Math 494

Yiwei Fu

Jan 27, 2022

Finish the proof on Hilbert's Nullstellenstaz.

Corollary. *If I is an ideal of $\mathbb{C}[x_1, \ldots, x_n]$ generated by $f_1, \ldots, f_k$, and V is the set of all $\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ s.t. $f_i(\alpha) = 0\ \forall i$, then the maximal ideals of R/I are in bijection with V.*

R/I is called the "coordinate ring".

Proof. Correpondence Theorem $\implies$ maximal ideals of R/I are $\pi(M)$ where $\pi : R \twoheadrightarrow R/I$ and M is a maximal ideal of R containing I. (also $M \neq M' \implies \pi(M) \neq \pi(M')$)

An ideal M of R contains $I \iff M$ contains $f_i\ \forall i$.

M is maximal $\iff M = (x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n)$. So $f_i \in M \iff f_i(\alpha) = 0$.

So the maximal idals of R containing I are $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ where $f_i(\alpha) = 0\ \forall i$. ■

Lemma (Zorn's lemma)**.** *If a partially ordered set S in which every chain has a upper bound, then S has at least one maximal element.*

Corollary. *If $R =$ ring and $I \neq (1)$ is an ideal of R, then I is contained in a maximal ideal.*

Proof. Let $S = \{$ideals containing I which aren't $(1)\}$ partially ordered under containment. If T is a totally ordered subset of S then let $J = \bigcup_{I' \in T} I'$. J is an ideal not containing (1). We can see that $J \in T$ and is an upper bounde of T.

By Zorn's lemma we conclude that S contains a maximal element, which is a maximum ideal containing I. ■

Corollary. *If a ring R has no maximal ideals then R is the zero ring.*

Corollary. *If $f_1, \ldots, f_k \in R := \mathbb{C}[x_1, \ldots, x_k]$ have no common zeros in $\mathbb{C}^n$, then the ideal*

$(f_1, \ldots, f_k)$ *is* (1) *i.e.*

$$1 = g_1 f_1 + \ldots + g_k f_k, g_1, \quad \ldots, g_k \in \mathbb{C}[x_1, \ldots, x_k]$$

Proof. If $(f_1, \ldots, f_k) \neq (1)$ then it is contained in a maximal ideal of R which is $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ and $f_i(\alpha) = 0\ \forall i \implies f_i$'s have a common zero, a contradiction. ∎

Theorem (Bezout's theorem)**.** *If $f(x,y)$ and $g(x,y)$ are polynomials in $\mathbb{C}[x,y]$ with no (non-constant) common factor. Then they only have finitely many common zeros.*

In fact

$$\#\text{of zeros} \leq (\text{total deg of } f(x,y)) \cdot (\text{total deg of } g(x,y)).$$

Proof. We have $\mathbb{C}[x,y] = (\mathbb{C}[y])[x] \subseteq (\mathbb{C}(y))[x]$.

The ideal (f,g) in $(\mathbb{C}(y))[x]$ is principal, say it's (h) where $h \in (\mathbb{C}(y))[x]$. If $(h) \neq (1)$ then

$$h = \frac{h_1(x,y)}{u(y)}, h_1 \in \mathbb{C}[x,y], u \in \mathbb{C}[y], u \neq 0.$$

But $u(y)$ is a unit in $\mathbb{C}(y)[x] \implies (h) = (h_1)$.

So we may assume $h \in \mathbb{C}[x,y], (h) \neq (1)$ and $h \mid f, h \mid g$ in $\mathbb{C}(y)[x]$

$$\begin{aligned} &\implies hA = f, hB = g, && A, B \in \mathbb{C}(y)[x] \\ &\implies hA_1 = fu_1, hB_1 = gu_2, && A_1, B_1 \in \mathbb{C}[x,y], u_1, u_2 \in \mathbb{C}[y] \end{aligned}$$

If $g_1 g_2 \in \mathbb{C}^*$ then there is a contradiction. So assume $u_1 \notin \mathbb{C}^*$. Then u_1 has a root α

$$\begin{aligned} &\implies h(x,\alpha)A_1(x,\alpha) = 0 \text{ in } \mathbb{C}[x] \\ &\implies h(x,\alpha) = 0 \text{ or } A_1(x,\alpha) \\ &\implies y - \alpha \mid h(x,\alpha) \text{ or } y - \alpha \mid A_1(x,\alpha) \end{aligned}$$

The latter is not possible, and we can always factor out $y - \alpha$ from $h(x,\alpha)$ and apply this process until we arrive at a contradiction. ∎