Points and Maximal Ideals

(a.k.a Hilbert's Nullstellensatz)

We establish an important bijection between the points of $Z_f(k)$ and the maximal ideals of C_f.

Definition

Let $g \in C_f$. The value of g at $(a,b) \in Z_f(k)$ is the element $\tilde{g}(a,b) \in k$ where $\tilde{g}(x,y) \in k[x,y]$ is any polynomial whose image in C_f is g.

Let $(a,b) \in Z_f(k)$. Define

$$M = \{ g \in C_f \mid g(a,b) = 0 \}.$$

$$N = (x-a)C_f + (y-b)C_f$$

that is the ideal generated by the images of $x-a, y-b \in k[x,y]$ in C_f

Claim $M = N$

Proof

As $k[x,y]/\langle x-a, y-b\rangle \cong k$, $\langle x-a, y-b\rangle$ is a maximal ideal in $k[x,y]$.

By the Taylor expansion

$$f(x,y) = \overset{0}{\overset{\shortparallel}{f(a,b)}} + (x-a)\frac{\partial f}{\partial x}(a,b) + (y-b)\frac{\partial f}{\partial y}(a,b) + \text{high order terms.}$$

$\Rightarrow$ $f(x,y) \in \langle x-a, y-b\rangle$. Thus, N is a maximal ideal of C_f.

Clearly, $N \subseteq M \neq C_f$ $\Rightarrow$ $N = M$ $\blacksquare$

Lemma

Let $f(x,y) \in k[x,y] \setminus k$. Then, $\langle f \rangle$ is not maximal.

Proof

We may assume that f is irr. o.w. $\langle f \rangle$ not even prime.

$\exists (a,b) \in \bar{k}$ s.t. $f(a,b) = 0$ (as we proved $|Z_f(\bar{k})| = \infty$). a is algebraic over k. Let $h(x) \in k[x]$ be its min poly over k. Let

$$\bar{m} = (x-a)\bar{k}[x,y] + (y-b)\bar{k}[x,y]$$

$$m = \bar{m} \cap k[x,y]$$

$\bar{m} \neq \bar{k}[x,y] \implies m \neq k[x,y]$.

Clearly $\langle f \rangle \subseteq m$. Also, $\langle h \rangle \subseteq m$.

Assume $\langle f \rangle$ max in $k[x,y]$ $\implies$ $\langle f \rangle = m$ $\implies$ $\exists g(x,y) \in k[x,y]$ with $h(x) = f(x,y)\,g(x,y)$.

Since $h(x)$ is irr $g(x,y) \in k[x,y]^*$. So,

$$k[x,y]/\langle f \rangle \cong k[x,y]/h(x) \cong \left(k[x]/\langle h \rangle\right)[y]$$

Not a field - contradiction to $\langle f \rangle$ max

$\blacksquare$

Lemma

A UFD. $M \in \operatorname{Max} A[y]$.

M not principal $\Rightarrow$ $M \cap A \neq 0$.

Proof

Let $P = M \cap A$ and L denote the field $A[y]/M$.

$P = 0 \Rightarrow \exists\, \varphi : A \hookrightarrow L$.

Extend φ to an injection $\bar{\varphi} : K \hookrightarrow L$.

This induces an extension of the natural quotient map $q : A[y] \to A[y]/M$, namely,

$\tilde{q} : K[y] \longrightarrow L$.

$K[y] \neq L$ as it is not a field

$K[y]/\ker\tilde{q} = \operatorname{Im}\tilde{q} \hookrightarrow L$

domain $\Leftarrow$ field

$\ker\tilde{q}$ is a nontrivial prime ideal in $K[y]$ that contains M.

$\Rightarrow \ker\tilde{q} = \langle f(y) \rangle$ $\quad f \in K[y]$ irr and monic - unique.

Let $f_1(y) \in A[y]$ be a primitive polynomial associated to $f(y)$.

Take $g(y) \in M = \ker q$. $\quad g(y) \in \ker \bar{q} \implies f(y) \mid g(y)$ in $K[y]$

$$\xrightarrow[\text{Lemma}]{\text{Gauss'}} \implies f_1(y) \mid g(y) \text{ in } A[y]$$

Thus, $M \subseteq f_1 A[y]$. $\quad M$ max $\implies M = f_1 A[y]$ contradiction. $\blacksquare$

Proposition

$M \in \operatorname{Max} k[x,y]$. Then, $\exists (a,b) \in \mathbb{A}^2(k)$ s.t. $M = \langle x-a, y-b \rangle$

Proof

M max ideal of $k[x,y]$ $\overset{\text{two lemmas ago}}{\Longrightarrow}$ M not principal

$\overset{\text{one lem ago \& since } k[x] \text{ UFD}}{\Longrightarrow}$ $P \triangleq M \cap k[x] \neq 0$.

Thus, $P = (x-a)\,k[x]$.

Let $\bar{M}$ be the ideal generated by the image of M in $k[x,y]/\langle x-a \rangle \cong k[y]$.

$\bar{M}$ is a maximal ideal of $k[x,y]/\langle x-a \rangle$.

The image of $\bar{M}$ in $k[y]$ is then generated by $y-b$. Thus,

$\bar{M} = (x-a)\,k[x,y] + (y-b)\,k[x,y]$.

$\blacksquare$

Theorem

$f \in k[x,y]$ irr. $M \in \operatorname{Max} C_f \iff$ it can be generated by the images in C_f of $x-a,\ y-b \in k[x,y]$ for some $(a,b) \in Z_f(k)$.

Proof

Let $I_f(a,b) = (x-a)C_f + (y-b)C_f$ for $(a,b) \in \mathbb{A}^2(k)$. $I_f(a,b) \in \operatorname{Max} C_f$.

If $I_f(a,b) = I_f(c,d) \Rightarrow I_f(a,b) \ni (x-a)-(x-c) = c-a \Rightarrow a=c$. So $b=d$.

Now, let $M \in \operatorname{Max} C_f$. $\tilde{M} \in \operatorname{Max} k[x,y]$ the corresponding ideal. $\exists (a,b) \in \mathbb{A}^2(k)$ s.t.

$\tilde{M} = (x-a)k[x,y] + (y-b)k[x,y]$. $f \in \tilde{M} \Rightarrow f(a,b) = 0 \Rightarrow Z_f(k) \ni (a,b) \Rightarrow I_f(a,b) = M$.