - uw \in J$, so $Z_K(J) \subseteq Z_K(v^2 - uw)$. Conversely, if $b^2 = ac$ then
 $(a, b, c) = (\alpha^2, \alpha\gamma, \gamma^2)$ for some $\alpha, \gamma \in K$ (choose square roots), so
 $g(a, b, c) = g(\alpha^2, \alpha\gamma, \gamma^2) = 0$ for all $g \in J$. Thus $\sqrt{J} = \sqrt{(v^2 - uw)}$.
But J is radical (R is a domain) and $(v^2 - uw)$ is prime ($v^2 - uw$ is irreducible),
so $J = (v^2 - uw)$ and $R \simeq K[u, v, w]/(v^2 - uw)$.

Similarly, $K[x^3, x^2y, xy^2, y^3] \simeq K[t, u, v, w]/(u^2 - tv, v^2 - uw, tw - uv)$,
but showing that this ideal is radical is harder.

Maximal ideals of polynomial rings over arbitrary fields

Let K be a field, $S := K[x_1, \dots, x_n]$, and $\mathfrak{m}_a := \{f \in S : f(a) = 0\}$ for $a \in \overline{K}^n$. Then $S/\mathfrak{m}_a \simeq K[a_1, \dots, a_n]$ is a domain of finite K -dimension (the a_i are integral), hence a field: for $r \neq 0$, $x \mapsto rx$ is injective, so surjective. Thus $\mathfrak{m}_a$ is maximal.

Proposition

Every maximal ideal of S is $\mathfrak{m}_a$ for some $a \in \overline{K}^n$, and $\mathfrak{m}_a = \mathfrak{m}_b$ if and only if $b = \sigma(a)$ for some $\sigma \in \text{Aut}(\overline{K}/K)$. Thus $a \mapsto \mathfrak{m}_a$ induces a bijection $\overline{K}^n / \text{Aut}(\overline{K}/K) \longrightarrow \{\text{maximal ideals of } S\}$.

Proof: To the blackboard!

Example

Maximal ideals of $\mathbb{R}[x]$: $(x - a)$ for $a \in \mathbb{R}$, and $((x - a)(x - \bar{a}))$ for $a \in \mathbb{C} \setminus \mathbb{R}$. They correspond to the orbits of complex conjugation on $\mathbb{C}$.

On the blackboard: maximal ideals over arbitrary fields

Proposition. Let K be a field, $S := K[x_1, \dots, x_n]$, and $\mathfrak{m}_a := \{f \in S : f(a) = 0\}$ for $a \in \overline{K}^n$. Every maximal ideal of S is $\mathfrak{m}_a$ for some $a \in \overline{K}^n$, and $\mathfrak{m}_a = \mathfrak{m}_b$ if and only if $b = \sigma(a)$ for some $\sigma \in \text{Aut}(\overline{K}/K)$.

Proof. Let $\mathfrak{m}$ be a maximal ideal of S . By the weak Nullstellensatz $S/\mathfrak{m}$ is a finite extension of K , so there is a K -embedding $S/\mathfrak{m} \rightarrow \overline{K}$. Composing with $S \twoheadrightarrow S/\mathfrak{m}$ gives a K -algebra map $\varphi: S \rightarrow \overline{K}$ with kernel $\mathfrak{m}$; if $a_i := \varphi(x_i)$ then $\varphi(f) = f(a)$, so $\mathfrak{m} = \ker \varphi = \mathfrak{m}_a$.

If $b = \sigma(a)$ with $\sigma \in \text{Aut}(\overline{K}/K)$, then for $f \in \mathfrak{m}_a$ we have $f(b) = f(\sigma(a)) = \sigma(f(a)) = \sigma(0) = 0$, since σ fixes the coefficients of f . So $\mathfrak{m}_a \subseteq \mathfrak{m}_b$, and $\mathfrak{m}_a = \mathfrak{m}_b$ because both are maximal.

Conversely, suppose $\mathfrak{m}_a = \mathfrak{m}_b$. The K -algebra maps $S \rightarrow \overline{K}$ given by $x_i \mapsto a_i$ and $x_i \mapsto b_i$ have the same kernel, so they induce a K -algebra isomorphism

$$K(a_1, \dots, a_n) = K[a_1, \dots, a_n] \simeq S/\mathfrak{m}_a = S/\mathfrak{m}_b \simeq K[b_1, \dots, b_n] = K(b_1, \dots, b_n)$$

with $a_i \mapsto b_i$. Any K -isomorphism between subfields of $\overline{K}$ extends to some $\sigma \in \text{Aut}(\overline{K}/K)$: extend it to a K -embedding $\overline{K} \rightarrow \overline{K}$ using Zorn's lemma; this is surjective because its image is an algebraically closed field over which $\overline{K}$ is algebraic. Then $\sigma(a) = b$, as required. $\square$

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

The Zariski topology and the spectrum of a ring

The Zariski topology on K^n has the subvarieties $Z_K(I)$ as its closed sets.

$\text{Max}(R)$, the set of maximal ideals of R , has closed sets $\{\mathfrak{m} \in \text{Max}(R) : \mathfrak{m} \supseteq I\}$.

For $K = \overline{K}$ the Nullstellensatz gives $K^n \simeq \text{Max}(K[x])$ and $Z_K(I) \simeq \text{Max}(K[x]/I)$.

But Max is not the right notion for general rings:

- many interesting rings have only one maximal ideal (e.g. $\mathbb{C}[[z]]$)!
- ring maps $R \rightarrow S$ should induce maps of spaces $S \rightarrow R$; for $K[x, y] \subseteq K(x)[y]$, should the maximal ideal (y) go to (x, y) or to $(x - 1, y)$?
(Nothing distinguishes them: $K[x, y] = K[x - 1, y]$.)

Definition

The spectrum $\text{Spec}(R)$ of a ring R is its set of prime ideals, partially ordered by inclusion, with the topology whose closed sets are $V(I) := \{\mathfrak{p} \in \text{Spec}(R) : \mathfrak{p} \supseteq I\}$.

$\text{Max}(R) \subseteq \text{Spec}(R)$ is a subspace, and $(y) \subseteq K(x)[y]$ now goes to $(y) \cap K[x, y] = (y)$.

Closed sets of $\text{Spec}(R)$

Proposition

Let R be a ring and let I, J, I_λ be ideals of R .

1. If $I \subseteq J$ then $V(J) \subseteq V(I)$.
2. $V(I) \cup V(J) = V(I \cap J) = V(IJ)$.
3. $\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda)$.
4. The open sets $D(f) := \text{Spec}(R) \setminus V(f)$ for $f \in R$ form a basis for the topology.
5. $\text{Spec}(R)$ is compact: every open cover has a finite subcover.

Proof: (1) and (3) are clear; for the rest, to the blackboard!

Since $V(0) = \text{Spec}(R)$ and $V(1) = \emptyset$, properties (2) and (3) show that the $V(I)$ are the closed sets of a topology. Properties (1)–(4) also hold for Z_K and the Zariski topology on K^n .

$\text{Spec}(R)$ is rarely Hausdorff: $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, so $\mathfrak{p}$ is a closed point iff $\mathfrak{p}$ is maximal.

On the blackboard: closed sets of $\text{Spec}(R)$

Proposition. Let R be a ring and I, J, I_λ ideals of R . (1) $I \subseteq J \Rightarrow V(J) \subseteq V(I)$; (2) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$; (3) $\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda)$; (4) the sets $D(f) := \text{Spec}(R) \setminus V(f)$ form a basis of open sets; (5) $\text{Spec}(R)$ is compact.

Proof. (1) and (3) are clear from the definition of V .

(2) Since $IJ \subseteq I \cap J \subseteq I, J$, (1) gives $V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$. If $\mathfrak{p} \in V(IJ)$ but $\mathfrak{p} \notin V(I) \cup V(J)$, pick $f \in I \setminus \mathfrak{p}$ and $g \in J \setminus \mathfrak{p}$; then $fg \in IJ \subseteq \mathfrak{p}$, contradicting the primality of $\mathfrak{p}$.

(4) Every open set is the complement of some $V(I) = \bigcap_{f \in I} V(f)$, hence equal to $\bigcup_{f \in I} D(f)$.

(5) Let $\{U_\lambda\}$ be an open cover of $\text{Spec}(R)$. By (4) each U_λ is a union of basic open sets, so we obtain a cover by sets $D(f_\mu)$, $\mu \in M$, with each $D(f_\mu)$ contained in some $U_{\lambda(\mu)}$. Then $\emptyset = \bigcap_\mu V(f_\mu) = V(J)$ with $J := (f_\mu : \mu \in M)$, by (3). Every proper ideal lies in a maximal ideal, which is prime, so $J = (1)$: we have $1 = r_1 f_{\mu_1} + \cdots + r_t f_{\mu_t}$ for some $\mu_1, \dots, \mu_t \in M$ and $r_i \in R$. Thus $(f_{\mu_1}, \dots, f_{\mu_t}) = (1)$, so $\bigcap_i V(f_{\mu_i}) = \emptyset$; that is, $D(f_{\mu_1}), \dots, D(f_{\mu_t})$ cover $\text{Spec}(R)$, and hence so do $U_{\lambda(\mu_1)}, \dots, U_{\lambda(\mu_t)}$. $\square$

Remark. Jeffries proves (5) for Noetherian R using the ascending chain condition, but as we see, it holds for every ring.

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

Maps on spectra

Definition

A ring map $\varphi: R \rightarrow S$ induces $\varphi^*: \operatorname{Spec}(S) \rightarrow \operatorname{Spec}(R)$, $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$; the preimage of a prime ideal is prime. When $R \subseteq S$ we write $\mathfrak{p} \cap R$ for $\varphi^{-1}(\mathfrak{p})$.

φ^* is continuous, since $(\varphi^*)^{-1}(V(I)) = V(IS)$.

But maximal ideals need not pull back to maximal ideals (consider $\mathbb{Z} \subseteq \mathbb{Q}$).

Lemma

Let $R \subseteq S$ be an integral extension with S a domain. Then every nonzero $s \in S$ has a nonzero multiple $st \in R$. If moreover R is a field, then S is a field.

Proof: Let $s^n + r_1 s^{n-1} + \cdots + r_n = 0$ with $r_i \in R$ and n minimal. Then $r_n \neq 0$, else we could cancel s ; and $r_n = st$ with $t := -(s^{n-1} + \cdots + r_{n-1}) \in S$. If R is a field then $s^{-1} = tr_n^{-1} \in S$.

Maps of finitely generated algebras

Proposition

*Let $\varphi: R \rightarrow S$ be a homomorphism of finitely generated K -algebras.
Then φ^* maps $\text{Max}(S)$ into $\text{Max}(R)$.*

Proof: For $\mathfrak{n} \in \text{Max}(S)$, $R/\varphi^{-1}(\mathfrak{n}) \subseteq S/\mathfrak{n}$ is a domain of finite K -dimension (Zariski), hence integral over K , hence a field by the lemma.

Proposition

*Let $K = \overline{K}$, $R = K[x_1, \dots, x_c]/I$, and $S = K[y_1, \dots, y_d]/J$. A K -algebra map $\varphi: R \rightarrow S$ has the form $\varphi(x_i) = f_i(y)$ with $f_i \in K[y_1, \dots, y_d]$,
and then $f := (f_1, \dots, f_c)$ maps $Z_K(J)$ into $Z_K(I)$, with $\varphi^*(\mathfrak{m}_a) = \mathfrak{m}_{f(a)}$.*

Proof: $g \in \varphi^{-1}(\mathfrak{m}_a) \Leftrightarrow \varphi(g)(a) = g(f(a)) = 0 \Leftrightarrow g \in \mathfrak{m}_{f(a)}$;
taking $g \in I$ (so $g = 0$ in R) shows that $f(a) \in Z_K(I)$.

Summary: the algebra–geometry dictionary

Let K be an algebraically closed field.

- Subvarieties $X \subseteq K^d \longleftrightarrow$ radical ideals $I(X) \subseteq K[x_1, \dots, x_d]$ (Nullstellensatz).
- Coordinate rings $K[X]$ are exactly the reduced finitely generated K -algebras.
- Points of $X \longleftrightarrow$ maximal ideals of $K[X] \longleftrightarrow K$ -algebra maps $K[X] \rightarrow K$.
- Polynomial maps $X \rightarrow Y \longleftrightarrow K$ -algebra maps $K[Y] \rightarrow K[X]$.
- For an arbitrary ring R , the space $\operatorname{Spec}(R)$ plays the role of X ; ring maps $R \rightarrow S$ induce continuous maps $\operatorname{Spec}(S) \rightarrow \operatorname{Spec}(R)$.