Noetherian Rings and Affine Algebraic Sets

Fall 2017

For reference: I will be using section 15.1 of Dummit and Foote.

Throughout this section: R is a commutative ring with $1 \neq 0$.

– Recall the definition of a *Noetherian ring* R: There are no infinite increasing chains of ideals in R.

Proposition 1. *If R is Noetherian and $I \trianglelefteq R$ then R/I is also Noetherian. Also, any homomorphic image of a Noetherian ring is Noetherian.*

Proof. If $I \trianglelefteq R$, then any infinite ascending chain of ideals in R/I corresponds to an infinite ascending chain of ideals in R (by *Lattice Isomorphism Theorem*):

$$(R/J)/(J/I) \cong R/I **$$

Thus, R/I is Noetherian if R is.

For any homomorphism $\varphi : R \to S$, the following holds by the First Isomorphism Theorem.

$$R/\ker\varphi \cong \varphi(R)$$

As R is Noetherian and $\ker\varphi \trianglelefteq R$, then by the first part, $R/\ker\varphi$ is Noetherian and hence $\varphi(R)$ is Noetherian by the isomorphism. □

Theorem 1. *TFAE:*

1. *R is Noetherian*

2. *Every non-empty set of ideals of R cotnains a maximal element under inclusion.*

3. *Every ideal of R is finitely generated.*

– This theorem follows directly by the analogous theorem for modules (taking $M = R$ as an R-module over itself), then ideals of R correspond exactly to R-submodules of R.

Theorem 2. *(Hilbert's Basis Theorem)*

If R is Noetherian, then $R[x]$ is Noetherian.

Proof. To show that $R[x]$ is Noetherian, let $I \trianglelefteq R[x]$ be an arbitrary ideal (i.e., will be shown that I is finitely generated).

Let $L = \{$all leading coefficients of polynomials in $I\}$. L is an ideal of R: $0 \in L$. Also, let $f = ax^d + \cdots +, g = bx^e + \cdots + \in I$ be polynomials of degree d and e and leading cofficients a and b. Let $r \in R$ be arbitrary.

$$\Rightarrow ra - b = 0 \text{ or it is the leading coefficient of } rf - g$$

Since $0 \in L$ and $(rf - g) \in I$, then $ra - b \in L$ for all $r \in R, a, b \in L$. Hence, $L \trianglelefteq R$.

As R is Noetherian, then L is finitely generated. For some $a_i \in R$, let

$$L = \langle a_1, a_2, \ldots, a_n \rangle$$

Associate $f_i \in I$ with leading coefficient a_i for each $i = 1, 2, \ldots, n$. Let:

$$e_i = \deg f_i;$$

$$N = \max\{e_1, e_2, \ldots, e_n\}$$

Now, for each $d \in \{0, 1, \ldots, N-1\}$, let

$$L_d = \{\text{leading coefficients of polynomials in } I \text{ of degree d}\} \cup \{0\}$$

Similar argument shows that $L_d \trianglelefteq R$ is an ideal. Again as R is Noetherian, then L_d is finitely generated for each d. For each $L_d \neq \{0\}$, let $b_{d,i} \in R$ be such that

$$L_d = \langle b_{d,1}, b_{d,2}, \ldots, b_{d,n_d} \rangle$$

Associate a polynomial $f_{d,i} \in I$ of degree d with leading coefficient $b_{d,i}$.

Claim:

$$I = \langle \{f_1, f_2, \ldots, f_n\} \cup \{f_{d,i} \mid 0 \leq d < N, q \leq i \leq n_d\} \rangle$$

To show this, denote $I' = \langle \{f_1, f_2, \ldots, f_n\} \cup \{f_{d,i} \mid 0 \leq d < N, q \leq i \leq n_d\} \rangle$.

Clear that $I' \subset I$ since all generators are elements of I.

On the other hand, if $I \neq I'$, then there exists $f \neq 0, f \in I$ of minimum degree with $f \notin I'$.

Let $d = \deg f$ and a the leading coefficient of f.

First, suppose $d \geq N$. Since $a \in L$, can write a as an R-linear combination of the generators of L:

$$a = r_1 a_1 + \cdots + r_n a_n$$

Then,

$$g = r_1 x^{d-e_1} f_1 + \cdots + r_n x^{d-e_n} f_n \in I'$$

and $\deg g = d$ and the leading coefficient of g is a. Then, $f - g \in I$ is a polynomial in I of smlaler degree than f. By *minimality* of f, this implies that $f - g = 0 \Rightarrow f = g \in I'$, ↯contradiction.

Now, suppose $d < N$. Then $a \in L_d$ for some $d < N$, so can write

$$a = r_1 b_{d,1} + \cdots + r_{n_d} b_{d,n_d}$$

for some $r_i \in R$. Then,

$$g = r_1 f_{d,1} + \cdots + r_{n_d} f_{n_d} \in I'$$

and $\deg g = d$ and leading coefficient $a \Rightarrow$ leads to the same contradiction as before.

$\Rightarrow$, $I = I'$ and so I is finitely generated $\Rightarrow R[x]$ is Noetherian.

□

Corollary 2. *The polynomial ring $k[x_1, x_2, \ldots, x_n]$ with coefficients from a field k is Noetherian.*

Definition 3. For a field k, a ring R is a *k-algebra* if $k \subseteq Z(R)$ and $1_k = 1_R$.

Definition 4. A *finitely generated k-algebra* R is generated by k together with some finite set $\{r_1, r_2, \ldots, r_n\} \subset R$.

Definition 5. A *k-algebra homomorphism* between two k-algebras R and S is a ring homomorphism $\psi : R \to S$ that is the identity on k: $\psi|_k = \mathrm{id}_k$.

Remark 6. If R is a k-algebra $\Rightarrow$ R is both a ring and a vector space over k. BUT, distinguish the generators:

- The polynomial ring $R = k[x_1, x_2, \ldots, x_n]$ is a finitely generated k-algebra since $x_1, x_2, \ldots, x_n$ are *ring* generators.
- For $n > 0$, R is *infinite dimensional* as a vector space over k.

Corollary 7. *The ring R is a finitely generated k-algebra if and only if there is some surjective k-algebra homomorphism $\varphi : k[x_1, x_2, \ldots, x_n] \to R$ from the polynomial ring in a finite number of variables onto R that is the identity map on k. Any finitely generated k-algebra is therefore Noetherian.*

Proof. $\Rightarrow$ First, if R is finitely generated as a k-algebra by $r_1, r_2, \ldots, r_n$, define

$$\varphi : k[x_1, x_2, \ldots, x_n] \to R$$

$$\varphi : x_i \mapsto r_i \text{ for all } i \text{ and}$$

$$\varphi : a \mapsto a \text{ for all } a \in k$$

$\Rightarrow$ φ extends uniquely to a surjective ring homomoprhism.

$\Leftarrow$ On the other hand, if $\varphi : k[x_1, x_2, \ldots, x_n] \to R$ is a surjective ring homomorphism, then the images of $x_1, x_2, \ldots, x_n$ generate R as a k-algebra, then R is finitely generated.

i.e., for any finitely generated k-algebra R, by the first isomorphism theorem:

$$k[x_1, \ldots, x_n]/\ker\varphi \cong R$$

Since $k[x_1, x_2, \ldots, x_n]$ is Noetherian, any finitely generated k-algebra is thus a quotient of a Noetherian ring $\Rightarrow$ hence also Noetherian by proposition (any homomorphic image of a Noetherian ring is Noetherian). □

Basic idea behind *algebraic geometry*: To equate geometric questions with algebraic questions involving ideals in rings such as $k[x_1, x_2, \ldots, x_n]$.

– Noetherian nature of these rings reduces questions to finitely many algebraic equations.

– First consider the principal geometric object: An *algebraic set* of points.

1 Affine Algebraic Sets

Definition 8. *Affine n-space over k*: The set $\mathbb{A}^n$ of n-tuples of elements of the field k.

Definition 9. *$k[\mathbb{A}^n]$: coordinate ring of $\mathbb{A}^n$* $\to$ Viewing polynomials in $k[x_1, x_2, \ldots, x_n]$ as k-valued functions $f : \mathbb{A}^n \to k$ on $\mathbb{A}^n$ by evaluating f at the points in $\mathbb{A}^n$:

$$k[\mathbb{A}^n] = \{f : \mathbb{A}^n \to k \mid f \in k[x_1, x_2, \ldots, x_n], f(a_1, a_2, \ldots, a_n) \in k\}$$

Define $\mathcal{Z}(S)$ for any $S \subset k[\mathbb{A}^n]$ as the set of points where all functions in S are zero:

$$\mathcal{Z}(S) = \{(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } f \in S\}$$

where

$$\mathcal{Z}(\varnothing) = \mathbb{A}^n$$

Definition 10. An *Affine Algebraic Set* is a subset $V \subset \mathbb{A}^n$ such that V is the set of common zeros of some set S of polynomials.

– i.e., $V = \mathcal{Z}(S)$ for some $S \subset k[\mathbb{A}^n] \Rightarrow V$ is called the *locus of S in $\mathbb{A}^n$*.

– If $S = \{f\}$ or $\{f_1, f_2, \ldots, f_m\}$: we write $\mathcal{Z}(f)$ or $\mathcal{Z}(f_1, \ldots, f_m)$ and call it the locus of f or $f_1, f_2, \ldots, f_m$.

– Note: locus of a single polynomial in the form $f - g$ is the same as the solutions in affine n-space of the equation $f = g \Rightarrow$ affine algebraic sets are the solution sets to systems of polynomial equations.

Example 11. If $n = 1$, then $\mathcal{Z}(f) = \{\text{the set of roots of } f \text{ in } k\}$ for $f \in k[x]$.

– Algebraic sets in $\mathbb{A}^1$ are $\varnothing$, any finite set, and k.

Example 12. Any finite subset of $\mathbb{A}^n$ is an algebraic set:

Since $\{(a_1, a_2, \dots, a_n)\} = \mathcal{Z}(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$.

Example 13. Can define lines, planes in $\mathbb{A}^n$: called *linear algebraic sets*: the loci of sets of linear polynomials of $k[x_1, x_2, \dots, x_n]$.

e.g., a line in $\mathbb{A}^2$ is defined by $ax + by = c$ which is the locus of the polynomial $f(x, y) = ax + by - c \in k[x, y]$.

– a line in $\mathbb{A}^3$ is the locus of 2 linear polynomials of $k[x, y, z]$ that are not multiples of each other.

$\rightsquigarrow$ The coordinate axes, coordinate planes, etc. in $\mathbb{A}^n$ are all algebraic sets.

– e.g., the x-axis in $\mathbb{A}^3$ is the zero set $\mathcal{Z}(y, z)$ and the xy-plane is the zero set $\mathcal{Z}(z)$.

Remark 14. $\mathcal{Z}(f)$ for a nonconstant polynomial f: called *hypersurface in $\mathbb{A}^n$*.

e.g., $\mathcal{Z}(y - x^2)$ is the parabola $y = x^2$.

- $\mathcal{Z}(x^2 + y^2 - 1)$ is the unit circle.

- $\mathcal{Z}(xy - 1)$ is the hyperbola $y = \frac{1}{x}$.

Properties of Affine Algebraic Sets

Let $S, T \subset k[\mathbb{A}^n]$.

1. If $S \subset T$ then $\mathcal{Z}(T) \subset \mathcal{Z}(S)$ ($\mathcal{Z}$ is *contravariant*).

2. $\mathcal{Z}(S) = \mathcal{Z}(I)$ where $I = (S)$ is the ideal in $k[\mathbb{A}^n]$ generated by S.

3. Intersection is an algebraic set. In fact:

$$\mathcal{Z}(S) \cap \mathcal{Z}(T) = \mathcal{Z}(S \cup T)$$

Generally: an arbitrary interscetion of algebraic sets is an algebriac set.

4. Union of 2 algebraic sets is an algebraic set:

$$\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$$

Where I and J are ideals.

5. $\mathcal{Z}(0) = \mathbb{A}^n$ and $\mathcal{Z}(1) = \varnothing$ (0 and 1 constant functions)

By property (2), **every algebraic set is the algebraic set corresponding to an *ideal* of the coordinate ring**:

$$\mathcal{Z} : \{\text{ideals of } k[\mathbb{A}^n]\} \to \{\text{affine algebraic sets in } \mathbb{A}^n\}$$

Since every ideal I in Noetherian ring $k[x_1, x_2, \ldots, x_n]$ is finitely generated, $I = (f_1, f_2, \ldots, f_q)$, then from property (3);

$$\mathcal{Z}(I) = \mathcal{Z}(f_1) \cap \mathcal{Z}(f_2) \cap \cdots \cap \mathcal{Z}(f_q)$$

$\Rightarrow$ **every algebraic set is the intersection of a finte number of hypersurfaces in** $\mathbb{A}^n$.

– If V is an algebraic set in $\mathbb{A}^n$, there may be many ideals I such that $V = \mathcal{Z}(I)$. i.e., the zeros of any polynomial are the same as the zeros of all its positive powers. So

$$\mathcal{Z}(I) = \mathcal{Z}(I^k) \text{ for all } k \geq 1$$

Definition 15. A unique largest ideal that determines V: The set of ALL polynomials that vanish on V.

For any subset $A \subset \mathbb{A}^n$, define $\mathcal{I}$ as the following:

$$\mathcal{I}(A) = \{f \in k[x_1, x_2, \ldots, x_n] \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } (a_1, a_2, \ldots, a_n) \in A\}$$

$\Rightarrow \quad \mathcal{I}(A) \trianglelefteq k[x_1, x_2, \ldots, x_n]$ is an ideal and it is the *unique* largest ideal of functions that are **identically zero on** A. Defines a correspondence:

$$\mathcal{I} : \{\text{subsets in } \mathbb{A}^n\} \to \{\text{ideals of } k[\mathbb{A}^n]\}$$

Example 16. In Euclidean plane, $\mathcal{I}$ (the x-axis) is the ideal generated by y in the coordinate ring $\mathbb{R}[x, y]$.

Example 17. Over any field k, ideal of functions vanishing at $(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ is a *maximal ideal* since it is the kernel of the surjective ring homomorphism:

$$\varphi : k[x_1, x_2, \ldots, x_n] \to k$$

$$\varphi : f(x_1, x_2, \ldots, x_n) \mapsto f(a_1, a_2, \ldots, a_n)$$

$$\Rightarrow \quad \ker \varphi = (a_1, a_2, \ldots, a_n)$$

$$\Rightarrow \quad k[x_1, x_2, \ldots, x_n]/(a_1, a_2, \ldots, a_n) \cong k$$

Since k is a field, then $(a_1, a_2, \ldots, a_n) \trianglelefteq k[x_1, x_2, \ldots, x_n]$ is maximal. And thus:

$$\mathcal{I}((a_1, a_2, \ldots, a_n)) = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$$

Properties of the map $\mathcal{I}$ Let $A, B \subset \mathbb{A}^n$.

1. If $A \subset B$, then $\mathcal{I}(B) \subset \mathcal{I}(A)$ ($\mathcal{I}$ is also *contravariant*).
2. $\mathcal{I}(A \cup B) = \mathcal{I}(A) \cap \mathcal{I}(B)$.
3. $\mathcal{I}(\varnothing) = k[x_1, x_2, \ldots, x_n]$ and if k is infinite, $\mathcal{I}(\mathbb{A}^n) = 0$.
4. $A \subset \mathcal{Z}(\mathcal{I}(A))$ and if I is any ideal, then $I \subset \mathcal{I}(\mathcal{Z}(I))$.
5. If $V = \mathcal{Z}(I)$ is an algebraic set then $V = \mathcal{Z}(\mathcal{I}(V))$ and if $I = \mathcal{I}(A)$, then $\mathcal{I}(\mathcal{Z}(I)) = I$.
   - i.e.,

$$\mathcal{Z}(\mathcal{I}(\mathcal{Z}(I))) = \mathcal{Z}(I) \text{ and}$$

$$\mathcal{I}(\mathcal{Z}(\mathcal{I}(A))) = \mathcal{I}(A)$$

- Last property shows that $\mathcal{Z}$ and $\mathcal{I}$ act as inverses of each other provided one restricts to the colelction of algebraic sets $V = \mathcal{Z}(I) \in \mathbb{A}^n$ and to the set of ideals in $k[\mathbb{A}^n]$ of the form $\mathcal{I}(V)$.

Definition 18. If $V \subset \mathbb{A}^n$ is an algebraic set, $k[\mathbb{A}^n]/\mathcal{I}(V)$: the *coordinate ring of V*, denoted by $k[V]$.

Remark 19. For $V = \mathbb{A}^n$ and k infinite $\Rightarrow \mathcal{I}(V) = 0$ (so terminology extends here).

– Polynomials in $k[\mathbb{A}^n]$ define k-valued functions on V simply by restricting these functions on $\mathbb{A}^n$ to the subset V.

– 2 such polynomial functions f and g define the SAME function on V iff $f - g = 0$ on V, i.e., $f - g \in \mathcal{I}(V)$.

$\Rightarrow$ the cosets $\overline{f} = f + \mathcal{I}(V)$ are precisely the restrictions to V of ordinary polynomial functions f from $\mathbb{A}^n$ to k.

– If x_i denotes the i^{th} coordinate function on $\mathbb{A}^n$ (i.e., projecting an n-tuple onto its i^{th} component), then the restriction $\overline{x}_i$ of x_i to V is an element of $k[V]$ (just gives the i^{th} component of the elements in V viewed as a subset of $\mathbb{A}^n$).

$\Rightarrow$ $k[V]$ is finitely generated as a k-algebra by $\overline{x}_1, \dots, \overline{x}_n$.

Example 20.

$V = \mathcal{Z}(xy - 1)$, this is the hyperbola $y = \frac{1}{x} \in \mathbb{R}^2$.

$\Rightarrow$ $\mathbb{R}[V] = \mathbb{R}[x, y]/(xy - 1)$

Then the polynomials $f(x, y) = x$ and $g(x, y) = x + (xy - 1)$ (different functions on $\mathbb{R}^2$) define the *same function on the subset V*.

e.g., at the point $(\frac{1}{2}, 2) \in V$, $f(\frac{1}{2}, 2) = g(\frac{1}{2}, 2) = \frac{1}{2}$.

In the quotient ring $\mathbb{R}[V]$,

$$\overline{xy} = 1$$

$$\Rightarrow \quad \mathbb{R}[V] \cong \mathbb{R}\left[x, \frac{1}{x}\right]$$

So for any function $\overline{f} \in \mathbb{R}[V]$ and any $(a, b) \in V$,

$$\overline{f}(a, b) = f\left(a, \frac{1}{a}\right)$$

where $f \in k[x, y] \mapsto \overline{f} \in k[V]$.

Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be two algebraic sets.

– Most natural algebraic maps between V and W will be defined by polynomials (since the sets are defined by the vanishing of polynomials).

Definition 21. A morphism of algebraic sets is a map $\varphi : V \to W$ such that there exist polynomials $\varphi_1, \varphi_2, \ldots, \varphi_m \in k[x_1, x_2, \ldots, x_n]$ such that

$$\varphi((a_1, a_2, \ldots, a_n)) = (\varphi_1(a_1, a_2, \ldots, a_n), \ldots, \varphi_m(a_1, a_2, \ldots, a_n))$$

for all $(a_1, a_2, \ldots, a_n) \in V$.

The map $\varphi : V \to W$ is an isomorphism of algberaic sets if there is a morphism

$$\psi : W \to V \text{ with}$$

$$\varphi \circ \psi = 1_W \text{ and } \psi \circ \varphi = 1_V$$

– morphism of algebraic sets is also called a *polynomial map* or *regular map* of algebraic sets.

Remark 22. In general, the polynomials $\varphi_1, \varphi_2, \ldots, \varphi_m \in k[x_1, x_2, \ldots, x_n]$ are NOT uniquely defined.

e.g., both $f = x$ and $g = x + (xy - 1)$ in the preceding example define the same morphism from $V = \mathcal{Z}(xy - 1)$ to $W = \mathbb{A}^1$.