0.1 Noetherian rings and the Hilbert Basis Theorem

Definition A ring R is *noetherian* if it satisfies the ascending chain condition, namely, that every ascending chain of ideals is eventually stationary.

Concretely, given a chain of ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$, there exists some m such that $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots$.

Lemma Let R be a ring. The following are equivalent.

- Every ideal of R is finitely generated.
- R satisfies ACC
- Every nonempty collection of ideals $\{\mathfrak{a}_i : i \in \mathcal{I}\}$ has a maximal element.

Proof *Suppose every ideal of R is finitely generated. Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ be an ascending chain of ideals. Let $\mathfrak{a} = \cup \mathfrak{a}_i$. It's an ideal of R. By hypothesis, $\mathfrak{a} = (f_1, \cdots, f_r)$ for r elements of $\mathfrak{a}$. For each i, $1 \le i \le r$, there's an n_i so that $f_i \in \mathfrak{a}_{n_i}$. Let $n = \max n_i$. Then $f_1, \cdots, f_r \in \mathfrak{a}_n$, so that $\mathfrak{a} \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \cdots \mathfrak{a}$; the chain is stationary at n.*

Suppose R satisfies the ACC. Take $i_1 \in \mathcal{I}$, and iterate the following. Suppose $i_1, \cdots, i_j$ have been chosen. If $\mathfrak{a}_{i_j}$ is maximal, stop. Otherwise, there is some $\mathfrak{a}_{i_{j+1}}$ which properly contains it. So, consider the chain $\mathfrak{a}_{i_1} \subset \mathfrak{a}_{i_2} \subset$. It's ascending, thus eventually stationary, and some $\mathfrak{a}_{i_m}$ is maximal.

Finally, suppose every nonempty collection of ideals has a maximal element. Let $\mathfrak{a}$ be any ideal. Consider the set S of all subideals of $\mathfrak{a}$ which are finitely generated. It has a maximal element, $\mathfrak{b}$. I claim that $\mathfrak{b} = \mathfrak{a}$. If not, there would be some $f \in \mathfrak{a} - \mathfrak{b}$. But then $(\mathfrak{b}, f)$ is also a finitely generated subideal of $\mathfrak{a}$, contradicting the maximality of $\mathfrak{b}$. □

A ring which satisfies these hypotheses is called noetherian.

Lemma A quotient of a noetherian ring is noetherian.

Proof Suppose R is noetherian, and consider R/I. Given $\bar{J} \subset R/I$, let $f_1, \cdots, f_r$ generate $J = \pi^{-1}(\bar{J})$; then $\bar{f}_1, \cdots, \bar{f}_r$ generate J. □

Lemma A ring R is noetherian if and only if $R[T]$ is noetherian.

Sketch Suppose $R[T]$ is noetherian. Then so is $R[T]/(T) \cong R$. Conversely, let R be noetherian, and $I \subset R[T]$ an ideal. We need to show that I is finitely generated.

Recall that a polynomial $f(T) \in R[T]$ can be written as

$$f(T) = \sum_{i=0}^{d} a_i T^i$$

where $a_i \in R$ and $a_d \neq 0$. Then $\deg(f) = d$, and the leading coefficient of f is $\mathrm{lc}(f) = a_d$.

Let $J = \mathrm{lc}(I) = \{\mathrm{lc}(f) : f \in I\}$. Show:

1. J is an ideal of R.
2. Since R is noetherian, $J = (\mathrm{lc}(f_1), \cdots, \mathrm{lc}(f_r))$ for some $f_1, \cdots, f_r \in I$. Now that that $I = (f_1, \cdots, f_r)$.

□

Corollary Let k be a field. Then any ideal in $k[x_1, \cdots, x_n]$ is finitely generated.

This means that any affine algebraic set is carved out by finitely many equations.

Definition *The Krull dimension of a ring R is the length of a largest chain of (proper) prime ideals;* $\dim R \geq n$ *if and only if there are prime ideals* $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subset \mathfrak{p}_n$.

This dimension does what you think it does – $\dim k[x_1, \cdots, x_n] = n$ *– but the proof is not obvious.*

0.2 Nullstellensatz

Lecture 3

We've indicated before that maximal ideals correspond to points, at least on the circle. This is a special case of a more general theorem, called the Nullstellensatz.

Lemma $A \subseteq B \subseteq C$ rings, A noetherian, C finitely generated as A-algebra, C finitely generated as a B-module. Then B is finitely generated as an A-algebra.

Proof *Let $x_1, \cdots, x_m$ generate C as A-algebra; we write $C = A[x_1, \cdots, x_m]$, even though these elements may not be independent, so C is not necessarily a ring of polynomials over A.*

Let $y_1, \cdots, y_n$ generate C as B-module, so that any element of C can be written as $\sum b_i y_i$, $b_i \in B$.

In particular, we can write

$$x_i = \sum_j b_{ij} y_j$$

$$y_i y_j = \sum_k b_{ijk} y_k$$

for some b_{ij}, b_{ijk} in B.

Let B_0 be the algebra, $A \subseteq B_0 \subseteq B$, generated over A by the b_{ij} and b_{ijk}. Then B_0 is noetherian.

Recall that $C = A[x_1, \cdots, x_m]$. Repeated use of the equations above means that each element of C is a B_0-linear combination of the elements $y_1, \cdots, y_m$. Therefore, C is a finitely generated B_0-module. Then – black box this – since B_0 is noetherian, and B is a submodule of C, it follows that B is a finitely generated B_0-module.

Since B_0 finitely generated as A-algebra, B is finitely generated as A-algebra. □

Zariski's lemma Let k be a field, K/k a field which is finitely generated as a k-algebra. Then K is a finite, algebraic extension of k.

Proof Choose a minimal set of generators for K as k-algebra, so that $K = k[x_1, \cdots, x_n]$. Suppose there's at least one element of K which is not algebraic. Reorder the variables so that $x_1, \cdots, x_r$ are algebraically independent over k, and $x_{r+1}, \cdots, x_n$ are algebraic over $F := k(x_1, \cdots, x_r)$. Then K is a finite algebraic extension of F, thus a finite F-module. Apply previous lemma; then F is a finitely generated k-algebra, say $F = k[y_1, \cdots, y_s]$. Can write $y_j = f_j/g_j$, $f_j, g_j \in k[x_1, \cdots, x_r]$.

Choose an irreducible polynomial h which is prime to each of the g_j, e.g., any factor of $g_1 \cdots g_s + 1$. Then $1/h \notin k[y_1, \cdots, y_s]$, since the "denominators" of $1/h$ are relatively prime to the g_j. But F is a field, thus this is a contradiction. Therefore, K is algebraic over k, thus finite algebraic. □

Nullstellensatz k algebraically closed, $R = k[x_1, \cdots, x_n]$. Then:

a. Every maximal ideal $\mathfrak{m} \subset R$ is of the form $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n) = \mathfrak{m}_P$ for some $P \in \mathbb{A}^n_k$.

b. If $J \subsetneq R$ is a proper ideal, then $\mathcal{Z}(J) \neq \emptyset$.

c. For every ideal $J \subset R$,

$$\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}.$$

Proof If $P = (a_1, \cdots, a_n) \in \mathbb{A}^n$, get a map

$$k[x_1, \cdots, x_n] \xrightarrow{\text{eval}_P} k$$

$$f \longmapsto f(a_1, \cdots, a_n)$$

Emphasize this: $f(P) = \text{eval}_P(f)$, and $f \in \mathcal{I}(P)$ if and only if $f \in \ker \text{eval}_P$.

Then $\ker \text{eval}_P$ is clearly maximal, and in fact $\ker \text{eval}_P = \mathfrak{m}_P$ as defined above. (To see this, use the change of coordinates $R = k[x_1 - a_1, \cdots, x_n - a_n]$; then eval_P sends f to its constant term, and the kernel is everything divisible by some $(x_i - a_i)$.)

Now suppose $\mathfrak{m} \subset R$ is any maximal ideal. Write $\pi : R \to R/\mathfrak{m}$ for the projection. Then

$$K := k[x_1, \cdots, x_m]/\mathfrak{m}$$

is a field, finitely generated over K, thus algebraic. Since k is algebraically closed, $k \cong K$, and we have

$$\begin{array}{ccccccc} k & \longrightarrow & k[x_1, \cdots, x_n] & \xrightarrow{\pi} & \dfrac{k[x_1, \cdots, x_n]}{\mathfrak{m}} & \longrightarrow & k \\ & & x_i & \longmapsto & & & b_i \\ a_i & \longmapsto & & & & & b_i \end{array}$$

Let b_i be the image of x_i, and let a_i be the preimage of b_i in k. Then for each i, $x_i - a_i \in \ker \pi$, so $\mathfrak{m}_{(a_1,\cdots,a_n)} \subseteq \ker \pi$. Since we already know that's maximal, this forces $\mathfrak{m} = \mathfrak{m}_{(a_1,\cdots,a_n)}$.

(b) Suppose $J \subset R$ is any proper ideal. Since R is noetherian, $J \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = \mathfrak{m}_P$ for some P, and $\{P\} = \mathcal{Z}(\mathfrak{m}_P) \subset \mathcal{Z}(J)$.

(c) Given $J \subset A$, let $V = \mathcal{Z}(J)$. We want to show that $\mathcal{I}(V) = \sqrt{J}$. Clearly, $\sqrt{J} \subseteq \mathcal{I}(V)$. Indeed, if $P \in V$, and $f \in \sqrt{J}$, then there' s some N so that $f^N \in J$. Then $f(P)^N = f^N(P) = 0$, so $f(P) = 0$.

Conversely, suppose that $f \notin \sqrt{J}$; we'll show that $f \notin \mathcal{I}(V)$. If $f \notin \sqrt{J}$, then "there is some prime divisor of J which doesn't divide f". Concretely, there's some prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \supseteq J$ but $f \notin \mathfrak{p}$. (If f were contained in every prime ideal which contains J, then f would be in the radical of J.)

Define $B = R/\mathfrak{p}$. Let $\overline{f}$ be the image of f in $R/\mathfrak{p}$. It's nonzero, thus not a zero divisor, so we can invert. Let $C = B[1/\overline{f}]$. Then C is a finitely generated k-algebra. Now choose a maximal ideal $\mathfrak{m} \subset C$. Since $\overline{f}$ is a unit in C, $\overline{f} \notin \mathfrak{m}$. (This property itself will be useful later...) Then $C/\mathfrak{m}$ is a field, finitely generated over k, thus isomorphic to k: and the image of $\overline{f}$ in C is nonzero.

Now consider

$$\begin{array}{ccccccc} k[x_1, \cdots, x_n] & \longrightarrow & B = \left(\dfrac{k[x_1, \cdots, x_n]}{\mathfrak{p}}\right) & \longrightarrow & B[1/\overline{f}] & \longrightarrow & C/\mathfrak{m} \cong k \\ x_i & \longmapsto & & & & & a_i \end{array}$$

Then consider the point $P = (a_1, \cdots, a_n)$. On one hand, $P \in \mathcal{Z}(J)$, since its maximal ideal contains J. On the other hand, $f(P) \neq 0$, since under the "evaluation at P" map it is not sent to zero. □

Corollary There is a one-to-one inclusion-reversing correspondence between algebraic sets in $\mathbb{A}^n$ and radical ideals of R.