Noether normalization and Hilbert Nullstellensatz

Today: All rings are commutative.

Recall: For field extensions, finite $\Leftrightarrow$ finitely generated + algebraic

We need a version of this for rings.

Definition. Let $A \subseteq B$ be a subring. An element $x \in B$ is called integral over A (在A上整) if it satisfies an equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for some $a_0, \ldots, a_{n-1} \in A$

monic!

(Here, we don't have the notion of "minimal" polynomials.)

Proposition The following are equivalent

(1) $x \in B$ is integral over A (analogue of "algebraic" for extensions)

(2) $A[x]$ (= all elements in B that can be expressed by a polynomial in x) is a finitely generated A-module.

(3) $A[x]$ is contained in a subring C of B such that C is a finitely generated A-module.

Proof: (modeled on for field extensions, finite $\Leftrightarrow$ finitely generated + algebraic)

(1) $\Rightarrow$ (2) Say $x^n + a_{n-1}x^{n-1} + \cdots + a_n = 0$ for some $a_i \in A$

So each $x^{n+r} = -a_{n-1}x^{n+r-1} - \cdots - a_0 x^r$ $\Rightarrow$ $A[x]$ is generated by $1, x, \ldots, x^{n-1}$ as an A-module.

(2) $\Rightarrow$ (3) Take $C = A[x]$

(3) $\Rightarrow$ (1) Assume C is generated by $e_1, \ldots, e_n$ as an A-module

Consider $xe_j = a_{1j}e_1 + a_{2j}e_2 + \cdots + a_{nj}e_n$ for $a_{ij} \in A$

$$\rightsquigarrow (e_1, \ldots, e_n)\, x = (e_1, \ldots, e_n) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

$$\Rightarrow (e_1, \ldots, e_n) \cdot \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ \vdots & & \ddots & \\ -a_{n-1} & & & x - a_{nn} \end{pmatrix} = 0$$

Consider $f(x) = \det\left(- \right) \in A[x]$.

But $e_i \cdot f(x) = 0 \ \forall i = 1, \cdots, n \Rightarrow f(x)$ kills all elements in $C \Rightarrow f(x) = 0$. $\square$

<u>Corollary</u> Let $x_1, \cdots, x_n$ be elements of B, each integral over A. Then $A[x_1, \cdots, x_n]$ is a finitely generated A-module.

Proof: Say $x_i^{m_i} + a_{i,m_i-1} x_i^{m_i-1} + \cdots = 0$

$\Rightarrow A[x_1, \cdots, x_n]$ is generated as A-modules by $x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ for $0 \le \lambda_i \le m_i - 1 \ \forall i$. $\square$

<u>Corollary</u>: The set C of elements of B which are integral over A is a subring of B containg A.

Proof: Given $x, y \in C \Rightarrow A[x,y]$ is a finitely generated A-module

so $x \pm y$, $x \cdot y \in A[x,y]$ are integral over A.

<u>Definition</u>. This C is called the <u>integral closure</u> (整闭包) of A in B

* If $C = A$, we say A is <u>integrally closed</u> in B (A在B中整闭)
* If $C = B$, we say B is <u>integral over A</u> (B在A上整).

<u>Corollary</u> If $A \subseteq B \subseteq C$ are rings and if B is integral over A and C is integral over B, then C is integral over A.

Proof: Let $x \in C$, $\rightsquigarrow x^n + b_{n-1} x^{n-1} + \cdots + b_0 = 0$ with $b_0, \cdots, b_{n-1} \in B$

Consider the subring $B' = A[b_0, \cdots, b_{n-1}] \subseteq B$.

B' is a finitely generated A-module as all b_i are integral over A.

Then, $x \in \underbrace{B'[x]}_{\text{a finitely generated } A\text{-module}}$ is integral $/ A$.

$$\begin{tikzcd}
B'[x] \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & C \arrow[d, dash] \\
B' = A[b_0, \cdots, b_{n-1}] \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & B \arrow[dl, dash] \\
A &
\end{tikzcd}$$

<u>Corollary</u>. $A \subseteq B$ be rings and $C =$ integrally closure of A in $B \Rightarrow C$ is integrally closed in B.

Proof: If $x \in C$ is integral $/B \Rightarrow x$ is integral over $A \Rightarrow x \in C$. $\square$

Noether normalization.

- Let k be a field, and R a finitely generated k-algebra, i.e.

$$R = k[x_1, \cdots, x_n]/I \qquad \text{for some ideal } I.$$

Theorem. $\exists\, r \leq n$ and an injective homomorphism

$$\varphi : k[\underline{Y}] = k[Y_1, \cdots, Y_r] \hookrightarrow R \qquad (\text{viewing } k[Y_1, \cdots, Y_r] \text{ as a subring})$$

such that R is integral over $k[Y]$.

Proof: (Nagata) We prove the theorem by induction on n (Suppose all R' generated by $n-1$ elts ✓)

Now, R is generated by $x_1, \cdots, x_n$, i.e. $R = k[x_1, \cdots, x_n]/I$

If $I = (0)$, nothing to prove; take $Y_i = x_i$, $r = n$.

Now suppose $0 \neq f(\underline{x}) \in I$.

Take positive integers $r_2, \cdots, r_n$ and put

$$z_2 = x_2 - x_1^{r_2}, \quad z_3 = x_3 - x_1^{r_3}, \quad \cdots, \quad z_n = x_n - x_1^{r_n}$$

Then under the isomorphism

$$\begin{array}{ccc}
k[x_1, \cdots, x_n] & \simeq & k[x_1, z_2, \cdots, z_n] \\
\cup\!\! \mid & & \cup\!\! \mid \\
I & & \tilde{I} \\
\in & & \in \\
f(\underline{x}) & \longmapsto & f(x_1, z_2 + x_1^{r_1}, \cdots, z_n + x_1^{r_n}) =: \tilde{f}
\end{array}$$

Suppose $0 \ll r_2 \ll r_3 \ll \cdots \ll r_n \Rightarrow \tilde{f} = a \cdot x_1^N + (\text{terms of degree} < N)$ for $a \in k^\times$

So, $k[x_1, z_2, \cdots, z_n]/(\tilde{f})$ is integral over $k[z_2, \cdots, z_n]$.

Now,

$$\begin{tikzcd}
k[x_1, z_2, \cdots, z_n]/(\tilde{f}) \arrow[r, two heads] & k[x_1, z_2, \cdots, z_n]/\tilde{I} = R & \\
k[z_2, \cdots, z_n] \arrow[u, "\text{finitely generated module}"'] \arrow[r, two heads] \arrow[ur, phantom, "\Longrightarrow"] & k[z_2, \cdots, z_n]/\tilde{I} \cap k[z_2, \cdots, z_n] \arrow[u, "\text{finitely generated module}"'] & k[y_1, \cdots, y_r] \arrow[l, "\text{integral}"']
\end{tikzcd}$$

$\Rightarrow R$ is integral over $k[y_1, \cdots, y_r]$. $\square$

<u>Hilbert Nullstellensatz</u> (weak form) Assume that k is algebraically closed.

Every maximal ideal of $k[x_1,\dots,x_n]$ is of the form $(x_1-a_1,\dots,x_n-a_n)$

There's a bijection $\{\text{maximal ideals of } k[x_1,\dots,x_n]\} \longleftrightarrow k^n$

What if k is not algebraically closed?

E.g. In $\mathbb{R}[x]$, (x^2+1) is a maximal ideal

$$\underset{(x+i)(x-i)}{\overset{\|}{}} \quad \text{"correspond" to two points } x=i \text{ and } x=-i$$

conjugates

In general, we get
$$\begin{array}{ccc} (k^{alg})^n & \xrightarrow{\mathcal{M}} & \{\text{maximal ideals of } k[x_1,\dots,x_n]\} \\ \Psi & & \\ \underline{a}=(a_1,\dots,a_n) & \longmapsto & m_{\underline{a}} := \ker\left(k[x_1,\dots,x_n] \xrightarrow{ev_{\underline{a}}} k(a_1,\dots,a_n) \subseteq k^{alg}\right) \\ & & x_i \longmapsto a_i \end{array}$$

<u>Theorem</u>. All maximal ideals of $k[x_1,\dots,x_n]$ arise this way.

But $\mathcal{M}$ is not one-to-one. For each $\sigma \in \mathrm{Gal}(k^{alg}/k) = \mathrm{Aut}(k^{alg}/k)$, we have

$$\begin{tikzcd} k[x_1,\dots,x_n] \arrow[r, "ev_{\underline{a}}"] \arrow[rr, bend right, "ev_{\sigma(\underline{a})}"'] & k^{alg} \arrow[r, "\sigma", "\simeq"'] & k^{alg} \end{tikzcd}$$

$\rightsquigarrow$ get $\ker ev_{\underline{a}} = \ker ev_{\sigma(\underline{a})}$.

<u>Claim</u>: $\mathcal{M}$ induces a bijection between $\mathrm{Gal}(k^{alg}/k)$-orbits on $(k^{alg})^n$ and maximal ideals.

<u>Proof</u>: Have seen $\ker ev_{\underline{a}} = \ker ev_{\sigma(\underline{a})}$.

Conversely, if $\ker ev_{\underline{a}} = \ker ev_{\underline{b}} = m$,

$$\begin{tikzcd} k[x_1,\dots,x_n] \arrow[r, two heads] & k[x_1,\dots,x_n]/m \arrow[d, "\wr\,\eta"] \simeq k(\underline{a}) \arrow[d, dashed, "\simeq\,\eta"] \subseteq k^{alg} \arrow[d, dashed, "\text{extend to } \tilde{\eta}: k^{alg} \xrightarrow{\sim} k^{alg}"] \\ k[x_1,\dots,x_n] \arrow[r, two heads] & k[x_1,\dots,x_n]/m = k(\underline{b}) \subseteq k^{alg} \end{tikzcd}$$

So $\underline{a} = \eta(\underline{b})$. $\square$

Lemma Let R be a field, and $S \subseteq R$ be a subring such that R is integral over S.

Then S is a field (and hence R is an algebraic extension of S.)

$$\begin{array}{l} R - \text{field.} \\ \big| \text{ integral} \\ S \end{array}$$

Proof: Clearly, S is an integral domain. Suffices to prove that $s \in S \Rightarrow s^{-1} \in S$.

Note $s^{-1} \in R$ is integral over S

$$\Rightarrow s^{-n} + b_{n-1} s^{1-n} + \cdots + b_1 s^{-1} + b_0 = 0$$

$$\Rightarrow s^{-1} = -b_{n-1} - b_{n-2} s - \cdots - b_0 s^{n-1} \in S. \quad \square$$

Nullstellensatz (Weak) Let k be a field. Then every maximal ideal of $k[x_1, \cdots, x_n]$ is of the form

* a finite extension ℓ of k
* $\underline{a} = (a_1, \cdots, a_n) \in \ell^n$
* the maximal ideal $m_{\underline{a}} = \ker \left(\begin{array}{c} k[x_1, \cdots, x_n] \longrightarrow \ell \\ x_i \longmapsto a_i \end{array} \right)$

In particular, when k is algebraically closed $\Rightarrow \ell = k$ and all maximal ideal $m_{\underline{a}} = (x_1 - a_1, \cdots, x_n - a_n)$

Proof: Let m be a maximal ideal

Consider
$$\begin{tikzcd} k[x_1, \cdots, x_n] \arrow[r, two heads] & k[x_1, \cdots, x_n]/m = \text{a field} \\ & k[y_1, \cdots, y_r] \arrow[u, "\text{integral (by Noether normalization)}"'] \end{tikzcd}$$

Lemma $\Rightarrow k[y_1, \cdots, y_r]$ is a field $\Rightarrow r = 0$

Thus, $k[x_1, \cdots, x_n]/m$ is an algebraic extension of $k \Rightarrow$ finite extension.

Write $\ell := k[x_1, \cdots, x_n]/m$, put a_i = image of x_i in $k[x_1, \cdots, x_n]/m = \ell$

So $m = \ker \left(\begin{array}{c} k[x_1, \cdots, x_n] \longrightarrow \ell \\ x_i \longmapsto a_i. \end{array} \right) \quad \square$

Nullstellensatz (strong form) k = algebraically closed.

For an ideal $I \subseteq k[x_1, \dots, x_n]$, $I(Z(I)) = \sqrt{I}$.

Proof: It is clear that $\sqrt{I} \subseteq I(Z(I))$

b/c if $f \in \sqrt{I} \Rightarrow f^n \in I$ for some n, then $\forall x \in Z(I)$, $f^n(x) = 0 \Rightarrow f(x) = 0$

So $f \in I(Z(I))$.

Conversely, we want to show $I(Z(I)) \subseteq \sqrt{I}$.

note: We don't need I to be finitely generated in this proof, although it is true that I is always finitely generated.

i.e. if $I = (f_1, \dots, f_m)$, if $g \in k[x_1, \dots, x_n]$ satisfies

$$\left[\{f_1(\underline{a}) = \dots = f_m(\underline{a}) = 0\} \overset{(*)}{\Rightarrow} g(\underline{a}) = 0\right] \Longleftrightarrow \{\underline{a} \mid f_1(\underline{a}) = \dots = f_m(\underline{a}) = 0, \underbrace{g(\underline{a}) \neq 0}_{\Updownarrow \ \exists b \text{ s.t. } g(\underline{a}) \cdot b = 1}\} = \emptyset.$$

then there exists $l \in \mathbb{N}$ s.t. $g^l \in (f_1, \dots, f_m)$.

Consider the ideal $J = I \cdot k[x_1, \dots, x_n, x_{n+1}] + (1 - g \cdot x_{n+1})$ in $k[x_1, \dots, x_{n+1}]$

Case 1: $J \neq (1)$. Then J is contained in a maximal ideal $M \subseteq k[x_1, \dots, x_{n+1}]$

By weak Nullstellensatz, $M = (x_1 - a_1, \dots, x_{n+1} - a_{n+1})$ for some $a_i \in k$.

Under the map $\varphi: k[x_1, \dots, x_{n+1}] \twoheadrightarrow k[x_1, \dots, x_{n+1}]/M = k$

$$f_i \in J \quad 0 \overset{\text{as}}{=} \varphi(f_i) = f_i(a_1, \dots, a_n) \quad \forall i \quad \xRightarrow{\text{by } (*)} g(a_1, \dots, a_n) = 0$$

$$1 - g x_{n+1} \in J \quad 0 \overset{\text{as}}{=} \varphi(1 - g x_{n+1}) = 1 - g(a_1, \dots, a_n) \cdot a_{n+1} \Rightarrow 0 = 1 - 0. \quad \text{※}.$$

Case 2: $J = (1)$. So there are polynomials $h_1, \dots, h_{m+1} \in k[x_1, \dots, x_{n+1}]$

$$\Rightarrow 1 = h_1 f_1 + \dots + h_m f_m + (1 - g \cdot x_{n+1}) h_{m+1} \quad \text{in } k[x_1, \dots, x_{n+1}].$$

In $k(x_1, \dots, x_n)$, substitute $x_{n+1} = g^{-1}$ gives

$$1 = (h_1 f_1 + \dots + h_m f_m)(x_1, \dots, x_n, g^{-1})$$

Clearing denominators $\Rightarrow$ $g^l = h_1^* f_1 + \dots + h_m^* f_m$, for some new polynomials h_i^*

$$\Rightarrow g \in \sqrt{I}.$$

Nullstellensatz (continued) There is a one-to-one bijection between

$$\{\text{Algebraic subsets of } k^n\} \longleftrightarrow \{\text{radical ideals of } k[x_1,\dots,x_n]\}$$

$$Z \longmapsto I(Z)$$

$$Z(I) \longleftarrow I$$

Moreover (1) $I_1 \subseteq I_2 \iff Z(I_1) \supseteq Z(I_2)$

(2) $Z(I_1+I_2) = Z(I_1) \cap Z(I_2)$

(3) $Z(I_1 \cap I_2) = Z(I_1) \cup Z(I_2)$

Proof: Need to show $I(Z(I)) = I$ if I is radical. (just proved)

If $Z = Z(J)$, $Z(I(Z)) = Z$

may assume $J = \sqrt{J}$ b/c $Z(J) = Z(\sqrt{J})$ $(f^n(x)=0 \Rightarrow f(x)=0)$

b/c $Z(I(Z(J))) \overset{?}{=} Z(J)$ ✓.

(1) and (2) obvious

(3) Clearly, $Z(I_1) \subseteq Z(I_1 \cap I_2)$, $Z(I_2) \subseteq Z(I_1 \cap I_2)$

Conversely, if $z \notin Z(I_1) \cup Z(I_2)$ then $\exists f_1 \in I_1, f_2 \in I_2 \Rightarrow f_1(z) \neq 0, f_2(z) \neq 0$

So $f_1 f_2 \in I_1 \cap I_2$ and $(f_1 f_2)(z) \neq 0 \Rightarrow z \notin Z(I_1 \cap I_2)$ $\square$