Algebra

May 5, 2017

0.1 The equivalence of algebra and geometry

In the following, k will be an algebraically closed field.

Def 1. The category of affine algebraic sets $\mathcal{G}$, which its objects and morphisms are defined as following.

objects: The objects are affine algebraic sets in k^n.

An **affine algebraic set** is the common zero set of $\{F_i\}_{i\in\Lambda} \subset k[x_1,\ldots,x_n]$ in k^n. We denote it by $V = \mathcal{V}(\{F_i\}_{i\in\Lambda}) \subset k^n$. (In fact, $I = \langle F_i : i \in \Lambda\rangle$ is Noetherian, so $I = \langle F_1,\ldots,F_n\rangle$ and $V = \mathcal{V}(I)$.)

morphisms: The morphisms are the polynomial map from k^n to k^m.

A **polynomial map** is a mapping as following:

$$\begin{aligned} k^n &\longrightarrow k^m \\ \alpha &\longmapsto (F_1(\alpha),\ldots,F_m(\alpha)) \end{aligned}$$

where each F_i is a polynomial in $K[x_1,\ldots,x_n]$.

Given two affine algebraic sets $V \subset k^n$ and $W \subset k^m$, if a map $F : V \to W$ is the restriction of a polynomial map from k^n to k^m, then F is a morphism from V to W.

Moreover, if $F : V \to W$ and $G : W \to V$ satisfy $F \circ G = \mathrm{Id}$ and $G \circ F = \mathrm{Id}$, then we say $V \cong W$.

Def 2. The category of finitely generated reduced k-algebra $\mathcal{A}$, which its objects and morphisms are defined as following.

objects: The objects are the reduced finitely generated k-algebra R.

A finitely generated k-algebra R is reduced if R has no non-zero nilpotent elements.

morphisms: The morphisms are the k-algebra homomorphisms.

Eg 0.1.1. It is easy to see that $\mathcal{V}(0) = k^n$ and $\mathcal{V}(1) = \varnothing$.

0.1.1 One-one correspondence between affine algebraic sets and radical ideals

Def 3. Define $\mathcal{I}(V) = \{\, f \in k[x_1,\ldots,x_n] \mid f(\alpha) = 0, \forall\, \alpha \in V \,\}$.

The one-one correspondence is given by

$$\begin{aligned} \{\,\text{affine algebraic sets in } \mathbb{A}^n_k\,\} &\longleftrightarrow \{\ \text{radical ideals in } k[x_1,\ldots,x_n]\,\} \\ V &\longmapsto \mathcal{I}(V) \\ \mathcal{V}(I) &\longmapsfrom I \end{aligned}$$

Prop 0.1.1.

- $\sqrt{\mathcal{I}(V)} = \mathcal{I}(V)$.

  Proof. For all $f^n \in \mathcal{I}(V)$, $f^n(\alpha) = 0, \forall\, \alpha \in V \implies f(\alpha) = 0, \forall\, \alpha \in V$. Thus $f \in \mathcal{I}(V)$. □

- If V is an affine set, then $\mathcal{V}(\mathcal{I}(V)) = V$.

  Proof. "$\supset$": $\forall\, \alpha \in V$, $f \in \mathcal{I}(V)$, $f(\alpha) = 0 \implies \alpha \in \mathcal{V}(\mathcal{I}(V))$.
  "$\subset$": Since V is an affine set, $V = \mathcal{V}(I)$, then $I \subset \mathcal{I}(V)$, so $\mathcal{V}(\mathcal{I}(V)) \subset \mathcal{V}(I) = V$. □

Lemma 1. Given $T/S/R$, a tower of rings. If R is Noetherian, T/S is a module finite and T/R is a ring finite, then S/R is a ring finite.

Proof. Let $T = R[a_1, \dots, a_n] = S\omega_1 + \cdots + S\omega_m$. Then $a_i = \sum_j r_{i,k}\omega_k$ for some $r_{i,k}$ and $\omega_{i,j} = \sum t_{i,j,k}w_k$ for some $t_{i,j,k}$.

Let $S' = R\big[\{ r_{i,k} \}, \{ t_{i,j,k} \}\big] \subseteq S$, which is Noetherian by the Hilbert basis theorem (R Noetherian $\implies$ $R[x]$ Noetherian). Thus $T = S'\omega_1 + \cdots + S'\omega_m$ is a Noetherian S'-module by the fact that finitely generated module over a Noetherian ring is a Noetherian module.

Since $S \subset T$, S is a finitely generated S' submodule, so $S = S'v_1 + \cdots + S'v_r = R\big[\{ r_{i,k} \}, \{ t_{i,j,k} \}, \{ v_i \}\big]$. □

Lemma 2. If $S = k(z_1, \dots, z_p)$, $p > 0$ with each z_i transcendental, then S/k is not ring finite.

Proof. If not, say $S = k[f_1, \dots, f_n]$ with $f_i = g_i/h_i$, $g_i, h_i \in k[z_1, \dots, z_p]$. Then for any irreducible polynomial p such that $p \nmid h_i$ for each h_i (This polynomial exists since for each h_i there are only finite degree 1 factors). Then $1/p \notin k[f_1, \dots, f_n]$ by checking the divisibility of the denominator under addition and multiplication, which leads to a contradiction. □

Lemma 3. If A/k is an extension of fields and ring finite, then A/k is algebraic.

Proof. If A/k is transcendental and let $\{ z_1, \dots, z_t \}$ be a transcendental base. Then $A/k(z_1, \dots, z_t)$ is algebraic, thus a module finite. By lemma 1, $k(z_1, \dots, z_t)$ is ring finite, which contradict with lemma 2. □

Theorem 1 (Weak form of Hilbert Nullstellensatz)**.**

$$I \subsetneq k[x_1, \dots, x_n] \implies v(I) \neq \varnothing$$

Proof. Since I proper, by lemma **??**, exists a maximal ideal M such that $I \subseteq M$. Consider $K \triangleq k[x_1, \dots, x_n]/M = k[\bar{x}_1, \dots, \bar{x}_n]$. By proposition **??**, K is a field, and by lemma 3, K/k is algebraic. Since k is already algebraically closed, $K = k$ and hence each $\bar{x}_i \in k$. Let $\alpha \triangleq (\bar{x}_1, \dots, \bar{x}_n) \in A_k^n$, then for any $f \in M$, $f(\alpha) = f(\bar{x}_1, \dots, \bar{x}_n) = \bar{f} = 0$, thus $\alpha \in \mathcal{V}(M) \subseteq \mathcal{V}(I)$. □

Theorem 2 (Strong form of Hilbert Nullstellensatz)**.** $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$

Proof. "$\supset$": If $f^n \in I$, then $f(\alpha) = 0, \forall\, \alpha \in \mathcal{V}(I) \implies f^n(\alpha) = 0, \forall\, \alpha \in \mathcal{V}(I)$, thus $f^n \in \mathcal{I}(\mathcal{V}(I))$.

"$\subset$": If $\mathcal{I}(\mathcal{V}(I)) = 0$, then $I \subseteq \sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(I)) = 0$, thus $I = 0$.

Otherwise, exists $0 \neq f \in \mathcal{I}(\mathcal{V}(I))$, Let $J = \langle I, ft - 1 \rangle \subset k[x_1, \dots, x_n, t]$. If $(a_1, \dots, a_n, t_0)$ is a zero of J, then $ft - 1 \in J \implies -1 = f(a_1, \dots, a_n)t_0 - 1 = 0$, which is a contradiction, so by theorem 1, $J = k[x_1, \dots, x_n, t]$.

Write $1 = \sum h_i f_i + s(ft - 1)$, where each $f_i \in I$ and $h_i, s \in k[x_1, \dots, x_n, t]$. This is a equation of variables, so if we set $t = 1/f$, the equation still holds. Now each h_i would be the form $\sum p_i/f^{k_i}$, so we could multiply each side by a suitable f^ρ and get $f^\rho = \sum c_i f_i$ with each $c_i \in k[x_1, \dots, x_n]$. This implies $f^\rho \in I$, thus $f \in \sqrt{I}$. □

Def 4. Let $V \in \mathcal{G}$, the coordinate ring of V is $k[V] \triangleq k[x_1, \dots, x_n]/\mathcal{I}(V)$

0.1.2 Equivalence of $\mathcal{G}$ and $\mathcal{A}$

We define a functor F from $\mathcal{G}$ to $\mathcal{A}$ by

$$\begin{aligned} F: \quad \mathcal{G} &\longrightarrow \mathcal{A} \\ V &\longmapsto k[V] \end{aligned}$$

And For a polynomial map $f : V \to W$, define

$$\begin{aligned} F(f) = f^*: \quad k[W] &\longrightarrow k[V] \\ g &\longmapsto g \circ f \end{aligned}$$

Conversely, define a functor G by

$$\begin{aligned} G: \qquad \mathcal{A} &\longrightarrow \mathcal{G} \\ k[x_1, \ldots, x_n]/I &\longmapsto \mathcal{V}(I) \end{aligned}$$

Then if

$$\begin{aligned} \varphi: \quad k[\ldots]/I &\longrightarrow k[\ldots]/J \\ \bar{x}_i &\longmapsto \bar{f}_i \end{aligned}$$

Define

$$\begin{aligned} G(\varphi) = \psi: \qquad \mathcal{V}(J) &\longrightarrow \mathcal{V}(I) \\ \alpha = (a_1, \ldots, a_m) &\longmapsto (f_1(\alpha), \ldots, f_n(\alpha)) \end{aligned}$$

0.2 Gröbner basis

0.2.1 Division algorithm in $K[X_1, \ldots, X_n]$

Eg 0.2.1. $I = \langle xy - 1, y^2 - 1\rangle \subseteq K[x, y]$, $f_1 = xy - 1$ and $f_2 = y^2 - 1$ $G = \{f_1, f_2\}$. Does $f = x^2y + xy^2 + y^2 \in I$?

- Choose a lexicographic monomial ordering: $x > y$
- The multidegree $\partial(f) = (2, 1)$, $\partial(f_1 = (1, 1))$, $\partial(f_2) = (0, 2)$
- The leading term $LT(f) = x^2y$, $LT(f_1) = xy$, $LT(f_2) = y^2$
- $LT(f) = xLT(f_1) \Rightarrow f = xf_1 + xy^2 + y^2 + x \Rightarrow f = \underset{h_1}{(x+y)}f_1 + \underset{h_2}{(1)}f_2 + \underset{\bar{f}^G}{(x+y+1)}$ or $f = \underset{h_1}{x}f_1 + \underset{h_2}{(x+1)}f_2 + \underset{\bar{f}^G}{(2x+1)}$.

Note: Divisor h_1, h_2 and remainder $\bar{f}^G$ are not unique!!

Def 5. Fix a monomial ordering and let I be an ideal of $K[X_1, \ldots, X_n]$. The ideal of leading terms in I is defined to be $LT(I) = \langle LT(f) | f \in I\rangle$.

Remark 1. Let $I = \langle f_1, \ldots, f_n\rangle$. In general, $\langle LT(f_1), \ldots, LT(f_n) \subsetneq LT(I)$.

Eg 0.2.2. Let $f_1 = xy^2 + y$, $f_2 = xy^2$. And, $xf_1 + yf_2 = xy \in \langle f_1, f_2\rangle$ but $xy \notin \langle xy^2, x^2y\rangle$.

Def 6. $G = \{ g_1, \ldots, g_m \}$ is called a Gröbner basis of I if $I = \langle g_1, \ldots, g_m\rangle$ and $LT(I) = \langle LT(g_1), \ldots, LT(g_m)\rangle$

Prop 0.2.1. $LT(I) = \langle LT(g_1), \ldots, LT(g_m)\rangle \Rightarrow I = \langle g_1, \ldots, g_m\rangle$

Proof. $\forall\, f \in I$, do division process. Then $f = \sum_{i=1}^{m} h_i g_i + r$, either $r = 0$ or $\bigstar$ = no term of r is divisible by any of $LT(g_1), \ldots, LT(g_m)$. Assume $r \neq 0$, then $r = f - \sum_{i=1}^{m} h_i g_i \in I \Rightarrow LT(r) \in LT(I) = \langle LT(g_1), \ldots, LT(g_m)\rangle$, a contradiction. Hence, r = 0 (i.e. $f \in \langle g_1, \ldots, g_m\rangle$). □

Theorem 3. Eaach ideal I has a Gröbner basis.

Proof. By Hilbert basis thm, $LT(I) = \langle f_1, \ldots, f_m\rangle$ for some f_i's. Write $f_i = \sum_{j=1}^{m_i} h_{ij} LT(g_{ij})$ $h_{ij} \in K[X_1, \ldots, X_m j]$, $g_{ij} \in I$. Then $LT(I) = \langle LT(g_{ij})\rangle$ $i = 1, \ldots, m$ $j = 1, \ldots, m_i$. □

Theorem 4. Let $G = \{ g_1, \ldots, g_m \}$ be a Gröner basis of I, then

- $\forall\ \in K[X_1, \ldots, X_n]$, $f = f_I + r$ where f_I, r are unique.

  Proof. By division algorithm, $f = \underset{\bigstar}{f_I + r} = \underset{\bigstar}{f'_I + r'}$, then $\underset{\bigstar}{r - r'} = f_I - f'_I$. But if $r - r' \neq 0$, then $LT(r - r') \in LT(I) = \langle LT(g_1, \ldots, g_2)\rangle$, a contradiction. Hence, $r - r' = 0 \Rightarrow f_I = f'_I$. □

- $f \in I \iff r = 0$.

  Proof. Suppose $f \in I$, then $f = \underset{\bigstar}{f_I + r}$, and if $r \neq 0$ $\underset{\bigstar}{r} = f - f_I \in I$, a contradiction. Hence, r = 0. Conversly, if $r = 0$, $f = f_I \in I$. □

0.2.2 Buchberger's algorithm

Def 7. Let $f, g \in K[X_1, \ldots, X_n]$ and M be the monic least common multiple of LT(f) and LT(g). $S(f,g) = \frac{M}{LT(f)}f - \frac{M}{LT(g)}g$ is called an S-polynomial of f, g.

Let $I = \langle g_1, \ldots, g_m \rangle$ and $G = \{ g_1, \ldots, g_m \}$. A Gröner basis of I can be constructed by the following algorithm:

1. Initially let $G_0 \leftarrow G$.
2. Repeatly construct $G_{i+1} \leftarrow G_i \cup \big(\{ S(f,g) \mod G_i \mid f, g \in G_i \} \backslash \{ 0 \} \big)$, until once $G_{i+1} = G_i$, then G_i is a Gröner basis.

Lemma 4. Let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ with $a_1, \ldots, a_m \in K$ satisfy $\partial(f_1) = \partial(f_2) = \cdots = \partial(f_m) = \alpha$ and $h = \sum_{i=1}^m a_i f_i$ with $\partial(h) < \alpha$. Then $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$ for some $b_i \in K$.

Proof. Write $f_i = c_i f_i'$ with $c_i \in K$ and f_i' being monic of multidegree $= \alpha$. Note: $S(f_i, f_j) = f_1' - f_2'$. Then,

$$\begin{aligned} h &= \sum_{i=1}^{m} (a_i c_i f_i') \\ &= a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \cdots + (a_1 c_1 + \cdots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') \\ &\quad + (a_1 c_1 + \cdots + a_m c_m) f_m' \\ &= \sum_{i=2}^{m} b_i S(f_{i-1}, f_i) + b_{m+1} f_m' \text{ with } b_i = \sum_{1}^{i-1} a_1 c_1. \end{aligned} \tag{1}$$

Also, $b_{m+1} = 0$, since $\partial(h) < \alpha$, $\partial(\sum_{i=2}^{m} b_i S(f_{i-1}, f_i)) < \alpha$ and $\partial(f_m') = \alpha$. Then, we have $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$. □

Theorem 5 (Buchberger's criterion)**.** Assume $I = \langle g_1, \ldots, g_m \rangle$, then $G = \{ g_1, \ldots, g_m \}$ is a Gröbner basis of $I \iff S(g_i, g_j) \equiv 0 \pmod{G}$ for each i, j.

Proof.

· Suppose G is a Gröbner basis of I. $S(g_i, g_j) \in I \Rightarrow S(g_i, g_j) = 0$ by thm 4.

· Converely, suppose $S(g_i, g_j) \equiv 0 \pmod{G}$ $\forall\, i, j$. For $f \in I$, $f \underset{not\ division}{=} \sum_{i=1}^{m} h_i g_i$ for some $h_i \in K[X_1, \ldots, X_2]$. Define $\alpha = max\{\partial(h_1 g_1), \ldots, \partial(h_m g_m)\}$. We have $\partial(f) \leq \alpha$ and we can select an expression $f = \sum_{i=1}^{m} h_i g_i$ for f s.t α is minimal.

Claim: $\partial(f) = \alpha$

(pf) Rewrite,

$$\begin{aligned} f &= \sum_{i=1}^{m} h_i g_i \\ &= \sum_{\partial(h_i g_i) = \alpha} h_i g_i + \sum_{\partial(h_i g_i) < \alpha} h_i g_i \\ &= \sum_{\partial(h_i g_i) = \alpha} LT(h_i) g_i + \sum_{\partial(h_i g_i) = \alpha} (h_i - LT(h_i) g_i) + \sum_{\partial(h_i g_i) < \alpha} h_i g_i \end{aligned} \tag{2}$$

Let $LT(h_i) = a_i h_i^0$ with h_i^0 being a monic monomial. Comparing the multidegree on both side, $\partial\left(\sum_{\partial(h_i g_i) = \alpha} a_i h_i^0 g_i \right) < \alpha$ By lemma 4, $\sum_{\partial(h_i g_i) = \alpha} \left(a_i h_i^0 g_i \right) = c_{12} S(h_{i_1}^0 g_{i_1}, h_{i_2}^0 g_{i_2}) + \ldots$ (finite) where

$\partial(h_{i_1}g_{i_1}) = \partial(h_{i_2}g_{i_2}) = \cdots = \alpha$. By def, if we set $\beta_{st} = M_{st} =$ the monic lcm of $LT(g_{i_s}), LT(g_{i_t})$, then

$$\begin{aligned} S(h^0_{i_s}g_{i_s}, h^0_{i_t}g_{i_t}) &= \frac{X^\alpha}{LT(h^0_{i_s}g_{i_s})}h^0_{i_s}g_{i_s} - \frac{X^\alpha}{LT(h_{i_t}g_{i_t})}h^0_{i_t}g_{i_t} \\ &= X^{\alpha-\beta_{st}}\left(\frac{X^{\beta_{st}}}{\cancel{h^0_{i_s}}\,LT(g_{i_s})}\cancel{h^0_{i_s}}g_{is} - \frac{X^{\beta_{st}}}{\cancel{h^0_{i_t}}\,LT(g_{i_t})}\cancel{h^0_{i_t}}g_{i_t}\right) \\ &= X^{\alpha-\beta_{st}}S\left(g_{i_s}, g_{i_t}\right) \\ &= X^{\alpha-\beta_{st}}\sum_{j=1}^{m} l_j g_j \text{ (by division)} \end{aligned} \tag{3}$$

Then, $\partial(l_j g_j) < \beta_{st} \Rightarrow \partial(f) \geq \alpha$. Therefore, $\partial(f) = \alpha \Rightarrow LT(f) = \sum_{\partial(h_i g_i)=\alpha} LT(h_i)LT(g_i) \Rightarrow LT(f) \in \langle LT(g_1, \ldots, LT(g_m\rangle$.

□

Theorem 6. The Buchberger's algorithm will terminate

Proof. .

- $\langle LT(G_i)\rangle \subsetneq \langle LT(G_{i+1})\rangle$ if $G_i \neq G_{i+1}$

$$G_i \neq G_{i+1} \Rightarrow \exists\, f, g \in G_i \text{ s.t. } S(f,g) \not\equiv 0 (\text{mod G}) \Rightarrow LT(S(s,g)) \notin \langle LT(G_i)\rangle$$

- $\langle LT(G_0)\rangle \subsetneq \langle LT(G_1)\rangle \subsetneq \ldots$ (Noetherian ACC condition).

□