4.6. Proof of the weak Nullstellensatz

Reminder: We still need to show Thm 4.2.1:

Assume K is algebraically closed.

For any ideal $I \subseteq K[X_1, \ldots, X_n]$,

if $I \neq K[X_1, \ldots, X_n]$, then $V(I) \neq \emptyset$.

This immediately follows from:

<u>Lemma 4.6.1</u> Assume K is alg. closed.

a) If $I \subseteq K[X_1, \dots, X_n]$ is a maximal ideal, then $V(I) \subseteq K^n$ consists of exactly one point.

b) If $\underset{\{P\}}{\overset{\shortparallel}{V}} \subseteq K^n$ consists of exactly one point, then $J(V) \subseteq K[X_1, \dots, X_n]$ is a maximal ideal.

<u>Pf</u> b) $V = \{(a_1, \dots, a_n)\}$

$\Rightarrow J(V) = (X_1 - a_1, \dots, X_n - a_n)$.

$$\begin{aligned} K[X_1, \dots, X_n] &\longrightarrow K \\ f &\longmapsto f(a_1, \dots, a_n) \end{aligned}$$

has kernel $J(V)$.

$\Rightarrow K[X_1, \dots, X_n]/J(V) \cong K$ is a field.

$\Rightarrow J(V)$ is a max. ideal.

a) I maximal ideal

$\Rightarrow L := K[X_1, \dots, X_n]/I$ is a field.

There's an obvious embedding

$$\begin{aligned} K &\hookrightarrow L = K[X_1, \dots, X_n]/I \\ c &\longmapsto c \bmod I, \end{aligned}$$

so we will consider L a field extension of K.

In fact, L is a ring-finite field ext. of K, generated by $X_1, \dots, X_n \bmod I$.

$$\underset{\substack{\uparrow \\ \text{Thm 4.5.8}}}{\Longrightarrow} \quad L \text{ is a finite-dimensional } K\text{-vector space}$$
(= module-finite)

$$\underset{\substack{\uparrow \\ \text{Lemma 4.5.3}}}{\Longrightarrow} \quad L \text{ is an algebraic ext. of } K$$

$$\underset{\substack{\uparrow \\ K \text{ is algebraically closed}}}{\Longrightarrow} \quad L = K$$

In other words, the embedding

$$\begin{aligned} K &\hookrightarrow L = K[X_1, \dots, X_n]/I \\ c &\mapsto c \bmod I \end{aligned}$$

is an isomorphism.

Let a_i be the preimage of $X_i \bmod I$.

$\Rightarrow X_i - a_i \in I$ for all i

$\Rightarrow I' := (X_1 - a_1, \dots, X_n - a_n) \subseteq I$.

Both I and I' are maximal ideals, so this implies $I = I$!

$\Rightarrow \mathcal{V}(I) = \mathcal{V}(I') = \{(a_1, \dots, a_n)\}$. $\square$

$$\boxed{\text{From now on, we'll always assume that } K \text{ is algebraically closed.}}$$

(unless stated otherwise...)

Summary

$$\left\{\begin{matrix}\text{subset} \\ V \subseteq K^n\end{matrix}\right\} \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} \left\{\begin{matrix}\text{ideal} \\ I \subseteq K[x_1, \dots, x_n]\end{matrix}\right\}$$

$$\mathcal{V}(\mathcal{I}(V)) = \overline{V}$$ (Zariski closure)

(= smallest alg. subset of K^n containing V)

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$$ (radical ideal)

We obtain bijections:

$$\begin{array}{ccc}
\left\{\begin{matrix}\text{algebraic} \\ \text{subset} \\ V \subseteq K^n\end{matrix}\right\} & \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} & \left\{\begin{matrix}\text{radical} \\ \text{ideal} \\ I \subseteq K[x_1, \dots, x_n]\end{matrix}\right\} \\
\cup\!\text{I} & & \cup\!\text{I} \\
\left\{\begin{matrix}\text{one-point} \\ \text{subset} \\ V \subseteq K^n\end{matrix}\right\} & \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} & \left\{\begin{matrix}\text{maximal} \\ \text{ideal} \\ I \subseteq K[x_1, \dots, x_n]\end{matrix}\right\}
\end{array}$$

5. Irreducibility

<u>Def</u> An algebraic set $\emptyset \neq V \subseteq K^n$ is <u>irreducible</u> if you can't write $V = V_1 \cup V_2$ with any algebraic sets $V_1, V_2 \subsetneq V$.

If you can, it is called <u>reducible</u>.

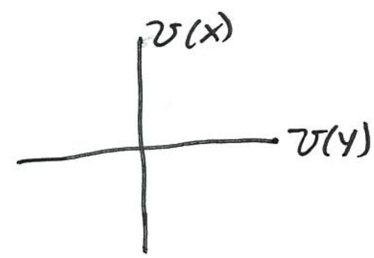
<u>Ex</u> Any one-point set is irreducible. $\bullet P$

$V = \{P\}$

<u>Ex</u> $\mathcal{V}(XY) \subseteq K^2$ is reducible

$\quad \| $

$\mathcal{V}(X) \cup \mathcal{V}(Y)$



<u>Ex</u> $\mathcal{V}(0) = K^1$ is irreducible

<u>Ex</u> $\mathcal{V}(X), \mathcal{V}(Y) \subseteq K^2$ are irreducible.

Thm 5.1 An algebraic subset $V \subseteq K^n$ is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal of $K[x_1, \dots, x_n]$.

Pf First, note that $V = \emptyset \iff \mathcal{I}(V) = K[x_1, \dots, x_n]$.
(not prime)

"$\Rightarrow$" Assume $\mathcal{I}(V) \subsetneq K[x_1, \dots, x_n]$ is not prime.

$\Rightarrow$ There are $f, g \notin \mathcal{I}(V)$ with $f g \in \mathcal{I}(V)$.

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\underbrace{V \cap \mathcal{V}(f)}_{V_1}, \underbrace{V \cap \mathcal{V}(g)}_{V_2} \subsetneq V \qquad \underbrace{(V \cap \mathcal{V}(f))}_{V_1} \cup \underbrace{(V \cap \mathcal{V}(g))}_{V_2} = V$$

$\Rightarrow V$ is reducible.

"$\Leftarrow$" Assume $V = V_1 \cup V_2$ with algebraic subsets $V_1, V_2 \subsetneq V$.

$$\Downarrow$$

$$\mathcal{I}(V_1), \mathcal{I}(V_2) \supsetneq \mathcal{I}(V)$$

Let $f \in \mathcal{I}(V_1) \setminus \mathcal{I}(V)$ and $g \in \mathcal{I}(V_2) \setminus \mathcal{I}(V)$.

Then, $f, g \notin \mathcal{I}(V)$, but $f g \in \mathcal{I}(V)$.

$\Rightarrow \mathcal{I}(V)$ is not prime. $\square$

<u>Rmk</u> Prime ideals are radical ideals.

<u>Cor 5.2</u> $\mathcal{V}(I) \subseteq K^n$ is irreducible if I is a prime ideal.

<u>Pf</u> $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$ is prime. $\square$

<u>Warning</u> $(x^2) \subseteq K[x]$ is not a prime ideal, but nevertheless $\mathcal{V}(x^2) = \mathcal{V}(x) = \{0\}$ is irreducible.
($\sqrt{(x^2)} = (x)$ is prime.)

<u>Ex</u> $\mathcal{V}(x) \subseteq K^2$ is irreducible because (x) is a prime ideal of $K[x,y]$ because $K[x,y]/(x) \cong K[y]$ is an integral domain.

<u>Ex</u> $\mathcal{V}(0) = K^n$ is irreducible.

<u>Lemma/Reminder 5.3</u>

If R is a unique factorization domain (such as $\mathbb{Z}$, $K[x_1, \dots, x_n]$), then (f) is a prime ideal if and only if $f = 0$ or $f \in R$ is irreducible.

<u>Ex</u> $V(x^2+y^2-1) \subseteq \mathbb{C}^2$ is irreducible because x^2+y^2-1 is.

$V(x^2+y^2-1)$

<u>Pf</u> Assume $X^2+Y^2-1 = fg$ for some nonconstant polynomials $f,g \in \mathbb{C}[X,Y]$.

Since X^2+Y^2-1 has degree 2 in X, either

a) f and g have degree 1 in X or

b) f has degree 0 in X and g has degree 2 in X or

c) f " 2 " g " 1 ".

Case b) (and similarly case c) is impossible:

If $f = f(Y)$ only depends on Y, take some root $b \in \mathbb{C}$ of $f(Y)$.

Then, $a^2+b^2-1 = f(b)\, g(a,b) = 0$ for all $a \in \mathbb{C}$. ↯

Hence, f and g have degree 1 in X.

Similarly, " Y.

Since X^2+Y^2-1 has total degree 2, both f and g then must have total degree 1.

$\Rightarrow f(X,Y) = pX + qY + r$ for some $p,q,r \in \mathbb{C}$ with $p,q \neq 0$.

~~(So the unit circle $V(X^2+Y^2-1)$ contains a line $V(pX+qY+r)$)~~ ↯

$\Rightarrow$ $a^2+b^2-1=0$ for all $(a,b)\in\mathbb{C}^2$ on the line given by $pa+qb+r=0$.

(The "unit circle" $V(X^2+Y^2-1)$ contains the line $V(pX+qY+r)$.)

$\rightarrow$ Plug in $a=-\dfrac{qb+r}{p}$:

$$
\begin{aligned}
0 &= p^2(a^2+b^2-1)\\
&= (qb+r)^2+p^2b^2-p^2\\
&= (q^2+p^2)b^2+2qrb+(r^2-p^2) \qquad \forall b\in\mathbb{C}
\end{aligned}
$$

$$
\Rightarrow \quad
\begin{aligned}
q^2+p^2 &= 0,\\
2qr &= 0, &\overset{q\neq 0}{\Longrightarrow}\ r=0\\
r^2-p^2 &= 0 &\Rightarrow\ p=0\ \lightning
\end{aligned}
$$

$\square$

<u>Warning</u> $X^2+Y^2-1=(X+Y+1)^2$ if $\operatorname{char}(K)=2$.