Hilbert basis Theorem

Thm. A = noeth ring. $\Rightarrow$ $A[x]$ is noeth.

$\Rightarrow$ $A[x_1,\ldots,x_n]$ is noeth.

pf. Suppose $F(x) = a_n x^n + \cdots + a_0$ nonzero, w/ $a_n \neq 0$.

Define $\mathrm{init}(F) = a_n x^n$, define $\mathrm{init}(0) = 0$.

If $I \subset A[x]$ ideal, define $\mathrm{init}(I)$ = additive subgroup gen by $\{\mathrm{init}(F) \mid F \in I\}$.

$\mathrm{init}(I)$ is an ideal: $\mathrm{init}(xF) = x\,\mathrm{init}(F)$

if $a\,\mathrm{init}(F) \neq 0$ for $a \in A$, then $a\,\mathrm{init}(F) = \mathrm{init}(aF)$.

Claim: If $I \subseteq J$ are ideals in $A[x]$ s.t. $\mathrm{init}(I) = \mathrm{init}(J)$, then $I = J$.

pf of claim: Suppose not, Then pick $F \in J \setminus I$ of lowest possible degree. Then $\mathrm{init}(F) \in \mathrm{init}(I)$, so $\exists\, G \in I$ s.t. $\mathrm{init}(G) = \mathrm{init}(F)$ but then $F - G \in J \setminus I$, but has smaller degree than F. $\rightarrow\leftarrow$

Suppose $A[x]$ not noeth. $\Rightarrow \exists$ $0 = I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq$ chain of ideals in $A[x]$.

$\Rightarrow$ $\mathrm{init}(I_1) \subsetneq \mathrm{init}(I_2) \subsetneq \cdots$ chain of ideals in $A[x]$.

For each i, pick $a_i x^{d_i} \in \mathrm{init}(I_i) \setminus \mathrm{init}(I_{i-1})$

~~By passing to subsequence~~, we may find $i_1 \le i_2 \le \cdots$

s.t. $d_{i_1} \le d_{i_2} \le \cdots$

Consider chain of ideals $(a_{i_1}) \subseteq (a_{i_1}, a_{i_2}) \subseteq \cdots$ in A

Chain stabilizes, so for some N, a_{i_n} generated by $a_{i_1}, \ldots a_{i_N}$ for all $n \ge N$

$\Rightarrow$ $a_{i_n} x^{d_{i_n}}$ gen by $a_{i_1} x^{d_{i_1}}, \dots, a_{i_N} x^{d_{i_N}}$ for all $n \geq N$

~~st~~ So $A[x]$ noeth.

For second $\Rightarrow$, use $A[x_1, \dots x_n] \cong (A[x_1, \dots x_{n-1}])[x]$. $\square$

Cor. A noeth ring, B f.g. A-algebra, Then B noeth.

Pf. $\exists n$ s.t. $B \cong \underset{\uparrow}{A[x_1, \dots, x_n]}/I$

noeth by basis Thm. $\square$

Hilbert Nullstellensatz

Lemma. let $A \subseteq B \subseteq C$ be rings.

Assume:
- A noeth
- C is f.g. as A-algebra
- C is f.g. as B-module

Then B is f.g. as A-algebra.

Pf. Idea: Find $A \subseteq B' \subseteq B$ s.t.
- B' is f.g. A-algebra
- C is f.g. B'-module.

Given that, B' is noeth by basis Thm.

$\Rightarrow$ C noeth B'-module

$\Rightarrow$ B is f.g. B'-module

$\Rightarrow$ B is f.g. A-algebra

let $x_1, \dots x_r \in C$ be A-algebra generators

$y_1, \dots, y_s \in C$ be B-module generators

$\Rightarrow$ $\exists b_{ij} \in B$ s.t. $x_i = \sum_{j=1}^{s} b_{ij} y_j$. $(*)$

Pick $z \in C$. Can write z as polynomial in x_i's:

$$z = \sum_I \alpha_I x^I \qquad (I = (i_1, \dots i_r),\ x^I = x_1^{i_1} \cdots x_r^{i_r})$$
$\alpha_I \in A$.

Use (*) can expand z as polynomial in y_j's w/ coeff. in B

$$z = \sum_J \beta_J y^J \qquad \beta_J \in B$$

Also, $\exists\ c_{ijk} \in B$ s.t. $y_i y_j = \sum_{k=1}^{s} c_{ijk} y_k$.

Using this, we can rewrite any product of y's as a linear combination of y's, coeff are in subring gen. by c_{ijk}.

$\Rightarrow$ z is linear comb. of $y_1, \dots y_s$ w/ coeff. in subring gen. by c_{ijk} & b_{ij}.

define this to be B'. $\square$

Thm. Hilbert nullstellensatz. Let $\mathbb{k} \subset E$ be field extension s.t. E is f.g. as $\mathbb{k}$-algebra. Then $\dim_{\mathbb{k}} E < \infty$.

Pf. Let $x_1, \dots x_n \in E$ be $\mathbb{k}$-algebra generators.

We may reorder so that x_i is transcendental over $\mathbb{k}(x_1, \dots x_{i-1})$ for $i = 1, \dots, r$ and x_j algebraic over $\mathbb{k}(x_1, \dots x_r) =: E'$ for $j = r+1, \dots n$.

$$\mathbb{k} \subset E' \subset E$$

Lemma $\Rightarrow$ E' is f.g. as $\mathbb{k}$-algebra.

If $r = 0$, we're done. Assume $r > 0$.

Let $\frac{f_1}{g_1}, \dots, \frac{f_m}{g_m}$ be $\mathbb{k}$-algebra generators for E',

$f_i, g_i \in \mathbb{k}[x_1, \dots x_r]$.

Note: $g_1 g_2 \cdots g_m \neq -1$

If equal, then $\frac{f_i}{g_i} = -f_i g_1 \cdots \hat{g_i} \cdots g_m \in \mathbb{k}[x_1, \ldots x_r]$

but these don't generate nontrivial rational functions $\rightarrow\leftarrow$

Define $h = g_1 \cdots g_m + 1 \ (\neq 0)$

Claim: $\frac{1}{h}$ is not generated by $\frac{f_1}{g_1} \cdots \frac{f_m}{g_m}$

If it were, then $\frac{1}{h} = \sum_I \alpha_I \left(\frac{f_1}{g_1}\right)^{i_1} \cdots \left(\frac{f_m}{g_m}\right)^{i_m}$ $\alpha_I \in \mathbb{k}$.

Clear denom: $\frac{g_1^{p_1} \cdots g_m^{p_m}}{h}$ = polynomial in $x_1, \ldots, x_r$

$\Rightarrow$ h divides $g_1^{p_1} \cdots g_m^{p_m}$ $\rightarrow\leftarrow$

$\square$

Hence $r=0$, so we're done

Cor. $\mathbb{k}$ field, $m \subset \mathbb{k}[x_1, \ldots x_n]$ maximal ideal.

Then $\mathbb{k} \rightarrow \mathbb{k}[x_1, \ldots x_n]/m$ is finite extension of fields.

In particular, if $\mathbb{k}$ alg. closed, then for every m $\exists\, \alpha_1, \ldots \alpha_n \in \mathbb{k}$

s.t. $m = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$.

Pf. $\mathbb{k}[x_1, \ldots x_n]/m$ is f.g. $\mathbb{k}$-algebra (generated by images of $x_1, \ldots x_n$)

Nullstellensatz $\Rightarrow$ $\mathbb{k} \subset \mathbb{k}[x_1 \ldots x_n]/m$ is finite extension.

If $\mathbb{k}$ alg. closed, then the composition $\mathbb{k} \rightarrow \mathbb{k}[x_1, \ldots x_n]/m$

has degree 1 as field extension. $\Rightarrow$ isomorphism

So in particular, $\exists!\ \alpha_1, \ldots \alpha_n \in \mathbb{k}$ that map to images of $x_1, \ldots x_n$. $\Rightarrow$ under $\mathbb{k}[x_1, \ldots x_n] \longrightarrow \mathbb{k}[x_1, \ldots x_n]/m$,

$x_i - \alpha_i$ map to 0, so belong to m.

But, $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ is already maximal ideal so must be equal to m. $\square$

Rmk. Suppose $\mathbb{k}$ alg. closed.

$$\begin{array}{ccc} \text{maximal ideals of } \mathbb{k}[x_1, \ldots x_n] & \longleftrightarrow & \mathbb{k}^n \\ \updownarrow & & \\ \text{closed points of } \mathrm{Spec}(\mathbb{k}[x_1, \ldots x_n]) & & \end{array}$$