Hilbert Basis Theorem
& Ideal-Variety Correspondence

MA434: Algebraic Geometry — Lecture: March 09, 2020
Presenters: Christopher & Lily
Scribe: Huan Q. Bui

Here is a summary of what we did in class on Mar 09, 2020. Christopher and Lily covered sections 3.3 to 3.6 in Reid's. We discussed the Hilbert Basis Theorem, followed by some corollaries and examples, and the correspondences $\mathcal{V}$ and $\mathcal{I}$. We ended the lecture with some tidbits by Fernando on the Hilbert basis theorem and, of course, the midterm exam (good luck ☺).

1 Review

Last time, we introduced the concept of Noetherian rings. Today, we will be using the following (equivalent) useful facts about Noetherian rings. Let a Noetherian ring $\mathcal{A}$ be given, then

- $\forall\, \mathcal{I} \overset{\text{idl}}{\subset} \mathcal{A}$, $\mathcal{I}$ is finitely generated (or *f.g.*, for short).
- Every ascending chain

  $$\mathcal{I} \subset \dots \subset \mathcal{I}_m \subset \dots$$

  with $\mathcal{I}_i \overset{\text{idl}}{\subset} \mathcal{A}$ eventually terminates, with $\mathcal{I}_N = \mathcal{I}_{N+1} = \dots$ for some $N \in \mathbb{N}$. This is called the ascending chain condition, or *a.c.c.*.

2 Hilbert Basis Theorem

Theorem 2.1.

$$\boxed{\text{Ring } \mathcal{A} \text{ is Noetherian } \implies \mathcal{A}[X] \text{ is Noetherian.}}$$

Proof. Let a Noetherian ring $\mathcal{A}$ be given. To show: every $\mathcal{J} \overset{\text{idl}}{\subset} \mathcal{A}[X]$, where $\mathcal{A}[X]$ is the *ring of polynomials whose coefficients are elements of $\mathcal{A}$*, is f.g..

Let any $\mathcal{J} \overset{\text{idl}}{\subset} \mathcal{A}[X]$ be given. We consider J_n, the subset of $\mathcal{A}$ that contains the coefficients of leading terms of degree-n polynomials in $\mathcal{J}$:

$$J_n = \left\{a \in \mathcal{A} \,|\, \exists f = aX^n + b_{n-1}X^{n-1} + \dots + b_0 \in \mathcal{J}\right\}.$$

Now, $J_n \overset{\text{idl}}{\subset} \mathcal{A}$, because:

- Because $\mathcal{J}$ is an ideal, for any $f_1 = aX^n + \dots$ and $f_2 = bX^n + \dots \in \mathcal{J}$, we have $f_1 + f_2 = (a+b)X^n + \dots \in \mathcal{J}$. And so we see that with $a, b \in J_n$, $(a+b) \in J_n \implies J_n$ is closed under $(+)$.
- Consider $a \in \mathcal{A}$ and $j \in J_n$. We can see that aj is going to be the coefficient for a leading term for some degree-n polynomial in $\mathcal{J}$. So, $aj \in J_n \implies J_n$ absorbs products.

We can also see that $J_n \subset J_{n+1}$, because for any degree-n polynomial $f \in \mathcal{J}$ with leading coefficient $j \in J_n$, the degree-$(n+1)$ polynomial Xf also has leading coefficient $j \in J_{n+1}$.

So, because $\mathcal{A}$ is Noetherian, $J_n \overset{\text{idl}}{\subset} \mathcal{A}$, and $J_n \subset J_{n+1}$, *a.c.c.* tells us that there is some $N \in \mathbb{N}$ for which

$$J_N = J_{N+1} = \dots$$

The goal now is to build a set of generators for $\mathcal{J}$. If we can somehow show there are *finitely many* generators for $\mathcal{J}$ then we're done. Here's how: each $J_i \overset{\text{idl}}{\subset} \mathcal{A}$ is f.g., for each $i \leq N$, we let $(a_{i1}, \dots, a_{m(i)})$ generate J_i. For each a_{ik}, we let $f_{ik} = a_{ik}X^i + \dots \in \mathcal{J}$ be an element of degree i and leading coefficient a_{ik}.

Intuitively, the set

$$\{f_{ik} \,|\, i = 0, 1, \dots, N; k = 1, \dots, m(i)\}$$

generates $\mathcal{J}$. We will see this explicitly: consider some $g \in \mathcal{J}$ with $\deg g = \gamma$, then the leading term of g is bX^γ with $b \in J_\gamma$. Now, J_γ is an ideal f.g. by the a_{ik}'s, so I can write b as a combination of these:

$$b = \sum_k c_{\gamma' k} a_{\gamma' k}$$

with $\gamma' = \gamma$ if $\gamma \leq N$, otherwise $\gamma' = N$. (This has to do with the fact that the ascending chain terminates at J_N - we won't worry about this too much.) From here, we consider this polynomial in $\mathcal{J}$:

$$g_1 = g - X^{(\gamma - \gamma')} \sum_k c_{\gamma' k} f_{\gamma' k}.$$

By how we define γ', there is no negative degree in g_1. Because the leading coefficient of each $f_{\gamma' j}$ is $a_{\gamma' j}$ (by construction), we can readily check that the term of degree γ is zero. And so,

$$\deg g_1 \leq \deg g - 1.$$

By induction, we will eventually get to some $g_\eta = 0$ This means that we will eventually be able to write g as a combination of the f_{ik}'s. So, $\mathcal{J}$ is f.g. $\implies \mathcal{A}[X]$ is Noetherian.

□

Here's a little "summary" of the proof: We want to show any $\mathcal{J} \overset{\text{idl}}{\subset} \mathcal{A}$ is f.g., so we look at

$$\mathcal{A}[X] \overset{\text{idl}}{\supset} \mathcal{J} \xrightarrow{\text{collect leading coefs...}} a = \text{ combo of } a_{i1}, \ldots, a_{im(i)} \in J_i \overset{\text{idl}}{\subset} \mathcal{A}.$$

From here, look at $g \in \mathcal{J}$ with $\deg g = \gamma$. Since $J_\gamma \overset{\text{idl}}{\subset} \mathcal{A}$, the leading coefficient can be written as $\sum c_{\gamma' k} a_{\gamma' k}$ where the $a_{\gamma' k}$'s generate J_γ. So, with each $f_{\gamma' k}$ having $a_{\gamma' k}$ as leading coef.,

$$\deg \left[g - \sum_k c_{\gamma' k} a_{\gamma' k} X^{\gamma - \gamma'} f_{\gamma' k} \right] \leq \gamma - 1.$$

By induction, we eventually get to the zero polynomial, which implies we can write g as a combination of the f_{ik}'s. This says $\mathcal{J}$ is f.g., and so $\mathcal{A}[X]$ is Noetherian.

2.1 Some consequences

Any field k is Noetherian (l.t.r.). So, we have that

$$k \text{ is a field } \implies k[X_1] \text{ is Noetherian.}$$

The proof is a direct application of Hilbert Basis Theorem.

But why stop at a single variable X_1 when we have a new Noetherian ring, namely $k[X_1]$? Applying Hilbert's Basis Theorem again to $k[X_1]$ we have that $k[X_1][X_2] \equiv k[X_1, X_2]$ is also Noetherian. Here $k[X_1][X_2]$ is the ring of polynomials in X_2 whose coefficients are (polynomial) elements in $k[X_1]$. It makes senses (and is true!) that $k[X_1][X_2] = k[X_1, X_2]$.

Of course we can do this *finitely many times* to get a more general result:

$$k \text{ is a field } \implies k[X_1, \dots, X_n] \text{ is Noetherian.}$$

Reid generalizes this a bit more in a corollary:

$$\boxed{k \text{ is a field } \implies \text{ a finitely generated } k-\text{algebra is Noetherian}}$$

A finitely generated k-algebra is a ring of the form $\mathcal{A} = k[a_1, \dots, a_n]$, which is generated (as a ring) by k and $a_1, \dots, a_n$. Every such ring is isomorphic to a quotient of the polynomial ring, i.e.,

$$\mathcal{A} \cong k[X_1, \dots, X_n]/I.$$

From our discussion above we already know that $k[X_1, \dots, X_n]$ is Noetherian, and so $k[X_1, \dots, X_n]/I$ is also Noetherian by Proposition 3.2(i), which I presented in the previous lecture ☺.

3 The correspondence $\mathcal{V}$

Definition 3.1. Let k be a field and $\mathcal{A} = k[X_1, \ldots, X_n]$. Given a polynomial $f(X_1, \ldots, X_n) \in \mathcal{A}$ and a point $P = (a_1, \ldots, a_n) \in \mathbb{A}_k^n \equiv k^n$ (think of this as just a k-tuple), we define the correspondence:

$$\left\{ J \overset{\text{idl}}{\subset} \mathcal{A} \right\} \xrightarrow{\mathcal{V}} \left\{ \text{subsets } X \in \mathbb{A}_k^n \right\}$$

by

$$J \to \mathcal{V}(J) = \left\{ P \in \mathbb{A}_k^n \mid f(P) = 0 \, \forall f \in J \right\},$$

where the notation $f(P)$ means "evaluating f at P."

Definition 3.2. When $\mathcal{V}(I) = X \subset \mathbb{A}_k^n$ for some I, then X is an *algebraic set*.

Proposition-Definition 3.3. The correspondence $\mathcal{V}$ satisfies the following formal properties:

1. $\mathcal{V}(\{0\}) = \mathbb{A}_k^n; \quad \mathcal{V}(\mathcal{A}) = \varnothing$.
2. $I \subset J \implies \mathcal{V}(I) \supset \mathcal{V}(J)$. Or, $\mathcal{V}$ "reverses inclusion."
3. $\mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$. Or, to make a bigger $\mathcal{V}(I)$, intersect the I's!
4. $\mathcal{V}\left(\sum_{\lambda \in \Lambda} I_\lambda\right) = \bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\lambda)$.

Proof:

1. By the definition of $\mathcal{V}(J)$, we see that if $J = \{0\}$ then $\mathcal{V}(J)$ is the set of points P at which $f(P) = 0$ for all $f \in J$. But $J = \{0\}$, so f is identically zero. So, any $P \in \mathbb{A}_k^n$ is in $\mathcal{V}(0)$. When J is all of $\mathcal{A}$, no point $P \in \mathbb{A}_k^n$ makes *every* $f \in J$ vanish because there are constant functions in J.
2. If $I \subset J$ then if a point $P \in \mathbb{A}_k^n$ is such that $f(P) = 0 \, \forall f \in J$ then $f(P) = 0 \, \forall f \in I$. So $\mathcal{V}(J) \subset \mathcal{V}(I)$.
3. - ($\supset$) Evidently, $\mathcal{V}(I) \subset \mathcal{V}(I \cap J)$ because $I \cap J \subset I$. Similarly, $\mathcal{V}(J) \subset \mathcal{V}(I \cap J)$ (by (2)). So, $\mathcal{V}(I) \cup \mathcal{V}(J) \subset \mathcal{V}(I \cap J)$.
   - ($\subset$) Assume $P \in \mathcal{V}(I \cap J)$. If $P \notin \mathcal{V}(I) \cup \mathcal{V}(J)$ then there is some $f \in I$ and $g \in J$ such that $f(P) \neq 0$ and $g(P) \neq 0$. But this means $f \circ g(P) \neq 0$, which implies $P \notin V(I \cap J)$. This is a contradiction.

   With these items, we're done with the proof.

4. - ($\subset$) First, let us write

   $$\mathfrak{L} \equiv \sum_{\lambda \in \Lambda} I_\lambda = \left\{ \mathfrak{f} = \sum_{\lambda \in \Lambda} f_\lambda \,\middle|\, f_\lambda \in I_\lambda \right\}.$$

   $\mathfrak{L}$ is an ideal (l.t.r.). For any point $P \in \mathcal{V}(\mathfrak{L})$, $\mathfrak{f}(P) = 0 \,\forall\, \mathfrak{f} \in \mathfrak{L}$, by definition. In particular, if we look at f_λ where $\mathfrak{L} \ni \mathfrak{f} = f_\lambda \in I_\lambda$, then $f_\lambda(P) = 0$. This holds for all $f_\lambda \in I_\lambda$ and for all λ, so the point P belongs to *every* $\mathcal{V}(I_\lambda)$, i.e., $\mathcal{V}(\mathfrak{L}) \subset \bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\lambda)$.

   - ($\supset$) Suppose $P \in \bigcap_{\lambda_\Lambda} V(I_\lambda)$, then for any $\lambda \in \Lambda$, $f(P) = 0 \,\forall\, f \in I_\lambda$. This tells us that any $\mathfrak{f} \in \mathfrak{L}$ (which is some combination of the f_λ's) vanishes at P as well. This means $P \in \mathcal{V}(\mathfrak{L})$. So, $\bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\lambda) \subset \mathcal{V}(\mathfrak{L})$.

With these items, we're done with the proof.

□

Side note: Reid briefly mentions that from these propositions-definitions the algebraic subsets of $\mathbb{A}^n_k$ form the closed sets of a topology on $\mathbb{A}^n_k$ called the *Zariski topology*. I'm just mentioning the name here, just in case it shows up in a different context. Reid says the Zariski topology "might cause trouble to some students", adding: "[...]since it is only being used as a language, and has almost no context, the difficulty is likely to be psychological rather than technical."

4 The correspondence $\mathcal{I}$

Definition 4.1. As a kind of inverse to $\mathcal{V}$ there is a correspondence

$$\left\{J \overset{\text{idl}}{\subset} \mathcal{A}\right\} \overset{\mathcal{I}}{\leftarrow} \left\{\text{subsets } X \in \mathbb{A}^n_k\right\}$$

defined by

$$\mathcal{I}(X) = \{f \in \mathcal{A} \,|\, f(P) = 0 \;\forall\; P \in X\} \leftarrow X.$$

Basic idea: $\mathcal{I}$ takes a subset X to the ideal of functions vanishing on it.

Proposition 3.2.

1. $\mathcal{I}(\mathbb{A}^n_k) = \{0\}$; $\quad \mathcal{I}(\varnothing) = \mathcal{A}$.
2. $X \subset Y \implies \mathcal{I}(X) \supset \mathcal{I}(Y)$. ("reverses inclusion")
3. For any $X \subset \mathbb{A}^n_k$, $X \subset \mathcal{V}(\mathcal{I}(X))$, with equality $\iff$ X is an algebraic set.
4. For $J \subset A$, $J \subset \mathcal{I}(\mathcal{V}(J))$, this inclusion may well be strict.

Proof:

1. By definition, $\mathcal{I}(\mathbb{A}^n_k)$ is the set of polynomials in $\mathcal{A}$ that vanish at *all* points $P \in \mathbb{A}^n_k$. This holds only if $f = 0$, i.e., $\mathcal{I}(\mathbb{A}^n_k) = \{0\}$. I'll get back to the second sub-item after proving item (4).
2. This one is similar to second item of Proposition 3.3. Suppose $X \subset Y \subset \mathbb{A}^n_k$. Then any $f \in \mathcal{A}$ such that $f(P) = 0, \forall P \in Y$ necessarily vanishes at all $P \in X$ as well. This means $f \in \mathcal{I}(X)$. So $\mathcal{I}(Y) \subset \mathcal{I}(X)$.
3. (*tautology + condition for equality*) If $\mathcal{I}(X)$ is the set of $f \in \mathcal{A}$ such that $f(P) = 0 \,\forall P \in X$, then evidently $\forall P \in X$, $f(P) = 0$, i.e., $X \in \mathcal{V}(\mathcal{I}(X))$. Therefore, $X \subset \mathcal{V}(\mathcal{I}(X))$. If $X = \mathcal{V}(\mathcal{I}(X))$ then X has the form $\mathcal{V}(\text{ideal})$. So X is an algebraic set, by definition 3.2. If $X = \mathcal{V}(I_0)$ is an algebraic set, then $\mathcal{I}(X)$ contains at least I_0, and so $\mathcal{V}(\mathcal{I}(X)) \subset \mathcal{V}(I_0) = X$ (by (2)). So, equality occurs exactly when X is an algebraic subset of $\mathbb{A}^n_k$.
4. (*tautology*) Staying with the definition: $\mathcal{I}(\mathcal{V}(J))$ is the set of functions vanishing at all points of $\mathcal{V}(J)$, and so for any point of $\mathcal{V}(J)$, any function of J vanishes at it. So $J \subset \mathcal{I}(\mathcal{V}(J))$.

5. As promised, we look at the statement $\mathcal{I}(\varnothing) = \mathcal{A}$ of item (1) again. By replacing J in item (4) by $\mathcal{A}$, we get $\mathcal{A} \subset \mathcal{I}(\mathcal{V}(\mathcal{A}))$. But $\mathcal{I}(\dots) \subset \mathcal{A}$ and $\mathcal{V}(\mathcal{A}) = \varnothing$ (by Proposition 3.3(1)), so we have $\mathcal{I}(\varnothing) = \mathcal{A}$.

□

Example 3.3. Here is an Fernando's example to illustrate the inclusion in item (3). Let $X = \{(x,0) \,|\, x > 0\}$, i.e. X is the positive x-axis. Then $\mathcal{I}(X)$ is the ideal generated by y of functions that vanish on X. But of course any function $f \in \mathcal{I}(X)$ will also vanish on the negative x-axis, and so $\mathcal{V}(\mathcal{I}(X))$ is the entire x-axis. We see that $X \subset \mathcal{V}(\mathcal{I}(X))$.

□

The following examples illustrate how the inclusion in (3) may be strict.

Example 3.4. This is Example 1 from Reid's. Suppose k is not algebraically closed, and let $f \in k[X]$ be a nonconstant polynomial not having root in k (because k is not algebraically closed). The ideal $J = \langle f \rangle \subset k[X]$. Since $1 \notin J$ (because any $f \in J$ is nonconstant), we have that $J \neq k[X]$. But

$$V(J) = \left\{ P \in \mathbb{A}_k^{n=1} | f(P) = 0 \,\forall\, f \in J \right\} = \varnothing,$$

(because any f has no root in k). So, $\mathcal{I}(\mathcal{V}(J)) = k[X]$, by item (1). Hence we see that $J \subsetneq \mathcal{I}(\mathcal{V}(X))$.

□

Example 3.5. For any $f \in k[X_1, \dots, X_n]$ and $a \geq 2$, $f^a(P) = 0 \iff f(P) = 0$ (l.t.r.). Therefore, $\mathcal{V}(\langle f^a \rangle) = \mathcal{V}(\langle f \rangle)$. Further, $f \in \mathcal{V}(\mathcal{I}(\langle f^a \rangle))$, but usually $f \notin \langle f^a \rangle$. So, we see that $\langle f \rangle \subsetneq \mathcal{V}(\mathcal{I}(\langle f^a \rangle))$, usually.

□

5 Addendum: “Hilbert Basis Theorem” origins

This article discusses the *theory of invariants*, from which the Hilbert Basis Theorem originated. The Hilbert Basis Theorem generalizes Paul Gordan’s results on invariants. Gordan was the person who famously said, about Hilbert’s proof of the theorem, “This is not mathematics; this is theology!”