

# Lecture 2-3

$$A^n = \mathbb{C}^n \quad R = \mathbb{C}[x_1, \dots, x_n]$$

$\mathcal{C} = \{Z(T) \mid \forall T \subset \mathbb{R}\}$  - affine closed

$U = \{A^n \setminus Z(T) \mid \forall T\}$  - open subsets

$$p \in A^n, p = (e_1, \dots, e_n), p = Z(x_1 - e_1, \dots, x_n - e_n)$$

Theorem (Weak Hilbert Nullstellensatz). - There is a bijection between points in  $A^n$  and maximal ideals in  $R$ , given as follows:  
 $p = (e_1, \dots, e_n) \longleftrightarrow (x - e_1, \dots, x - e_n) \subset R$ .

Proof:

Fact:  $I \subsetneq R$ ,  $I$  is maximal  $\Leftrightarrow R/I$  is a field

Part 1: The ideal  $(x - a) \subset \mathbb{C}[x]$  is maximal.

$$\mathbb{C}[x] \xrightarrow{\sigma} \mathbb{C}$$

$\sigma$  is onto

$$f(x) \mapsto f(a)$$

$$\ker(\sigma) = (x - a) \Rightarrow \mathbb{C} \cong \mathbb{C}[x]/(x - a) \Rightarrow (x - a) \text{ is maximal.}$$

↑  
goal.

Part 2: goal: every maximal ideal  $M \subset R$  is  $M = (x - a)$  ( $\exists a \in \mathbb{C}$ ).

The ring  $\mathbb{C}[x]$  is P.I.D ( $\forall$  ideal  $I$  can be generated by 1 el.)

$$\exists g \in \mathbb{C}[x]: M = (g)$$

$\mathbb{C}$  is alg. closed  $\Rightarrow \exists a \in \mathbb{C}: g(a) = 0 \Rightarrow g(x) = (x - a)q(x)$ ,  $q$ -polynomial,  $\deg q < \deg g$ .

The ideal  $(x - a) \supset (g)$ .

$\Rightarrow$  they are equal!

↑  
a maximal ideal  
↖ a maximal by hyp.

General case, Part 1:  $\forall m$  goal:  $(x_1 - a_1, \dots, x_m - a_m)$  is maximal in  $R$ .

$$\mathbb{C}[x_1, \dots, x_m] \xrightarrow{\sigma} \mathbb{C}$$

$\sigma$  is onto

$$f(x_1, \dots, x_m) \mapsto f(a_1, \dots, a_m)$$

Claim:  $\ker \sigma = (x_1 - a_1, \dots, x_m - a_m)$ ,  $a_i = 0 \forall i = 1, \dots, m$ .

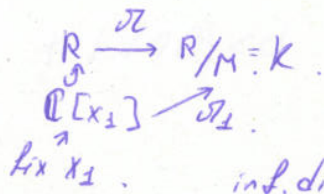
$$g \in \ker \sigma, g = \sum_{i=1}^m c_i x_i + \text{higher degree monoms} = \sum_{i=1}^m x_i h_i(x_1, \dots, x_m) \Rightarrow$$

$$\Rightarrow g \in (x_1, \dots, x_m)$$

Change coord.:  $x_i' = x_i - a_i$ .

Part 2:  $\forall$  max. ideal  $M \subset R$  is of type  $M = (x_1 - a_1, \dots, x_m - a_m)$ .

$R/M = K$  - a field.



Claim:  $\pi_1$  is not injective.  
 b.e.  $\pi_1$  is injective  $\Rightarrow$

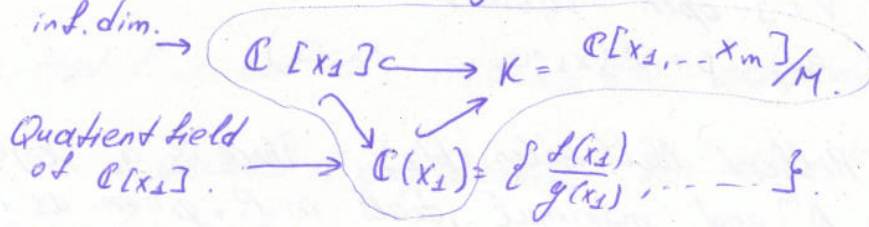
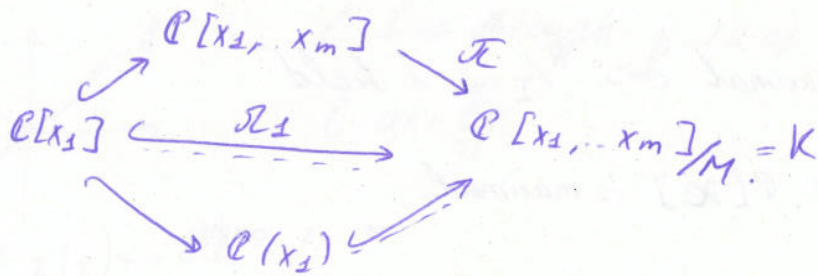


Diagram of  $\mathbb{C}$ -vector spaces.



$\dim_{\mathbb{C}} \mathbb{C}[x_1, \dots, x_m] = \#\mathcal{N}$  (is countable)  $\Rightarrow \dim_{\mathbb{C}} K$  is countable

Claim:  $\dim_{\mathbb{C}} \mathbb{C}(x) = \#\mathbb{C}$ .

$\mathcal{L} = \left\{ \frac{1}{x-a} \mid \forall a \in \mathbb{C} \right\}$ .  $\#\mathcal{L} = \#\mathbb{C}$ :

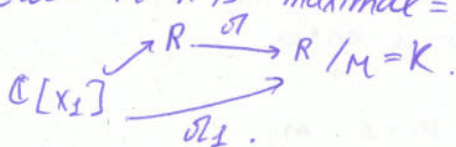
Suppose  $\sum_{j=1}^t \frac{c_j}{x-a_j} = 0$ ,  $c_j \in \mathbb{C} \setminus \{0\}$ .

$\left| -\frac{c_1}{x-a_1} \right| = \left| \sum_{j=2}^t \frac{c_j}{x-a_j} \right| \leq \sum_{j=2}^t \left| \frac{c_j}{x-a_j} \right|$

Near  $x=a_1$  this is not bounded  $\leftarrow$  is bounded. Contradiction!  $\Rightarrow$

$\Rightarrow \dim_{\mathbb{C}} \mathbb{C}(x) \geq \#\mathbb{C} \Rightarrow$  diagram is not possible!

goal:  $M \subset R$  is maximal  $\Rightarrow M = (x_1 - a_1, \dots, x_m - a_m)$ .



$\ker \pi_1 = (f) \exists f \neq 0, f \neq \text{const.}$

We can choose  $f$  of minimal degree and monic.

$\exists a \in \mathbb{C} : f(a) = 0 \Rightarrow f = (x-a)g(x)$ ,  $\deg g < \deg f$ .

$\pi_1(f) = 0 \Rightarrow \pi_1(x-a) \cdot \pi_1(g) = 0$ .

$\uparrow$   
 $K$ -field  $\mid \Rightarrow \begin{cases} \pi_1(g) = 0 \\ \pi_1(x-a) = 0 \end{cases}$  by our choice of  $f \Rightarrow f = x-a$ .



$$\Rightarrow \ker \sigma_1 = (x_1 - a_1).$$

So,  $x_1 - a_1 \in \ker \bar{\sigma}$ . (Diagram is com.)

$\forall i \in \{1, \dots, m\} \exists a_i : x_i - a_i \in \ker \bar{\sigma} \Rightarrow (x_1 - a_1, \dots, x_m - a_m) \in \ker \bar{\sigma} =$   
 $= M.$  by def. of  $\bar{\sigma}$

So,  $(x_1 - a_1, \dots, x_m - a_m) \in M$ , but  $(x_1 - a_1, \dots)$  is maximal  $\Rightarrow$   
 $\Rightarrow (x_1 - a_1, \dots) = M.$

Def:  $X \subset A^n$ ,  $\mathcal{J}(X) := \{f \in R \mid f(p) = 0 \forall p \in X\}$  - ideal of  $R$  (triv.)

Example:  $X = \{p\} \Rightarrow \mathcal{J}(p)$  is max. ideal.

Corollary of WHN: Let  $f_1, \dots, f_n \in A$ .  $\mathcal{Z}(f_1, \dots, f_n) = \emptyset \Leftrightarrow \exists h_1, \dots, h_n \in R:$

$$\sum_{i=1}^n h_i \cdot f_i = 1.$$

$$p \in \mathcal{Z}(f_1, \dots, f_s) \Leftrightarrow f_i \in \mathcal{J}(p) \quad \forall i = 1, \dots, s.$$

$\mathcal{Z}(f_1, \dots, f_n) = \emptyset \Leftrightarrow (f_1, \dots, f_n) \not\subset \mathcal{J}(p) \quad \forall p \in A^m \Leftrightarrow (f_1, \dots, f_n)$  is not contained in any max. ideal.  
 $\Leftarrow$  - triv.

$\Rightarrow (f_1, \dots, f_n) = 1 \Leftrightarrow \exists h_1, \dots, h_n : \sum h_i \cdot f_i = 1$ . - v.s.g.  
 $\uparrow$   
 by Zorn lemma.

Let  $\mathbb{C}^2 = A^2$ ,  $\mathbb{C}[x, y] = R$ .

$I = (x^3)$ ,  $X = \mathcal{Z}(I)$  is a line

$$\mathcal{J}(X) = (x).$$

Def: Let  $I$  be an ideal  $I \subset R$ , the radical of  $I$  is  $\sqrt{I} = \{f \in A : \exists d \in \mathbb{N} : f^d \in I\}$ .  $I$  is called radical if  $I = \sqrt{I}$ .

Example: 1)  $(x)$  is radical in  $\mathbb{C}[x, y]$ .

2) A maximal ideal is radical.

(Indeed,  $I \subset \sqrt{I}$ .)

Lemma:  $\mathcal{J}(X)$  is a radical ideal for every  $X$ .

proof:  $f \in \sqrt{\mathcal{J}(X)} \Leftrightarrow \exists d : f^d \in \mathcal{J}(X) \Leftrightarrow \forall p \in X (f(p))^d = 0 \Leftrightarrow f(p) = 0 \forall p \in X \Rightarrow f \in \mathcal{J}(X)$ .

Question? Let  $I_1, I_2$  be radical ideals of  $R$ .

Suppose  $\mathcal{Z}(I_1) = \mathcal{Z}(I_2)$ . Does it follow that  $I_1 = I_2$ ? Yes.

Theorem: (Hilbert Nullstellensatz): let  $I \subset R$ -ideal. If  $f \in R$  such that  $f(p) = 0 \forall p \in Z(I)$ , then  $f \in \sqrt{I}$ .

(In particular, the answer to the question is yes).

Proof: Goal:  $\sqrt{I} = J(Z(I))$ .

"<" - easy. (exercise)

goal:  $J(Z(I)) \subset \sqrt{I}$ .

$I = (f_1, \dots, f_r)$ . Let  $g \in J(Z(I))$  (i.e.  $g$  vanishes wherever  $f_1, \dots, f_r$  vanish).

(goal:  $\exists d: g^d \in I$ )

consider  $\mathbb{C}[x_1, \dots, x_m, y] \supset R$ .

$$l = l(x_1, \dots, x_m, y) = g \cdot y - 1.$$

Let  $q \in A^{m+1}$

$$g(q) = 0 \Rightarrow l(q) = -1 \neq 0. \Rightarrow$$

$\Rightarrow Z(l, f_1, \dots, f_r) = \emptyset$ . By the coroll.,  $1 = h_1 f_1 + \dots + h_{r+1} l$ , where

$$h_i = h_i(x_1, \dots, x_m, y).$$

$$l(x_1, \dots, x_m, \frac{1}{g}) = g \cdot \frac{1}{g} - 1 = 0.$$

$$1 = f_1(x) h_1(x, \frac{1}{g(x)}) + \dots + f_r(x) h_r(x, \frac{1}{g(x)}) + 0.$$

$$1 = \frac{f_1 \tilde{h}_1(x) + \dots + f_r \tilde{h}_r(x)}{g^d} \Rightarrow g^d = \sum_{i=1}^r \tilde{h}_i f_i \Rightarrow g^d \in I. \quad \therefore g \in \sqrt{I}$$