SI112: Advanced Geometry	Spring 2018
Lecture 20-21 — May 10th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

1 Lecture 20-21

1.1 Overview of This Lecture

The goal of this two lectures is to prove Hilbert's Nullstellensatz (and its consequences).

1.2 Proof of Things

Definition 1.2.1. A proper ideal I of a ring R is called *prime* if $ab \in I$ implies $a \in I$ or $b \in I$ for any elements $a, b \in R$.

Definition 1.2.2 (maximal ideal)**.** A proper ideal m of a ring R is called *maximal* if $m \subset I$ implies $m = I$ or $I = R$ for any ideal $I \subset R$.

Example 1.2.3. The zero ideal of some ring R is prime if and only if R is an integral domain. For a field $\mathbb{F}$ the zero ideal $0 \subset \mathbb{F}$ is prime and maximal at the same time.

Proposition 1.2.4. *Let R be a ring and $I \subset R$ an ideal. Then I is prime if and only if R/I is an integral domain.*

Proof. Let $a, b \in R$ (i.e., $\overline{a}, \overline{b} \in R/I$). Then

$$ab \in I \Rightarrow a \in I \text{ or } b \in I$$

is equivalent to

$$\overline{a}\overline{b} = 0 \Rightarrow \overline{a} = 0 \text{ or } \overline{b} = 0.$$

□

Proposition 1.2.5. *Let R be a ring and m an ideal of R. Then m is a maximal ideal of the ring R if and only if R/m is a field.*

Proof.

- $\Rightarrow$) To prove that R/m is a field, we need to show that every nonzero element in R/m is invertible. Let $a + m \in R/m$ be a nonzero element in R/m. Then $Ra + m$ is an ideal properly containing m (you should verify that $Ra + m$ is an ideal). This means $Ra + m = R$. Then there exists $r \in R, \mu \in m$ such that

$$ra+\mu = 1 \iff ra+\mu+m = 1+m \iff ra+m = 1+m \iff (r+m)(a+m) = 1+m.$$

This implies that $a + m$ is invertible.

- $\Leftarrow$) Since R/m is a field, it must contain at least two elements: $0 + m = m$ and $1 + m$. Hence, m is a proper ideal of R. Let I be an ideal properly containing m. We need to show that $I = R \iff 1 \in I$. Let $a \in I - M$. Since $a + m$ is a nonzero element in a field, there exists an element $b+m$ in R/M such that $ab+m = (a+m)(b+m) = 1+m$. Hence there exists an element $\mu \in m$ such that $ab + \mu = 1 \Rightarrow 1 \in I$.

$\square$

The following corollary is a direct consequence of Proposition 1.2.4 and Proposition 1.2.5.

Corollary 1.2.6. *Let m be a maximal ideal of a ring. Then m is prime.*

Proposition 1.2.7. *The ring $\mathbb{C}[x_1, x_2, \ldots, x_n]$ contains a maximal ideal.*

Proof. $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is Noetherian. $\square$

Proposition 1.2.8. *Let I be a proper ideal in $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then there exists a maximal ideal $m \subset \mathbb{C}[x_1, x_2, \ldots, x_n]$ such that $I \subset m$.*

Proof. $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is Noetherian. $\square$

Theorem 1.2.9. *Let m be an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then m is maximal if and only if $m = \langle x_1 - \alpha_1, \ldots, x_1 - \alpha_n \rangle$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$.*

Proof.

- $\Rightarrow$) Cor 7.10\ AM (difficult).
- $\Leftarrow$) It is enough to show that $\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{\langle x_1-\alpha_1,\ldots,x_n-\alpha_n\rangle}$ is a field. For $i = 1, 2, \ldots, n$, we have $[x_i] = [\alpha_i]$ since $x_i - \alpha_i \in \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$. Hence (before this "hence", ask yourself: what is the equivalence class of $p \in \mathbb{C}[x_1, x_2, \ldots, x_n]$?)

$$\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle} \cong \mathbb{C}[\alpha_1, \alpha_2, \ldots, \alpha_n] = \mathbb{C}$$

is a field.

$\square$

Theorem 1.2.10 (Hilbert's Nullstellensatz, weak form)**.** *Let $T \neq \emptyset$ be a set of polynomials in $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then $Z(T) = \emptyset$, where $Z(T) = \{v \in \mathbb{C}^n : f(v) = 0, \forall f \in T\}$, if and only if the ideal I generated by T contains* 1.

Proof.

- $\Rightarrow$) Suppose $1 \notin I$. We will show that $Z(T) \neq \emptyset$. $1 \notin I$ implying $I \neq \mathbb{C}[x_1, x_2, \ldots, x_n]$, by Proposition 1.2.8 and Theorem 1.2.9, there exists a maximal ideal $m = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ in $\mathbb{C}[x_1, x_2, \ldots, x_n]$ such that $I \subset m$. Hence $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in Z(T)$: Let $p(\underline{x}) = \Sigma c_{\underline{w}} \underline{x}^{\underline{w}} \in T \subset m$. Then

$$0 = [p(\underline{x})] = [\Sigma c_{\underline{w}} \underline{x}^{\underline{w}}] = \Sigma c_{\underline{w}} [\underline{x}]^{\underline{w}} = \underline{\alpha} = p(\underline{\alpha}).$$

- $\Leftarrow$) There exist $t_1, t_2, \ldots, t_l \in T, r_1, r_2, \ldots, r_l \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ such that

$$r_1 t_1 + r_2 t_2 + \cdots + r_l t_l = 1.$$

  Hence $Z(T) = \emptyset$, for otherwise let $v \in Z(T)$ then we have

$$0 = r_1(v) t_1(v) + r_2(v) t_2(v) + \cdots + r_l(v) t_l(v) = 1,$$

  a contradiction.

$\square$

Definition 1.2.11. The spectrum of a ring R, denoted by $\mathrm{Spec}(R)$, is the set of all prime ideals in R.

Exercise 1.2.12. Let J be an ideal of a ring R, prove that the radical

$$\sqrt{J} = \{r \in R : r^l \in J \text{ for some } l \in \mathbb{N}^+\}$$

of J is an ideal of R.

Let R be a ring and let $f \in R$ be such that f is not nilpotent. Note that in general f is not invertible in R. What we want to do now is to construct a ring R_f and a homomorphism $\phi : R \to R_f$ such that $\phi(f)$ is invertible in R_f. Then we may want to have some manipulations on $\phi(f)$, and return back to R (e.g., via ϕ^{-1}). The construction process is called *localization*, described as below.

Let R be a ring and let $f \in R$ be such that f is not nilpotent. Define a set $T = \{1, f, f^2, \cdots\}$ and define a relation $\sim$ on $R \times T$ by

$$(r, t) \sim (r', t') \iff \text{there is some } t'' \in T \text{ such that } t''(rt' - r't) = 0.$$

The relation is an equivalence relation as you should verify.

Now consider the set $(R\times T)/\sim$ of all equivalence classes in $R\times T$ under the relation $\sim$ and write $\frac{r}{t}$ for the class of an element $(r,t)\in R\times T$, i.e., $(R\times T)/\sim=\{\frac{r}{t}: r\in R, t\in T\}$. The set $(R\times T)/\sim$ is a ring under the standard addition and multiplication of fractional arithmetic

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}, \frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}.$$

You should first verify that these two operations are well-defined. Furthermore, it is easily checked that $\frac{0}{1}$ is the zero element and $\frac{1}{1}$ is the unit element. As a more handy notation, we will write R_f instead of $(R\times T)/\sim$.

The inclusion map $i: R\to R\times T$ maps $r\in R$ to $(r,1)\in R\times T$ and the canonical homomorphism $\pi: R\times T\to R_f$ maps $(r,t)\in R\times T$ to its equivalence class $\frac{r}{t}\in R_f$. This implies $\pi i(f)$ is invertible in R_f, as desired.

Definition 1.2.13 (localization of a ring by an element in the ring)**.** Let R be a ring and $f\in R$ be such that f is not nilpotent. Let $T=\{1,f,f^2,\cdots\}$ Then $R_f=(R\times T)/\sim$ is called the *localization* of R by f.

Theorem 1.2.14 (Hilbert's Nullstellensatz, strong form)**.** *Let J be an ideal of $\mathbb{C}[x_1,x_2,\dots,x_n]$ and let $Y=Z(J)$. Then $I_Y=\sqrt{J}$.*

Proof. Let $g\in\sqrt{J}$, i.e., there exists m such that $g^m\in J$. Then g^m vanishes on $Z(J)$, and thus g vanishes on $Z(J)$ ($\mathbb{C}[x_1,x_2,\dots,x_n]$ is an integral domain). Hence $g\in I_{Z(J)}$. It remains to be shown that $I_{Z(J)}\subset\sqrt{J}$.

Suppose that the polynomial $f\in\mathbb{C}[x_1,x_2,\dots,x_n]$ vanishes on $Y=Z(J)$, i.e., $f\in I_{Z(J)}$. If f is nilpotent, i.e., $f^m=0\in\sqrt{J}$ for some $m\in\mathbb{N}^+$, we are done. Now suppose f is not nilpotent.

The set of polynomials $J\cup\{1-x_{n+1}f\}\subset\mathbb{C}[x_1,x_2,\dots,x_{n+1}]$ has no roots in $\mathbb{C}^{n+1}$ (for otherwise there is $v=(v_1,v_2,\dots,v_{n+1})\in\mathbb{C}^{n+1}$ such that $p(v)=0$ for all $p\in J$ and $1-v_{n+1}f(v)=0$, implying $v\in Z(J)\iff f(v)=0$, then $1=0$). Then by Theorem 1.2.10, 1 is in the ideal generated by $J\cup\{1-x_{n+1}f\}$. Hence, (a little bit tricky) there exist

$$p_1,p_2,\dots,p_s\in J,$$

$$h_1,h_2,\dots,h_s\in\mathbb{C}[x_1,x_2,\dots,x_n],$$

$$h_1',h_2',\dots,h_s'\in\mathbb{C}[x_{n+1}],$$

and

$$h\in\mathbb{C}[x_1,x_2,\dots,x_{n+1}]$$

such that

$$1=p_1h_1h_1'+p_2h_2h_2'+\cdots+p_sh_sh_s'+h(1-x_{n+1}f).$$

Let $p_i' = p_i h_i \in J$ for $i = 1, 2, \cdots, s$, then we have

$$1 = p_1' h_1' + p_2' h_2' + \cdots + p_s' h_s' + h(1 - x_{n+1} f).$$

Now let

$$\phi : \mathbb{C}[x_{n+1}] \to (\mathbb{C}[x_{n+1}])_f = \{\frac{g}{f^l} : g \in \mathbb{C}[x_{n+1}], l \in \mathbb{N}\}$$

be a ring homomorphism that maps $q(x_{n+1}) \in \mathbb{C}[x_{n+1}]$ to $q(\frac{1}{f}) \in (\mathbb{C}[x_{n+1}])_f$. For example, ϕ maps $q(x_{n+1}) = x_{n+1}^2 + x_{n+1}$ to $q(\frac{1}{f}) = \frac{1}{f^2} + \frac{1}{f}$. Noticing that $\phi(1) = \frac{1}{1}, \phi(x_{n+1}) = \frac{1}{f}$ and $\phi(h_i'(x_{n+1})) = h_i'(\frac{1}{f})$ for $i = 1, 2, \cdots, s$, we have

$$\frac{1}{1} = p_1'(x_1, x_2, \ldots, x_n) h_1'(\frac{1}{f}) + \cdots + p_s'(x_1, x_2, \ldots, x_n) h_s'(\frac{1}{f}). \tag{1.2.1}$$

Let d be the maximal degree of h_i's. Multiplying Eq. 1.2.1 by f^d we obtain

$$\frac{f^d}{1} = p_1'(x_1, x_2, \ldots, x_n)(h_1'(\frac{1}{f}) f^d) + \cdots + p_s'(x_1, x_2, \ldots, x_n)(h_s'(\frac{1}{f}) f^d).$$

Notice that for $i = 1, 2, \cdots, s$, $h_i'(\frac{1}{f}) f^d$ is of the form $\frac{g_i(f)}{1}$ where $g_i \in \mathbb{C}[x_{n+1}]$. There is a homomorphism $\psi : (\mathbb{C}[x_{n+1}])_f \to \mathbb{C}[x_{n+1}]$ that maps $\frac{g_i(f)}{1}$ to $g_i(f)$. Then

$$f^d = p_1'(x_1, x_2, \ldots, x_n) g_1 + \cdots + p_s'(x_1, x_2, \ldots, x_n) g_s,$$

which means that $f^d \in J$ and hence $f \in \sqrt{J}$. □

Proposition 1.2.15. *Let J be an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then $Z(J) = Z(\sqrt{J})$.*

Proof. We have $Z(\sqrt{J}) \subset Z(J)$ since $J \subset \sqrt{J}$. Now let $v \in Z(J)$. For each $p \in \sqrt{J}$, there is some $m \in \mathbb{N}^+$ such that $p^m \in J$, then $p^m(v) = 0 \iff (p(v))^m = 0$. Hence $p(v) = 0$ for $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is an integral domain. □

Theorem 1.2.16. *There is a one-to-one correspondence between closed sets of $\mathbb{C}^n$ and radical ideals of $\mathbb{C}[x_1, x_2, \ldots, x_n]$.*

Proof. Let Y be closed, i.e., $Y = Z(J)$ for some J being an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then

$$Y \mapsto I_Y = \sqrt{J} \mapsto Z(\sqrt{J}) = Z(J) = Y.$$

□

Remark 1.2.17. Let X be any set of $\mathbb{C}^n$. Then

$$X \mapsto I_X \mapsto Z(I_X) = \overline{X} \mapsto \sqrt{I_X} = I_{\overline{X}}.$$

Theorem 1.2.18 (Hartshorne\Prp I.1.5, p5)**.** *Let Y be a closed set $\iff$ $Y = Z(J)$ $\iff$ Y algebraic variety. Then Y can be uniquely written as $Y = Y_1 \cup \cdots \cup Y_s$, where Y_i's are irreducible closed sets.*

Proof. □

Lemma 1.2.19. *Let R be a ring and P a prime ideal. Let $J_1, J_2, \ldots, J_s$ be ideals of R. If $J_1 \cap \cdots \cap J_s \subset P$, then $J_i \subset P$ for some i.*

Proof. Suppose $J_i \not\subset P$ for any $i = 1, 2, \cdots, s$. Then for any $i = 1, 2, \cdots, s$ there is some $\alpha_1 \subset J_i$ such that $\alpha_i \notin P$. Let $\alpha = \alpha_1 \alpha_2 \cdots \alpha_s$. Then $\alpha \notin P$ since P is prime. But $\alpha \in J_1 \cap \cdots \cap J_s \subset P$ since J_i's are ideals of R. This is a contradiction. □

Definition 1.2.20 (Irreducible Space)**.** A topological space X is called *irreducible* if X is not the union of any two proper closed sets, i.e., there are no closed subsets $Y_1, Y_2 \subsetneq X$ such that $X = Y_1 \cup Y_2$.

Theorem 1.2.21. *Let Y be a closed set of $\mathbb{C}^n$. Then Y is irreducible if and only if I_Y is prime.*

Proof.

- $\Rightarrow$) Let $f, g \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ such that $fg \in I_Y$. Then we have

  $$\langle fg \rangle \subset I_Y \Rightarrow Y = \overline{Y} = Z(I_Y) \subset Z(\langle fg \rangle) = Z(fg) = Z(f) \cup Z(g),$$

  which implies $Y = (Z(f) \cap Y) \cup (Z(g) \cap Y)$. Since Y is irreducible and $Z(f) \subset Y, Z(g) \subset Y$ are closed, either $Y = Z(f) \cap Y$ or $Y = Z(g) \cap Y$. Without loss of generality let $Y = Z(f) \cap Y$, then we have

  $$Y \subset Z(f) \Rightarrow \langle f \rangle \subset \sqrt{\langle f \rangle} = I_{Z(\langle f \rangle)} = I_{Z(f)} \subset I_Y.$$

  Hence I_Y is prime.

- $\Leftarrow$) Suppose $Y = Y_1 \cup Y_2$ where Y_1, Y_2 are closed subsets of Y. Then we have

  $$I_Y = I_{Y_1 \cup Y_2} = I_{Y_1} \cap I_{Y_2} \Rightarrow I_Y \subset I_{Y_1}, I_Y \subset I_{Y_2}. \tag{1.2.2}$$

  By Lemma 1.2.19, we have either $I_{Y_1} \subset I_Y$ or $I_{Y_2} \subset I_Y$ and hence either

  $$I_{Y_1} = I_Y \iff Y_1 = Z(I_{Y_1}) = Z(I_Y) = Y$$

  or

  $$I_{Y_2} = I_Y \iff Y_2 = Z(I_{Y_2}) = Z(I_Y) = Y.$$

  Consequently Y is irreducible.

□

1.3 Further Reading

- Chapter 1, Algebraic Geometry and Commutative Algebra: https://www.springer.com/la/book/9781447148289
- Chapter 16, Abstract Algebra: Theory and Applications