Invariant theory

Problem: understand functions <u>invariant</u> under action of a group G.

- We will look at the case k a field & G acting on comm. k-alg

$$P = k[x_1, \dots, x_n] :$$

that is, we have a group hom

$$G \longrightarrow c\text{-}k\text{-}Alg(P,P)$$

$$g \longmapsto g.- : P \longrightarrow P$$

a k-alg hom

st. $e.f = f$ where $e \in G$ is unit &

$(g.h).f = g.(h.f)$ for $g,h \in G$.

- The <u>invariants</u> of the action are its fixpoints: those polys f s.t.

$$g.f = f \quad \forall g \in G.$$

- These form a <u>subalgebra</u> $P^G \overset{i}{\hookrightarrow} P$

Example - symmetric Functions

Symmetric group S_n acts on $\{x_1, \ldots, x_n\}$ by permuting elements.

Induces action of S_n on $K[x_1, \ldots, x_n]$ by permuting variables eg.

eg. $(12)(2x_1x_2^2+3) = 2x_2x_1^2+3$.

- Then P^{S_n} = K-alg. of symmetric functions.

Examples are the elementary symm. functions:

$$f_0 = 1$$

$$f_1 = x_1 + \ldots\ldots + x_n$$

$$f_2 = \sum_{1 \le i \le j \le n} x_i x_j$$

$$\vdots$$

$$f_n = x_1 . x_2 \ldots\ldots x_n$$

In fact, P^{S_n} is f.g. as a K-alg by the el. s.f.'s : in fact, each $f \in P^{S_n}$ is uniquely a lin comb of multiples of the esf.

Fundamental problem of invariant theory

- Determine whether ρ^G has a finite set of
- generators (ie. is a f.g. K-algebra).

We will show this is true in wide generality.

Firstly, we need to know something about graded K-algebras.

Graded algebras & homogenous polynomials

Def^n) A graded K-algebra A is a K-algebra together with a grading:
a decomposition $A = \bigoplus_{n \in \mathbb{N}} A_n$
where $A_n \leq A$ are K-submodules such that $1 \in A_0$ & if $a \in A_n$, $b \in A_m$ then $a.b \in A_{n+m}$.

The elts of A_n are called homogenous of degree n.

- A morphism $f: A \longrightarrow B$ of graded K-algebras is a K-alg map pres homog. components: ie $f(A_n) \subseteq B_n$ for $n \in \mathbb{N}$.

Example

$P = K[x_1, \dots, x_n]$ is a graded K-alg.

To see this, recall:

- a monomial is a product of the $x_1, \dots, x_n$ - eg. $x_1 x_2^2$.
- Each polynomial is uniquely a lin. comb. of monomials ~ ie. they form a basis for P as K-module.
- The degree of a monomial is sum of it's powers - eg. 3 in above example.
- A poly is homogenous of degree d if all it's monomials have degree d.

  eg. $x_1 x_2^2 + 4x_1x_2x_3 + 7x_6^3$ is homogenous of degree 3.
- let $P_d \subseteq P$ consist of homogenous polys of degree d; then as each poly. is a sum of hom. components, this makes P a graded K-algebra:

eg. $x_1x_2^2 + 7x_4 + 8x_9 + 4x_1x_2x_3 + 1$

$$= \underset{\substack{\Uparrow \\ P_0}}{1} + \underset{\substack{\Uparrow \\ P_1}}{(7x_4 + 8x_9)} + \underset{\substack{\Uparrow \\ P_3}}{(x_1x_2^2 + 4x_1x_2x_3)}$$

- Observe also that the action of S_n on P in previous example preserves the graded algebra structure :

eg (12) : $\underset{\underset{P_3}{\cap}}{x_1 x_2^2 + x_1 x_2 x_3} \longmapsto \underset{\underset{P_3}{\cap}}{x_2 x_1^2 + x_2 x_1 x_3}$

Exercise : let f be homogenous & $f = \sum g_i f_i$ where the f_i are homogenous. Show that $f = \sum_i \bar{g}_i f_i$ where $\bar{g}_i$ is homogenous of degree $\deg f - \deg f_i$.

(Hint : let $\bar{g}_i$ be the homog. component of g_i in degree $\deg f - \deg f_i$)

$$f = g_1 f_1 + g_2 f_2$$

$$g_1 = \bar{g}_1 + (g_1 - \bar{g}_1)$$
$$g_2 = \bar{g}_2 + (g_2 - \bar{g}_2)$$

$$f = \bar{g}_1 f_1 + (g_1 - \bar{g}_1) F_1 + \bar{g}_2 F_2 + (g_2 - \bar{g}_2) F_2$$

poly w/ zero comp of degree F

hom of deg f

so 0

Theorem (Hilbert's finite gen. of invariants)

Let K be a field of char 0 (eg. $\mathbb{R}$ or $\mathbb{C}$) & G a finite group acting on $P = K[x_1, \dots, x_n]$ such that the action respects the grading: ie. $g.- : P \to P$ maps P_d into P_d $\forall d \in \mathbb{N}$. Then P^G is a fin. gen. K-algebra.

Proof

- Consider the inclusion $i : P^G \hookrightarrow P$ of comm. K-algs.
- As this is a ring hom, we can view P as a P^G-module by restriction (ie $\lambda . p := i(\lambda) . p$) & $i : P^G \hookrightarrow P$ as a P^G-module map.
- The key is $\exists$ a P^G-module map
$$p : P \longrightarrow P^G \text{ with } pi = 1.$$
This is the averaging map:
$$p(a) = \frac{1}{|G|} \sum_{g \in G} g . a$$
which we will meet again in Maschke's Thm in group representation theory.
- As $g.-$ is **an abelian group homomorphism** so is the finite sum of such maps, hence so is p.

- To see p is a P^G-module map, let $b \in P^G$.

Then $p(b.a) = \frac{1}{|G|}\sum_g g.(b.a)$

$= \frac{1}{|G|}\sum_g (g.b).(g.a)$ as $g.-$ a K-alg hom.

$= \frac{1}{|G|}\sum_g b.(g.a)$ as $b \in P^G$

$= b.\frac{1}{|G|}\sum_g (g.a) = b.p(a)$

as required.

- To see $p(a) \in P^G$, let $h \in G$:

$h.p(a) = h.\frac{1}{|G|}\sum_g g.a$

$= \frac{1}{|G|}\sum_g h.(g.a)$ as $h.-$ K-mod map

$= \frac{1}{|G|}\sum_g (hg).a$ as G-action

$= \frac{1}{|G|}\sum_g g.a$ as elts hg run through all elts of G i.e. $h.- : G \to G$ is a bij^n of sets.

$= p(a)$.

- Finally, let $a \in P^G$ & consider

$pi(a) = \frac{1}{|G|}\sum_g g.a$

$= \frac{1}{|G|}\sum_g a = \frac{1}{|G|}|G|a = a$,

as required.

So far, we have P^G-module maps

$$\begin{tikzcd} P^G \arrow[r, "i"] \arrow[rr, bend right, "1"'] & P \arrow[r, "\rho"] & P^G \end{tikzcd}$$

where

$$\rho(a) = \frac{1}{|G|} \sum_{g \in G} g \cdot a$$

Remark: ρ also preserves homog. components of degree d since each $g \cdot -$ does & homog. comps of degree d closed under k-linear sums.

- Now let $I \subseteq P$ be the ideal generated by homogenous elements of P^G of degree >0: it contains sums $h_1 k_1 + \dots + h_m k_m$ where $k_i \in P^G$ is homogenous of degree >0 & $h_i \in P$

- As k is field, it is Noetherian; hence by Hilb. basis thm P is Noetherian. Hence I is finitely generated by finitely many sums as above. Hence can choose the generators $f_1, \dots, f_m$ to be homogenous elts of P^G of degree >0.

That is,

$$I = \{ h_1 f_1 + \cdots + h_m f_m : h_i \in P \}$$

- Now let $A \leq P^G$ be the <u>K-subalgebra</u> generated by $f_1, \ldots, f_m$.

<u>Will prove $A = P^G$.</u>

- Let $f \in P^G$. Must show $f \in A$.
  Write $f = \sum m_i f_i$ as sum of its homog comps.
  $\underset{K}{\rotatebox{90}{$\in$}}$

- As each g preserves homogenous components
  $\sum m_i f_i = g.\sum m_i f_i = \sum m_i\, g.f_i$ implies $f_i = g.f_i$
- Hence each $f_i \in P^G$ & if we can show these belong to A we will be done.
- So let $f \in P^G$ be homogenous.
  Must show $f \in A$.
- Argue by induction.
- If f has degree 0, $f = r.1 \in A$ as A a K-alg.
  $\underset{K}{\rotatebox{90}{$\in$}}$

- If $\deg f > 0$, then $f \in I$ so
$$f = \sum_{i=1}^{m} h_i . f_i = \sum_{i=1}^{m} f_i . h_i$$

- From the exercise, can assume h_i is homogeneous of degree $\deg f - \deg f_i < \deg f$.

- Applying $\rho : P \longrightarrow P^G$, since $f, f_i \in P^G$ & ρ a P^G-module map, we have
$$f = \rho(f) = \sum_{i=1}^{m} f_i \, \rho(h_i) = \sum_{i=1}^{m} \rho(h_i) f_i$$
where $\deg(\rho(h_i)) = \deg(h_i) < \deg(f)$.
But as $\rho(h_i) \in P^G$, then $\rho(h_i) \in A$ by induction.

- As each $f_i \in A$, then as A a k-alg, $f = \sum_{i=1}^{m} \rho(h_i) f_i \in A$ too. $\square$

Grobner bases

- So far, proved that if k is a Noetherian ring, then each ideal of $k[x_1, \dots, x_n]$ is of form $\langle f_1, \dots, f_n \rangle$ and described application of this.
- In computational settings, one often wants to ask questions like:

① is $f \in \langle g_1, \dots, g_n \rangle$?

- If k is a field, this has a simple solution in 1 variable.

  Indeed then each ideal is principal, so just have to check if $f \in \langle g \rangle$ –

  i.e. if g divides f.

Can do this using algorithm for division with remainder:

we consider $q = \dfrac{\text{leading term of } f}{\text{leading term of } g} = \dfrac{LTf}{LTg}$

if $\deg(g) \leq \deg(f)$.

Eg. $f = 2x^2+3x+4$, $g = x+1$ • $q = 2x^2/x = 2x$.

• Then $f = q.(g) + \underbrace{(f-qg)}_{r = f_1}$ where

$\deg(f_1) < \deg(f)$.

Then repeat with f_1 & g & continue with $f_2, \dots$ until $f_n = 0$ or lower deg than g.

Eg. $2x^2+3x+4 =$

$$2x(x+1) + (x+4)$$

$$x+4 = (x+1) + 3 \quad \rightarrow$$

$$2x^2+3x+4 = 2x(x+1) + (x+1)+3$$
$$= (2x+1)(x+1)+3.$$

Key to algorithm

- We can define the leading term LTf of $f(x)$.
- Implicitly uses ordering on monomials

$$\ldots > x^3 > x^2 > x > 1$$

- For $k[x_1, \ldots, x_n]$, let's write a poly as

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$$ so eg $X^{(1,0,3)}$ denotes $x_1 x_3^3$.

- Monomials are polys of form x^α.
- Need ordering on monomials.

E.g. lexicographic ordering:

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} > x_1^{\beta_1} \cdots x_n^{\beta_n} = x^\beta \text{ if } \exists i \text{ st}$$

$$\alpha_j = \beta_j \text{ all } j < i \ \& \ \alpha_i > \beta_i.$$

This is a total order on monomials that :

① $x^\alpha \geq x^\beta \Rightarrow x^\alpha x^\gamma \geq x^\beta x^\gamma$

② it is a well order (every subset has least elt).

Def) A monomial ordering is a total ordering $<$ on monomials sat ①, ②.

Given a monomial ordering $<$, consider non-zero $f = \sum_\alpha a_\alpha x^\alpha$

$$= a_\alpha x^\alpha + \sum_{\beta < \alpha} a_\beta x^\beta$$

Define

$LT(f) = a_\alpha x^\alpha$, $LM(f) = x^\alpha$, $LC(f) = a_\alpha$.

l. term   l. monomial   l. coefficient

- Now let us say that non-zero f is reducible by g if $LT(f)$ is divisible by $LT(g)$
- Otherwise irreducible by g.

- Then let $q = \frac{LT(f)}{LT(g)}$.

Then $f = qg + \underbrace{(f - qg)}_{\text{smaller leading monomial than } f}$.

- Similarly say non-zero f is reducible by $\{g_1, \ldots, g_k\} = G$ if it is reducible by some g_i; else irreducible.

Algorithm for deciding if $f \in I = \langle g_1, \dots, g_n \rangle$.

- Check if f is reducible by some g_i.
- If so, $f = \frac{LT(f)}{LT(g_i)} g_i + \left(f - \frac{LT(f)}{LT(g_i)} g_i\right)$

  set $f \mapsto f - \frac{LT(f)}{LT(g_i)} g_i$ & repeat
- Gives rise to sum

$$f = \sum_i k_i g_i + r$$

where r is G-irreducible.

- Write $f \to_G r$ if f reduces to r in this way.
- The algorithm will work well if G is a Grobner basis.

Def^n) A set of generators $g_1, \dots, g_n$ $I = \langle g_1, \dots, g_n \rangle$ for an ideal I is a Grobner basis if

$f \in I$ non-zero $\Rightarrow$ $LT(f)$ is divisible by $LT(g_i)$ for some i.

Proposition

Let $I = \langle g_1, \dots, g_n \rangle$ be a Gröbner basis.
Then $f \in I \iff f \to_G 0$.

~~Proof~~ Suppose $f \to_G 0$.

- Then $f = \sum_i k_i g_i + \underbrace{r}_{\text{irred.}} = \sum k_i g_i$
  so $f \in I$.

- Suppose $f \in I$.
  Then $r = f - \sum k_i g_i \in I$.
  If $r \neq 0$ then, by def of Grob. basis, it is reducible.
  Contradiction.
  Hence $r = 0$. $\square$

- The question then becomes : how do we find a Grobner basis for $I = \langle g_1, \dots, g_n \rangle$?
- One issue : given f, we might be able to reduce it via g_i & g_j,

$$\begin{tikzcd} & f - \frac{LT(f)}{LT(g_i)} g_i \\ f \arrow[ur, "g_i"] \arrow[dr, "g_j"'] & \\ & f - \frac{LT(f)}{LT(g_j)} g_j \end{tikzcd}$$

& it is natural to consider the difference

$$(*) \quad \boxed{\frac{LT(f)}{LT(g_i)} g_i - \frac{LT(f)}{LT(g_j)} g_j}$$

& ask whether it reduces $\to_G 0$.

Def^n) Given $g_i, g_j \in K[x_1, \dots, x_n]$ non-zero, let $S(g_i, g_j) = \frac{p}{LT(g_i)} \cdot g_i - \frac{p}{LT(g_j)} \cdot g_j$

where $p = LCM(LM(g_i), LM(g_j))$.

This is called the S-polynomial of g_i & g_j.

Remark) $S(g_i, g_j)$ divides $(*)$ as $p \mid LT(f)$.

Buchberger's criterion

$I = \langle g_1, \ldots, g_n \rangle$ is a Gröbner basis
$\iff$ $S(g_i, g_j) \longrightarrow_G 0$ all $i \neq j$

$\boxed{\text{No proof}}$

Algorithm for constructing Gröbner basis

① Compute $S(g_i, g_j)$ all $i \neq j$.
② If $S(g_i, g_j) \not\to_G 0$, add it to the basis.
- Now repeat ① & ② for the new basis.
- The process eventually stabilises, & the result is a Gröbner basis.

Remarks) • As $S(g_i, g_j) \in I$, adding them does not change the ideal I.
- The reason process stabilises is that if $S(g_i, g_j) \not\to_G 0$, then $LT(S(g_i, g_j)) \notin \langle LT(g_1), \ldots, LT(g_n) \rangle$ so by adding such polynomials, we create increasing sequence of ideals of leading terms, but as $K[x_1, \ldots, x_n]$ is Noetherian, it must stabilise.